HikCentral Professional Web Client

User Manual

Legal Information

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 of this Manual at the Hikvision website (***https://www.hikvision.com/***).

Please use this Manual with the guidance and assistance of professionals trained in supporting the Product.

Trademarks

HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.

Other trademarks and logos mentioned are the properties of their respective owners.

Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS MANUAL AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION 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, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.

YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR

PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.

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 Web Client

1.1 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 system activation, 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.

1.2 Introduction

The system is developed for central management of surveillance 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, 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.

Module	Introduction
System Management Service (SYS)	• Provides the unified authentication service for connecting with the clients and servers. • Provides the central management for the users, roles, permissions, devices, and services. • Provides the configuration interface for surveillance and management module.
Streaming Service (Optional)	Provides 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 connected to the system, such as live view, remote playback, PTZ control, and so on.

Chapter 2 Login

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

2.1 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 11 and above, Firefox 57 and above, Google Chrome 61 and above, Safari 11 and above (running on Mac OS X 10.3/10.4).

Note

You should run the web browser as administrator.

2.2 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.

2.2.1 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.

Steps

1. In the address bar of the web browser, enter the address of the PC running SYS service and press **Enter** key.

Example

If the IP address of PC running SYS 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 SYS. For details, refer to ***Set Transfer Protocol*** .
- You should set the SYS's IP address before accessing the SYS 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 change your password regularly, especially in the high security system, changing 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 → Normal → User Preference** . See ***Set User Preference*** for details.

2.2.2 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.

Steps

1. In the address bar of the web browser, input the address of the PC running SYS service and press the **Enter** key.

   Example

   If the IP address of PC running SYS 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 SYS's IP address in WAN Access of System Configuration before accessing the SYS 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 **Log In** 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.

2.3 Login via Web Client

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

Steps

1. In the address bar of the web browser, input the address of the PC running SYS service and press **Enter** key.

   Example

   If the IP address of PC running SYS 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 SYS's IP address in WAN Access of System Configuration before accessing the SYS via WAN. For details, refer to ***Set WAN Access*** .

2. Enter the user name and password.
3. Click **Log In** 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.

2.4 Change Password for Reset User

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

Steps

1. In the address bar of the web browser, enter the address of the PC running SYS service and press **Enter** key.

   Example

   If the IP address of PC running SYS 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 SYS's IP address in WAN Access of System Configuration before accessing the SYS via WAN. For details, refer to ***Set WAN Access*** .

2. Enter the user name and initial password set by the administrator.
3. Click **Log In** 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.

2.5 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 change your password regularly, especially in the high security system, changing 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 3 Download Mobile Client

On the login page of Web Client, you can scan the QR code to download the Mobile Client that is used for accessing the system via mobile terminal (e.g., mobile phone).

Perform this task when you need to download the Mobile Client.

Note

You can also search and download the Mobile Client in the App Store or Google Play.

Steps

1. In the address bar of the web browser, enter the address of the PC running SYS service and press **Enter** key.

   Example

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

   Note

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

2. Scan the corresponding QR code with your mobile terminal to download the Mobile Client.

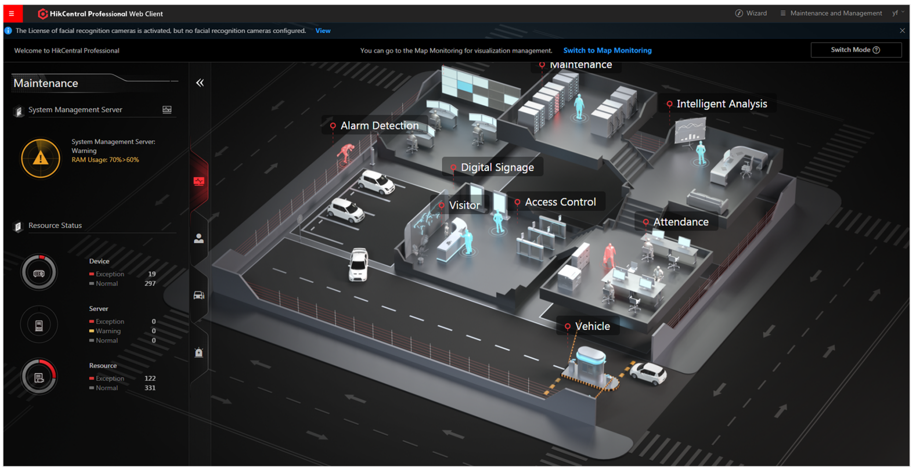
Chapter 4 Web Control

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 5 Home Page Overview

The Home page of the Web Client provides an overview of navigation and menu about the function modules. It contains several sections for the modules, such as Navigation, Overview Panel, Map Configuration on Home Page, Wizard, Maintenance and Management, Mode Switch, etc. You can access the modules you want quickly and conveniently via the Home page.

The HikCentral Professional Web Client is composed of the following modules.



The License of facial recognition cameras is activated, but no facial recognition cameras configured.

Welcome to HikCentral Professional

You can go to the Map Monitoring for visualization management.

System Management Server: Warning
RAM Usage: 70%>60%

Device	
Exception	19
Normal	297

Server	
Exception	0
Warning	0
Normal	0

Resource	
Exception	122
Normal	331

Figure 5-1 Modules on Home Page

Table 5-1 Modules on Home Page

Section	Module	Description
Navigation Icon		The navigation bar shows the available functions determined by the Licenses you purchased. You can add some frequently used or important modules to the navigation bar for convenient access. See details in ***Customize Navigation Bar*** .
Overview Panel	Maintenance	The Maintenance module provides the overview of device network status, service running status, and health checking results. You can refresh to view the real-time service running status. See more details in ***Maintenance*** .
	Access Control	The Access Control module provides today's access record statistics, today's access trend, and top 5 of today's abnormal record types.

Section	Module	Description
		You can refresh to view the real-time trend and top 5 of types, or export them in different formats. See more details in ***Manage Access Control*** .
	Entrance & Exit	The Entrance & Exit module provides the statistics of parking spaces and vacant parking spaces in list, overtime vehicle counting, and today's vehicle passing trend. You can refresh to view the real-time amount of vacant parking spaces or overtime vehicles, and the real-time vehicle passing trend. You can also export them in different formats. See more details in ***Manage Vehicle*** .
	Alarm	The Alarm module provides today's alarm statistics, the last 7 days' alarm trend, top 5 of today's event and alarms, and top 5 of today's alarms in one region. You can refresh to view the trend and top 5 of alarms, or export them in different formats. See more details in ***Configure Event and Alarm*** .
Map Configuration on Home Page		The default Home page is a navigation map of the Web Client for accessing modules. You can go to the Map Monitoring to configure the map for visualization management as needed. See more details in ***Manage Map*** .
Wizard	Video	A wizard which guides you through the management and applications of Video. You can also view the flow chart which introduces the video resource management, recording configurations, and video application in ***Flow Chart*** .
	Access Control	A wizard which guides you through the basic configurations of Access Control. You can also view the flow chart which introduces the configurations and operations of access control in ***Flow Chart*** .
	Entrance & Exit	A wizard which guides you through the management and applications of Entrance & Exit. You can also view the flow chart which introduces the management of parking lots, vehicles, and entry & exit rules and vehicle search in ***Flow Chart*** .

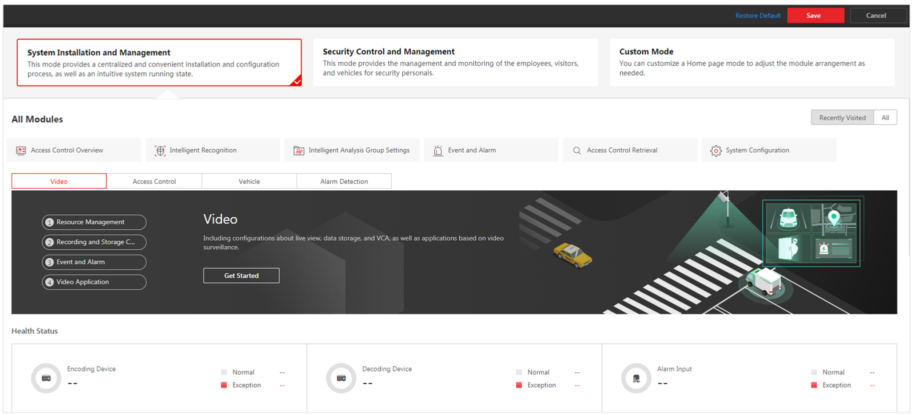
Section	Module	Description
	Alarm Detection	A wizard which guides you through the management and configurations of Alarm Detection. You can also view the flow chart which introduces the management of security control panels and alarm inputs, defense template configuration, and event & alarm management in ***Flow Chart*** .
Maintenance and Management	License	You can view the License details, activate, upgrade, and deactivate the License if needed. For more details, refer to ***Manage License*** .
	Back Up and Restore System Data	You can manually back up the data in the system, or configure a schedule to run the backup task regularly. When an exception occurs, you can restore the database if you have backed up the database. For more details, refer to ***Set System Data Backup*** and ***Restore System Data*** .
	Export Configuration Data	You can export and save configuration data to your local PC. For more details, refer to ***Export Configuration File*** .
	Download Installation Package	Download the installation package of other clients, such as Control Client.
	About	Check the version information of the Web Client. View the License Agreement and Open-Source License Agreement.
Home Page Mode Switch		The Mode Switch module provides three predefined modes of Home page, i.e., Default Mode, System Installation and Management Mode, and Security Control and Management Mode for different scenarios. You can also customize the Home page mode as needed. See more details in ***Customize and Switch Home Page Mode*** .
Others	Change Password	Change the password of the current user. For more details, refer to ***Change Password of Current User*** .
	Logout	Log out of the system and back to the login page.

5.1 Customize and Switch Home Page Mode

You can switch to the default Home page mode to two predefined modes (that are, System Installation and Management, and Security Control Management) for different scenarios or customize a mode as needed.

Steps

1. In the top right corner of Home page, click **Switch Mode** to enter the mode switch page.



System Installation and Management
This mode provides a centralized and convenient installation and configuration process, as well as an intuitive system running state.

Security Control and Management
This mode provides the management and monitoring of the employees, visitors, and vehicles for security personals.

Custom Mode
You can customize a Home page mode to adjust the module arrangement as needed.

Video
Including configurations about live view, data storage, and VCA, as well as applications based on video surveillance.

Figure 5-2 Customize and Switch Home Page Mode

2. **Optional:** In the All Modules field, click **Recently Visited** or **All** to show and quickly access to the recently visited modules or all available modules.

Note

The displayed modules in the **Recently Visited** tab will keep refreshing according to the modules visited by the current user.

3. **Optional:** Customize a mode.
   1) At the left, click **Custom Mode** to display mode configuration panel.
   2) In the module name field, click + to add module(s) to the mode.

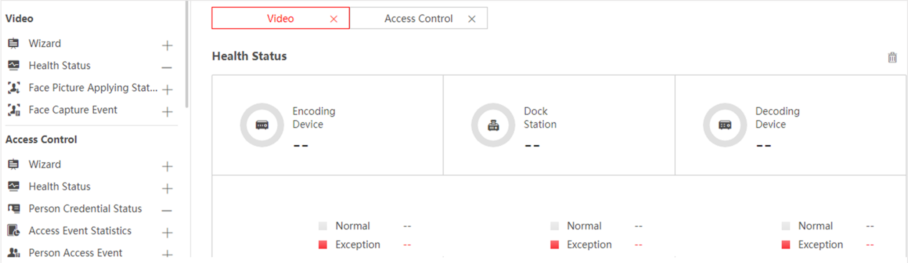


Figure 5-3 Customize Mode for Home Page

   The added module(s) are displayed under the **All Modules** field.

   3) **Optional:** Click 🗑 or × to remove the module(s) or section(s) from the mode.
4. At the top of the page, click a predefined or custom mode to switch the Home page mode.

The modules contained in the mode are displayed under the **All Modules** field. You can click the tabs to switch the detailed and visual views of different modules.

5. **Optional:** In the top right corner of mode switching page, click **Cancel** to cancel setting mode.
6. **Optional:** In the top right corner of mode switching page, click **Restore Default** to switch to the default mode.
7. In the top right corner of mode switching page, click **Save** to save the mode settings.

5.2 Customize Navigation Bar

To conveniently access some frequently used or important modules, you can customize the navigation bar.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** to display the navigation bar and All Modules panel.

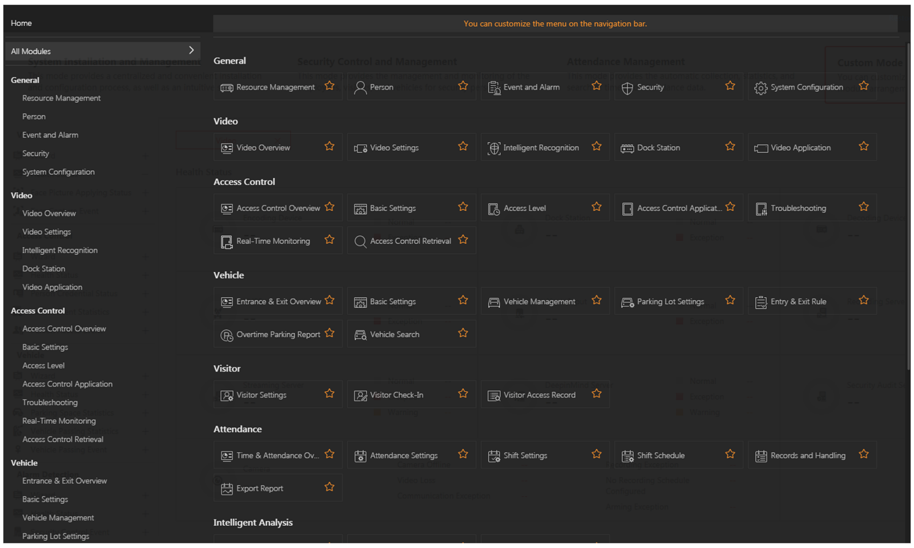


Figure 5-4 Navigation Bar and All Modules Panel

2. On the All Modules panel, move the cursor to a module item.

   A icon ☆ appears beside the module name.
3. Click ☆ to add the selected module to the navigation bar.

   The icon ☆ of the corresponding module turns to ★ .
4. **Optional:** Click ★ to remove the module from the navigation bar.

Chapter 6 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.

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 Storage and 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 7 Manage License

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

Two types of License are available for HikCentral Professional:

- **Base:** You need to purchase at least one basic License to activate the HikCentral Professional.
- **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.

7.1 Activate License - Online

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

Steps

1. Log in to HikCentral Professional via the Web Client. Refer to ***Login via Web Client*** .
2. On the Home page, click **Activate** to open the Activate License panel.
3. Click **Online Activation** to activate the License in online mode.
4. 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.
   - The activation code should contain 16 characters or 32 characters (except dashes).

5. Check **I accept the terms of the agreement** to open the License Agreement panel and click **OK**.
6. **Optional:** Check the **Hot Spare**, select type, and enter the IP address if you want to build a hot spare system.

   Note

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

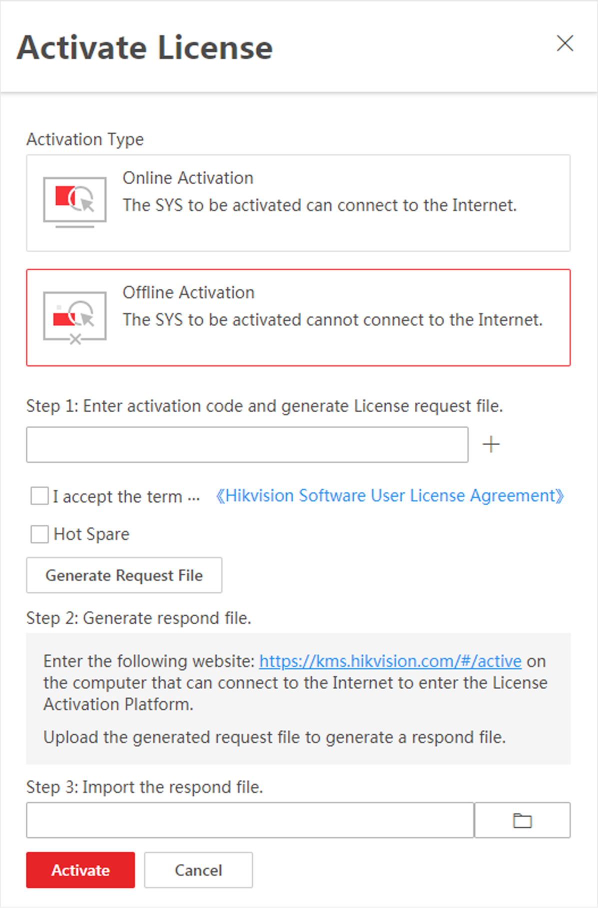
7. Click **Activate**.

7.2 Activate License - Offline

If the SYS server to be activated cannot connect to the Internet, you can activate the License in offline mode.

Steps

1. Log in to HikCentral Professional via the Web Client.
2. On the Home page, click **Activate** to open the Activate License panel.
3. Click **Offline Activation** to activate the License in offline mode.



Activate License

Activation Type

Online Activation
The SYS to be activated can connect to the Internet.

Offline Activation
The SYS to be activated cannot connect to the Internet.

Step 1: Enter activation code and generate License request file.

□ I accept the term ... 《Hikvision Software User License Agreement》

□ Hot Spare

Step 2: Generate respond file.

Enter the following website: https://kms.hikvision.com/#/active on the computer that can connect to the Internet to enter the License Activation Platform.

Upload the generated request file to generate a respond file.

Step 3: Import the respond file.

Figure 7-1 Activate License in Offline Mode

4. 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.
- The activation code should contain 16 characters or 32 characters (except dashes).

5. Check **I accept the terms of the agreement** to open the License Agreement panel and click **OK**.

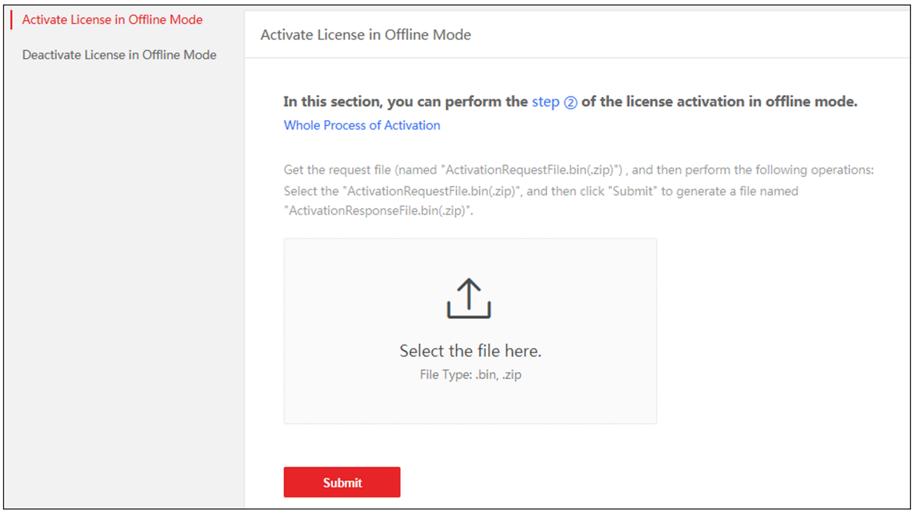
6. **Optional:** Check the **Hot Spare**, select type, and enter the IP address if you want to build a hot spare system.

Note

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

7. Click **Generate Request File**.

   A request file named "ActivationRequestFile.bin" will be downloaded. Save the request file to the proper directory or the removable storage medium (e.g., USB flash disk).
8. Copy the request file to the computer that can connect to the Internet.
9. On the computer which can connect to the Internet, enter the following website: ***https://kms.hikvision.com/#/active*** .
10. Click ⇪ and then select the downloaded request file.


Activate License in Offline Mode
Deactivate License in Offline Mode
Activate License in Offline Mode
Whole Process of Activation
Select the file here.
File Type: .bin, .zip
Submit

In this section, you can perform the step ② of the license activation in offline mode.

Get the request file (named "ActivationRequestFile.bin(.zip)") , and then perform the following operations: Select the "ActivationRequestFile.bin(.zip)", and then click "Submit" to generate a file named "ActivationResponseFile.bin(.zip)".

Figure 7-2 Select Request File

11. Click **Submit**.

    A respond file named "ActivationResponseFile.bin" will be downloaded. Save the respond file to the proper directory or the removable storage medium (e.g., USB flash disk).
12. Copy the respond file to the proper directory of the computer that accesses HikCentral Professional via the Web Client.
13. In the Offline Activation panel, click 🗀 and select the downloaded respond file.
14. Click **Activate**.

7.3 Update License - Online

As your project grows, you may need to increase the connectable number of resources (e.g., cameras) for your HikCentral Professional. If the SYS 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.

Steps

1. Log in to HikCentral Professional via the Web Client. Refer to ***Login via Web Client*** for details.
2. In the top right corner of Home page, move the cursor to the **Maintenance and Management** to show the drop-down menu.
3. Click **Update License** in the drop-down menu to open the Update License panel.
4. Click **Online Update** to update the License in online mode.
5. 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.
- The activation code should contain 16 characters or 32 characters (except dashes).

6. Check **I accept the terms of the agreement** to open the License Agreement panel and click **OK**.
7. Click **Update**.

7.4 Update License - Offline

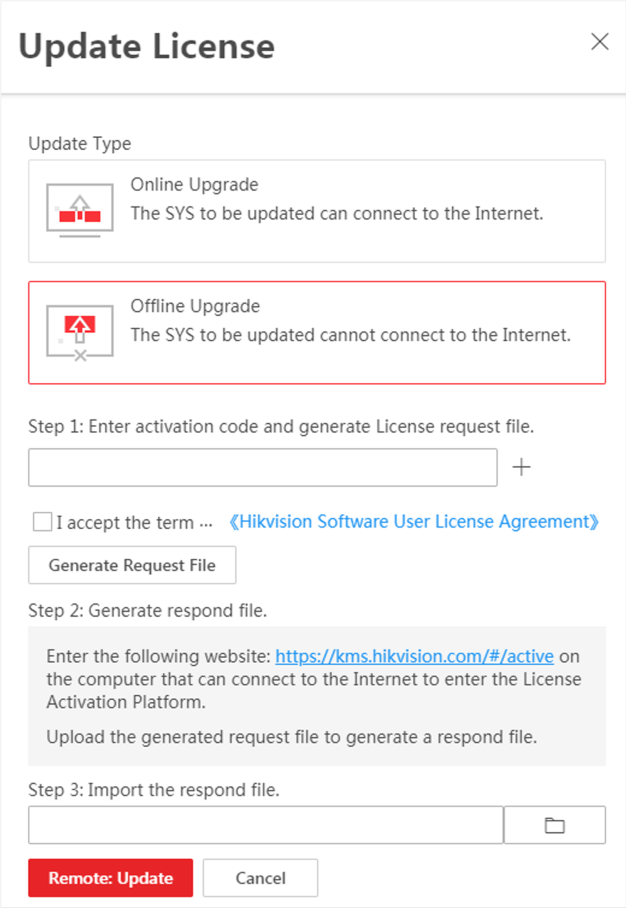
As your project grows, you may need to increase the connectable number of cameras for your HikCentral Professional. If the SYS to be updated cannot connect to the Internet, you can update the system in offline mode.

Before You Start

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

Steps

1. Log in to HikCentral Professional via the Web Client.
2. In the top right corner of Home page, move the cursor to the **Maintenance and Management** to show the drop-down menu.
3. Click **Update License** in the drop-down menu to open the Update License panel.
4. Click **Offline Update** to update the License in offline mode.



Update License

Update Type

Online Upgrade
The SYS to be updated can connect to the Internet.

Offline Upgrade
The SYS to be updated cannot connect to the Internet.

Step 1: Enter activation code and generate License request file.

□ I accept the term ... 《Hikvision Software User License Agreement》

Generate Request File

Step 2: Generate respond file.

Enter the following website: https://kms.hikvision.com/#/active on the computer that can connect to the Internet to enter the License Activation Platform.

Upload the generated request file to generate a respond file.

Step 3: Import the respond file.

Remote: Update   Cancel

Figure 7-3 Update License in Offline Mode

5. Enter the activation code of your additional License.

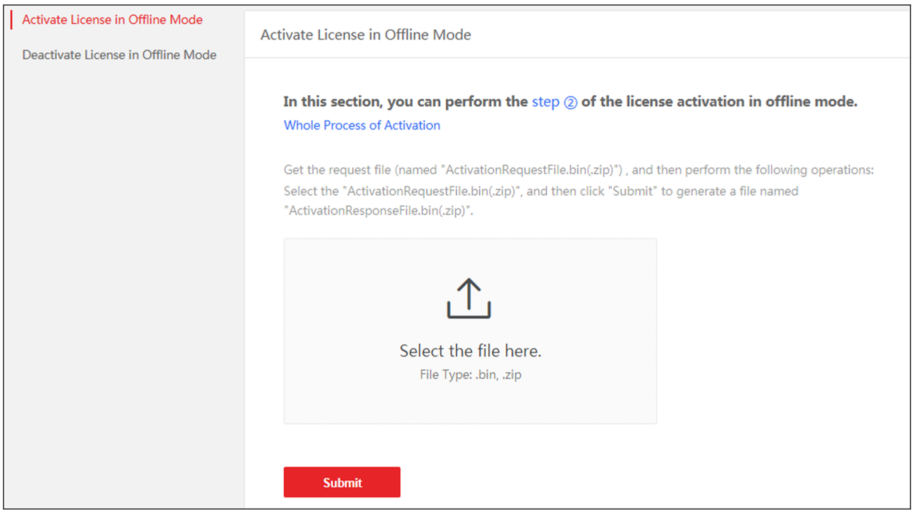
Note

- If you have purchased more than one License, you can click + and enter other activation codes.
- The activation code should contain 16 characters or 32 characters (except dashes).

6. Check **I accept the terms of the agreement** to open the License Agreement panel and click **OK**.
7. Click **Generate Request File**.

   A request file named "ActivationRequestFile.bin" will be downloaded. Save the request file to the proper directory or the removable storage medium (e.g., USB flash disk).

8. Copy the request file to the computer that can connect to the Internet.
9. On the computer which can connect to the Internet, enter the following website: ***https://kms.hikvision.com/#/active*** .
10. Click ⇧ and then select the downloaded request file.



Activate License in Offline Mode

Deactivate License in Offline Mode

Activate License in Offline Mode

In this section, you can perform the step ② of the license activation in offline mode.

Whole Process of Activation

Get the request file (named "ActivationRequestFile.bin(.zip)") , and then perform the following operations: Select the "ActivationRequestFile.bin(.zip)", and then click "Submit" to generate a file named "ActivationResponseFile.bin(.zip)".

Select the file here.

File Type: .bin, .zip

Submit

Figure 7-4 Select Request File

11. Click **Submit**.

    A respond file named "ActivationResponseFile.bin" will be downloaded. Save the respond file to the proper directory or the removable storage medium (e.g., USB flash disk).

12. Copy the respond file to the proper directory of the computer that accesses HikCentral Professional via the Web Client.
13. In the offline update panel, click 🗀 and select the downloaded respond file.
14. Click **Update**.

7.5 Deactivate License - Online

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

Steps

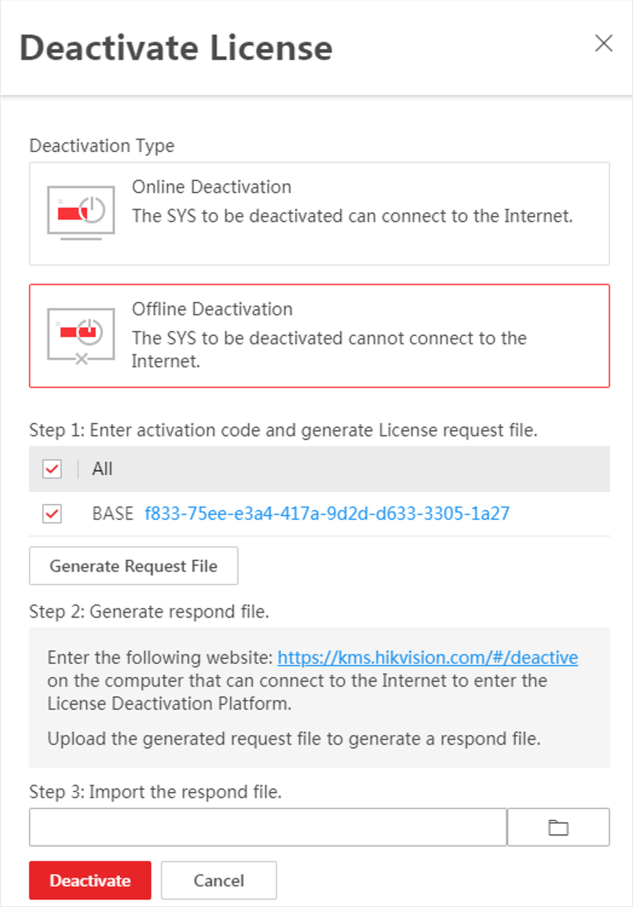
1. Log in to HikCentral Professional via the Web Client. Refer to ***Login via Web Client*** .
2. In the top right corner of Home page, move the cursor to the **Maintenance and Management** to show the drop-down menu.
3. Click **Deactivate License** in the drop-down menu to open the Deactivate License panel.
4. Click **Online Deactivation** to deactivate the License in online mode.
5. Check the activation code(s) to be deactivated.
6. Click **Deactivate**.

7.6 Deactivate License - Offline

If you want to run the SYS on another computer or server, you should deactivate the SYS first and then activate the SYS again. If the SYS to be deactivated cannot connect to the Internet, you can deactivate the License in offline mode.

Steps

1. Log in to the HikCentral Professional via Web Client.
2. In the top right corner of Home page, move the cursor to the **Maintenance and Management** to show the drop-down menu.
3. Click **Deactivate License** in the drop-down menu to open the Deactivate License panel.
4. Click **Offline Deactivation** to deactivate the License in offline mode.



Deactivate License

Deactivation Type

Online Deactivation
The SYS to be deactivated can connect to the Internet.

Offline Deactivation
The SYS to be deactivated cannot connect to the Internet.

Step 1: Enter activation code and generate License request file.

☑ All

☑ BASE f833-75ee-e3a4-417a-9d2d-d633-3305-1a27

Generate Request File

Step 2: Generate respond file.

Enter the following website: https://kms.hikvision.com/#/deactive on the computer that can connect to the Internet to enter the License Deactivation Platform.

Upload the generated request file to generate a respond file.

Step 3: Import the respond file.

Deactivate Cancel

Figure 7-5 Deactivate License in Offline Mode

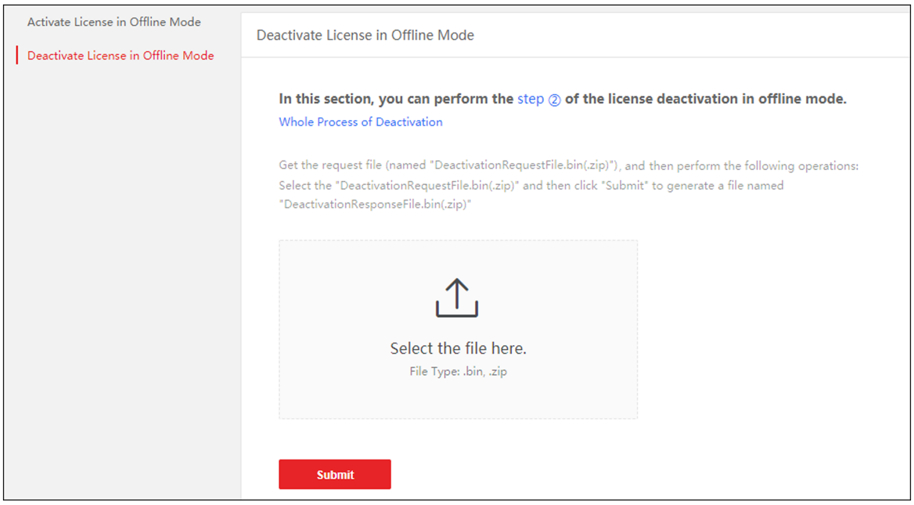
5. Check the activation code(s) to be deactivated.
6. Click **Generate Request File**.

Note

After the request file is generated, the selected activation code(s) will be unavailable.

A request file named "ActivationRequestFile.bin" will be downloaded. Save the request file to the proper directory or the removable storage medium (e.g., USB flash disk).

7. Copy the request file to the computer that can connect to the Internet.
8. On the computer which can connect to the Internet, enter the following website: ***https://kms.hikvision.com/#/deactive*** .
9. Click ⇧ and then select the downloaded request file.


Activate License in Offline Mode
Deactivate License in Offline Mode
Deactivate License in Offline Mode

In this section, you can perform the step ② of the license deactivation in offline mode.

Whole Process of Deactivation

Get the request file (named "DeactivationRequestFile.bin(.zip)"), and then perform the following operations: Select the "DeactivationRequestFile.bin(.zip)" and then click "Submit" to generate a file named "DeactivationResponseFile.bin(.zip)"

Select the file here.
File Type: .bin, .zip
Submit

Figure 7-6 Select Request File

10. Click **Submit**.

    A respond file named "DectivationResponseFile.bin" will be downloaded. Save the respond file to the proper directory or the removable storage medium (e.g., USB flash disk).
11. Copy the respond file to the proper directory of the computer that accesses HikCentral Professional via the Web Client.
12. In the Offline Deactivation panel, click 🗀 and select the downloaded respond file.
13. Click **Deactivate**.

7.7 Set SUP Upgrade Prompt

SUP (Software Upgrade Program) refers to the system's maintenance time, which has an expire date and needs to be upgraded before expiration. You can set SUP upgrade prompt in the system. After that, when the SUP is going to expire, you can receive an email reminding the expiration every day during the set period.

Steps

1. In the top right corner of Home page, select **Maintenance and Management → License Details** to open the License Details panel.
2. Go to the bottom of details list and click **Expiration Prompt Configuration** to enter the SUP Expiration Prompt Settings panel.
3. Set the **Overdue Reminder** switch to ON.
4. Set the days when you will receive the prompt email before expiration.

Note

- You should enter an integer between 1 to 365.
- By default, the system will send a prompt email 30 days before expiration.

5. Click **Add User** to add user(s) who can receive upgrade prompt.

Note

- You should configure the users' email addresses before adding them as recipients. The added users can receive upgrade prompt via the bound email addresses.
- Up to 64 recipients can be added.
- You can click × to delete the added user(s).

6. Click **Add Email** to add email address(es).

Note

You can add email of both the system user(s) and other user(s). The system will send upgrade prompt to the added email address(es).

7. Click **Save**.

Chapter 8 Manage Resource

HikCentral Professional supports multiple resource types, such as encoding device, access control device, Remote Site, and decoding device. 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, add Remote Site for central management of multiple systems, add Recording Server for storing the videos, and add Streaming Server for getting the video data stream from the server.

8.1 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 platform. Besides activating the device one by one, you can also deal with multiple ones at the same time. The devices which are batch activated should have the same password.

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 HikCentral Professional 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. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Encoding Device** on the left.
3. View the device status (shown on Security column) and select one or multiple inactive devices.
4. Click 💡 to open the Device Activation window.
5. 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 change your password regularly, especially in the high security system, changing 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 **Save** to create the password for the device.

   An **Operation completed.** message is displayed when the password is set successfully.
7. Click ✎ in the Operation column to change the device's IP address, subnet mask, gateway, etc., if needed.

   Note

   For details, refer to ***Edit Online Device's Network Information*** .

8.2 Edit Online Device's Network Information

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

Before You Start

For some devices, you should 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 creating password for the encoding device as an example.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Encoding Device** on the left.
3. In the Online Device area, select a network type.

   Server Network

   The detected online devices in the same local subnet with the SYS server will be listed.

   Local Network

   The detected online devices in the same local subnet with the Web Client will be listed.
4. View the device status on Security column, and click ✎ in the Operation column of an active device.
5. 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.

6. Click ✔ .
7. Enter device's password.
8. Click **Save**.

8.3 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,

8.3.1 Add Detected Online Device

The system can perform an automated detection for available encoding devices in the network where the Web Client or 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 a Detected Online Encoding Device

For the detected online encoding devices, you can add the device one by one to HikCentral Professional by specifying its user name, password and some other 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 HikCentral Professional via network.
- The devices to be added should be activated. Refer to ***Create Password for Inactive Device(s)*** for details about activating devices.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Encoding Device** on the left.

3. 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 SYS server will be listed in the Online Device area.

   Local Network

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

4. In the Online Device area, select **Hikvision Private Protocol**/ **Hikvision ISUP Protocol**/**ONVIF Protocol** to filter the detected online devices.

   Note

   Select **Hikvision Private Protocol**/**Hikvision ISUP Protocol** to add a Hikvision device and select **ONVIF Protocol** to add a third-party device.

5. In the Online Device area, select the active device to be added.
6. Click **Add to Device List** to open the Add Online Device window.
7. 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 port number is 8000.

   Mapped Port

   This function is only available when you select **Hikvision Private Protocol** in Step 3. If you want to download pictures from the device, switch **Mapped Port** to on and enter the picture downloading port. By default, the port No. is 80.

   Verify Stream Encryption Key

   Switch **Verify Stream Encryption Key** 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 SYS server for security purpose.

   Note

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

   Device Name

   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 HikCentral Professional 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 change your password regularly, especially in the high security system, changing 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. **Optional:** Select a time zone for the device in drop-down list of **Time Zone of Device**.

Note

You can check **Apply to Device** so that when the time zone of the device and the system are not consistent, the system will automatically apply the time zone settings to the device.

9. **Optional:** Switch **Add Resource to Area** 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 operations such as live view, playback, event settings, etc., for the cameras.

10. **Optional:** If you choose to add channels to area, select a Streaming Server to get the video stream of the channels via the server.
11. **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.

pStor Cluster Service

pStor Cluster Service is a service that can manage multiple pStors. When there are multiple pStors storing a large number of video files, use pStor Cluster Service to manage these pStors.

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.

12. 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.
13. Click **Add**.
14. **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

- You can only change the password for online HIKVISION devices currently.
- If the devices have the same password, you can select multiple devices to change the password for them at the same time.

What to do next

For facial recognition camera/ANPR camera, click **Maintenance and Management → License Details →** › **→ Configuration** , and then select the added cameras as these three types of cameras respectively. Otherwise, these cameras' functions (facial recognition, plate recognition, and temperature report) cannot be performed normally in the system.

Add Detected Online Encoding Devices in a Batch

For the detected online encoding devices, if they have the same user name and password, you can batch add multiple devices to HikCentral Professional.

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 HikCentral Professional 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. In the top left corner of Home page, select ≡ **→ All Modules → General → Resource Management** .
2. Click **Device and Server → Encoding Device** on the left.
3. 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 SYS 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.
4. In the Online Device area, select **Hikvision Private Protocol/ Hikvision ISUP Protocol/ONVIF Protocol** to filter the detected online devices.

   Note

   Select **Hikvision Private Protocol/Hikvision ISUP Protocol** to add Hikvision devices and select **ONVIF Protocol** to add third-party devices.
5. In the Online Device area, check the active devices to be added.
6. Click **Add to Device List** to open the Add Online Device dialog.
7. **Optional:** Switch **Mapped Port** to on and enter the picture downloading port if you want to download pictures from the device.

Note

This function is only available when you select **Hikvision Private Protocol** in Step 3. By default, the port No. is 80.

8. **Optional:** Switch **Verify Stream Encryption Key** to on, and enter stream encryption key in **Stream Encryption Key on Device** field.

   Note

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

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

9. 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 HikCentral Professional 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 change your password regularly, especially in the high security system, changing 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.

10. **Optional:** Select a time zone for the device in drop-down list of **Time Zone of Device**.

    Note

    You can check **Apply to Device** so that when the time zone of the device and the system are not consistent, the system will automatically apply the time zone settings to the device.

11. **Optional:** Switch **Add Resource to Area** 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 operations such as live view, playback, event settings, etc., for the cameras.

12. **Optional:** Select a Streaming Server to get the video stream of the channels via the server.
13. Click **Add**.
14. **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

- You can only change the password for online HIKVISION devices currently.
- If the devices have the same password, you can select multiple devices to change the password for them at the same time.

What to do next

For facial recognition camera/ANPR camera, click **Maintenance and Management → License Details →** › **→ Configuration** , and then select the added cameras as these three types of cameras respectively. Otherwise, these cameras' functions (facial recognition, plate recognition, and temperature report) cannot be performed normally in the system.

8.3.2 Add Encoding Device by IP Address or Domain Name

When you know the IP address or domain name of a device, you can add it to the platform by specifying the IP address (or domain name), user name, password, etc.

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 HikCentral Professional via network.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Encoding Device** on the left.
3. Click **Add** to enter the Add Encoding Device page.
4. Select **Hikvision Private Protocol**/**ONVIF Protocol** as the Access Protocol.

   Note

   Select **Hikvision Private Protocol** to add a Hikvision device, while select **ONVIF Protocol** to add a third-party device.

5. Select **IP/Domain** as the adding mode.
6. Enter the required information.

   Device Address

   The IP address or domain name of the device.

   Device Port

   By default, the device port No. is 8000.

   Mapped Port

   This function is used for downloading pictures from devices added by **Hikvision Private Protocol**. Set the **Mapped Port** switch to on and enter the picture downloading port No. that you have configured in the remote configuration page of the device. The default port No. is 80.

   Verify Stream Encryption Key

   This button is for **Hikvision Private Protocol** only. Switch **Verify Stream Encryption Key** to on, and enter the stream encryption key in the following **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 SYS server for security purpose.

   Note

   This function should be supported by the devices. For details about getting the key, refer to the user manual of the device.

   Device Name

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

   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 change your password regularly, especially in the high security system, changing 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:** Select a time zone for the device in drop-down list of **Time Zone of Device**.

Note

You can check **Apply to Device** so that when the time zone of the device and the system are not consistent, the system will automatically apply the time zone settings to the device.

8. **Optional:** Switch **Add Resource to Area** 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 operations such as live view, playback, event settings, etc., for the cameras.

9. **Optional:** If you choose to add resources to area, select a Streaming Server to get the video stream of the channels via the server.
10. **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.

pStor Cluster Service

pStor Cluster Service is a service that can manage multiple pStors. When there are multiple pStors storing a large number of video files, use pStor Cluster Service to manage these pStors.

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.

11. 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.

12. 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.

13. Optional: Perform the following operation(s) 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

- You can only change the password for online HIKVISION devices currently.
- If the devices have the same password, you can select multiple devices to change the password for them at the same time.

What to do next

For facial recognition camera/ANPR camera, click **Maintenance and Management → License Details →** › **→ Configuration → View** , and then select the added cameras as these three types of cameras respectively. Otherwise, these cameras' functions (facial recognition, plate recognition, and temperature report) cannot be performed normally in the system.

8.3.3 Add Encoding Devices by IP Segment

When multiple encoding devices to be added have the same port number, user name, password, and have different IP addresses within a range, you can add devices by specifying the IP segment and some 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 HikCentral Professional via network.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Encoding Device** on the left.
3. Click **Add** to enter the Add Encoding Device page.
4. Select **Hikvision Private Protocol**/**ONVIF Protocol** as the Access Protocol.

   Note

   Select **Hikvision Private Protocol** to add a Hikvision device, while select **ONVIF Protocol** to add a third-party device.

5. Select **IP Segment** as the adding mode.
6. Enter the required information.

   Device Address

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

   Device Port

   By default, the device port No. is 8000.

   Mapped Port

   This function is used for downloading pictures from devices added by **Hikvision Private Protocol**. Set the **Mapped Port** switch to on and enter the picture downloading port No. that you have configured in the remote configuration page of the device. The default port No. is 80.

   Verify Stream Encryption Key

   This button is for **Hikvision Private Protocol** only. You can switch **Verify Stream Encryption Key** to on, and enter the stream encryption key in the following **Stream Encryption Key on Device** field. Then when starting live view or remote playback of the device, the client will verify the key stored inSYS 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 HikCentral Professional 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 change your password regularly, especially in the high security system, changing 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:** Select a time zone for the device in drop-down list of **Time Zone of Device**.

Note

You can check **Apply to Device** so that when the time zone of the device and the system are not consistent, the system will automatically apply the time zone settings to the device.

8. **Optional:** Switch **Add Resource to Area** to on to import the resources of the added devices to an area.

Note

- You can import all the resources 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 resources to area, you cannot perform the live view, playback, event settings, etc., for the resources.

9. **Optional:** If you choose to add resources to area, select a Streaming Server to get the video stream of the resources via the server.
10. Set the quick recording schedule for added resources.
    - Check **Get Device's Recording Settings** to get the recording schedule from the device and the resources 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.

11. 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.

12. 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

- You can only change the password for online HIKVISION devices currently.
- If the devices have the same password, you can select multiple devices to change the password for them at the same time.

What to do next

For facial recognition camera/ANPR camera, click **Maintenance and Management → License Details →** › **→ Configuration → View** , and then select the added cameras as these three types of cameras respectively. Otherwise, these cameras' functions (facial recognition, plate recognition, and temperature report) cannot be performed normally in the system.

8.3.4 Add Encoding Devices by Port Segment

When multiple encoding devices to be added have the same IP address, user name, password, and have different port numbers within a range, you can add devices by specifying the port segment and some 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 HikCentral Professional via network.

Steps

1. In the top left corner of Home page, select ≡ **→ All Modules → General → Resource Management** .

2. Click **Device and Server → Encoding Device** on the left.
3. Click **Add** to enter the Add Encoding Device page.
4. Select **Hikvision Private Protocol**/**ONVIF Protocol** as the access protocol.

   Note

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

5. Select **Port Segment** as the adding mode.
6. Enter the required information.

   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.

   Mapped Port

   This function is used for downloading pictures from devices added by **Hikvision Private Protocol**. Set the **Mapped Port** switch to on and enter the picture downloading port No. that you have configured in the remote configuration page of the device. The default port No. is 80.

   Verify Stream Encryption Key

   This button is for **Hikvision Private Protocol** only. You can switch **Verify Stream Encryption Key** to on, and enter the stream encryption key in the following **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 SYS 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 HikCentral Professional 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 change

your password regularly, especially in the high security system, changing 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:** Select a time zone for the device in drop-down list of **Time Zone of Device**.

Note

You can check **Apply to Device** so that when the time zone of the device and the system are not consistent, the system will automatically apply the time zone settings to the device.

8. **Optional:** Switch **Add Resource to Area** 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.

9. **Optional:** If you choose to add resources to area, select a Streaming Server to get the video stream of the channels via the server.
10. 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.
11. 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.
12. **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

- You can only change the password for online HIKVISION devices currently.
- If the devices have the same password, you can select multiple devices to change the password for them at the same time.

What to do next

For facial recognition camera/ANPR camera, click **Maintenance and Management → License Details →** › **→ Configuration** , and then select the added cameras as these three types of cameras respectively. Otherwise, these cameras' functions (facial recognition, plate recognition, and temperature report) cannot be performed normally in the system.

8.3.5 Add Encoding Device by Hik-Connect DDNS

You can add encoding devices with dynamic IP addresses to the system by domain name solutions of Hik-Connect. Currently, the system only supports domain name solutions function of Hik-Connect.

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 HikCentral Professional via network.
Make sure you have enabled Hik-Connect service for devices to be added on device web page. For details, refer to the user manual of Hik-Connect.

Steps

1. In the top left corner of Home page, select ≡ **→ All Modules → General → Resource Management** .
2. Click **Device and Server → Encoding Device** on the left.
3. Click **Add** to enter the Add Encoding Device page.
4. Select **Hikvision Private Protocol** as the Access Protocol.
5. Select **Hik-Connect DDNS** as the adding mode.
6. **Optional:** Set the **Mapped Port** switch to on and enter the picture downloading port No. that you have configured on the remote configuration page of the device. The default port No. is 80.
7. Select a device source.

   New Device

   Add a new device to HikCentral Professional by Hik-Connect service.

   Hik-Connect Device List

   For users with a Hik-Connect account, you can add devices managed in your Hik-Connect account to HikCentral Professional in a batch.
8. Enter the required information.

Hik-Connect Server Address

Enter the address of the Hik-Connect service. By default, it's ***https://open.ezvizlife.com***.

Serial No.

Enter the serial No. of the device.

Verification Code

Enter the verification code of the device.

Stream Encryption Key on Device

After switching **Verify Stream Encryption Key** to on, you should 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 SYS server for security purpose.

Note

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

Device Name

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 change your password regularly, especially in the high security system, changing 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. **Optional:** Select a time zone for the device in drop-down list of **Time Zone of Device**.

Note

You can check **Apply to Device** so that when the time zone of the device and the system are not consistent, the system will automatically apply the time zone settings to the device.

10. Switch **Add Resource to Area** 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.

11. **Optional:** If you choose to add resources to an area, select a Streaming Server to get the video stream of the channels via the server.
12. **Optional:** 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.
13. 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.
14. **Optional:** Perform the following operation(s) 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

- You can only change the password for online HIKVISION devices currently.
- If the devices have the same password, you can select multiple devices to change the password for them at the same time.

What to do next

For facial recognition camera/ANPR camera, click **Maintenance and Management → License Details →** › **→ Configuration** , and then select the added cameras as these three types of cameras respectively. Otherwise, these cameras' functions (facial recognition, plate recognition, and temperature report) cannot be performed normally in the system.

8.3.6 Add Encoding Device by Device ID

For the encoding devices supporting ISUP Protocol, you can add them by specifying a predefined device ID, key, etc. This is a cost-effective choice when you need to manage an encoding device without fixed IP address by HikCentral Professional.

Before You Start

- Make sure the encoding 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 HikCentral Professional via network.
- Before adding devices supporting Hikvision ISUP 2.6/4.0 protocol to the system, you need to set related configuration to allow these devices to access the system. For details, refer to ***Device Access Protocol*** .

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Encoding Device** on the left.
3. Click **Add** to enter the Add Encoding Device page.
4. Select **Hikvision ISUP Protocol** as the Access Protocol.
5. Select **Device ID** as the adding mode.
6. Enter the required parameters, including the device ID and device name.

   Note

   For devices supporting ISUP 5.0 protocol to the system, you should enter the key.

7. **Optional:** Set **Picture Storage** switch to on to enable picture storage for the encoding device.
8. **Optional:** Select the storage location from the drop-down list.

   Note

   The pictures uploaded from the devices, such as alarm triggered pictures, captured face pictures and captured plate license pictures, can be stored on the storage location you select.

9. **Optional:** Select a time zone for the device in drop-down list of **Time Zone of Device**.

   Note

   You can check **Apply to Device** so that when the time zone of the device and the system are not consistent, the system will automatically apply the time zone settings to the device.

10. **Optional:** Switch **Add Resource to Area** to ON to import the resources of the added devices to an area.

    Note

    - You can import all the resources including cameras, alarm inputs and alarm outputs, or the specified camera(s) to the corresponding area.
    - For video access control terminal of a device, the camera on the terminal will also be imported to the corresponding area.
    - You can create a new area by the device name or select an existing area.
    - If you do not import resources to area, you cannot perform operations such as live view, playback, event settings, etc., for the cameras.

11. **Optional:** If you choose to add resources to area, select a Streaming Server to get the video stream of the resources via the server.
12. **Optional:** Check **Get Device's Recording Settings** to get the recording schedule from the device and the resources of the device will start recording according to the schedule.
13. 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.
14. **Optional:** Perform the following operation(s) 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

- You can only change the password for online HIKVISION devices currently.
- If the devices have the same password, you can select multiple devices to change the password for them at the same time.

8.3.7 Add Encoding Devices by Device ID Segment

If you need to add multiple encoding devices which have no fixed IP addresses and support ISUP Protocol toHikCentral Professional, you can add them to HikCentral Professional at a time after configuring a device ID segment for the devices.

Before You Start

- Make sure the encoding 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 HikCentral Professional via network.
- Before adding devices supporting ISUP 2.6/4.0 protocol to the system, you need to set related configuration to allow these devices to access the system. For details, refer to ***Device Access Protocol*** .

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Encoding Device** on the left.
3. Click **Add** to enter the Add Encoding Device page.
4. Select **Hikvision ISUP Protocol** as the Access Protocol.
5. Select **Device ID Segment** as the adding mode.
6. Enter the required parameters, including the start device ID and end device ID.

   Note

   For devices supporting ISUP 5.0 protocol to the system, you should enter the key.

7. **Optional:** Set **Picture Storage** switch to on to enable picture storage for the encoding device.
8. **Optional:** Select the storage location from the drop-down list.

Note

The pictures uploaded from the devices, such as alarm triggered pictures, captured face pictures and captured plate license pictures, can be stored on the storage location you select.

9. **Optional:** Select a time zone for the device in drop-down list of **Time Zone of Device**.

Note

You can check **Apply to Device** so that when the time zone of the device and the system are not consistent, the system will automatically apply the time zone settings to the device.

10. **Optional:** Switch **Add Resource to Area** to on to import the resources of the added devices to an area.

Note

- You can import all the resources including cameras, alarm inputs and alarm outputs, or the specified camera(s) to the corresponding area.
- For video access control terminal of a device, the camera on the terminal will also be imported to the corresponding area.
- You can create a new area by the device name or select an existing area.
- If you do not import resources to area, you cannot perform operations such as live view, playback, event settings, etc., for the cameras.

11. **Optional:** If you choose to add resources to area, select a Streaming Server to get the video stream of the resources via the server.
12. **Optional:** Check **Get Device's Recording Settings** to get the recording schedule from the device and the resources of the device will start recording according to the schedule.
13. 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.

8.3.8 Add Encoding Devices in a Batch

When there are multiple devices to be added, you can edit the predefined template containing the required device information, and import the template to HikCentral Professional to add devices in a batch.

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 HikCentral Professional via network.

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

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Encoding Device** on the left.
3. Click **Add** to enter the Add Encoding Device page.
4. Select **Hikvision Private Protocol/Hikvision ISUP Protocol/** as the access protocol.

   Note

   Select **Hikvision Private Protocol/Hikvision ISUP Protocol** to add a Hikvision device and select **ONVIF Protocol** to add a third-party device.

5. Select **Batch Import** as the adding mode.
6. Click **Download Template** and save the predefined template (excel file) on your PC.
7. Open the exported template file and enter the required information of the devices to be added on the corresponding column.
8. Click ••• and select the edited file.
9. **Optional:** Select a time zone for the device in drop-down list of **Time Zone of Device**.

   Note

   You can check **Apply to Device** so that when the time zone of the device and the system are not consistent, the system will automatically apply the time zone settings to the device.

10. 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 next batch of devices.
11. **Optional:** Perform the following operation(s) 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

    - You can only change the password for online HIKVISION devices currently.
    - If the devices have the same password, you can select multiple devices to change the password for them at the same time.

What to do next

For facial recognition camera/ANPR camera, click **Maintenance and Management → License Details →** › **→ Configuration** , and then select the added cameras as these three types of cameras respectively. Otherwise, these cameras' functions (facial recognition, plate recognition, and temperature report) cannot be performed normally in the system.

8.3.9 Limit Bandwidth for Video Downloading

You can limit bandwidth for video downloading of specific NVRs to save video on the total bandwidth, and thus ensuring the fluency of main features such as live view.

Note

The NVR should be of V4.1.50 or later versions.

In the top left corner of Home page, select ≡ **→ All Modules → General → Resource Management → Device and Server → Encoding Device** to enter the encoding device management page, select encoding device(s) and click **Edit Bandwidth for Video Downloading** to set the bandwidth upper-limit for video downloading of the selected device(s).

8.3.10 Set N+1 Hot Spare for NVR

You can form an N+1 hot spare system with several NVRs (Network Video Recorder). The system consists of several host servers and a spare server. When the host server fails, the spare server switches into operation (such as video recording, searching video for playback, etc.), and thus increasing the video storage reliability of HikCentral Professional.

Before You Start

- At least two online NVRs should be added to form an N+1 hot spare system. For details about adding NVR, see ***Manage Encoding Device*** .
- Make sure the NVRs 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 HikCentral Professional via network.

If the N+1 hot spare settings have already been configured on the NVR, select ≡ **→ All Modules → General → Resource Management → Device and Server → Encoding Device → N+1 Hot Spare → Get Hot Spare Settings from Device** to upload the hot spare settings from the device to HikCentral Professional. If the N+1 hot spare settings haven't been configured on the device, perform the following task to set N+1 hot spare for the NVR.

Steps

Note

- The N+1 hot spare function is only supported by NVRs and Hybrid Storage Area Networks. For details about configuring N+1 hot spare system with Hybrid Storage Area Networks, see ***Set N+1 Hot Spare for Hybrid SAN*** .
- 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. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Encoding Device** → **N+1 Hot Spare** to enter the N+1 Configuration page.
3. Click **Add** to set N+1 hot spare.
4. Select a NVR in the **Spare** drop-down list to set it as the spare server.
5. Select the NVR(s) in the **Host** field to set them as the host server.
6. Click **Add**.

   Note

   The recording schedules configured on the NVR will be deleted after setting it as the spare Recording Server.

7. Click **Apply Hot Spare Settings to Device** to apply the Hot Spare settings to the devices to take effect.
8. **Optional:** Perform the following operations after setting the hot spare.

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

   Delete Hot Spare
   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.

8.4 Manage Access Control Device

You can add the access control devices to the system for access permission configuration, etc.

8.4.1 Add Detected Online Device

The active online access control devices in the same local subnet with the current Web Client or SYS 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 a Detected Online Access Control Device

The platform automatically detects online access control devices on the same local subnet with the client or SYS server. You can add the detected access control devices to the platform one by one if they have different user account.

Before You Start

- Make sure the devices you are going to add 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 HikCentral Professional via network.
- Make sure you have activated the devices. Refer to ***Create Password for Inactive Device(s)*** for detailed instructions on activating devices.

Follow the steps to add a detected online access control device to the platform.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Select **Device and Server** → **Access Control Device** on the left.
3. In the Online Device area, select a network type.

   Server Network

   All detected online devices on the same local subnet with the SYS server.

   Local Network

   All detected online devices on the same local subnet with the current Web Client.
4. Select **Hikvision Private Protocol**, **Hikvision ISUP Protocol** or **ONVIF Protocol** to filter the detected devices by protocol types.
5. Select an active device that you want to add to the platform.
6. Click **Add to Device List**.
7. Configure settings for 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 change your password regularly, especially in the high security system, changing 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. **Optional:** Select a time zone for the device in drop-down list of **Time Zone of Device**.

Note

You can check **Apply to Device** so that when the time zone of the device and the system are not consistent, the system will automatically apply the time zone settings to the device.

9. **Optional:** Switch on **Add Resource to Area** to import the resources (including alarm inputs, alarm outputs, and access points) to an area.

Note

- You can create a new area by device name or select an existing area.
- You can import all the access points or specific access point(s) to the area.
- For the video access control terminal of a device, the camera on the terminal will also be imported to the corresponding area.
- If you do not import access points to area, you cannot perform further configurations for the access point.

10. **Optional:** Check **Restore Default** to restore configured device parameters to default settings.

Note

- Not all the device parameters will be restored. Network parameters such as IP address, port No., and password will be kept.
- It is recommended that you should restore to default when adding an online device that has been added to other platforms for the first time.

11. Click **Add**.
12. **Optional:** Perform further operations on the added device(s).

Configure Device
Click ⚙ in the **Operation** column to enter the corresponding device configuration page to edit the time parameters, reboot the device, restore the device, or set other parameters. See ***Configure Device Parameters*** for detailed instructions.

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

Note

- You can only change the password for online HIKVISION devices currently.
- If the devices share the same password, you can select multiple devices to change the password together.

Restore Default

Select the added device(s) and click **Restore** to restore the configured device parameters excluding network parameters and account information.

Note

If you want to restore all the device parameters, you should check **Restore device parameters excluding network parameters and account information, such as user name and password.** in the pop-up window.

Add Detected Online Access Control Devices in a Batch

If the detected online access control devices share the same user name and password, you can add multiple devices at a time.

Before You Start

- Make sure the devices you are going to add 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 HikCentral Professional via network.
- Make sure you have activated the devices. Refer to ***Create Password for Inactive Device(s)*** for detailed instructions on activating devices.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Select **Device and Server** → **Access Control Device** on the left.
3. In the Online Device area, select a network type.

   Server Network

   All detected online devices on the same local subnet with the SYS server.

   Local Network

   All detected online devices on the same local subnet with the current Web Client.
4. Select **Hikvision Private Protocol**, **Hikvision ISUP Protocol** or **ONVIF Protocol** to filter the detected devices by protocol types.
5. Select the active devices that you want to add to the platform.
6. Click **Add to Device List**.
7. Set parameters for the devices.

⚠ **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 change your password regularly, especially in the high security system, changing 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. **Optional:** Select a time zone for the device in drop-down list of **Time Zone of Device**.

Note

You can check **Apply to Device** so that when the time zone of the device and the system are not consistent, the system will automatically apply the time zone settings to the device.

9. **Optional:** Switch on **Add Resource to Area** to import the resources (including alarm inputs, alarm outputs, and access points) to an area.

Note

- You can create a new area by device name or select an existing area.
- You can import all the access points or specific access point(s) to the area.
- For the video access control terminal of a device, the camera on the terminal will also be imported to the corresponding area.
- If you do not import access points to area, you cannot perform further configurations for the access point.

10. **Optional:** Check **Restore Default** to restore configured device parameters to default settings.

Note

- Not all the device parameters will be restored. Network parameters such as IP address, port No., and password will be kept.
- It is recommended that you should restore to default when adding an online device that has been added to other platforms for the first time.

11. Click **Add**.
12. **Optional:** Perform further operations on the added device(s).

Configure Device	Click ⚙ in the **Operation** column to enter the corresponding device configuration page to edit the time parameters, reboot the device, restore the device, or set other parameters. See ***Configure Device Parameters*** for detailed instructions.
Change Password	Select the added device(s) and click **Change Password** to change the password for the device(s).

Note

- You can only change the password for online HIKVISION devices currently.
- If the devices share the same password, you can select multiple devices to change the password together.

Restore Default

Select the added device(s) and click **Restore** to restore the configured device parameters excluding network parameters and account information.

Note

If you want to restore all the device parameters, you should check **Restore device parameters excluding network parameters and account information, such as user name and password.** in the pop-up window.

8.4.2 Add an Access Control Device by IP Address

If you know the IP address of the access control device you want to add to the platform, you can add the device by specifying its IP address, user name, password, etc.

Before You Start

- Make sure the devices you are going to add 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 HikCentral Professional via network.
- Make sure you have activated the devices. Refer to ***Create Password for Inactive Device(s)*** for detailed instructions on activating devices.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Select **Device and Server** → **Access Control Device** on the left.
3. Click **Add** to enter the Add Access Control Device page.
4. Select **Hikvision Private Protocol** as the access protocol.
5. Select **IP Address** as the adding mode.
6. Enter the required parameters.

Note

By default, the device port 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 change your password regularly, especially in the high security system, changing 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:** Select a time zone for the device in drop-down list of **Time Zone of Device**.

Note

You can check **Apply to Device** so that when the time zone of the device and the system are not consistent, the system will automatically apply the time zone settings to the device.

8. **Optional:** Switch on **Add Resource to Area** to import the resources (including alarm inputs, alarm outputs, and access points) to an area.

Note

- You can create a new area by device name or select an existing area.
- You can import all the access points or specific access point(s) to the area.
- For the video access control terminal of a device, the camera on the terminal will also be imported to the corresponding area.
- If you do not import access points to area, you cannot perform further configurations for the access point.

9. Finish adding the device(s).
   - Click **Add** to add the device(s) and return to the device management page.
   - Click **Add and Continue** to add the device(s) and continue to add other devices.
10. **Optional:** Perform further operations on the added device(s).

Configure Device	Click ⚙ in the **Operation** column to enter the corresponding device configuration page to edit the time parameters, reboot the device, restore the device, or set other parameters. See ***Configure Device Parameters*** for detailed instructions.
Change Password	Select the added device(s) and click **Change Password** to change the password for the device(s).

Note

- You can only change the password for online HIKVISION devices currently.
- If the devices share the same password, you can select multiple devices to change the password together.

Restore Default

Select the added device(s) and click **Restore** to restore the configured device parameters excluding network parameters and account information.

Note

If you want to restore all the device parameters, you should check **Restore device parameters excluding network parameters and account information, such as user name and password.** in the pop-up window.

8.4.3 Add Access Control Devices by IP Segment

If the access control devices you want to add to the platform share the same user account, and they are in the same IP segment, you can add them to the platform by specifying the start/end IP address, user name, password, etc.

Before You Start

- Make sure the devices you are going to add 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 HikCentral Professional via network.
- Make sure you have activated the devices. Refer to ***Create Password for Inactive Device(s)*** for detailed instructions on activating devices.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Select **Device and Server** → **Access Control Device** on the left.
3. Click **Add** to enter the Add Access Control Device page.
4. Select **Hikvision Private Protocol** as the access protocol.
5. Select **IP Segment** as the adding mode.
6. Enter the required the information.

   Note

   By default, the device port number 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 change your password regularly, especially in the high security system, changing 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:** Select a time zone for the device in drop-down list of **Time Zone of Device**.

Note

You can check **Apply to Device** so that when the time zone of the device and the system are not consistent, the system will automatically apply the time zone settings to the device.

8. **Optional:** Switch on **Add Resource to Area** to import the resources (including alarm inputs, alarm outputs, and access points) to an area.

Note

- You can create a new area by device name or select an existing area.
- You can import all the access points or specific access point(s) to the area.
- For the video access control terminal of a device, the camera on the terminal will also be imported to the corresponding area.
- If you do not import access points to area, you cannot perform further configurations for the access point.

9. Finish adding the device(s).
   - Click **Add** to add the device(s) and return to the device management page.
   - Click **Add and Continue** to add the device(s) and continue to add other devices.
10. **Optional:** Perform further operations on the added device(s).

Configure Device
Click ⚙ in the **Operation** column to enter the corresponding device configuration page to edit the time parameters, reboot the device, restore the device, or set other parameters. See ***Configure Device Parameters*** for detailed instructions.

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

Note

- You can only change the password for online HIKVISION devices currently.
- If the devices share the same password, you can select multiple devices to change the password together.

Restore Default

Select the added device(s) and click **Restore** to restore the configured device parameters excluding network parameters and account information.

Note

If you want to restore all the device parameters, you should check **Restore device parameters excluding network parameters and account information, such as user name and password.** in the pop-up window.

8.4.4 Add an Access Control Device by Device ID

For access control devices supporting ISUP 4.0 or later protocol, you can add them by specifying a predefined device ID and key. This is a cost-effective choice when you need to manage access control devices that do not have fixed IP addresses.

Before You Start

- Make sure the devices you are going to add 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 HikCentral Professional via network.
- Make sure you have activated the devices. Refer to ***Create Password for Inactive Device(s)*** for detailed instructions on activating devices.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Select **Device and Server** → **Access Control Device** on the left.
3. Click **Add** to enter the Add Access Control Device page.
4. Select **Hikvision ISUP Protocol** as the access protocol.
5. Select **Device ID** as the adding mode.
6. Enter the required the information.
7. Switch on **Picture Storage** to set the storage location for pictures.
    1) Select the storage device from the drop-down list.
    2) Select storage locations for face picture library and captured pictures.

Note

The storage location of captured pictures and face picture libraries cannot be the same.

8. **Optional:** Select a time zone for the device in drop-down list of **Time Zone of Device**.

Note

You can check **Apply to Device** so that when the time zone of the device and the system are not consistent, the system will automatically apply the time zone settings to the device.

9. **Optional:** Switch on **Add Resource to Area** to import the resources (including alarm inputs, alarm outputs, and access points) to an area.

Note

- You can create a new area by device name or select an existing area.
- You can import all the access points or specific access point(s) to the area.
- For the video access control terminal of a device, the camera on the terminal will also be imported to the corresponding area.
- If you do not import access points to area, you cannot perform further configurations for the access point.

10. Finish adding the device(s).
    - Click **Add** to add the device(s) and return to the device management page.
    - Click **Add and Continue** to add the device(s) and continue to add other devices.
11. **Optional:** Perform further operations on the added device(s).

Configure Device

Click ⚙ in the **Operation** column to enter the corresponding device configuration page to edit the time parameters, reboot the device, restore the device, or set other parameters. See ***Configure Device Parameters*** for detailed instructions.

Change Password

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

Note

- You can only change the password for online HIKVISION devices currently.
- If the devices share the same password, you can select multiple devices to change the password together.

Restore Default

Select the added device(s) and click **Restore** to restore the configured device parameters excluding network parameters and account information.

Note

If you want to restore all the device parameters, you should check **Restore device parameters excluding network parameters and account information, such as user name and password.** in the pop-up window.

8.4.5 Add Access Control Devices by Device ID Segment

If you need to add multiple access control devices which support ISUP 5.0 protocol and have no fixed IP addresses to the platform, you can add them all at once after configuring a device ID segment for the devices.

Before You Start

- Make sure the devices you are going to add 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 HikCentral Professional via network.
- Make sure you have activated the devices. Refer to ***Create Password for Inactive Device(s)*** for detailed instructions on activating devices.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Select **Device and Server** → **Access Control Device** on the left.
3. Click **Add** to enter the Add Access Control Device page.
4. Select **Hikvision ISUP Protocol** as the access protocol.
5. Select **Device ID Segment** as the adding mode.
6. Enter the required parameters.
7. Switch on **Picture Storage** to set the storage location for pictures.
   1) Select the storage device from the drop-down list.
   2) Select storage locations for face picture library and captured pictures.

   Note

   The storage location of captured pictures and face picture libraries cannot be the same.
8. **Optional:** Select a time zone for the device in drop-down list of **Time Zone of Device**.

   Note

   You can check **Apply to Device** so that when the time zone of the device and the system are not consistent, the system will automatically apply the time zone settings to the device.
9. **Optional:** Switch on **Add Resource to Area** to import the resources (including alarm inputs, alarm outputs, and access points) to an area.

Note

- You can create a new area by device name or select an existing area.
- You can import all the access points or specific access point(s) to the area.
- For the video access control terminal of a device, the camera on the terminal will also be imported to the corresponding area.
- If you do not import access points to area, you cannot perform further configurations for the access point.

10. Finish adding the device(s).
- Click **Add** to add the device(s) and return to the device management page.
- Click **Add and Continue** to add the device(s) and continue to add other devices.

11. **Optional:** Perform further operations on the added device(s).

Configure Device
Click ⚙ in the **Operation** column to enter the corresponding device configuration page to edit the time parameters, reboot the device, restore the device, or set other parameters. See ***Configure Device Parameters*** for detailed instructions.

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

Note

- You can only change the password for online HIKVISION devices currently.
- If the devices share the same password, you can select multiple devices to change the password together.

Restore Default
Select the added device(s) and click **Restore** to restore the configured device parameters excluding network parameters and account information.

Note

If you want to restore all the device parameters, you should check **Restore device parameters excluding network parameters and account information, such as user name and password.** in the pop-up window.

8.4.6 Add Access Control Devices in a Batch

You can download and enter access control device information in the predefined spreadsheet to add multiple devices at a time.

Before You Start

- Make sure the devices you are going to add 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 HikCentral Professional via network.
- Make sure you have activated the devices. Refer to ***Create Password for Inactive Device(s)*** for detailed instructions on activating devices.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules → General → Resource Management** .
2. Select **Device and Server → Access Control Device** on the left.
3. Click **Add** to enter the Add Access Control Device page.
4. Select **Hikvision Private Protocol** or **Hikvision ISUP Protocol** as the access protocol.
5. Select **Batch Import** as the adding mode.
6. Click **Download Template** and save the predefined spreadsheet (XLSX format) to local disk.
7. Open the spreadsheet and edit the required device information.
8. Click ··· and select the edited spreadsheet.
9. **Optional:** Select a time zone for the device in drop-down list of **Time Zone of Device**.

Note

You can check **Apply to Device** so that when the time zone of the device and the system are not consistent, the system will automatically apply the time zone settings to the device.

10. Finish adding the device(s).
    - Click **Add** to add the device(s) and return to the device management page.
    - Click **Add and Continue** to add the device(s) and continue to add other devices.
11. **Optional:** Perform further operations on the added device(s).

Configure Device

Click ⚙ in the **Operation** column to enter the corresponding device configuration page to edit the time parameters, reboot the device, restore the device, or set other parameters. See ***Configure Device Parameters*** for detailed instructions.

Change Password

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

Note

- You can only change the password for online HIKVISION devices currently.
- If the devices share the same password, you can select multiple devices to change the password together.

Restore Default

Select the added device(s) and click **Restore** to restore the configured device parameters excluding network parameters and account information.

Note

If you want to restore all the device parameters, you should check **Restore device parameters excluding network parameters and account information, such as user name and password.** in the pop-up window.

8.4.7 Configure Device Parameters

You can configure parameters for the access control device, including device time, linkage settings (linked device actions), maintenance settings, etc.

Configure Wiegand Parameters

Based on the knowledge of uploading rule for the third-party Wiegand, you can configure Wiegand parameters to communicate between the device and the third-party card readers.

Before You Start

Make sure you have wired the third-party card readers to the access control device.

Steps

Note

- By default, the device disables the custom Wiegand function. If you enable the custom Wiegand function, all Wiegand ports in the device will use the customized Wiegand protocol.
- You can configure up to 5 custom Wiegand devices.

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Select **Device and Server** → **Access Control Device** on the left.
3. Click ⚙ in the Operation column to enter the configuration page of a device.
4. Switch on **Custom Wiegand**.
5. Configure the Wiegand parameters.

   Total Length

   Wiegand data length.

   Parity Type

   Set the valid parity for Wiegand data according to property of the third party card reader. You can select **Nothing**, **Odd Even Check**, or **XOR Parity**.

   If you select **Odd Even Check**, you can configure the following:

   Odd Start, Length

If the odd parity start bit is 1 and the length is 12, then the platform will start odd parity calculation from bit 1. It will calculate 12 bits. The result will be in bit 0 (Bit 0 is the first bit).

Even Start, Length

If the even parity start bit is 12, and the length is 12, then the platform will start even parity calculation from bit 12. It will calculate 12 bits. The result will be in the last bit.

If you select **XOR Parity**, you can configure the following:

XOR Parity Start Bit, Length per Group, Length for Parity

Depending on the table displayed below, the start bit is 0, the length per group is 4, and the length for parity is 40. It means that the platform will calculate from bit 0, calculate every 4 bit, and calculate 40 bits in total (10 groups in total). The result will be in the last 4 bits (The result length is the same as the length per group).

Output Rule

Set the output rule.

Card ID Start Bit, Length, and Decimal Digit

If you use the transformation rule, these items are available. Depending on the table displayed below, the card ID start bit is 0, the length is 32, and the decimal digit is 10. It represents that from bit 0, there are 32 bits represent the card ID. (The length here is calculated by bit.) And the decimal digit length is 10 bits.

Site Code Start Bit, Length, and Decimal Digit

If you use the transformation rule, these items are available. For detailed information, see the explanation of the card ID.

OEM Start Bit, Length, and Decimal Digit

If you use the transformation rule, these items are available. For detailed information, see the explanation of the card ID.

Manufacturer Code Start Bit, Length, and Decimal Digit

If you use the transformation rule, these items are available. Depending on the table displayed below, the manufacturer code start bit is 32, length is 8, and decimal digit is 3. It represents that from bit 32, there are 8 bits are manufacturer code. (The length here is calculated by bit.) And the decimal length is 3.

Note

Take Wiegand 44 for example, the setting values in the Custom Wiegand are as follows:

Custom Wiegand Name	Wiegand 44
Total Length	44
Transformation Rule (Decimal Digit)	byFormatRule[4]=[1][4][0][0]

Parity Type	XOR Parity				
Odd Parity Start Bit		Length			
Even Parity Start Bit		Length			
XOR Parity Start Bit	0	Length per Group	4	Total Length	40
Card ID Start Bit	0	Length	32	Decimal Digit	10
Site Code Start Bit		Length		Decimal Digit	
OEM Start Bit		Length		Decimal Digit	
Manufacturer Code Start Bit	32	Length	8	Decimal Digit	3

Configure Device Actions for Access Event

You can set the linkage actions of an access control device for the device's events, so that when a specific event occurs, the device can execute actions such as capturing a picture, recording video footage, triggering alarm output, triggering buzzer, arming/disarming zones, locking/unlocking access points, etc.

Steps

Note

This feature requires device support. Parameters vary with different device types and models.

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Select **Device and Server** → **Access Control Device** on the left.
3. Click ⚙ in the Operation column to enter the configuration page of a device.
4. Click **Add** in the Linkage section.
5. Configure event source.
   1) Select **Event Linkage** as the linkage type.
   2) Select an event type from the **Event Type** drop-down list and then select a specific event.

   Note

   - If you select **Alarm Input Event**, you need to select an alarm input.
   - If you select **Door Event**, you need to select an access point.
   - If you select **Card Reader Event**, you need to select a card reader.
6. Configure linkage target.

   Buzzing

Buzzer on Controller

ON

Turn on the buzzer on the access controller when the specified event is triggered.

OFF

Turn off the buzzer on the access controller when the specified event is triggered.

No Linkage

Disable the linkage action.

Buzzer on Reader

ON

Turn on the buzzer on the card reader when the specified event is triggered.

OFF

Turn off the buzzer on the card reader when the specified event is triggered.

No Linkage

Disable the linkage action.

Capture/Recording

Capture

Enable the device's linked camera to capture a picture when the specified event is triggered.

Recording

Enable the device's linked camera to record video footage when the specified event is triggered.

Alarm Output

ON

Trigger the alarm output when the specified event is triggered.

OFF

Stop the alarm output when the specified event is triggered.

No Linkage

Disable the linkage action.

Zone

ON

Arm the zone when the specified event is triggered.

OFF

Disarm the zone when the specified event is triggered.

No Linkage

Disable the linkage action.

Access Point

Unlock

Unlock the access point (door or barrier) when the specified event is triggered.

Lock

Lock the access point when the specified event is triggered.

Remain Unlocked

The access point will remain unlocked when the specified event is triggered.

Remain Locked

The access point will remain locked when the specified event is triggered.

No Linkage

Disable the linkage action.

7. Click **Save** to add the linkage.
8. **Optional:** Perform further operations on linkages.

Delete a Linkage	Click 🗑 to delete the linkage.
Delete All Linkages	Click **Delete All** to delete all linkages.
Edit Linkage	Click ✎ to edit the linkage.

Configure Device Actions for Card Swiping

You can set the linkage actions of an access control device for card swiping, so that when the device detects a specific card, the device can execute actions such as capturing a picture, triggering alarm output, triggering buzzer, locking/unlocking access point, etc. In this way, you can monitor the behaviors and whereabouts of the card holder.

Steps

Note

This feature requires device support. Parameters vary with different device types and models.

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Select **Device and Server** → **Access Control Device** on the left.
3. Click ⚙ in the Operation column to enter the configuration page of a device.
4. Click **Add** in the Linkage section.
5. Configure event source.
   1) Select **Card Linkage** as the linkage type.
   2) Select a card from the **Card Number** drop-down list.
   3) Select a card reader from the **Card Reader** drop-down list.
6. Configure linkage target.

Buzzing

Buzzer on Controller

ON

Turn on the buzzer on the access controller when the specified event is triggered.

OFF

Turn off the buzzer on the access controller when the specified event is triggered.

No Linkage

Disable the linkage action.

Buzzer on Reader

ON

Turn on the buzzer on the card reader when the specified event is triggered.

OFF

Turn off the buzzer on the card reader when the specified event is triggered.

No Linkage

Disable the linkage action.

Capture/Recording

Capture

Enable the device's linked camera to capture a picture when the specified event is triggered.

Recording

Enable the device's linked camera to record video footage when the specified event is triggered.

Alarm Output

ON

Trigger the alarm output when the specified event is triggered.

OFF

Stop the alarm output when the specified event is triggered.

No Linkage

Disable the linkage action.

Zone

ON

Arm the zone when the specified event is triggered.

OFF

Disarm the zone when the specified event is triggered.

No Linkage

Disable the linkage action.

Access Point

Unlock

Unlock the access point (door or barrier) when the specified event is triggered.

Lock

Lock the access point when the specified event is triggered.

Remain Unlocked

The access point will remain unlocked when the specified event is triggered.

Remain Locked

The access point will remain locked when the specified event is triggered.

No Linkage

Disable the linkage action.

7. Click **Save** to add the linkage.
8. **Optional:** Perform further operations on linkages.

Delete a Linkage	Click 🗑 to delete the linkage.
Delete All Linkages	Click **Delete All** to delete all linkages.
Edit Linkage	Click ✎ to edit the linkage.

Configure Device Actions for Person ID

You can set the linkage actions of an access control device for person ID, so that when the device detects the credentials of the person, it can execute actions such as capturing a picture, triggering alarm output, triggering buzzer, locking/unlocking access point, etc. In this way, you can monitor the behaviors and whereabouts of the person.

Steps

Note

This feature requires device support. Parameters vary with different device types and models.

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Select **Device and Server** → **Access Control Device** on the left.
3. Click ⚙ in the Operation column to enter the configuration page of a device.
4. Click **Add** in the Linkage section.
5. Configure event source.
   1) Select **Person Linkage** as the linkage type.
   2) Select a person ID from the **Person** drop-down list.
   3) Select a card reader from the **Card Reader** drop-down list.

6. Configure linkage target.

Buzzing

Buzzer on Controller

ON

Turn on the buzzer on the access controller when the specified event is triggered.

OFF

Turn off the buzzer on the access controller when the specified event is triggered.

No Linkage

Disable the linkage action.

Buzzer on Reader

ON

Turn on the buzzer on the card reader when the specified event is triggered.

OFF

Turn off the buzzer on the card reader when the specified event is triggered.

No Linkage

Disable the linkage action.

Capture/Recording

Capture

Enable the device's linked camera to capture a picture when the specified event is triggered.

Recording

Enable the device's linked camera to record video footage when the specified event is triggered.

Alarm Output

ON

Trigger the alarm output when the specified event is triggered.

OFF

Stop the alarm output when the specified event is triggered.

No Linkage

Disable the linkage action.

Zone

ON

Arm the zone when the specified event is triggered.

OFF

Disarm the zone when the specified event is triggered.

No Linkage

Disable the linkage action.

Access Point

Unlock

Unlock the access point (door or barrier) when the specified event is triggered.

Lock

Lock the access point when the specified event is triggered.

Remain Unlocked

The access point will remain unlocked when the specified event is triggered.

Remain Locked

The access point will remain locked when the specified event is triggered.

No Linkage

Disable the linkage action.

7. Click **Save** to add the linkage.
8. **Optional:** Perform further operations on linkages.

Delete a Linkage	Click 🗑 to delete the linkage.
Delete All Linkages	Click **Delete All** to delete all linkages.
Edit Linkage	Click ✎ to edit the linkage.

Configure Device Actions for MAC Address

You can set access control device's linkage actions for MAC address of mobile devices, so that when the device detects a specific MAC address, the device can execute actions such as capturing a picture, triggering alarm output, triggering buzzer, locking/unlocking access point, etc.

Steps

Note

This feature requires device support. Parameters vary with different device types and models.

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Select **Device and Server** → **Access Control Device** on the left.
3. Click ⚙ in the Operation column to enter the configuration page of a device.
4. Click **Add** in the Linkage section.
5. Select **MAC Linkage** as the linkage type, and then edit the MAC address.
6. Configure linkage target.

Buzzing

Buzzer on Controller

ON

Turn on the buzzer on the access controller when the specified event is triggered.

OFF

Turn off the buzzer on the access controller when the specified event is triggered.

No Linkage

Disable the linkage action.

Buzzer on Reader

ON

Turn on the buzzer on the card reader when the specified event is triggered.

OFF

Turn off the buzzer on the card reader when the specified event is triggered.

No Linkage

Disable the linkage action.

Capture/Recording

Capture

Enable the device's linked camera to capture a picture when the specified event is triggered.

Recording

Enable the device's linked camera to record video footage when the specified event is triggered.

Alarm Output

ON

Trigger the alarm output when the specified event is triggered.

OFF

Stop the alarm output when the specified event is triggered.

No Linkage

Disable the linkage action.

Zone

ON

Arm the zone when the specified event is triggered.

OFF

Disarm the zone when the specified event is triggered.

No Linkage

Disable the linkage action.

Access Point

Unlock

Unlock the access point (door or barrier) when the specified event is triggered.

Lock

Lock the access point when the specified event is triggered.

Remain Unlocked

The access point will remain unlocked when the specified event is triggered.

Remain Locked

The access point will remain locked when the specified event is triggered.

No Linkage

Disable the linkage action.

7. Click **Save** to add the linkage.
8. **Optional:** Perform further operations on linkages.

Delete a Linkage	Click 🗑 to delete the linkage.
Delete All Linkages	Click **Delete All** to delete all linkages.
Edit Linkage	Click ✎ to edit the linkage.

Configure Card Swiping Parameters

You can configure card swiping parameters to allow authentication by entering card number on keypad, enable NFC clone card, enable Mifare encryption, etc.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Select **Device and Server** → **Access Control Device** on the left.
3. Click ⚙ in the Operation column to enter the configuration page of a device.
4. In Card Swiping section, configure card swiping parameters.

Note

Parameters vary with different device types and models.

Input Card Number On Keypad

If checked, visitors can enter card number on keypad for authentication.

Enable NFC Card

If enabled, visitors can use cloned cards for authentication.

Mifare Encryption

If enabled, only the card with the same encrypted sector can be granted access.

Voice Prompt

If enabled, an audio prompt will be played when swiping cards.

Upload Picture after Linked Capture

Upload the pictures captured by the linked camera(s) to the platform automatically.

Note

For details about linking a camera to an access point, see ***Edit Door for Current Site*** .

Picture Storage

If checked, the captured pictures will be automatically saved to the storage location you configured in picture storage settings for the access points.

Note

For details about configuring picture storage settings, see ***Edit Door for Current Site*** .

Picture Size

Select a picture size from the drop-down list for the captured pictures saved to the storage location.

Picture Quality

Select a picture quality from the drop-down list for the captured pictures saved to the storage location.

Configure Other Parameters

You can configure other parameters for an access control device and restore or reboot the device on the device configuration page.

Note

- Device support required. Parameters vary with different device types and models.
- For more remote configurations, click **Configuration** at the end of the device configuration page. For detailed instructions, refer to the user manual of the device.

Time

You can view the time zone where the device locates and set the following parameters.

Device Time

Click the **Device Time** field to custom time for the device.

Sync with Server Time

Synchronize the device time with the server of the platform.

Skin-surface Temperature

Set **Temperature Screening** to on to enable temperature screening function.

Threshold(℃)

Set the range of normal skin-surface temperature. The detected temperature that is not in this range is abnormal temperature. The maximum temperature must be higher than the minimum temperature.

Open Door When Temperature is Abnormal

If enabled, the door will open when person's skin-surface temperature is abnormal. By default, the door will not open for abnormal temperature.

Linked Thermal Camera

Enter the device IP address of the linked thermal camera for temperature screening.

Note

It is used for the access control devices that do not support temperature screening.

Mask Settings

Set **Mask Detection** to on to enable mask detection function. Once enabled, the device can detect persons without a face mask.

Open Barrier when No Mask

If checked, the barrier will still open for persons without a mask.

RS-485

RS-485 Communication Redundancy

You can check **RS-485 Communication Redundancy** to enable the function if you wire the RS-485 card to the device redundantly.

Turnstile Parameters

You can configure passing mode for the turnstile linked to the device.

Based on Lane Controller's DIP Mode

The device will follow the lane controller's DIP settings to control the turnstile. The settings on the main controller will be invalid.

Based on Main Controller's Settings

The device will follow the settings of main controller to control the turnstile. The DIP settings of the lane controller will be invalid.

Maintenance

You can reboot a device remotely and restore it to its default settings.

Reboot

Reboot the device.

Restore Default

Restore the device to its default settings. The device needs to be activated after restoring.

Facial Recognition Mode

You can check **Deep Mode** to enable the function. Once enabled, all the face credentials applied to the device will be cleared. Go to **Access Control → Access Level** and click 🗎 to apply the data in the platform to the device.

More

You can click **Configuration** to open the remote configuration page of the device and configure more parameters.

8.5 Manage Video Intercom Device

You can add video intercom devices (indoor station, door station, outer door station, and master station) to the system for management, including editing and deleting the devices, remote configuration, changing online devices' password, etc. You can also perform further operations such as video intercom, unlocking door remotely, etc. based on the added devices.

- **Indoor Station:** The indoor station is an intelligent terminal which can provide two-way audio, network transmission, data storage, remote unlocking, etc. It is mainly applied in the community.
- **Door Station:** The door station can send call to indoor station (residents) and master station. It is mainly applied in the community and office buildings.
- **Outer Door Station:** The outer door station can send call to indoor station (residents) and master station. It is mainly applied in the community and office buildings.
- **Master Station:** The master station is an intelligent terminal, which can be used to unlock door remotely, send call to residents and respond to residents' call. It is mainly applied in large community.

8.5.1 Add Online Video Intercom Device

The system can perform an automated detection for available video intercom devices (including indoor station, door station, outer door station, and master station) in the same local subnet with the current Web Client or SYS server. You can add one online device at a time to the system by specifying device name, password, device location information, etc.

Add a Detected Online Indoor Station

The online video intercom devices on the same local subnet with the current Web Client or SYS server can be displayed in the list, and you can add the detected indoor station to the system one by one.

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 HikCentral Professional via network.
- The devices to be added should be activated. Refer to ***Create Password for Inactive Device(s)*** for detailed operation about activating devices.

Steps

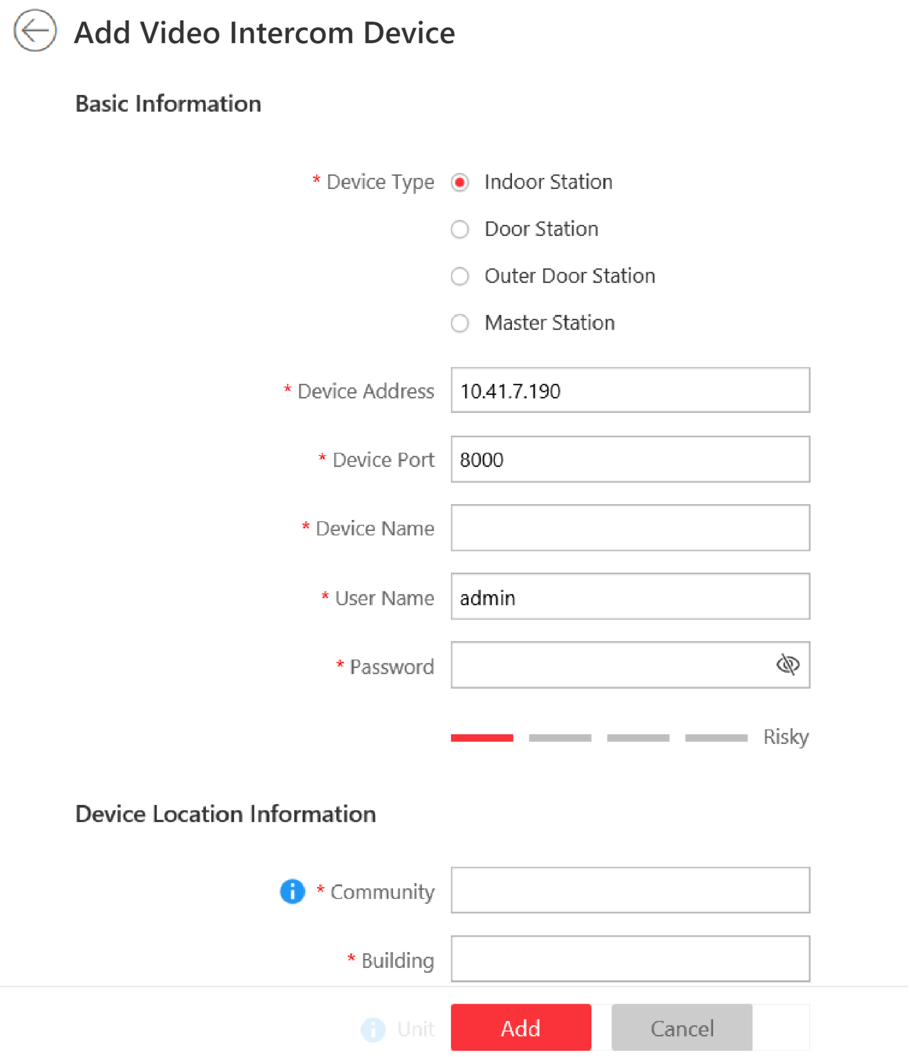
1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Video Intercom Device** on the left.
3. In the Online Device area, select a network type.

   Server Network

   As the default selection, the detected online devices on the same local subnet with the SYS server will be listed in the Online Device area.

   Local Network

   The detected online devices on the same local subnet with the current Web Client will be listed in the Online Device area.
4. In the Online Device area, select the active device to be added.
5. Click ⊕ in the Online Device area to open the Add Video Intercom Device window.
6. Select **Indoor Station** as the device type.



Add Video Intercom Device

Basic Information

* Device Type ● Indoor Station
○ Door Station
○ Outer Door Station
○ Master Station

* Device Address 10.41.7.190

* Device Port 8000

* Device Name

* User Name admin

* Password

Risky

Device Location Information

* Community

* Building

Unit

Figure 8-1 Add Video Intercom Device

7. Enter the required information.

Device Address

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

Device Port

The port No. of the device, which is shown automatically. The default port No. is 8000.

Device Name

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

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 change your password regularly, especially in the high security system, changing 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. Set the device location information, including community, building, unit (optional) and room.

Note

- You should enter an integer between 101 and 9999 in the **Room** Field. The room is composed of floor No. and room No. For example, for room 2 on the 12th floor, enter 1202.
- For example, if the device is located in community 1, building 2, unit 5, and room 305, you should enter 1, 2, 5, 305 respectively in the corresponding input box.

9. **Optional:** Select a time zone for the device in drop-down list of **Time Zone of Device**.

Note

You can check **Apply to Device** so that when the time zones of the device and the system are not consistent, the system will automatically apply the time zone settings to the device.

10. **Optional:** Switch **Add Resource to Area** to on to import the resources of the added devices to an area.

Note

- You can import all the alarm inputs or the specified alarm input to the corresponding area.
- You can create a new area by the device name or select an existing area.
- If you do not import resources to area, you cannot perform further operations for the alarm inputs.

11. In the Resident Information Area, click to select resident(s) to be linked with the device.

Note

Up to 10 residents can be linked to the device.

12. **Optional:** Check **Restore Default** to restore configured device parameters to default settings.

Note

- Not all the device parameters will be restored. Network parameters such as IP address, port No., and password will be kept.
- It is recommended that you should restore to default when adding an online device that has been added to other platforms for the first time.

13. Click **Add**.

14. Perform the following operation(s) after adding the online device.

Remote Configurations

Click ⚙ to set the remote configurations of the corresponding device. For details, refer to ***Configure Device Parameters*** .

Change Password

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

Note

- You can only change the password for online HIKVISION devices currently.
- If the devices have the same password, you can select multiple devices to change the password for them at the same time.

Add Related Camera

Click ◉ to relate camera(s) with the added indoor station(s). For details, refer to ***Relate Camera with Indoor Station*** .

Apply Device Settings

If the parameters in the system are inconsistent with the parameters on the video intercom device(s) after the device location information or device IP address is edited, ● will be displayed on the right side of the icon 🗎 . Click 🗎 to apply the current settings in the system to the device(s).

Restore Default

Select the added device(s), and click ⚙ to restore the configured device parameters.

Note

If you want to restore the device parameters configured on the system, you can check **Restore device network parameters and account information, such as user name and password.** in the pop-up window.

Link Doorbell with Indoor Station

Click 🔔 to link the added doorbell(s) with indoor station(s). For details, refer to ***Relate Doorbell with Indoor Station*** .

Add a Detected Online Door Station

The online video intercom devices in the same local subnet with the current Web Client or SYS server can be displayed on the list, and you can add the detected door station to the system one by one.

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 HikCentral Professional via network.
- The devices to be added should be activated. Refer to ***Create Password for Inactive Device(s)*** for detailed operation about activating devices.

Steps

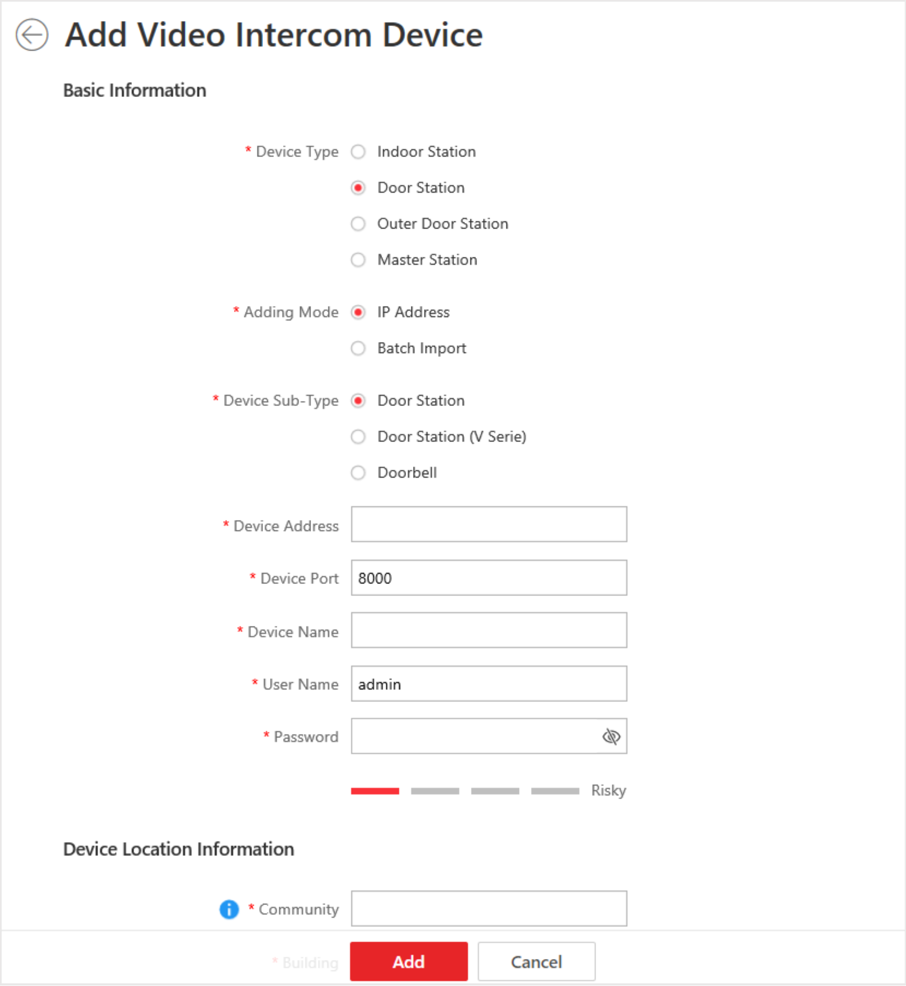
1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Video Intercom Device** on the left.
3. In the Online Device area, select a network type.

   Server Network

   As the default selection, the detected online devices in the same local subnet with the SYS server will be listed in the Online Device area.

   Local Network

   The detected online devices in the same local subnet with the current Web Client will be listed in the Online Device area.
4. In the Online Device area, select the active device to be added.
5. Click 🗋 in the Online Device area to open the Add Video Intercom Device window.
6. Select **Door Station** as the device type.



Add Video Intercom Device

Basic Information

* Device Type ○ Indoor Station
● Door Station
○ Outer Door Station
○ Master Station

* Adding Mode ● IP Address
○ Batch Import

* Device Sub-Type ● Door Station
○ Door Station (V Serie)
○ Doorbell

* Device Address

* Device Port 8000

* Device Name

* User Name admin

* Password

Risky

Device Location Information

* Community

* Building

Figure 8-2 Add Video Intercom Device

7. Select **Door Station**, **Door Station (V Serie)**, or **Doorbell** as the device sub-type.
8. Enter the required information.

Device Address

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

Device Port

The port No. of the device, which is shown automatically. The default port No. is 8000.

Device Name

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

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 change your password regularly, especially in the high security system, changing 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. Set the device location information, including community, building and unit (optional).

Note

For example, if the device is located in community 1, building 2, unit 5, you should enter 1, 2, 5 respectively in the corresponding input box.

10. **Optional:** Select an indoor station from the drop-down list to link the doorbell with an indoor station.

Note

For details, refer to ***Relate Doorbell with Indoor Station*** .

11. **Optional:** Select a time zone for the device in drop-down list of **Time Zone of Device**.

Note

You can check **Apply to Device** so that when the time zones of the device and the system are not consistent, the system will automatically apply the time zone settings to the device.

12. **Optional:** Switch **Add Resource to Area** to on to import the resources of the added devices to an area.

Note

- You can import all the resources (including cameras and doors) or the specified door to the corresponding area.
- You can create a new area by the device name or select an existing area.
- If you do not import resources to area, you cannot perform further operations such as such as live view, playback, etc., for the cameras.

13. Click **Add**.
14. Perform the following operation(s) after adding the online device.

Remote Configurations	Click ⚙ to set the remote configurations of the corresponding device. For details, refer to ***Configure Device Parameters*** .

Change Password

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

Note

- You can only change the password for online HIKVISION devices currently.
- If the devices have the same password, you can select multiple devices to change the password for them at the same time.

Apply Device Settings

In some cases such as you have edited the device location information or device IP address, the parameters in the system are inconsistent with the parameters on the video intercom device(s), and the icon ● will display on the right side of the 🖹 . Click 🖹 to apply the current settings in system to the device(s).

Restore Default

Select the added device(s), and click ⚙ to restore the configured device parameters.

Note

If you want to restore the device parameters configured on the system, you can check **Restore device network parameters and account information, such as user name and password.** in the pop-up window.

Add a Detected Online Outer Door Station

The online video intercom devices on the same local subnet with the current Web Client or SYS server can be displayed on the list, and you can add the detected outer door station to the system one by one.

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 HikCentral Professional via network.
- The devices to be added should be activated. Refer to ***Create Password for Inactive Device(s)*** for detailed operation about activating devices.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Video Intercom Device** on the left.
3. In the Online Device area, select a network type.

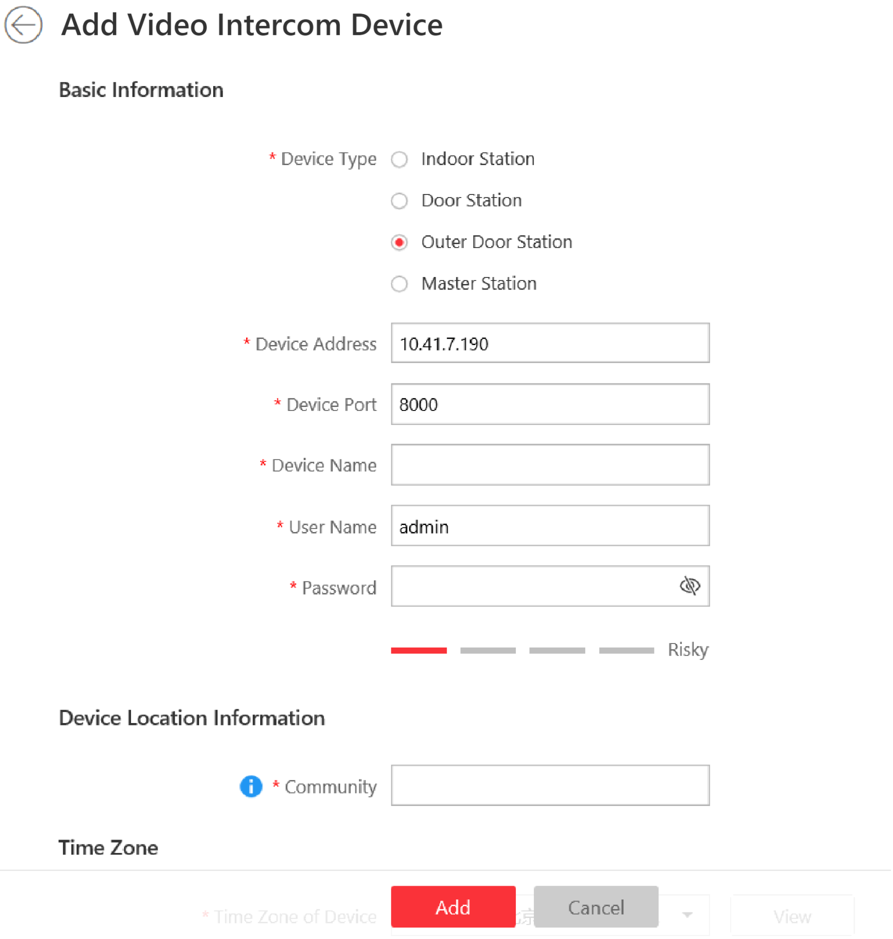
   Server Network

As the default selection, the detected online devices on the same local subnet with the SYS server will be listed in the Online Device area.

Local Network

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

4. In the Online Device area, select the active device to be added.
5. Click in the Online Device area to open the Add Video Intercom Device window.
6. Select **Outer Door Station** as the device type.



Add Video Intercom Device

Basic Information

* Device Type ○ Indoor Station ○ Door Station ● Outer Door Station ○ Master Station

* Device Address: 10.41.7.190

* Device Port: 8000

* Device Name:

* User Name: admin

* Password:

Risky

Device Location Information

* Community:

Time Zone

* Time Zone of Device

Figure 8-3 Add Video Intercom Device

7. Enter the required information.

Device Address

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

Device Port

The port No. of the device, which is shown automatically. The default port No. is 8000.

Device Name

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

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 change your password regularly, especially in the high security system, changing 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. Enter an integer in the **Community** field.

Note

If the community is divided into different sections, you should enter the corresponding number. If not, enter 1 in the input box.

9. **Optional:** Select a time zone for the device in drop-down list of **Time Zone of Device**.

Note

You can check **Apply to Device** so that when the time zones of the device and the system are not consistent, the system will automatically apply the time zone settings to the device.

10. **Optional:** Switch **Add Resource to Area** to on to import the resources of the added devices to an area.

Note

- You can import all the resources (including cameras and doors) or the specified door to the corresponding area.
- You can create a new area by the device name or select an existing area.
- If you do not import resources to area, you cannot perform further operations such as live view, playback, etc., for the cameras.

11. **Optional:** Check **Restore Default** to restore configured device parameters to default settings.

Note

- Not all the device parameters will be restored. Network parameters such as IP address, port No., and password will be kept.
- It is recommended that you should restore to default when adding an online device that has been added to other platforms for the first time.

12. Click **Add**.

Note

If you have checked **Restore Default** in Step 10, you should click **OK** confirm the settings.

13. Perform the following operation(s) after adding the online device.

Remote Configurations

Click ⚙ to set the remote configurations of the corresponding device. For details, refer to ***Configure Device Parameters*** .

Change Password

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

Note

- You can only change the password for online HIKVISION devices currently.
- If the devices have the same password, you can select multiple devices to change the password for them at the same time.

Apply Device Settings

When you have edited the device location information or device IP address, the parameters in the system are inconsistent with the parameters on the video intercom device(s), and the icon ⓘ will be displayed on the right side of the 🗎 . Click 🗎 to apply the current settings in the system to the device(s).

Restore Default

Select the added device(s), and click ⚙ to restore the configured device parameters.

Note

If you want to restore the device parameters configured on the system, you can check **Restore device network parameters and account information, such as user name and password.** in the pop-up window.

Add a Detected Online Master Station

The online video intercom devices on the same local subnet with the current Web Client or SYS server can be displayed on the list, and you can add the detected indoor station to the system one by one.

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 HikCentral Professional via network.
- The devices to be added should be activated. Refer to ***Create Password for Inactive Device(s)*** for detailed operation about activating devices.

Steps

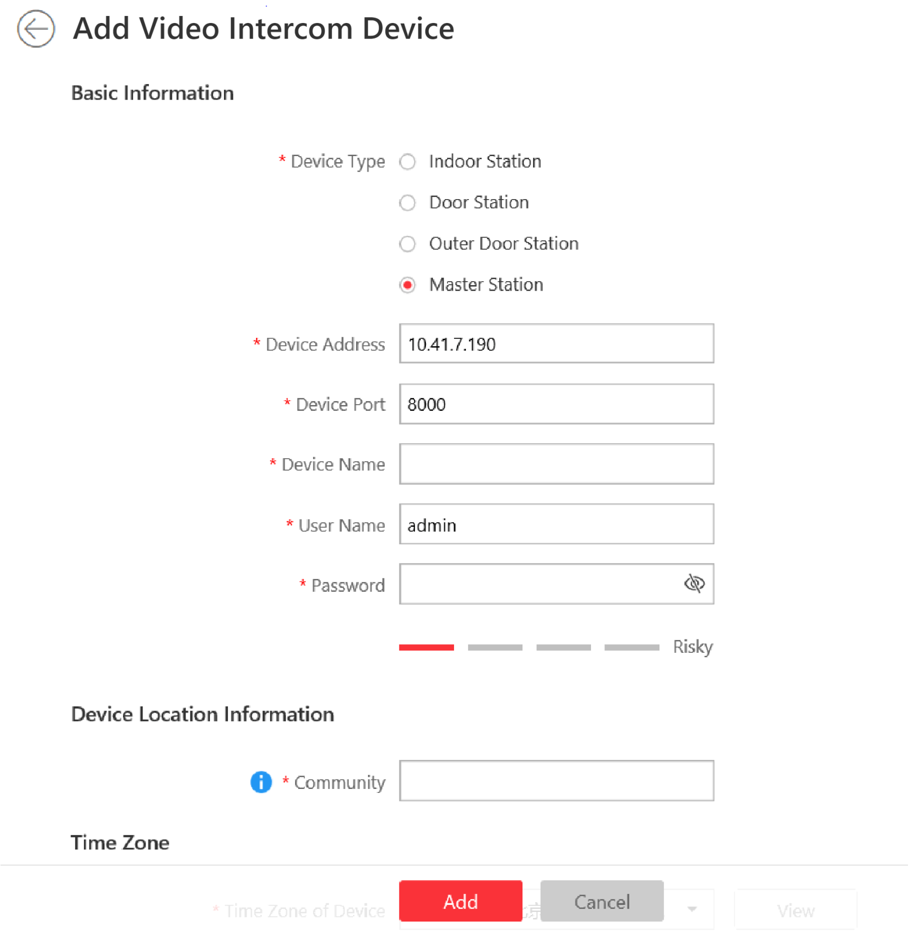
1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Video Intercom Device** on the left.
3. In the Online Device area, select a network type.

   Server Network

   As the default selection, the detected online devices in the same local subnet with the SYS server will be listed in the Online Device area.

   Local Network

   The detected online devices in the same local subnet with the current Web Client will be listed in the Online Device area.
4. In the Online Device area, select the active device to be added.
5. Click 🗋 in the Online Device area to open the Add Video Intercom Device window.
6. Select **Master Station** as the device type.



Add Video Intercom Device

Basic Information

* Device Type ○ Indoor Station ○ Door Station ○ Outer Door Station ● Master Station

* Device Address 10.41.7.190

* Device Port 8000

* Device Name

* User Name admin

* Password

Risky

Device Location Information

* Community

Time Zone

* Time Zone of Device

Figure 8-4 Add Video Intercom Device

7. Enter the required information.

Device Address

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

Device Port

The port No. of the device, which is shown automatically. The default port No. is 8000.

Device Name

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

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 change your password regularly, especially in the high security system, changing 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. Enter an integer in the **Community** field.

   ℹ **Note**

   If the community is divided into different sections, you should enter the corresponding number. If not, enter 1 in the input box.

9. **Optional:** Select a time zone for the device in drop-down list of **Time Zone of Device**.

   ℹ **Note**

   You can check **Apply to Device** so that when the time zones of the device and the system are not consistent, the system will automatically apply the time zone settings to the device.

10. **Optional:** Check **Restore Default** to restore configured device parameters to default settings.

    ℹ **Note**

    - Not all the device parameters will be restored. Network parameters such as IP address, port No., and password will be kept.
    - It is recommended that you should restore to default when adding an online device that has been added to other platforms for the first time.

11. Click **Add**.
12. Perform the following operation(s) after adding the online device.

    Remote Configurations
    Click ⚙ to set the remote configurations of the corresponding device. For details, refer to ***Configure Device Parameters*** .

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

    ℹ **Note**

    - You can only change the password for online HIKVISION devices currently.
    - If the devices have the same password, you can select multiple devices to change the password for them at the same time.

Apply Device Settings

When you have edited the device location information or device IP address, the parameters in the system are inconsistent with the parameters on the video intercom device(s), and the icon ⓘ will be displayed on the right side of the 🗎 . Click 🗎 to apply the current settings in the system to the device(s).

Restore Default

Select the added device(s), and click ⚙ to restore the configured device parameters.

Note

If you want to restore the device parameters configured on the system, you can check **Restore device network parameters and account information, such as user name and password.** in the pop-up window.

8.5.2 Add Indoor Station by IP Address

When you know the IP address of a indoor station, you can add it to the system by specifying the IP address, user name, password, etc. for management and further video intercom applications.

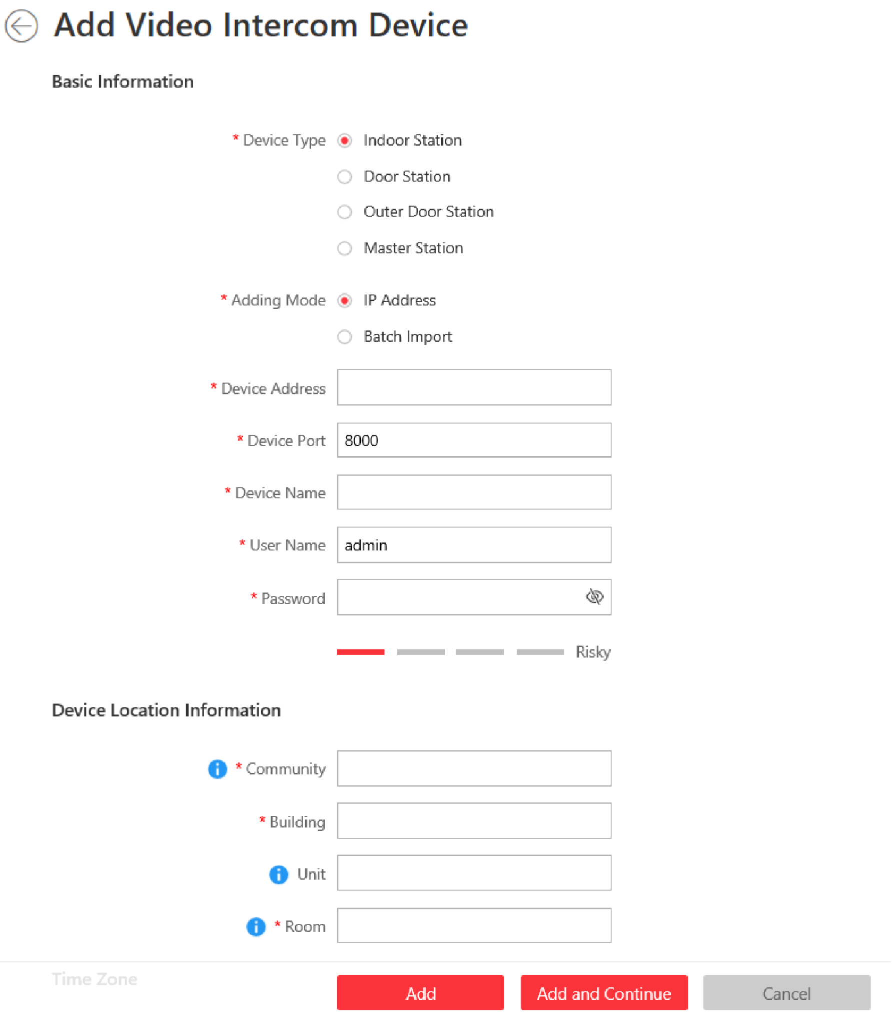
Before You Start

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 HikCentral Professional via network.

The system supports configuring calling priority for indoor stations. By default, the first indoor station added to the system is the main indoor station and the others are the indoor extensions.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Video Intercom Device** on the left.
3. Click + to enter Add Video Intercom Device page.
4. Select **Indoor Station** as the device type.



Add Video Intercom Device

Basic Information

* Device Type ● Indoor Station
○ Door Station
○ Outer Door Station
○ Master Station

* Adding Mode ● IP Address
○ Batch Import

* Device Address

* Device Port 8000

* Device Name

* User Name admin

* Password

Risky

Device Location Information

* Community

* Building

Unit

* Room

Time Zone

Figure 8-5 Add Indoor Station

5. Select **IP Address** as the adding mode.
6. Enter the required information.

   Device Address

   The IP address of the device.

   Device Port

   By default, the device port No. is 8000.

   Device Name

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

   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 change your password regularly, especially in the high security system, changing 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. Set the device location information, including community, building, unit (optional) and room.

Note

- You should enter an integer between 101 and 9999 in the **Room** Field. The room is composed of floor No. and room No. For example, for room 2 on the 12th floor, enter 1202.
- For example, if the device is located in community 1, building 2, unit 5, and room 305, you should enter 1, 2, 5, 305 respectively in the corresponding input box.

8. **Optional:** Select a time zone for the device in drop-down list of **Time Zone of Device**.

Note

You can check **Apply to Device** so that when the time zones of the device and the system are not consistent, the system will automatically apply the time zone settings to the device.

9. **Optional:** Switch **Add Resource to Area** to on to import the resources of the added devices to an area.

Note

- You can import all the alarm inputs or the specified alarm input to the corresponding area.
- You can create a new area by the device name or select an existing area.
- If you do not import resources to area, you cannot perform further operations for the alarm inputs.

10. In the Resident Information Area, click to select resident(s) to be linked with the device.

Note

Up to 10 residents can be linked to the device.

11. **Optional:** Check **Restore Default** so that all the parameters of the device configured on the system will be restored to default settings.
12. Finish adding the device.
    - Click **Add** to add the indoor station and back to the video intercom device list page.
    - Click **Add and Continue** to save the settings and continue to add the next indoor station.
13. Perform the following operation(s) after adding the devices.

Remote Configurations

Click ⚙ to set the remote configurations of the corresponding device. For details, refer to ***Configure Device Parameters*** .

Change Password

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

Note

- You can only change the password for online HIKVISION devices currently.
- If the devices have the same password, you can select multiple devices to change the password for them at the same time.

Add Related Camera

Click to relate camera(s) with the added indoor station(s). For details, refer to ***Relate Camera with Indoor Station*** .

Apply Device Settings

In some cases such as you have edited the device location information or device IP address, or the calling priority of the devices is changed, the parameters in the system are inconsistent with the parameters on the video intercom device(s), and the icon ℹ will be displayed on the right side of the . Click to apply the current settings in system to the device(s).

Link Doorbell with Indoor Station

Click 🔔 to link the added doorbell(s) with indoor station(s). For details, refer to ***Relate Doorbell with Indoor Station*** .

8.5.3 Add Door Station by IP Address

When you know the IP address of a door station, you can add it to the system by specifying the IP address, user name, password, etc., for management and further video intercom applications.

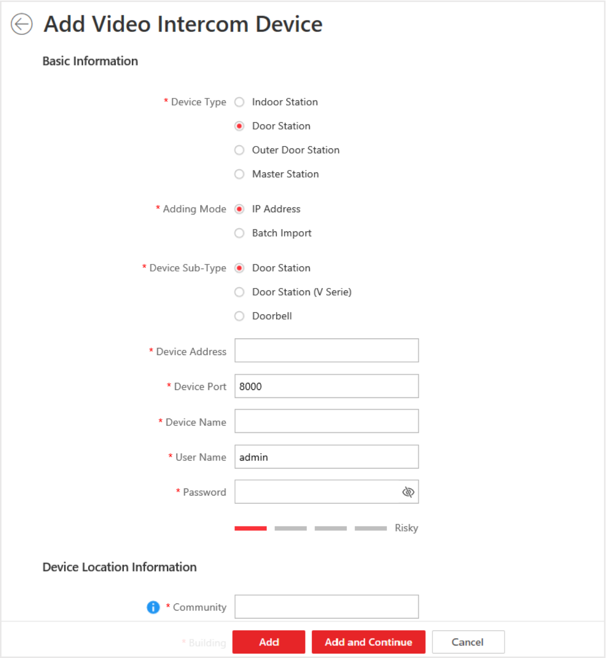
Before You Start

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 HikCentral Professional via network.

The system supports configuring calling priority for door stations. By default, the first door station added to the system is the main door station and the others are the sub door stations.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Video Intercom Device** on the left.
3. Click + to enter Add Video Intercom Device page.
4. Select **Door Station** as the device type.



Add Video Intercom Device

Basic Information

* Device Type ○ Indoor Station
● Door Station
○ Outer Door Station
○ Master Station

* Adding Mode ● IP Address
○ Batch Import

* Device Sub-Type ● Door Station
○ Door Station (V Serie)
○ Doorbell

* Device Address

* Device Port 8000

* Device Name

* User Name admin

* Password

Risky

Device Location Information

* Community

* Building

Figure 8-6 Add Door Station

5. Select **IP Address** as the adding mode.
6. Select **Door Station**, **Door Station (V Serie)**, or **Doorbell** as the device sub-type.
7. Enter the required information.

Device Address

The IP address of the device.

Device Port

By default, the device port No. is 8000.

Device Name

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

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 change your password regularly, especially in the high security system, changing 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. Set the device location information, including community, building and unit (optional).

   Note

   For example, if the device is located in community 1, building 2, unit 5, you should enter 1, 2, 5 respectively in the corresponding input box.

9. **Optional:** Select an indoor station from the drop-down list to link the doorbell with an indoor station.

   Note

   For details, refer to ***Relate Doorbell with Indoor Station*** .

10. **Optional:** Select a time zone for the device in drop-down list of **Time Zone of Device**.

    Note

    You can check **Apply to Device** so that when the time zones of the device and the system are not consistent, the system will automatically apply the time zone settings to the device.

11. **Optional:** Switch **Add Resource to Area** to on to import the resources of the added devices to an area.

    Note

    - You can import all the resources (including cameras and doors) or the specified door to the corresponding area.
    - You can create a new area by the device name or select an existing area.
    - If you do not import resources to area, you cannot perform further operations such as such as live view, playback, etc., for the cameras.

12. **Optional:** Check **Restore Default** so that all the parameters of the device configured on the system will be restored to default settings.
13. Finish adding the device.
    - Click **Add** to add the door station and back to the video intercom device list page.
    - Click **Add and Continue** to save the settings and continue to add the next door station.
14. Perform the following operation(s) after adding the devices.

Remote Configurations	Click ⚙ to set the remote configurations of the corresponding device. For details, refer to ***Configure Device Parameters*** .
Change Password	Select the added device(s) and click 🔑 to change the password for the device(s).

Note

- You can only change the password for online HIKVISION devices currently.
- If the devices have the same password, you can select multiple devices to change the password for them at the same time.

Apply Device Settings

When you have edited the device location information or device IP address, the parameters in the system are inconsistent with the parameters on the video intercom device(s), and the icon ⓘ will be displayed on the right side of the 🗎 . Click 🗎 to apply the current settings in the system to the device(s).

8.5.4 Add Outer Door Station by IP Address

When you know the IP address of an outer door station, you can add it to the system by specifying the IP address, user name, password, etc. for management and further video intercom applications.

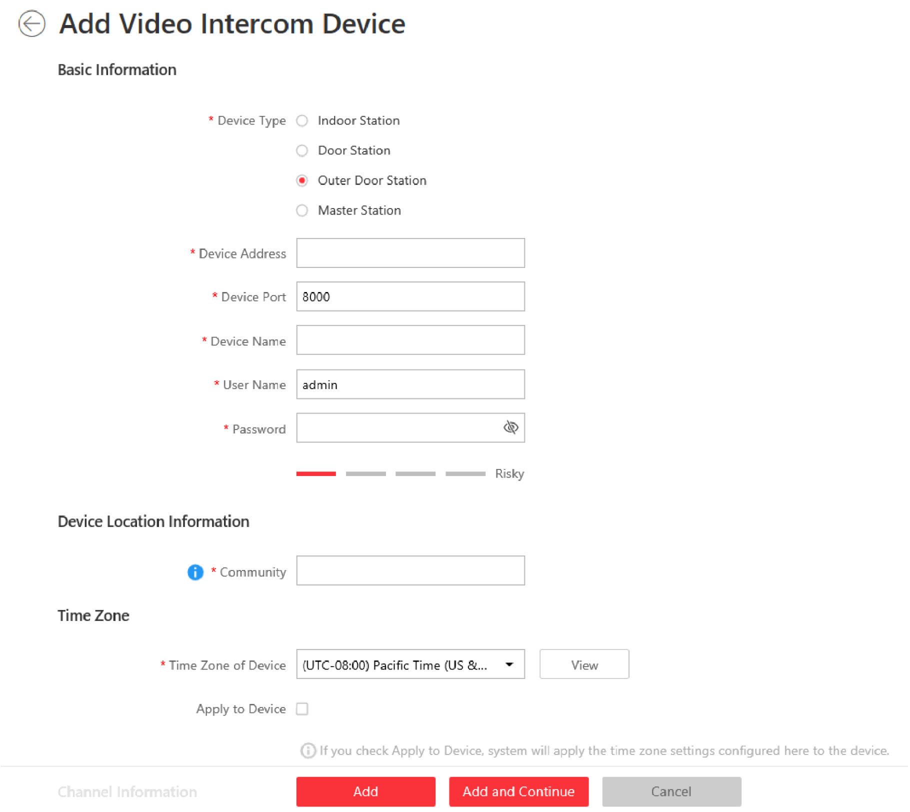
Before You Start

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 HikCentral Professional via network.

The system supports configuring calling priority for outer door stations. By default, the first outer door station added to the system is the main outer door station and the others are the sub outer door stations.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Video Intercom Device** on the left.
3. Click + to enter Add Video Intercom Device page.
4. Select **Outer Door Station** as the device type.



Add Video Intercom Device

Basic Information

* Device Type ○ Indoor Station
○ Door Station
● Outer Door Station
○ Master Station

* Device Address

* Device Port 8000

* Device Name

* User Name admin

* Password

Risky

Device Location Information

* Community

Time Zone

* Time Zone of Device (UTC-08:00) Pacific Time (US &... View

Apply to Device □

If you check Apply to Device, system will apply the time zone settings configured here to the device.

Figure 8-7 Add Outer Door Station

5. Enter the required information.

Device Address

The IP address of the device.

Device Port

By default, the device port No. is 8000.

Device Name

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

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 change your password regularly, especially in the high security system, changing 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. Enter an integer in the **Community** field.

Note

If the community is divided into different sections, you should enter the corresponding number. If not, enter 1 in the input box.

7. **Optional:** Select a time zone for the device in drop-down list of **Time Zone of Device**.

Note

You can check **Apply to Device** so that when the time zones of the device and the system are not consistent, the system will automatically apply the time zone settings to the device.

8. **Optional:** Switch **Add Resource to Area** to on to import the resources of the added devices to an area.

Note

- You can import all the resources (including cameras and doors) or the specified door to the corresponding area.
- You can create a new area by the device name or select an existing area.
- If you do not import resources to area, you cannot perform further operations such as live view, playback, etc., for the cameras.

9. **Optional:** Check **Restore Default** so that all the parameters of the device configured on the system will be restored to default settings.
10. Finish adding the device.
    - Click **Add** to add the outer door station and back to the video intercom device list page.
    - Click **Add and Continue** to save the settings and continue to add the next outer door station.
11. Perform the following operation(s) after adding the devices.

Remote Configurations	Click ⚙ to set the remote configurations of the corresponding device. For details, refer to ***Configure Device Parameters*** .
Change Password	Select the added device(s) and click 🔑 to change the password for the device(s). **Note** • You can only change the password for online HIKVISION devices currently. • If the devices have the same password, you can select multiple devices to change the password for them at the same time.

Apply Device Settings

In some cases such as you have edited the device location information or device IP address, or the calling priority of the devices is changed, the parameters in the system are inconsistent with the parameters on the video intercom device(s), and the icon ⓘ will be displayed on the right side of the 🗎 . Click 🗎 to apply the current settings in system to the device(s).

8.5.5 Add Master Station

When you know the IP address of a master station, you can add it to the system by specifying the IP address, user name, password, etc. for management and further video intercom applications.

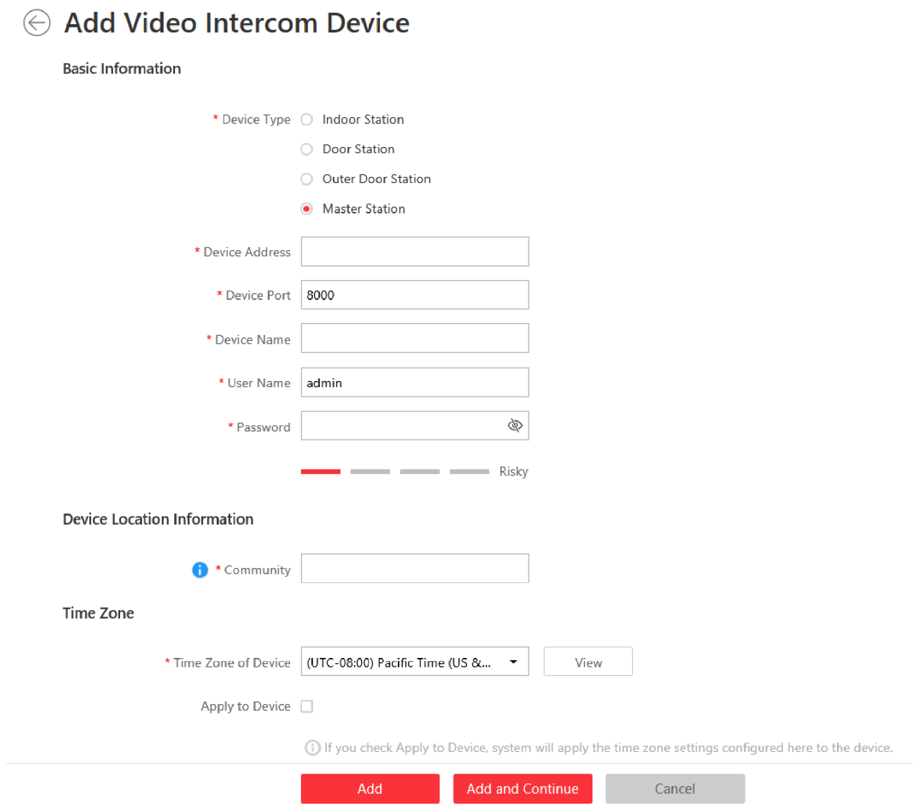
Before You Start

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 HikCentral Professional via network.

The system supports configuring calling priority for master stations. By default, the first master station added to the system is the main master station and the others are the sub master stations. The main master station can be used as the SIP server.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Video Intercom Device** on the left.
3. Click + to enter Add Video Intercom Device page.
4. Select **Master Station** as the device type.



Add Video Intercom Device

Basic Information

* Device Type
○ Indoor Station
○ Door Station
○ Outer Door Station
● Master Station

* Device Address

* Device Port: 8000

* Device Name

* User Name: admin

* Password

Risky

Device Location Information

* Community

Time Zone

* Time Zone of Device: (UTC-08:00) Pacific Time (US &...

Apply to Device □

If you check Apply to Device, system will apply the time zone settings configured here to the device.

Figure 8-8 Add Master Station

5. Enter the required information.

   Device Address

   The IP address of the device.

   Device Port

   By default, the device port No. is 8000.

   Device Name

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

   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 change your password regularly, especially in the high security system, changing 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. Enter an integer in the **Community** field.

   Note

   If the community is divided into different sections, you should enter the corresponding number. If not, enter 1 in the input box.

7. **Optional:** Select a time zone for the device in drop-down list of **Time Zone of Device**.

   Note

   You can check **Apply to Device** so that when the time zones of the device and the system are not consistent, the system will automatically apply the time zone settings to the device.

8. **Optional:** Check **Restore Default** so that all the parameters of the device configured on the system will be restored to default settings.
9. Finish adding the device.
   - Click **Add** to add the master station and back to the video intercom device list page.
   - Click **Add and Continue** to save the settings and continue to add the next master station.
10. Perform the following operation(s) 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

- You can only change the password for online HIKVISION devices currently.
- If the devices have the same password, you can select multiple devices to change the password for them at the same time.

Apply Device Settings

In some cases such as you have edited the device location information or the device IP address, or the calling priority of the devices is changed, the parameters in the system are inconsistent with the parameters on the video intercom device(s), and the icon ❗ will display on the right side of the 🗎 . Click 🗎 to apply the current settings in system to the device(s).

8.5.6 Add Indoor Stations and Door Stations in a Batch

You can add indoor stations and door stations in a batch to the system by entering the device information to the predefined template and importing the template to the system.

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 HikCentral Professional via network.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Video Intercom Device** on the left.
3. Click + to enter Add Video Intercom Device page.
4. Select **Indoor Station** or **Door Station** as the device type.
5. Click **Batch Import** as the adding mode.
6. Click **Download Template** to save the predefined template (Excel file) on your PC.
7. Open the exported template file and enter the required information of the devices to be added.
8. Click ··· and select the template file.
9. **Optional:** Select a time zone for the device in drop-down list of **Time Zone of Device**.

   Note

   You can check **Apply to Device** so that when the time zones of the device and the system are not consistent, the system will automatically apply the time zone settings to the device.

10. Finish adding the devices.
    - Click **Add** to add the door stations/outer door stations in a batch, and back to the video intercom device list page.
    - Click **Add and Continue** to save the settings and continue to add other door stations/outer door stations.
11. Perform the following operation(s) 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 - You can only change the password for online HIKVISION devices currently. - If the devices have the same password, you can select multiple devices to change the password for them at the same time.
Add Related Camera	Click to relate camera(s) with the added indoor station(s). For details, refer to ***Relate Camera with Indoor Station*** .

8.6 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, Axiom wireless security control panel, security radar etc., which are widely applied to many scenarios. You can also add the channels (including cameras, alarm inputs, alarm outputs and radars) of the security control device to the area.

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.

Security radar is an detecting device used to detect the target by electromagnetic wave. Security radar event will be triggered when the security radar detects object(s) entering the radar zone, and the calibration camera(s) will start to work to capture more details about this event.

8.6.1 Add Detected Online Device

The active online security control devices in the same local subnet with the current Web Client or SYS 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 a Detected Online Security Control 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 system via network.
- The devices to be added should be activated. Refer to ***Create Password for Inactive Device(s)*** for detailed operation about activating devices.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Security Control Device** .
3. 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 SYS 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.
4. In the Online Device area, select **Hikvision Private Protocol** or **Hikvision ISUP Protocol** to filter the detected online devices.
5. In the Online Device area, select the active device to be added.
6. Click ⎘ to open the Add Online Device window.
7. Enter the required information.

Note

The device's IP address and port number can be automatically shown in **Device Address** field and **Device Port** 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 change your password regularly, especially in the high security system, changing 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. **Optional:** Select a time zone for the device in drop-down list of **Time Zone of Device**.

Note

You can check **Apply to Device** so that when the time zone of the device and the system are not consistent, the system will automatically apply the time zone settings to the device.

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

Note

- You can select **Specified Alarm Input and Radar** and select the specified alarm inputs and radars 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 resources to area, you cannot perform the further configurations for the resources.

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 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** • You can only change the password for online HIKVISION devices currently. • If the devices have the same password, you can select multiple devices to change the password for them at the same time.

Add Detected Online Security Control 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 system via network.
- The devices to be added should be activated. Refer to ***Create Password for Inactive Device(s)*** for detailed operation about activating devices.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Security Control Device** .
3. In the Online Device area, select a network type.

   Server Network

   The detected online devices in the same local subnet with the SYS 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.
4. In the Online Device area, select **Hikvision Private Protocol** or **Hikvision ISUP Protocol** to filter the detected online devices.
5. In the Online Device area, select the active devices to be added.
6. Click ⎘ to open the Add Online Device window.
7. 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 change your password regularly, especially in the high security system, changing 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. **Optional:** Select a time zone for the device in drop-down list of **Time Zone of Device**.

Note

You can check **Apply to Device** so that when the time zone of the device and the system are not consistent, the system will automatically apply the time zone settings to the device.

9. **Optional:** Set the **Add Resource to Area** switch to on to import the resources (including cameras, alarm inputs, alarm outputs and radars) of the added security control device to an area.

Note

- You can select **Specified Alarm Input and Radar** and select the specified alarm inputs or radars 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 resources to area, you cannot perform the further configurations for the resources.

10. Click **Add**.
11. **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

- You can only change the password for online HIKVISION devices currently.
- If the devices have the same password, you can select multiple devices to change the password for them at the same time.

8.6.2 Add Security Control 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 system via network.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Security Control Device** .
3. Click **Add** to enter the Add Security Control Device page.
4. Select **Hikvision Private Protocol** as the Access Protocol.
5. Select **IP Address** as the adding mode.
6. Enter the required the information.

   Note

   - By default, the device port is 8000.
   - For wireless security control panel, the default port is 80.

   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 change your password regularly, especially in the high security system, changing 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:** Select a time zone for the device in drop-down list of **Time Zone of Device**.

   Note

   You can check **Apply to Device** so that when the time zone of the device and the system are not consistent, the system will automatically apply the time zone settings to the device.

8. **Optional:** Set the **Add Resource to Area** switch to on to import the resources (including cameras, alarm inputs, alarm outputs and radars) of the added security control device to an area.

   Note

   - You can select **Specified Alarm Input and Radar** and select the specified alarm inputs or radars 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 resources to area, you cannot perform further operations for the resources.
- Up to 10 radars can be imported in one area. If you don't import radars to area, you cannot perform further operations for the radars.

9. 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.

10. 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

- You can only change the password for online HIKVISION devices currently.
- If the devices have the same password, you can select multiple devices to change the password for them at the same time.

8.6.3 Add Security Control Device by Hik-Connect DDNS

You can add security control devices with dynamic IP addresses to the system by domain name solutions of Hik-Connect. Currently, the system only supports domain name solutions function of Hik-Connect.

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 system via network.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Security Control Device** .
3. Click **Add** to enter the Add Security Control Device page.
4. Select **Hikvision Private Protocol** as the Access Protocol.
5. Select **Hik-Connect DDNS** as the adding mode.

6. Select a device source.

   New Device

   Add a new device to both Hik-Connect and the system.

   Hik-Connect Device List

   Add devices managed by Hik-Connect to the system in a batch by getting the device list.

7. Set required parameters.

   Hik-Connect Server Address

   Enter the address of the Hik-Connect service. By default, it's ***https://open.ezvizlife.com***.

   Note

   If you select Hik-Connect Device List as source type, you can click **Get Device List** to get the device list in the account.

   Serial No.

   For adding a new device, enter the serial No. of the device.

   Verification Code

   For adding a new device, enter the verification code of the device.

8. **Optional:** Select a time zone for the device in drop-down list of **Time Zone of Device**.

   Note

   You can check **Apply to Device** so that when the time zone of the device and the system are not consistent, the system will automatically apply the time zone settings to the device.

9. **Optional:** Set the **Add Resource to Area** switch to on to import the resources (including cameras, alarm inputs, alarm outputs and radars) 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 resources to area, you cannot perform the further configurations for the resources.

10. 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.

11. **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

- You can only change the password for online HIKVISION devices currently.
- If the devices have the same password, you can select multiple devices to change the password for them at the same time.

8.6.4 Add Security Control Devices 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 system via network.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Security Control Device** .
3. Click **Add** to enter the Add Security Control Device page.
4. Select **Hikvision Private Protocol** as the Access Protocol.
5. Select **IP Segment** as the adding mode.
6. 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 change your password regularly, especially in the high security system, changing 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:** Select a time zone for the device in drop-down list of **Time Zone of Device**.

Note

You can check **Apply to Device** so that when the time zone of the device and the system are not consistent, the system will automatically apply the time zone settings to the device.

8. **Optional:** Set the **Add Resource to Area** switch to on to import the resources (including cameras, alarm inputs, alarm outputs and radars) 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 resources to area, you cannot perform the further configurations for the resources.

9. 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.
10. 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

- You can only change the password for online HIKVISION devices currently.
- If the devices have the same password, you can select multiple devices to change the password for them at the same time.

8.6.5 Add Security Control Devices 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 HikCentral Professional via network.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Security Control Device** .
3. Click **Add** to enter the Add Security Control Device page.
4. Select **Hikvision Private Protocol** as the Access Protocol.
5. Select **Port Segment** as the adding mode.
6. 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 change your password regularly, especially in the high security system, changing 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:** Select a time zone for the device in drop-down list of **Time Zone of Device**.

   Note

   You can check **Apply to Device** so that when the time zone of the device and the system are not consistent, the system will automatically apply the time zone settings to the device.

8. **Optional:** Set the **Add Resource to Area** switch to on to import the resources (including cameras, alarm inputs, alarm outputs and radars) 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 resources to area, you cannot perform the further configurations for the resources.

9. 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.

10. 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

- You can only change the password for online HIKVISION devices currently.
- If the devices have the same password, you can select multiple devices to change the password for them at the same time.

8.6.6 Add Security Control Device by Device ID

For the security control devices supporting ISUP, you can add them by specifying a predefined device ID, ISUP login password, etc. This is an economic choice when you need to manage a security control device in the public network but without fixed IP address by HikCentral Professional.

Before You Start

- Make sure the security control device 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 HikCentral Professional via network.
- Make sure you have enabled the ISUP registration function on the security control device. For details, refer to the user manual of security control device.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Security Control Device** .
3. Click **Add** to enter the Add Security Control Device page.
4. Select **Hikvision ISUP Protocol** as the Access Protocol.
5. Select **Device ID** as the adding mode.
6. Enter the required information, including device ID, ISUP login password, and device name.
7. **Optional:** In the Recording Settings field, set the **Video Storage** switch to on, and select the storage location from the drop-down list to store videos.
8. **Optional:** Select a time zone for the device in drop-down list of **Time Zone of Device**.

   Note

   You can check **Apply to Device** so that when the time zone of the device and the system are not consistent, the system will automatically apply the time zone settings to the device.

9. **Optional:** Set the **Add Resource to Area** switch to on to import the resources (including cameras, alarm inputs, alarm outputs and radars) 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 resources to area, you cannot perform the further configurations for the resources.

10. 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.
11. 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

- You can only change the password for online HIKVISION devices currently.
- If the devices have the same password, you can select multiple devices to change the password for them at the same time.

8.6.7 Add Security Control Device by Device ID Segment

If you need to add multiple security control devices which have no fixed IP address and support ISUP to HikCentral, you can add them to HikCentral Professional at a time after configuring a device ID segment for the devices.

Before You Start

- Make sure the security control device 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 HikCentral Professional via network.
- Make sure you have enabled the ISUP registration function on the security control device. For details, refer to the user manual of security control device.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Security Control Device** .
3. Click **Add** to enter the Add Security Control Device page.
4. Select **Hikvision ISUP Protocol** as the Access Protocol.
5. Select **Device ID Segment** as the adding mode.
6. Enter the required information, including the start device ID, the end device ID, and the ISUP login password.
7. **Optional:** In the Recording Settings field, set the **Video Storage** switch to on, and select the storage location from the drop-down list to store videos.
8. **Optional:** Select a time zone for the device in drop-down list of **Time Zone of Device**.

   Note

   You can check **Apply to Device** so that when the time zone of the device and the system are not consistent, the system will automatically apply the time zone settings to the device.

9. **Optional:** Set the **Add Resource to Area** switch to on to import the resources (including alarm inputs and radars) 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 resources to area, you cannot perform the further configurations for the resources.

10. 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.
11. 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

- You can only change the password for online HIKVISION devices currently.
- If the devices have the same password, you can select multiple devices to change the password for them at the same time.

8.6.8 Add Security Control Devices 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 device 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 HikCentral Professional via network.
- Make sure you have enabled the ISUP registration function on the security control device when adding devices via Hikvision ISUP. For details, refer to the user manual of security control device.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Security Control Device** .

3. Click **Add** to enter the Add Security Control Device page.
4. Select **Hikvision Private Protocol** or **Hikvision ISUP Protocol** as the Access Protocol.
5. Select **Batch Import** as the adding mode.
6. Click **Download Template** and save the predefined template (excel file) in your PC.
7. Open the exported template file and edit the required information of the devices to be added on the corresponding column.
8. Click ··· and select the template file.
9. **Optional:** In the Video Storage field, set the **Video Storage** switch to on, and select the storage location from the drop-down list to store video.

   Note

   This field displays when you select **Hikvision ISUP Protocol** as the access protocol.

10. **Optional:** Select a time zone for the device in drop-down list of **Time Zone of Device**.

    Note

    You can check **Apply to Device** so that when the time zone of the device and the system are not consistent, the system will automatically apply the time zone settings to the device.

11. 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.
12. 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** • You can only change the password for online HIKVISION devices currently. • If the devices have the same password, you can select multiple devices to change the password for them at the same time.

8.7 Manage Dock Station

You can add a dock station to the system by IP/domain. You can also add multiple dock stations to the system by IP segment, port segment, or importing a pre-defined template which contains the required dock stations' information.

8.7.1 Add Dock Station by IP/Domain

When you know the IP address or domain name of the dock station to be added, you can add the device to the system by specifying the IP address, user name, password, and other related parameters.

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 HikCentral Professional via network.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Dock Station** on the left.
3. Click **Add** to enter the Add Dock Station page.
4. Select **IP Address** as the adding mode.
5. Enter the required information.

   Device Address

   IP address or domain name of the dock station.

   User Name

   User name of the dock station.

   Password

   Password of the dock station.

6. **Optional:** Set time zone for the dock station.
   1) Select a time zone in drop-down list of **Time Zone of Device**.
   2) Set time zone of the dock station via the dock station's web page, and make sure the device's time zone is the same with the time zone selected in the previous sub-step.
7. Finish adding the dock station.
   - Click **Add** to add the current dock station and go back to the dock station list page.
   - Click **Add and Continue** to add the current dock station and add more other dock stations.
8. **Optional:** Perform the following operations after adding the dock station.

   Edit Dock Station Click the dock station alias on the device list to edit the dock station.

   Delete Dock Station Select dock station(s) and then click **Delete** to delete them.

8.7.2 Add Dock Stations by IP Segment

When multiple dock stations to be added have the same port number, user name, password, and have different IP addresses within a range, you can add devices by specifying the IP segment and some other related parameters.

Before You Start

Make sure the dock stations 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 HikCentral Professional via network.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Dock Station** on the left.
3. Click **Add** to enter the Add Dock Station page.
4. Select **IP Segment** as the adding mode.
5. Enter the required information.

   Device Address

   Enter the start IP address and the end IP address. For example, if five dock stations need to be added, and their IP address are "10.41.7.231", "10.41.7.232", "10.41.7.233", "10.41.7.234", and "10.41.7.235" respectively, you should enter ***10.41.7.231*** and ***10.41.7.235***.
6. **Optional:** Set time zone for the dock station.
   1) Select a time zone in drop-down list of **Time Zone of Device**.
   2) Set time zone of the dock station via the dock station's web page, and make sure the device's time zone is the same with the time zone selected in the previous sub-step.
7. Finish adding the dock stations.
   - Click **Add** to add the dock stations and back to the dock station list page.
   - Click **Add and Continue** to save the settings and continue to add more dock stations.
8. **Optional:** Perform the following operations after adding the dock stations.

Edit Dock Station	Click the dock station alias on the device list to edit the dock station.
Delete Dock Station	Select dock station(s) and then click **Delete** to delete them.

8.7.3 Add Dock Stations by Port Segment

When multiple dock stations to be added have the same IP address, user name, password, and have different port numbers within a range, you can add devices by specifying the port segment and some other related parameters.

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 HikCentral Professional via network.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Dock Station** on the left.
3. Click **Add** to enter the Add Dock Station page.
4. Select **Port Segment** as the adding mode.
5. Enter the required information.

   Device Address

   The same IP address where the devices are located.

   Device Port

   Enter the start port number and the end port number. For example, if there are five dock stations need to be added, and their port number are 80, 81, 82, 83, and 84 respectively, you should enter ***80*** and ***84***.

   User Name

   The same user name of the dock stations.

   Password

   The same password of the dock stations.
6. **Optional:** Set time zone for the dock station.
   1) Select a time zone in drop-down list of **Time Zone of Device**.
   2) Set time zone of the dock station via the dock station's web page, and make sure the device's time zone is the same with the time zone selected in the previous sub-step.
7. Finish adding the device.
   - Click **Add** to add the dock stations and back to the dock station list page.
   - Click **Add and Continue** to save the settings and add more dock stations by port segment.
8. **Optional:** Perform the following operations after adding the dock stations.

Edit Dock Station	Click the dock station alias on the device list to edit the dock station.
Delete Dock Station	Select dock station(s) and then click **Delete** to delete them.

8.7.4 Add Dock Stations in Batch

When there are multiple dock stations need to be added to HikCentral Professional, you can download a predefined template and fill in the required information about the dock stations, and then import the template to the system to add multiple dock stations at a time.

Before You Start

Make sure the dock stations you are going to use are correctly installed and connected to the network as specified by the manufacturer. Such initial configuration is required in order to be able to connect the device to the HikCentral Professional via network.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Dock Station** on the left.
3. Click **Add** to open the Add Dock Station page.
4. Select **Batch Import** as the adding mode.
5. Click **Download Template** and save the predefined template (CSV file) on your PC.
6. Open the template file and enter the required information of the devices to be added on the corresponding column.
7. Click ··· and select the template file.
8. **Optional:** Set time zone for the dock station.
   1) Select a time zone in drop-down list of **Time Zone of Device**.
   2) Set time zone of the dock station via the dock station's web page, and make sure the device's time zone is the same with the time zone selected in the previous sub-step.
9. Finish adding the dock stations.
   - Click **Add** to add the dock stations and back to the dock station list page.
   - Click **Add and Continue** to save the settings and continue to add more dock stations.
10. **Optional:** Perform the following operation(s) after adding the dock stations.

Edit Dock Station	Click the dock station alias on the device list to edit the dock station.
Delete Dock Station	Select dock station(s) and then click **Delete** to delete them.

8.8 Network Transmission Device Management

Network transmission devices (switch, network bridge and fiber converter) can be added to the system for management, to help the system monitor the network status of the managed devices.

After the network transmission devices are added to the system, the Control Client will automatically draw a network topology according to the location of the added devices, and display the information (IP address, port No., port status and stream rate) and network link status (fluent, busy, congested, disconnected).

8.8.1 Add Online Network Transmission Device

The system can perform an automated detection for available network transmission device s in the network where the Web Client or 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 a Detected Online Network Transmission 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 only one device every time to add it to HikCentral Professional. 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 network device (switch, bridge or fiber converter) you are going to use is 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 device to the HikCentral Professional via network.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Network Transmission Device** on the left.
3. In the Online Device area, select a network type.

   Server Network

   The detected online devices in the same local subnet with the SYS server will be listed.

   Local Network

   The detected online devices in the same local subnet with the Web Client will be listed.
4. In the Online Device area, select the active device to be added.
5. Click **Add to Device List** to open the Add Encoding Device window.
6. 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.

   Device Name

   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 HikCentral Professional 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 change your password regularly, especially in the high security system, changing 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. Click **Add**.
8. **Optional:** Perform the following operations after adding the device.

Remote Configuration

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 🔑 **Change Password** to change the password for the device(s).

Note

- You can only change the password for online HIKVISION devices currently.
- If the devices have the same password, you can select multiple devices to change the password for them at the same time.

Set the System Connected Device

Select the device, click ⚙ **System Connected Switch** to set the switch as the system connected device.

Note

System connected switch is the switch that is directly connected with the SYS server.

Add Detected Online Network Transmission Devices in a Batch

For the detected online transmission network devices, if they have the same user name and password, you can add multiple devices to HikCentral Professional at a time.

Before You Start

Make sure the network devices (switch, bridge or fiber converter) 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 HikCentral Professional via network.

Steps

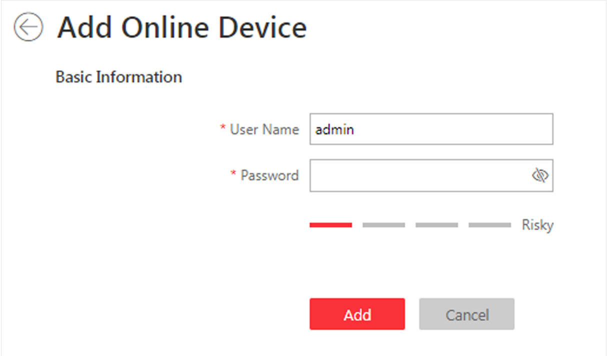
1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Network Transmission Device** on the left.
3. In the Online Device area, select a network type.

   Server Network

   The detected online devices in the same local subnet with the SYS server will be listed.

   Local Network

   The detected online devices in the same local subnet with the Web Client will be listed.
4. In the Online Device area, select the devices to be added.
5. Click **Add to Device List** to enter the Add Online Device window.



Add Online Device

Basic Information

* User Name: admin

* Password:

Figure 8-9 Add Online Devices in a Batch

6. Enter 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 HikCentral Professional 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 change your password regularly, especially in the high security system, changing 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. Click **Add**.
8. **Optional:** Perform the following operations after adding devices.

Remote Configuration

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 🔑 **Change Password** to change the password for the device(s).

Note

- You can only change the password for online HIKVISION devices currently.
- If the devices have the same password, you can select multiple devices to change the password for them at the same time.

Set the System Connected Device

Select the device, click ⚙ **System Connected Switch** to set the switch as the system connected device.

Note

System connected switch is the switch that is directly connected with the SYS server.

8.8.2 Add Network Transmission Device by IP Address

When you know the IP address of a device, you can add it to the system by specifying the IP address, user name, password, etc.

Before You Start

Make sure the network device (switch, bridge or fiber converter) you are going to use is 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 device to the HikCentral Professional via network.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Network Transmission Device** on the left.
3. Click **Add** to enter the Add Network Transmission Device window.
4. Select **IP Address** as the adding mode.
5. Enter the required information.

   Device Address

   Enter the IP address of the device.

   Device Port

   The default device port is 8000.

   Device Name

   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 administrator account which is created when activating the device, or the non-administrator account, such as operator. When adding device by non-administrator, the permission might be limited.

   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 change your password regularly, especially in the high security system, changing 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. Finish adding the device.
   - Click **Add** to add the current device and back to the device list page.
   - Click **Add and Continue** to finish adding the current device and continue adding other devices.
7. **Optional:** Perform the following operations after adding devices.

Remote Configuration	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 **Change Password** to change the password for the device(s).

Note

- You can only change the password for online HIKVISION devices currently.
- If the devices have the same password, you can select multiple devices to change the password for them at the same time.

Set the System Connected Device

Select the device, click **System Connected Switch** to set the switch as the system connected device.

Note

System connected switch is the switch that is directly connected with the SYS server.

8.8.3 Import Network Transmission Devices in a Batch

If there are large number of devices to be added, you can enter the device information in the pre-defined template and upload the template to add the network transmission devices in a batch.

Before You Start

Make sure the network devices (switch, bridge or fiber converter) 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 HikCentral Professional via network.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Network Transmission Device** on the left.
3. Click **Add** to enter the Add Network Transmission Device window.
4. Select the adding mode as **Batch Import**.
5. Click **Download Template** to download the template to the local PC.
6. Open the downloaded template file, and enter the required device information.
7. Click ··· to select the edited template file.
8. Finish adding the device.
   - Click **Add** to add the current device and back to the device list page.

- Click **Add and Continue** to finish adding the current device and continue adding other devices.

9. **Optional:** Perform the following operations after adding devices.

Remote Configuration

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 🔑 **Change Password** to change the password for the device(s).

Note

- You can only change the password for online HIKVISION devices currently.
- If the devices have the same password, you can select multiple devices to change the password for them at the same time.

Set the System Connected Device

Select the device, click ⚙ **System Connected Switch** to set the switch as the system connected device.

Note

System connected switch is the switch that is directly connected with the SYS server.

8.9 Add Display Screen

Display screens can be used in places such as the entrance of the parking lot to indicate the real-time number of the free parking spaces so that the drivers can find a parking space easily. You can add a display screen to the system by entering its LAN IP address and setting a name for the display screen.

In the top left corner of Home page, select ≡ → **All Modules → General → Resource Management → Device and Server → Display Screen** . Click **Add** to enter the adding display screen page.

Enter the **LAN IP address** of the display screen and set a name for it.

Click **Add** to finish adding the display screen, or click **Add and Continue** to continue adding other display screens.

Note

After adding a display screen, you should link a lane with the display screen and configure the related information for the screen via the system.

8.10 Upgrade Device Firmware

You can upgrade the firmwares of the devices added to the system via the current Web Client or Hik-Connect.

Via Current Web Client

The following devices are supported to be upgraded the firmwares via the current Web Client:

Table 8-1 Device List

No.	Device Type
1	Camera
2	NVR (Network Video Recorder)
3	DVR (Digital Video Recorder)
4	Decoding Device
5	Access Control Device
6	Card Reader
7	Security Control Panel (including Axiom Security Control Panel)
8	Security Radar
9	Indoor Station
10	Door Station **Note** Upgrading the card reader linked to the door station is not supported.
11	Master Station

Note

You can also upgrade the cameras access to the NVR in a batch.

Via Hik-Connect

The following devices are supported to be upgraded the firmwares via Hik-Connect:

Table 8-2 Device List

No.	Device Type
1	Camera
2	NVR
3	DVR
4	Indoor Station
5	Door Station **Note** Upgrading the card reader linked to the door station is not supported.
6	Master Station

Note

You can also upgrade the cameras linked to the NVR in a batch.

8.10.1 Upgrade Device Firmware via Current Web Client

You can upgrade device firmware via the current Web Client.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Click **Firmware Upgrade** on the left.
3. Select the **Via Current Web Client** tab.
4. In **Upgrade By** field, select the upgrade method.
5. In **Simultaneous Upgrade** field, set the maximum number of devices for simultaneous upgrade.

   Example

   If you set the value to 5, up to 5 devices can be selected for batch upgrade.
6. Select a upgrade package from the local computer and then click **Next**.

   The upgradable devices will be displayed.
7. **Optional:** Filter devices by device type, device firmware version, or device model.
8. Select device(s) and then click **Next**.
9. Select a upgrade schedule to upgrade the selected device(s).
   - Select **Upgrade Now** from the **Upgrade Schedule** drop-down list to start upgrade.
   - Select **Custom** from the **Upgrade Schedule** drop-down list and then customize a time period to upgrade the selected device(s).
10. Click **OK** to save the firmware upgrade settings.

    The upgrade task list will be open.

11. **Optional:** In the top right corner of firmware upgrade page, click **Upgrade Tasks** to view the task details and control the task status.

8.10.2 Upgrade Device Firmware via Hik-Connect

You can upgrade device firmware via Hik-Connect, which is a cloud service.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Click **Firmware Upgrade** on the left.
3. Select the **Via Hik-Connect** tab.
4. In **Upgrade By** field, select the upgrade method.
5. In **Simultaneous Upgrade** field, set the maximum number of devices for simultaneous upgrade.

   Example

   If you set the value to 5, up to 5 devices can be selected for batch upgrade.
6. Click **Next**.
7. Install the required web plug-in.

   Note

   If you select Local PC as the upgrade method, you should install the required web plug-in if the prompt pops up.

   The upgradable devices will be displayed.
8. Select device(s) and click **Next** to enter the upgrade schedule page.
9. Select a upgrade schedule to upgrade the selected device(s).
   - Select **Upgrade Now** from the **Upgrade Schedule** drop-down list to start upgrade.
   - Select **Custom** from the **Upgrade Schedule** drop-down list and then customize a time period to upgrade the selected device(s).
10. Click **OK** to save the firmware upgrade settings.

    The upgrade task list will be open.
11. **Optional:** In the top right corner of firmware upgrade page, click **Upgrade Tasks** to view the task details and control the task status.

8.11 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*** .

8.11.1 Reset Device Password

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

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 HikCentral Professional 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 creating password for the encoding device as an example.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Encoding Device** on the left.
3. In the Online Device area, view the device status (shown on Security column) and click icon ↺ in the Operation column of an active device.

   The Reset Password window pops up.
4. Click **Export File** to save the device file on your PC.
5. Send the file to the technical support.

Note

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

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 change your password regularly, especially in the high security system, changing 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.

8.11.2 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 platform 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 HikCentral Professional 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. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Encoding Device** on the left.
3. 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.
4. 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 change your password regularly, especially in the high security system, changing 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.

8.12 Manage Recording Server

You can add the Recording Server to the system for storing the videos and pictures. Currently, the Recording Server supports Hybrid Storage Area Network, Cloud Storage Server, pStor, and NVR (Network Video Recorder). You can also form an N+1 hot spare system with several Hybrid Storage Area Networks to increase the video storage reliability of system.

Note

NVR can only be used to store pictures.

8.12.1 Add pStor

You can add pStor server as Recording Server to the HikCentral Professional for storing the video files and pictures.

Before You Start

- Make sure the pStor 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 HikCentral Professional via network.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management**
2. Click **Device and Server** → **Recording Server** on the left.
3. Click **Add** to enter the Add Recording Server page.
4. Select **pStor**.
5. Enter the network parameters.

   Address

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

   Control Port

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

   Network Port

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

   Signaling Gateway Port

   The signaling gateway port No. of the pStor server. If it is not changed, use the default value.
6. Enter the user's access key and secret key of the pStor server for downloading pictures via Control Client.

Note

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

7. **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.

8. **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.
9. Enter the alias, user name, and password of the pStor 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 change your password regularly, especially in the high security system, changing 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.

10. 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.
11. **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 server displays. You can log in and configure the pStor server.

8.12.2 Add Hybrid Storage Area Network

You can add the Hybrid Storage Area Network (hereafter simplyfied as Hybrid SAN) as Recording Server to the HikCentral Professional 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 HikCentral Professional via network.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Recording Server** on the left.
3. Click **Add** to enter the Add Recording Server page.
4. Select **Hybrid Storage Area Network**.
5. Enter the network parameters.

   Address

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

   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.
6. **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 one.
   3) Set signaling gateway port No.. If the picture downloading port No. is not changed, use the default one.
   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 the technical support to get them.
7. **Optional:** Set the **Enable WAN Access** switch to ON to access the server via WAN.

   Note

   When enabled, you should set the corresponding parameters including IP address of the server, the control port No., the network port No., etc.
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 change your password regularly, especially in the high security system, changing 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 Hybrid SAN displays. You can log in and configure the Hybrid SAN.
One-Touch Configuration	If the Hybrid SAN 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.

8.12.3 Add Network Video Recorder

You can add an NVR (Network Video Recorder) as a Recording Server to HikCentral Professional for storing pictures.

Before You Start

Make sure the NVR 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 system via network.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Recording Server** on the left.
3. Click **Add** to enter the adding server page.
4. Select **Network Video Recorder** as the server type.
5. Set the required information.

Address

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

Control Port

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

Network Port

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

Picture Download Port

The picture downloading port of the NVR. If it not changed, use the default value.

Signaling Gateway Port

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

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

Note

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

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 NVR.

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 change your password regularly, especially in the high security system, changing 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 NVR.
   - Click **Add** to add the NVR and back to the server list page.
   - Click **Add and Continue** to save the settings and continue to add other NVRs.
10. **Optional:** Perform the following operations after adding the NVR.

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

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

Configure NVR
Click ⚙ , and the login interface of the NVR will be displayed. You can log in and configure the NVR.

8.12.4 Manage Cloud Storage Server

You can add a Cloud Storage Server as a Recording Server to the HikCentral Professional 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 SYS server's. Before adding the Cloud Storage Server to the platform, you should import the certificate stored in the SYS server to the Cloud Storage Server.

Before You Start

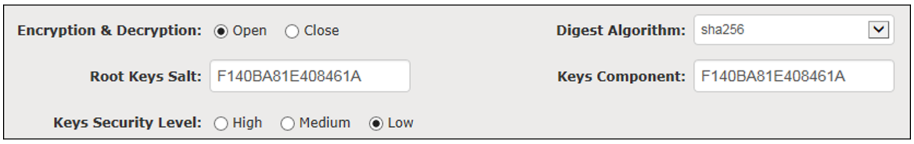
Make sure the Cloud Storage Server you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the HikCentral Professional via network.

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. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **System Configuration** .
2. Click **Security** → **Service Component Certificate** on the left side.
3. Click **Export** to export the certificate stored in the SYS server.
4. Log in the configuration page of the Cloud Storage Server via web browser.
5. Click **System** → **Configuration** → **Cloud Configuration** .
6. 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

7. Click **Set**.

What to do next

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

Add Cloud Storage Server

You can add Cloud Storage Server as Recording Server to the HikCentral Professional 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 HikCentral Professional 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.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Recourse Management** .
2. Click **Device and Server** → **Recording Server** on the left.
3. Click **Add** to enter the adding server page.
4. Select **Cloud Storage Server**.
5. Enter the network parameters.

   Address

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

   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.
6. 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 HikCentral Professional 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**).
7. **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.
8. **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.
9. 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 change your password regularly, especially in the high security system, changing 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.

10. 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.

11. 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.

8.12.5 Add pStor Cluster Service

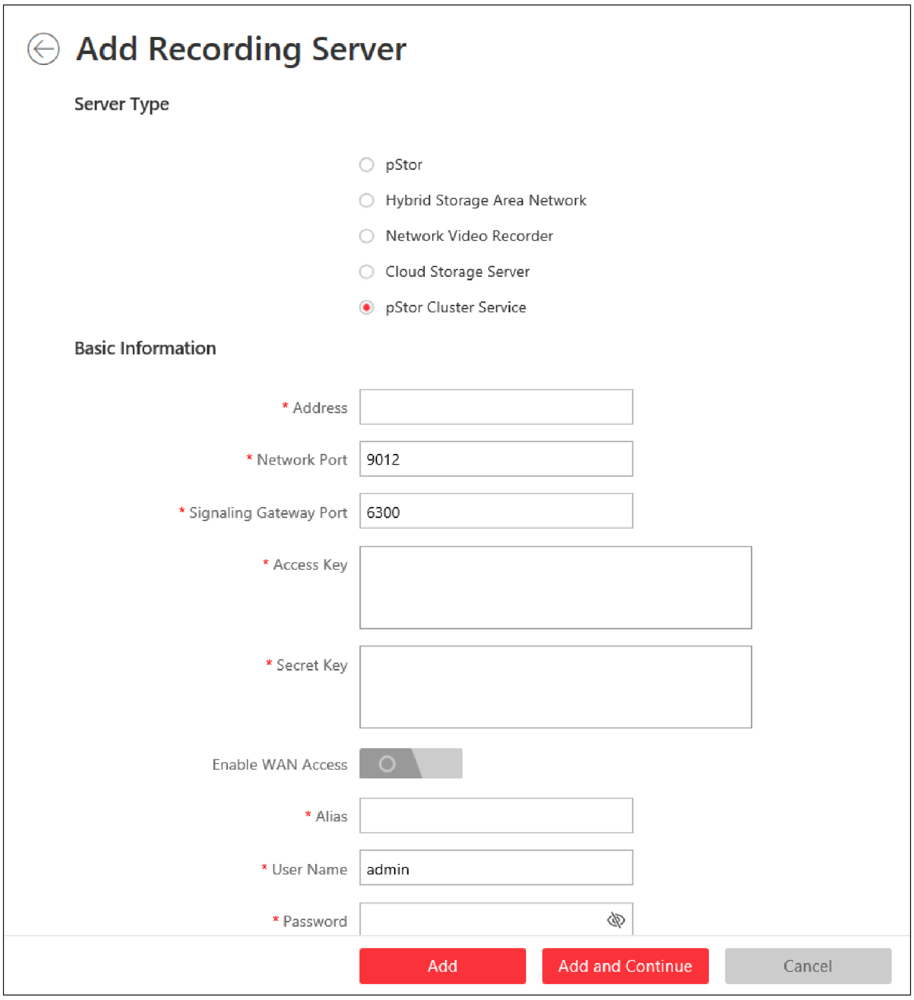
pStor Cluster Service is a service that can manage multiple pStors and the connected disks of pStors. When there are multiple pStors storing a large number of video files, you can add pStor cluster service to the HikCentral Professional for managing pStors. It is also an efficient way to add multiple pStors.

Before You Start

Make sure the pStor cluster service 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 HikCentral Professional via network.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Recourse Management** .
2. Click **Device and Server** → **Recording Server** on the left.
3. Click **Add** to enter the Add Recording Server page.
4. Select **pStor Cluster Service**.



Add Recording Server

Server Type

○ pStor

○ Hybrid Storage Area Network

○ Network Video Recorder

○ Cloud Storage Server

● pStor Cluster Service

Basic Information

* Address
* Network Port: 9012
* Signaling Gateway Port: 6300
* Access Key
* Secret Key

Enable WAN Access

* Alias
* User Name: admin
* Password

Figure 8-10 Add pStor Cluster Service

5. Enter the required network parameters.

   Address

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

   Network Port

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

   Signaling Gateway Port

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

6. Enter the user's access key and secret key of the pStor cluster service.

Note

You can download these two keys on the Web Client page (enter ***device's IP address: 9012*** in the browser) of pStor cluster service.

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 device name, user name, and password of the pStor cluster service.

⚠ **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 change your password regularly, especially in the high security system, changing 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 basic information of the server, view its connected device(s) storage information.
Delete Server	Select the server(s) from the list, and click **Delete** to remove the selected server(s).
Configure Server	Click ⚙ to enter the login interface of the pStor cluster service. You can log in and configure the pStor cluster service.

8.12.6 Set N+1 Hot Spare for Hybrid SAN

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 HikCentral Professional.

Before You Start

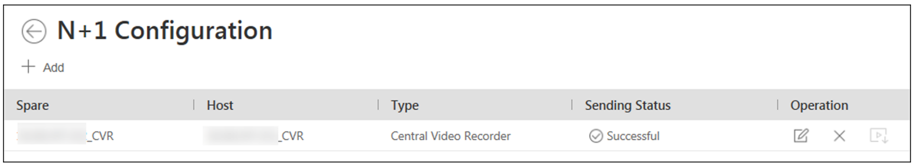
- Make sure the Hybrid Storage Area Networks you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the HikCentral Professional via network.
- At least two online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

Steps

Note

- The N+1 hot spare function is only supported by Hybrid Storage Area Networks and NVRs. For details about configuring N+1 hot spare system with NVRs, see ***Set N+1 Hot Spare for NVR*** .
- 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. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **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 8-11 N+1 Configuration Page

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

Note

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

7. **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.

8. **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.

8.13 Manage Streaming Server

You can add the Streaming Server to the HikCentral Professional 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.

8.13.1 Input Certificate Information to Streaming Server

For data security purpose, the Streaming Server's certificate should be the same with the SYS server's. Before adding the Streaming Server to the platform, you should enter the certificate information stored in the SYS server to the Streaming Server.

Steps

Note

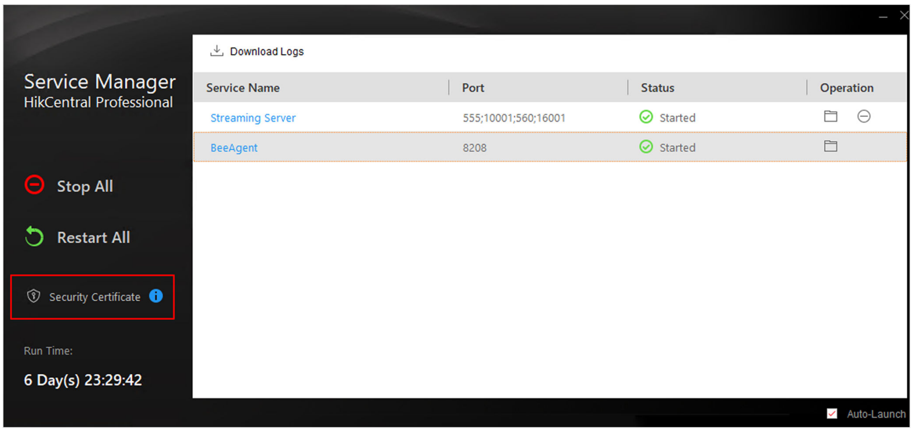
If the service component certificate is updated, you should enter the new certificate information to the Streaming Server again to update.

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

   You will enter the Home page of the Web Client.
2. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **System Configuration** .
3. Click **Security** → **Service Component Certificate** on the left.
4. Click **Generate Again** to generate the security certificate for Streaming Server verification.

   Note

   You need to enter the account password for verification to generate the security certificate.
5. On the computer which has installed with Streaming Service, open the Service Manager.
6. Click **Security Certificate**.



Run Time:
6 Day(s) 23:29:42

Service Name	Port	Status	Operation
Streaming Server	555;10001;560;16001	Started	
BeeAgent	8208	Started	

Figure 8-12 Enter Security Certificate

7. Enter the certificate information you generate in step 4.

8.13.2 Add Streaming Server

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

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Streaming Server** on the left.
3. Click **Add** to enter the Add Streaming Server page.
4. Enter the required information.

   Alias

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

   Network Location

      Select **LAN IP Address** if the Streaming Server and the SYS server are in the same LAN. Otherwise, select **WAN IP Address**.

5. **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.

   Note

   The **Enable WAN Access** switch is available when you set Network Location as **LAN IP Address**.

6. 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. You can check the related information of the added servers on the list.

8.14 Add DeepinMind Server

When you know the related parameters such as IP address and port No. of the DeepinMind server, you can add it to the platform for intelligent functions, such as facial recognition, behavior analysis, and intrusion detection.

Before You Start

Make sure the DeepinMind server you are going to use is 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 HikCentral Professional via network.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **DeepinMind Server** on the left.
3. Click **Add** to enter the Add DeepinMind Server page.
4. Set the required basic information such as device address, device port number, and WAN access.

   Device Address

   IP address of the DeepinMind server.

   Enable WAN Access

   Enable the DeepinMind server to access WAN (Wide Area Network).

   Note

   After enabling the WAN Access, you need to set the WAN IP address and port number of the DeepinMind server for WAN access.

5. Finish adding the DeepinMind server.
   - Click **Add** to finish adding the server.
   - Click **Add and Continue** to add the current server and continue to add more.
6. **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.
Delete Server	Select the server(s) from the list, and click **Delete** to delete the selected server(s).
Configure Server	Click ⚙ , and the login interface of the server displays. You can log in and configure the server.

8.15 Add Security Audit Server

You can add the Security Audit Server to the system, to receive the security audit exception logs (e.g., injection attack logs, XSS events) of encoding devices from the server, and trigger related alarms in the system.

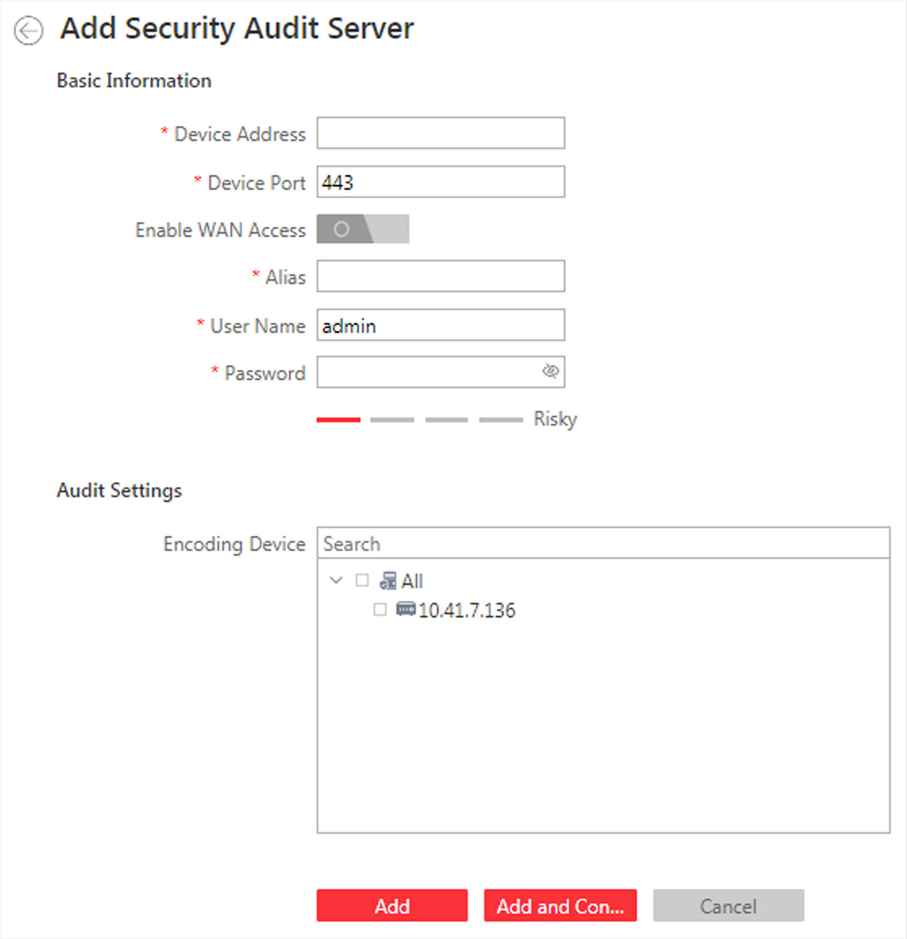
Before You Start

Make sure the Security Audit 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 HikCentral Professional via network.

Steps

- Adding security audit server is controlled by the system's license.
- Up to 8 security audit servers can be added to the system if the license permits.

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Security Audit Server** on the left.
3. Click **Add** to enter the Add Security Audit Server page.



Add Security Audit Server

Basic Information

* Device Address	
* Device Port	443
Enable WAN Access	○
* Alias	
* User Name	admin
* Password	

Audit Settings

Encoding Device

Figure 8-13 Add Security Audit Server Page

4. Set the required basic information such as device address, device port number, and WAN access.

   Device Address

   IP address of the Security Audit Server.

   Device Port

   The device port of the Security Audit Server. By default, the port is 443, which means the security audit server access to HikCentral Professional by HTTPS.

   Enable WAN Access

   Enable the Security Audit Server to access WAN.

   Note

   After enabling the WAN Access, you need to set the WAN IP address and log collection port for WAN access.

   Alias

   Enter an alias for the Security Audit Server.

User Name

Enter the user name that has the privilege to log into the Security Audit Server.

Password

Enter the password of the user that has the privilege to log into the Security Audit Server.

5. Select the encoding devices for security audit.

Note

The system can receive the security audit exception logs (e.g., injection attack logs, XSS events) of selected encoding devices from the server, and trigger related alarms in the system.

6. Finish adding the Security Audit Server.
   - Click **Add** to finish adding the server.
   - Click **Add and Continue** to add the server and continue to add more.

Chapter 9 Manage Area

HikCentral Professional 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.

9.1 Add Area

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

9.1.1 Add Area for Current Site

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

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Click **Area** on the left.
3. **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.

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

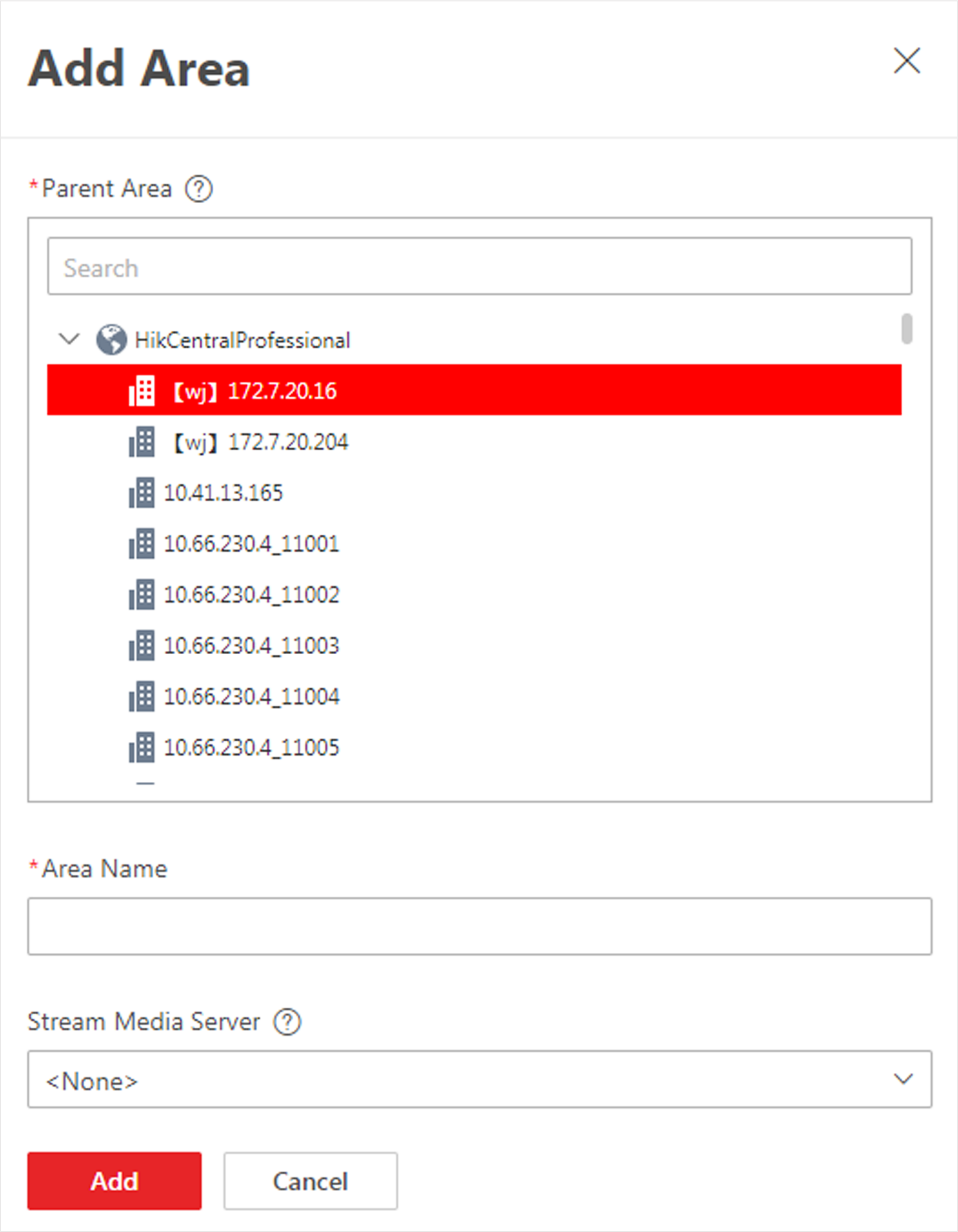


Figure 9-1 Add Area for Current Site

5. Select the parent area to add a sub area.
6. Create a name for the area.

7. **Optional:** Select a Streaming Server for the area to get the video stream of the cameras belonging to this area via the server.
8. Click **Add**.
9. **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 a selected area, or press **Ctrl** on your keyboard and select multiple areas and then click 🗑 to delete areas in a batch.

Note

After deleting the area, the resources in the area (cameras, doors, radars, alarm inputs, and alarm outputs) 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 of the area list panel to search the area.

Move Area
Drag the added area to other parent area as the child area.

9.1.2 Add Area for Remote Site

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

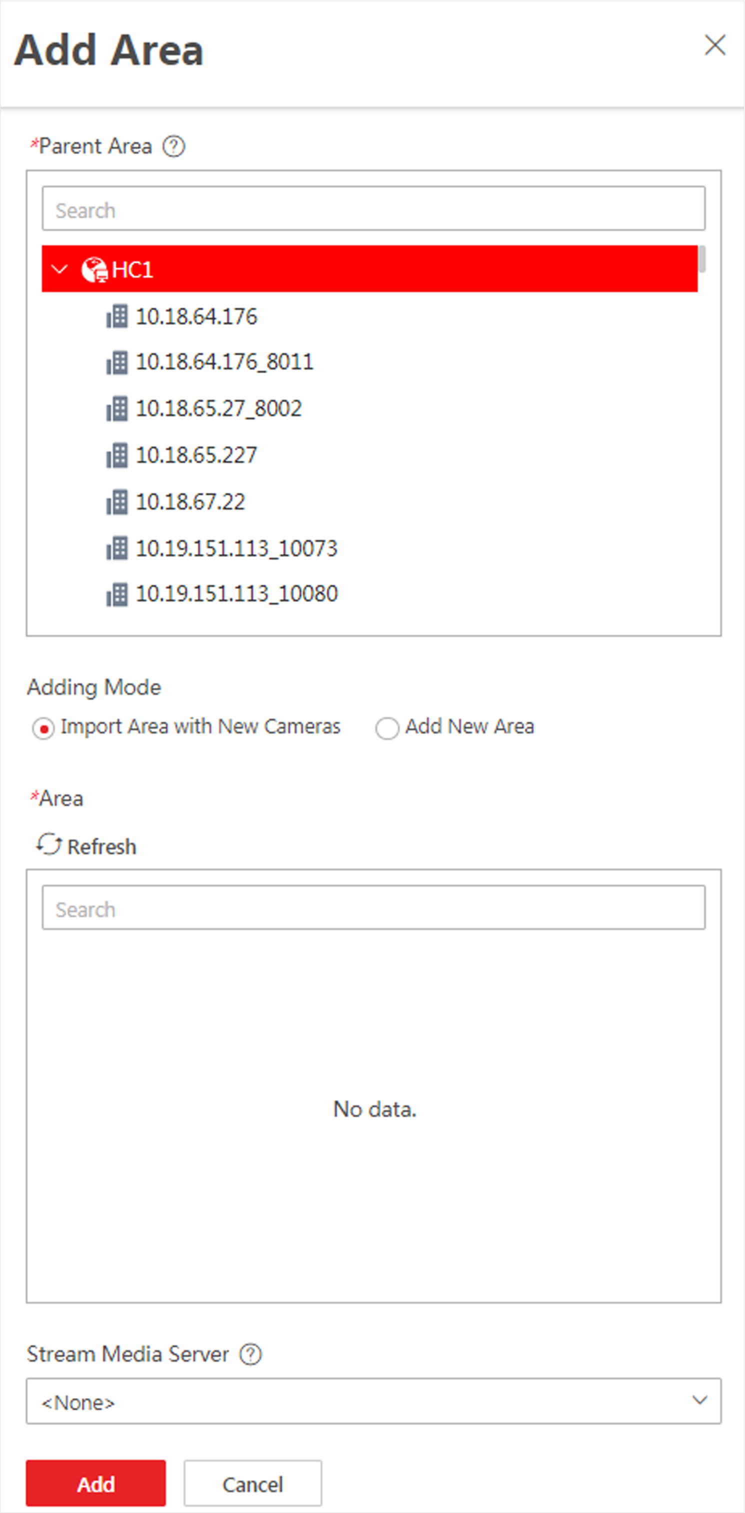
Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Click **Area** on the left.
3. 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.

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



Add Area

*Parent Area

- HC1
  - 10.18.64.176
  - 10.18.64.176_8011
  - 10.18.65.27_8002
  - 10.18.65.227
  - 10.18.67.22
  - 10.19.151.113_10073
  - 10.19.151.113_10080

Adding Mode

● Import Area with New Cameras ○ Add New Area

*Area

No data.

Stream Media Server

<None>

Figure 9-2 Add Area for Remote Site

5. Select the parent area to add a sub area.
6. 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.

7. **Optional:** Select a Streaming Server for the area to get the video stream of the cameras belonging to this area via the server.
8. Click **Add**.
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, or press **Ctrl** on your keyboard and select multiple areas and then click 🗑 to delete areas in a batch.

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 of the area list panel to search the area.

Move Area
Drag the added area to other parent area as the child area.

9.2 Add Element to Area

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

9.2.1 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 cameras need to be added to the HikCentral Professional for area management. Refer to ***Manage Encoding Device*** for details.

Steps

Note

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

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Click **Area** on the left.
3. 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.

4. Select the **Camera** tab.
5. Click + on the element page to enter the Add Camera page.
6. Select the device type.
7. Select the cameras to add.
8. **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.

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 ↑↓ to get the cameras' names from the device in a batch.

Note

You can only synchronize the camera name of online HIKVISION device.

Apply Camera Name

Select the cameras and click to apply the cameras' names to the device in a batch.

Get Recording Schedule

Select the cameras and click to get the recording schedules from the devices 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**.

Add Camera to Map

Click to enter Map Settings page and drag the camera to the map. See ***Add Hot Spot on Map*** for details.

Display Cameras of Child Areas

Check **Include Sub-area** to display the cameras of child areas.

9.2.2 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 HikCentral Professional for area management. Refer to ***Manage Encoding Device*** for detailed configuration about adding devices.

Steps

Note

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

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Click **Area** on the left.
3. 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.

4. Select an area for adding cameras to in the area list panel.
5. Click + on the Camera page to enter the Add Camera page.

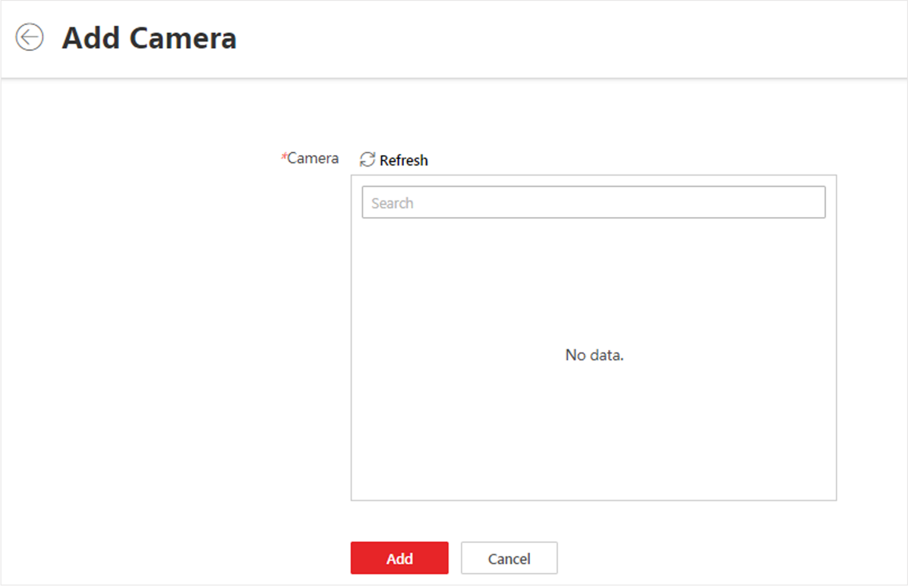


Figure 9-3 Add Camera to Area for Remote Site

6. Select the cameras to add.

Note

Up to 64 cameras can be added to one area.

7. Click **Add**.
8. **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.

Set Camera ID
Click to enter Camera ID page. Then edit the default identifier number in the **ID** column of each camera and click **Save**.

Note

The camera ID is unique and used to display certain camera's live view on smart wall via the network keyboard.

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.

9.2.3 Add Door to Area for Current Site

You can add doors to areas for the current site for management.

Before You Start

The access control devices need to be added to the HikCentral Professional for area management. Refer to ***Manage Access Control Device*** for details.

Steps

Note

One door can only belong to one area. You cannot add one door to multiple areas.

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Click **Area** on the left.
3. Select an area for adding doors to in the area list panel.

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.

4. Select the **Door** tab.

5. Click + on the element page to enter the Add Door page.
6. Select the device type.
7. Select the door(s) to add.
8. Click **Add**.
9. **Optional:** After adding the doors, you can do one or more of the followings.

Synchronize Door Name

Select the doors and click ↑↓ to synchronize the doors' names from the device in a batch.

Note

You can only synchronize the door name of online HIKVISION device.

Apply Door Name

Select the doors and click to apply the doors' names to the device in a batch.

Move to Other Area

Select the doors and click . Then select the target area to move the selected doors to and click **Move**.

Add Door to Map

Click to enter Map Settings page and drag the door to the map. See ***Add Hot Spot on Map*** for details.

Display Doors of Child Areas

Check **Include Sub-area** to display the doors in child areas.

9.2.4 Add Radar to Area for Current Site

You can add radars to different areas of the current site according to their locations, so that you will be informed when an alarm/event is triggered if you have configured an alarm/event.

Before You Start

The devices need to be added to the HikCentral Professional for area management. Refer to ***Manage Resource*** for details.

Steps

Note

You cannot add a radar to multiple areas.

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Click **Area** on the left.
3. In the area list panel, select the added current site in the drop-down site list to show its areas.

Note

The icon 🌐 indicates that the site is current site.

4. Select an area for adding radars to.
5. Click **Radar** tab.
6. Click + to enter the Add Radar page.
7. Select a radar in the **Radar** field.
8. Click **Add**.
9. **Optional:** After adding the radars, you can do one or more of the followings

Arm/Disarm Radar
Select the radar(s) and click ⌂ / ⌂ to arm/disarm the selected radar(s).

> **Note**
>
> An event will be triggered if anybody or an object enters an armed radar's detection area.

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

Add Radar to Map
Click ⚙ to enter Map Settings page and drag the radar to the map. See ***Add Hot Spot on Map*** for details.

Display Radars of Child Areas
Check **Include Sub-area** to display the radars of child areas.

9.2.5 Add Alarm Input to Area

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

Before You Start

The devices need to be added to the HikCentral Professional for area management. Refer to ***Manage Resource*** for details.

Steps

> **Note**
>
> One alarm input can only belong to one area. You cannot add an alarm input to multiple areas.

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Click **Area** on the left.
3. 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.

4. Select the **Alarm Input** tab.
5. Click + to enter the Add Alarm Input page.
6. Select the device type.
7. 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.

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 . Then select the target area to move the selected alarm inputs to and click **Move**.

Add Alarm Input to Map
Click to enter Map Settings page and drag the alarm input to the map. See ***Add Hot Spot on Map*** for details.

Display Alarm Inputs of Child Areas
Check **Include Sub-area** to display the alarm inputs of child areas.

View Alarm Input Status
In the **Status** column, the alarm input's online status, arming status, bypass status, alarm status, fault status, and detector connection status are displayed.

- **Online Status**: ✓ indicates alarm input online; ✕ indicates alarm input offline.
- **Arming Status**: indicates alarm input armed; indicates alarm input disarmed.
- **Bypass Status**: indicates alarm input bypassed; indicates bypass restored.
- **Fault Status**: ⚠ indicates alarm input exception.
- **Alarm Status**: indicates that the alarm input is alarming.
- **Detector Connection Status**: 🔗 indicates alarm input not enrolled or offline; indicates detector online.
- **Battery Status**: indicates normal alarm input's battery status; indicates abnormal alarm input's battery status.

Bypass/ Restore Bypass Alarm Input
When an exception of alarm input occurs, and other alarm inputs can work normally, click to bypass the abnormal alarm input, otherwise, you cannot arm the security control partition which the alarm input belongs to. When a bypassed alarm input works normally, click to restore bypass.

9.2.6 Add Alarm Output to Area

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

The devices need to be added to the HikCentral Professional for area management. Refer to ***Manage Resource*** for details.

Steps

Note

One alarm output can only belong to one area. You cannot add an alarm output to multiple areas.

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Click **Area** on the left.
3. 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.

4. Select the **Alarm Output** tab.
5. Click + to enter the Add Alarm Outputs page.
6. Select the device type.
7. Select the alarm outputs to add.
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 ↗ . Then select the target area to move the selected alarm outputs to and click **Move**.
Add Alarm Output to Map	Click 📍 to enter Map Settings page and drag the alarm output to the map. See ***Add Hot Spot on Map*** for details.
Display Alarm Outputs of Child Areas	Check **Include Sub-area** to display the alarm outputs of child areas.

9.3 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, and hardware settings for doors, and so on.

9.3.1 Edit Camera for Current Site

You can edit basic information, recording settings, and picture storage settings of the camera for current site.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Click **Area** on the left.
3. 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.

4. Select an area.
5. Select the **Camera** tab to show the added cameras.
6. Click a camera's name in the **Name** column to enter the camera editing page.
7. Edit the camera's basic information, including camera name and protocol type.

Note

If you changes the camera's name, you can click 🗒 in the added cameras list page to apply the new name to the device.

8. **Optional:** Click **Live View** to view the live view of the camera and hover over the window and click ▶ in the lower-right corner to switch to playback.
9. Edit the recording settings of the camera. See ***Configure Storage and Recording*** for details.

Note

- If no recording settings have been configured for the camera, you can click **Configuration** to set the parameters.
- You can also select multiple cameras and click **Get Device's Recording Settings** in the added cameras list page to get recording schedules of the devices in a batch.

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.
- For cameras added by ISUP protocol, this function is not available. You should click **Configuration** to edit the picture storage configurations.

11. **Optional:** Click **Configuration on Device** in the top right corner of camera editing panel or click ⚙ in the **Operation** column of the added camera list page 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.

12. **Optional:** In the top right corner of camera editing panel, click **Copy to** to select configuration item and copy the settings of this camera to other cameras.
13. Click **Save**.

9.3.2 Edit Door for Current Site

You can edit basic information, related cameras, picture storage settings, card reader settings, and face recognition terminal settings of the door on current site.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Click **Area** on the left.
3. In the area list panel, select the added current site from the drop-down site list to show its areas and select one area.
4. Select the **Door** tab to show the added doors in this area.
5. Click a door's name in the **Name** column to enter the Edit Door page.
6. Edit the door's basic information.

   Name

   Edit the name for the door.

   Note

   If you changes the name, you can click ☰ in the door list page to apply the new name to the device.

   Door Contact

   The door contact's connection mode.

   Exit Button Type

   The exit button connection mode.

   Open Duration

The time interval between the door is unlocked and locked again.

Extended Open Duration

The time interval between the door is unlocked and locked again for the person whose extended access function enabled.

Door Open Timeout Alarm

After enabled, if the door 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 a 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.

7. Relate cameras to the door, 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 door.

8. **Optional:** For video access control terminal, set the **Picture Storage** switch to ON and select the storage location from the drop-down list for storing the pictures (captured by the device's camera) to the specified location. Refer to ***Configure Storage for Uploaded Pictures*** for details.
9. In the Card Reader panel, set the **Card Reader 1** or **Card Reader 2** switch to ON and set the card reader related parameters.

Min. Card Swipe Interval

After enabled, you cannot swipe the same card again within the minimum card swiping interval.

Reset Entry on Keypad after

Set the maximum time interval of pressing two keys on the keypad. If timed out, the first entry will be reset.

Failed Card Attempts Alarm

After enabled, if the door 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 door 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.

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.

Note

The parameters displayed vary according to the model of the access control device. For details about the parameters, refer to the user manual of the device.

10. **Optional:** For the turnstile, set **Face Recognition Terminal** switch to on and add the face recognition terminals to link the selected turnstile.
    1)Click **Add** to enter Add Face Recognition Terminal page.
    2)Select **IP Address**, **Online Devices**, or **Device ID** as the adding mode, and set the required parameters, which may vary according to different terminals.
    3)Click **Add** to link the terminal to turnstile.
11. Click **Save**.
12. **Optional:** If needed, enter the Edit Door page again and click **Copy to** to apply the current settings of the door to other door(s).

9.3.3 Edit Radar for Current Site

After adding a radar to an area of the current site, you can edit the radar name, view the drawn zones or trigger lines, and view the related calibrated cameras.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Click **Area** on the left.
3. 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.

4. Select an area.
5. Select the **Radar** tab to show the added radars.
6. Click a radar's name in the **Name** column to enter the Edit Radar page.
7. Edit the radar's name.
8. **Optional:** In the **Zone** field, view the drawn zones of the radar.

Note

If there is no zone drawn for the radar, you should go to Map Settings module to draw. Refer to ***Draw Zone or Trigger Line for Radar*** for details.

9. **Optional:** In Related Calibrated Camera field, view the calibrated cameras related to the radar.

Note

If there is no calibrated camera related to the radar, you should go to Map Settings module to configure. Refer to ***Relate Calibrated Camera to Radar*** for details.

10. Click **Save** to save the settings for the radar.

9.3.4 Edit Alarm Input for Current Site

You can edit the basic information of alarm input and relate detector to the security control panel's alarm input for current site.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Click **Area** on the left.
3. 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.

4. Select the **Alarm Input** tab to show the added alarm inputs.
5. Click an alarm input name in the **Name** column to enter the Edit Alarm Input page.
6. Edit the alarm input name.
7. **Optional:** For the alarm input of security control panel, set the **Related Detector** switch to ON to configure related detector for the alarm input.
   1) Click **Add** to add a detector.
   2) Enter the detector name.
   3) Click ✓ to save the detector type.

Note

- Only the alarm input of a security control panel supports this function. Make sure you have added a security control device to the system, and have added its zone to area as an alarm input. See ***Add Alarm Input to Area*** for details.
- On Map Settings page, the detectors related to the alarm input of a security control panel will be displayed in the resource list of alarm input on the right panel. When selecting the alarm

input and dragging it to the map, the related detectors will also be added to the map, and the relations among them will be marked with lines. If you only drag the alarm input to the map without selecting it, the related detectors will not be added to the map.
- You cannot edit the detector type here. If you want to edit it, go to the Remote Configuration page of security control panel, and click **Input Settings → Zone** .

8. Click **Save**.

9.3.5 Edit Alarm Output for Current Site

You can edit the alarm output name for current site.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules → General → Resource Management** .
2. Click **Area** on the left.
3. 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.

4. Select the **Alarm Output** tab to show the added alarm outputs.
5. Click an alarm input name in the **Name** column.
6. Edit the alarm output name in the pop-up window.
7. Click **Save**.

9.3.6 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.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules → General → Resource Management** .
2. Click **Area** on the left.
3. 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.

4. Select an area to show its cameras.
5. Click a camera's name in the **Name** column to enter the camera editing page.
6. Edit the camera's basic information, including camera name and protocol type.

Note

If you changes the camera's name, you can click ☰ in the added cameras list page to apply the new name to the device.

7. **Optional:** Click **Live View** to view the live view of the camera and hover over the window and click ▶ in the lower-right corner to switch to playback.
8. Edit the recording settings of the camera.

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***).

9. **Optional:** Click **Configuration on Device** in the top right corner of camera editing panel or click ⚙ in the **Operation** column of the added camera list page 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.

10. **Optional:** Click **Copy to** to copy the current camera's specified configuration parameters to other cameras of the Remote Site.
11. Click **Save**.

9.4 Remove Element from Area

You can remove the added cameras, alarm inputs, alarm outputs, and doors from the area.

9.4.1 Remove Element from Area for Current Site

You can remove the added cameras, doors, radars, alarm inputs, and alarm outputs from the area for current site.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Click **Area** on the left.
3. 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.

4. Select the **Camera**, **Door**, **Radar**, **Alarm Input**, or **Alarm Output** tab to show the added elements.
5. Select the elements.
6. Click 🗑 to remove the cameras from the area for current site.

9.4.2 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.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Click **Area** on the left.
3. 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.

4. Select an area to show its added cameras.
5. Select the cameras.
6. Click 🗑 to remove the cameras from the area for remote site.
7. **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.

Chapter 10 Manage Person

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), etc. After adding the persons, you can edit and delete the person information if needed.

10.1 Add Person Group

When there are a large number of persons managed in the system, you can put the persons in different person groups. For example, you can group employees of a company to different departments.

Steps

Note

The person groups (including group quantity) being viewed by different users are different. You can go to **General → Security → Roles** to edit the role assigned to the user. Click a role, select **Permission Settings → Resource Access → Person Group** , and check the person group(s) that will be viewed by the selected role.

1. In the top left corner of Home page, select ≡ → **All Modules → General → Person** to enter the person page.
2. Click + to enter the Add Person Group page.
3. Set person group information, including parent group, group name, etc.
4. Confirm to add the person group.
   - Click **Add** to finish adding the current person group and go back to person group page.
   - Click **Add and Add Person** to finish adding the current person group and continue to add other person groups.

10.2 Add Person

10.2.1 Add a Person

You can add a person to the system by entering her/his information and set more configurations for the person.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules → General → Person** .
2. Click **Add** to enter the adding person page.
3. Set basic information for the person.

   ID

The default ID is generated by the system. You can edit it if needed.

Note

If the person is a police officer or a security guard with body cameras, make sure the person ID is same as the police ID configured on the body camera.

Person Group

Select a person group for the person.

Note

See ***Add Person Group*** for details about adding a person group.

Person Picture

Hover the cursor on the person picture field, and you can select from three modes to add a picture:

From Device

Select **Access Control Device**, **Video Intercom Device**, or **Enrollment Station** to collect the face picture. This mode is suitable for non-face-to-face scenario when the person and the system administrator are in different locations.

Note

- For access control devices, only face recognition terminals (including DS-K5671, DS-K1T671, DS-K1T331, DS-K1T341, DS-K1T672, DS-K1T642, etc.) are supported.
- For video intercom devices, door stations and outer door stations are supported.
- For enrollment stations, you need to set related parameters, including device address, port, user name, password, face anti-spoofing, and security level.

Take a Picture

Click **Take a Picture** and select one of the PC's webcam(s) to take a picture.

Upload Picture

Click **Upload Picture** to select a picture in 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.
- You can drag the picture to change its position or zoom in/out before cutting it.
- You can set **Verify Profile Quality** switch to on and select a device to check profile quality. Click **Save** to start checking. You will be informed if the picture is not qualified, while the cut picture will be put in the profile position if it is qualified.

Skin-surface Temperature

Enter the person's skin-surface temperature and select the corresponding temperature status.

Note

For example, if a person's skin-surface temperature is 37℃, then you can select her/his temperature status as normal.

Effective Period

Set the effective period for the person in access control application. For example, if the person is a visitor, his/her effective period may be short and temporary.

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.

Extended Access

When the person accesses the 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

The extended access and super user functions cannot be enabled concurrently.

PIN Code

The PIN code must be used after card or fingerprint when accessing. It cannot be used independently.

Note

It should contain 1 to 8 digits.

4. **Optional:** Set access control permission for the person to define which access point(s) the person can access in the authorized period.
   1) Click **Relate**.
   2) Select one or more access levels for the person.
   3) Click **Add** to add the person to the selected access level(s).

Note

You can click 🗎 to view its access point(s) and access schedule.

5. **Optional:** View shift schedule of the person in the table.

Note

You can click ‹ or › to switch the time (month).

6. **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*** .

7. **Optional:** Add the person to the existing dock station group(s) and set the login password which is used for the dock station(s) in the group to log into the body cameras.

Note

By default, the login password is 123456.

The videos and pictures stored on the person's body camera can be copied to the person's linked dock station(s).

8. Set resident information to link the person with the indoor station and room number.

Note

Make sure the room number is consistent with the actual location information of the indoor station.

9. 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.
10. **Optional:** After adding the person, you can do one or more of the following.

Edit Person

Click the person name to edit the person details.

Delete Person

Check the person(s) and click **Delete** to delete the selected person(s).

Delete All Persons

Click ⌄ beside **Delete** and click **Delete All** to delete all the persons in the person list.

Export Added Person Information

Click **Export** 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 which is required when decompressing the downloaded ZIP file before exporting.

Move Person

You can move the person(s) to other person group. After that, the access level and shift schedule of the selected person(s) will be changed.

Select one or more persons, click **Move**, select the target person group to move the persons to, and click **Move**.

Clear Access Levels

Select one or more persons, click **Clear Access Levels** to clear the access levels of the selected persons.

Note

Clearing the persons' access levels cannot be restored.

Check Person Authorization

Select one or more persons, click **Check Person Authorization** to enter Check Person Authorization page, and view the credential details of the selected persons.

10.2.2 Batch Add Persons by Importing Person Information File

You can add the information of multiple persons to the platform by importing an excel file with person information. Also, by entering the name of a person group/access group/face comparison group/dock station group of multiple persons in the excel file, you can add them to a group in a batch.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Person** .
2. Click **Import** → **Import an Excel File** .
3. In the pop-up window, click **Download Template** to save the template file in your PC.
4. In the downloaded template, enter the person information following the rules in the template.
5. Click ··· , and select the excel file with person information from local PC.
6. **Optional:** Check **Replace Repeated Person** to replace the person's information if the imported ID is the same with an existing person in the list.
7. **Optional:** Check **Auto Replace Card No.** to replace the card No. automatically if it already exists in the platform.
8. Click **Import** to start importing.

   Note

   - The importing process cannot stop once started.
   - You can batch issue cards to persons by importing the excel file with card No. entered.

   The importing progress shows and you can check the results.

   Note

   You can export the person information which failed to be imported, and try again after editing.
9. **Optional:** Perform the following operation(s).

   Edit Person

   Click the person name to edit the person details.

   Delete Person

   Select one or more persons 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.

Filter Person

Click ▽ to filter persons by setting conditions, after which click **Export All** to export information of the filtered persons.

Move Person

You can move the person(s) to other person group. After that, the access level and shift schedule of the selected person(s) will be changed.

Select one or more persons, click **Move**, select the target person group to move the persons to, and click **Move**.

Clear Access Levels

Select one or more persons, click **Clear Access Levels** to clear the access levels of the selected persons.

Note

Clearing the persons' access levels cannot be restored.

Check Person Authorization

Select one or more persons, click **Check Person Authorization** to enter Check Person Authorization page, and view the credential details of the selected persons.

10.2.3 Import Domain Persons

You can import the users in the AD domain in a batch to the platform 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. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Person** .
2. Click **Import** → **Import Domain Persons** to enter the Import Domain Persons page.
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. **Optional:** When selecting **Person** as the importing mode, select a person group to import the persons to.
5. Set the effective period for the person as needed.
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 platform, you can click the person name to view and edit her/his details.

Note

- If the profile/email in the domain is linked to the profile/email in the platform, the persons' profile/email will be imported to the platform from the domain as well. You can view the profile/email in the person details page but you cannot edit it.
- If the profile/email in the domain is NOT linked to the profile/email in the platform, you can take a picture or upload a picture as the person's profile and enter the email address.
- For linking the person information in the domain to the person information in the platform, refer to ***Set Active Directory*** .

8. **Optional:** If the person information in domain is changed, click **Synchronize Domain Persons** to get the latest information of the persons imported to the platform.

Note

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).

10.2.4 Batch Add Profiles

You can add multiple person pictures to the system. If you access the system via the Web Client running on the SYS server, you need to specify a path where the profiles are stored. If you access the system via the Web Client running on other computers, you can import a ZIP file containing person pictures. In this way, you can also add these person to specific face comparison group(s).

Steps

Note

If the ID in the profile name is duplicate with the person's in the system, it will edit the existing person's ID. If the ID in the profile name doesn't exist in the system, or the profile name only contains person name, the system will create a new person with the profile, person name, or ID.

1. Name the profile photos according to the person name or person ID.

Note

- The naming rule of photo is: Person Name, Person ID, or Person Name ID. The person name should contain first name and then last name, separated with a plus sign.
- Recommendation for each photo: Dimensions: 295×412. Size: 60 KB to 100 KB.
- The photos should be in JPG, JPEG, or PNG format.

2. **Optional:** If you access the system via the Web Client running on the SYS server, packet these photos in one folder and compress it in ZIP format.

   Note

   The ZIP file should be smaller than 4 GB, or the uploading will fail.

3. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Person** .
4. Click **Import** → **Import by Importing Profiles** .
5. Select the profiles.
   - If you access the system via the Web Client running on the SYS server, select a path where the profiles are stored.
   - If you access the system via the Web Client running on other computers, select the ZIP file containing the person photos.

     Note

     You can hold CTRL key and select multiple ZIP files. Each file should be no larger than 4 GB.
6. **Optional:** Select a person group from the Person Group drop-down list if you are importing profile pictures for newly added persons.
7. **Optional:** Perform the following operations if required.

   Verify Face Quality by Device
   Set the **Verify Face Quality by Device** switch to on and then select an access control device for verifying the face quality.

   Note

   You should have added the access control devices which support face recognition. For details about adding access control device, see ***Manage Access Control Device*** for details.

   Add to Face Comparison Group
   Set the **Add to Face Comparison Group** switch to on and select the face comparison group(s) to add the persons to these group after importing.
8. Click **Import** to start importing.

   The importing progress shows and you can check the results.
9. **Optional:** After importing profiles, click **Export Failure Details** to export the Excel file to the local PC and view the failure details including department, person name and person ID.

10.2.5 Import Persons from Device

If the added device such as an access control device has been configured with person information, you can get person information from the device and import it to the system for further operations. The person information that can be imported to the system includes person name, profile, credentials (PIN codes, cards, and fingerprints), effective period, person roles (super user and the disabled), etc.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Person** .
2. Click **Import** → **Import from Device** .
3. Set the device type as access control device.
4. Check one or more devices from the device list.

   Note

   You can enter a key word (supports fuzzy search) in the search box to search the target device(s) quickly.

5. Select a person group to import the persons to.
6. **Optional:** Check **Replace Profile** to replace the existed person profile with the new one.

   This function is applicable for persons who already have their profiles in the platform and now have new profiles.

7. Click **Import** to start importing.

   Note

   When importing, the platform will compare persons on the device with persons in the system based on the person name. If the person name exists on the device but do not exists in the platform, the system will create a new person. If the person name exists both on the device and in the system, the person information in the platform will be replaced by the data on the device.

10.2.6 Import Persons from Enrollment Station

You can apply the required person information to the enrollment station via a template or platform person list, and then enroll the persons' credentials on the scene. After that, the person and credential information needs to be imported from enrollment station to the HikCentral Professional. This mode is mainly available for the scenes without network. You can specify the IP address, port number, user name and password to access the enrollment station and complete importing persons through two stages above.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Person** .
2. Click **Import** → **Import from Device** .
3. Select **Enrollment Station** from the device list.
4. Set device address, port No., user name and password for accessing the enrollment station.
5. Set importing stage and method.

   Apply Person Information

      These persons whose credentials need to be enrolled will be applied to the enrollment station.

      Import from Template

If the persons are not added to the platform, download the template from the enrollment station and then edit the template and apply it to the enrollment station for enrolling the persons' credentials.

Import from Person List

If the persons have been added to the platform, select the person group to apply the persons to the enrollment station for enrolling the persons' credentials.

Copy Back Person and Credential Information

When the persons' credentials are enrolled, select the person group to import the person and credential information to.

6. Click **Import** to start importing.

10.3 Person Self-Registration

If there are persons to be added to the system, you can generate a QR code for them to scan. After scanning the generated QR code by smart phone, the persons can enter their personal information (including profile) on Self-Registration page. If you have enabled Review Self-Registered Persons function, you need to review and approve their person information, otherwise they cannot be added to the system.

This function is applicable to circumstances like a company where there are a large amount of new employees to be added to the system. For example, you print the generated QR code for the new employees to scan. After scanning the QR code by smart phone, new employees will enter Self-Registration page to import their personal information.

Note

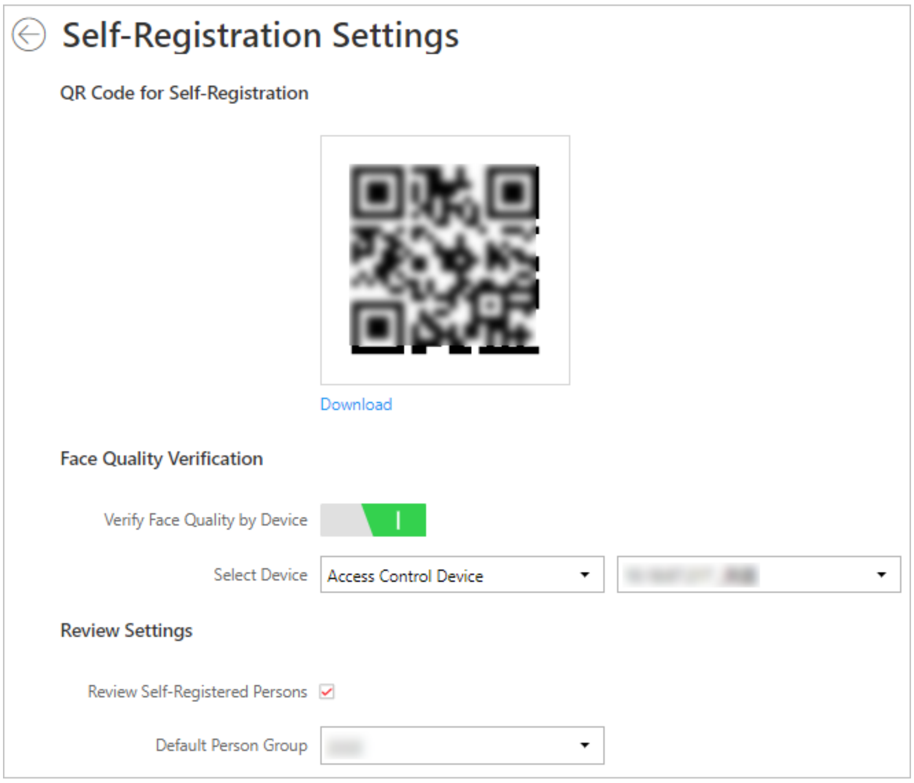
You should set self-registration parameters beforehand. See ***Set Self-Registration Parameters*** for details.

10.3.1 Set Self-Registration Parameters

Before starting self-registration, you need to set self-registration parameters. A QR code is necessary for the persons to register their information by themselves. Besides, you can configure face quality verification and person information review.

In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Person** → **Self-Registration** → **Self-Registration Settings** to enter the Self-Registration Settings page.

1.



Self-Registration Settings

QR Code for Self-Registration

Download

Face Quality Verification

Verify Face Quality by Device: on

Select Device: Access Control Device ▾ [redacted] ▾

Review Settings

Review Self-Registered Persons ☑

Default Person Group: [redacted] ▾

Figure 10-1 Self-Registration Settings

QR Code for Self-Registration

The system will generate a QR code for you to download. After downloading the QR code, you can print it or send it to persons who are going to register.

Face Quality Verification

After the person uploads profile by a cellphone, the selected device will automatically start checking the profile's quality. If the profile is not qualified, the person will be notified. Only when the uploaded profile is qualified can the person register successfully. Otherwise, the person's information cannot be uploaded to the system.

Note

To use this function properly, make sure you have added an access control device or video intercom device to the system beforehand.

Review Self-Registered Persons

Set a default person group. After registering person information successfully, the person will be added to this group.

If you enable **Review Self-Registered Persons**, after registration, you need to review the person information on the Persons to be Reviewed page. After verification, the person will be added to the selected person group. See ***Review Self-Registered Person Information*** for details about how to review.

10.3.2 Scan QR Code for Self-Registration

If a person needs to register by self-service, the person should use a smart phone to scan the self-registration QR code to enter the Self-Registration page and enter person information. After registration, the person details will be uploaded to the platform for review.

Before You Start

The administrator can print the QR code or send the QR code to persons to scan. See ***Set Self-Registration Parameters*** about how to generate a self-registration QR code.

Steps

1. Use your smart phone to scan the self-registration QR code to enter the Self-Registration page.
2. Tap the profile frame to upload a face picture.

   Note

   - You can select a picture from your phone album, or take a photo by phone.
   - After uploading a profile, profile quality checking will automatically start. If the profile is not qualified, you will be notified. Only when the uploaded profile is qualified can you register successfully. Otherwise, your personal information cannot be uploaded to the platform. See ***Set Self-Registration Parameters*** for details about setting Face Quality Verification function.

3. Set your personal information, including name, ID, gender, email, phone number, etc.
4. Enter the verification code.
5. Tap **Save**.
   - If **Review Self-Registered Persons** function is enabled, wait for the review. If you are approved, you will be added to the platform. See ***Review Self-Registered Person Information*** about how to review.
   - If **Review Self-Registered Persons** function is disabled, the person information will be uploaded to the platform.

10.3.3 Review Self-Registered Person Information

If you have enabled **Review Self-Registered Persons** function when you set self-registration parameters, after the persons registered, their person information will be displayed on the Persons to be Reviewed page, and their status will be displayed as **To be Reviewed**. You should review their personal information to approve. After approving, they will be added to the target person group.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Person** → **Self-Registration** → **Persons to be Reviewed** .
2. **Optional:** Click ▽ to filter registered persons by name, ID, gender, or status to quickly find your wanted persons.
3. Review the displayed person information and verify them.

Operations	Description
Approve Self-Registered Person Information	If the self-registered person information is correct, approve the information to add the registered persons into the platform. • Select a registered person, and click 👤 to approve the person. • Check multiple registered persons, and click **Approve** to approve them all.
Reject Self-Registered Person Information	If there is something wrong or missing with the self-registered person information, reject the person and tell the person to register again with right information. • Select a registered person, and click 👤 to reject the person. • Check multiple registered persons, and click **Reject** to reject them in a batch.
Delete Self-Registered Person Information	• Select a registered person, and click 🗑 to delete the person from the Persons to be Reviewed list. • Check multiple registered persons, and click **Delete** to delete them all from the Persons to be Reviewed list.

Note

Approved persons will be added to the target person group; rejected persons will not be added to the target person group, but they will stay in the Persons to be Reviewed list.

10.4 Batch Issue Cards to Persons

The platform provides a convenient way to issue 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 temporary cards.

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Person** .
2. Select the persons to issue the card to.
3. Click **Card** → **Batch Issue Cards to Persons** .
4. In the pop-up window, set the related parameters.

Note

For details about setting the card issuing mode and parameters, refer to ***Set Card Issuing Parameters*** .

5. Issue one card to one person according to the issuing mode you select.
   - If you select the issuing mode as **Card Enrollment Station**, place the card on the card enrollment station. The card number will be read automatically and the card will be issued to the first person in the list.
   - If you select the issuing mode as **Card Reader**, swipe the card on the card reader. The card number will be read automatically and the card will be issued to the first person in the list.
   - If you select the issuing mode as **Enrollment Station**, place the card on the enrollment station. The card number will be read automatically and the card will be issued to the first person in the list.
   - If you select the issuing mode as **Enter Manually**, enter the card number manually in the Card Number field. Press **Enter** key on the keyboard to issue the card to the person.

   Note

   You can check **Auto Increment Card Number** and enter a start card number to issue cards with incremental numbers to the selected persons in the list.
6. Click **Start** to start issuing cards.
7. Repeat step 5 to issue the cards to the persons in the list in sequence.

Note

You cannot change the card issuing mode once you issue one card to one person.

8. Click **Save**.

10.5 Set Card Issuing Parameters

HikCentral Professional provides multiple modes for reading a card's number: via card enrollment station, via enrollment station, or via the card reader of the access control device. You can connect a card enrollment station to the PC running the Web Client, and place the card on it to read the card number. Or you can specify the IP address, port number, user name and password to access the enrollment station to enroll card number. 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. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Person** .
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**. If not, select **Normal**.

Reading Frequency

If your card supports dual frequency (both IC and ID), select **Dual**. If not, select **Single**.

Note

If you select **Dual**, you can not set card encryption for the card.

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.

Audio

Turn on or turn off the audio.

Enrollment Station

You can enroll the card number remotely via enrollment station and copy back to the system.

If you select this mode, you should set the required parameters as follows.

Device Address

The IP address of the enrollment station.

Device Port

The port number of the enrollment station.

User Name

The user name used to log in to the enrollment station.

Password

The password used to log in to the enrollment station.

RF Card Type

EM card, M1 card, and ID card are supported.

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**.

10.6 Report Card Loss

If the person cannot find his/her card, he/she should contact the card issuer as quickly as possible and the card issuer should report card loss via Web Client immediately to freeze the access level on the lost card. The card issuer can issue a temporary card with effective period and access level to the person. When his/her card is found, the card issuer will recycle the temporary card and cancel the card loss, then the found card will be active again.

10.6.1 Report Loss for One Card

If the person cannot find his/her card, you can report the card loss so that the related access level will be inactive.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Person** .
2. **Optional:** Click ⌄ to search the person you want to report card loss for.
3. Click the name in the added person list to enter editing person information page.
4. In the Card area, move the cursor on the lost card and click 🔒 .
5. Click **OK** to confirm the operation.
6. Click **Save**.

   After reporting card loss, the access levels of this card will be inactive. However, the biometric credentials (such as fingerprints or faces) linked with this lost card can still be active after linking them to a temporary card.

10.6.2 Issue a Temporary Card to Person

If the card is reported loss, you can issue a temporary card to the person and set the card's effective period, which is used for temporary purpose. When you issue a temporary card to the person, other cards linked to this person will be inactive, and the biometric credentials (such as fingerprints and profile) linked to these inactive cards will be linked to this temporary card.

Before You Start

The person has reported the card loss.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Person** .
2. **Optional:** Click ⌄ to search the person you want to issue temporary card to.
3. Click the name in the added person list to enter editing person information page.
4. In the Card area, click + (Temporary Card).

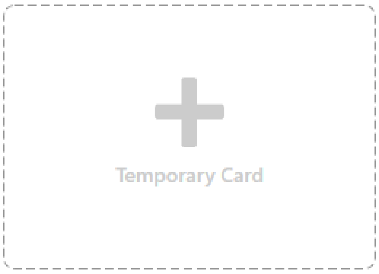


Figure 10-2 Add Temporary Card

5. Click **OK** to confirm the operation.
6. Enter the card number.
7. Set the expiry date when the temporary card becomes invalid.
8. Click **Save**.

Note

You can delete the temporary card for the person. After that, the inactive cards of the person will recover to be active, and their previously linked fingerprints and profiles will also recover.

10.6.3 Cancel Card Loss

If the lost card is found, you can cancel the card loss for the person. After that, the card's access level will be active and the original biometric credentials (such as fingerprints and profile) will be linked to this card again.

Before You Start

The person has reported card loss and has no temporary card.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Person** .
2. **Optional:** Click ⌄ to search the person you want to report card loss for.
3. Check the person(s) in the person list.
4. Click **Card** → **Cancel Card Loss** .

Note

When canceling card loss for the person, the person's temporary card will be deleted.

5. Click **OK** to confirm the operation.

10.7 Customize Additional Information

You can customize the additional information items which are not pre-defined in the basic information according to actual needs.

Steps

Note

Up to 20 additional information can be customized.

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Person** .
2. Click ⚙ **Customize Additional Information** to enter the customizing addition information page.
3. Click **Add**.
4. Create a name for this item.

   Note

   You can enter up to 32 characters.

5. Select the type to restrict the format for the additional item.

   Example

   For example, if you select general text, you need to enter words for the item. If you select date, you can only set the date for the item.

6. Click **Save**.
7. **Optional:** Do one or more of the following.

   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 11 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.

11.1 Add Role

Role is a group of platform permissions. You can add roles and assign permissions to roles, so that users can be assigned with different roles to get different permissions.

Steps

Note

The platform has predefined two default roles: Administrator and Operator. You can click the role name to view details. The two default roles cannot be edited or deleted.

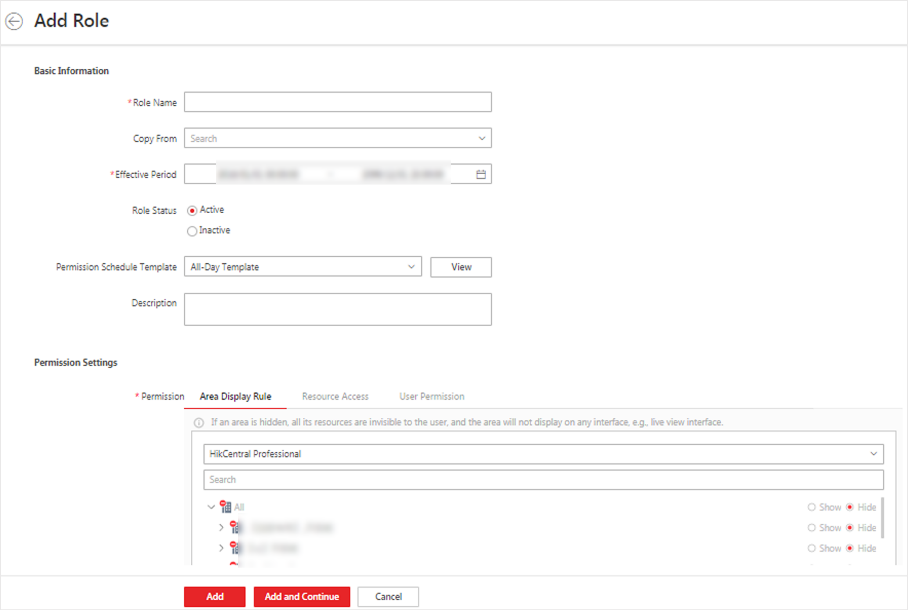
Administrator

Role that has all permissions of the platform.

Operator

Role that has all permissions for operating the Control Client and has the permission for operating the Applications (Live View, Playback, and Local Configuration) on the Web Client.

1. On the top left corner of Home page, select ≡ → **All Modules** → **General** → **Security** .
2. Click **Roles** on the left.
3. Click **Add**.



Add Role

Basic Information

*Role Name

Copy From: Search

*Effective Period

Role Status: ● Active ○ Inactive

Permission Schedule Template: All-Day Template | View

Description

Permission Settings

*Permission: Area Display Rule | Resource Access | User Permission

If an area is hidden, all its resources are invisible to the user, and the area will not display on any interface, e.g., live view interface.

HikCentral Professional

Search

All ○ Show ● Hide

○ Show ● Hide

○ Show ● Hide

Add | Add and Continue | Cancel

Figure 11-1 Add Role Page

4. Set the basic information of the role, including role name, effective period, role status, permission schedule template, description, etc.

Copy From

Copy all settings from an existing role.

Effective Period

Set the time range within which the role takes effect. The role is inactive outside the effective period.

Permission Schedule Template

Set the authorized time period when the role's permission is valid. Select **All-day Template**/ **Weekday Template**/**Weekend Template** as the permission schedule of the role, or click **Add New** to customize a new permission schedule template.

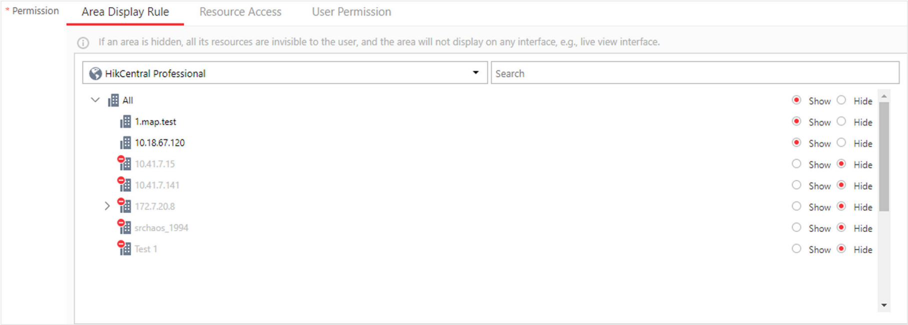
Note

- When role expires or the role's permission is invalid after editing the permission schedule, users assigned with the role will be forced to log out and not able to log in.
- The permission schedule's time zone is consistent with that of the platform.
- By default, the role will be linked with All-day Template after updating the platform.
- The permission schedule also goes for RSM client and OpenSdk client.

5. Configure permission settings for the role.

Area Display Rule

Show or hide specific area(s) for the role. If an area is hidden, the user assigned with the role cannot see and access the area and its resources.



If an area is hidden, all its resources are invisible to the user, and the area will not display on any interface, e.g., live view interface.

All	● Show	○ Hide
1.map.test	● Show	○ Hide
10.18.67.120	● Show	○ Hide
10.41.7.15	○ Show	● Hide
10.41.7.141	○ Show	● Hide
172.7.20.8	○ Show	● Hide
srchaos_1994	○ Show	● Hide
Test 1	○ Show	● Hide

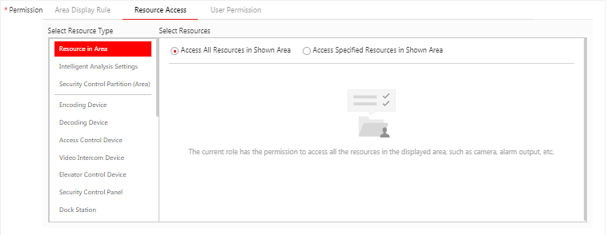
Figure 11-2 Area Display Rule

Resource Access Permission

Select the functions from the left panel and select resources from right panel to assign the selected resources' permission to the role.

Note

If you do not check the resources, the resource permission cannot be applied to the role.



● Access All Resources in Shown Area ○ Access Specified Resources in Shown Area

The current role has the permission to access all the resources in the displayed area, such as camera, alarm output, etc.

Figure 11-3 Resource Access Permission

User Permission

Assign resource permissions, configuration permissions, and operation permissions to the role.

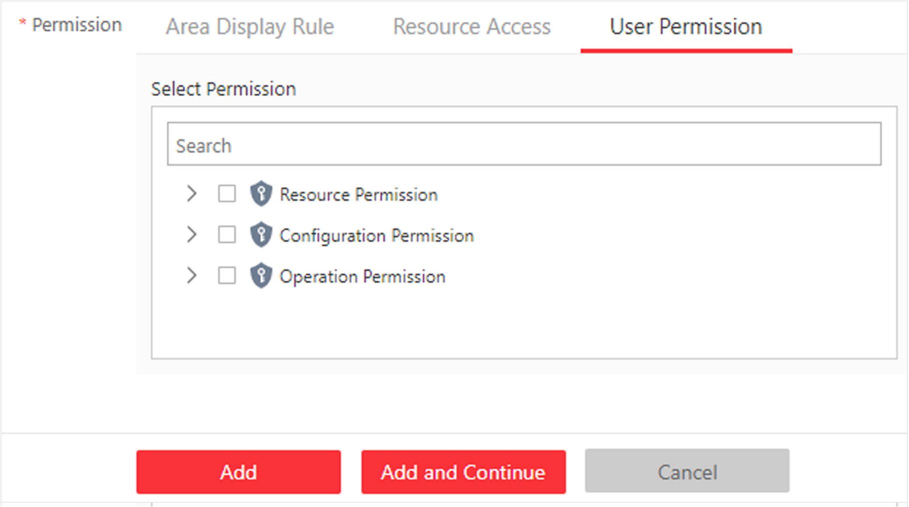
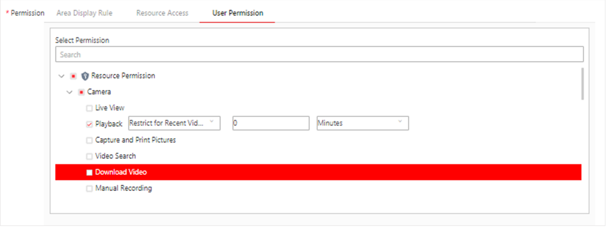


Figure 11-4 User Permission

Note

In **Resource Permission**, you can set time restriction for video playback permission. Once set, the role's permission of viewing and downloading video playback will be restricted within the configured time period. For example, if you set restriction for recent video to 6 minutes, the role can only view video playback of the last 6 minutes.



☑ Playback: Restrict for Recent Vid... 0 Minutes

Figure 11-5 Playback Permission

6. Do one of the following to complete adding the role.
   - Click **Add** to add the role and return to the role management page.
   - Click **Add and Continue** to save the settings and continue to add another role.
7. **Optional:** Perform further operations on added roles.

Edit Role Click role name to view and edit role settings.

Delete Role Check a role and click **Delete** to delete the role.

Inactivate Role Check a role and click **Inactivate** to set the role status to **Inactive**.

Activate Role Check an inactive role and click **Activate** to set the role status to **Active**.

Refresh Role Click **Refresh All** to get the latest status of the roles.

Filter Role Click ▽ to expand the filter conditions. Set the conditions and click **Filter** to filter the roles according to the set conditions.

11.2 Add Normal User

You can add normal users and assign roles to them for accessing the system and assign role to the normal user. Normal users refer to all users except the admin user.

Steps

1. On the top left corner of Home page, select ≡ → **All Modules** → **General** → **Security** .
2. Click **Users** on the left.
3. Click **Add**.
4. Set basic information for the user.

   User Name

   Can contain letters (a-z, A-Z), digits (0-9), and "-" only.

   Password

   Create an initial password for the user. The user will be asked to change the password when logging in for first time. See ***First Time Login for Normal User*** for details.

   Note

   We highly recommend you to create a strong 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 change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.

   Expiry Date

   The date when the user account becomes invalid.

   Email

   The system can notify user by sending an email to the email address. The user can also reset the password via email.

   Note

   The email address of the admin user can be edited by the user assigned with the role of administrator.

   User Status

   If you select **Inactive**, the user account will be inactivated until you activate it.

   Restrict Concurrent Logins

   To limit the maximum IP addresses logged in to the system using the user account, switch on **Restrict Concurrent Logins** and set the maximum number of concurrent logins.
5. Configure permission settings for the user.

   PTZ Control Permission

Set the permission level (1-100) for PTZ control. 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 of a camera.

Automatically Receive Alarm

Switch on and users with this role will receive resource alarms no matter configured as recipients of each alarm individually or not.

Assign Role

Select the roles that you want to assign to the user.

Note

If you want to add new roles, click **Add New Role**. See ***Add Role*** for details.

6. Do one of the following to complete adding the user.
   - Click **Add** to add the user and return to the user management page.
   - Click **Add and Continue** to save the settings and continue to add another user.
7. **Optional:** Perform further operations on the added normal users.

Edit User

Click user name to view and edit user settings.

Reset Password

Click user name and click **Reset** to set a new password for the user.

Note

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 details about changing password, refer to ***Change Password for Reset User*** .

Delete User

Select a users and click **Delete** to delete the selected user.

Force Logout

Select an online user and click **Force Logout** to log out the online user.

Inactivate/ Activate User

- The admin user or user with administrator permission can inactivate or activate a user.
- Select an active users and click **Inactivate/Activate** to inactivate/ activate the user.

Refresh User

Click **Refresh All** to get the latest status of all users.

Filter User

Click ▽ to set conditions and filter the users.

11.3 Import Domain Users

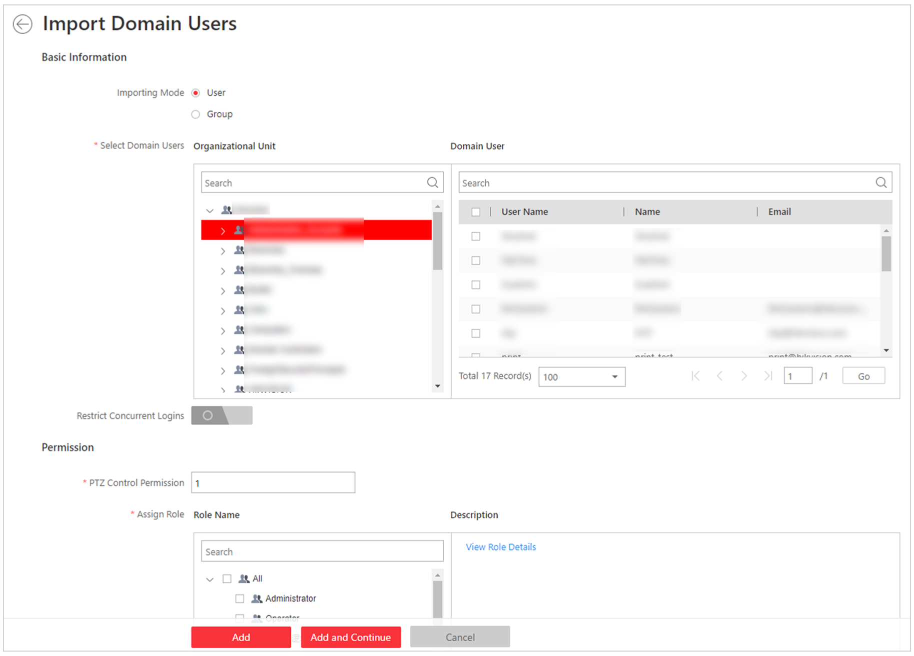
You can import the users (including the user name, real name, and email) in the AD domain to the system in a batch and assign roles to the domain users.

Before You Start

Make sure you have configured active directory settings. See ***Set Active Directory*** for details.

Steps

1. On the top left corner of Home page, select ≡ → **All Modules** → **General** → **Security** .
2. Click **Users** on the left.
3. Click **Import Domain Users**.



Import Domain Users

Basic Information

Importing Mode ● User ○ Group

* Select Domain Users

Organizational Unit

Search

[redacted]

Domain User

Search

□	User Name	Name	Email
□	[redacted]	[redacted]	
□	[redacted]	[redacted]	
□	[redacted]	[redacted]	
□	[redacted]	[redacted]	[redacted]
□	[redacted]	[redacted]	[redacted]

Total 17 Record(s) 100 1 /1 Go

Restrict Concurrent Logins

Permission

* PTZ Control Permission 1

* Assign Role

Role Name

Search

□ All

□ Administrator

□ Operator

Description

View Role Details

Figure 11-6 Import Domain Users

4. Select an importing mode.

   User

   Import individual 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 users in groups.

5. **Optional:** To limit the maximum IP addresses logged in to the system using the user account, switch on **Restrict Concurrent Logins** and enter the maximum number of concurrent logins.
6. 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 two users control the PTZ unit at the same time, the user who has the higher PTZ control permission level takes control of the PTZ.

7. Select the roles that you want to assign to the domain users.

Note

- If no role has been added, two default roles are selectable: administrator and operator.

  Administrator

  The role that has all permissions of the HikCentral Professional.

  Operator

  The role that has all permissions of the HikCentral Professional Control Client.
- If you want to add new roles, you can click **Add New Role**. See ***Add Role*** for details.

8. Complete importing the domain users.
   - Click **Add** to import the domain users and return to the user management page.
   - Click **Add and Continue** to save the settings and continue to import other domain users.
9. **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

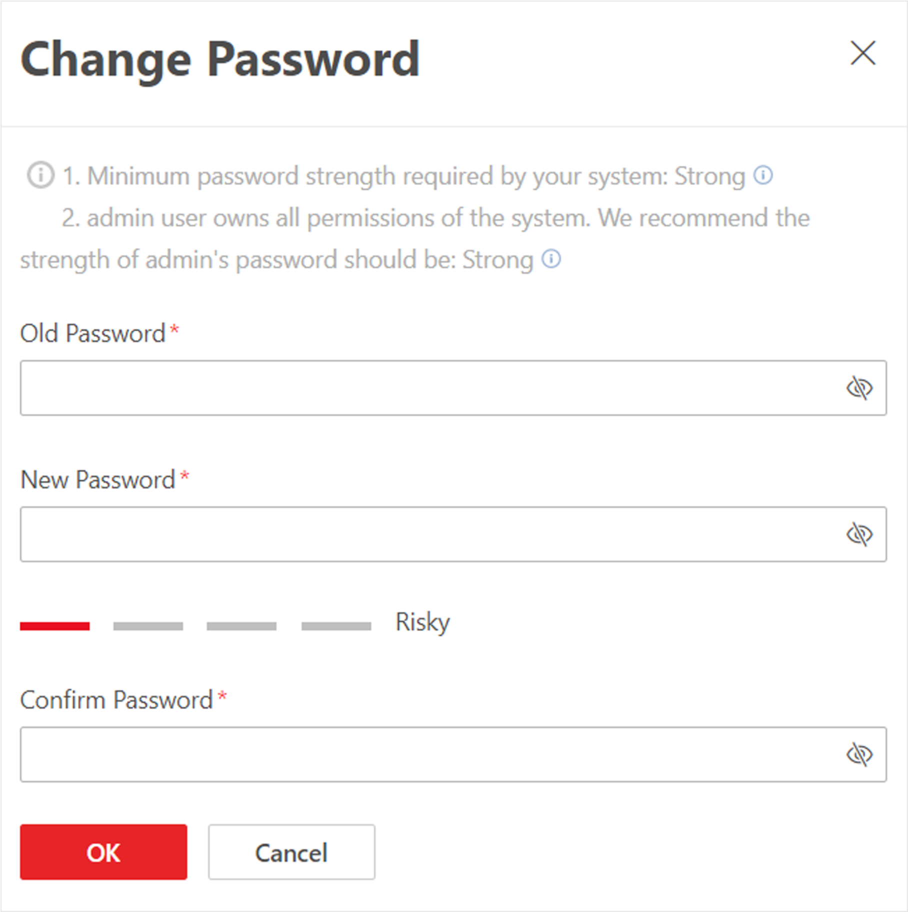
After successfully adding the domain users, the users can log in to the HikCentral Professional via the Web Client, Control Client, and Mobile Client with their domain account and password.

11.3.1 Change Password of Current User

You can change the password of your currently logged-in user account via Web Client.

Steps

1. Move the cursor to the user name at the top-right corner of the Web Client.
2. In the drop-down list, click **Change Password** to open the Change Password panel.



Change Password

ⓘ 1. Minimum password strength required by your system: Strong ⓘ
2. admin user owns all permissions of the system. We recommend the strength of admin's password should be: Strong ⓘ

Old Password*

New Password*

Risky

Confirm Password*

Figure 11-7 Change Password Panel

3. Enter the old password and new password, and confirm the new 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 save the change.

11.4 Reset Password for Admin User

If you forget the password of the admin user, you can reset the password for the admin user.

Steps

1. Use a web browser to enter the IP address of the PC running SYS service.

   Example

   If the IP address of PC running SYS is 172.6.21.96, you should enter ***http://172.6.21.96*** in the address bar.

   Note

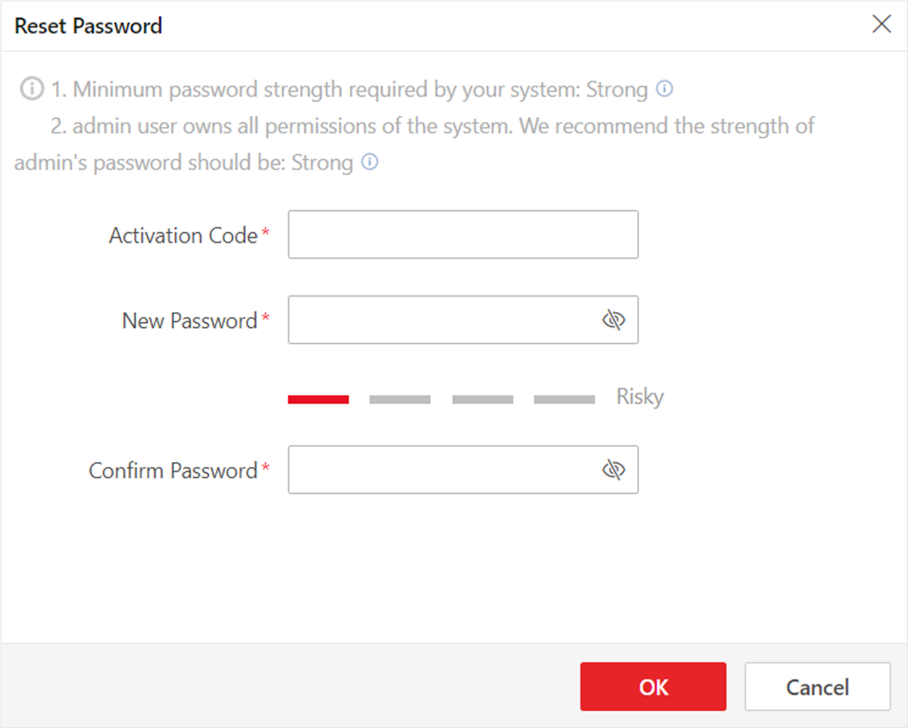
   You need to configure the SYS's IP address in **System Configuration → Network → WAN Access** before accessing the SYS via WAN. For details, refer to ***Set WAN Access*** .

2. **Optional:** When you log in for the first time, you need to 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.

3. Enter ***admin*** in **User Name**.
4. Click **Forgot Password** to open the Reset Password panel.



Reset Password

1. Minimum password strength required by your system: Strong
2. admin user owns all permissions of the system. We recommend the strength of admin's password should be: Strong

Activation Code*

New Password*

Risky

Confirm Password*

Figure 11-8 Reset Password

5. Enter the activation code and new password, and confirm the new 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.

6. Click **OK** to reset the password for admin user.

11.5 Reset Password for Normal User

If a normal user forget the password, the admin user or users with administrator role can reset the password for the normal user.

Steps

Note

If the normal user account is configured with an email address, the user can set a new password via email without requesting help from the admin user or user with administrator role. For details about setting user email address, refer to ***Add Normal User*** .

1. In the top left corner of Home page, select ≡ → **All Modules** → **Security** .
2. Click **Users** on the left.
3. Click the name of the user to enter the user detail page.
4. Click **Reset** and set a new password for the user.

11.6 Configure Permission Schedule

Permission schedule defines when a role's permissions are valid. During unauthorized time periods, the user assigned with the role will be forced to log out and cannot log in. The platform provides 3 permission schedule presets: All-day Template, Weekday Template, and Weekend Template. You can add new templates according to actual needs.

Steps

1. On the top left corner of Home page, select ≡ → **All Modules** → **Security** .
2. Click **Permission Schedule Template** on the left.
3. Click **Add** to create a blank template.
4. Set basic information.

   Name

Create a name for the template.

Copy from

To copy the settings of another existing template, select the template from the drop-down list.

5. In the **Weekly Schedule Template** box, set a schedule pattern for each day.
   1) Click **Scheduled Time** and select or draw in the box to define the authorized time periods.
   2) Click **Erase** and select or draw on the authorized time periods to clear the selection.

Note

You can set up to 8 separate time periods for each day.

6. **Optional:** Holiday schedule has a higher priority than weekly schedule. Set a holiday schedule if you want different schedules for specific days.
   1) Click **Add Holiday**.
   2) Select existing holiday templates, or click **Add New** to create a new holiday template (see ***Set Holiday*** for details).
   3) Click **Add**.
   4) Set a schedule pattern for holidays.
7. Do one of the following to finish adding the permission schedule template.
   - Click **Add** to save and add the template.
   - Click **Add and Continue** to add the template and continue to add another template.
8. **Optional:** Perform further operations on added templates.

View and Edit Template Details	Click the template to view and edit its configurations.
Delete Template	Click a template item and click 🗑 to delete it.

What to do next

Set permission schedules for roles to define in which period the permissions in the roles are valid. For detailed instructions, refer to ***Add Role*** .

Chapter 12 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.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Security** .
2. Click **Security Settings** on the left.
3. Set **Lock IP Address** switch to ON and the number of failed login attempts is limited.
   1) Select the allowable login attempts for accessing HikCentral Professional.

      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.
4. Select the **Minimum Password Strength** to define the minimum complexity requirements that the password should meet.
5. Set the maximum password age.
   1) Switch on **Enable Maximum Password Age** 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 predefined time length or customize the time length.
6. 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 predefined time period or customize the time period.
7. Click **Save**.

Chapter 13 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:

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, audible warning, etc.

13.1 About Event and Alarm

Event

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, 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.
The rule of an event includes four elements, namely, "**event source**" (i.e., the device which detects the event), "**triggering event**" (specified event type), "**what to do**" (linkage actions after this alarm is triggered), and "**when**" (during specified time period, the linkage actions can be triggered).

Example
The event can be defined as intrusion (**triggering event**) which happens in the bank vault and be detected by cameras mounted in the bank vault (**event source**) on weekend (**when**), and trigger the camera to start recording (**what to do**) once happened.

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 check the received real-time alarm message via the Control Client and search the history alarms.
The rule of an alarm includes six elements, namely, "**alarm source**" (i.e., the device which detects the triggering event), "**triggering event**" (specified event type occurred on the alarm source and triggers the alarm), "**when**" (during specified time period, the alarm can be triggered), "**recipient**" (the user in the system who can receive this alarm), "**priority**" (the priority of this alarm), and "**what to do**" (linkage actions after this alarm is triggered). Besides these five elements, you can also set other properties for this alarm such as alarm description, etc.

Example
The alarm can be defined as intrusion (**triggering event**) which happens in the bank vault and be detected by cameras mounted in the bank vault (**alarm source**) on weekend (**when**), and trigger the camera to start recording (**what to do**) once happened. this alarm is marked as High priority (**priority**), and users including admin and operators (**recipient**) can receive this alarm notification and check the alarm details.

13.1.1 Supported Events and Alarms

Currently, the system supports events and alarms for the following types of resources:

Video

Camera

The video exception or the events detected in the monitoring area of the camera, such as motion detection, line crossing, and so on.

Alarm Input

The event or alarm triggered by the alarm input of the video device in the system.

Access Control

Door

The access control event or alarm triggered at the doors (doors of access control devices and video intercom devices), such as access event, door status event, etc.

Alarm Input

The event or alarm triggered by the alarm input of the access control device in the system.

Person

The event or alarm detected by facial recognition camera or temperature screening cameras, such as face matched event or alarm, face mismatched event or alarm, rarely appeared event or alarm, abnormal skin-surface temperature, no mask event or alarm, etc.

Alarm

Security Radar

The radar arming event or alarm and the event ot alarm detected by the radars, such as auto-arming event, line crossing event, etc.

Alarm Input

The event or alarm triggered by the alarm input of the resources in the system, such as a smoke detector and zones of a security control panel.

Maintenance

The operating exceptions of the resources (e.g. camera, door, dock station, recording server, security audit server) added to the system, such as camera offline, server exception, and so on.

User-Defined Event

The event or alarm triggered by the user-defined event added in the system.

Combined Alarm

The combined alarm added in the system.

13.1.2 Define Alarm Priority, Alarm Category, and Alarm Icon

The system predefines several alarm priorities, alarm categories, and alarm icons 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.

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 categories 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.

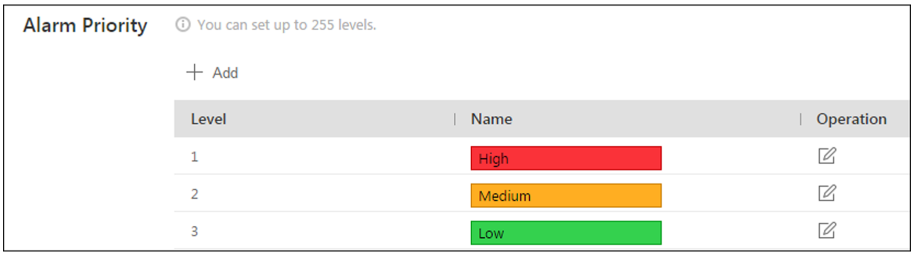
Alarm Icon When Alarm Occurs

The system pre-defines some icons of resources for several special alarms.

For example, it pre-defines the icon for the Door Opened Abnormally alarm. When this alarm is triggered, the door icon will turn to the icon displayed here to notify the users.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Event and Alarm** → **Basic Settings** → **Alarm Custom Settings** to enter the alarm custom 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	✎

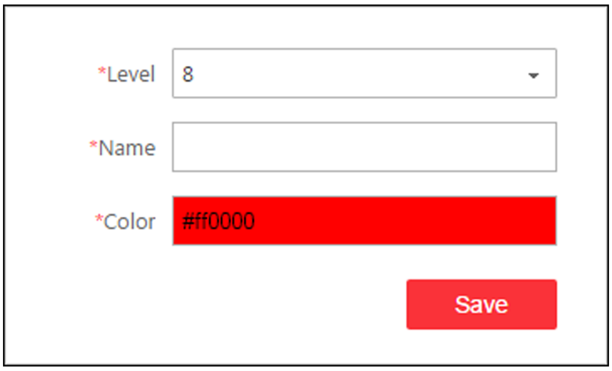
Figure 13-1 Alarm Priority Page

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.



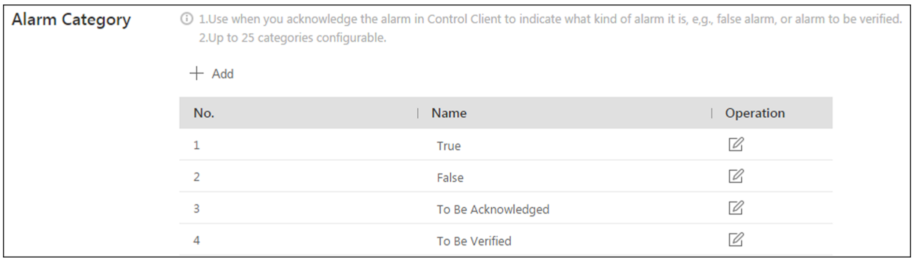
*Level	8
*Name	
*Color	#ff0000

Figure 13-2 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.

＋ Add

No.	Name	Operation
1	True	✎
2	False	✎
3	To Be Acknowledged	✎
4	To Be Verified	✎

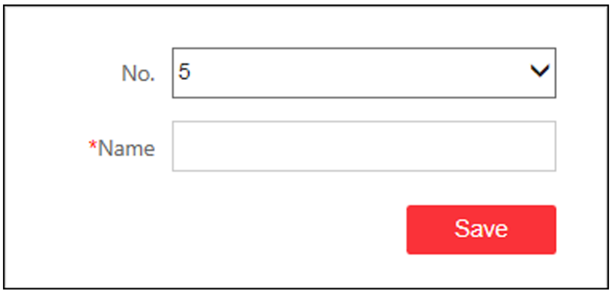
Figure 13-3 Alarm Category Page

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 13-4 Alarm Category Settings Window

4) Click **Save** to add the alarm category.

   The alarm category will be displayed on the alarm category list.

4. In the Alarm Icon When Alarm Occurs field, you can view the alarm icons provided by the system which are used to notify the users that the alarm is triggered.

Note

These pre-defined alarm icons cannot be edited and deleted.

5. 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.

13.1.3 Add Event and Alarm

In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Event & Alarm** → **Event & Alarm** and click **Add** to add an alarm or event.

Triggering Event and Source

The fields in the following image indicate two elements in the rule: "triggering event" and "event or alarm source".

Source Type

This field refers to **"event or alarm source"** in the rule, defining the specific the type of source that can trigger this event and alarm.

Triggering Event

This field refers to **"triggering event"** in the rule. The specific event type detected on the event source will trigger an event or alarm.

Source

This field refers to **"event or alarm source"** in the rule, defining the specific entity (such as cameras, devices, servers, etc.) which can trigger this event and alarm.

When setting a thermal related event and alarm for thermal cameras, you can select areas, points, or lines as event and alarm sources.

Threshold

If the source type you selected is **Regional People Counting**, you need to set extra conditions to define the triggering event.

Currently, you can set **Person Amount More/Less than Threshold** and **Person Amount More/Less than Threshold (Pre-Alarm)** for people counting group. For these two alarms, you need to set the threshold which determines whether the selected people counting groups will trigger an alarm when the detected number of people stayed less than or more than the threshold.

For example, if you set the threshold as ***"≥ 100 or ≤ 10"***, when the number of people detected in the selected people counting group is more than 100 or less than 10, an alarm will be triggered to notify the security personnel.

Card No.

If the source type you selected is **Person** and the triggering event is **Card Number Matched Event**, you need to select cards from the Person Group so that when someone presents these cards on the card readers of the alarm sources, an alarm will be triggered.

For example, if the card of one resident is stolen, you can set a card number matched alarm for this card. If someone punches this card on the card readers to gain access, an alarm will be triggered and you can quickly locate the suspect.

Frequency

If the source type you selected is **Parking Lot** and the triggering event is **Frequently Appeared Vehicle**, you can predefine the frequency.

For example, if you set the frequency to daily 3 times, when the devices in the source parking lot detect the license plate numbers of the vehicles in the selected vehicle list for more than 3 times in one day, an alarm will be triggered.

Vehicle Type

If the source type you selected is **Vehicle Features** and the triggering event is **Vehicle Type Matched Event**, you need to specify the vehicle type(s). When the source camera detects a vehicle the type of which matches with the one(s) you selected here, a vehicle type matched alarm will be triggered.

For example, if oil tank truck is not allowed on one road, you can set a vehicle type matched alarm for the camera mounted on this road and set the vehicle type as **Oil Tank Truck**. When the camera detects an oil tank truck, an alarm will be triggered.

Color

Click the color to select the color to indicate this event or alarm, which will be displayed in the event center. You can set the color according to the emergency of this event or alarm. For example, you can set red color for the urgent alarm and set green color for the prompt event.

Ignore Recurring Events

This function is used to avoid the same event or alarm occurs frequently in a short time. You need to set the **Ignore Alarms Recurred in (s)** which is the threshold of the recurring events or alarms.

For example, if you set **Ignore Alarms Recurred in (s)** to ***30 s***, the events or alarms of the same type occurred on the same camera within 30 s will be regarded as one event or alarm.

Note

The **Ignore Alarms Recurred in (s)** is 15 s by default. You can set it from 15 s to 1800 s.

Delay Alarm

If the source type you selected is **Camera** and the triggering event is **Camera Offline**, you can enable this function and set a delay duration. During the delay duration, when the source detects the triggering event, the triggering event will not be uploaded to the system. After this duration, if the source still detects this triggering event, the triggering event will be uploaded to the system and trigger an alarm.

With this function, when the system detects that the camera is offline, if the camera gets online again within the delay duration, it will not trigger a camera offline alarm. Thus the maintainers can focus on the cameras which are truly disconnected.

When

The field in the following image indicates one element in the rule: "when". It defines during specified time period, the alarm can be triggered.

Notification Schedule

The event or alarm source is armed during the notification schedule and when the source detects the triggering event, an event or alarm will be triggered and link the configured linkage actions. The system provides two types of notification schedule:

- **Schedule Template:** Select a notification schedule template for the event or alarm to define when the event or alarm can be triggered. For setting customized template, refer to ***Configure Notification 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. You can set the **Auto-End Arming** switch to on and set the specified time to automatically end arming for this event or alarm even if the end event does not occur.

Note

For example, assume that you have set event A as start event, event B as end event, and set the value of **Auto-End Arming in** to ***60 s***. Under these conditions, when event A occurs at T1, if event B occurs within 60 s , the arming schedule ends at the occurrence of event B (see the following figure Arming Schedule 1); if not, ends at 60 s after the occurrence of event A (see the following figure Arming Schedule 2).

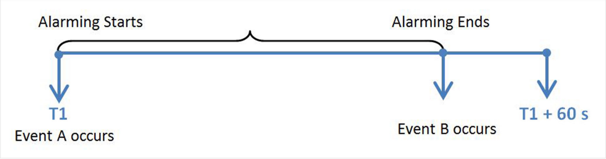


Figure 13-5 Notification Schedule 1

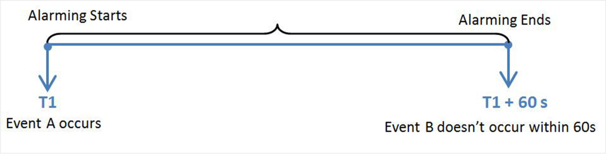


Figure 13-6 Notification Schedule 2

When A occurs at time T1, the event or alarm will be armed from T1, if A occurs again at time T2 but B doesn't occur, the event or alarm will be armed from T2 again.

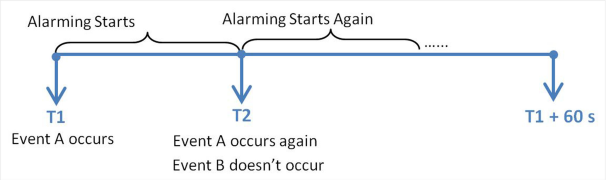


Figure 13-7 Notification Schedule 3

Priority

The field in the following image indicates one element in the rule: "recipient".

It defines the priority for the alarm. Priority can be used for filtering alarms in the Control Client.

Recipient

The field in the following image indicates one element in the rule: "recipient". It defines when the alarm is triggered, which users can receive the alarm notification and check the alarm details.

Select the user to send the alarm information to and the user can receive the alarm information when he/she logs in to HikCentral Professional via the Control Client or Mobile Client.

Note

By default, the admin user and the users configured with the permission of receiving alarms will be automatically selected as the recipients and cannot be unselected.

What to Do

The fields in the Additional Settings indicate one element in the rule: "what to do". It defines what actions the system will take to record the alarm details and notify security personnel.

Trigger Recording

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.
- **Display Video by Default:** Set the video to be displayed by default on the Control Client when receiving the triggered alarm information. You can select the recorded video or the live video to be displayed.

Note

- Make sure the related camera(s) have been configured with recording schedule.
- Up to 16 cameras can be set as related camera.

Capture Picture

Select one camera to capture pictures during the alarm, and you can view the captured pictures when checking the alarm in the Alarm & Event Search of the Control Client.

Note

Only one camera can be set for capturing pictures.

- If the alarm source is a camera, you can set to trigger the source camera itself for capturing pictures by selecting **Source Camera**.
- To trigger other camera for capturing pictures, select **Specified Camera** and select one camera for capturing pictures.

Capture Picture When: Specify the number of seconds to define when the camera will capture pictures for the alarm. After you set the number of seconds for pre/post-event (here the event refers to the triggering event), the camera will capture one picture at three time points respectively: at the configured seconds before the alarm starts, at the configured seconds after the alarm ends, and at the middle of the alarm (as shown in the picture below).

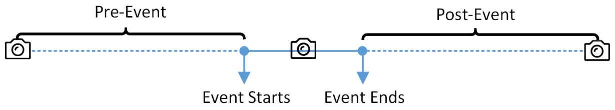


Figure 13-8 Capture Pictures

Note

The pre-event picture is captured from the camera's recorded video footage. This pre-event capture function is only supported by the camera which is set to store the video in the Recording Server (Cloud Storage Server, Hybrid SAN, or pStor).

Create Tag

Select the cameras to record video when the event occurs and set the storage location for storing the video files. The system will add a tag to the event triggered video footage for convenient search. The tagged video can be searched and checked via the Control Client.

- If the event source is a camera, you can set to trigger the source camera itself for tagged recording by selecting **Source Camera**.
- To trigger other cameras for tagged recording, select **Specified Camera** and click **Add** to add other cameras.

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 length of the video footage. For example, you can set to record the tagged video started from 5 seconds before the event and lasted until10 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.

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*** .

Link Access Point

You can enable this function to trigger the access points (including doors).

For doors, the doors can be locked, unlocked, remained locked, or remained unlocked when the alarm occurs.

For example, you can set to trigger all the doors remaining locked when intrusion of suspicious person is detected.

- **All Access Points:** When the alarm occurs, the system will trigger all the doors to take certain action.
- **Specified Access Point:** Click **Add** to select specified access points or emergency operation groups as the linkage targets. When the alarm occurs, the system will trigger these doors in the emergency operation groups to take certain action.

Link Alarm Input

Select alarm inputs and these alarm inputs will be armed or disarmed when the alarm occurs.

For example, when adding an intrusion alarm of camera A, which is mounted at the entrance of the building, you can link to arm the alarm input B, C, and D, which are PIR detectors mounted in different rooms in the building and are disarmed usually. When camera A detects intrusion alarm, these PIR detectors will be armed and trigger other events or alarms (if rules configured), so that the security personnel will get to known where the suspect goes.

Link Alarm Output

Select alarm output (if available) and the external device connected can be activated when the alarm 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 time period (unit: s) after which that the alarm output(s) will be closed automatically.

Trigger PTZ

Call the preset, patrol or pattern of the selected cameras when the alarm occurs.

Note

Up to 64 PTZ linkages can be selected as event linkage.

Send Email

Select an email template to send the alarm information according to the defined email settings.

You can select **Add New** to create a new email template.

Note

For details about setting email template, refer to ***Set Email Template*** .

Attach with Entry & Exit Counting

If the source type you selected is **Alarm Input**, you can select an entry & exit counting group from the drop-down list to attach a report of entry & exit counting in the sent email.

For example, if the fire alarm input detects fire in the building, the security personnel will receive a file, which contains the information such as the number of people still in the building, their names and profiles, phone numbers, and locations of last access.

Link Printer

If the source type you selected is **Alarm Input**, you can link to print the entry & exit counting report of certain entry & exit counting group.

For example, if the fire alarm input detects fire in the building, the platform will automatically send the entry & exit counting report to all the printers configured in the system so that they can get the information such as how many people are still in the building, their names and profiles, phone numbers, and locations of last access.

For details about printer settings, refer to ***Set Printer*** .

Trigger User-Defined Event

Trigger the user-defined event(s) when alarm is triggered.

You can select the pre-defined user-defined event(s) in the event list.

You can also click **Add New** below to set a new user-defined event(s).

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*** .

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.

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). You can check the map in the Alarm Center and Alarm & Event Search of the Control Client.

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.

Other Operations After Adding an Alarm

After adding an alarm, you can perform the following operations if needed.

Table 13-1 Other Operation

Operation	Description
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.

13.1.4 Add Combined Alarm

For some complicated scenarios, the alarm should be triggered when multiple events or alarms are detected or triggered. For example, the system detects intrusion in area B, then the arming of area A starts. After that, if the system detects intrusion in area A, then an alarm will be triggered to notify the security personnel.

In this section, we suppose the combined alarm is alarm A, the triggering event is event B. (The system detects event B, the arming of alarm A starts.)

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Event and Alarm** → **Combined Alarm** .
2. Click **Add** to open the Add Combined Alarm window.
3. Set the parameters in the page.

   Alarm Triggered Area

   Select the area of the alarm (alarm A) happened.

   Alarm Priority

   The priority including low, medium, high and custom level which indicates the urgent degree of this alarm (alarm A).

   Alarm Name

   Create a name for this alarm (alarm A).

   Description

   Describe the alarm (alarm A) according to your requirements.

   Ignore Recurring Alarms

   Enable **Ignore Recurring Alarms** and set the time. After enabled, the system will ignore the recurring alarm(alarm A) within the time period.

4. Configure the Schedules, which defines the arming schedule of this alarm (alarm A).
   1) Click ⊕ .
   2) Select the schedule template as **All-day Template**, **Weekday Template** or **Weekend Template**.
   3) Click **Save**.

   Note

   You can click the configured Schedule panel to edit the arming schedule, or move the cursor on the Schedule panel and click 🗑 appeared in the top right corner to delete it. If the schedule is deleted, all related conditions and actions will also be deleted.

5. Configure the Condition, which defines the triggering condition of this alarm (alarm A).
   1) Click ⊕ .
   2) Select the triggering logic.
   3) Click ⊕ to select the event type and event source (event B) that trigger this alarm (alarm A).
   4) Click **Save**.
   5) **Optional:** Click ⊕ at the right of selected event type and source panel to select more event types and sources.

   Note

   You can click the configured Condition panel to edit all conditions, or move the cursor to the Condition panel and click 🗑 appeared in the top right corner to delete all configured conditions at the same time. If the conditions are deleted, all related actions will also be deleted.

6. Configure the Actions, which defines the linkage action (such as trigger recording, capture picture, and create tag) and recipient after this alarm (alarm A) is triggered.
   1) Click ⊕ at the right of Condition module.
   2) Click **Add Linkage Action** and select the Alarm Recipients.

   Note

   If **Automatically Receive Alarm** is enabled for some users (refer to ***Add Normal User*** for details), an action panel of **Alarm Recipients** will be automatically generated after setting the conditions, and the users will be selected as the recipient. You can click the generated action panel to edit the alarm recipients, but the selected users cannot be unselected.

   3) Select user(s) to receive the alarm information.
   4) Click **Save**.
   5) **Optional:** Click ⊕ below the alarm recipient panel to add more linkage actions and configure action parameters.
7. Click **Save** in the upper-right corner of this page, and this alarm (alarm A) will be added to the system.

   Note

   If the alarm recipients are not configured for this combined alarm, you cannot save the combined alarm.

8. **Optional:** Perform the following operations according to your requirements.

   Add to Map
   Click **Add to Map** to add this alarm to the map. After that, the alarm will be marked in the map when the alarm is triggered.

   Copy Parameters to Existed Alarm
   Click **Copy**, and then select the items (such as basic information, actions, arming schedule, receiving mode) to copy, and select the target alarm to copy to.

   Delete Alarm
   Click **Delete** to delete this alarm.

   Test
   Click **Test** to trigger this alarm manually, and you can check whether the linkage actions take effect and whether the recipients receive the notification.

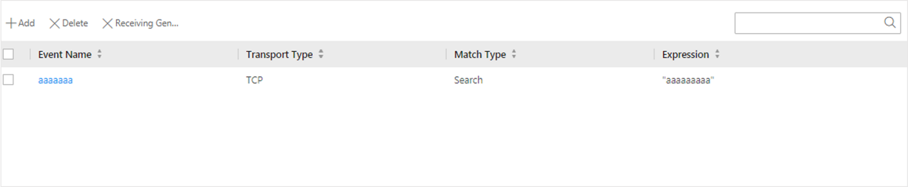
   Enable
   Click **Enable** to enable this alarm. After enabled, this alarm is armed.

13.2 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.

Steps

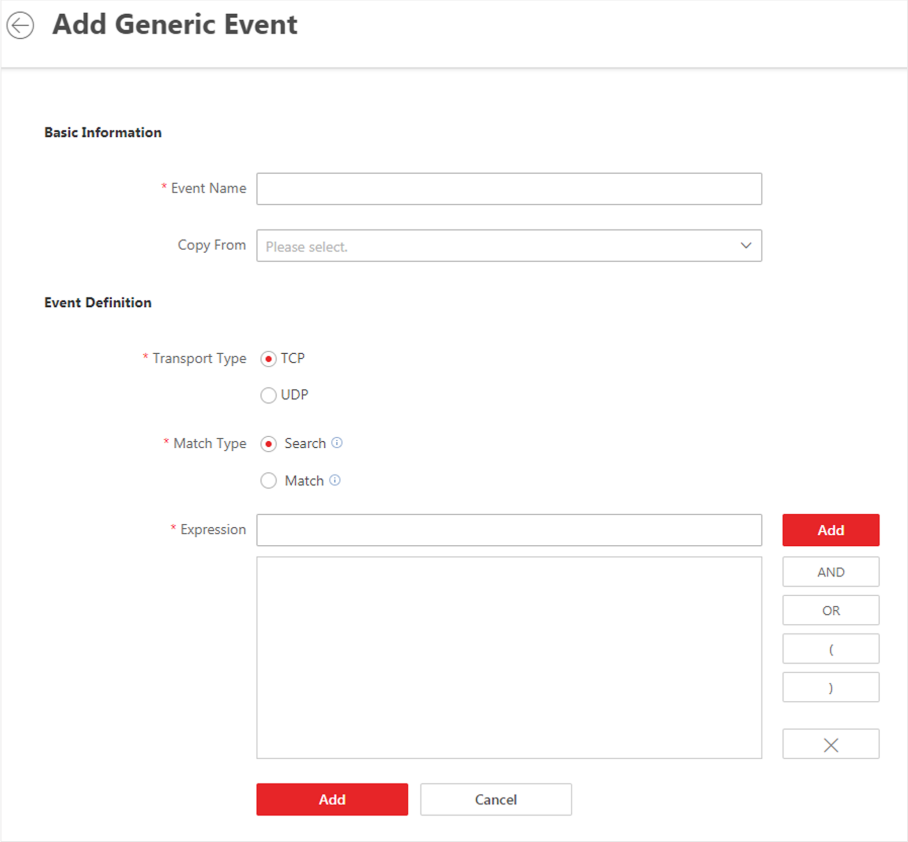
1. In the top left corner of Home page, select ≡ → **All Modules → General → Event and Alarm → Basic Settings → Generic Event** to enter the generic event settings page.



□	Event Name	Transport Type	Match Type	Expression
□	aaaaaaa	TCP	Search	"aaaaaaaaa"

Figure 13-9 Generic Event Settings Page

2. Click **Add** to enter the Add Generic Event page.



Add Generic Event

Basic Information

* Event Name

Copy From: Please select.

Event Definition

* Transport Type: ● TCP ○ UDP

* Match Type: ● Search ○ Match

* Expression

Figure 13-10 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 select the package transmission method as 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" or "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. Click **Add** to add the event and back to the event list page.
9. View in the Generic Event list to check whether the event has been added successfully.
10. **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
Select the event(s) and click **Delete** to delete the selected event settings.

Delete All Event Settings
Check the check box in the heading row, and click **Delete** to delete all the event settings.

Receive 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 select the event(s), and click **Receive Generic Event** to enable receiving the generic event.

13.3 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.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Event and Alarm** → **Basic Settings** → **User-Defined Event** to enter the user-defined event management page.
2. Click **Add** to open the following window.

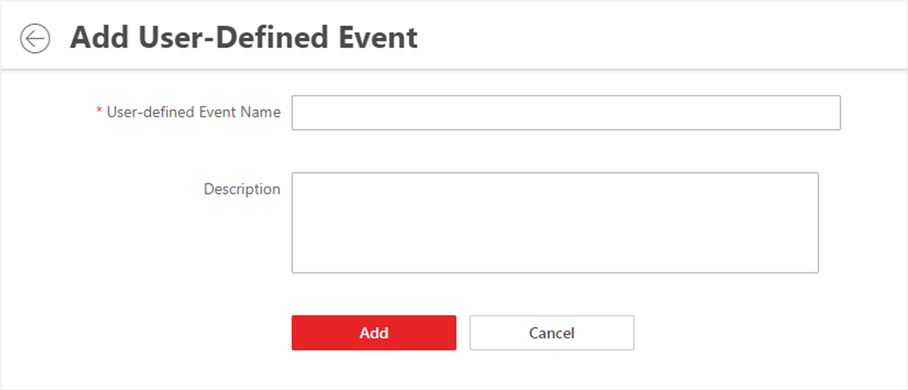


Figure 13-11 Add User-Defined Event

3. Create a name for the event.
4. **Optional:** Enter the description information to describe the event details.
5. Click **Add** to add the event and go back to the event list page.

   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 HikCentral Professional by using the data received from the third-party system. You can trigger the user-defined events outside the HikCentral Professional. For details, contact our technical support.

Note

- For configuring the alarm source, arming schedule, and alarm action, refer to ***Configure Event and Alarm*** .
- For triggering the user-defined event on the Control Client, refer to *User Manual of HikCentral Professional Control Client*.

13.4 Configure Notification Schedule Template

When setting event and alarm, you can select the pre-defined notification schedule template to define when the event or alarm can be triggered and notifying the recipients. The system pre-defines three default notification schedule templates: All-day Template, Weekday Template, and Weekend Template. You can also add a customized template according to actual needs.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Event and Alarm** → **Basic Settings** → **Notification Schedule Template** .

2. Click **Add** to enter the adding notification schedule page.

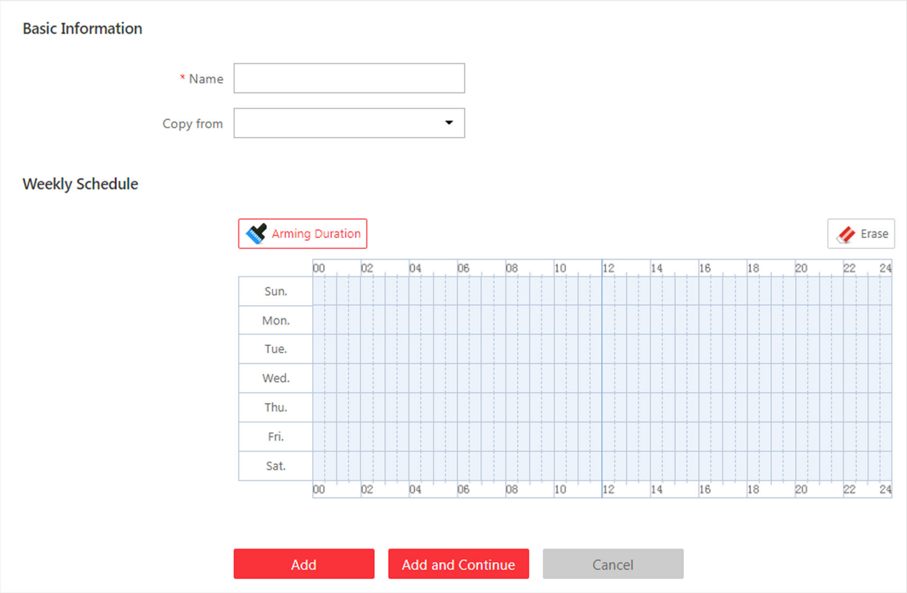


Figure 13-12 Add Notification Schedule Template

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. Click **Notification Duration** and drag on the time bar to set the time periods. During the time periods, the event can be triggered on the event source and notify the recipients in HikCentral Professional.

   Note

   Up to 4 time periods can be set for each day.

5. **Optional:** Click **Erase** and click on the drawn time period to clear the corresponding time period.
6. Finish adding the notification schedule template.
   - Click **Add** to add the template and go back to the notification schedule template list page.
   - Click **Add and Continue** to add the template and continue to add other template.

   The notification schedule template will be displayed on the notification schedule template list.

7. **Optional:** Perform the following operations after adding the notification 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.

13.5 Event and Alarm Search

On the event & alarm search module, you can view the alarm overview, search the historical event or alarm by setting search condition as required.

13.5.1 Alarm Overview

In the alarm overview module, it gives you an overview of the alarm distribution, top 5 alarms and top 5 warning zones.

In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Event & Alarm** → **Event & Alarm Search** → **Overview** to enter the Alarm Analysis page.

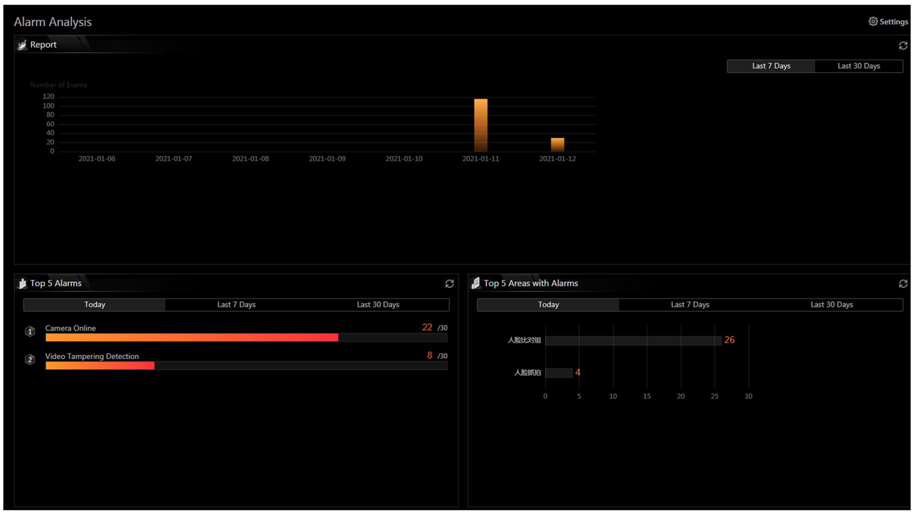


Figure 13-13 Alarm Analysis

You can click **Set** in the upper-right corner to customize the event or alarm types to be calculated in the overview page.

In the upper area of the page, the number of events triggered in the last 7 days or last 30 days are displayed in vertical bar chart.

In the lower-left area of the page, the top 5 alarms triggered in today, last 7 days or last 30 days are displayed in horizontal bar chart.

In the lower-right area of the page, the top 5 areas with alarm in today, last 7 days or last 30 days are displayed in horizontal bar chart.

13.5.2 Search Event/Alarm Logs

You can search the event and alarm log files of the added resource for checking.

Before You Start

You should configure the event and alarm settings first.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Event & Alarm** → **Event & Alarm Search** → **Event & Alarm Search** to enter the Event & Alarm Search page.
2. Set the time range for search.
   - Select a predefined time period for search.
   - Select **Custom Time Interval** and specify the start time and end time for search.
3. Select the event type as **All**, **Not Trigger Alarm** or **Trigger Alarm**.

   All

   Both events and alarms.

   Not Trigger Alarm

   The events happened but were not triggered as alarms.

   Trigger Alarm

   The events happened and were triggered as alarms.
4. Enable **Area** and then click 🗋 to select the area of the event source.
5. Enable **Triggered By** and then select the types of event source in the drop-down list.

   Note

   The Remote Site is only available for the Central System with Remote Site Management module (based on the license you purchased).
6. Click 🗋 to select the triggering event(s)/alarm(s) and source(s).
7. Enable **Alarm Name** to select the alarm name in the drop-down list.
8. **Optional:** If you select **Trigger Alarm**, you can set the following filter conditions.

   Marking Status

   Turn the **Marked** switch to on, and select **Marked** or **Unmarked** to filter the marked or unmarked alarms/events.

   Acknowledging Status

   Turn the **Status** switch to on, and select **Acknowledged** or **Unacknowledged** to filter the acknowledged or unacknowledged alarms/events.

   Priority

   Turn the **Priority** switch to on, and select the priority level to filter the alarms/events by priority.

   Category

Turn the **Priority** switch to on, and select the category to filter the alarms/events by category.

9. Click **Search**.

The matched event or alarm logs display on the list.

10. Optional: Perform the following operation(s) after searching alarms or events.

View Event or Alarm Details
Click the **Name** field of the searched event or alarm to view the details and the linked picture, video, and map.

Export Alarms or Events
Click **Export** and select the format and saving path to save the found events or alarms to your PC.

Click on the Operation column to export the specified event or alarm to your PC.

Note

You can view the exporting process in the Download Center by clicking in the top of the interface.

13.6 Send Event and Alarm Report Regularly

You can set a regular report rule for specified events or alarms, and the system can send an email with a report attached to the target recipients daily or weekly, showing the details of specified events or alarms triggered on 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. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Event and Alarm** → **Basic Settings** → **Report** .

2. Click **Add**.

3. Create a name for the report.

4. Set the event(s) or alarms contained in the report.

1) In the Report Target field, click **Add**.

All the added events and alarms 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. Select the **Report Language**.
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.

Chapter 14 Manage Video

After adding encoding devices to the system, you need to set video related parameters to ensure the security personnel can not only view live videos streamed from these devices via the Control Client and Mobile Client, but also access other important functions such as playback and intelligent recognition. These functions can provides great help and convenience for their works such as security surveillance and investigation.

14.1 Flow Chart

The two flow charts below show the process of configurations and operations required for viewing videos of encoding devices and other related functions on current site and remote site respectively.

View Videos of Encoding Devices on the Current Site

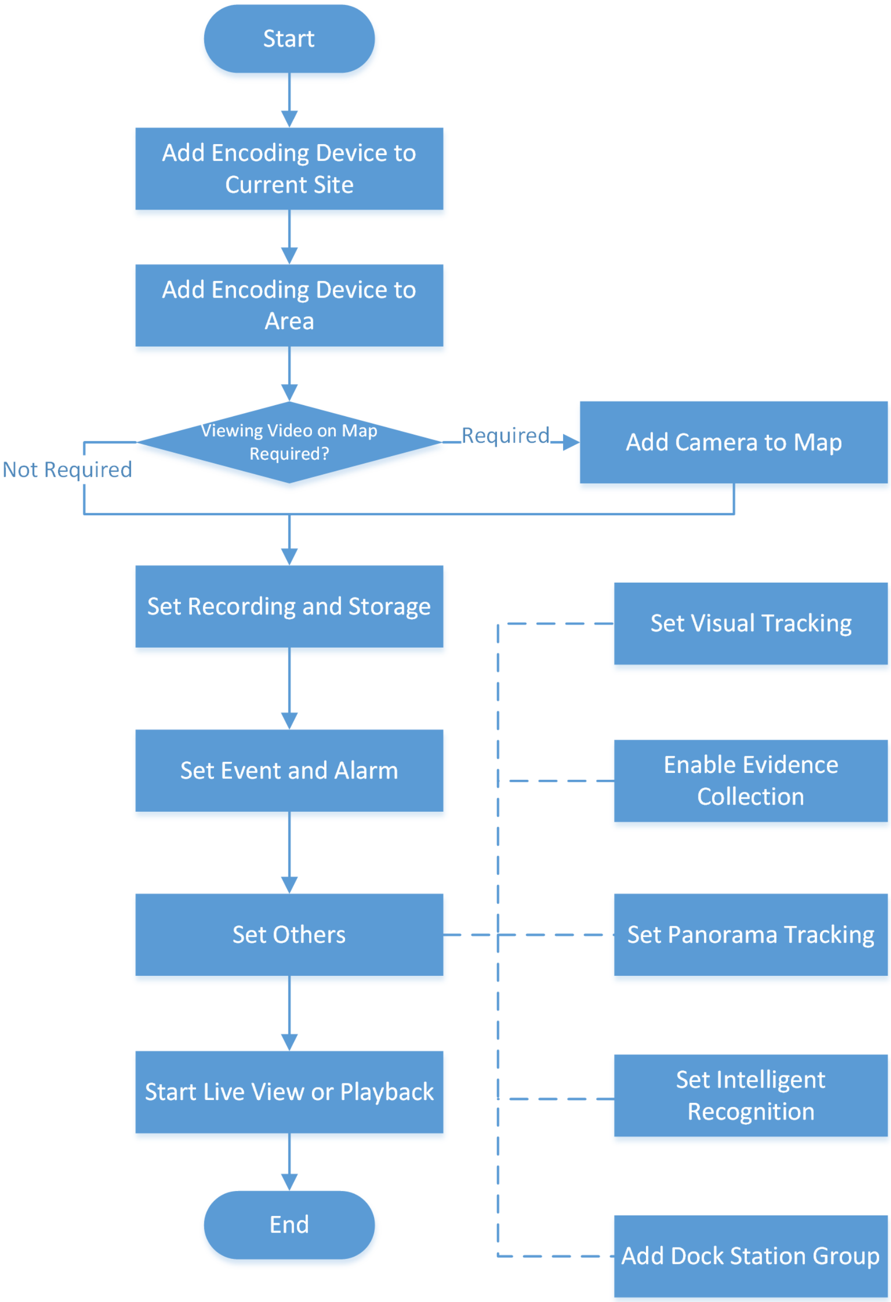

Start
Add Encoding Device to Current Site
Add Encoding Device to Area
Viewing Video on Map Required?
Required
Not Required
Add Camera to Map
Set Recording and Storage
Set Event and Alarm
Set Others
Start Live View or Playback
End
Set Visual Tracking
Enable Evidence Collection
Set Panorama Tracking
Set Intelligent Recognition
Add Dock Station Group

Table 14-1 Flow Chart Description

Procedure	Description
Add Encoding Device to Current Site	Add encoding device to the current HikCentral Professional site by online detection, IP address, port segment, **Hik-Connect DDNS**, device ID, device ID segment, etc.

Procedure	Description
	For details, see ***Manage Encoding Device*** .
Add Encoding Device to Area	Group encoding devices to different areas according to the locations of the devices for convenient management. For details, see ***Manage Area*** .
Add Camera to Map	Add cameras to a map as hot spots to view videos on map. After that, you can get the video information and camera location information at the same time. For details about adding cameras to map, see ***Add Hot Spot on Map*** .
Configure Recording and Storage	Define the periods during which video recording is activated. And set the storage location for the recorded video footage and the uploaded pictures (e.g., alarm related pictures). For details about configuring recording and storage, see ***Configure Storage and Recording*** .
Configure Event and Alarm	Configure linkage actions for the events detected by the encoding devices. For details, see ***Configure Event and Alarm*** .
Configure Others	You can configure other video related functions including visual tracking, panorama tracking, intelligent recognition, and dock station group. • Configure Video Tracking: Video tracking is a target tracking function that allows you to track a target (e.g., a suspect) moving across fields of view of multiple cameras by switching views of camera nearly seamlessly. For details about the configuration, see ***Configure Visual Tracking*** . • Configure Panorama Tracking: Panorama Tracking is a target tracking function based on the linkage between a box/bullet camera and a speed dome. When a VCA event is detected or a target is selected manually, the bullet/box camera, through its video analysis function, can work together with the speed dome to locate, zoom in, and track the target. For details about configuring this function, see ***Configure Panorama Tracking*** . • Configure Intelligent Recognition: Intelligent recognition refers to the recognition of faces, body features, or behaviors, etc., by intelligent analysis devices added to the platform. For details configuring this function, see ***Intelligent Recognition*** . • Configure Dock Station Group: A dock station group refers to a group of persons (e.g., police officers) related to a same dock

Procedure	Description
	station — a data collector which can automatically detect and back up law-enforcement data from body camera(s) connected to it. After relating persons to a dock station, the videos and pictures stored on the persons' body cameras can be copied to the dock station. For details about configure dock station group, see ***Add Dock Station Group*** .
Start Live View or Playback	Start playing live videos or video footage of the encoding devices. For details, see ***Video Application*** .

View Videos of Encoding Devices on Remote Site

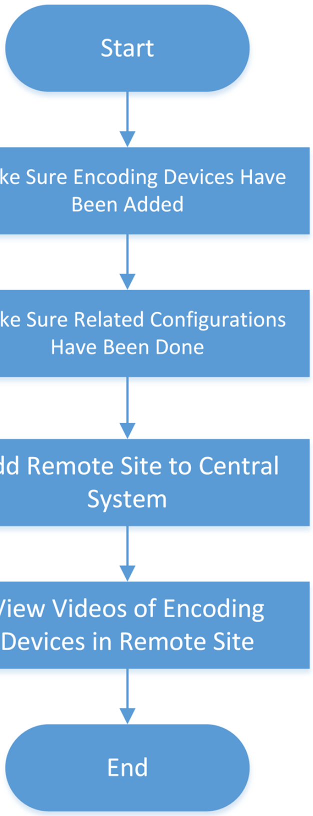

Start
Make Sure Encoding Devices Have Been Added
Make Sure Related Configurations Have Been Done
Add Remote Site to Central System
View Videos of Encoding Devices in Remote Site
End

Table 14-2 Flow Chart Description

Procedures	Description
Make Sure Encoding Devices Have Been Added	Make sure encoding devices has been added to a remote site by the administrator of the site.
Make Sure Related Configurations Have Been Done	Make sure recording and storage configurations and other required configurations (refer to configuration descriptions in ***Table 14-1***) have been done by the administrator of the site.

Procedures	Description
Add Remote Site to Central System	Add the remote site to the current site under the prerequisite that the latter has the Remote Site Management (RSM) module. The HikCentral Professional site with the RSM module is also called the Central System. For details about adding remote site to a Central System, see ***Add Remote Site by IP Address or Domain Name*** , ***Add Remote Site Registered to Central System*** , or ***Add Remote Sites in a Batch*** .
View Videos of Encoding Devices on Remote Site	Select the remote site and then select an encoding device on it to view the live video and video footage of the device. For details, see ***Video Application*** .

14.2 Manage Remote Site

You can add other HikCentral Professional without RSM (Remote Site Management) module to the HikCentral Professional 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.

Remote Site

If the HikCentral Professional 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 HikCentral Professional 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.

14.2.1 Add Remote Site by IP Address or Domain Name

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

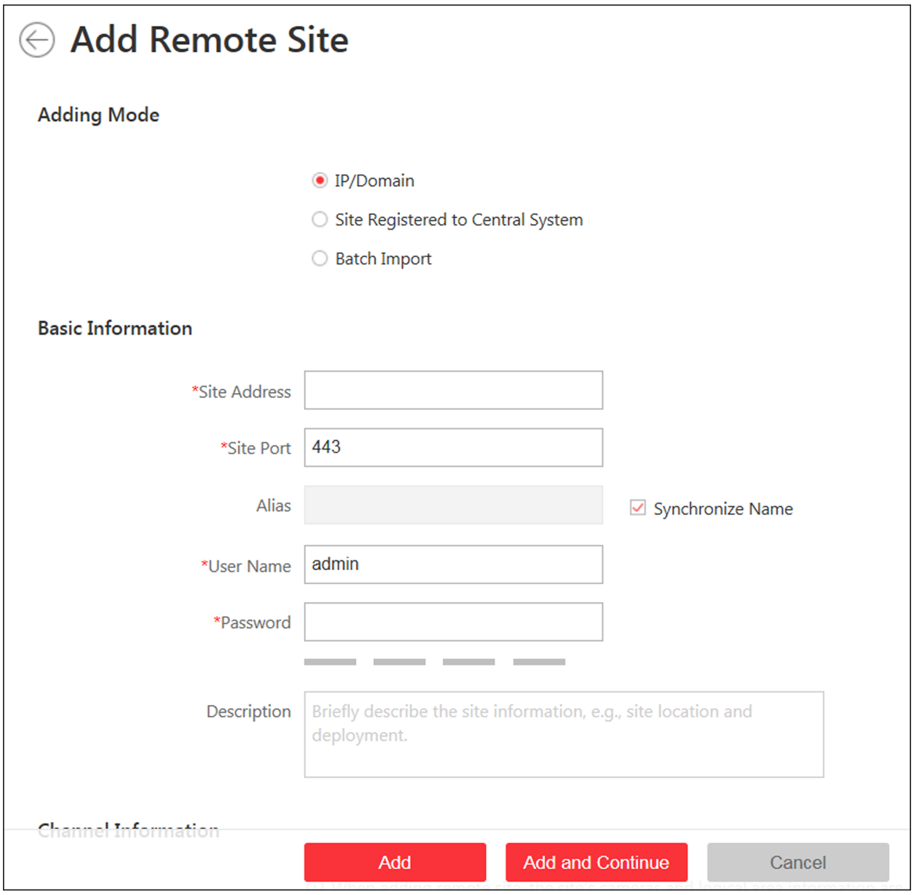
Perform this task when you need to add Remote Site by IP address or domain name.

Steps

Note

- When adding Remote Site, the site's cameras and area information are imported to the Central System by default.
- When you perform the following steps, the progress of the whole task will be displayed on the upper right side.

1. In the top left corner of Home page, select ≡ → **All Modules** → **Video** → **Remote Site Management** .
2. Enter the Add Remote Site page.
   - If no Remote Site is 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.



Add Remote Site

Adding Mode

● IP/Domain
○ Site Registered to Central System
○ Batch Import

Basic Information

*Site Address
*Site Port 443
Alias ☑ Synchronize Name
*User Name admin
*Password
Description Briefly describe the site information, e.g., site location and deployment.

Channel Information

Add | Add and Continue | Cancel

Figure 14-1 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 443.

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.

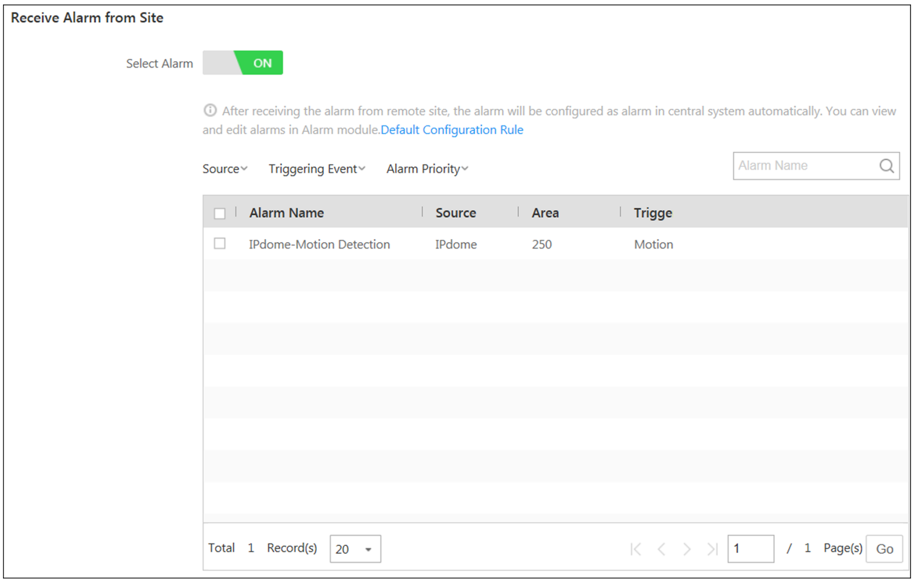
Description

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 change your password regularly, especially in the high security system, changing 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.



Receive Alarm from Site

Select Alarm ON

ⓘ After receiving the alarm from remote site, the alarm will be configured as alarm in central system automatically. You can view and edit alarms in Alarm module.Default Configuration Rule

Source˅ Triggering Event˅ Alarm Priority˅ Alarm Name

□	Alarm Name	Source	Area	Trigge
□	IPdome-Motion Detection	IPdome	250	Motion

Total 1 Record(s) 20 ▾ 1 / 1 Page(s) Go

Figure 14-2 Receive Alarm from Site Page

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 Event and Alarm module. For details about setting the event and alarm, refer to ***Configure Event and 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.

14.2.2 Add Remote Site Registered to Central System

If the Remote Sites have been registered to 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 ientering the Central System's network parameters (see ***Set Network Parameters*** for details).
- Make sure the receiving site registration function has been enabled on the Central System. (see ***Set Network Parameters*** for details).

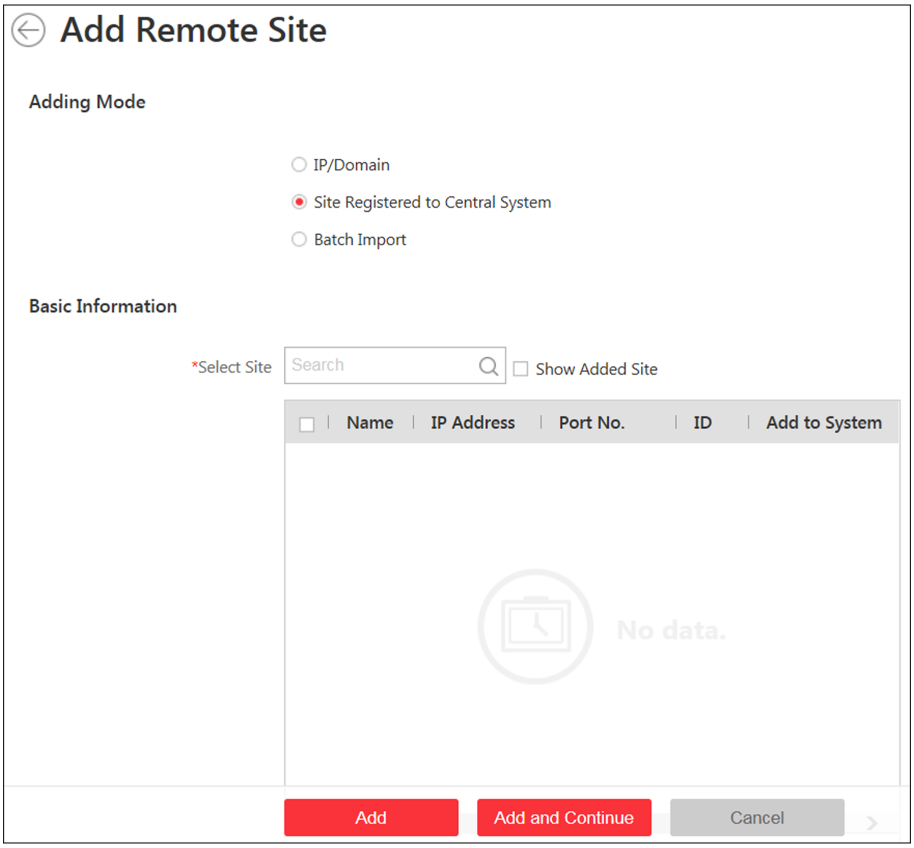
Perform this task when you need to add the site which has registered to the Central System.

Steps

Note

- When adding Remote Site, the site's cameras and logical area information are imported to the Central System by default.
- When you perform the following steps, the progress of the whole task will be displayed on the upper right side.

1. In the top left corner of Home page, select ≡ → **All Modules** → **Video** → **Remote Site Management** .
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.



Add Remote Site

Adding Mode

○ IP/Domain

● Site Registered to Central System

○ Batch Import

Basic Information

*Select Site: Search □ Show Added Site

□	Name	IP Address	Port No.	ID	Add to System

No data.

Figure 14-3 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 change your password regularly, especially in the high security system, changing 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.

14.2.3 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.

Steps

Note

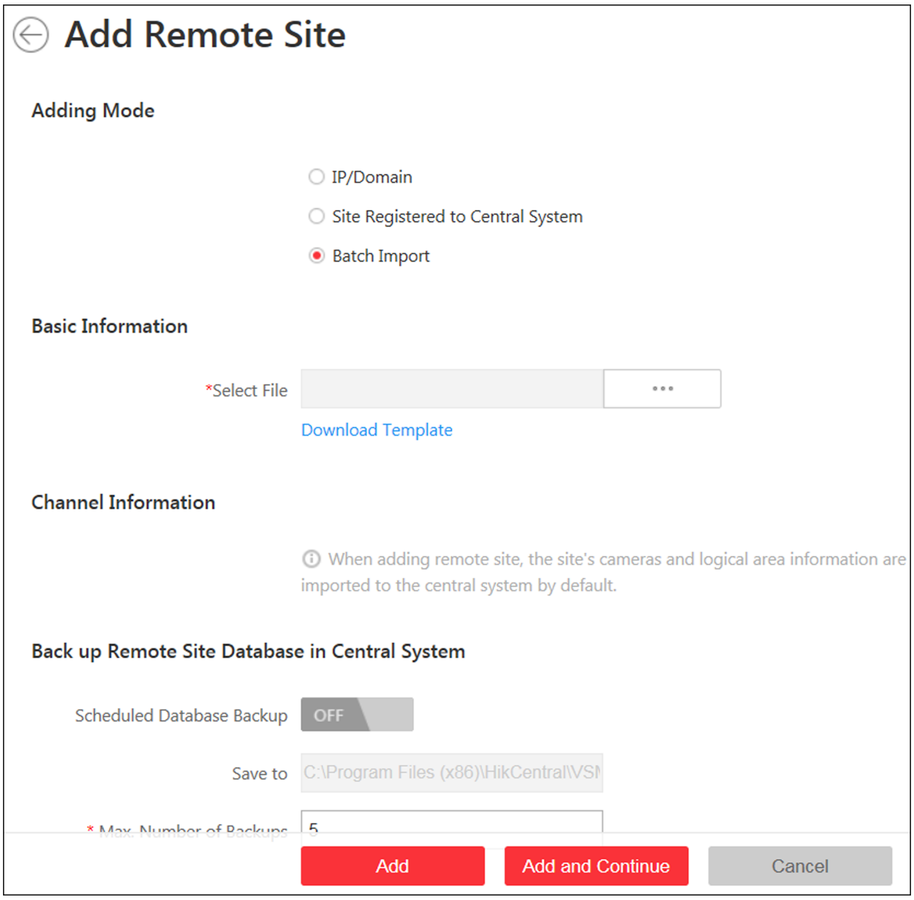
- When adding Remote Site, the site's cameras and logical area information are imported to the Central System by default.
- When you perform the following steps, the progress of the whole task will be displayed on the upper right side.

1. In the top left corner of Home page, select ≡ → **All Modules** → **Video** → **Remote Site Management** .

    Note

    If you have customized the menu (see ***Customize Navigation Bar*** for details), click **Remote Site Management** on navigation bar 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.



Add Remote Site

Adding Mode

○ IP/Domain

○ Site Registered to Central System

● Batch Import

Basic Information

*Select File ...

Download Template

Channel Information

ⓘ When adding remote site, the site's cameras and logical area information are imported to the central system by default.

Back up Remote Site Database in Central System

Scheduled Database Backup: OFF

Save to: C:\Program Files (x86)\HikCentral\VSI

* Max. Number of Backups: 5

Figure 14-4 Add Remote Site

3. Select **Batch Import** as the adding mode.
4. Click **Download Template** and save the predefined template 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.

14.2.4 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.

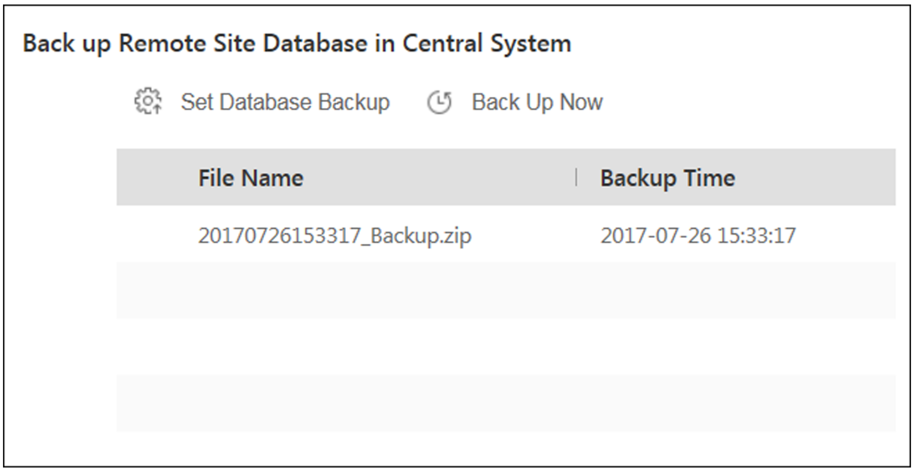
Steps

1. In the top left corner of the Home page, select ≡ → **All Modules** → **Video** → **Remote Site Management** .

Note

If you have customized the menu (see ***Customize Navigation Bar*** for details), click **Remote Site Management** on navigation bar to enter the Remote Site management page.

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

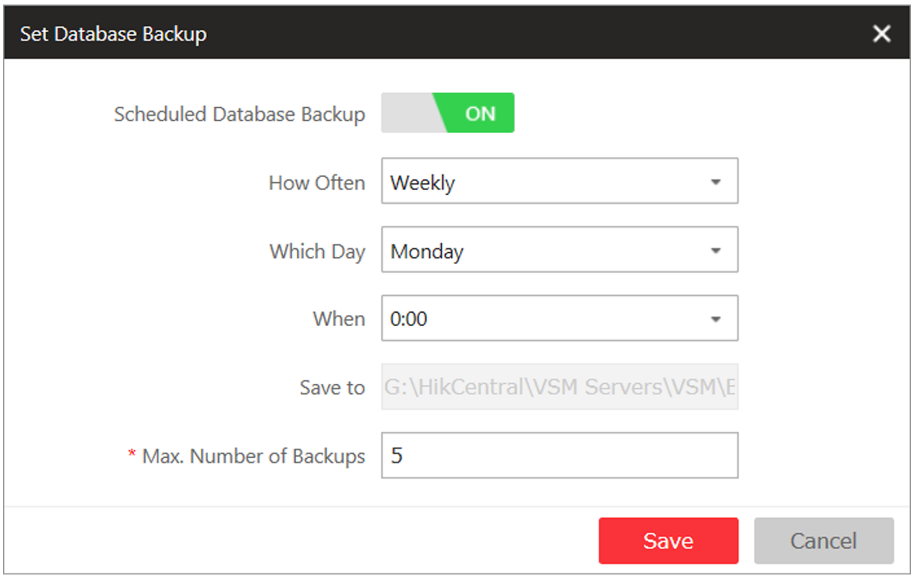


Back up Remote Site Database in Central System

File Name	Backup Time
20170726153317_Backup.zip	2017-07-26 15:33:17

Figure 14-5 Back up Remote Site Database in Central System

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



Set Database Backup

Scheduled Database Backup: ON

How Often: Weekly

Which Day: Monday

When: 0:00

Save to: G:\HikCentral\VSM Servers\VSM\E

* Max. Number of Backups: 5

Figure 14-6 Set Database Backup

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.

14.2.5 Edit Remote Site

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

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **Video** → **Remote Site Management** .

Note

If you have customized the menu (see ***Customize Navigation Bar*** for details), click **Remote Site Management** on navigation bar to enter 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**.

14.2.6 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.

Steps

Note

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

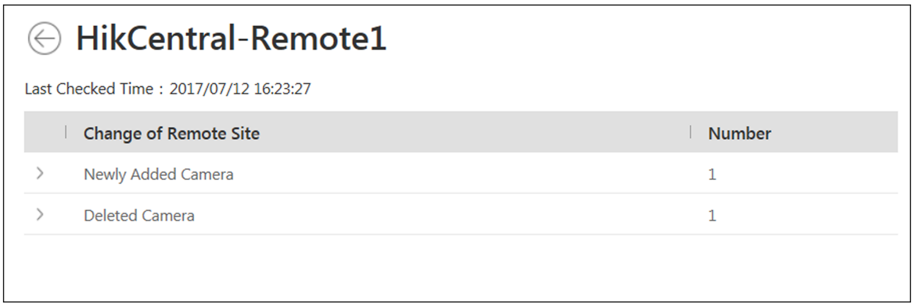
1. In the top left corner of the Home page, select ≡ → **All Modules** → **Video** → **Remote Site Management** .

Note

If you have customized the menu (see ***Customize Navigation Bar*** for details), click **Remote Site Management** on navigation bar to enter the Remote Site management page.

2. Click ⟳ in the site list on the left to get the latest status of the Remote Sites.
3. Click the site name whose resources are changed to enter its details page.

4. Click **Changes of Remote Site** to view the changes.



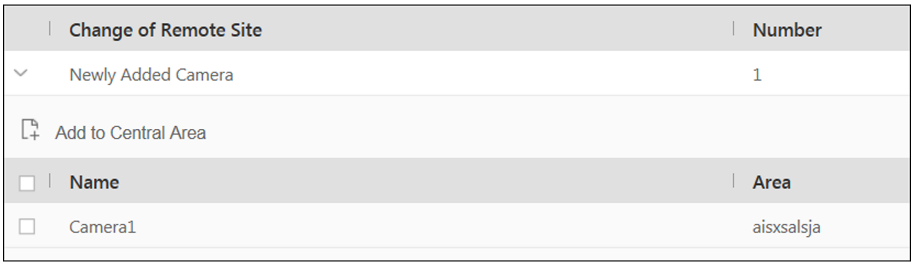
HikCentral-Remote1

Last Checked Time：2017/07/12 16:23:27

Change of Remote Site	Number
Newly Added Camera	1
Deleted Camera	1

Figure 14-7 Remote Site Management

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

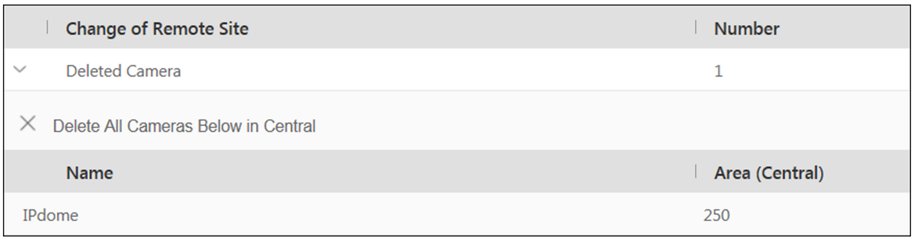
□ Name	Area
□ Camera1	aisxsalsja

Figure 14-8 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

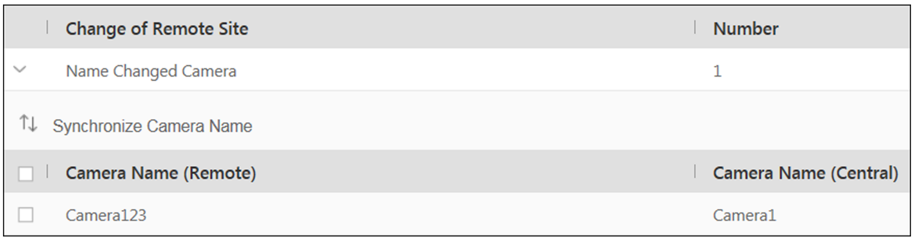
Name	Area (Central)
IPdome	250

Figure 14-9 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 14-10 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.

14.3 Configure Storage and Recording

Before you can play back video files recorded by cameras, you need to set the time periods for video recording and the location for storing video files and pictures first. And before you can import pictures (e.g., static e-map picture) and view pictures (e.g., alarm-related pictures) uploaded from devices, you need to set storage locations for these pictures and set related parameters.

HikCentral Professional provides four storage locations (encoding devices, Hybrid Storage Area Network, Cloud Storage Server, or pStor) for storing the recorded video files of the cameras.

Encoding Device

Store video files on the encoding devices (i.e., DVR, NVR, and network camera) locally. Take NVR for an example, the video files recorded by the cameras linked to it will be stored in its storage medium (e.g., HDDs, Net HDDs, and SD/SDHC cards) if you select **Encoding Device** as the storage location.

To store video files in this way, you need to make sure the encoding device is equipped with a storage medium and the storage medium should have been formatted.

Perform the following operations to format storage medium if required:

Go to the remote configuration page of the encoding device (≡ → **All Modules** → **General** → **Device Management** → **Encoding Device** → ⚙), and then click **Storage** → **General** , and then select the HDD, Net HDD or SD/SDHC card, and finally 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*** .

pStor Cluster Service

pStor Cluster Service is a service that can manage multiple pStors. When there are multiple pStors storing a large number of video files, use pStor Cluster Service to manage these pStors. For details about adding pStor Cluster Service, refer to ***Add pStor Cluster Service*** .

14.3.1 Configure Recording for Cameras on Current Site

For the cameras on the current site, HikCentral Professional provides five storage methods (storing on encoding devices, Hybrid Storage Area Network, Cloud Storage Server, pStor or pStor Cluster Service) 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 HikCentral Professional for area management. Refer to ***Manage Resource*** for detailed configuration about adding devices.

Steps

1. Enter the **Recording Setting** tab.
   1) In the top left corner of the Home page, select ≡ → **All Modules** → **General** → **Resource Management** → **Area** → .
   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 its name to enter camera settings page.
   4) Select the **Recording Settings** tab.
2. Turn on **Main Storage**.
3. Select the storage location for storing the recorded video file.

   Note

   If you select **Hybrid Storage Area Network**, **Cloud Storage Server**, **pStor**, or **pStor Cluster Service**, specify a server and (optional) select a Streaming Server to get video streams from cameras via it.

4. Select the storage type and configure other required parameters.

- Select **Real-Time Storage** as the storage type to store the recorded video files in the specified storage location in real time.

Note

If you select **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 the time periods 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, pStor or pStor Cluster Service, 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, Cloud Storage Server, pStor, or pStor Cluster Service. 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.

Recording Server Gets Video from Camera

If you select **Hybrid Storage Area Network**, **Cloud Storage Server**, **pStor** or **pStor Cluster Service** as the storage location, set the **Recording Server Gets Video from Camera** switch to on. And then configure the camera IP address, camera port, user name and password.

Note

- After the function is enabled, the recording server gets videos from the camera directly, avoiding the risk that if the NVR camera connected is offline, the recording server can not get video from the offline NVR.
- By default, the camera IP address is the IP address of current camera, you can also edit the IP address as the other camera's.

- Select **Scheduled Copy-Back** as the storage type to copy 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 scheduled copy-back is not configurable.
- The recordings can be copied only from the encoding device to Hybrid Storage Area Network, Cloud Storage Server, pStor or pStor Cluster Service, or from pStor to another pStor.

Copy to

Specify the time period to copy the recorded video files to the specified storage location.

Recording for Copy-Back

Select the type of recorded video file 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, pStor, or pStor Cluster Service is set as the auxiliary storage location, you can select **Real-Time Storage** to store recorded video files or select **Scheduled Copy-Back** to copy recordings from the encoding device or pStor (main storage) to specified auxiliary storage location according to the scheduled period.
- Before setting **Scheduled Copy-Back**, make sure you have configured real-time recording schedule stored in device local storage or pStor for the main storage.
- The recordings can be copied only from the encoding device to Hybrid Storage Area Network, Cloud Storage Server, pStor or pStor Cluster Service, or from pStor to another pStor.

6. Click **Save**.

14.3.2 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, pStor or pStor Cluster Service).

Steps

1. Go to the **Recording Settings** tab.
   1) In the top left corner of the Home page, select ≡ → **All Modules** → **General** → **Resource Management** → **Area** .
   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 the cameras added to it.
   4) Select a camera and click its name to enter the camera settings page.
   5) Select **Recording Settings** tab.
2. In the Recording Settings area, turn on **Storage in Central System**.
3. Select the storage location for storing the recorded video file.

Note

You can select **Hybrid Storage Area Network**, **Cloud Storage Server**, **pStor**, or **pStor Cluster Service**, 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.

     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, or sub-stream.

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, pStor, or pStor Cluster Service, 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 Copy-Back** 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.

5. Click **Save**.

14.3.3 Configure Storage for Imported Pictures

The pictures imported by the users, such as the original undercarriage pictures imported on Vehicle page, static e-map pictures, the face pictures in the person list, can be stored on the HDD of SYS server.

Before You Start

Make sure that you have at least 1GB of free space for picture storage.

Steps

Note

You can configure the storage only when the current Web Client is running on SYS server.

1. In the top left corner of the Home page, select ≡ → **All Modules** → **General** → **System Configuration** → → **Storage** → **Storage on SYS Server** .

   The disks of the SYS server are displayed with current free space and total capacity.
2. Select the disk to store the imported pictures.
3. **Optional:** Set the **Set Quota for Pictures** switch to on to allocate the quota for storing the pictures.
4. Click **Save**.

14.3.4 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 SYS server, Hybrid Storage Area Network, Cloud Storage Server, pStor, or NVR (Network Video Recorder).

Steps

1. Enter the picture storage setting page.
   1) In the top left corner of the Home page, select ≡ → **All Modules** → **General** → **Resource Management** → **Area** → **Camera** .
   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 its name to enter the camera settings page.
2. Select the **Picture Storage Settings** tab.
3. Switch on **Picture Storage**.
4. Select the storage location from the drop-down list.

Note

If you select System Management Server, the pictures will be stored on the SYS server. Click **Configuration** to view the disk on SYS server and storage quota, which can be edited via the Web Client running on the SYS server. Refer to ***Configure Storage for Imported Pictures*** for details.

5. Click **Save** to save the uploaded pictures to the specified location.

14.3.5 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.

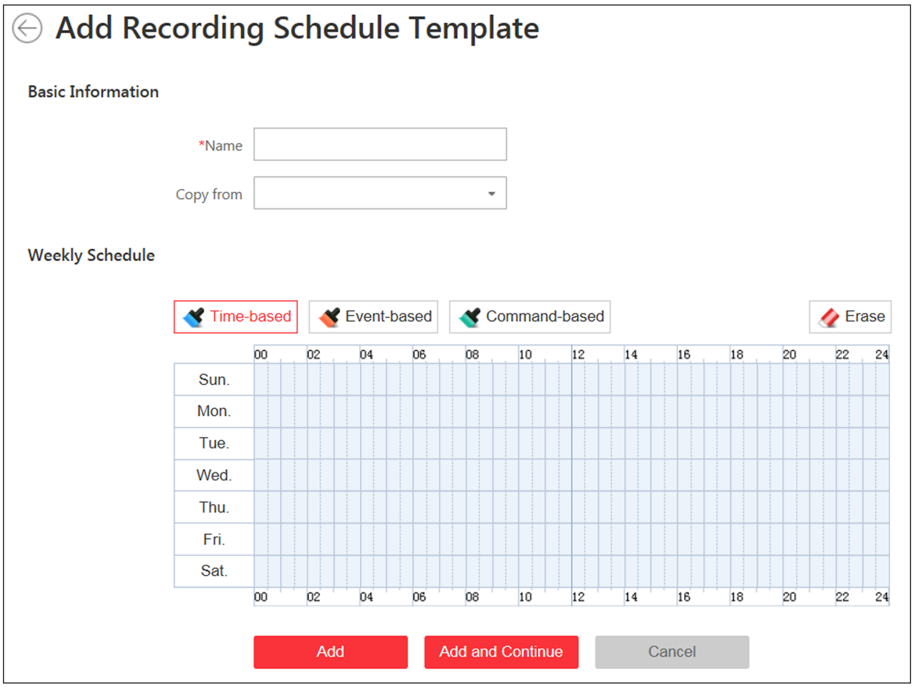
Perform this task when you need to customize the schedule to record the video files.

Steps

1. In the top left comer of the Home page, select ≡ → **All Modules** → **Video** → **Video Settings** → **Recording Schedule Template** .
2. Click + to enter the adding recording schedule page.

Note

Up to 32 templates can be added.



Add Recording Schedule Template

Basic Information

*Name

Copy from

Weekly Schedule

Figure 14-11 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).

14.4 Configure Visual Tracking

Visual tracking allows you to track an individual (such as a suspect) across different areas without losing sight of her/him. Before you can use this function, you need to associate a camera (hereafter named as "camera A") with other cameras nearby. After that, icons representing the nearby cameras will be overplayed on the view of camera A. You can click these icons to redirect to the associated cameras' views during live view or playback.

Steps

1. In the top left corner of the Home page, select ≡ → **All Modules** → **Video** → **Video Settings** → **Visual Tracking** .
2. Select an area from the area list.

   The page will display the thumbnails of the latest view of the cameras that support visual tracking settings in the selected area.
3. **Optional:** Check **Include Sub-Area** to display the available cameras in the sub-area(s) of the selected area.
4. More the cursor to one of the thumbnail, and then click the appeared **Set Visual Tracking** to open visual tracking setting page.
5. **Optional:** Click **Refresh** to get the latest view of the camera.
6. Click **Add Related Camera** to open the camera list panel, and select a camera from the camera list or search for a specific camera by keywords, and then click **OK**.

   The icon representing the related camera will be displayed on the view of the current camera. And the thumbnail of the view of the related camera will be listed on the right side.

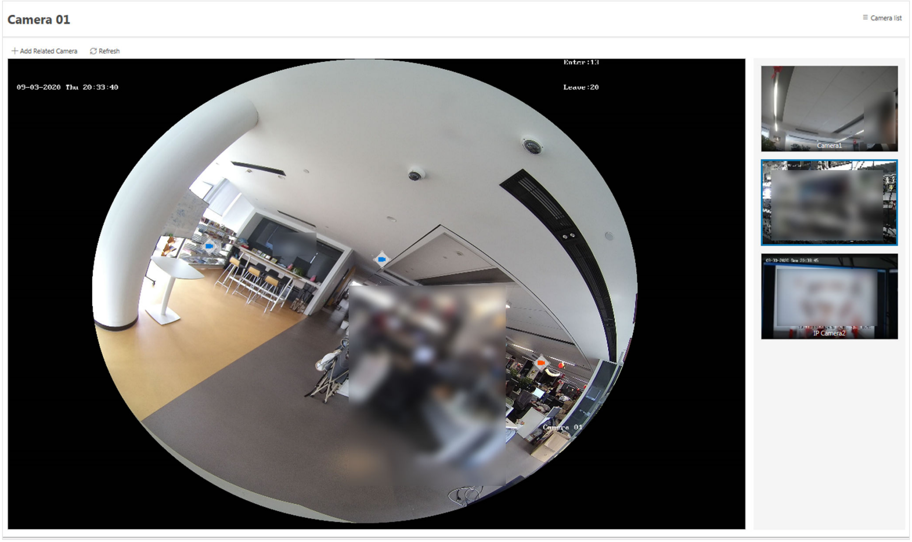


Figure 14-12 Set Visual Tracking

7. Drag the icon to a proper position on the view according to its actual mounting position.
8. Click **Save**.

   The security personnel will be able to use the video tracking function on the Control Client.
9. **Optional:** Perform the following operations if required.

   Cancel Association
   Hover the cursor over the thumbnail list on the right side, and then click **Delete** to cancel the association between the camera and the current camera.

   Set Visual Tracking for Related Camera
   Hover the cursor over the thumbnail list on the right side, and then click **Set Visual Tracking** to set visual tracking for the related camera.

Example

Visual Tracking in Hallway

The following picture shows the surveillance image of camera A in a hallway. There are three directions: B, C, and D, and each direction is monitored by camera B, C, and D respectively.

In this case, you can drag camera B to the B position so as to overlay the icon of camera B on the surveillance image, and then do similar operations for camera C and camera D. After that, when an individual passes by the hallway and turns to direction B, the security personnel can click the icon of camera B on the view of camera A to redirect to the view of camera B.

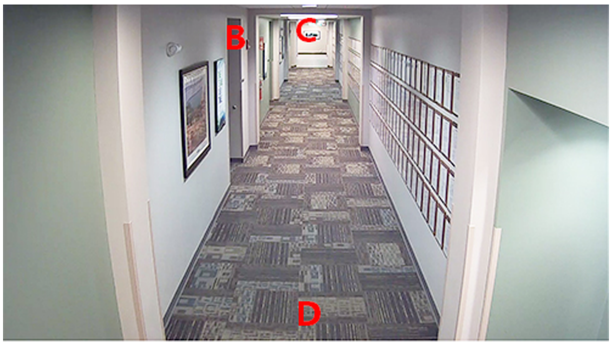


Figure 14-13 Surveillance Image of Camera A

14.5 Set Network Parameters

You can set parameters for registering the platform without Remote Site Management module (or Remote Site) to the Central System, set access mode for encoding and decoding devices, and set the waiting time for the configurations.

Steps

1. In the top left corner of the Home page, select ≡ → **All Modules** → **Video** → **Video Settings** → **Network** .
2. Set network parameters.

   Register to Central System

   Switch on **Register to Central System** and enter the IP address and port No. of Central System to allow the system without Remote Site Management module (as we called Remote Site) to be registered to the Central System. Central System is the system that has Remote Site Management module and can group multiple Remote Sites together to form a larger-scale union. The purpose of grouping Central System and Remote Sites is to allow Central System's users to view and manage resources belonging to multiple Remote Sites simultaneously as if they were on the same system.

   Note

   - Before registering to the Central System, make sure you have enabled the Central System to receive the site registration. Refer to the parameter **Receive Site Registration** for details.
   - Registering to Central System is only available for the system without Remote Site Management module.
   - Open Service Manager (installed on the PC running central system's SYS service), and click **HikCentral Professional System Management Service** if you need to view or edit the Central System's port.

   Receive Site Registration

Check the **Receive Site Registration** to allow the system with Remote Site Management module (or Central System) to receive the registration from Remote Sites. Remote Site is the system that does not have Remote Site Management module and can register to Central System to form a larger-scale union. The purpose of joining Central System and Remote Sites is to allow Central System's users to view and manage resources belonging to multiple Remote Sites simultaneously as if they were on the same system.

Note

- If a remote site needs to register to the Central System, it should open the Remote Site's Web Client and enter **Register to Central System** to configure the Central System's parameters. See ***Set Network Parameters*** for details.
- Allowing remote site registration is only available for the system with Remote Site Management module.

Device Access Mode

Set the device access mode as Automatically Judge or Proxy mode to define how the system accesses all the added encoding devices and decoding devices.

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.

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 there is no response within the configured timeout time.

The minimum default waiting time of the interactions between the configurations and SYS server is 60s, the minimum time between SYS 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 SYS server.

Note

The two parameters **Register to Central System** and **Receive Site Registration** are not available at the same time.

3. Click **Save**.

14.6 Configure Panorama Tracking

Panorama tracking is a target tracking function based on the linkage between a bullet/box camera and a speed dome. After you configure panorama tracking on the Web Client, the security personnel will be allowed to enable this function during the live view of the bullet/box camera on the Control Client. If this function is enabled, when a Video Content Analysis (VCA) event is detected by the bullet/box camera, or the security personnel manually select a target, the bullet/box camera will work together with the speed dome to locate, zoom in, and track the target.

Before You Start

Make sure you have added the device supporting this function.

Steps

1. In the top left corner of the Home page, select ≡ → **All Modules** → **Panorama Tracking Settings** .
2. Select one area on the area list.
3. In the Basic Information, click **Panorama Tracking** to open the Panorama Tracking Settings window.
4. Select a speed dome from the list for linking the camera to the speed dome.
5. Select **Manual Calibrating** or **Auto Calibrating** as calibration mode and click **Next**.
6. Calibrate the camera and the linked speed dome, and then click **Next**.
   - **Manual Calibrating**: In Manual Calibrating mode, click **Add Calibration Point**, and click the position on the left image of box/bullet camera to add a calibration point. Select the calibration point, and then pan, tilt, and zoom in or out the view of speed dome by digital zoom and PTZ control to make sure the live view of speed dome and the target position of the camera are mostly same.

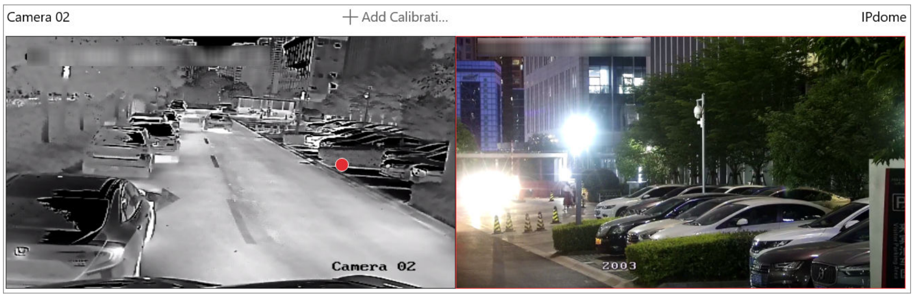


Figure 14-14 Manual Calibrating

Note

- You can repeat the operations to add more calibration points. At least 4 calibration points should be added. It is recommended to add at least 9 calibration points in one scene. For higher tracking precision, up to 12 calibration points are required.
- Click the added calibration point, and you can move it to other position, or delete it.
- It is recommended to place calibration points at distinct positions in live image (for example, corners). If no distinct position is available, you can place the points at something (for example, box, stool, or people) to mark the position.

- **Auto Calibrating**: In Auto Calibrating mode, click **Start Calibration** to add calibration points automatically.

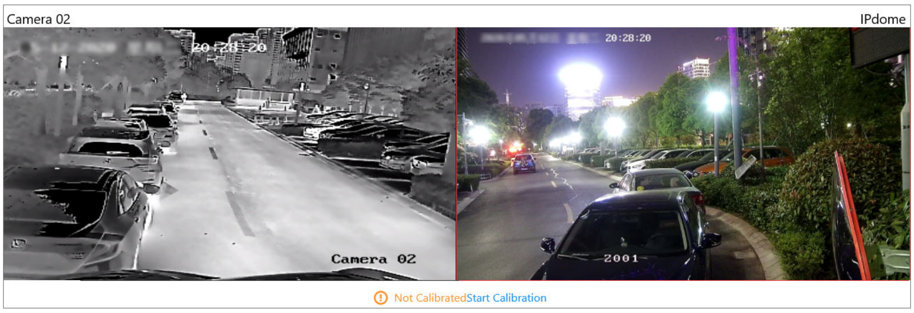


Figure 14-15 Auto Calibrating

Note

You should avoid using auto calibrating for vast similar scenes (for example, lake, lawn, or public square) or dark scenes (for example, night scenes).

7. Set other parameters.

Auto-Tracking

If **Auto-Tracking** is checked, when the VCA event is triggered during live view, the speed dome will track the target automatically.

Note

You need to configure VCA rule for the bullet/box camera on the device. For more details, refer to the user manual of the device.

Target Tracking Mode

Track One Target Continuous

The speed dome tracks the target continuously until the target disappears in the scene.

Track One Target for Certain Duration

Select this mode and set the duration of tracking. The speed dome switches to next target after the set duration time.

Set Tracking Initial Position

Select a preset as tracking initial position, or adjust the view by PTZ control and click **Save** to save the preset as tracking initial position. When tracking finishes or timed out, speed dome returns to the tracking initial position. When tracking initial position is not set, the speed dome stays where tracking finishes or timed out.

8. Click **Save and Test** to finish configuring panorama tracking.

   To test the panorama tracking settings, click or draw a rectangle on the video of box/bullet camera, and the speed dome will show the close-up view.

9. **Optional:** After configuring panorama tracking, perform the following operations.

Edit Panorama Tracking Settings	Click **Edit** to reconfigure panorama tracking.
Cancel Panorama Tracking	Click **Cancel Panorama Tracking** to delete all configurations about panorama tracking.

14.7 Intelligent Recognition

Intelligent recognition refers to the recognition and analysis of human face, body features, behaviors, vehicles in video images based on intelligent algorithms. The platform will record each recognition and the records can be searched via the Control Client and Mobile Client. The functionality is useful in various scenarios across industries for purposes such as searching for fugitive and finding out security threat.

14.7.1 Manage Face Comparison Group

HikCentral Professional supports face recognition and comparison functions. After adding devices which support face recognition, the devices can recognize faces and compare with the persons in the system.

On the Web Client, after adding the persons to the person group, the administrator 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, the administrator should 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.

Add Face Comparison Group

You need to add a face comparison group and add person(s) to the group for face comparison for further configurations such as intelligent recognition task settings.

Steps

Note

For details about intelligent recognition task settings, see ***Manage Intelligent Recognition Task*** .

1. In the top left corner of the Home page, select ≡ → **All Modules → Video → Intelligent Recognition → Face Comparison Group** .
2. Click + to open the Add Face Comparison Group panel.
3. Create a name for the face comparison group.
4. **Optional:** Enter a description about the face comparison group.
5. Click **Add**.

   The face comparison group will be displayed in the group list.
6. **Optional:** Select a group from the group list and then click 🗑 to delete the group.
7. Click **Add → Add New Person** or **Add → Add Existing Person** to add person(s) to the group.

   Add New Person Select the group from the group list, and then click **Add → Add New Person** to enter the Add New Person page, and then enter the required person information including ID, first name, and last name, and then click **Add** or **Add and Continue** to add the person to the group.

   Add Existing Person Select the group from the group list, and then click **Add → Add Existing Person** to open the person list window, and then search for person(s) or select person(s) from the person list, and then click **Add**.

   Note

   You can check **Include Sub-Group** to include the persons in sub-groups to the persons available for your selection.

   The added person(s) will be displayed in the person list of the group.
8. Enter the required person information such as ID, first name, and last name.
9. Add face picture if the profile photo field is empty.
   - Add from Device: Hover the cursor onto the empty profile photo field, click **Add from Device**, and then select a device.
   - Add by Taking a Picture: Hover the cursor onto the empty profile photo field, and then click **Take a Photo** to take a photo.
   - Add by Uploading Picture: Hover the cursor onto the empty profile photo field, and then click **Upload Picture** to upload a face picture from the local PC.
10. **Optional:** Delete person(s) added to a group.

    Delete Specific Person(s) Select a group from the group list, and then select specific added person(s), and then click **Delete** to delete them.

    Delete All Persons Select a group from the group list, and then hover the cursor over ⌄ and click **Delete All** to delete all persons from the group.
11. **Optional:** Perform one or more of the following operations.

Manage Persons in Face Comparison Group

Click the added face comparison group and the persons in this group will be displayed on the right.

You can add more persons into this group, or perform other operations such as importing and exporting persons. For details, refer to ***Manage Person*** .

Edit Face Comparison Group

Click ✎ in the Operation column to edit its details and edit the cameras that it is applied to.

Export All Face Information in a Group

a. Click **Export** to open the password settings window.
b. Create a password for decompressing the exported file, and then confirm it.

Delete Face Comparison Group

Select one face comparison group and click 🗑 to delete it.

Delete All Face Comparison Groups

Click **Delete All** to delete all the added face comparison groups.

Import Face Comparison Group from Device

You can import face picture libraries from an encoding device to the platform as face comparison groups. After you importing the face picture libraries, the face information contained in them will also be imported.

Steps

1. In the top left corner of the Home page, select ≡ → **All Modules** → **Video** → **Intelligent Recognition** → **Face Comparison Group** .
2. Click ⇤ to open the Import Face Comparison Group from Device panel.
3. Select **Encoding Device** from the Device Type field.

   The available device(s) will be displayed.
4. Click › to show the face comparison group(s) of a device.
5. Select face comparison group(s), and the click **Import**.

   The Import Face Comparison Group window pops up, displaying the import results.

   Note

   If a face picture library fails to be imported, you can view the failure details such as library name, device name, and the failure reason.

Import Zipped Profile Photos

You can batch import profile photos zipped in an archive file.

Before You Start

Make sure you have named the to-be-imported profile photos in this rule: "First Name + Last Name" or "First Name + Last Name_ID" (e.g., David Lennon or David Lennon_777816547).

Steps

Note

The platform only supports importing photos in the format of JPG, JPEG, or PNG.

1. In the top left corner of the Home page, select ≡ → **All Modules** → **Video** → **Intelligent Recognition** → **Face Comparison Group** .
2. Select a face comparison group from the group list.
3. Hover the cursor over **Import**, and then click **Import Zipped Profile Photo** to open the Import Zipped Profile Photo panel.
4. Click ··· to select a ZIP file from the local PC.
5. Click **Import**.

Import Person Information by Template

HikCentral Professional provides a template (an XLSX file) for batch importing person information from the local PC. You can use the template to import large amount of person information to a specific face comparison group with minimum efforts.

Steps

1. In the top left of the Home page, select ≡ → **All Modules** → **Video** → **Intelligent Recognition** → **Face Comparison Group** .
2. Select the face comparison group that needs importing person information.
3. Click **Import** → **Import by Template** to open the Import by Template panel.
4. Click **Download Template** in the panel to download the template.
5. Fill required information in to the template, and then click ··· to select the filled-in template from the local PC.
6. **Optional:** Check **Replace Repeated Person** to allow the system to overwrite the person information already exists in the face comparison group when you import the information.
7. Click **Import**.

Import Face Information from Enrollment Station

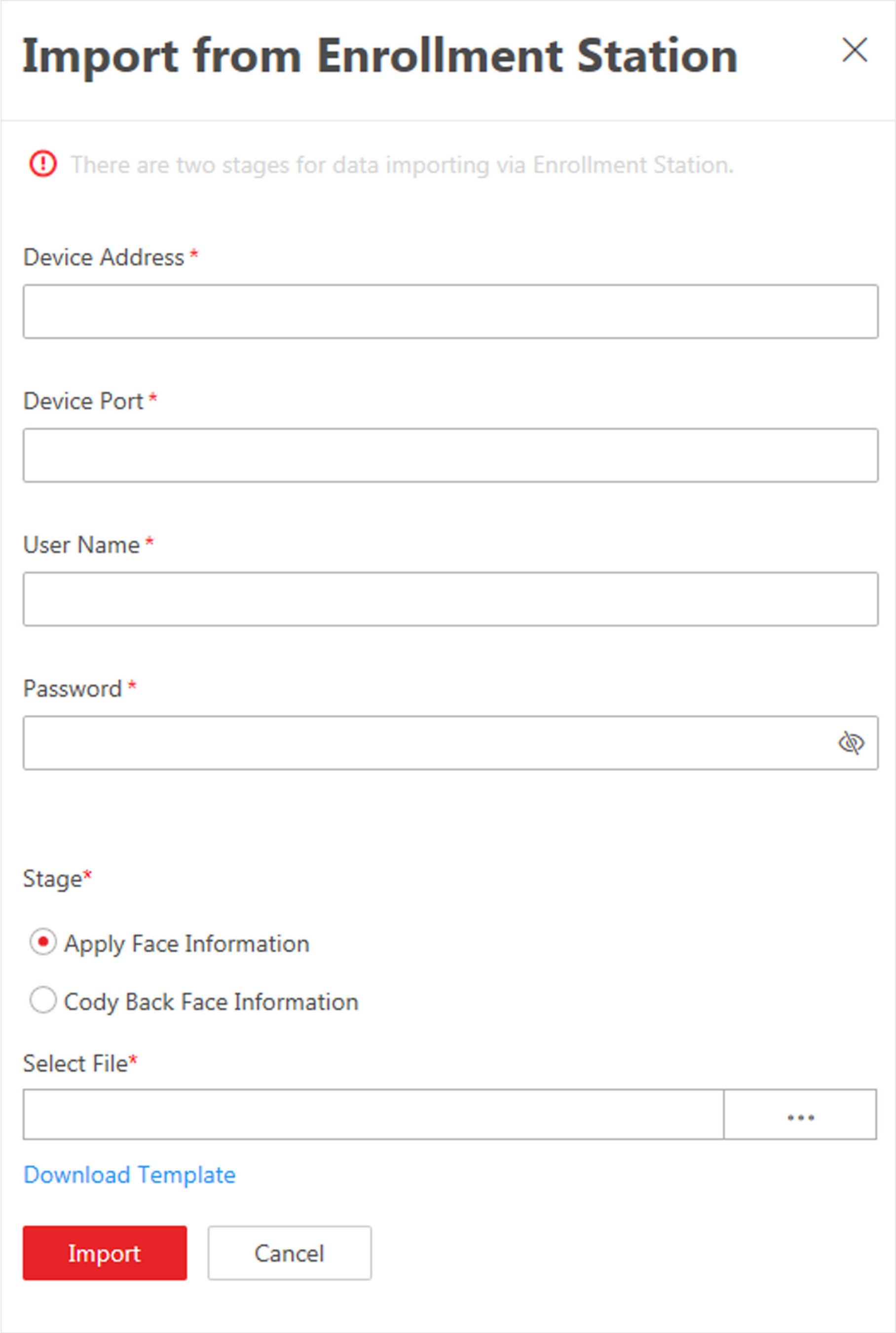
You can import face information from an enrollment station if you know its IP address, device port, user name, and password.

Before You Start

Make sure you have added the enrollment station to the platform.

Steps

1. In the top left corner of the Home page, select ≡ → **All Modules** → **Video** → **Intelligent Recognition** → **Face Comparison Group**
2. Select a face comparison group.
3. Click **Import** → **Import from Enrollment Station** to open the Import from Enrollment Station panel.



Import from Enrollment Station

There are two stages for data importing via Enrollment Station.

Device Address *

Device Port *

User Name *

Password *

Stage*

● Apply Face Information

○ Cody Back Face Information

Select File*

Figure 14-16 Import from Enrollment Station

4. Set the required information, such as device IP address, device port, and password.

   Stage

   Apply Face Information

   Import specific face information from the enrollment station to the face comparison group.

   Select File

   Click **Download Template** to download a template and fill in it according to its prompts, and then click ··· and select the filled-in template to import specific face information from the enrollment station to the selected face comparison group.

   Copy Back Face Information

   Copy back all the face information acquired by the enrollment station to the selected face comparison group.

5. Click **Import**.

14.7.2 Manage Intelligent Recognition Task

You can add an intelligent recognition task to define the conditions such as the device and time for intelligent recognition. The task types include facial comparison, people feature analysis, frequently appeared person analysis, rarely appeared person analysis, and behavior analysis.

Add Face Comparison Task

You can add face comparison task to define the time, device, face comparison group, similarity threshold, and so on, for face comparison. Once a face comparison task is added, the security personnel can view real-time matched face information during live view and search face comparison records via the Control Client and Mobile Client.

Before You Start

Make sure you have set face comparison groups. For details, see ***Manage Face Comparison Group*** .

Steps

1. In the top left of the Home page, select ≡ → **All Modules → Video → Intelligent Recognition → Intelligent Recognition Task → Face Comparison** .
2. Click **Add** to enter the Add Face Comparison Task page.
3. Set parameters, such as task name, description, and task schedule template.

   Note

   The parameter marked with a red asterisk is required.

   Task Schedule Template

Select a task schedule template from the drop-down list to define the time when the face comparison functionality is activated.

You can click **View** to view the details of the scheduled time.

Note

For details about adding task schedule template, see ***Add Task Schedule Template*** .

Device for Analysis

Select a type of face comparison device.

Camera

Select camera(s) from the Available list, and then click > to add selected one(s) to the Selected list.

Face Comparison Group

Select face comparison group(s). The faces detected by the specified camera(s) will be compared with the face pictures in the selected group(s).

Similarity

Drag the slider to adjust the similarity threshold based on your face comparison requirements. The higher the threshold, the preciser the comparison will be. The lower the threshold, the higher comparison rate will be.

Once the similarity between a detected face and a face picture in the selected face comparison group(s) reaches the threshold, the detected face will be recognized and a face comparison record will be generated.

4. Complete adding this task.
   - Click **Add** to complete adding this task.
   - Click **Add and Continue** to complete adding this task and continue adding more.

   The face information in the selected face comparison group(s) will be applied to the selected camera(s).
5. **Optional:** Perform the following operations after adding task(s).

Delete a Task	Select a task from the task list, and then click **Delete**.
Delete All Tasks	Click ⌄ next to **Delete**, and then click **Delete All**.
Filter Tasks	Click ▽ and set filter conditions such as task name, and then click **Filter**.

Add People Feature Analysis Task

You can add a people feature analysis task to define conditions such as time, device(s), and detection area, for people feature analysis, which recognizes and records body features of the people appeared in the fields of view of the cameras linked to the people feature analysis device. Once a people feature analysis task is added, the security personnel can search and view people feature analysis records via the Control Client and Mobile Client.

Steps

1. In the top left of the Home page, select ≡ → **All Modules → Video → Intelligent Recognition → Intelligent Recognition Task → People Feature Analysis** .
2. Click **Add** to enter the Add People Feature Analysis Task page.
3. Set parameters, such as task name, description, and task schedule template.

   Note

   The parameter marked with a red asterisk is required.

   Task Schedule Template

   Select a task schedule template from the drop-down list to define the time when the people feature analysis functionality is activated.

   You can click **View** to view details of the scheduled time.

   Note

   For details about adding task schedule template, see ***Add Task Schedule Template*** .

   Device for Analysis

   Select a type of people feature analysis device for the execution of people feature analysis.

   Camera

   Select cameras for detecting persons.

   Detection Area

   Click **Draw Area** and the drag the cursor on the image to draw an area for detecting persons.
4. Complete adding the task.
   - Click **Add** to complete adding this task.
   - Click **Add and Continue** to complete adding this task and continue adding more.
5. **Optional:** Perform the following operations after adding task(s).

Delete a Task	Select a task from the task list, and then click **Delete**.
Delete All Tasks	Click ∨ next to **Delete**, and then click **Delete All**.
Filter Tasks	Click ▽ and set filter conditions such as task name, and then click **Filter**.

Add Frequently Appeared Person Analysis Task

You can add a frequently appeared person analysis task to define the time, device(s), appeared times threshold, and so on, for frequently appeared person analysis, which searches out the frequently appeared person in a specific area within a specific period. The function is useful for finding out persons who should not have appeared frequently in a specific area. For example, it can be used in a jewelry store for detecting persons who may commit robbery.

Before You Start

Make sure you have set facial comparison groups. For details, see ***Manage Face Comparison Group*** .

Steps

1. In the top left of the Home page, select ≡ → **All Modules** → **Video** → **Intelligent Recognition** → **Intelligent Recognition Task** → **Frequently Appeared Person Analysis** .
2. Click **Add** to enter the Add Frequently Appeared Person Analysis Task page.
3. Set parameters, such as task name, description, and task schedule template.

Note

The parameter marked with a red asterisk is required.

Task Schedule Template

Select a task schedule template from the drop-down list to define the time when frequently appeared person analysis is activated.

You can click **View** to view detailed scheduled time.

Note

For details about adding task schedule template, see ***Add Task Schedule Template*** .

Device for Analysis

Select the device type for frequently appeared person analysis.

Camera

Select camera(s) for detecting persons.

Face Comparison Group

Select face comparison group(s). The faces detected by the specified camera(s) will be compared with the face pictures in the selected group(s).

Time Period

Set a time period for counting the appearance times of a detected person.

Appeared Times

Set threshold times for regarding a detected person as a frequently appeared person.

If the times that a person is detected by the specified camera(s) reaches or exceeds the threshold within the time period you set, he/she will be regarded as a frequently appeared person.

Counting Interval

Set a time interval for filtering out invalid counting.

If a person is detected for multiple times within the time interval, the system will regard he/she only appeared for one time.

Similarity

Drag the slider to adjust the similarity threshold based on your facial recognition requirements. The higher the threshold, the preciser the recognition will be. The lower the threshold, the higher recognition rate will be.

Once the similarity between a detected face and a face picture in the selected face comparison group(s) reaches the threshold, the detected face will be recognized and a face comparison record will be generated.

4. Complete adding this task.
   - Click **Add** to complete adding this task.
   - Click **Add and Continue** to complete adding this task and continue adding more.
5. **Optional:** Perform the following operations after adding task(s).

Delete a Task	Select a task from the task list, and then click **Delete**.
Delete All Tasks	Click ⌄ next to **Delete**, and then click **Delete All**.
Filter Tasks	Click ▽ and set filter conditions such as task name, and then click **Filter**.

Add Rarely Appeared Person Analysis Task

You can add a rarely appeared person analysis task to define the time, device(s), appeared times threshold, and so on, for searching out the rarely appeared person in a specific area within a specific period. Rarely appeared person analysis is useful for finding out specific persons who shall appear regularly in a specific area. For example, in a community where many senile people live alone, when a senile person rarely leaves home (i.e., rarely been detected by the cameras in the community), he/she may need living assistance due to health problems.

Before You Start

Make sure you have set facial comparison groups. For details, see ***Manage Face Comparison Group*** .

Steps

1. In the top left of the Home page, select ≡ → **All Modules** → **Video** → **Intelligent Recognition** → **Intelligent Recognition Task** → **Rarely Appeared Person Analysis**
2. Click **Add**to enter the Rarely Appeared Person Analysis Task page.
3. Set related information, such as task name, description, and task schedule template.

Note

The information marked with a red asterisk is required.

Task Schedule Template

Select a task schedule template from the drop-down list to define the time when rarely appeared person analysis is activated.

You can click **View** to view detailed scheduled time.

Note

For details about adding task schedule template, see ***Add Task Schedule Template*** .

Device for Analysis

Select the device type for rarely appeared person analysis.

Camera

Select camera(s) for detecting persons.

Face Comparison Group

Select face comparison group(s). The faces detected by the specified camera(s) will be compared with the face pictures in the selected group(s).

Time Period

Set a time period for counting the appearance times of a detected person.

Reporting Time

The time when the results of rarely appeared person analysis is reported to system each day.

Appeared Times

Set threshold times for regarding a detected person as a frequently appeared person.

If the times that a person is detected by the specified camera(s) is not larger than the threshold within the time period you set, he/she will be regarded as a rarely appeared person.

Counting Interval

Set a time interval for filtering out invalid counting.

If a person is detected for multiple times within the time interval, the system will regard he/she only appeared for one time.

Similarity

Drag the slider to adjust the similarity threshold based on your facial recognition requirements. The higher the threshold, the preciser the recognition will be.

Once the similarity between a detected face and a face picture in the selected face comparison group(s) reaches the threshold, the detected face will be recognized and a face comparison record will be generated.

4. Complete adding this task.
   - Click **Add** to complete adding this task.
   - Click **Add and Continue** to complete adding this task and continue adding more.
5. **Optional:** Perform the following operations after adding task(s).

Delete a Task	Select a task from the task list, and then click **Delete**.
Delete All Tasks	Click ⌄ next to **Delete**, and then click **Delete All**.
Filter Tasks	Click ▽ and set filter conditions such as task name, and then click **Filter**.

Add Behavior Analysis Task

Behavior analysis refers to the analysis of behaviors of people, vehicle, and other objects for purposes such as finding out security threat. The available behavior analysis types include perimeter protection (e.g., intrusion detection), street behavior analysis, prisoner behavior analysis, and people density analysis. You can add a behavior analysis task to define conditions such as time, device, and detection area for behavior analysis. Once a behavior analysis task is added, the specified device will perform behavior analysis in the specified detection area during the specified periods.

Before You Start

Make sure you have added behavior analysis server to the system. For details, see ***Add DeepinMind Server*** for details.

Steps

1. In the top left of the Home page, select ≡ → **All Modules** → **Video** → **Intelligent Recognition** → **Intelligent Recognition Task** → **Behavior Analysis** .
2. Click **Add** to enter the Add Behavior Analysis Task page.
3. Set parameters, such as task name, description, and task schedule template.

Note

- The parameter marked with a red asterisk is required.
- The parameters vary with different behavior types. Here we only introduce part of the parameters. For details about the settings of each type of behavior analysis, see the user manual of the device.

Behavior Type

Select a behavior type.

The behavior types are categorized into different groups based on their usage scenarios, including people density analysis, perimeter protection, prison behavior, and street behavior.

Task Schedule Template

Select a task schedule template from the drop-down list to define the time when behavior analysis is activated.

Device for Analysis

Select a device for behavior analysis.

Camera

Select camera(s) for detecting behaviors.

Detection Area

Draw an area or line for behavior analysis.

Take line crossing detection for an example, you need to click **Draw Detection Line** to draw a line on the image, and then set the following two parameters.

Change Line Crossing Direction

Set the crossing direction to determine whether line crossing detection is triggered. For example, if you select **Bidirectional**, when a person crosses the line, no matter what direction the person crosses, line crossing detection will be triggered.

4. Complete adding this task.
   - Click **Add** to complete adding this task.
   - Click **Add and Continue** to complete adding this task and continue adding more.
5. **Optional:** Perform the following operations after adding task(s).

Delete a Task	Select a task from the task list, and then click **Delete**.
Delete All Tasks	Click ⌄ next to **Delete**, and then click **Delete All**.
Filter Tasks	Click ▽ and set filter conditions such as task name, and then click **Filter**.

14.7.3 Applying Center

In Applying Center, you can apply the face comparison group settings to the face recognition cameras to make the these settings take effect on the cameras. You can also view the cameras that fail to receive the settings and the face information that fails to be applied to the cameras, and then apply the face information again.

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 device which supports face 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 platform will automatically apply the data in the group to the device to take effect.

Before You Start

- Make sure you have added devices which supports face picture comparison to the system.
- Make sure your license supports facial recognition functionality. Or turn to Home page, select **Maintenance and Management → License Details →** > , and then click **Configuration** next to Facial Recognition Camera to added cameras as facial recognition cameras. Otherwise, facial recognition will be unavailable in the system.

Steps

Note

- You can only apply face comparison groups to cameras which support face picture comparison.
- The maximum number of groups that can be applied to the camera depends on the camera capability.

1. In the top left of the Home page, select ≡ → **All Modules** → **Video** → **Intelligent Recognition** .
2. Select a facial comparison group from the group list on the left side.
3. Click **Face to Be Applied** to display the to-be-applied face information of the selected group.
4. Apply face information to device(s).
   - Apply Specific Face Information: Select face information, and then click **Apply**.
   - Apply All Face Information in the Group: Click **Apply All**.
5. Select the camera(s) to apply the selected face comparison group(s) to.
6. Click **Apply** to start applying.

View Applying Status

You can view the status of the applying of face comparison groups from different perspectives, including the cameras failed to receive face comparison group, the cameras to which certain face comparison groups need to be applied, the person information failed to be applied, and the person information to be applied.

In the top left of the Home page, select ≡ → **All Modules** → **Video** → **Intelligent Recognition** → **Applying Center** .

Cameras Failing to Receive Faces

Select a device from the device list on the left side, and then click a camera on the camera list to view the details of applying failure, including face comparison group, analysis device, and exception details (e.g., the device reaches its maximum face comparison group capacity, the face comparison group reaches its maximum face picture capacity, face pictures not qualified, etc.) If face pictures are not qualified, you can click 🗎 to view failure details.
You can also view network status of the listed camera(s). To ensure the success of the applying of face information to these camera(s), make sure they are online.

Cameras to Be Applied To

Select a device from the device list on the left side, and then click a camera on the camera list to view the details of the applying of face comparison groups: the applying status of each face comparison group that need to be applied to the camera will be list.
You can also view network status of the listed camera(s). To ensure the success of the applying of face information to these camera(s), make sure they are online.

Faces Failing to Be Applied

Select a person group from the person group list on the left side to view the face information that fails to be applied to devices, and then click a piece of face information to view its exception details.

Faces to Be Applied

Select a person group from the person group list on the left side, and then the faces to be applied will be displayed on the right side.

Apply Abnormal Applying Record Again

Applying of face information may fail due to various reasons. To ensure recognition of the target persons in your scenarios, it is important to check the abnormal applying records and apply the face information again.

Steps

1. In the top left of the Home page, select ≡ → **All Modules → Video → Intelligent Recognition → Applying Center** .
2. Apply abnormal face applying records again.
   - Click **Cameras Failing to Receive Faces**, select an area from the area list in the left side, and then click **Apply All** to apply face information to all the listed camera(s) again.
   - Click **Cameras to Be Applied To**, select an area from the area list in the left side, and then click **Apply All** to apply face information to all the listed camera(s) again
   - Click **Face Failed to Be Applied**, select a person group from the person group list in the left side, and then select face information and then click **Apply** to apply the select face information again, or click **Apply All** to apply all face information again.
   - Click **Faces to Be Applied**, select a person group from the person group list in the left side, and then select face information and then click **Apply** to apply the select face information again, or click **Apply All** to apply all face information again.

14.7.4 Add Task Schedule Template

A task schedule template is used for defining the weekly time arrangement for an intelligent recognition task. An all-day template is available by default. If you apply the all-day template to an intelligent recognition task, the task will be activated 24*7 hours. If the all-day template cannot meet your demands, you can add a custom template as required.

Perform the following operations to add a custom template.

Steps

1. In the top left of the Home page, select ≡ → **All Modules → Video → Intelligent Recognition → Task Schedule Template** .
2. Click + to add a schedule template.
3. Create a name for the template.
4. **Optional:** Select an existing template from the **Copy to** drop-down list.
5. Edit weekly schedule.

Draw Task Time
Click **Draw Task Time** and then click a grid or drag the cursor on the time line to draw a time period during which the task is activated.

Set Precise Time
Click **Draw Task Time**, move the cursor to a drawn period, and then adjust the period in the pop-up dialog shown as .

04 : 00 — 04 : 30

Erase Task Time	Click **Erase**, and then click a grid or drag the cursor on the time line to erase the drawn time period.

6. Click **Add**.
7. **Optional:** Select a task from the task list, and then click 🗑 to delete it.

14.8 Dock Station

The dock station is a data collector which can automatically detect and back up law-enforcement data from body camera(s) connected to it. The dock station can also be used to charge the body cameras.

After adding dock stations to the system, you can search the data (video footage, pictures, and audio files) backed up on the dock stations and download the data via the Control Client for convenient management. You can also monitor the online status of the dock stations, and perform other operations such as playing video footage backed up on the dock stations.

Note

- For more details about dock station, see the user manual of the device.
- For details about searching video footage of the dock stations, see the *User Manual of HikCentral Professional Control Client*.

14.8.1 Add Dock Station Group

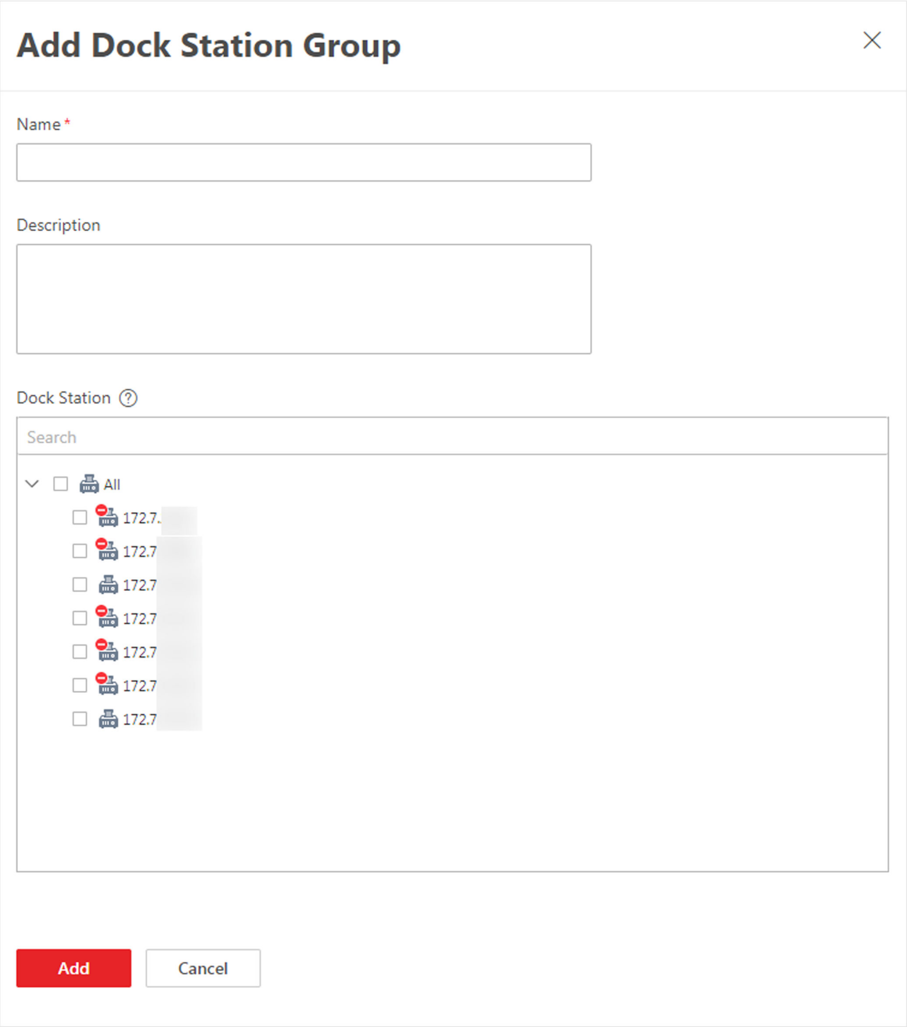
Dock station group is a group of persons who are linked to the same dock station(s). After linking persons to dock station(s), the videos and pictures on the persons' body cameras can be copied to these dock station(s).

Steps

Note

Up to 64 dock station groups can be added.

1. In the top left corner of the Home page, select ≡ → **All Modules** → **Video** → **Dock Station** .
2. Click + to open Add Dock Station Group panel.



Add Dock Station Group

Name *

Description

Dock Station

Search

□ All

□ 172.7. [redacted]

□ 172.7

□ 172.7

□ 172.7

□ 172.7

□ 172.7

□ 172.7

Figure 14-17 Add Dock Station Group

3. Set the basic information.

   Name

   Create a name for the dock station group.

   Description

   Enter the descriptive information for the group. E.g., This dock station group is for security guards in Team A.

   Dock Station

   Select dock station(s).

4. Click **Add**.

   The dock station will be displayed in the dock station list.

5. **Optional:** Click ✎ to edit the dock station group.
6. Add person(s) to the dock station group.

Note

Up to 20 persons can be added to one dock station group.

1) Click **Add** to open the Add Person/Person Group window.
2) Select a person group from the person group list in the window.
3) Select specific person(s) or check **Select All** to select all persons in the group.
4) Click **Add**.

   The person(s) will be displayed in the person list.
5) **Optional:** Select person(s) from the person list, and then click delete to delete the selected person(s). Or hover the cursor onto ⌄ next to **Delete**, and then click the pop-up **Delete All** to delete all persons in the group.

14.9 Video Application

The HikCentral Professional provides functionality of live view, playback, and local configuration through web browser.

Note

- If the SYS's transfer protocol is HTTPS, the Video Application module (including Live View, Playback, and Local Configuration) is available only when accessing the Web Client via Internet Explorer.
- If the SYS's transfer protocol is HTTP, the Live View and Playback modules are available for Internet Explorer, Google Chrome, Firefox, and Safari 11 and above. But Local Configuration module is available for Internet Explorer only.

14.9.1 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.

Start Live View

After adding cameras into areas, you can use live view to play the live footage of cameras and perform basic operations via the Web Client.

Before You Start

- Make sure you have added cameras to areas. For details, refer to ***Add Camera to Area for Current Site*** .
- If the system is Central System with Remote Site Management module, you can also view the live image of the cameras imported from remote sites. For managing remote site's cameras, refer to ***Add Camera to Area for Remote Site*** .

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **Video** → **Video Application** .
2. Click **Live View** on the left.
3. **Optional:** If you have added remote site to the platform, select a site from the drop-down list to show the area and cameras in the site.
4. **Optional:** Move the cursor to a camera to see the live view thumbnail.

Note

To search a camera or area, enter a keyword of camera name or area name in the search field and search.

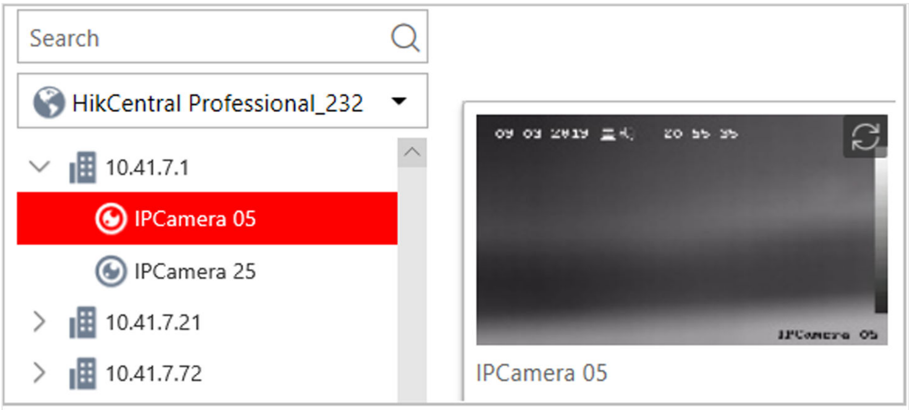


Figure 14-18 Thumbnail

5. Do one of the following to start live view.
   - To start the live view of a camera, drag the camera to a display window or select a display window and then double-click the camera.
   - To start the live view of all cameras in an area, drag the area to any display window or double-click the area. Window division will automatically adapt to the number of cameras in the area.
6. **Optional:** To change window division mode, click ⊞ on the live view toolbar at the bottom and select a mode.
7. **Optional:** Move the cursor over the display window during live view to show the camera toolbar. You can perform basic operations to cameras, such as digital zoom, instant playback, two-way audio, fisheye dewarping, and PTZ control, etc.

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.

Note

The PTZ control function should be supported by the camera.

In the live video display window, you can also click the icon to enable window PTZ control. Move the cursor to the direction you desired and click on the image to pan or tilt. You can also click and drag the cursor with a white arrows to the direction you desired for a quick direction control.

Configure Preset

A preset is a predefined camera position which contains configurations for pan, tilt, zoom, focus, and other parameters. You can also set a virtual preset after enabling digital zoom.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules → Video → Video Application** .
2. Click **Live View** on the left.
3. Start live view. For details, see ***Start Live View*** .
4. Click in the live view toolbar to open the PTZ control panel.

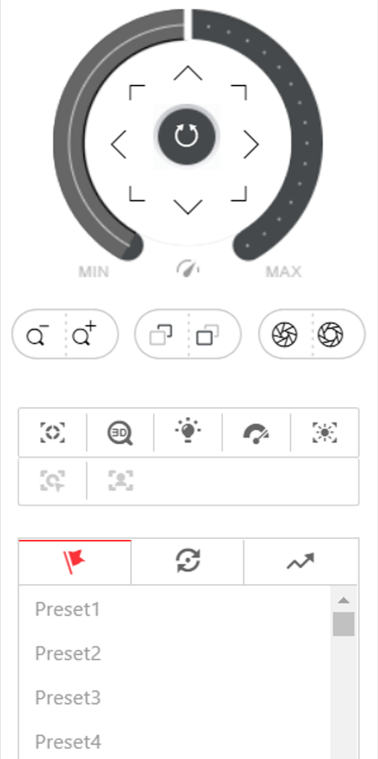


Figure 14-19 PTZ Control Panel

5. Use PTZ control to adjust the camera image to the desired direction and adjust other parameters such as zoom, focus, and iris to optimize the image.
6. Click to show the preset list.
7. Select an unconfigured PTZ preset (gray) in the preset list.
8. Click to create a name for the preset.
9. Click **OK** to save the settings.

Note

Up to 256 presets can be stored.

10. Optional: Perform further operations after configuring presets.

Call Preset Double-click a configured preset, or select the preset and click ▶ to call the preset.

Edit Preset Select a configured preset and click ✎ to edit it.

Delete Preset Select a configured preset 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 programmable scanning speed between adjacent presets and dwell time of each preset.

Before You Start

Add at least two presets for a PTZ camera. For instructions, see ***Configure Preset*** .

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **Video** → **Video Application** .
2. Click **Live View** on the left.
3. Start live view. For details, see ***Start Live View*** .
4. Click 👤 in the live view toolbar to open the PTZ control panel.
5. Click ⟳ to show the patrol list.

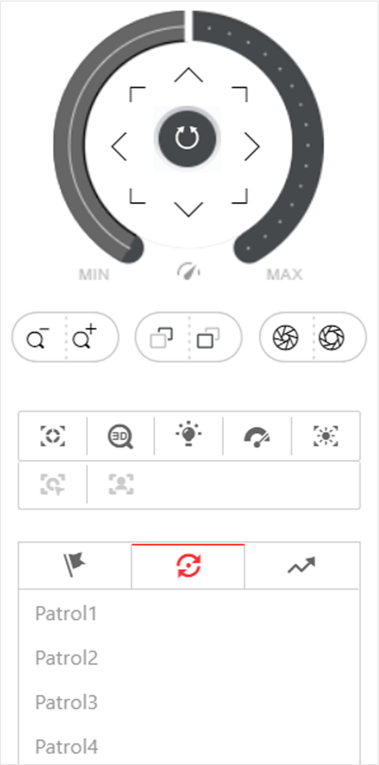
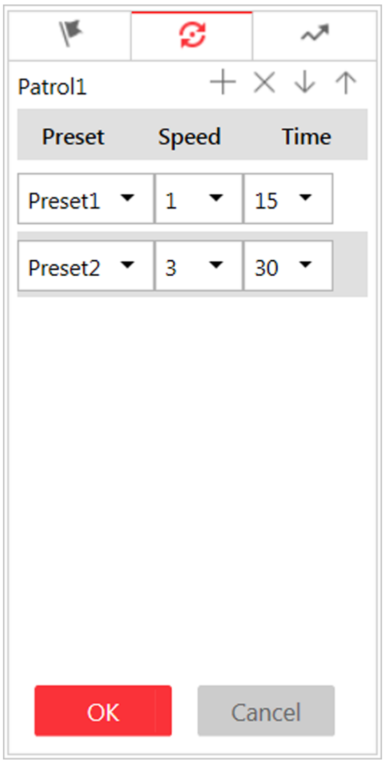


Figure 14-20 Configure Patrol

6. Select a unconfigured patrol (gray) and click ✎ .
7. Click + to add a preset, and set the dwell time and the patrol speed.

Note

- Patrol speed ranges from 1 to 40.
- Preset dwell time ranges from 15 to 30s.



Patrol1

Preset	Speed	Time
Preset1	1	15
Preset2	3	30

Figure 14-21 Add Preset to Patrol

8. Repeat the previous step to add other presets to the patrol.
9. **Optional:** Perform further operations after adding presets.

Remove Preset from Patrol Select an added preset and click ✕ to remove the preset from the patrol.

Adjust Preset Sequence Select an added preset and click ↑ ↓ to adjust the preset sequence.

10. Click **OK** to save the patrol settings.

Note

Up to 8 patrols can be stored.

11. **Optional:** Perform further operations after configuring patrols.

Call Patrol Click ▶ to start the patrol.

Stop Calling Patrol Click ■ to stop the patrol.

Configure Pattern

A pattern is a record of manual manipulation of PTZ movement. You can configure a pattern to record the movement of a camera.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **Video** → **Video Application** .
2. Click **Live View** on the left.
3. Start live view. For details, see ***Start Live View*** .
4. Click in the live view toolbar to open the PTZ control panel.
5. Click to show the pattern list.

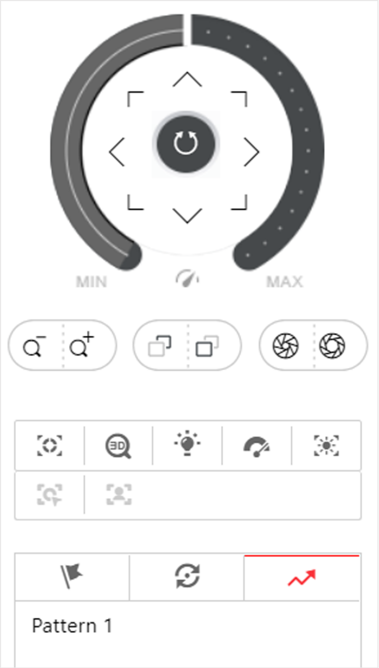


Figure 14-22 Configure Pattern

6. Click to start recording the pattern path.
7. Control the PTZ movement.
8. Click to stop and save the pattern recording.

Note

Only one pattern can be stored. Newly-defined pattern will overwrite the previous pattern.

9. **Optional:** Perform further operations after configuring the pattern.

Call Pattern	Click to start the pattern.
Stop Calling Pattern	Click to stop the pattern.
Delete Pattern	Click ✕ to delete the pattern.

14.9.2 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.

Search Video File

You can search the video footage of cameras and filter the video footage by video type or storage location.

Before You Start

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*** .

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **Video** → **Video Application** .
2. Click **Playback** on the left.
3. In the area and camera list, find the camera that you want to search playback video files.

Note

To search a camera or area, enter the keyword of camera name or area name in the search field and search.

4. **Optional:** To see the live view thumbnail of a camera, move the cursor to the camera.
5. **Optional:** If the camera is configured with auxiliary storage, click the camera and select a location in the Storage Type box below the area and camera list.

Note

For setting storage location for recording, refer to ***Configure Storage and Recording*** .

6. Drag a camera to the display window or double-click the camera to start playback.
7. **Optional:** To search the video footage at an exact time, click the date and time on the playback toolbar to show the calendar panel. Specify a date and time.

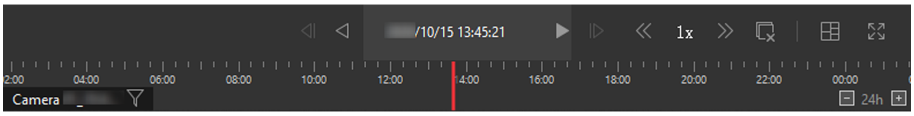


Figure 14-23 Playback Toolbar

Note

- In the calendar panel, dates that have video files are marked with a badge.
- The calendar panel is not available to cameras in remote sites.

8. **Optional:** To filter video files by recording types, click ▽ on the playback toolbar.
9. **Optional:** If the camera is configured with dual-stream recording, select a stream type.
   1) Move the cursor to the display window of the camera to show the camera toolbar.
   2) On the camera toolbar, click or and select a stream type.
10. Play and control the playback video file. For details, see ***Play Video File*** .

Play Video File

After searching video footage, the playback starts. You can control the video playback via timeline. The timeline indicates the duration time of the video footage.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **Video** → **Video Application** .
2. Click **Playback** on the left.
3. Search the video file of a camera. For details, see ***Search Video File*** .

   Playback starts.
4. To control the playback, click the icons on the playback toolbar.

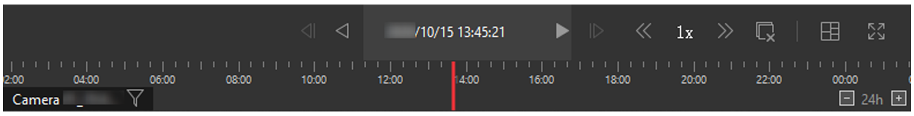


Figure 14-24 Playback Toolbar

5. Click or drag the timeline to play the video footage from a specific time.

   Note

   You can click ⊞ or ⊟ , or use the mouse wheel to scale up or scale down the timeline.
6. **Optional:** Move the cursor to the display window of a camera to show the camera toolbar. Perform further operations via the camera toolbar.

Control Digital Zoom

Click 🔍 to enable digital zoom and draw a rectangle on the video to zoom in. Click again to disable digital zoom.

Note

When the playback is in software decoding mode, you can also capture the zoomed-in picture after using digital zoom.

Check Camera Status

Click 📈 to show the camera's recording status, signal status, connection number, etc.

Switch Stream

Click □ , □ , or □ (if supported) to switch the live view stream to main stream, sub-stream, or smooth stream (if supported).

Note

The smooth stream is available if the device supports the feature. You can switch to smooth stream in low-bandwidth network environment to make the playback more fluent.

Control Audio

Click 🔊 or 🔇 to turn off/on the sound.

Note

You can adjust the volume by moving the cursor to 🔈 .

14.9.3 Local Configuration

HikCentral Professional provides live view and playback for cameras via the Web Client. You can set network transmission parameters (hardware decoding, stream type, etc.) to optimize the performance of live view and playback for your current Web Client. You can also check the current saving path of video files and captured pictures on your PC.

Steps

Note

The parameters in Local Configuration only affect the current Web Client.

1. In the top left corner of Home page, select ≡ → **All Modules** → **Video** → **Video Application** .
2. Click **Local Configuration** on the left.
3. Click **Network Transmission** to configure network transmission parameters.

   GPU Hardware Decoding

   Enable GPU decoding for live view and playback to save CPU resources.

   Note

   - To enable GPU hardware decoding, your PC must support the feature.
   - After enabling GPU hardware decoding, restart live view or playback to take effect.
   - If the client displays a blurred screen after enabling GPU hardware decoding, disable it.

   Global Stream

   If a device does not support smooth stream, it will use sub-stream. If a device does not support sub-stream, it will use main stream.

   If the network connection is good, select main stream or sub-stream for better image quality. If the network connection is poor, select smooth stream for speed.

   Threshold for Main/Sub-Stream

   If the window division of display window is larger than the configured threshold, the stream type will automatically switch to main stream. If not, the stream type will switch to sub-stream.

   For example, if you set the threshold to ¼ and you set window division to 9-window mode, the cameras' stream type will switch to sub-stream.

   Note

   This parameter is only available when **Main Stream** is set as **Global 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 SYS server is 60s. The minimum waiting time between SYS server and devices is 5s. The minimum waiting 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 it to **Small (1 Frame)**, **Medium (6 Frames)**, or **Large (15 Frame)**. Larger frame caching results in better video performance but requires more network and computer resources.

Time Zone

Set the time reference for live view and playback to client time or device time.

Picture Format

Set the file format for the captured pictures during live view or playback.

Device Access Mode

Default Configuration

Restore the device access mode.

Automatically Judge

Judge the device access mode according to the network.

Directly Access

Access the device directly, not via HikCentral Professional Streaming Service.

Proxy

Access the device via HikCentral Professional Streaming Gateway and HikCentral Professional Management Service.

Note

By default, the platform will judge the device access mode according to the network. If you change to other modes, it only affects the client you currently logged in.

4. **Optional:** Click **Default Value** to restore to default settings.
5. Click **Save** to save the settings.
6. **Optional:** Click **Saving Path** on the left to view the saving path of the video files and captured pictures during live view or playback on your local PC.

Chapter 15 Manage Access Control

The system supports access control functions. Access control is a security technique that can be used to regulate who can get access to the specified doors.

On the Web Client, the administrator can add access control devices and video intercom devices to the system, group resources (such as doors) into different areas, and define access permissions by creating 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.

15.1 Flow Chart

The following flow chart shows the process of the configurations and operations of access control. For access control, you can also enter the **Access Control Quick Start** module on the Home page of the Web Client to go through the basic configurations.

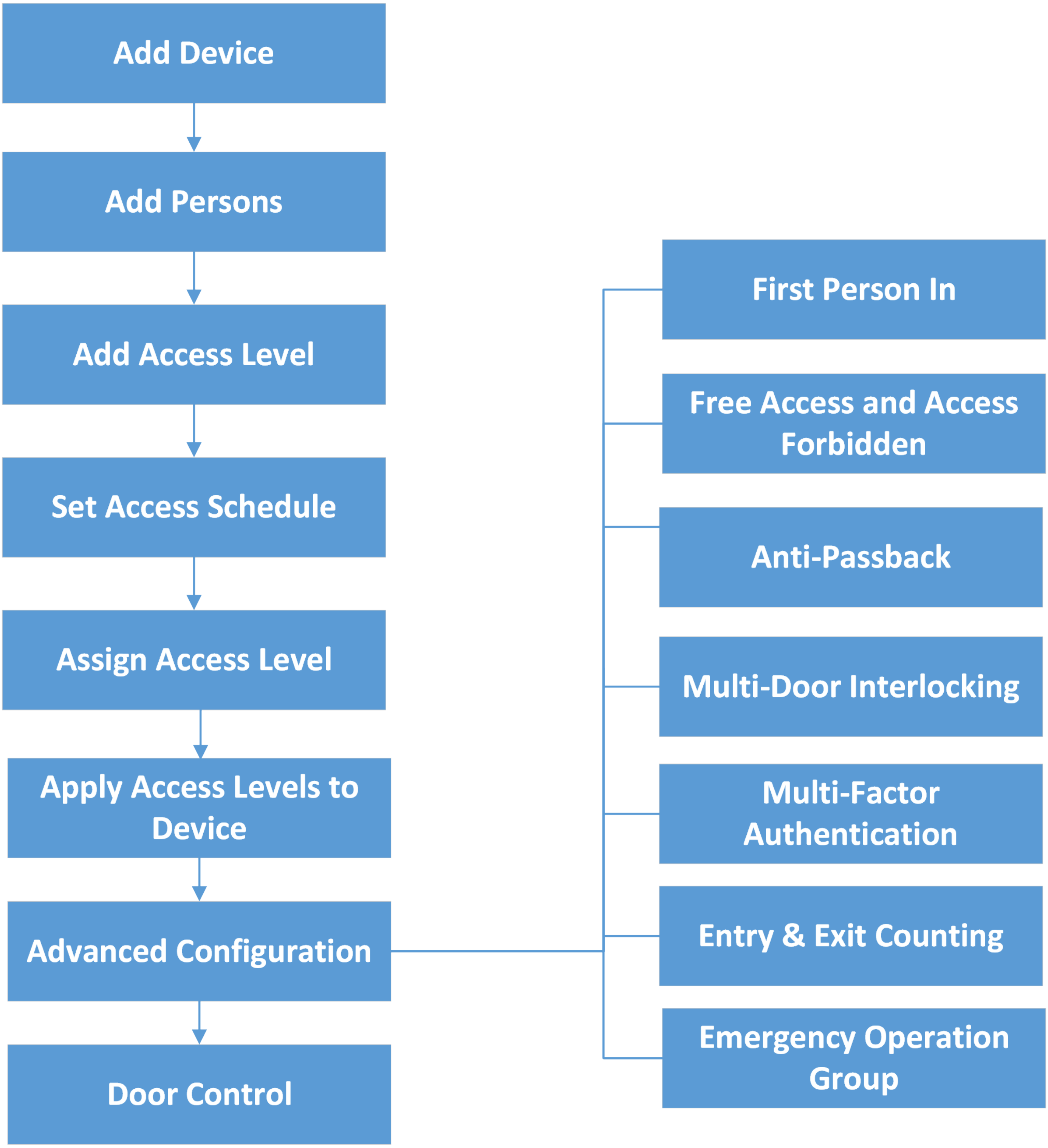


Figure 15-1 Flow Chart of Access Control

- **Add Device:** You need to add the access control devices and video intercom devices to the system. The system provides multiple methods for adding them. For details, refer to ***Manage Access Control Device*** and ***Manage Video Intercom Device*** .
- **Add Persons:** Add person information and set person's credentials (such as PIN, issuing a card, fingerprint, etc.). For details, refer to ***Manage Person*** .
- **Add Access Group:** Access group is a group of persons who have the same access level. The persons in the access group can access the same doors during the same authorized time period. For details, refer to ***Add Access Group*** .
- **Add Access Level:** Access level is a group of doors. After assigning access level, the assigned objects can get access to which doors during the authorized time period. For details, refer to ***Manage Access Level*** .
- **Set Access Schedule:** The access schedule defines when the person can access the access point with credentials. For details, refer to ***Set Access Schedule Template*** .
- **Assign Access Level:** You need to assign access levels to persons, so that the assignees can have the access to the access points in the access levels. You can assign an access level to multiple persons or assign multiple access levels to a person, person group, or access group.
- **Apply Access Levels to Device:** After setting the linkage between access group and access level, you need to apply the person's access level settings to the access control device of the doors linked to the access level to take effect. After that, the persons in the access group can access these doors during the authorized time period defined by the related access level. For details, refer to ***Apply Persons' Access Levels to Device*** .
- **Advanced Configuration:** The system provides some advanced configurations such as first person in rule, free access and access forbidden rule, emergency operation group, anti-passback, multi-door interlocking, multi-factor authentication, and entry & exit counting. For details about these configurations, refer to ***Configure First Person In Rule*** , ***Configure Free Access and Access Forbidden Rules*** , ***Add Emergency Operation Group*** , ***Configure Anti-Passback*** , ***Configure Multi-Door Interlocking*** , ***Configure Multi-Factor Authentication Rule*** , and ***Add Entry and Exit Counting Group*** .
- **Door Control:** After the above configurations on the Web Client, you can control the door's status during live view, view real-time access events, search history access records, etc. See ***Door Control*** for details.

15.2 Manage Access Level

In access control, access level is a group of doors. Assigning access level to persons, person groups, or access groups can define the access permission that which persons can get access to which doors during the authorized time period.

15.2.1 Add Access Level

To define access permission, you need to add an access level to group the access points (doors).

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **Access Control** → **Access Level** .
2. Click **Manage Access Level** on the left.
3. Click **Add** to enter the Add Access Level page.
4. Create a name for the access level.
5. **Optional:** Edit the description for the access level.
6. Select the access point(s) to add to the access level.
   1) In the **Available** list, select the access point(s) you want to add to the system and click > . You can view your selection in the **Selected** list.
   2) **Optional:** In the **Selected** list, select the access point(s) that you no longer want to add to the system, and click < to undo selection.

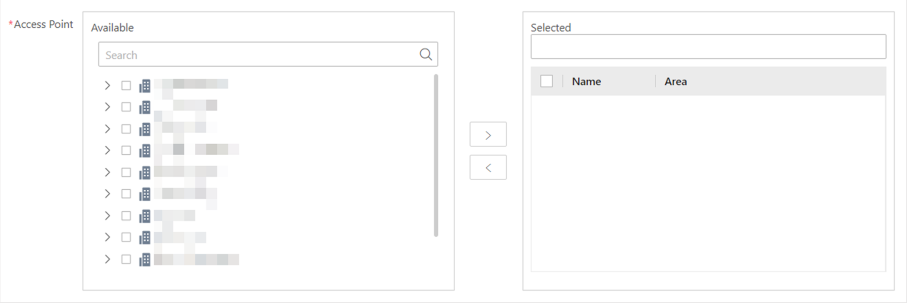


Figure 15-2 Select Access Points

7. Select an access schedule to define in which time period, persons are authorized to access the access points you select in the previous step.

Note

All default and custom access schedules are shown in the **Access Schedule** drop-down list. You can click **New Access Schedule Template** to customize a schedule. Or you can predefine access schedule templates. For details, refer to ***Set Access Schedule Template*** .

8. Click **Add** to add the access level and return to the access level management page.
9. **Optional:** Perform further operations on the added access level(s).

Edit Access Level	Click the name of an access level to view and edit its configurations.
Delete Access Level	Select an access level and click **Delete** to delete it.
Delete All Access Levels	Click ∨ → **Delete All** to delete all access levels.

What to do next

You need to assign the access level to persons, so that the assignees can have the access to the access points in the access level according to the access schedule. For details, refer to ***Assign Access Level*** .

15.2.2 Add Access Group

Persons in the same access group have the same access levels. You need to create access groups before assigning access levels to each access group.

Before You Start

Make sure your have added persons to the system. For details, refer to ***Manage Person*** .

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **Access Control** → **Access Level** .
2. Click **Assign by Access Group** on the left.
3. Click to enter the Manage Access Group page.
4. Click **Add**.
5. Configure the new access group.
   1) In **Group Name** field, create a name for the access group.
   2) In **Group Member** list, click **Add** to show the person group list.
   3) Select the persons you want to add to the access group and then click **Add**.
6. Click **Add** to add the access group and return to the Manage Access Group page.
7. **Optional:** Perform further operations on the added access group(s).

Edit Access Group	Click the name of an access group to view and edit its configurations.
Delete Access Group	Select an access group and click **Delete** to delete it. Or click ⌄ → **Delete All** to delete all access groups.

What to do next

You need to assign an access level to the access group, so that persons in the group can have the access to the access points in the access level according to the access schedule. For details, refer to ***Assign by Access Group*** .

15.2.3 Assign Access Level

You need to assign access levels to persons, so that the assignees can have the access to the access points in the access levels. You can assign an access level to multiple persons or assign multiple access levels to a person, person group, or access group.

Assign by Access Level

You can assign an access level to multiple persons so that the assigned persons can have the access to the access points in the access level.

Before You Start

- Make sure you have added access levels to the system. For details, refer to ***Add Access Level*** .
- Make sure you have added persons to the system. For details, refer to ***Manage Person*** .

Follow the steps to assign an access level to persons.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **Access Control** → **Access Level** .
2. Click **Assign by Access Level** on the left.
3. Click on the access level that you want to assign to persons.

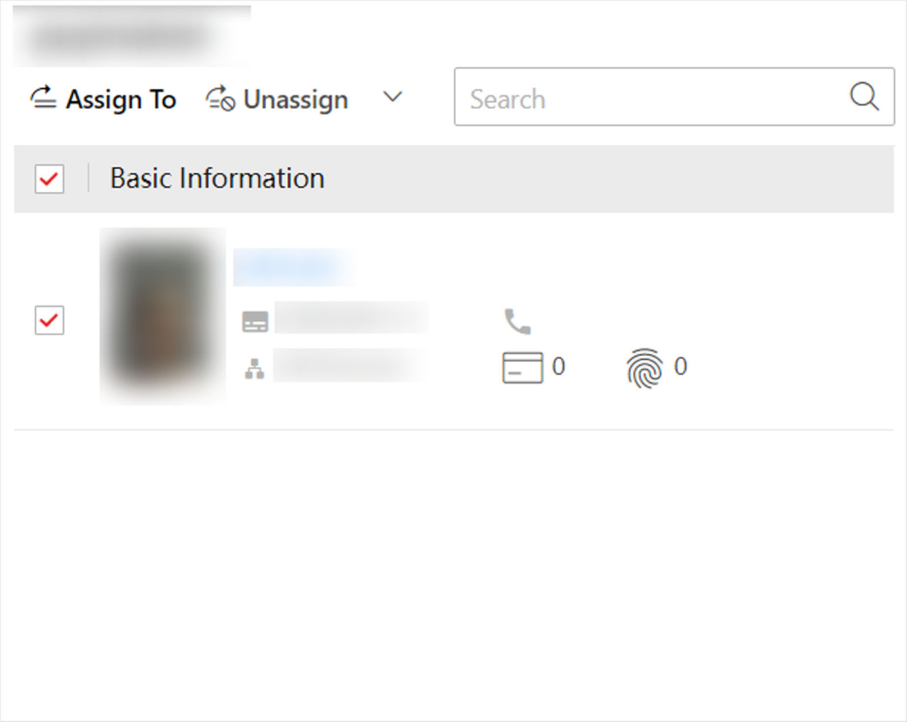


Figure 15-3 Assignee Panel

4. On the assignee panel, click **Assign To** to show person list.
5. Select the persons whom you want to assign the access level to and click **Add**.
6. Do one of the following to apply access level settings to devices.
   - In the pop-up window, click **Apply Now** to apply the settings immediately.
   - In the pop-up window, click **Apply Later**. When ready, click 🗎 to apply the settings. You can also set a schedule to apply automatically. For details, refer to ***Regularly Apply Access Level Settings to Devices*** .
7. **Optional:** To unassign a person from the access level, select the person and click **Unassign**. To unassign all, click ⌄ → **Unassign All** .

What to do next

Test your access control configurations and devices before putting them into use. For details, refer to ***Access Control Test*** .

Assign by Person

You can assign access levels to persons, so that the assignees can have the access to the access points in the access levels.

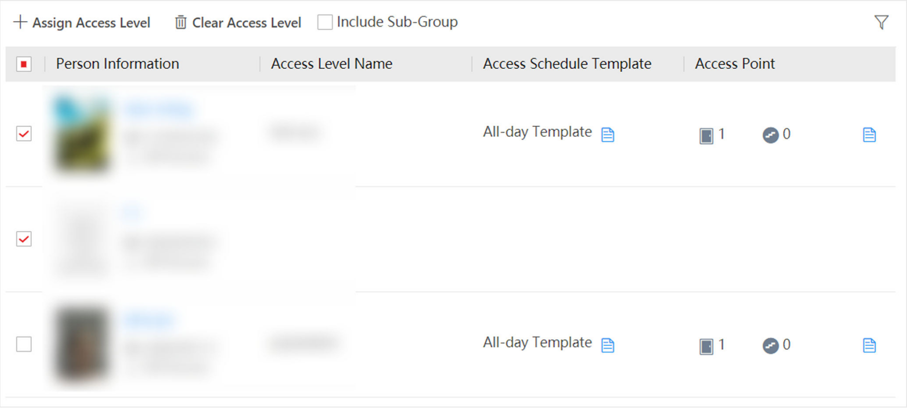
Before You Start

- Make sure you have added persons to the system. For details, refer to ***Manage Person*** .
- Make sure you have added access levels to the system. For details, refer to ***Add Access Level*** .

Follow the steps to assign one or more access levels to specific persons.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **Access Control** → **Access Level** .
2. Click **Assign by Person** on the left.
3. In the person group list, click a person group.
4. In the person information panel on the right, select the persons to whom you want to assign access levels.



☒	Person Information	Access Level Name	Access Schedule Template	Access Point	
☑	[illegible]	[illegible]	All-day Template 🗎	▣ 1 ● 0	🗎
☑	[illegible]				
□	[illegible]	[illegible]	All-day Template 🗎	▣ 1 ● 0	🗎

Figure 15-4 Person Information Panel

Note

You can click on person's name to view the details about the person.

5. Click **Assign Access Level**.
6. In the Assign Access Level panel, select the access levels that you want to assign to the selected persons.
7. Click **Add**.
8. Do one of the following to apply access level settings to devices.
   - In the pop-up window, click **Apply Now** to apply the settings immediately.
   - In the pop-up window, click **Apply Later**. When ready, click 🗎 to apply the settings. You can also set a schedule to apply automatically. For details, refer to ***Regularly Apply Access Level Settings to Devices*** .

9. **Optional:** To clear a person's access levels, select the person and click **Clear Access Level**. For details, refer to ***Clear Persons' Access Levels*** .

What to do next

Test your access control configurations and devices before putting them into use. For details, refer to ***Access Control Test*** .

Assign by Person Group

You can assign access levels to person groups, so that the persons in the person group can have the access to the access points in the access levels.

Before You Start

- Make sure you have added person groups and persons to the system. For details, refer to ***Manage Person*** .
- Make sure you have added access levels to the system. For details, refer to ***Add Access Level*** .

Follow the steps to assign one or more access levels to specific person groups.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **Access Control** → **Access Level** .
2. Click **Assign by Person Group** on the left.
3. Do one of the following to assign access levels to person groups.
   - Assign access levels to each person group one by one.
     a. In the person group list, click on a person group.
     b. In the assigned access level panel on the right, click **Assign Access Level**.
     c. In the Assign Access Level panel, select the access levels you want to assign to the selected person group.
     d. Click **Add**.
   - Assign access levels to multiple person groups at a time.
     a. Click .
     b. In the person group list, select the person groups where you want to assign access levels.

     Note

     Sub-groups are excluded from selection by default. To include all sub-groups of each person group, check **Select Sub-Groups**.

     c. In access level list, select the access levels you want to assign to the person groups.
     d. Click **Save**.

Note

After assigning access levels to a person group, you can still modify the access levels for each person in the group, and it will not affect the settings for the person group. For details, refer to ***Assign by Person*** .

4. Do one of the following to apply access level settings to devices.
   - In the pop-up window, click **Apply Now** to apply the settings immediately.
   - In the pop-up window, click **Apply Later**. When ready, click 🗎 to apply the settings. You can also set a schedule to apply automatically. For details, refer to ***Regularly Apply Access Level Settings to Devices*** .
5. **Optional:** To unassign an access level from the person group, select the access level and click **Unassign**. To unassign all access levels, click ∨ → **Unassign All** .

What to do next

Test your access control configurations and devices before putting them into use. For details, refer to ***Access Control Test*** .

Assign by Access Group

You can assign multiple access levels to an access group, so that the persons in the access group can have the access to the access points in the access levels.

Before You Start

- Make sure you have added access groups to the system. For details, refer to ***Add Access Group*** .
- Make sure you have added access levels to the system. For details, refer to ***Add Access Level*** .

Follow the steps to assign one or more access levels to an access group.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **Access Control** → **Access Level** .
2. Click **Assign by Access Group** on the left.
3. Click on the access group where you want to assign access levels.
4. Click **Assign Access Level**.
5. In the Assign Access Level window, select the access levels that you want to assign to the access group.
6. Click **Add**.
7. Do one of the following to apply access level settings to devices.
   - In the pop-up window, click **Apply Now** to apply the settings immediately.
   - In the pop-up window, click **Apply Later**. When ready, click 🗎 to apply the settings. You can also set a schedule to apply automatically. For details, refer to ***Regularly Apply Access Level Settings to Devices*** .
8. **Optional:** To unassign an access level from the access group, select the access level and click **Unassign**. To unassign all access levels, click ∨ → **Unassign All** .

What to do next

Test your access control configurations and devices before putting them into use. For details, refer to ***Access Control Test*** .

15.2.4 Apply Persons' Access Levels to Device

After setting or modifying the linkage between persons and access levels, you need to apply the access level settings to the access control devices to take effect. After that, the persons can access these doors during the authorized time period defined by the related access level.

Manually Apply Access Level Settings to Device

After setting access levels and assigning access levels to persons, person groups, or access groups, you need to apply the relations between persons and access points to the devices.

Before You Start

Make sure you have assigned access levels to persons in the system. For details, refer to ***Assign Access Level*** .

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **Access Control** → **Access Level** .
2. Click **Assign by Access Level**, **Assign by Person**, **Assign by Person Group**, or **Assign by Access Group** on the left.
3. Click 🗎 .
4. In the Apply Access Level Settings panel, select the persons to apply the access level settings.
   - To apply the access level settings of all persons, select **All Persons**.
   - To apply the access level settings of specific persons, select **Specified Persons**, click 🗋 , select the persons, and click **Add**.
5. Select the access points to apply the persons' access level settings.
   - To apply the access level settings of all access points, switch off **Specified Access Point**.
   - To apply the access level settings of specific access points, switch on **Specified Access Point** and select the access points.
6. Apply access level settings to devices.
   - To clear all persons' access level configurations on the devices first and then apply the configurations in the system to the devices, check **Apply (Initial)** and click **Apply**.

     Note

     - Only available when you select **All Persons** previously.
     - During the initialization process, the devices will be offline, and persons cannot access these access points.
   - To apply changed (newly added, edited, deleted) access level settings to the devices, uncheck **Apply (Initial)** and click **Apply**.
7. **Optional:** If persons' access level settings (such as linked access levels, person credentials, etc.) are changed or the applying process failed, ⓘ will appear next to 🗎 , indicating some access level settings are pending to be applied to the devices. You can hover the cursor over ⓘ to view the details.

Note

For troubleshooting the applying process, refer to ***Access Control Test*** .

Regularly Apply Access Level Settings to Devices

You can set a schedule to apply the access level settings in the system to devices automatically.

Before You Start

Make sure you have assigned access levels to persons in the system. For details, refer to ***Assign Access Level*** .

Steps

1. In the top left corner of Home page, click ≡ → **All Modules** → **Access Control** → **Basic Settings** .
2. Click **Apply to Device (Scheduled)** on the left.
3. Switch on **Apply to Device (Scheduled)**.
4. Select an applying mode.
   - **Apply at Fixed Time**: Apply the changed access level settings and the settings that failed to be applied last time to devices at a specific time (System Management Server time) on a daily basis. You can select a time in the **Auto-Apply At** drop-down list.
   - **Apply Every Certain Hours**: Apply the changed access level settings and the settings that failed to be applied last time to devices immediately and every certain hours afterward. You can select an interval in the **Auto-Apply** drop-down list.
5. Click **Save**.

15.2.5 Clear Persons' Access Levels

You can clear the access levels of persons so that they cannot access the access points in the access levels. For example, if there is no access record of certain persons entering or exiting for a long time, the administrator can clear their access levels to make sure the persons' credentials will not be misused.

In the top left corner of Home page, click ≡ → **All Modules** → **Access Control** → **Access Level** .

Click **Assign by Person** on the left.

Select a person group to show all persons in the group. You can filter the target persons by setting search conditions.

Select the target persons and click **Clear Access Level**.

Note

After clearing, the previous access level settings of the persons cannot be restored. You need to re-assign access levels for them again when needed.

After clearing the access level settings of the selected persons, these persons will be removed from the related access groups. You need to apply the access level settings of these persons to the devices to take effect. You can click **Apply Now** in the pop-up window to apply the settings immediately. Or click **Apply Later**. When ready, click . You can also set a schedule to apply automatically. For details, refer to ***Regularly Apply Access Level Settings to Devices*** .

After applying to the devices, the access level settings of the persons will be deleted on the devices.

15.2.6 Set Access Schedule Template

Access schedule defines when persons can open access points in an access level with credentials, or when access points remain unlocked so that persons can open the access points with free access. The system provides three default access control schedule templates: All-day Template, Weekday Template, and Weekend Template. You can also add customized templates according to your needs.

Steps

1. In the top left corner of Home page, click ≡ → **All Modules** → **Access Control** → **Basic Settings** .
2. Click **Access Schedule Template** on the left.
3. Click + to create a blank template.
4. Configure the template in the template information panel on the right.

   Name

   Create a name for the template.

   Copy from

   Optionally, you can select to copy the settings from existing templates.
5. In the **Weekly Schedule Template** box, set a schedule pattern for each day.
   1) Click **Authorize** and select or draw in the box to define the authorized time periods.
   2) **Optional:** Click **Erase** and select or draw on the authorized time periods to clear the selection.

   Note

   You can set up to 8 separate time periods for each day.
6. **Optional:** Set a holiday schedule if you want different schedules for specific days.

   Note

   Holiday schedule has a higher priority than weekly schedule.

   1) Click **Add Holiday**.
   2) Select existing holiday templates, or click **Add New** to create a new holiday template (see ***Set Holiday*** for details).
   3) Click **Add**.

4) Set a schedule pattern for holidays.

7. Click **Add** to save the template.

8. **Optional:** Perform further operations on added templates.

View and Edit Template Details	Click a template item to view and edit its configurations.
Delete Template	Click a template item and click 🗑 to delete it.

What to do next

Set access schedule for access level to define in which time period persons are authorized to access the access points in the access level. For details, refer to ***Add Access Level*** .

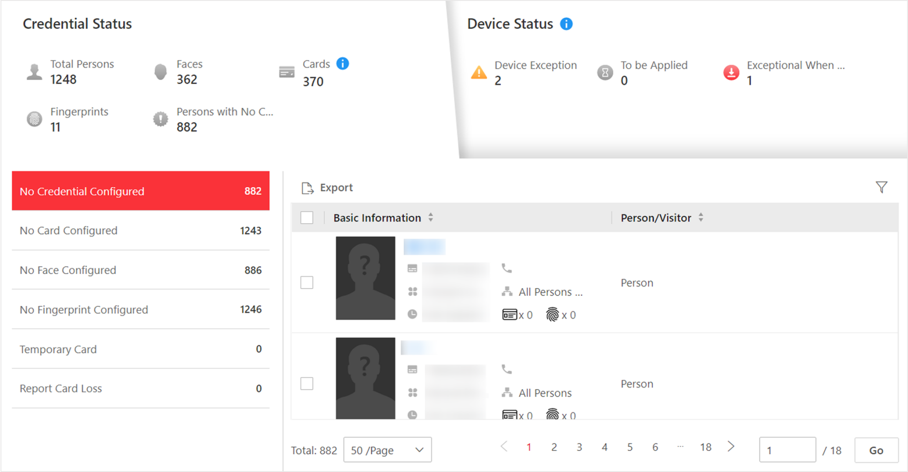
15.3 Access Control Test

HikCentral Professional provides **Access Control Test**. It is a tool through which you can test whether the configurations about access control (such as persons' credentials and access levels for access control and video intercom) are set correctly and completely and whether the devices are running properly.

In the top left corner of Home page, click ≡ → **All Modules** → **General** → **Access Control** → **Troubleshooting** .

Check Credential Status

Select **Credential Status** tab to view the status of the added credentials.



Credential Status

Total Persons 1248
Faces 362
Cards 370
Fingerprints 11
Persons with No C... 882

Device Status

Device Exception 2
To be Applied 0
Exceptional When ... 1

No Credential Configured	882
No Card Configured	1243
No Face Configured	886
No Fingerprint Configured	1246
Temporary Card	0
Report Card Loss	0

Export

□	Basic Information	Person/Visitor
□	All Persons ... x 0 x 0	Person
□	All Persons x 0 x 0	Person

Total: 882 50 /Page ‹ 1 2 3 4 5 6 ··· 18 › 1 / 18 Go

Figure 15-5 Credential Status

There are 6 types of exceptions on credential settings in the system. The number next to each exception type indicates the number of persons whose credential settings are exceptional.

Click each exception type to view the information about the persons with exceptions.

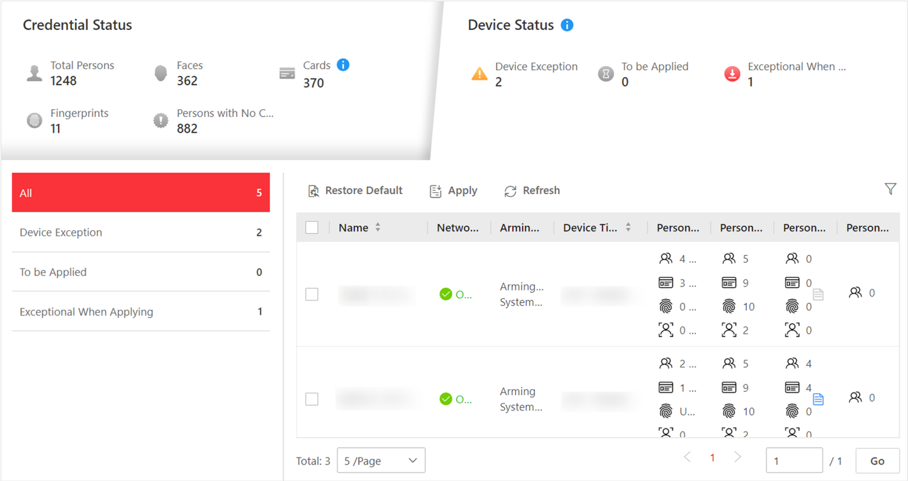
You can click person's name to edit the credentials if necessary.

Check Device Status

Select **Device Status** tab to view the status of the devices (including access control devices and video intercom devices). You can check person information and credential information that are already applied to the devices, configured in the system, failed to apply, and persons to be applied to the devices.

Note

Only the status of the devices which have been configured with access levels are shown.



Credential Status

Total Persons 1248 | Faces 362 | Cards 370

Fingerprints 11 | Persons with No C... 882

Device Status

Device Exception 2 | To be Applied 0 | Exceptional When ... 1

All	5
Device Exception	2
To be Applied	0
Exceptional When Applying	1

Restore Default | Apply | Refresh

□	Name	Netwo...	Armin...	Device Ti...	Person...	Person...	Person...	Person...
□		O...	Arming... System...		4 ... 3 ... 0 ... 0 ...	5 9 10 2	0 0 0 0	0
□		O...	Arming System...		2 ... 1 ... U... 0	5 9 10 2	4 4 0 0	0

Total: 3 | 5 /Page | 1 | 1 / 1 | Go

Figure 15-6 Device Status

Click each exception type to view the information about the persons with exceptions.

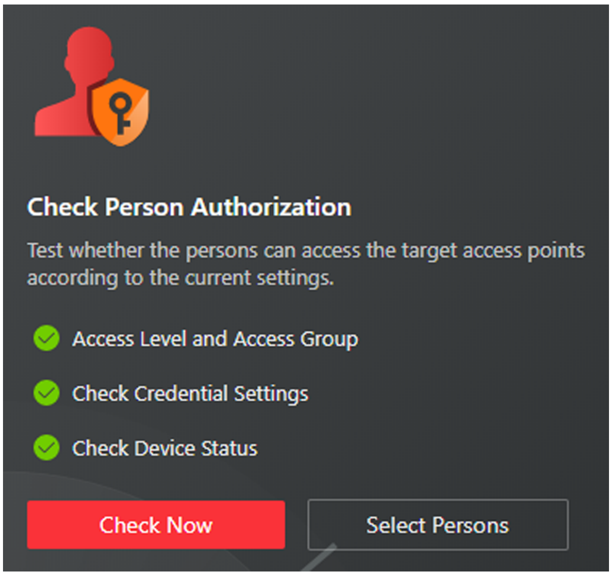
You can select the devices and click the following buttons to solve device issues.

Restore Default	Restore the settings on the devices to the default value.
Apply	Apply person information and credential settings to these devices again.
Refresh	Refresh the list to get the latest device status.

Check Authorization Settings of Persons

You can check the authorization settings (such as access levels and access group settings, credential settings, and applying status) of specific persons in the system. This function helps you to test whether the persons can access the target access points according to the current settings.

Click « to expand the side panel.



Check Person Authorization

Test whether the persons can access the target access points according to the current settings.

✓ Access Level and Access Group

✓ Check Credential Settings

✓ Check Device Status

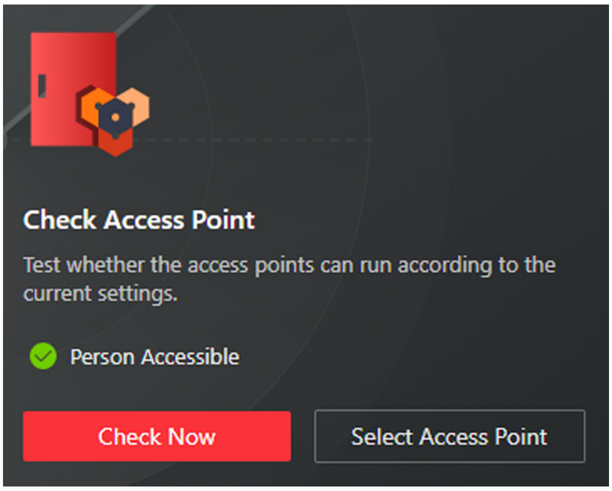
Figure 15-7 Check Authorization Settings

In the **Check Person Authorization** section, select the item(s) of information you want to check.
Click **Check Now** to test the authorization settings of all existing persons.
Or click **Select Persons** to select the persons you want to test and then click **Check Now** to test the authorization settings of the selected persons.

Check Access Point Settings

You can test whether the persons can access the access points according to the settings in the system.

Click « to expand the side panel.



Check Access Point

Test whether the access points can run according to the current settings.

✓ Person Accessible

Figure 15-8 Check Access Point Settings

In the **Check Access Point** section, select the item(s) of information you want to check.
Click **Check Now** to test the settings of all existing access points in the system.

Or click **Select Access Points** to select the access points you want to test and then click **Check Now** to test the settings of the selected access points.

Note

The access points which are not added to any access levels will not be checked.

15.4 Advanced Functions

15.4.1 Configure Free Access and Access Forbidden Rules

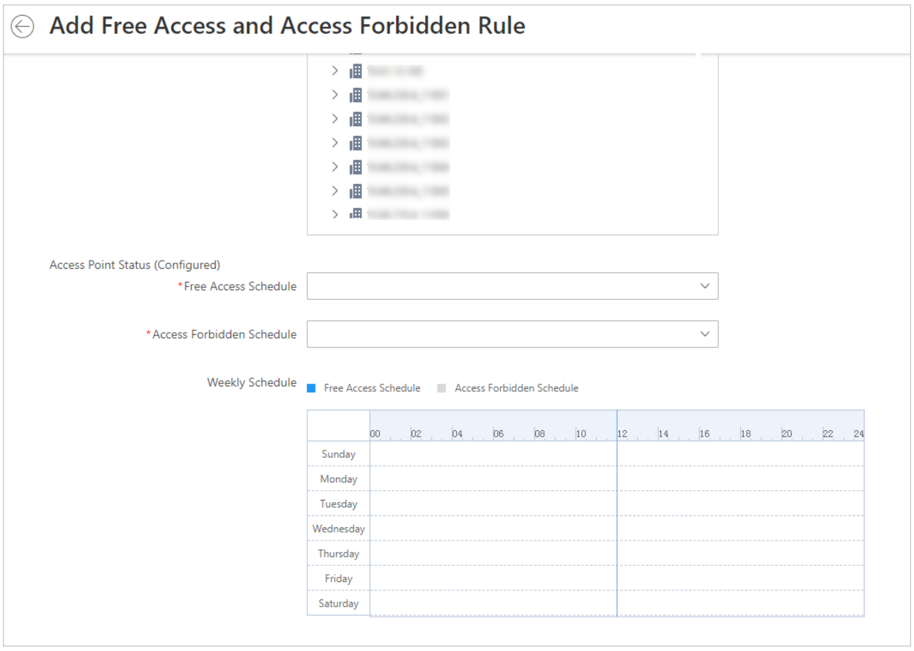
You may need to set doors accessible or inaccessible during certain periods. To perform this function, you need to configure free access and access forbidden rule for certain doors.

Steps

Note

This function should be supported by the device.

1. In the top left corner of Home page, select ≡ → **All Modules** → **Access Control** → **Access Control Application** .
2. Click **Free Access and Access Forbidden** on the left.
3. Click **Add** to enter the Add Free Access and Access Forbidden Rule page.
4. Enter the rule name.
5. Select an access point from the following area list.
6. Select free access schedule or access forbidden schedule.



Add Free Access and Access Forbidden Rule

Access Point Status (Configured)

*Free Access Schedule

*Access Forbidden Schedule

Weekly Schedule

Figure 15-9 Add Free Access and Access Forbidden Rule Page

Free Access Schedule

During free access period, all persons can access the selected doors without credentials required.

Access Forbidden Schedule

During access forbidden period, no persons can access the selected doors even if he/she has the authorized credentials, except the super users.

Note

- You can click **Add New** to add a custom access schedule or holiday schedule. See ***Set Access Schedule Template*** for details.

7. Click **Add**.

   The system will automatically apply the schedule(s) to devices.

8. **Optional:** Perform the following operations.

View Schedule Details	Click 🗎 to show the schedule details.
Copy Schedule to Other Access Point	Click a rule name to enter the rule page. Click **Copy to** on the top right to copy the schedule to other access points.

15.4.2 Configure First Person In Rule

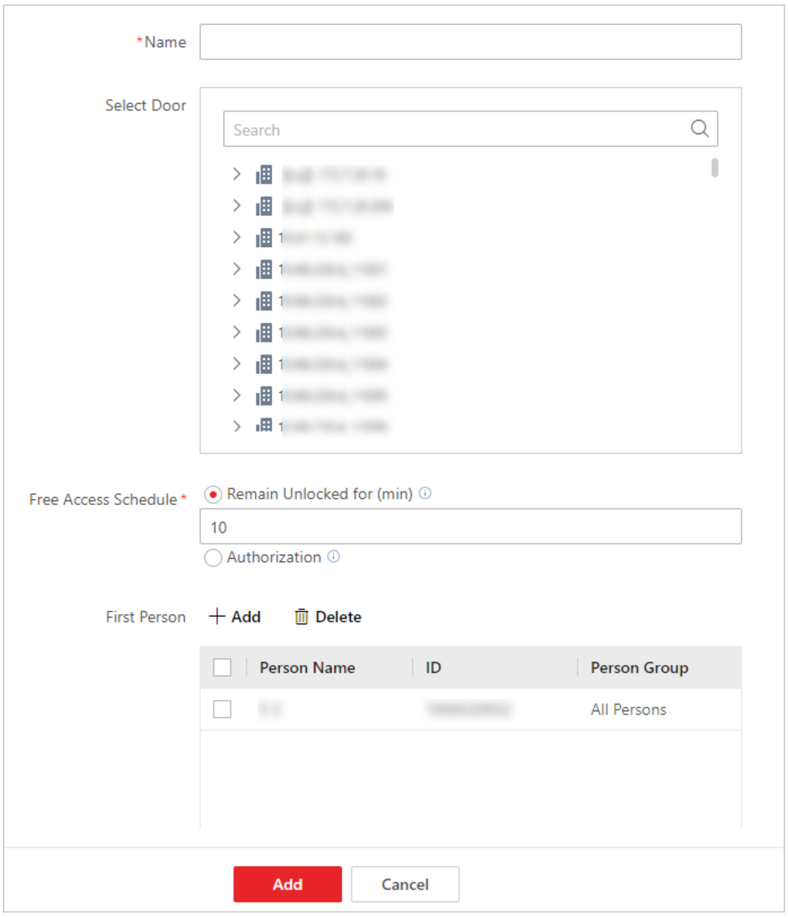
First Person In refers to a rule that only after the first person is authorized to enter with his or her card, fingerprint, or face, can other people's permission be activated. There are two modes for First Person In, the Remaining Open after First Person and the Authorization by First Person.

Steps

Note

This function should be supported by the device.

1. In the top left corner of Home page, select ≡ → **All Modules** → **Access Control** → **Access Control Application** .
2. Click **First Person In Rules** on the left.
3. Click **Add** to enter the Add First Person In Rules page.
4. Enter the rule name.
5. Select a door from the following area list.
6. Set **Free Access Schedule**.



*Name

Select Door

Search

Free Access Schedule *

● Remain Unlocked for (min)

10

○ Authorization

First Person + Add 🗑 Delete

□	Person Name	ID	Person Group
□	[redacted]	[redacted]	All Persons

Add Cancel

Figure 15-10 Add First Person In Rule Page

Remain Unlocked for

When the door is locked, if the first person swipes card, the door will remain unlocked during the configured period.

Authorization

The door is locked and access is denied with any credentials (except during the free access schedule) until you swipe the first card. After the first person swipes card, the door is authorized and the persons with corresponding access level are granted to access. The authorization will be invalid at 00:00 a.m. every day.

7. Click **Add** to select first person(s).
8. Click **Add** to add the rule.

15.4.3 Add Emergency Operation Group

An emergency operation group is a group for access points which need to be operated (remaining locked/unlocked) in a batch. This function is mainly applicable for emergent situation. For example, after grouping the doors of the school's main entrances and exits into one emergency operation group, the school's security personnel can lock down the doors in this group by quick operation on the Control Client, so that the school closes and no one can get into the school except for high level admins. This function would block out teachers, custodians, students, etc.

Before You Start

Add the access points into different areas first. For details, refer to ***Add Element to Area*** .

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **Access Control** → **Access Control Application** .
2. Click **Access Control Rule** → **Emergency Operation Group** on the left.
3. Click **Add**.

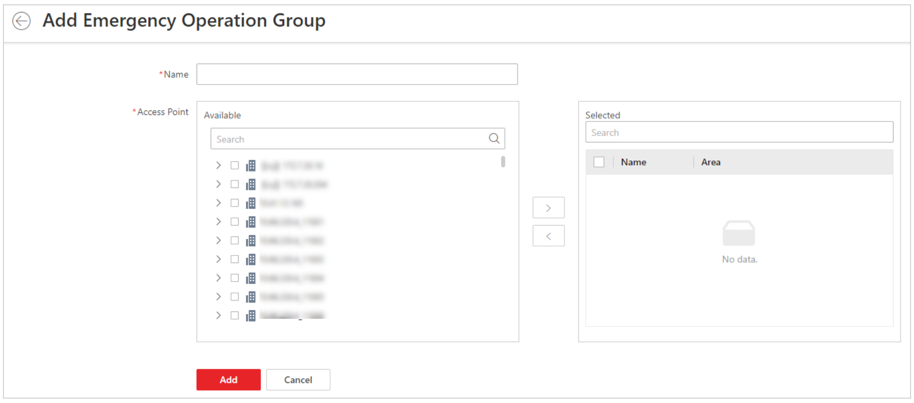


Figure 15-11 Add Emergency Operation Group Page

4. Create a name for the group.
5. Select the access points and click **>** to add them to the group.

Note

You can add doors of access control devices and doors of video intercom devices to the emergency operation group.

6. Click **Add**.

   The emergency operation group is added in the table and you can view the access points in the group.

15.4.4 Configure Anti-Passback

The anti-passback feature is designed to minimize 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 door in the anti-passback group if he/she enters via the door in the anti-passback group.

Before You Start

Add the access points into different areas first. For details, refer to ***Add Element to Area*** .

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **Access Control** → **Access Control Application** .
2. Click **Anti-Passback** on the left.
3. In the Anti-Passback field, click **Add**.
4. Create a name for the group.
5. Select doors and click **>**.
6. **Optional:** Enable **Forgive Anti-Passback Regularly** to set a fixed time so that the platform can forgive the anti-passback violations occurred in this group automatically everyday.

   Anti-Passback Violation

   When a person attempts to use a card out of anti-passback rule's sequence, the access will be denied. This is called "Anti-Passback Violation". When an anti-passback violation occurs, no entry is allowed unless the anti-passback violation event is forgiven.

   Note

   You cannot set forgiving anti-passback violations regularly when there is only one door in the anti-passback group.

7. Click **Add**.
8. **Optional:** Perform one or more of the following operations after adding the anti-passback group to the area.

   Edit Anti-Passback Group Click group name to edit the anti-passback group settings.

You can edit the name of the group, add or delete doors in the group, change the forgiving anti-passback violation regularly settings, and edit the locations of the group and doors on the map.

Set/Cancel Forgiving Anti-Passback Regularly to All

When a person attempts to use a card out of anti-passback rule's sequence, the access will be denied. This is called "Anti-Passback Violation". When anti-passback violation occurs, no entry is allowed unless the anti-passback violation event is forgiven.

Click **Set Forgiving Anti-Passback Regularly to All** and specify a fixed time so that the platform can automatically forgive the anti-passback violations occurred in all the anti-passback groups at that time everyday.

Delete Anti-Passback Group

Click × to delete the added anti-passback group.

15.4.5 Configure Multi-Door Interlocking

Multi-door interlocking is used to control the entry of persons to a secure area such as a clean room, where dust or small particles may cause a major issue. One multi-door interlocking group is composed of at least two doors and only one door can be opened simultaneously.

Before You Start

Add the access points into different areas first. For details, refer to ***Add Element to Area*** .

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **Access Control** → **Access Control Application** .
2. Click **Multi-Door Interlocking** on the left.
3. Click **Add**.
4. Create a name for the group.
5. Select doors and click **>**.
6. Click **Add**.

15.4.6 Manage Multi-Factor Authentication

Multi-Factor Authentication is an access authentication scheme which requires all the predefined persons to be present and get authentication. Multi-Factor Authentication is generally used in places such as bank vault to ensure the security of important assets and data. To perform this function, you need to configure multi-factor authentication rule and add multi-factor authentication group first. Besides, you can add persons to receive remote door open request.

Configure Multi-Factor Authentication Rule

In access control, multi-factor authentication is an authentication method in which the door will unlock only after multiple persons present authenticating multiple credentials in turn. This method is mainly used for locations with high security requirements, such as bank vault. With the mutual supervision of the persons, multi-factor authentication provides higher security for the assets in these locations.

Steps

Note

This function should be supported by the device.

1. In the top left corner of Home page, select ≡ → **All Modules** → **Access Control** → **Access Control Application** .
2. Click **Access Control Rule** → **Multi-Factor Authentication** on the left.
3. Click **Add** to enter the Add Multi-Factor Authentication Rule page.
4. Enter the rule name.
5. Select a door from the following area list.
6. Set the access mode of the door.

   Unlock After Access Granted

   The door will be unlocked automatically after the persons swiping their cards (or other type of credentials) on the card readers of the door and the access is granted.

   Remotely Unlock After Granted

   After the persons swiping their cards (or other type of credentials) on the card readers of the door and the access is granted, a window will pop up on the Control Client. The operator of the Control Client should confirm to unlock the door remotely and then the door will be unlocked successfully.

   Enter Super Password After Granted

   After the persons swiping their cards (or other type of credentials) on the card readers of the door and the access is granted, they should enter the super password on the card reader. After that, the door will be unlocked successfully.
7. Set the access schedule to define in which time period, the persons are authorized to access the door.

   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 Schedule Template*** .
8. Set the card swiping interval and make sure the interval between two authentications on the card reader is within this value.

Example

When you set the interval as 5s, if the interval between two authentications is longer than 5s, the authentications will be invalid, and you should authenticate again from the beginning.

9. Click **Add** to set the access group(s) to define who have the permission to access the door.

   Number of Persons for Authentications

   Define how many persons should authenticate on the card reader.

   For example, if you set 3 for access group Security Guard and 1 for access group Bank Manager, it means three security guards should swipe cards on the card reader (or other access mode), and one bank manager should swipe card on the card reader (or other access mode) for this multi-factor authentication.

   Note

   This value should be no larger than the number of persons in the access group.

   Card Swiping Order

   Click ↑ or ↓ in the **Operation** column to set the authentication order of different access groups.

10. Click **Save**.

Add Multi-Factor Authentication Group

To perform multi-factor authentication function, you need to create a multi-factor authentication group and appoint persons as the member of the group first. Persons in the group have the permission for multi-factor authentication of specific doors.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **Access Control** → **Access Control Application** .
2. Click **Multi-Factor Authentication** on the left.
3. Click **Multi-Factor Authentication Group Management** on the top.
4. Click **Add** to open the Add Multi-Factor Authentication Group panel.
5. Enter the multi-factor authentication group name.
6. Click **Add** to select group number from the person list.
7. Click **Add**.

Add Person to Receive Remote Door Open Request

To handle remote door open request on the Control Client, you need to appoint persons to receive these request beforehand.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **Access Control** → **Access Control Application** .
2. Click **Multi-Factor Authentication** on the left.
3. Click **Persons to Receive Remote Door Open Request** on the top.
4. Click **Add** to open the Add Persons to Receive Remote Door Open Request panel.
5. Select persons from the person list.
6. Click **Add**.

15.4.7 Set Card Reader Access Mode

You can set the card reader access mode to face authentication or card-swiping, or both of them in normal time period or custom time period according to your actual need.

Before You Start

Make sure you have added doors to area. See ***Add Element to Area*** for details.

Steps

Note

This function should be supported by the device.

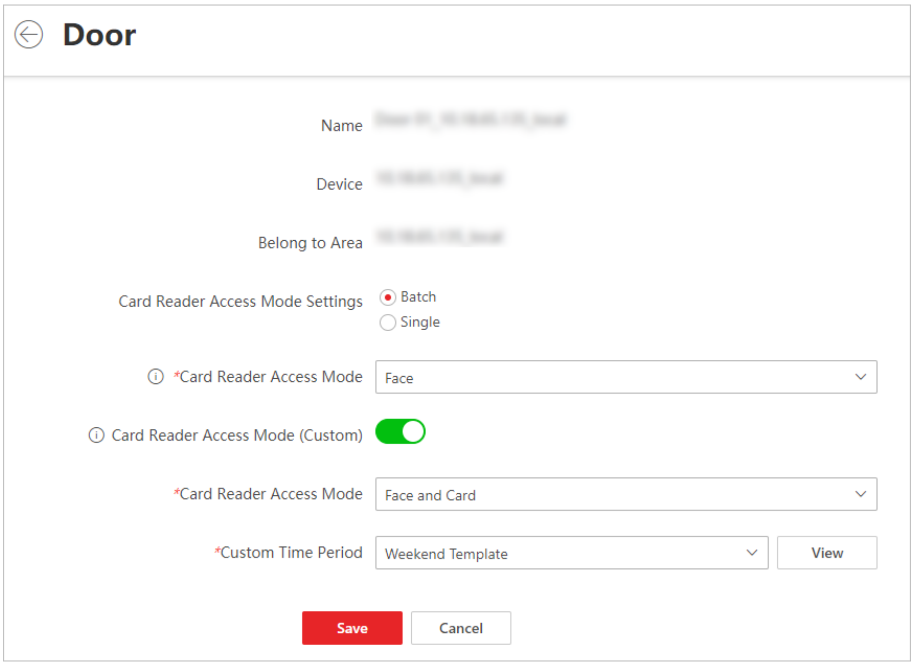
1. In the top left corner of Home page, select ≡ → **All Modules** → **Access Control** → **Access Control Application** → **Card Reader Access Mode** .
2. Select an area from the area list.
3. Click a door name on the right.
4. Select the Card Reader Access Mode Settings.

   Batch

   Set the same card reader access mode for all the card readers of a door.

   Single

   If you want to set different card reader access modes for different card readers, select this mode.



Door

Name [illegible]

Device [illegible]

Belong to Area [illegible]

Card Reader Access Mode Settings ● Batch ○ Single

*Card Reader Access Mode: Face

Card Reader Access Mode (Custom): on

*Card Reader Access Mode: Face and Card

*Custom Time Period: Weekend Template

Figure 15-12 Set Card Reader Access Mode Page

5. Select Card Reader Access Mode.

Card Reader Access Mode

Set the card reader's access mode in normal time periods. For example, if you select **Card**, you should open the door by swiping the card for each authentication.

Card Reader Access Mode (Custom)

When you want to open the door via another access mode in some special time periods, set the card reader's access mode and select the custom time period. For example, if you select Fingerprint and Weekend Schedule, you should open the door via fingerprint at weekends.

6. **Optional:** Click **Copy to** on the top right to apply the settings to other doors.
7. Click **Save**.

15.4.8 Add Entry and Exit Counting Group

The entry and exit counting group is used to group the doors in certain region. You can set some doors as the region border. Only the persons accessing these doors are counted, and other doors inside the region are ignored. By grouping these doors, the system provides counting functions based on the entry and exit records on these doors. With this function, you can know who enters/ exits this region and how many persons still stay in this region. This is applicable for certain emergency scene. For example, during a fire escape, the number of the remaining/stayed-in persons and name list are required for rescue.

Before You Start

Add the access points into different areas. For details, refer to ***Add Element to Area*** .

Steps

Note

After setting entry & exit counting group, you can perform entry & exit counting in **Identity Access Search → Entry & Exit Counting** on the Control Client to count the number of people who are still in the region and view who enters/exits this region.

1. In the top left corner of Home page, select ≡ → **All Modules → Access Control → Access Control Application** .
2. Click **Entry and Exit Counting Group** on the left.
3. Click **Add**.
4. Create a name for the group.
5. Click **Add** and select doors from the area list.
6. Set the entering or exiting direction of the card readers of the selected doors.

   The access records on the entering card reader will be counted as person entering this region while the access records on the exiting one will be counted as person exiting this region.
7. Click **Add**.

   The entry & exit counting group is added in the table and you can view the doors in the group.

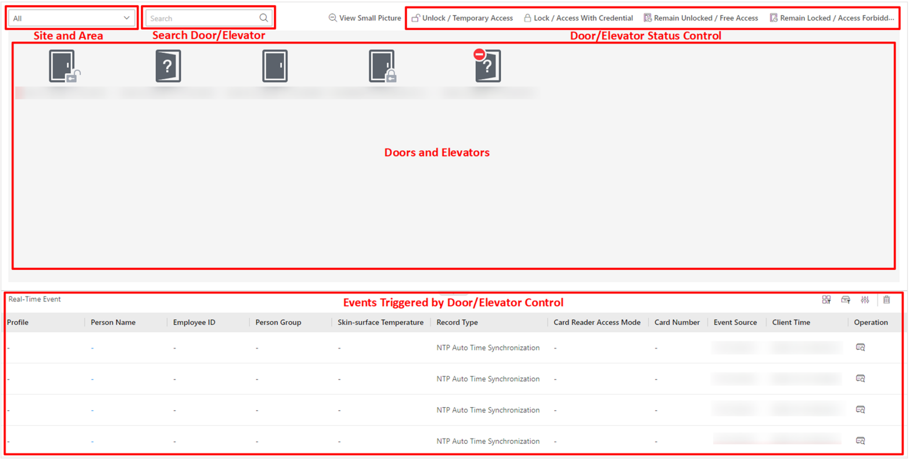
15.5 Door Control

With emergency operation group, you can control door status in a batch when an emergency happens. For example, after grouping the doors of a school's main entrances and exits into one emergency operation group, school's security personnel can lock down the doors in the group, so that no one can enter or leave the school except for maintenance and high-level admins. This function can also block out teachers, custodians, students, etc.

You can control all or part of the doors in the selected site and area according to your need. When the emergency is over, you can restore the status to Access with Credential.

Note

Only the users with Administrator or Operator role can control all doors in a batch.


All
Search
View Small Picture
Unlock / Temporary Access
Lock / Access With Credential
Remain Unlocked / Free Access
Remain Locked / Access Forbidd...
Site and Area
Search Door/Elevator
Door/Elevator Status Control
Doors and Elevators
Real-Time Event
Events Triggered by Door/Elevator Control

Profile	Person Name	Employee ID	Person Group	Skin-surface Temperature	Record Type	Card Reader Access Mode	Card Number	Event Source	Client Time	Operation
-	-	-	-	-	NTP Auto Time Synchronization	-	-	[redacted]	[redacted]	
-	-	-	-	-	NTP Auto Time Synchronization	-	-	[redacted]	[redacted]	
-	-	-	-	-	NTP Auto Time Synchronization	-	-	[redacted]	[redacted]	
-	-	-	-	-	NTP Auto Time Synchronization	-	-	[redacted]	[redacted]	

Figure 15-13 Access Control Real-time Monitoring

15.5.1 View Real-Time Access Event

In **Access Control** module, you can view events of doors. You can also control door status according to the event details, search more event information, and so on.

In the top left corner of Home page, select ≡ → **All Modules** → **Access Control** → **Real-Time Monitoring** .

Select the site and area that you want to view the access events. Real-time access events are displayed at the bottom of the page.

Search Device Records	Click in the Operation column to go to Device Recorded Data Retrieval page to search records by customizing searching conditions.
Filter Events	You can filter the real-time events by setting conditions according to record types and event source. Click to set conditions.
Custom Column	Click to customize the column to only show the most relevant event information.
Clear Events	Click 🗑 to clear all events in the list.

15.5.2 Door Control

You can change the status of all doors in a site or doors in specific emergency operation groups to locked, unlocked, remaining locked, or remaining unlocked.

Note

Make sure you have grouped doors into an emergency operation group. See details in ***Add Emergency Operation Group*** .

In the top left corner of Home page, select ≡ → **All Modules** → **Access Control** → **Real-Time Monitoring** .

Control all or part of the doors in the current site.

Unlock

When a door is locked, if you unlock the door, it will be unlocked. When open duration is over, the door will be locked again automatically.

Click **Unlock / Temporary Access** → **All** to unlock all doors in the current site.

Click **Unlock / Temporary Access** → **Part** and select the emergency operation groups you want to unlock. Click **OK** to unlock the doors in the selected emergency operation groups.

Note

For details about setting the door's open duration, see ***Edit Door for Current Site*** .

Lock

When the door is unlocked, if you lock the door, it will be closed and locked. Person who has the access permission can access the door with credentials.

Click **Lock / Access with Credential** → **All** to lock all doors in the current site.

Click **Lock / Access with Credential** → **Part** and select the emergency operation groups that you want to lock. Click **OK** to lock the doors in the selected emergency operation groups.

Remain Unlocked

Doors will be unlocked. All persons can access the door with no credentials required (free access). This function is used when an emergency happens and all people are required to leave as quickly as possible, such as in a fire escape.

Click **Remain Unlocked / Free Access** → **All** and all doors in the current site will remain unlocked.

Click **Remain Unlocked / Free Access** → **Part** and select the emergency operation groups. Click **OK** and the doors in the selected emergency operation groups will remain unlocked.

Remain Locked

Door will be closed and locked. No person, except for the super users, can access the door even with authorized credentials. This function is applicable for situations such as preventing a theft in the building from getting away.

Click **Remain Locked / Access Forbidden** → **All** to lock down all the doors in the site.

Click **Remain Locked / Access Forbidden** → **Part** and select the emergency operation groups. Click **OK** and the doors in the selected emergency operation groups will remain locked.

Note

For setting person's super user privilege, refer to ***Manage Role and User*** .

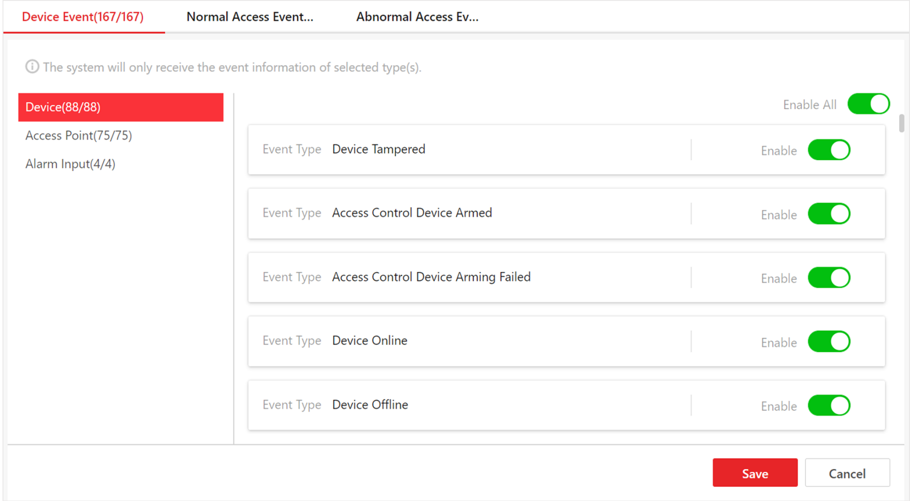
15.6 Subscribe for Device and Access Events

You can subscribe for device events and access events, so that when these events occur, you can see the real-time event records via the Web Client and Mobile Client.

Follow the steps to enable the subscription for device and access events.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **Access Control** → **Basic Settings** .
2. Click **Device Event Subscription** on the left.



ⓘ The system will only receive the event information of selected type(s).

Event Type		
Event Type	Device Tampered	Enable ●
Event Type	Access Control Device Armed	Enable ●
Event Type	Access Control Device Arming Failed	Enable ●
Event Type	Device Online	Enable ●
Event Type	Device Offline	Enable ●

Figure 15-14 Device and Access Event Subscription

3. Select an event category from **Device Event**, **Normal Access Event**, and **Abnormal Access Event**.
4. Switch on the event types to subscribe for these events.
5. **Optional:** Switch off the event types whose real-time event records you do not want to receive.

Note

If you switch off a event type, the Web Client and Mobile Client will no longer receive real-time event records of the event. However, you can still search for the device/access records via the Web Client. For details, see ***Search Access Records*** and ***Search Data Recorded on Device*** .

6. Click **Save** to save the settings.

What to do next

View the real-time event records of the device and access events that you subscribe for. For details, see ***View Real-Time Access Event*** .

15.7 Set User to Receive Access Control Calls

You can specify users to receive calls from the access control devices on the Control Client, and then the users can remotely perform the access control, such as remotely open door.

In the top left corner of Home page, select ≡ → **All Modules** → **Access Control** → **Basic Settings** → **Call Recipient Settings** .

Click **Add** to select user(s) to receive access control calls on the Control Client.

15.8 Search Access Records

You can search persons' access records triggered on specified access points via the Client by setting search conditions. For example, if you select specific access points and set the event type to access denied by card, you can get all access denied events (accessing by swiping a card) triggered on the access points.

Before You Start

Make sure you have configured access point event. See ***Add Event and Alarm***

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **Access Control** → **Access Control Retrieval** .
2. Select **Access Record Retrieval** on the left.
3. In the Time drop-down list, select the time during which the access records are generated.

   Note

   - You can click **Custom Time Interval** to set a precise start time and end time.

4. In the **Access Points** area, click ⊕ and select door(s) from the resource list.
5. In the **Record Type** area, click ⊕ to select record type(s).
6. In the **Access Result** drop-down list, select an access result type to quickly filter access granted records or access denied records.
7. Select **Person** or **Card No.** as the searching mode.
8. **Optional:** If you select **Person** as the searching type, select a person type.
9. If you select **Person** as the searching type, select a search mode.

   Select Person

   Select persons in the person list.

   Fuzzy Matching

   Enter a keyword to search persons whose information contains the keyword.

10. Find a person by selecting person, or fuzzy matching, or entering person card No. in the text box below.

11. Filter temperature status: Switch on **Skin-surface Temperature Status** and select a temperature status that you want to filter.
12. Filter mask wearing: Switch on **Wearing Mask or Not** and select **Wearing Mask** or **No Mask**.
13. Click **Search**.

    Matched access records are listed on the right.
14. **Optional:** Perform the following operations after searching access records.

    View Record Details

    Click the person name in the Name column to view the record details, such as the recorded video or captured picture of the related camera (if configured), person information, and access information.

    Filter Search Results by Person Type

    Click ▼ next to **Person** and select **Person** or **All** to filter the search results.

    Forgive Anti-Passback Violation

    When a person attempts to use a card out of anti-passback rule's sequence, the access will be denied. This is called "Anti-Passback Violation". When anti-passback violation occurs, no entry is allowed unless the anti-passback violation event is forgiven.

    You can forgive an anti-passback event by clicking ↺ in the Operation column. Or click **Forgive Anti-Passback** on the top to forgive all the anti-passback violation events in the search results.

    Export Single Record

    Click ⎘ in the Operation column to save a record as an excel file in your PC, including the event details, the person information, person profile, recorded video file (if configured), etc.

    Export All Searched Records

    Click **Export** to save the searched access records details (including person name, person ID, event time, access result, etc) in your PC as an excel or CSV file. If you select **Excel**, you can check **Export Picture** to save the captured pictures as well.

    Note

    - Up to 500 records can be exported each time.

15.9 Search Data Recorded on Device

Data recorded on device are records (e.g. triggered events/alarms, card-swiping records, etc.) stored in access control devices and video intercom devices. The records can be triggered by human behaviors detected by devices and events/alarms triggered by devices (such as device faults). You can search the records in different dimensions according to your needs.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **Access Control** → **Access Control Retrieval** .

2. Select **Device Recorded Data Retrieval** on the left.
3. In the Time drop-down list, select a time range for searching.

Note

You can click **Custom Time Interval** to set a precise start time and end time.

4. Switch on the resource types where you want to search records.

Access Points

Access points include doors of access control devices and video intercom devices). The records can be access records, operation records, and alarms triggered by human behaviors.

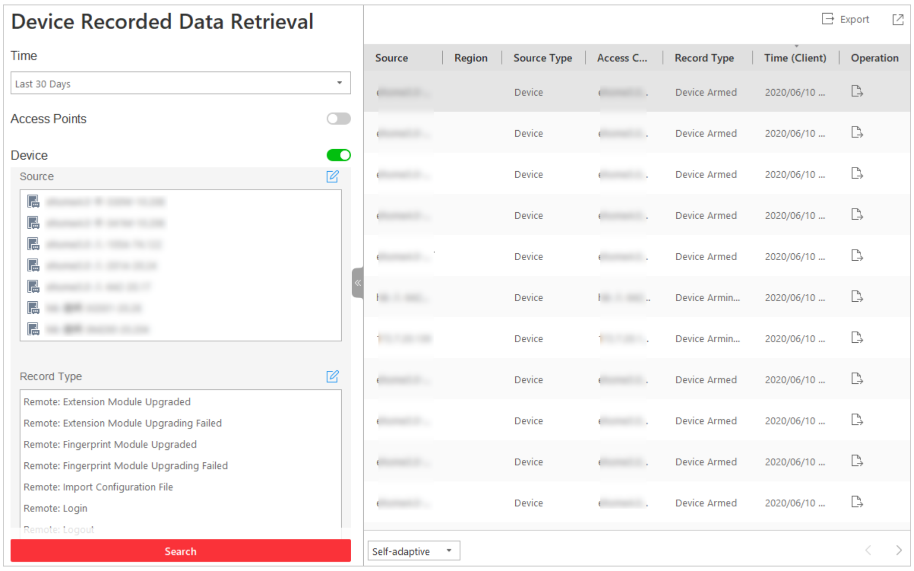
Device

Devices include access control devices and video intercom devices. The data recorded in these devices covers all events triggered by devices (such as device fault).

Alarm Input

The alarm inputs included in devices. The records are arming status changes.

5. Select record source and record type.
6. Click **Search**.



Device Recorded Data Retrieval

Time: Last 30 Days

Access Points ○

Device ●

Source

[redacted]

Record Type

Remote: Extension Module Upgraded
Remote: Extension Module Upgrading Failed
Remote: Fingerprint Module Upgraded
Remote: Fingerprint Module Upgrading Failed
Remote: Import Configuration File
Remote: Login
Remote: Logout

Source	Region	Source Type	Access C...	Record Type	Time (Client)	Operation
[redacted]		Device	[redacted]	Device Armed	2020/06/10 ...	🗋
[redacted]		Device	[redacted]	Device Armed	2020/06/10 ...	🗋
[redacted]		Device	[redacted]	Device Armed	2020/06/10 ...	🗋
[redacted]		Device	[redacted]	Device Armed	2020/06/10 ...	🗋
[redacted]		Device	[redacted]	Device Armed	2020/06/10 ...	🗋
[redacted]		Device	[redacted]	Device Armin...	2020/06/10 ...	🗋
[redacted]		Device	[redacted]	Device Armin...	2020/06/10 ...	🗋
[redacted]		Device	[redacted]	Device Armed	2020/06/10 ...	🗋
[redacted]		Device	[redacted]	Device Armed	2020/06/10 ...	🗋
[redacted]		Device	[redacted]	Device Armed	2020/06/10 ...	🗋
[redacted]		Device	[redacted]	Device Armed	2020/06/10 ...	🗋

Figure 15-15 Device Recorded Data Retrieval

7. **Optional:** Perform further operations on the searched records.

Export Single Record	Click 🗋 to save the record to the local disk as a CSV file.
Export All Searched Records	Click **Export** to save all the searched records to the local disk as an Excel or CSV file.

15.10 Perform Entry & Exit Counting

By grouping the doors (adding entry & exit counting group), the system provides counting functions based on the entry and exit records on these doors. With this function, you can check who enters/exits this region and how many persons still stay in this region. The function is applicable for certain emergency scene. For example, during a fire escape, all people are required to exit the region.

Before You Start

Make sure you have added entry & exit counting groups to group the doors. See ***Add Entry and Exit Counting Group*** .

Steps

Note

Currently, the platform only supports searching persons with access records in the last 24 hours.

1. In the top left corner of Home page, select ≡ → **All Modules** → **Access Control** → **Access Control Retrieval** .
2. Select **Entry & Exit Counting** on the left.
3. In the **Source** list, select an entry & exit counting group.
4. In the **Entry & Exit Counting Type** drop-down list, select the type of persons you want to search.

   All

   All the entering and exiting access records in the last 24 hours will be listed.

   People Stayed

   Persons who are still staying in the region will be listed. The system filters the persons whose entering record is found but exiting record is not found.

   People Exited

   Persons who entered and exited the region afterward will be listed.
5. Click **Search**.

   All matched access records will be listed, showing information such as person details, location of last access, etc.
6. **Optional:** Perform further operations after searching.

   View Event Details
   Click the person name in the Name column to view the record details, including the recorded video of the access point's related camera (if configured), person information, and access information.

   Export Single Record
   Click 📄 in the Operation column to download the record, including the person information, person profile, phone number, location of last access, etc.

Export All Searched Records	Click **Export** in the upper-right corner to export the searched access control events details (including the person information, person profile, phone number, location of last access, etc.). **Note** Up to 100,000 records can be exported each time.

Chapter 16 Manage Vehicle

HikCentral Professional also provides parking service: managing the vehicles access in and out of a parking facility. The system can open the barrier gate at the entrance and exit of the parking facility according to the entry & exit rules you set.

On the Web Client, you need to create a parking lot and set its entrances and exits as well as lanes according to the actual needs. Meanwhile, you need to import the vehicle information to the system first and categorize them into different vehicle lists if needed, so that you can predefine entry & exit rules for these vehicles. For the vehicles not managed in the system, you can also set an entry & exit rule to define how to open the barrier when these vehicles are detected at the entrances and exits. On the Entrance and Exit Overview page, you can view the health status of parking lot, parking space statistics, vehicle passing statistics, and vehicle passing event. Besides, you can jump to different page according to your need.

16.1 Flow Chart

The following flow chart shows the process of the configurations and operations of vehicle.

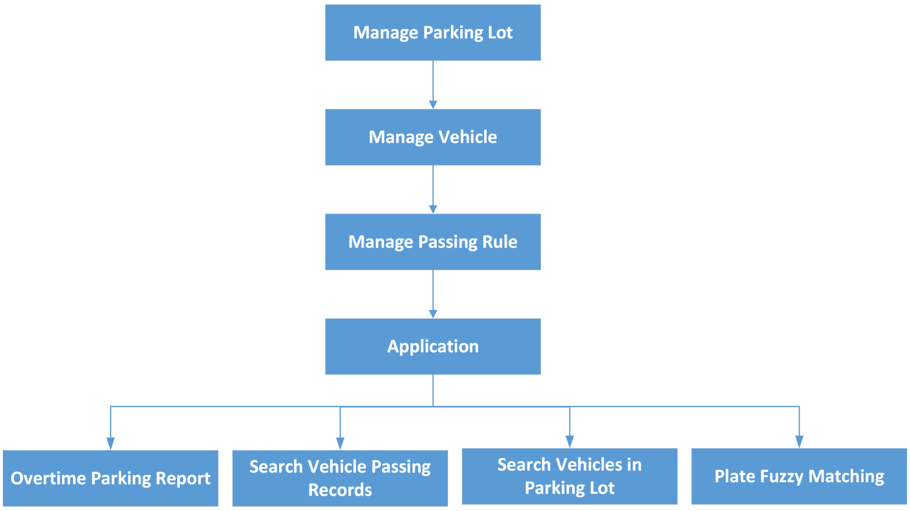


Figure 16-1 Flow Chart of Managing Vehicle

- **Parking Lot Management**: Parking lot is a parking facility that is intended for parking vehicles. You need to create a parking lot in the system and set its entrances and exits as well as lanes according to actual needs.
- **Vehicle Management**: On the Web Client, the administrator can add vehicle information to the system, and set events and alarms to define whether an event or alarm will be triggered when the recognized plate number matches or mismatches with the license plate numbers of the vehicles managed in the system, or whether an event or alarm will be triggered when the recognized vehicle type matches the specified vehicle type. For entrance and exit control, the

administrator can set entry & exit rules for the vehicles managed in the system to define whether to allow the vehicles to enter or exit the parking lot.

- **Passing Rule Management**: An entry & exit rule defines how to open barrier when the system detects a vehicle at the lane. The system can open the barrier automatically when detects a vehicle, or you can also open it manually by clicking **Allow** button on the Control Client after verifying its identity.
- **Application**: After completing the above-mentioned configurations, you can perform operations including sending overtime parking lot regularly, searching vehicle passing records, searching vehicles in parking lot, and license plate fuzzy searching.

16.2 Manage Parking Lot

Parking lot is a parking facility that is intended for parking vehicles. You need to create a parking lot in the system and set its entrances and exits as well as lanes according to actual needs.

There are three elements in the parking system:

Parking Lot

A parking facility that is intended for parking vehicles. The system only supports one parking lot and you need to create it in the system at the very beginning.

Entrance & Exit

The vehicles can enter or exit the parking lot via entrance & exit.

Lane

Each entrance & exit should contain at least one lane. The lane can be linked with a capture unit, an access control device, or a video intercom device, which can be used for capturing and recognition, identity verification, video intercom, as well as controlling barrier to open or close. You can also mount one LED screen at the lane and link it with the lane to display information such as entering/exiting time, number of available parking spaces, etc.

The two pictures below shows the typical relation of parking lot, entrances & exits, and lanes.

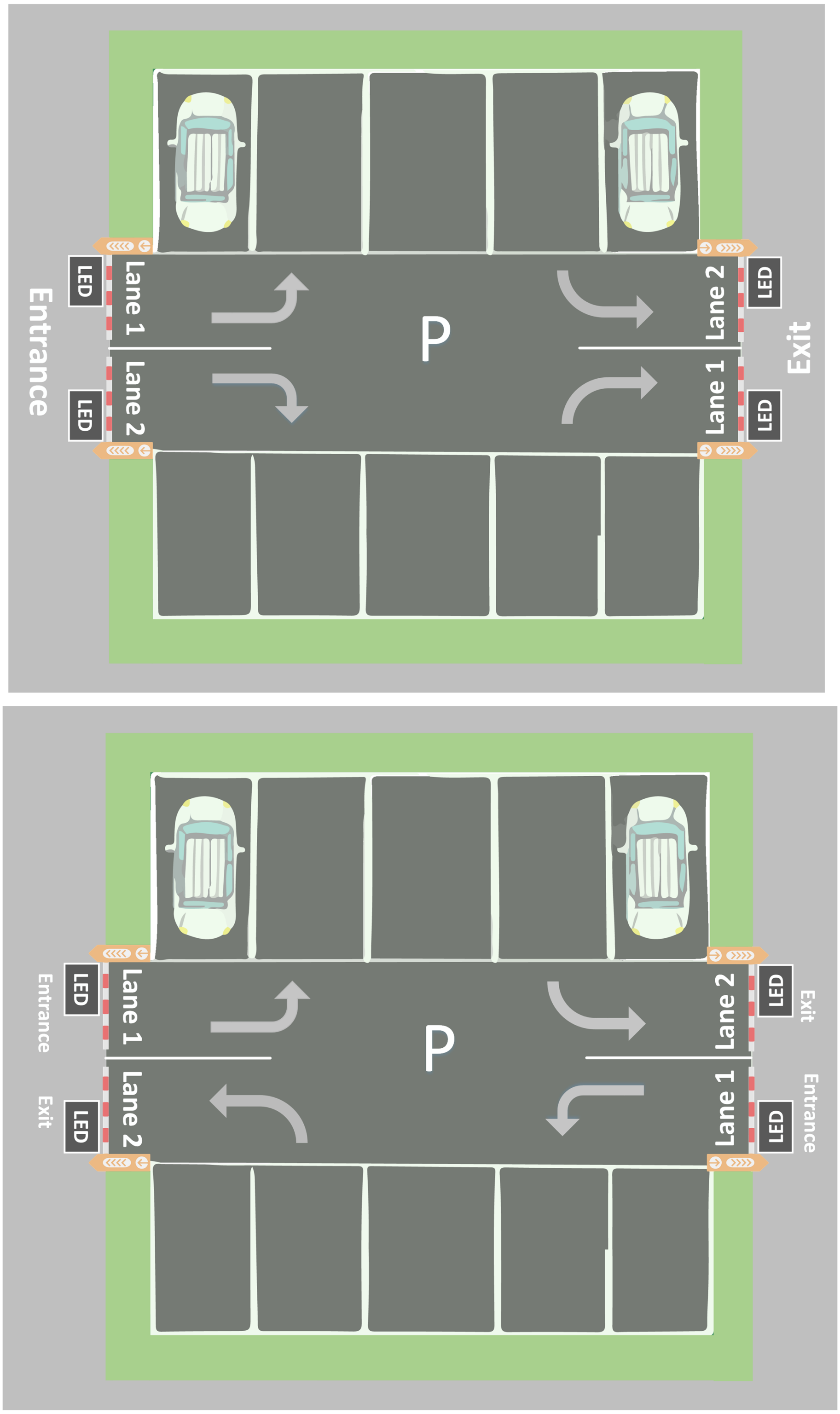


Figure 16-2 Parking Lot

16.2.1 Add Parking Lot

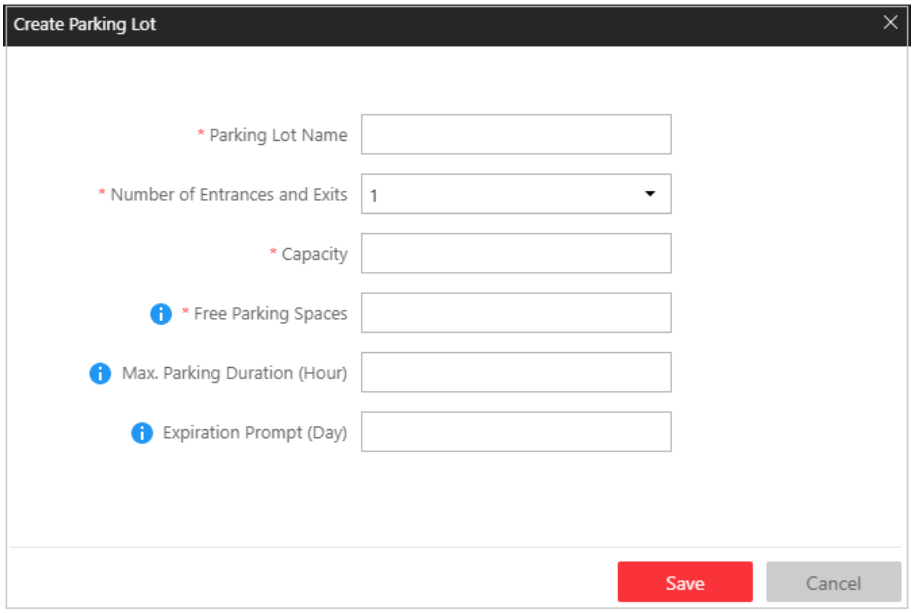
You can add a parking lot for management of vehicle entering and exiting.

Steps

Note

Only one parking lot can be added and the parking lot cannot be deleted once added.

1. In the top left corner of Home page, select ≡ → **All Modules** → **Vehicle** → **Parking Lot Settings** .
2. Click **Create Parking Lot** to open the Create Parking Lot window.



Create Parking Lot

* Parking Lot Name

* Number of Entrances and Exits: 1

* Capacity

* Free Parking Spaces

Max. Parking Duration (Hour)

Expiration Prompt (Day)

Figure 16-3 Create Parking Lot Window

3. Enter the parking lot information.

   Number of Entrances and Exits

   The amount of entrances and exits of the created parking lot.

   Capacity

   The total number of parking spaces in the created parking lot.

   Vacant Parking Spaces

   Amount of parking spaces without parked vehicles.

   Max. Parking Duration (Hour)

   The maximum parking duration of a car parked in the created parking lot. You can configure an event or alarm which will be triggered when a vehicle's parking is due. For example, you enter 12, an event or alarm (if any) will be triggered if a vehicle has parked for more than 12 hours.

Expiration Prompt (Day)

Take a vehicle which expires at Jan. 6th, 2020 as an example, if you enter 5, the expiration prompt will be displayed on the LED screen linked to the parking lot from Jan. 1st, 2020 to Jan. 5th, 2020.

4. Click **Save** to create the parking lot.
5. **Optional:** Edit parking lot information.
   1) Click ✎ beside the parking lot name to open the Edit Parking Lot window.
   2) Edit the parking lot name/capacity/vacant parking spaces/Max. parking duration/expiration prompt.

      Example

      Vacant Parking Spaces: if the vacant parking space amount is not the same with the actual amount, you can edit it here.
   3) Click **Save**.

16.2.2 Add Entrance and Exit

An entrance or exit helps control vehicles to enter/exit the parking lot or prevent vehicles from entering/exiting the parking lot. For example, the entrance or exit allows a vehicle in the VIP list to enter/exit the parking lot, and prevent a vehicle in the blocklist from entering the parking lot. You need to configure lanes linked with devices for an entrance and exit to control the barriers.

Before You Start
Make sure you have added a parking lot. See ***Add Parking Lot*** for details.

Steps
1. In the top left corner of Home page, select ≡ → **All Modules** → **Vehicle** → **Parking Lot Settings** .
2. Click **+** on the top left.
3. Enter the entrance and exit name.
4. Click **Save**.

What to do next
Add lane for the entrance and exit. See ***Add Lane*** for details.

16.2.3 Add Lane

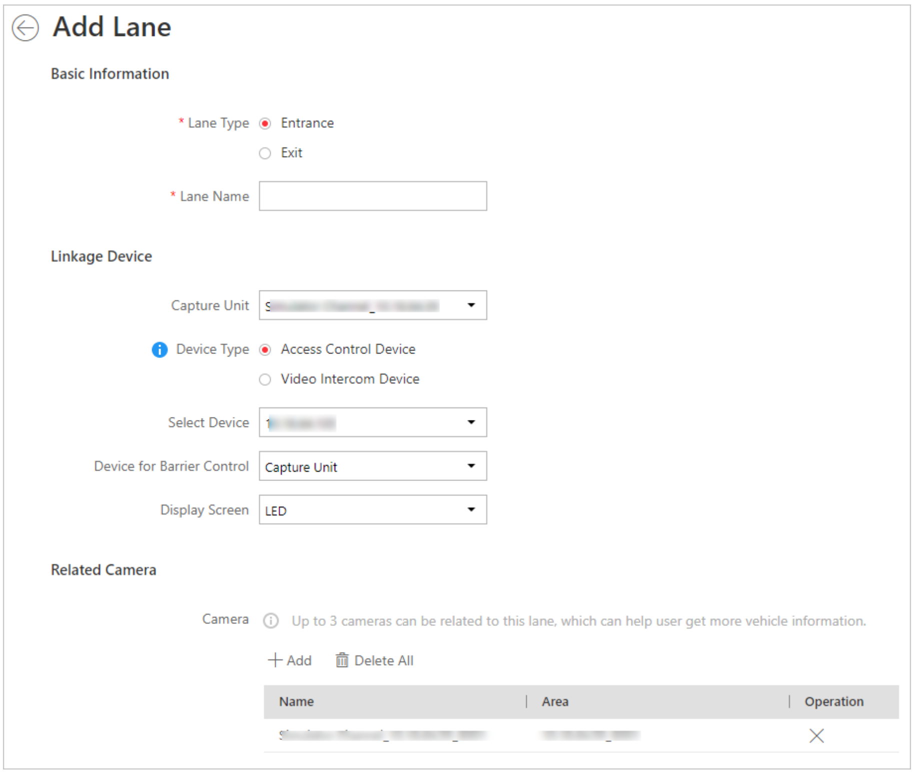
A lane linked with a capture unit or card-swiping device is used for controlling the barrier. A capture unit linked to a lane can recognize a vehicle at the lane, and compare the vehicle information with vehicles in a vehicle list. Then, the capture unit opens the barrier automatically to allow the vehicle to enter/exit according to entry and exit rule of the vehicle list if the vehicle has been added to a vehicle list. An access control device/video intercom device opens the barrier when a vehicle owner swipes card on it to open the barrier to allow the vehicle to enter or exit the parking lot. Meanwhile, the capture unit does not open the barrier for the recognized license plate number which is added to the blocklist; the access control device/video intercom device cannot control the barrier without swiping a card specialized for the parking lot. You can also relate a camera with the lane. The camera will capture a picture (it can be a vehicle, human face, or other) which will be displayed on the Control Client. You can view the pictures captured by the related camera on the Control Client if needed.

Before You Start

- Make sure you have added at least an entrance/exit for the parking lot.
- You may need to have added a capture unit to the system for barrier control.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **Vehicle** → **Parking Lot Settings** .
2. Select an entrance or exit on the left.
3. Click + to enter the Add Lane page.
4. Select the lane type as **Entrance** or **Exit**.
5. Enter the lane name.



Add Lane

Basic Information

* Lane Type ● Entrance ○ Exit

* Lane Name

Linkage Device

Capture Unit [redacted]

Device Type ● Access Control Device ○ Video Intercom Device

Select Device [redacted]

Device for Barrier Control Capture Unit

Display Screen LED

Related Camera

Camera Up to 3 cameras can be related to this lane, which can help user get more vehicle information.

+ Add Delete All

Name	Area	Operation
[redacted]	[redacted]	×

Figure 16-4 Add Lane Page

6. **Optional:** Configure linked devices for the lane.
   1) Select a capture unit in the drop-down list.

Note

A capture unit is used for capturing and recognizing license plate number. For example, the capture unit will open the barrier to allow the vehicle to enter the parking lot when recognizing a license plate number in the vehicle list, and will not open the barrier to prevent the vehicle from entering the parking lot when recognizing a license plate number in the blocklist. See ***Manage Entry & Exit Rule*** for details about setting an entry & exit rule.

2) Select **Access Control Device** or **Video Intercom Device** as the **Device Type**.
3) Select a device for swiping card or video intercom from the **Select Device** drop-down list, or click **Add New** to add a device to the system.

Access Control

If you selected a card (already issued to the owner for card authentication) for the owner when adding a vehicle, you actually bind the card with the vehicle license plate number. So the barrier will open when you swipe the card at the lane with an access control/video intercom device. In this circumstance, a capture unit is not needed.

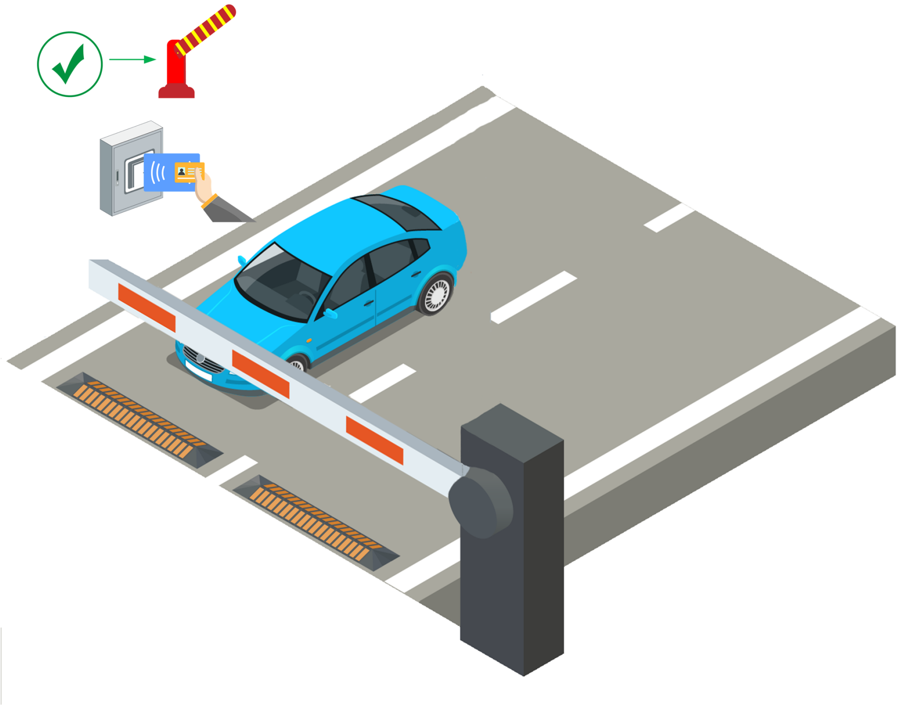


Figure 16-5 Opening Barrier by Card Swiping

Video Intercom

a. The vehicle owner calls the security guard by the video intercom device (some access control devices can also be used for video intercom).
b. The security guard verifies the owner's identity by viewing her/him by the video intercom device or license plate number captured by a capture unit.
c. The security guard opens the barrier manually if the vehicle owner is authenticated.

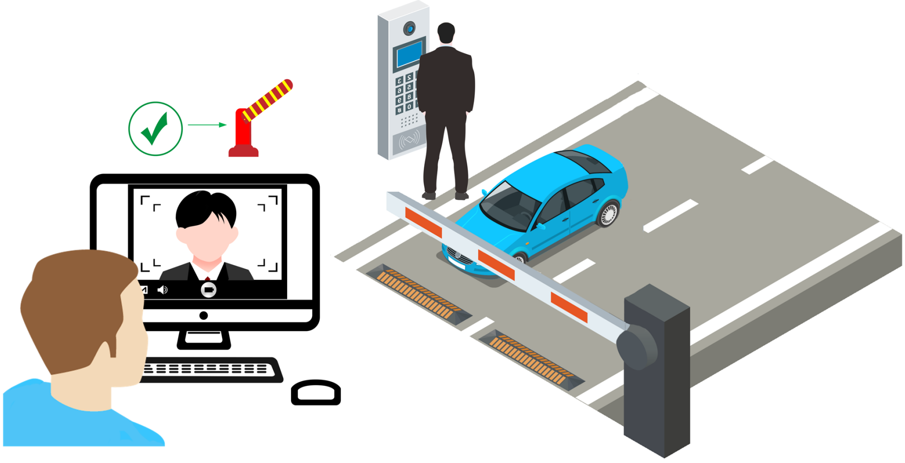


Figure 16-6 Opening Barrier by Video Intercom

4) Select a display screen for the lane.

Note

A display screen is used for displaying information such as free parking space amount, vehicle expiration date. See ***Set Contents Displayed on Display Screen*** for details.

5) Select either **Capture Unit** or **Access Control /Video Intercom Device** selected by the above step as the device for barrier control.

7. Relate the lane with camera(s).

Note

- Make sure you have enabled picture storage for the camera. Otherwise, you cannot see the captured pictures on the Control Client. See ***Manage Area*** for details about how to enable picture storage for a camera.
- Up to three different cameras can be related with the lane.
- One camera can be related with multiple lanes.
- You can view the pictures captured by the related camera in the passing vehicle information on the Control Client.

1) Click **Add** to open the resource list.
2) Select a camera from the resource list.
3) Click **Add** to save the related camera.

8. Click **Add**.

16.2.4 Set Contents Displayed on Display Screen

A display screen linked to the lane can be used for displaying date and time, parking duration, plate number, and expiration prompt.

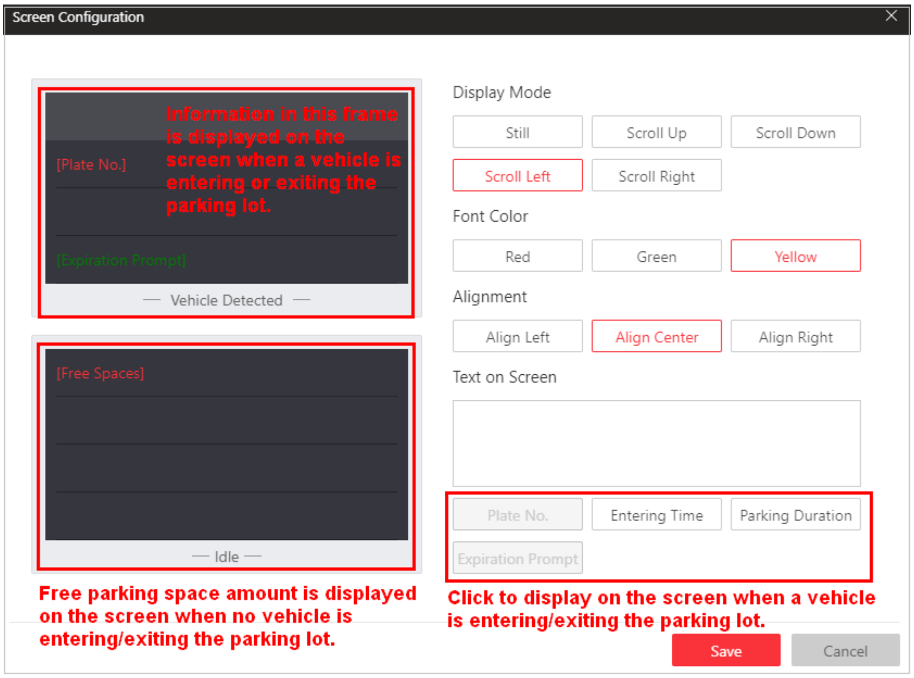
Before You Start

Make sure you have linked a display screen to a lane. See ***Add Display Screen*** for details about how to add a display screen.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **Vehicle** → **Parking Lot Settings** .
2. Select an entrance or exit in the Entrance and Exit list.

   The display screen linked to the entrance/exit is displayed in the entrance/exit area.
3. Click ✎ beside the display screen name to open the Screen Configuration window.



Information in this frame is displayed on the screen when a vehicle is entering or exiting the parking lot.

Free parking space amount is displayed on the screen when no vehicle is entering/exiting the parking lot.

Click to display on the screen when a vehicle is entering/exiting the parking lot.

Figure 16-7 Screen Configuration Window

4. Click the four different lines in the**Vehicle Detected** screen and select information type under the **Text on Screen** frame. You can display **Plate No./Entering Time/Parking Duration/Expiration Prompt** on the screen.

   Plate No.

   Used for displaying license plate number recognized by the capture unit. Click to add it to the **Text on Screen** area.

   Entering Time

   The time when a recognized vehicle enters the parking lot.

Parking Duration

The duration (exiting time minus entering time) a vehicle parked for. Click to add it to the **Text on Screen** area and enter a number as required.

Expiration Prompt

Inform the vehicle owners that their vehicles are about to expire. You need to enable the expiration prompt for a parking lot and set when to inform vehicle owners the expiration date. See ***Add Parking Lot*** for details.

5. Click each different line in the **Vehicle Detected** screen and select display mode, font color, and alignment for information in each line.
6. Click a line in the **Idle** screen and click **Free Spaces**, and the free spaces amount will be displayed in the selected line when there is no vehicle detected at the lane.
7. Click the line displaying free spaces and select a display mode, font color, and alignment for it.
8. Click **Save** to save the screen settings.

16.3 Manage Vehicle

HikCentral Professional provides ANPR (Automatic Number-Plate Recognition) functions. After adding cameras which support ANPR, the cameras can recognize the license plate number of the detected vehicles. The system also provides entrance and exit management and it can control the entry and exit of the detected vehicles.

On the Web Client, the administrator can add vehicle information to the system, and set events and alarms to define whether an event or alarm will be triggered when the recognized plate number matches or mismatches with the license plate numbers of the vehicles managed in the system, or whether an event or alarm will be triggered when the recognized vehicle type matches the specified vehicle type. For entrance and exit control, the administrator can set entry & exit rules for the vehicles managed in the system to define whether to allow the vehicles to enter or exit the parking lot.

16.3.1 Add Vehicle List

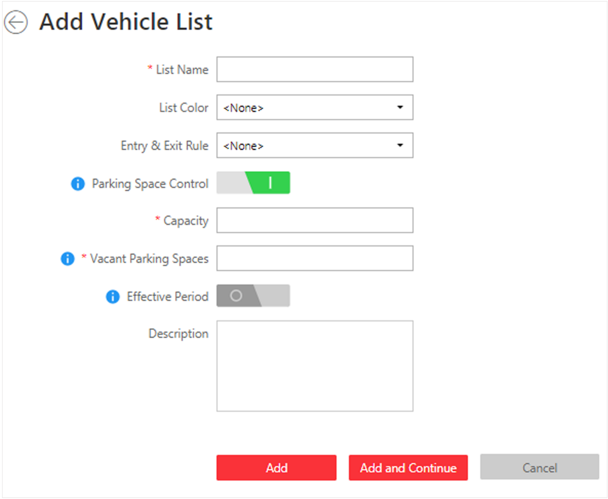
To add vehicle information to the system, you should create a vehicle list first. When you are adding a vehicle list, you configure an entry & exit rule (when and how to open the barrier for entry & exit), set parking space information, and effective period for it. Vehicle list helps you manage the different vehicles. For example, you add a list for VIP vehicles that enjoy certain privileges, or add a blocklist in which vehicles will not be allowed to enter/exit the parking lot.

Steps

Note

Up to 100 vehicle lists can be added to the system.

1. On the top left corner of Home page, select ≡ → **All Modules** → **Vehicle** → **Vehicle Management** .
2. On the top left, click + to enter the add vehicle list page.



Add Vehicle List

* List Name

List Color <None>

Entry & Exit Rule <None>

Parking Space Control

* Capacity

* Vacant Parking Spaces

Effective Period

Description

Figure 16-8 Add Vehicle List Page

3. Set a descriptive name for the vehicle list.
4. **Optional:** Select a color for the vehicle list, and the color will be displayed with the list name.

Note

The color can be used for marking different vehicle list type.

5. **Optional:** Select an entry & exit rule for the vehicle list, or create a new rule for the vehicle list.

   Entry & Exit Rule

   An entry & exit rule defines how to open barrier when the system detects a vehicle at the lane. The system can open the barrier automatically when detects a vehicle, or you can also open it manually by clicking **Allow** button on the Control Client after verifying its identity. If you set **Automatic**, you need to define when the barrier gate will open automatically.

6. **Optional:** Enable and configure parking space control.

   Example

   Company A and company B share the same parking lot of 1000 parking spaces, and each company has 500 parking spaces. So you can add vehicle list A and B for them respectively, and set the capacity as 500 for each of them. When there is no vacant parking space of company A and a visitor of company A needs to park at the parking lot, you can manually allow the vehicle to enter (this function is called Advanced Opening Barrier Gate) and give a parking space of company B to the vehicle for a temporary parking. See *User Manual of HikCentral Professional Control Client* for details about Advanced Opening Barrier Gate.

   1) Switch on **Parking Space Control**.
   2) Enter the capacity and vacant parking spaces of the parking lot.

Note

Vehicles will not be allowed to enter the parking lot if there is no vacant parking space. You can open the barrier manually on the Control Client to allow the vehicles to enter the parking lot.

7. **Optional:** Enable **Effective Period** and set the effective period for the vehicle list. Vehicles in the list will not be allowed to enter the parking lot when the vehicle list expired.

   Note

   When you are adding a vehicle to this list later, you do not need to set an effective period for the vehicle, because the vehicle shares the same effective period with its list.

8. Click **Add** to add the vehicle list, or click **Add and Continue** to add the current vehicle list and start adding another vehicle list.

   The added vehicle list will be displayed on the left of the Vehicle page.

9. **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	Select a vehicle list and click 🗑 to delete it, or press **Ctrl** on your keyboard and select multiple vehicle lists and then click 🗑 to delete the vehicle lists in a batch.

16.3.2 Add Vehicle Information

After adding the vehicle list, you can add vehicle information to the list.

You can import the vehicle information in a batch, or add the vehicle information manually.

Note

Each vehicle list can contain up to 5,000 vehicles.

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.

Steps

Note

Each vehicle list can contain up to 5,000 vehicles.

1. In the top left corner of Home page, select ≡ → **All Modules** → **Vehicle** → **Vehicle Management** .
2. Select a vehicle list in the left column.
3. Click **Import** to open the Import window.

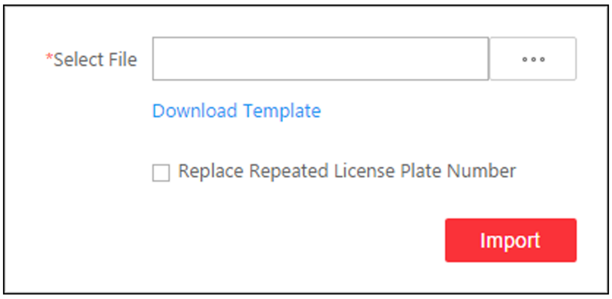


Figure 16-9 Import Window

4. Click **Download Template** on the Import window to save the template file 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.
Delete All Vehicle Information	Click ⌄ beside the **Delete** icon, and click **Delete All** to delete all vehicle information from the current vehicle list.
Delete Expired Vehicle Information	Click **Delete Expired Vehicle** to delete all expired vehicle information from the current vehicle list.
Move Vehicle to Other Vehicle List	Check one or more vehicle, and then click **Move**. Select a vehicle list and click **OK** to move the checked vehicles to the selected vehicle list.
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.

Manually Add Vehicle Information

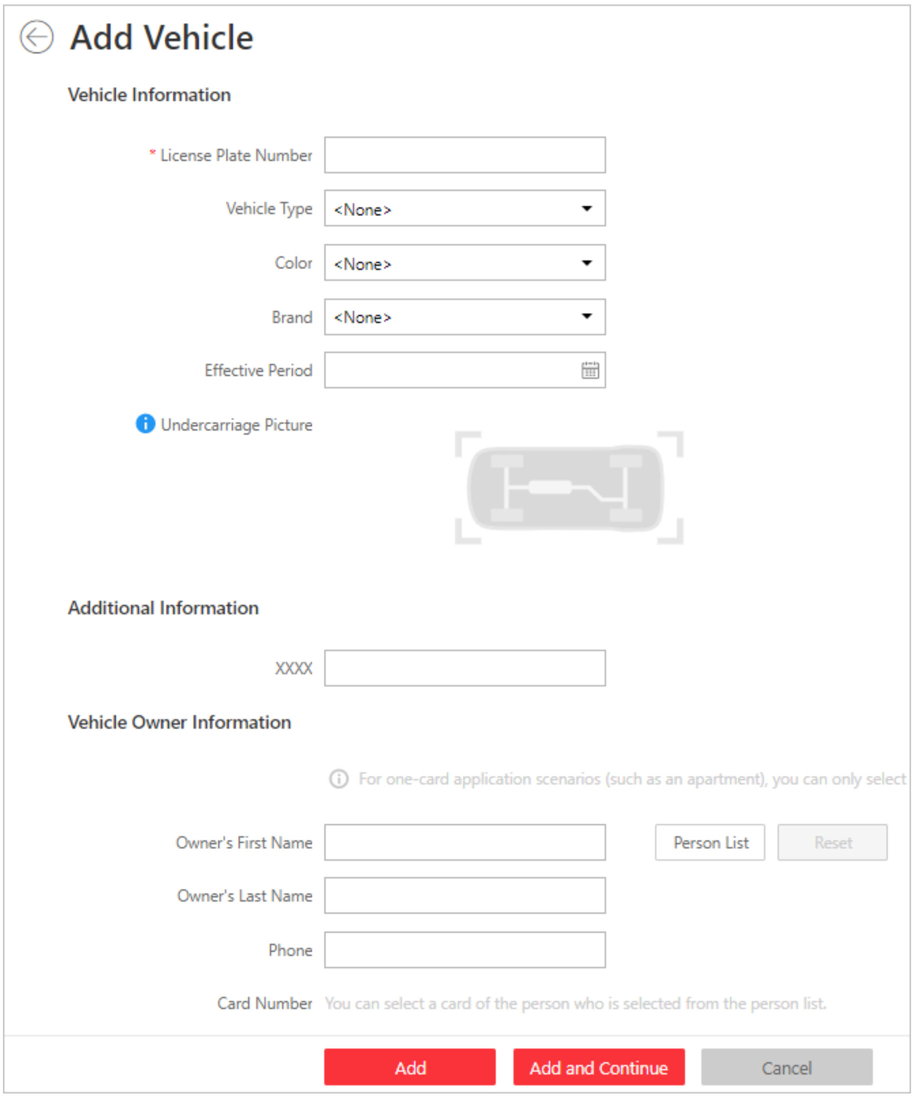
You can add single vehicle information manually.

Before You Start

You should add the vehicle list before you can add the vehicle information. Refer to ***Add Vehicle List*** for details.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **Vehicle** → **Vehicle Management** .
2. Select a vehicle list in the left column.
3. Click **Add** to enter the adding vehicle page.



Add Vehicle

Vehicle Information

* License Plate Number

Vehicle Type <None>

Color <None>

Brand <None>

Effective Period

Undercarriage Picture

Additional Information

XXXX

Vehicle Owner Information

For one-card application scenarios (such as an apartment), you can only select

Owner's First Name

Owner's Last Name

Phone

Card Number You can select a card of the person who is selected from the person list.

Figure 16-10 Add Vehicle Page

4. Set vehicle information.

1) Enter the license plate number, vehicle type, color, and brand.
2) **Optional:** Set the effective period for this vehicle if you did not set effective period for the vehicle list.

   Note

   If you have configured an effective period for the vehicle list to add this vehicle to, the added vehicle shares the same effective period with the vehicle list, and this function will be unavailable.

   Expired license plate number neither triggers any event or alarm when license plate number matched if license plate number matched event/alarm is configured, nor be allowed to enter or exit a parking lot.
3) **Optional:** Upload an undercarriage picture for this vehicle.
   a. Move the cursor to the image area and click **Upload**.
   b. 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.

5. Set the additional information for the vehicle.

   Note

   You can customize the name and type of additional information. See ***Custom Additional Information*** for details.

6. **Optional:** Enter the owner's name and phone number, or Select a person in the person list as a vehicle owner as the following steps.
   1) Click **Person List** to open the Select Person panel.

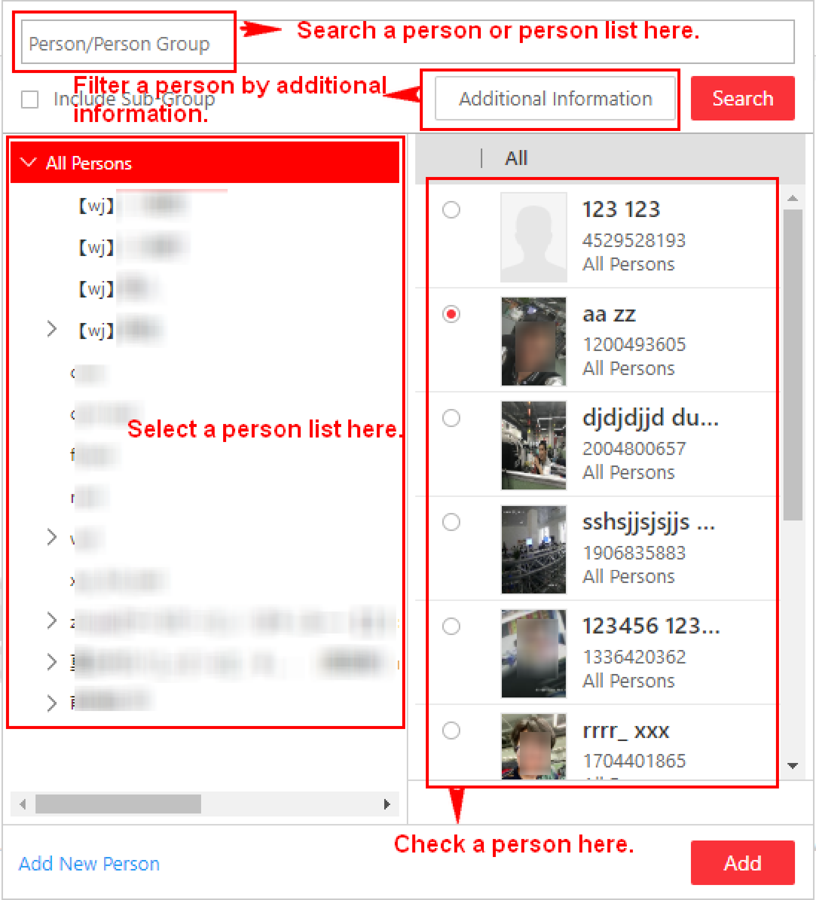


Figure 16-11 Add Person in Person List as Vehicle Owner

2) Select a person list on the left, or you can enter a person list name on the top to search it.
3) Check a person in the selected person list, or enter a person name on the top to search her/him, or click **Additional Information** to filter a person by additional information, or click **Add New Person** to add a new person.
4) Click **Add**.
5) **Optional:** Select a card number for the owner in the **Card Number** drop-down list which contains all the cards of the owner. The owner can swipe the selected card on the access control device or video intercom device linked to the lane to control the barrier for entrance/exit.

7. 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.

8. **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.

Delete All Vehicle Information
Click ⌄ beside the **Delete** icon, and click **Delete All** to delete all vehicle information in the current vehicle list.

Delete Expired Vehicle Information
Click **Delete Expired Vehicle** to delete all expired vehicle information from the current vehicle list.

Move Vehicle to Other Vehicle List
Check one or more vehicle, and then click **Move**. Select a vehicle list and click **OK** to move the checked vehicles to the selected vehicle list.

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.

16.3.3 Custom Additional Information

You can customize the additional information items which are not pre-defined in the basic information according to your actual needs.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **Vehicle** → **Vehicle Management** .
2. Select a vehicle list in the left column.
3. Click **Custom Additional Information**.
4. Click **Add**, and then enter the title and select the type for the additional information.

   General Text

   0 to 128 characters are allowed except certain special characters.

   Number

   Only digits are allowed. And up to 32 digits are allowed.

   Date

   Select a data from the calendar.

   Single Selection

You need to set options for the information. When adding a vehicle, you select from the options.

5. Click **Save**.
6. **Optional:** Perform the following operations if you need.

Edit Additional Information	Select an additional information, and click ✎ to edit the additional information's title and type.
Delete Additional Information	Select an additional information, and click × to delete it.

16.4 Manage Entry & Exit Rule

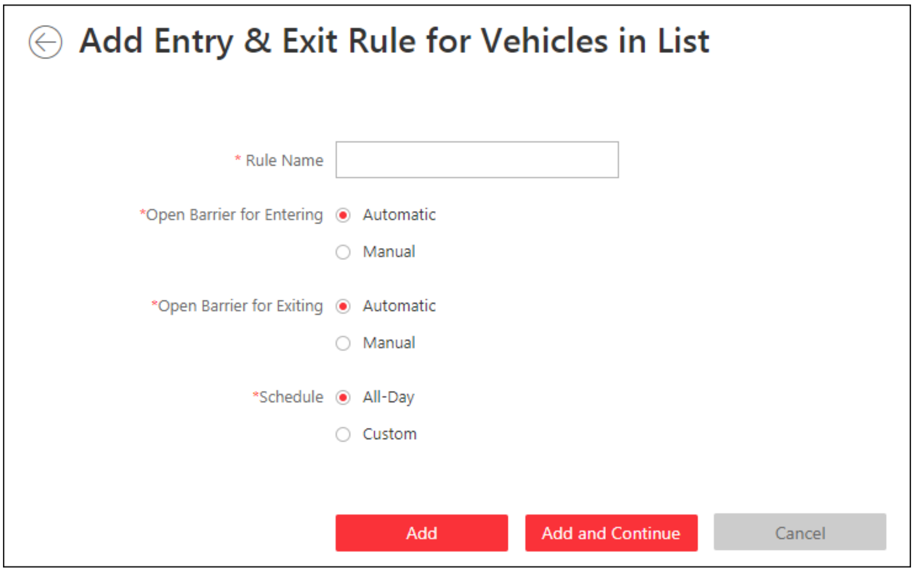
An entry & exit rule defines how to open barrier when the system detects a vehicle at the lane. The system can open the barrier automatically when detects a vehicle, or you can also open it manually by clicking **Allow** button on the Control Client after verifying its identity.

You can set entry & exit rules for vehicles in the vehicle lists and temporary vehicles which are not in any vehicle lists.

16.4.1 Set Entry & Exit Rule for Vehicles in Vehicle List

For vehicles managed in the system, you can set entry & exit rules for them to define whether and when the barrier gate of the entrance and exit will open automatically. You need to define an entry & exit rule first and then assign it to one vehicle list when adding a vehicle list.

In the top left corner of Home page, select ≡ → **All Modules** → **Vehicle** → **Entry & Exit Rule** → **Rule for Vehicles in List** . Click **Add** to add an entry & exit rule for vehicles in vehicle list.



Add Entry & Exit Rule for Vehicles in List

* Rule Name

*Open Barrier for Entering ● Automatic ○ Manual

*Open Barrier for Exiting ● Automatic ○ Manual

*Schedule ● All-Day ○ Custom

Figure 16-12 Set Entry & Exit Rule for Vehicles in Vehicle List

Rule Name

Create a name for the rule.

Open Barrier for Entering

Set whether the barrier gate of the entrance lane will open automatically when detecting a vehicle which is in the linked vehicle list.

Automatic

The barrier gate of the entrance lane will open automatically when detecting a vehicle which is in the vehicle list linked with this entry & exit rule.

For example, if the vehicle list is a list for VIP vehicles, you can set to open the barrier gate automatically when detecting a vehicle in the VIP list.

Manual

The barrier gate of the entrance lane will not open automatically.

For example, if the vehicle list is a "blocklist" for vehicles that are not allowed to enter the parking lot, you can set it as **Manual**.

Open Barrier for Exiting

Set whether the barrier gate of the exit lane will be open automatically when detecting a vehicle which is in the linked vehicle list.

Automatic

The barrier gate of the exit lane will open automatically when detecting a vehicle which is in the vehicle list linked with this entry & exit rule.

For example, if the vehicle list is a list for VIP vehicles, you can set to open the barrier gate automatically when detecting a vehicle in the VIP list.

Manual

The barrier gate of the exit lane will not open automatically.

For example, if the vehicle list is a "blocklist" for vehicles that are not allowed to exit the parking lot, you can set it as **Manual**.

Schedule

If you set **Automatic** in the above settings, you need to define when the barrier gate will open automatically.

All-Day

Whenever the system detects a vehicle in the vehicle list linked with the entry & exit rule, the barrier gate will open automatically.

Custom

Drag or click on the time bar to draw the time periods when the barrier can open automatically.

Note

Up to 4 time periods can be set for each day.

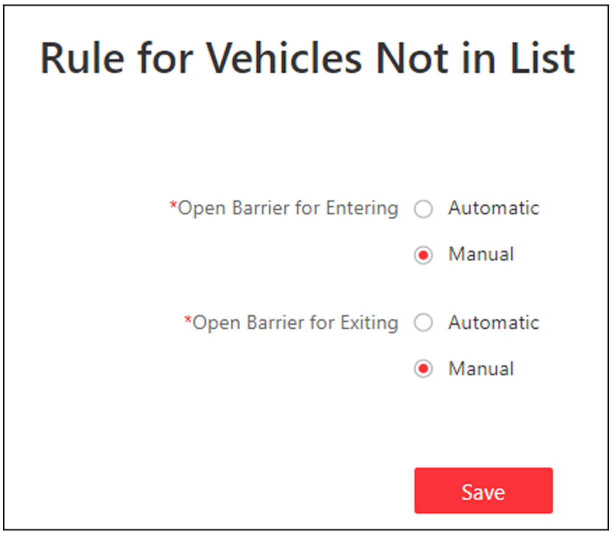
You can click **Erase** and click on the drawn time period to clear the corresponding drawn time period.

After adding an entry & exit rule for the vehicles in the vehicle list, you need to assign one rule for each vehicle list. For details, refer to ***Add Vehicle List*** .

16.4.2 Set Entry & Exit Rule for Vehicles Not in Vehicle List

For vehicles not managed in the system, you can also set an entry & exit rule for them to define whether the barrier gate of the entrance and exit will open automatically. For example, when a visitor wants to enter the parking lot to park her/his vehicle, the system detects that this license plate number is not in any vehicle lists in the system. If you set to manually open the barrier for the vehicles not in the vehicle list, the barrier gate will not open automatically. The security personnel needs to verify her/his identity and judge whether to allow it to enter the parking lot.

In the top left corner of Home page, select ≡ → **All Modules** → **Vehicle** → **Entry & Exit Rule** → **Rule for Vehicles Not in List** .



Rule for Vehicles Not in List

*Open Barrier for Entering ○ Automatic ● Manual

*Open Barrier for Exiting ○ Automatic ● Manual

Figure 16-13 Set Entry & Exit Rule for Vehicles Not in List

Open Barrier for Entering

Set whether the barrier gate of the entrance lane will open automatically when detecting a vehicle which is not in any vehicle lists.

Automatic

The barrier gate of the entrance lane will open automatically when detecting a vehicle which is not in any vehicle lists

Manual

The barrier gate of the entrance lane will not open automatically.

Open Barrier for Exiting

Set whether the barrier gate of the exit lane will be open automatically when detecting a vehicle which is not in any vehicle lists.

Automatic

The barrier gate of the exit lane will open automatically when detecting a vehicle which is not in any vehicle lists.

Manual

The barrier gate of the exit lane will not open automatically.

16.5 Send Overtime Parking Report Regularly

You can set a regular overtime parking report rule for the parking lot added to the system, and the system can send an email with a report attached to the target recipients daily, weekly, or monthly, showing the records of overtime parking vehicles detected by 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*** .
- Make sure the parking lot has been added to the system. For details, refer to ***Add Parking Lot*** .

Steps

Note

- One report can contain up to 10,000 records in total.
- The report will be an Excel file.

1. In the top left corner of Home page, select ≡ → **All Modules** → **Vehicle** → **Overtime Parking Report** .
2. Click **+** to enter the Create Report page.
3. Create a name for the report.
4. 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 records of overtime parking 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 records of overtime parking 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 the records of overtime parking vehicles detected between last Monday and Sunday.

5. 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*** .

6. Select the **Report Language**.
7. Click **Add** to add the report and go back to the report list page.

16.6 Search Vehicle Passing Records

If the added Automatic Number-Plate Recognition (ANPR) camera and entrance and exit are properly configured, and the vehicle license plate number is recognized by the cameras or capture units linked to the entrance and exit, you can search the related vehicle passing information.

Steps

Note

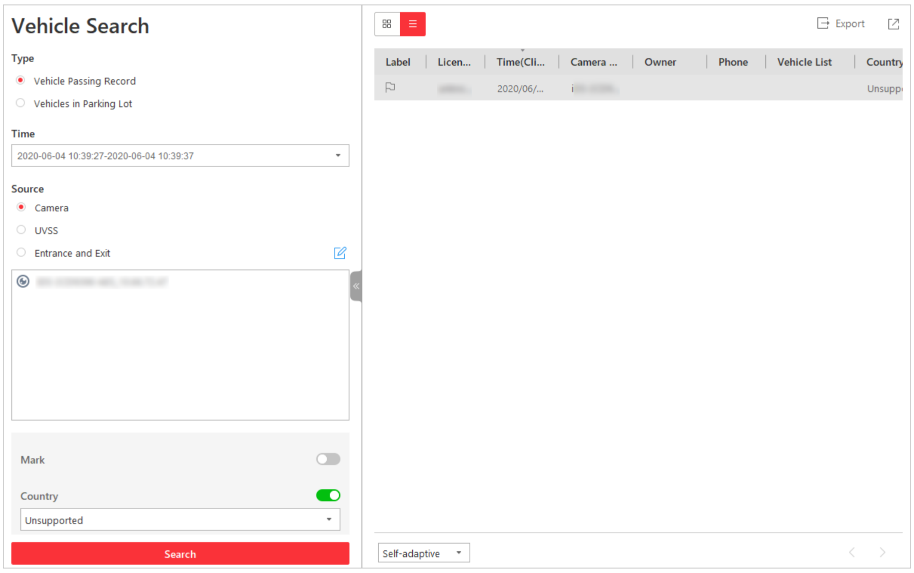
Make sure your license supports ANPR function. Otherwise, ANPR function cannot perform normally in the system.

1. In the top left corner of Home page, select ≡ → **All Modules** → **Vehicle** → **Vehicle Search** .
2. Select **Vehicle Passing Record** as the Type.
3. Set a time range for searching.
   - Select to search the vehicle passing records generated today, yesterday, current week, last 7 days, or last 30 days.
   - Click **Custom Time Interval** to set the search time range.
4. Select **Camera** or **Entrance and Exit** as the source of passing vehicle records.

   The camera or entrance/exit will be automatically displayed under the Source.

Note

For camera, you can click 📝 , select the current site or a Remote Site from the drop-down list and select the ANPR camera(s).



Vehicle Search

Type

● Vehicle Passing Record

○ Vehicles in Parking Lot

Time

2020-06-04 10:39:27-2020-06-04 10:39:37

Source

● Camera

○ UVSS

○ Entrance and Exit

[redacted]

Mark

Country

Unsupported

Search

Label	Licen...	Time(Cli...	Camera ...	Owner	Phone	Vehicle List	Country
	[redacted]	2020/06/...	[redacted]				Unsupp

Figure 16-14 Vehicle Search Page

5. Set searching conditions according to your needs.

   Mark

   Search marked or unmarked vehicles' passing records.

   Country

   Select the country where the vehicle's license plate number is registered.

   License Plate Number

   Select **No License Plate** to search vehicles without license plate number; select **With License Plate** and enter a vehicle's license plate number or key word of license plate number.

   Owner

   Enter the vehicle owner's name or keyword of name.

   Driving Direction

   - **Forward**: the vehicle moves toward the camera with its headstock facing the camera.
   - **Reverse**: the vehicle moves away from the camera with its rear facing the camera.

   Vehicle List

   Search vehicle passing records of vehicles in certain vehicle list(s).

6. Click **Search**.

   The vehicle passing records that match the search conditions will display on the right.

Note

You can click ☰ or ⊞ to switch between List Mode and Thumbnail Mode.

7. **Optional:** Perform the following operations after searching.

   Export All Vehicle Passing Records

   a. Click **Export** in the upper-right corner to open the Export panel.
   b. Select **Excel**, **CSV**, or **PDF** as the format of the exported file. Check **Export Picture** to save vehicles' pictures in your PC with the Excel file.
   c. Click **Browse** to select a saving path.
   d. Click **Save**.

Note

Up to 500 vehicle passing records with captured pictures can be exported at one time. Up to 100,000 vehicle passing records without pictures can be exported at one time.

16.7 Search Vehicles in Parking Lot

If the actual free parking space number is different from the number displayed on parking lot screens, you can search vehicles that already left but still recorded in the parking lot to edit the vehicle information. For example, for parking lots requiring all on-site vehicles out at the end of a day, you can search the vehicles that are still in the parking lot and export the vehicles' information. Another example is, if a vehicle is manually allowed to exit the parking lot, the free parking space amount may be not updated on time. In this situation, you can search the vehicle and delete it from the vehicle list of the parking lot to update the free parking space amount.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **Vehicle** → **Vehicle Search** .
2. Select **Vehicles in Parking Lot** as the searching type.
3. Set searching conditions according to your needs.

   Mark

   Search marked or unmarked vehicles in the parking lot.

   Country

   Select the country where the vehicle's license plate number is registered.

   License Plate Number

   Select **No License Plate** to search vehicles without license plate number; select **With License Plate** and enter a vehicle's license plate number or key word of license plate number.

   Owner

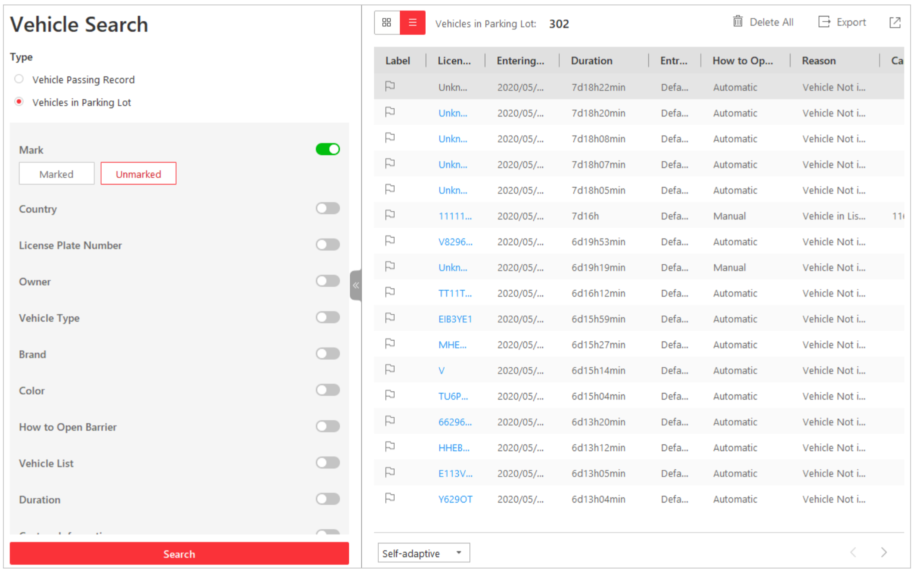
   Enter the vehicle owner's name or keyword of name.

   How to Open Barrier

It refers to how the barrier was opened when a vehicle exits the parking lot. **Manual** indicates that the a security guard manually controls the barrier to open after identifying the vehicle owner; **Automatic** indicates that the barrier was opened automatically after the capture unit recognizing the license plate number.

Duration

The parking duration of the searched vehicles in the parking lot.



Vehicle Search

Type

○ Vehicle Passing Record

● Vehicles in Parking Lot

Mark: on (Marked / Unmarked)

Country, License Plate Number, Owner, Vehicle Type, Brand, Color, How to Open Barrier, Vehicle List, Duration: off

Search

Vehicles in Parking Lot: 302

Delete All Export

Label	Licen...	Entering...	Duration	Entr...	How to Op...	Reason	Ca
⚐	Unkn...	2020/05/...	7d18h22min	Defa...	Automatic	Vehicle Not i...	
⚐	Unkn...	2020/05/...	7d18h20min	Defa...	Automatic	Vehicle Not i...	
⚐	Unkn...	2020/05/...	7d18h08min	Defa...	Automatic	Vehicle Not i...	
⚐	Unkn...	2020/05/...	7d18h07min	Defa...	Automatic	Vehicle Not i...	
⚐	Unkn...	2020/05/...	7d18h05min	Defa...	Automatic	Vehicle Not i...	
⚐	11111...	2020/05/...	7d16h	Defa...	Manual	Vehicle in Lis...	11
⚐	V8296...	2020/05/...	6d19h53min	Defa...	Automatic	Vehicle Not i...	
⚐	Unkn...	2020/05/...	6d19h19min	Defa...	Manual	Vehicle Not i...	
⚐	TT11T...	2020/05/...	6d16h12min	Defa...	Automatic	Vehicle Not i...	
⚐	EIB3YE1	2020/05/...	6d15h59min	Defa...	Automatic	Vehicle Not i...	
⚐	MHE...	2020/05/...	6d15h27min	Defa...	Automatic	Vehicle Not i...	
⚐	V	2020/05/...	6d15h14min	Defa...	Automatic	Vehicle Not i...	
⚐	TU6P...	2020/05/...	6d15h04min	Defa...	Automatic	Vehicle Not i...	
⚐	66296...	2020/05/...	6d13h20min	Defa...	Automatic	Vehicle Not i...	
⚐	HHEB...	2020/05/...	6d13h12min	Defa...	Automatic	Vehicle Not i...	
⚐	E113V...	2020/05/...	6d13h05min	Defa...	Automatic	Vehicle Not i...	
⚐	Y629OT	2020/05/...	6d13h04min	Defa...	Automatic	Vehicle Not i...	

Self-adaptive

Figure 16-15 Search Vehicles in Parking Lot

4. Click **Search**.

   The searched vehicles in the parking lot will be displayed on the right panel.

5. Perform the following operations if you need.

Operation | Description

Delete Vehicles from Parking Lot

- Select a searched vehicle and click 🗑 to delete the vehicle from the parking lot.
- Click **Delete All** to delete all searched vehicles from the parking lot.

Export Vehicle Information to PC

- Select a vehicle and click 🗋 to save the vehicle's information (CSV file), vehicle passing picture, and recorded file in your PC. The vehicle passing picture and recorded file will be saved in the same folder as the CSV file.
- Save information of all searched vehicles as a file in PC.
  a. Click **Export** on the top right of the Control Client to open the Export panel.
  b. Select **Excel** or **CSV** as the format of the exported file. Check **Export Picture** to save vehicles' pictures in your PC with the Excel file.
  c. Click **Browse** to select a saving path.
  d. Click **Save**.

Note

After deleting a searched vehicle, there will be one more free parking space in the parking lot of the system.

16.8 Set User to Receive Entrance & Exit Calls

You can specify users to receive calls from the entrance & exit devices on the Control Client, and then the user can remotely perform the further operations for the vehicles, such as correcting license plate number and manually allowing passing.

In the top left corner of Home page, select ≡ → **All Modules** → **Vehicle** → **Basic Settings** → **Call Recipient Settings** .

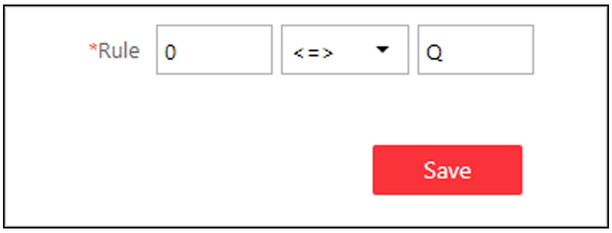
Click **Add** to select user(s) to receive entrance & exit calls on the Control Client.

16.9 Add Fuzzy Matching Rules for License Plate Search

When searching vehicles by license plate number on the Control Client, the system supports fuzzy matching. You can first set the fuzzy matching rules according to actual needs. By default, the system provides 6 ready-made rules including 0<=>Q, 0<=>O, Q<=>O, 1<=>I, G<=>6, and D<=>O.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **Basic Settings** → **Plate Fuzzy Search** .
2. Click **Add**.



*Rule 0 <=> Q

Figure 16-16 Add a Fuzzy Matching Rule

3. Set the rule.

   <=>

   Enter an uppercase letter or a digit before and after this symbol respectively.

   For example, 0<=>Q means: If you enter 0 or Q for search, the recognized license plate numbers with 0 and the ones with Q will be filtered.

   =>

   Enter an uppercase letter or a digit before and after this symbol respectively.

For example, G=>6 means: If you enter G for search, the recognized license plate numbers with G and the ones with 6 will be filtered. But if you enter 6 for search, the ones with G will not be filtered.

Note

- By default, 6 rules are added when you log in for the first time.
- Up to 16 rules can be added.

4. Click **Save**.
5. **Optional:** After adding the rules, you can do one or more of the followings.

Edit Rule	Click ✎ in the Operation column to edit this rule.
Enable/Disable Rule	Click ✓ / ⊖ in the Operation column to enable/disable this rule.
Delete Rule	Click × in the Operation column to delete this rule.

Chapter 17 Intelligent Analysis Report

Reports, created for a specified period, are essential documents, which are used to check whether a business runs smoothly and effectively. In HikCentral Professional, reports can be generated daily, weekly, monthly, annually, and by custom time period. The reports can also be added to the dashboard for browsing at a glance. You can use reports as basis in creating decisions, addressing problems, checking tendency and comparison, etc.

17.1 Customize Report Dashboard

The report dashboard provides an at-a-glance view for the reports supported by the system, such as vehicle analysis report. You can customize the report dashboard as required.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **Intelligent Analysis** → **Intelligent Analysis Report** .
2. **Optional:** Click ∨ → **Add Dashboard** on the report dashboard page to add a new dashboard.

   Note

   You can add up to 100 dashboards.

   The new dashboard appears and it is named as "Dashboard + The Time When It was Added" by default. For example, in "Dashboard20190916102436", "2019" represents year, "09" month, "16" date, "10" hour, "24" minute, and "26" second.
3. **Optional:** Edit dashboard(s).
   1) Click ∨ to expanded the added dashboard(s).
   2) Click ✎ to edit the dashboard name or click 🗑 to delete the dashboard.
4. Add report(s) to a dashboard and edit the report(s).
   1) Select a report type and generate the report.
   2) Click **Add** on the report page to add the report to dashboard.

      The report appears on the selected dashboard.
   3) Perform the following operations.
      - Add More Reports: Click **Add Report** to add more reports to the dashboard.
      - View Report in Larger Window: Click ⤢ to view the report in larger window.
      - Edit Report Name: Click ··· and then click **Edit**.
      - Delete Report from Dashboard: Click ··· and then click **Delete**.

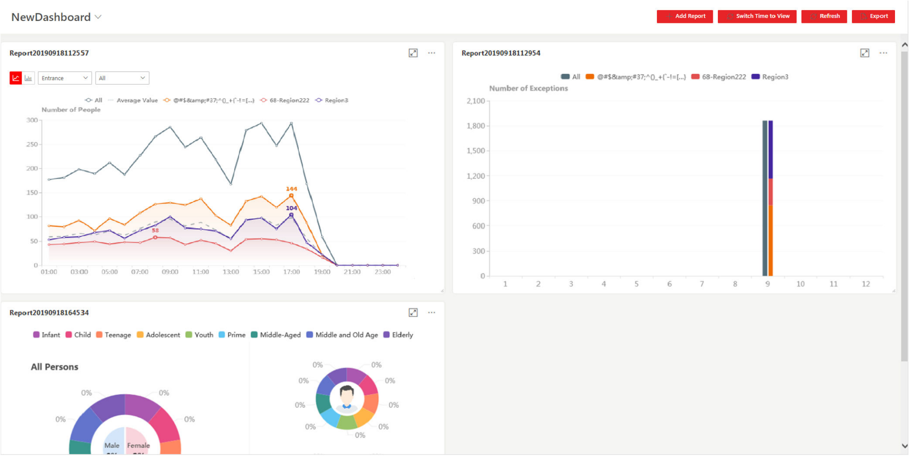


Figure 17-1 Report Dashboard

5. Switch time to view report data.
    1) Select a dashboard and then click **Switch Time to View** to set the report type and time.

       Report Type

       Select the time basis for the reports. For example, daily report shows data on a daily basis.

       Time

       Set the specific time for generating the reports. For example, if you select **Custom Time Interval** as the report type, you can click 📅 to specify a time interval for generating report data.
    2) Click **Save** to change the default time basis of all the reports in the dashboard to the time you set in the previous sub step.
6. **Optional:** Export report(s) on the dashboard to the local PC.
    1) Click **Export** to display the Export panel.
    2) Select report(s) from the report list.
    3) Select **Excel** or **CSV** as the format of the exported report(s).
    4) Click **Export**.

17.2 Add People Counting Group

The people counting group is used to group the doors and people counting cameras of certain region. You can set some doors and cameras as the region border. Only the persons accessing these doors or detected by the cameras are calculated, and other doors and cameras inside the region are ignored. By grouping these doors and cameras, the system provides counting functions based on the detected records on these doors and cameras. With this function, you can know how many persons still stay in this region. This is available for certain emergency or commercial scenarios. For example, for emergency scenario, during a fire escape, the number of the stayed persons will be displayed on the map which is required for rescue. For commercial scenario, the shopping mall manager can get the people counting report to know the number of people entering each stores.

Steps

Note

After setting rules, the security personnel can perform people counting in Intelligent Analysis module. For details, refer to ***Intelligent Analysis Report*** .

1. In the top left corner of Home page, select ≡ → **All Modules** → **Intelligent Analysis** → **Intelligent Analysis Group Settings** .
2. Click **People Counting Group** on the left.
3. Click **Add**.
4. Create a name for the group.
5. Select a site.
6. In the **RES for People Stayed CALC** area, click **Add** to select the resources (including doors and people counting cameras) for calculating the number of people stayed in this region.
7. Set the entering or exiting direction of the card readers of the selected doors and the entering or exiting direction of the cameras.

   Note

   Number of People Stayed in Region = Number of People Entered - Number of People Exited.

   For doors, the access records on the entering card reader will be calculated as person entering this region while the access records on the exiting one will be calculated as person exiting this region.

   For people counting cameras, the people crossing along the entering direction will be calculated as person entering this region while the people crossing along the exiting one will be calculated as person exiting this region.
8. **Optional:** Set the **Regularly Clear All** switch to ON and set a time for clearing all regularly.
9. **Optional:** Set the **Maximum Number of Persons** switch to ON and enter the maximum number of persons that can enter the area monitored by this group.
10. Click **Add**.

    The people counting group is added in the table and you can view the resources in the group.
11. **Optional:** Locate the people counting group on the map by setting the locations of the doors and cameras in the group and setting the border of the region for detection.

    1)Click **Set Geographic Location** to enter the Map Settings page.

    2)Drag the people counting group from the Resource Group list on the right to the map.

    The region as well as the doors and cameras in the group will be added on the map.

    3)Drag to draw the region according to the actual needs.

    4)Drag the icons of the doors and cameras to set the their locations on the map.

    5)Right click to finish.

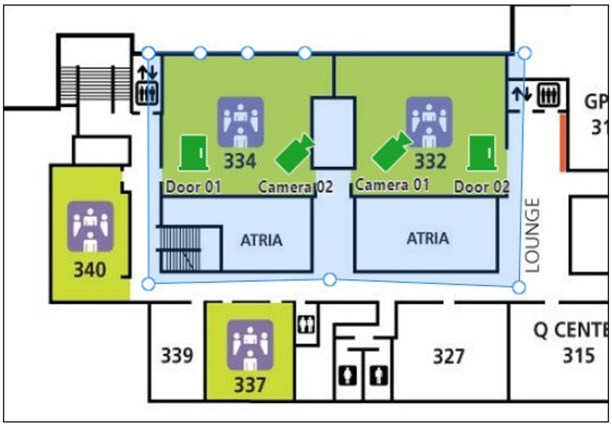


Figure 17-2 Draw People Counting Group on Map

After adding the people counting group on the map, you can view the real-time number of people entered, exited the region, or stayed in the region on the Control Client. Meanwhile, when an alarm is triggered in the region (such as people amount more/less than threshold), the client will notify the user by highlighting the region on the map.

17.3 Vehicle Analysis Report

Vehicle analysis report shows the number of passing vehicles detected by the specified cameras during specified time period.

You can set a regular report rule for the specified ANPR cameras, and the system will send emails with reports attached to the target recipients daily, weekly, or monthly. You can also manually generate a vehicle analysis report at any time to view the data if required.

17.3.1 Generate Vehicle Analysis Report

For ANPR cameras, you can generate a report to show the number of passing vehicles detected by the specified cameras during specified time period.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **Intelligent Analysis** → **Intelligent Analysis Report** .
2. Click **Vehicle Analysis** on the left.
3. Select the camera(s) for statistics.
   1) Click ⎘ in the camera panel.
   2) Select a current site or Remote Site from the drop-down site list to show its ANPR cameras which support this function.

   Note

   Only ANPR cameras will be displayed here.

3) Check the camera(s) for statistics.

   The cameras will be added to the camera list.

4. Select camera(s) for the report in the camera list.

Note

Up to 20 ANPR cameras can be selected for statistics at the same time.

5. Select the report type as daily report, weekly report, monthly report, annual report, or customize the time interval for a report.

Daily Report

Daily report shows data on a daily basis. The system will calculate the number of vehicles in each hour of one day.

Weekly Report, Monthly Report, Annual Report

As compared to daily report, weekly report, monthly report, and annual report can be less time-consuming, since they are not to be submitted every day. The system will calculate the number of vehicles in each day of way week, in each day of one month, and in each month of one year.

Custom Time Interval

Users can customize the days in the report to analyze the number of vehicles in each day or month of the custom time interval.

6. Set the time or time period in the Time field for statistics.

Note

For custom time interval report, you need to set the start time and end time to specify the time period.

7. Click **Generate Report**.

   The passing vehicles statistics detected by all the selected cameras are displayed in the right panel.

8. **Optional:** Export the report to the local PC.

   1) Click **Export**.

      The Export panel will display with camera selected and time configured according to the range you defined previously.

   2) (Optional) Select the camera and set the report type and report time if needed.
   3) Select shorter time period to view more detailed data of each camera.

      Example

      For example, if you select Daily Report, you can select **By Day** or **By Hour**, and it will export 1or 24 records respectively for each camera.

Note

If you select **By Minute**, the records amount depends on the configuration on the device. For example, if the device reports vehicle analysis data to the system every minute, it will export 24*60 records for each camera.

4) Set the format of the exported file as Excel or CSV.
5) Click **Export**.

17.3.2 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 ***Add Email Template for Sending Report Regularly*** .
- 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 32,000 records in total.
- The report will be an Excel file.

1. In the top left corner of Home page, select ≡ → **All Modules** → **Intelligent Analysis** → **Intelligent Analysis Group Settings** .
2. Click **Timing Report Configuration**.
3. Click **Add** to open the Create Report page.
4. Select the report category as **Vehicle Analysis**.
5. Create a name for the report.
6. Set the ANPR camera(s) contained in the report.
   1) Select the ANPR camera(s).
   2) Click › .
7. 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.

8. 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.

9. 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 ***Add Email Template for Sending Report Regularly*** .

10. Select the **Report Language**.
11. Click **Add**.

17.4 Generate Skin-surface Temperature Analysis Report

You can generate skin-surface temperature analysis report to view the variation trend of the number people whose skin-surface temperatures are abnormal.

Before You Start

- Make sure you have added devices that support temperature screening to HikCentral Professional.
- Make sure you have enabled temperature screening on the device. For details, see the user manual of the device.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **Intelligent Analysis** → **Intelligent Analysis Report** .
2. Click **Skin-surface Temperature Analysis** on the left.
3. Select temperature screening point or person group as the analysis type.

   Temperature Screening Point

A skin-surface temperature report based on data from temperature screening points (e.g. cameras) you select will be generated.

Person Group

A skin-surface temperature report based on the data from the person groups you select will be generated.

4. Select temperature screening point(s) or person group(s) based on the analysis type you set in the previous step.
   1) Click ✎ to open the camera list panel or person group panel.
   2) Select temperature screening point(s) or person group(s) for statistics.

Note

- You can also enter keywords of the camera name to search the temperature screening points or person groups.
- If you selects person group as the analysis type, you can check **Select Sub-Groups** to select the sub-groups of the person group that you have selected.

5. Set the report type to daily report, weekly report, monthly report, or customize the time interval for a report.

Daily Report

Daily report shows data on a daily basis. The system will calculate the peak amount of people appeared in the images of the camera in each hour of one day.

Weekly Report, Monthly Report

Compared to generating daily report, generating weekly report and monthly report can be less time-consuming. The system will calculate the peak amount of people on each day of one week and on each day of one month respectively.

Custom Time Interval

Users can customize the days in the report to analyze the peak amount of people in each day or month of the custom time interval.

6. In the Time field, select a pre-defined time period or customize a time period for search.
7. Click **Generate Report**.

The statistics of the selected item(s) will be displayed.

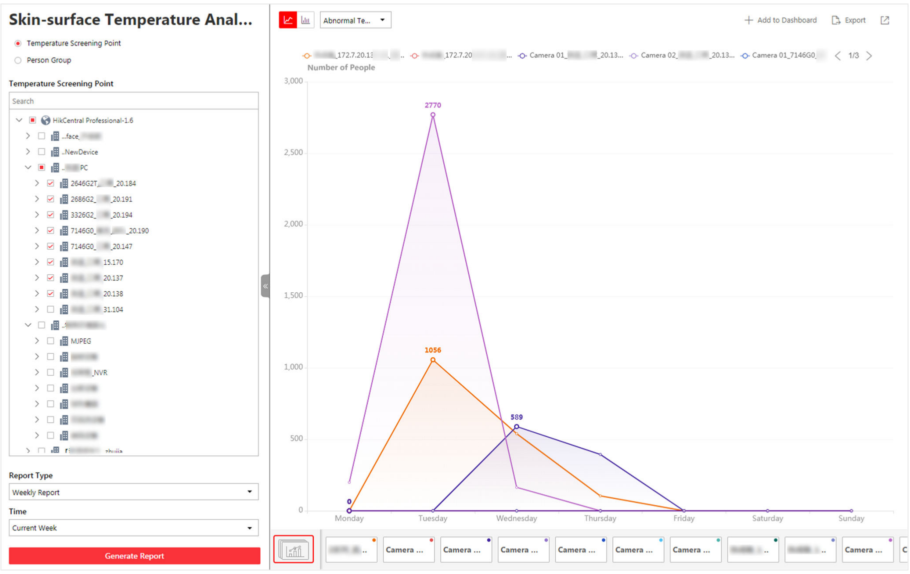


Figure 17-3 Skin-surface Temperature Analysis Report

8. **Optional:** Perform the following operations if required.

Show/Hide Certain Data	Click the legend to show or hide the data of certain element, such as certain camera.
Switch Between Line Chart and Histogram	Click 📈 / 📊 to switch between line chart and histogram. **Note** Daily report only supports histogram.
Add a Report to Dashboard	a. Click **Add to Dashboard** in the upper-right corner of the page. b. Create a report name. c. Select a dashboard. Or click **New** to create a new board and then select it. d. Click **OK** or **Add and Go to Dashboard**.

9. **Optional:** Export the report to the local PC.
   1) Click **Export**.

      The Export panel will be displayed.
   2) (Optional) Select the temperature screening point(s) or person group(s) and set the report type and report time if needed.
   3) Select shorter time period to view more detailed data of each camera.

      Example

      For example, if you select Daily Report, you can select **By Day** or **By Hour**, and it will export 1or 24 records respectively for each camera.
   4) Set the format of the exported file as Excel or CSV.
   5) Click **Export**.

Chapter 18 Alarm Detection

A security control device detects people, vehicles, etc., entering a predefined region, triggers events and alarms, and reports events/alarms information (such as location) to security personnel.

On the Web Client, after adding a security control device to the system, the administrator needs to group the device's alarm inputs into security control partitions in the system. You also need to set one defense schedule for the alarm inputs in a security control partition which 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 (alarm inputs) into area 1 first, then link the zones into security control partitions and set a defense schedule to these security control partitions. After that, the zones can be armed according to the schedules respectively.

18.1 Flow Chart

The following flow chart shows the process of the configurations and operations of alarm detection.

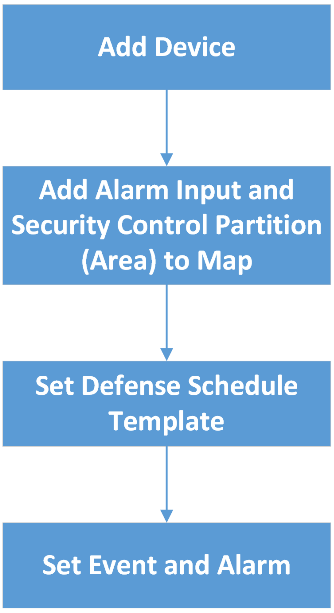

Add Device
Add Alarm Input and Security Control Partition (Area) to Map
Set Defense Schedule Template
Set Event and Alarm

Figure 18-1 Flow Chart of Alarm Detection

- **Add Device**: Add security control device to detect persons, vehicles, or other emergency events in the detection region to trigger alarms, and then notifies security personnel of alarm information. And then, add alarm input and partition (area) to area for management. Refer to

Manage Security Control Device , *Add Alarm Input to Area* , and ***Add Security Control Partitions (Area) from Device*** for details.

- **Add to Map**: Add alarm input and partition (area) on map to view their geographic locations, arm or disarm, bypass, and clear alarms. Refer to ***Add Hot Spot on Map*** for details.
- **Set Defense Schedule Template**: Set defense schedule template for a specified partition (area) to specify arming schedule and alarm linkage of alarm inputs in this partition (area). Refer to ***Configure Defense Schedule Template*** for details.
- **Event and Alarm**: Set event and alarm parameters and linkage actions to view event and alarm details on client or mobile client, timely remind the security personnel to handle, or search history events and alarms when some emergency situations occurred. Refer to ***Configure Event and Alarm*** for details.

18.2 Add Security Control Partitions (Area) from Device

HikCentral Professional provides areas to manage the added resources in different groups. You can group the resources into different areas according to the locations of the resources. After adding security control devices to the platform, you need to import the partitions (area) configured on the devices to different areas as well as group the alarm inputs (zones) in the partitions (area) into different areas for further operations.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **Alarm Detection** → **Security Control Partition (Area)** .
2. In the Security Control Partition (Area) field, click **+** or **Add**.

   In the Partition (Area) list, all the security control devices with partitions (areas) which are not added to the platform will be displayed.
3. Select the partitions (areas) that you want to add to the platform.
4. **Optional:** Check **Import Alarm Inputs** if you want to add the alarm inputs (zones) in the selected partitions (areas) to this area.

   Note

   After adding the alarm inputs to this area, you can manage them by different areas.
5. Click **Save**.

   The partitions (areas) will be displayed in the Security Control Partition (Area) list.
6. **Optional:** Set a defense schedule for this partition, which defines how and when to arm the alarm inputs in the security control partition (area).
7. **Optional:** Perform one or more of the following operations after adding the security control partitions (areas) to the area.

   Edit Security Control

   Click ✎ to edit the partition (area) settings.

   You can edit the partition (area) name, locations of the partition (area) and alarm inputs on the map, and set the defense schedule for this partition

Partition (Area)

(area), which defines how and when to arm the alarm inputs in the partition (area).

> **Note**
>
> For the partition (area) of AX security control panel, you cannot edit the defense schedule via platform. Only editing on device is supported.

Bypass Zone

When some exception occurs in one zone, and other zones can work normally, you need to bypass the abnormal zone to turn off the protection of it. Otherwise, you cannot arm the security control partition (area) which the zone belongs to. To bypass the zone, click ✎ to enter the partition (area) details page, and click ⊘ in the Operation column of the Alarm Input list to bypass the alarm input.

When you want to recover the zone that is bypassed to make it work normally, click ↺ in the Operation column to recover it.

Arm or Disarm Security Control Partition (Area)

After arming the partitions (areas), the platform can receive the triggered alarms in the partitions (areas).

There are three arming modes available.

- **Away Armed:** This mode is usually 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 Armed:** This mode is usually used when people stay inside the detection area. During stay armed, 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.
- **Instant Armed:** This mode is usually 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.

In the Security Control Partition (Area) list, select the partitions (areas) and click these buttons to arm the partitions (areas), or click **Disarm** to disarm them. After disarmed, when there are alarms triggered by the zones in the partitions (areas), the platform will not receive any alarms.

Clear Alarms

Click 🔕 to clear the generated alarms in the security control partition (area).

Delete Security Control Partition (Area)

Click × to delete the added security control partition (area).

18.3 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 armed, instant armed, or away armed 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. In the top left corner of Home page, select ☰ → **All Modules → Alarm Detection → Defense Schedule Template** .
2. Click **+** to enter the adding defense 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 an arming mode and drag on the time bar to draw a time period.

   Note

   By default, the Time-based is selected.

   Instant Armed

   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 Armed

   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 Armed

   It is used when people stay inside the detection area. During stay armed, 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.

Chapter 19 Manage Video Intercom

Video intercom is an audiovisual communication and security technique used in a building or a small collection of buildings. With microphones and cameras at both sides, it enables the intercommunication via video and audio signals and provides a safe and easy monitoring solution for apartment buildings and private houses.

On the Web Client, you can add video intercom devices to the system, group resources (such as doors and cameras) into different areas, and link person with indoor station. After settings related parameters, the person can view the live video of the camera, call indoor station, answer call via Control Client, etc.

19.1 Flow Chart

For the first time, you can follow the flow chart to perform configurations and operations.

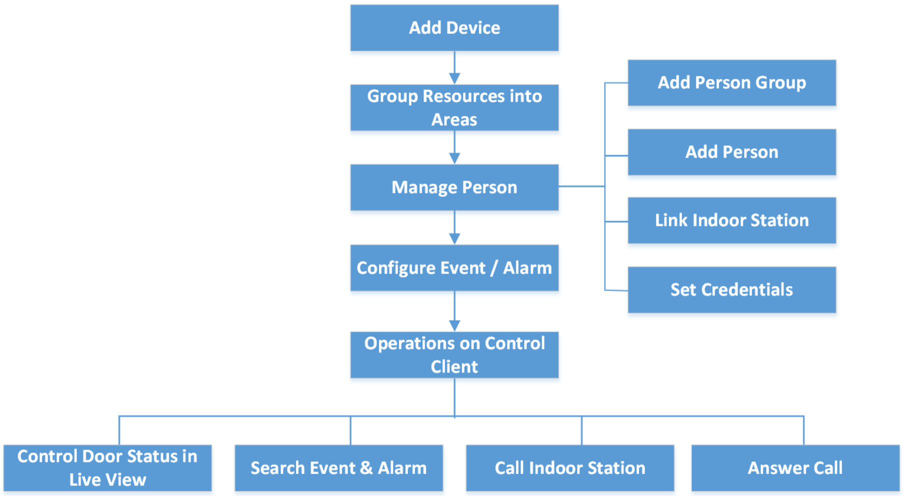


Figure 19-1 Flow Chart of Video Intercom

- **Add Device**: Add video intercom devices (such as master station, outer door station, indoor station, and door station) to HikCentral Professional and configure device parameters remotely. For more details, refer to ***Manage Video Intercom Device*** and ***Configure Device Parameters*** .
- **Group Resources into Areas**: After adding the devices to the system, you need to group the devices' resources (such as doors and cameras) into different areas according to the resources' locations. For details, refer to ***Manage Area*** .
- **Manage Person**: Add person group and person to the system, link person with indoor station, and set credential information. For more detail, refer to ***Manage Person*** .

- **Configure Event / Alarm**: Configure event and alarm for video intercom resources. For more details, refer to ***Configure Event and Alarm*** .
- **Operations on Control Client**: After the above configurations on the Web Client, you can control door status during live view, search event and alarm, call indoor station and answer call. For more details, refer to *User Manual of HikCentral Professional Control Client*.

Note

The doors of video intercom device can be used similarly as the doors of access control device. For more details about related configurations and operations of the doors, refer to ***Flow Chart*** .

19.2 Relate Camera with Indoor Station

After adding indoor station to the system, you can relate camera with the added indoor station to view video of the related camera(s) on the indoor station. Up to 16 cameras can be related to one indoor station.

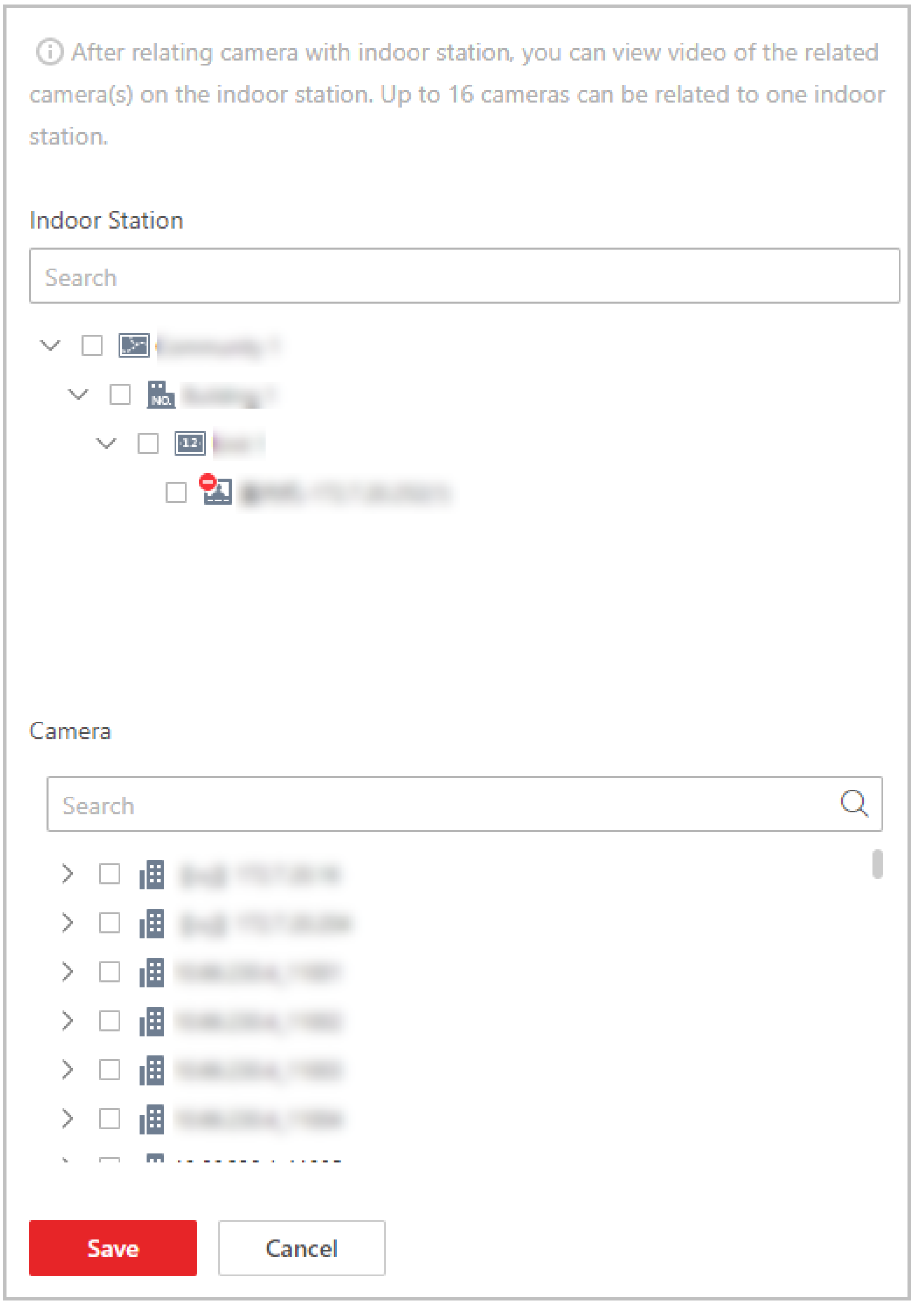
Before You Start

Make sure you have added indoor station(s) to the system. For details, refer to ***Add Indoor Station by IP Address*** .

Make sure the camera(s) to be related are correctly installed and are added to the system by Hikvision Private Protocol/ONVIF Protocol.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Video Intercom Device** on the left.
3. Select an indoor station in the video intercom device list.
4. Click **Add Related Camera**.



ⓘ After relating camera with indoor station, you can view video of the related camera(s) on the indoor station. Up to 16 cameras can be related to one indoor station.

Indoor Station

Search

Camera

Search

Figure 19-2 Add Related Camera

Note

You can also relate camera with indoor station in the configuration page of the indoor station. For details, refer to ***Configure Device Parameters*** .

5. In the Indoor Station list, check one or more indoor station(s).

Note

You can enter a keyword to search for the target indoor station(s). And the keyword of corresponding device(s) will be displayed in red.

6. In the Camera list, check one or more cameras.

Note

You can enter a keyword to search for the target camera(s). And the keyword of corresponding camera(s) will be displayed in red.

7. Click **Add**.

Note

You can also delete the related camera(s) in the configuration page of the indoor station.

19.3 Batch Link Persons with Indoor Station

The person needs to be linked with an indoor station, which is used for calling residents. You can link single person with an indoor station or multiple persons with indoor station(s) at a time. Here we introduce you how to batch link persons with indoor station(s) conveniently.

Steps

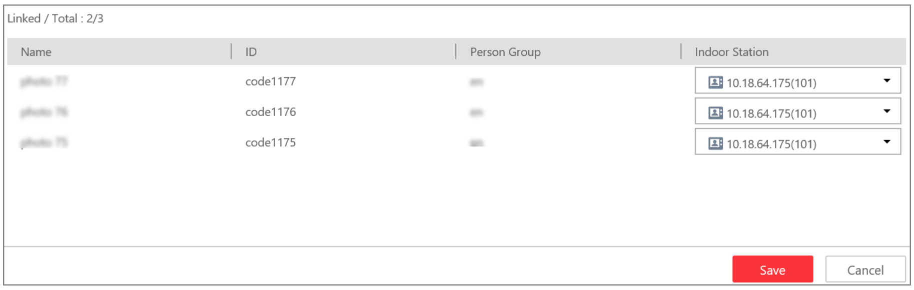
Note

For more details about linking single person with an indoor station, refer to ***Add a Person*** .

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Person** .
2. Select person group on the left to filter the persons.
3. Select the person(s) for linking with indoor station.
4. Click **Link with Indoor Station**.
5. Select desired indoor station on Indoor Station column for each person.

Note

Up to 10 persons can be linked with one indoor station and the person cannot be linked with multiple indoor stations.



Linked / Total : 2/3

Name	ID	Person Group	Indoor Station
[redacted]	code1177	[redacted]	10.18.64.175(101)
[redacted]	code1176	[redacted]	10.18.64.175(101)
[redacted]	code1175	[redacted]	10.18.64.175(101)

Figure 19-3 Batch Link Persons with Indoor Station(s)

6. Click **Save**.

   The linked person information will be applied to the indoor station(s).

19.4 Relate Doorbell with Indoor Station

You can relate a doorbell with an indoor station. If Call Management Center function of this doorbell is disabled, you can call the related indoor station by the doorbell.

If you have added the doorbell to the system, you can relate the doorbell with an indoor station as the following steps. If not, you can also relate the doorbell with an indoor station when adding the doorbell (see ***Manage Video Intercom Device*** for more details).

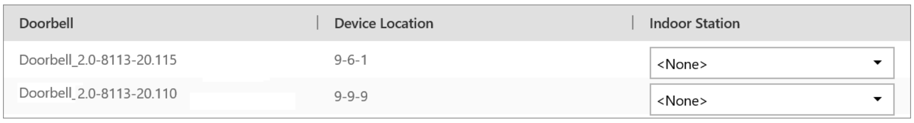
Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Video Intercom Device** on the left.
3. Click **Link Doorbell with Indoor Station** to enter Link Doorbell with Indoor Station.

   The added doorbells are displayed in the list.
4. From drop-down list, select the corresponding indoor station that the doorbell is to be related with.

Note

The location information of the indoor station is same as that of the doorbell.



Doorbell	Device Location	Indoor Station
Doorbell_2.0-8113-20.115	9-6-1	<None>
Doorbell_2.0-8113-20.110	9-9-9	<None>

Figure 19-4 Relate Doorbell with Indoor Station

5. Click **Save**.

Result

The doorbell will be related with the selected indoor station.

19.5 Configure Device Parameters

After adding the video intercom devices, you can configure parameters for them remotely, including device time, maintenance settings, etc.

Note

The parameters may vary with different models of devices.

Time

You can view the time zone where the device locates and set the following parameters.

Device Time

Click **Device Time** field to customize time for the device.

Sync with Server Time

Synchronize the device time with that of the SYS server of the system.

Call Management Center

For door station, you can set this function switch to on and select a shortcut button. When the configured button on the device is pressed, it will call management center. The default button is 1

Card Swiping

For outer door station and door station which supports Mifare encryption, you can enable **Mifare Encryption** and select the sector. Only the card with the same encrypted sector can be granted by swiping the card on the card reader.

Related Cameras

For indoor station, you can relate the camera(s) with it to view the video of the related camera(s) on the indoor station. You can also delete the related camera(s). Up to 16 related cameras are supported.

Maintenance

You can reboot a device remotely, and restore it to its default settings.

Reboot

Reboot the device.

Restore Default

Restore the device to its default settings. The device should be activated after restoring.

More

For more configurations, you can click **Configuration** to go to Remote Configuration page of the device.

Chapter 20 Skin-Surface Temperature

After adding the temperature screening cameras and access control devices with temperature screening function to the system, you can view the temperature of the detected persons in the Skin-Surface Temperature module. The system also shows whether the detected person is wearing a mask or not. With skin-surface temperature screening and mask detection functions, the system provides an alert if an individual is running a fever or not wearing a mask.

In the Skin-Surface Temperature module, you can view the real-time and history temperature screening records and mask detection records. You can also generate a report about these records to view the overall information.

Note

The mask detection function will show when the mask related function is turned on in the **System → Normal → User Preference** page. For details, refer to ***Set User Preference*** .

20.1 Temperature Screening Configuration

Before temperature screening, you should set temperature screening point groups and add related temperature screening points to the added groups. Also, for the temperature screening points, you can configure their parameters including temperature screening threshold and alarm threshold.

20.1.1 Group Temperature Screening Points

You can group multiple temperature screening points for convenient management. For example, you can group all the temperature screening points on the same floor into a group.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules → Temperature Screening → Configuration** .
2. Create temperature screening point group(s).
   1) Click + on the upper left corner of the page.
   2) Enter the name for the temperature screening point group as desired.
   3) Click **Save**.
3. Add temperature screening point(s) for the added temperature screening point group.

   Note

   Temperature screening points can be cameras and access control points that support temperature screening.

   1) Click **Add**.
   2) In the pop-up device list, check temperature screening point(s) as desired.

Note

You can enter a key word (supports fuzzy search) in the search box to quickly search for the target device(s).

3) Click **Add**.

4. **Optional:** After adding temperature screening point(s), perform following operations.

Add	Click **Add** to add more temperature screening point(s) as desired.
Delete	• Click 🗑 to delete single temperature screening point. • Check multiple temperature screening points, and click **Delete** to batch delete the selected devices.
Configure Parameters	Check one or multiple temperature screening points, and click **Configuration** to configure related parameters for the selected device(s). **Note** For details, refer to ***Configure Temperature Screening Parameters*** .
Export	Click **Export** to export detailed information of temperature screening point(s) such as device type, serial No., and temperature screening threshold to the local PC.

20.1.2 Configure Temperature Screening Parameters

For the added temperature screening point(s), you can configure the related parameters including temperature screening threshold and alarm threshold.

Check one or more added temperature screening point(s), and click **Configuration** to configure temperature screening parameters.

Temperature Screening Threshold

Set the threshold for temperature screening. When the detected skin-surface temperature is higher than the threshold, a temperature screening event will be triggered.

Alarm Threshold

Set the threshold for alarm. When the detected skin-surface temperature is higher than the threshold, an alarm will be triggered.

Note

- The temperature screening threshold should be smaller than alarm threshold.
- For temperature screening points which are access control points, you should configure their temperature screening parameters on the device parameters configuration page. For details, refer to ***Configure Other Parameters*** .

20.2 Real-Time Skin-Surface Temperature Monitoring

You can view the latest skin-surface temperature information detected by screening points. If there are persons whose skin-surface temperatures are abnormal, you will know at the first time. Besides, you will be able to quickly locate the persons according to the displayed screening point name and screening group. For unregistered persons, you can quickly register for them.

In the top left corner of Home page, select ≡ → **All Modules** → **Temperature Screening** → **Skin-Surface Temperature** . Select a temperature screening point group on the left. Red number indicates the number of skin-surface temperature screening points. Black number indicates the total number of devices in a temperature screening point group.

In the Picture area, the latest captured picture is displayed on the left. When new pictures are captured and displayed here, old captured pictures will be displayed on the right as thumbnails with faces, screening point name, person name, similarity, temperature, wearing mask or not, and detecting time.

Persons with different features will be marked by different colors. Orange means the captured person is not wearing a mask, but skin-surface temperature is normal; red means the captured person's skin-surface temperature is abnormal and the person wears no mask; green means the captured person's skin-surface temperature is normal and the person is wearing a mask. Click **More** to jump to the History page to view more captured pictures.

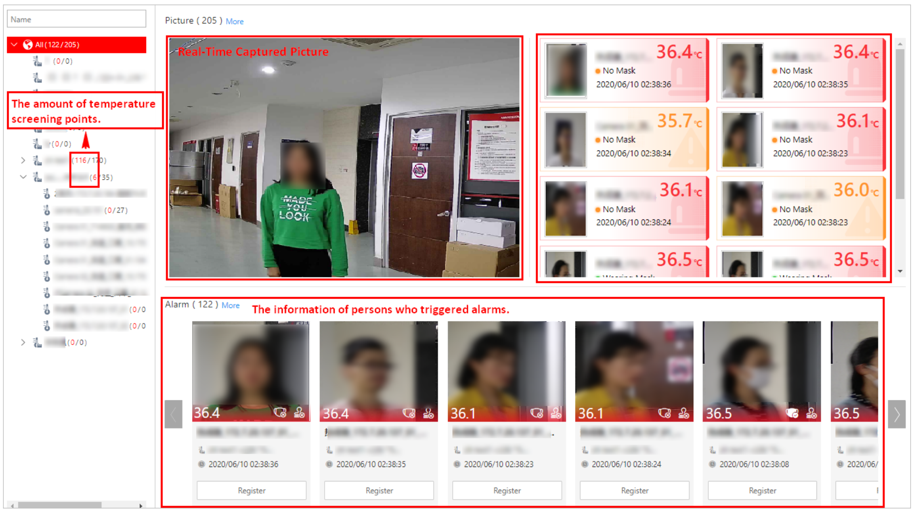


Figure 20-1 Real-Time Skin-Surface Temperature

When a person's skin-surface temperature exceeds the threshold you set, or the person is not wearing a mask, an alarm will be triggered. In the Alarm area, the pictures and information of persons who have triggered alarms are displayed. Following the title Alarm, the alarm amount is displayed. See *The User Manual of HikCentral Professional Web Client* for details about how to set a temperature threshold.

The person information includes skin-surface temperature, wearing mask or not, registered or unregistered, temperature screening point name, temperature screening point group name, and detecting time. You can click **Register** to register for the person, or click **More** to go to the History page to view more alarm information.

20.3 Search History Temperature Screening Data

You can set search conditions such as start time, end time, and skin-surface temperature to search for history temperature screening data.

Before You Start

Temperature screening data has been generated in real-time skin-surface temperature monitoring.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **Temperature Screening** → **History** .
2. Select a temperature screening point group or a temperature screening point from the list.
3. Set the search condition(s) including start time, end time, skin-surface temperature, etc.
4. Click **Filter**.

   History temperature screening data that meets the search condition(s) will be displayed below.
5. **Optional:** For the searched results, perform the following operations as desired.

   View Result Details

   You can view the detailed information of the searched results, including temperature screening group, temperature screening point, captured time, person's skin-surface temperature, whether wearing masks, etc.

   Note

   represents that the person wears a mask, and represents that the person doesn't wear a mask.

   Edit/Register Person Information

   You can edit or register person information based on the different icons.

   - : The person is registered. For the registered person, click **Edit** to edit the person information.
   - : The person is unregistered. For the unregistered person, click **Register** to enter person's registration information. For details, refer to ***Register Person Information*** .

   Export

   Click **Export** to export temperature screening data including temperature screening point, temperature screening point group, temperature status, etc., in excel file.

20.4 Registration

To manage the people who have been screened skin-surface temperature conveniently, you can register for them by entering their personal information. After registration, you can view and filter the registered persons' information.

20.4.1 Register Person Information

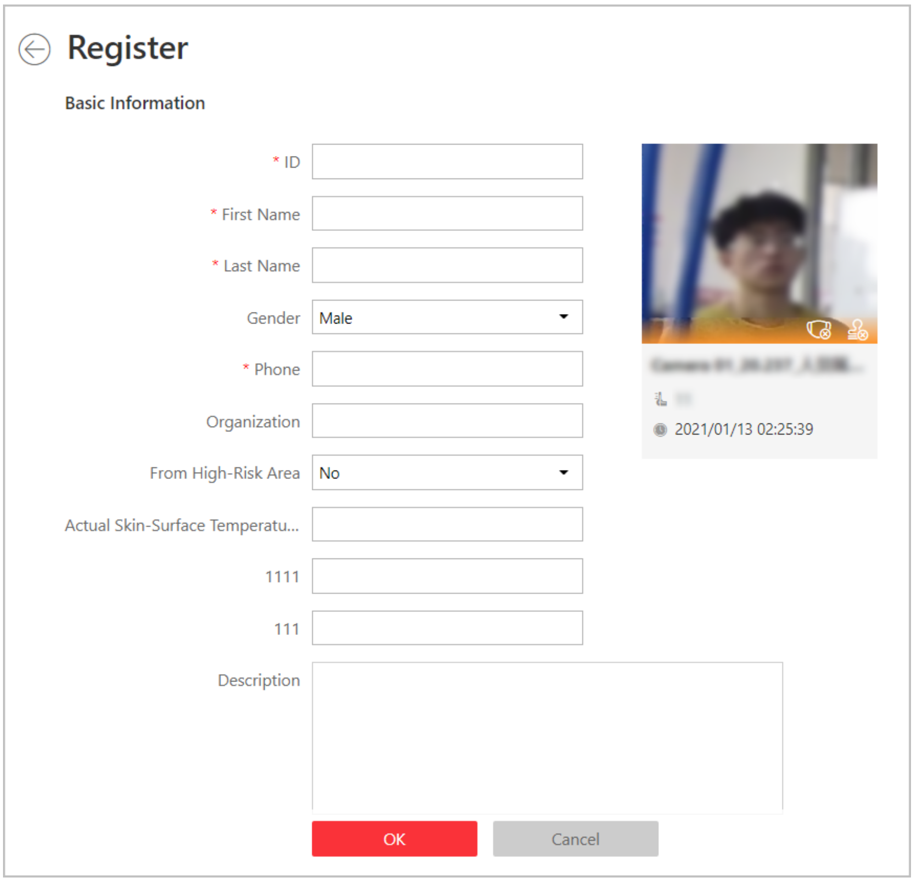
For unregistered persons displayed on real-time skin-surface temperature page or history page of skin-surface temperature, you can register for them.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **Temperature Screening** → **Skin-Surface Temperature** (or **History**).

   The skin-surface temperature screening information will be displayed.

2. If a screened person is not registered, you can click **Register** to enter the Register page to register for the person.



Register

Basic Information

* ID

* First Name

* Last Name

Gender: Male

* Phone

Organization

From High-Risk Area: No

Actual Skin-Surface Temperatu...

1111

111

Description

2021/01/13 02:25:39

OK | Cancel

Figure 20-2 Register Page

3. Set personal information, including ID, name, phone number, whether from high-risk areas etc.

Note

You can custom the information displayed on this page according to your needs. See ***Custom Registration Template*** for details.

4. Click **OK** to finish the registration.

   Registered persons' information will be displayed on Registration page for a centralized management. See ***View Registered Person Information*** for details.

20.4.2 Custom Registration Template

You can set customized person information for registration which are not pre-defined in the system according to your actual needs.

Steps

Note

Up to 5 additional items can be added.

1. In the top left corner of Home page, select ≡ → **All Modules** → **Temperature Screening** → **Registration** .
2. Click ⚙ **Registration Template** to enter the Registration Template page.
3. Click **Add**.
4. In the Title field, create a name for the additional item.

   Note

   Up to 32 characters are allowed for the name.

5. Select the format type as general text, number, date or single selection for the additional item.

   Example

   For example, if you select general text, you need to enter words for this item when registering person information.

6. Click **Save**.
7. **Optional:** Perform one or more of the following operations.

   Edit Name Click ✎ to edit the name.

   Delete Click × to delete the additional item.

20.4.3 View Registered Person Information

For the registered persons, you can view their detailed information including person name, ID, gender, phone, skin-surface temperature, wearing mask or not, etc.

In the top left corner of Home page, select ≡ → **All Modules** → **Temperature Screening** → **Registration** .

You can view person name, ID, gender, phone, skin-surface temperature, wearing mask or not, registering time and other information in the list.

Click ✎ in the Operation column to edit person information as desired.

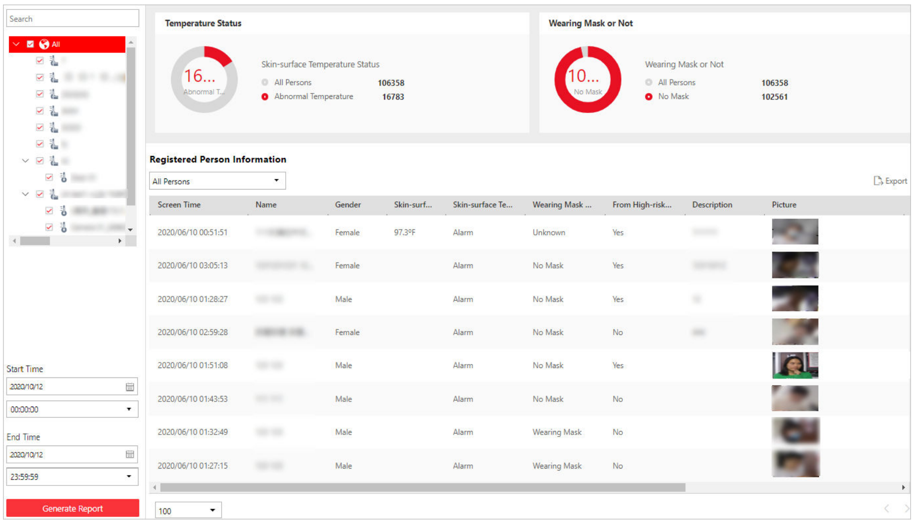
Click **Export** on the upper left corner of the page to export and view detailed registered person information in excel file.

20.5 Generate Report

Skin-surface temperature report gives you an overview of skin-surface temperature, mask-wearing detecting results, and registered person information. Based on the temperature status and mask-wearing detecting results, you will quickly learn how many person's skin-surface temperatures are abnormal, and how many persons are not wearing masks. With registered person information, you can quickly filter persons with abnormal skin-surface temperature or with no mask to learn their detailed information including name, location, face picture, from high-risk area or not, etc.

In the top left corner of Home page, select ≡ → **All Modules** → **Temperature Screening** → **Report** .

Select a temperature screening point group or temperature screening point, set time range at the bottom and click **Generate Report**.



Skin-surface Temperature Status

○ All Persons	106358
● Abnormal Temperature	16783

Wearing Mask or Not

○ All Persons	106358
● No Mask	102561

Start Time 2020/10/12 00:00:00

End Time 2020/10/12 23:59:59

Registered Person Information

All Persons

Screen Time	Name	Gender	Skin-surf...	Skin-surface Te...	Wearing Mask ...	From High-risk...	Description	Picture
2020/06/10 00:51:51	[redacted]	Female	97.3°F	Alarm	Unknown	Yes	[redacted]	
2020/06/10 03:05:13	[redacted]	Female		Alarm	No Mask	Yes	[redacted]	
2020/06/10 01:28:27	[redacted]	Male		Alarm	No Mask	Yes	[redacted]	
2020/06/10 02:59:28	[redacted]	Female		Alarm	No Mask	No	[redacted]	
2020/06/10 01:51:08	[redacted]	Male		Alarm	No Mask	Yes		
2020/06/10 01:43:53	[redacted]	Male		Alarm	No Mask	No		
2020/06/10 01:32:49	[redacted]	Male		Alarm	Wearing Mask	No		
2020/06/10 01:27:15	[redacted]	Male		Alarm	Wearing Mask	No		

100

Figure 20-3 Skin-Surface Temperature Report

Temperature Status

Temperature Status gives you the total number of persons whose skin-surface temperatures are screened and the number of persons with abnormal temperature.

Wearing Mask or Not

It gives you the total number of persons who had been detected whether they are wearing a mask, and the number of persons wearing no mask.

Registered Person Information

You can filter persons with abnormal skin-surface temperature or wearing no mask quickly to view their detailed information. For example, If a person with abnormal skin-surface temperature does not wear a mask, you need to pay attention to him or her. Based on the temperature screening point name or temperature screening point group name, you can quickly locate a person.
Click 📄 to view a person's detailed information including an enlarged face picture, event details, and registered information.
Click **Export** to save the registered person information in your PC as an Excel file.

Chapter 21 Manage Map

One type of map is available: E-map. 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.

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 both Web Client and Control Client, and get a notification message from the map via Control Client when an alarm is triggered.

21.1 Add E-Map for 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.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **Map** → **Map Settings** to enter the map settings page.
2. Select an area on the left.
3. Click **Add Map** at the center of the page.
4. Select an adding mode.
5. Select map.
   - If you select **Add E-Map** as the adding mode, select a map picture saved on the PC.
   - If you select **Link Map of Other Area**, select an area from the following list.
6. Click **Add**.
7. **Optional:** Set a map scale.

   Note

   The scale of a map is the ratio of a distance on the map to the corresponding distance on the ground. The client can calculate two locations' distance on the map according to the distance on the ground. An accurate map scale is essential for defining a radar's detection area. Perform this step if you plan to add a radar to the map.

   1) Click **Calibrate** on the top right of the map.
   2) Click two locations on the map to form a line.
   3) Enter the real distance between the two points in the Actual Length field.
   4) Click **OK** to finish setting the map scale.

8. **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.

9. **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.

21.2 Add Hot Spot on Map

You can add elements (e.g., cameras, access points, alarm inputs, etc.) as the hot spot and place the hot spot on the e-map. Then you can view the elements on the map and perform further operations via Control Client. For example, you can get the live view, actual access points, and alarm information of the surveillance scenarios, lock access point, unlock access point, and so on.

Before You Start

A map should have been added. Refer to ***Add E-Map for Area*** for details about adding e-map.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **Map** → **Map Settings** to enter the map settings page.
2. Select an area on the left.
3. **Optional:** Select a map.
4. Click **Resource** on the right.
5. Select a device type and an area from the drop-down lists.
6. Select a device and drag it to the map.

   The hot spot is displayed on the map.
7. **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 selecting icon style).

   For camera and radar 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.

21.3 Add Hot Region on Map

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 ***Add E-Map for Area*** for details about adding maps.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **Map** → **Map Settings** to enter the map settings page.
2. Select an area on the left.
3. **Optional:** Select a static map.
4. Click **+** on the **Hot Region** icon on the right.
5. Click a position on the map to select it as the location of the hot region.
6. Select an area from the area list.
7. Click **Save** on dialog to add the hot region.

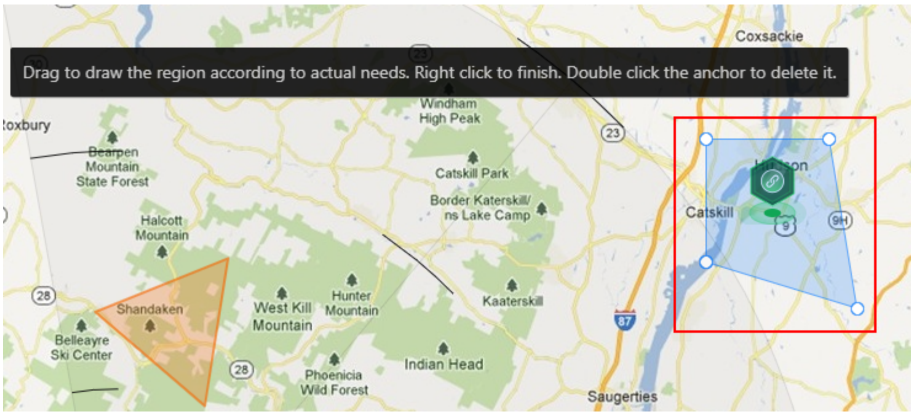
   The added hot region icon will be displayed on the parent map.
8. **Optional:** Perform the following operation(s) after adding the hot region.

   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 hot region name, icon style, name color, and remarks on the appearing dialog.

   Edit Hot Region Area
   Drag the white point on the hot region's line to edit the hot region's size or shape as the following picture.

   Delete Hot Region
   Click the hot region icon on the map and click **Delete** on the appearing dialog to delete the hot region.



Drag to draw the region according to actual needs. Right click to finish. Double click the anchor to delete it.

Figure 21-1 Edit Hot Region Area

21.4 Add Label on Map

You can add labels with description on the map.

Before You Start

At least one map should have been added. Refer to ***Add E-Map for Area*** for details about adding e-map.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **Map** → **Map Settings** to enter the map settings page.
2. Select an area on the left.
3. **Optional:** Select a static map.
4. Click **+** on the **Label** icon on the right.
5. 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.

21.5 Add Resource Group on Map

You can also add the resource groups on the map by locating the resources in the group on the map and setting the border of the region for detection.

Currently, the following resource groups can be added on the map for further operations:

People Counting Group

After adding the people counting group on the map, you can view the real-time number of people entered, exited the region, or stayed in the region in the Monitoring module on the Control Client. Meanwhile, when an alarm is triggered in the region (such as people amount more/less than threshold), the client will notify the user by highlighting the region on the map.

For details about how to add a people counting group on the map, refer to ***Add People Counting Group*** .

Anti-Passback Group

After adding the anti-passback group on the map, when an anti-passback alarm is triggered by the doors in the group, the client will notify the user by highlighting the region on the map and you can view the real-time alarms triggered in the region in the Monitoring module on the Control Client.

For details about how to add an anti-passback group on the map, refer to ***Configure Anti-Passback*** .

Multi-Door Interlocking Group

After adding the multi-door interlocking group on the map, when multi-door interlocking alarm is triggered by the doors in the group, the client will notify the user by highlighting the region on the map and you can view the real-time alarms triggered in the region in the Monitoring module on the Control Client.

For details about how to add a multi-door interlocking group on the map, refer to ***Configure Multi-Door Interlocking***

Entry & Exit Counting Group

After adding the entry &exit counting group on the map, you can view the real-time number of people entered, exited the region, or stayed in the region in the Monitoring module on the Control Client. Meanwhile, when an alarm is triggered in the region (such as people amount more/less than threshold), the client will notify the user by highlighting the region on the map.

For details about how to add an entry &exit counting group on the map, refer to ***Add Entry and Exit Counting Group*** .

Emergency Operation Group

After adding the emergency operation group on the map, you can operate access points (remaining locked/unlocked) in the group in a batch.

This function is mainly applicable for emergent situation. For example, after grouping the doors of the school's main entrances and exits into one emergency operation group, the school's security personnel can lock down the doors in this group by quick operation on the Control Client, so that the school closes and no one can get into the school except for maintenance and high level admins. This function would block out teachers, custodians, students, etc.

For details about adding an emergency operation group, refer to ***Add Emergency Operation Group*** .

Security Control Partition (Area)

After adding the security control partition (area) on the map, the security control device's alarm inputs will be grouped according to the zones on the device and displayed on map, and you can set a defense schedule to define when and how to arm the alarm inputs in a batch.

For details about adding a security control partition, refer to ***Add Security Control Partitions (Area) from Device*** .

21.6 Add Entrance and Exit on Map

You can add an entrance and exit on the map to locate the entrance and exit for a visualized monitoring.

Before You Start

A map should have been added. Refer to ***Add E-Map for Area*** for details about adding e-map.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **Map** → **Map Settings** to enter the map settings page.
2. Select an area on the left.
3. **Optional:** Select a map.
4. Click **Entrance and Exit** on the right.
5. Drag an entrance or exit to the map.

   The entrance or exit is displayed on the map.
6. **Optional:** Perform the following operations after adding the entrance and exit.

   Adjust Entrance and Exit Location
   Drag the added entrance and exit on the map to the desired locations.

   Edit Entrance and Exit
   Click the added entrance and exit icon on the map and click **Edit** to edit the detailed information (such as selecting icon style).

   Delete Entrance and Exit
   Click the entrance and exit icon on the map and click **Delete** to remove the entrance and exit from the map.

21.7 Add Combined Alarm on Map

You can add the combined alarms on map to locate the alarm for a visualized monitoring.

Before You Start

Make sure you have added a map. Refer to ***Add E-Map for Area*** for details about adding e-map.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **Map** → **Map Settings** to enter the map settings page.
2. Select an area on the left.
3. **Optional:** Select a map.
4. Click **Combined Alarm** on the right.
5. Drag a combined alarm to the map.

   The combined alarm is displayed on the map.
6. **Optional:** Perform the following operations after adding the combined alarm.

   Adjust Combined Alarm Location
   Drag the added combined alarm on the map to the desired locations.

   Edit Combined Alarm
   Click the added combined alarm icon on the map and click **Edit** to edit the detailed information (such as selecting icon style).

   Delete Combined Alarm
   Click the combined alarm icon on the map and click **Delete** to remove the combined alarm from the map.

21.8 Operate Hot Spot

The resources (including cameras, alarm inputs, alarm outputs, access points, and radars) added on the map are called the hot spots. The hot spots show the locations of the resources. You can operate the hot spot, such as starting live view of the camera and door, arming or disarming the resources.

21.8.1 Preview Hot Spot

You can view locations of hot spots including cameras, alarm inputs, alarm outputs, access points, radars, sites, etc. on the map. Also, you can set the arming control and view history alarms of surveillance scenarios through the hot spots.

Before You Start

Configure the map settings via the Web Client. For details, see ***Manage Map*** .

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **Map** → **Map Monitoring** .
2. Click 🖼 on the left of the map.
3. On the top left of the map, select an area from the **Select Map** drop-down list.

   All maps of the area will be displayed.
4. Select a map to enter the map.
5. **Optional:** Perform the following operations on the map.

Filter Resource on Map	Click and check resource type(s) as desired.
More Tools	: Add a label on map. **2D/3D**: Switch the displaying dimension of the map. Search : Search hot spot or location on the map.

6. Click the hot spot to open the dialog which displays its related functions.

   Note

   If there is an alarm triggered on the hot spot, the hot spot icon will turn into red alarm mode . Click the red icon, and you can view the detailed alarm information.

7. Operate in the dialog.
   - For camera hot spot: Check the live view and playback of the camera, view its status, area, and remark, set the arming control, and view the history alarms.

     Note

     - To view the live view and playback of the camera, the user should be assigned with permissions of live view and playback of the camera. For details, refer to the *User Manual of HikCentral Professional Web Client*.
     - For details about arming control, see ***Perform Arming Control*** .
     - For details about viewing history alarms, see ***View History Alarm*** .
   - For alarm input hot spot: View its status, area, and remark, set the arming control, and view the history alarms.
   - For alarm output hot spot: Turn on or off the linked alarm output.
   - For access point hot spot: View the access point status, check the live view and playback of the access point's related camera(s), view the access point's basic information, control the door status, set the arming control, and view the history alarms and access records.
   - For radar hot spot: View the radar status, area and remark, check the live view and playback of the radar's related camera(s), set the arming control, view the history alarms.
   - For radar PTZ camera hot spot: View camera's field of view and view the object's moving pattern.
   - For site hot spot: View the site's resources and alarms which are not handled.
   - For partition hot spot: Set the arming control including alarm clearing, disarming, away arming, stay arming, instant arming. For details, refer to ***Perform Arming Control*** .

21.8.2 Draw Zone or Trigger Line for Radar

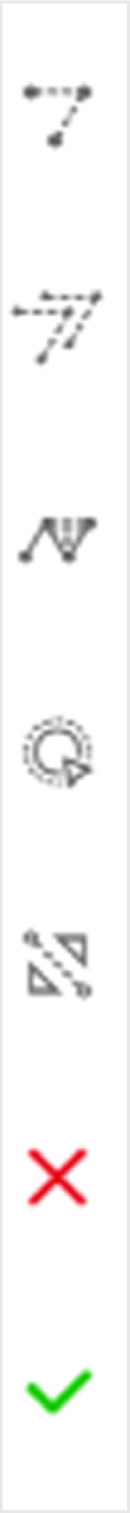
You can draw zones or trigger lines for radar, so if an object is detected to have crossed the trigger line or entered the area shaped by the dual-trigger line or zone, the event and alarm will be triggered.

Before You Start

A radar has been added to the area and map. Refer to ***Add Radar to Area for Current Site*** and ***Add Hot Spot on Map*** for details.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **Map** → **Map Settings** .
2. Click the radar's icon on the map and then select **Draw Zone/Trigger Line** from the drop-down list to start drawing zone or trigger line for radar.
3. Select a zone drawing method in the tool bar in the upper-left corner of the map.

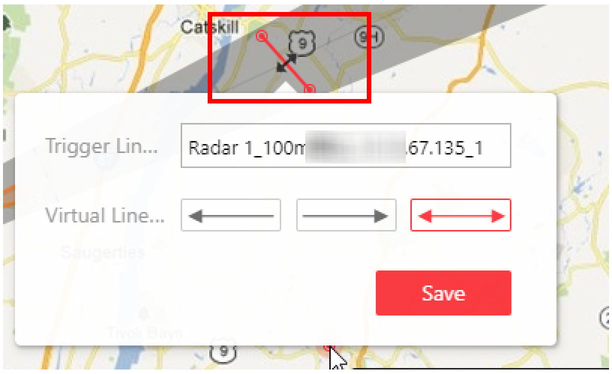


Draw Trigger Line

A trigger line is a virtual line drawn in the radar's detection area. An event or alarm will be triggered if an object is detected to have crossed the line. Click to draw a trigger line in the detection area. Select a direction for the trigger line. The three directions indicate three directions to which a detected object crosses the line. You can drag the anchor (the red point on the trigger line) to reshape the trigger line, or drag the trigger line to move it to another place.

Note

No more than 4 trigger lines can be drawn.



Trigger Lin... Radar 1_100m[redacted].67.135_1

Virtual Line... ← → ↔

Figure 21-3 Trigger Line in the Detection Area

Draw Dual-Trigger Line

A dual-trigger line consists of 2 virtual lines drawn in the radar's detection area. Generally, it is used to mark an area in the radar's detection area. An event or alarm will be triggered if an object is detected to have entered the area shaped by the dual-trigger line. Click to draw a dual-trigger line in the detection area. Select a direction for the trigger line. The three directions indicate three directions to which a detected object crosses the line. You can drag the anchor (the red point on the trigger line) to reshape the dual-trigger line, or drag the dual-trigger line to move it to another place.

Note

Only 1 dual-trigger line can be drawn in the radar's detection area.

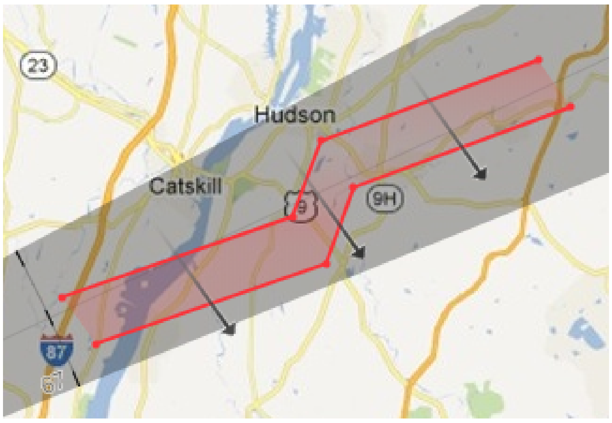


Figure 21-4 Dual-Trigger Line in the Detection Area

Manually Draw

You can draw any shape for the zone using this method.

Zone Segmentation

Split a zone into two smaller zones by a line.

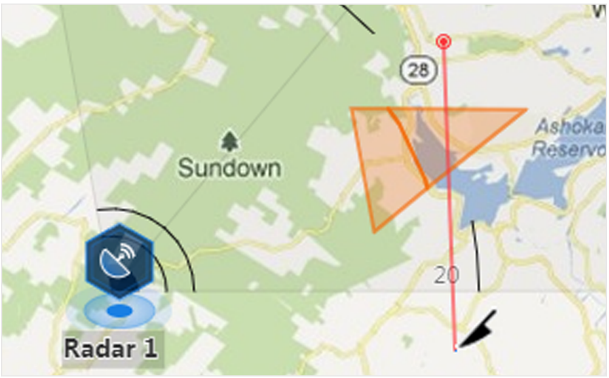


Figure 21-5 Zone Segmentation

Distance Segmentation

Split a zone into two smaller zone by an arc.

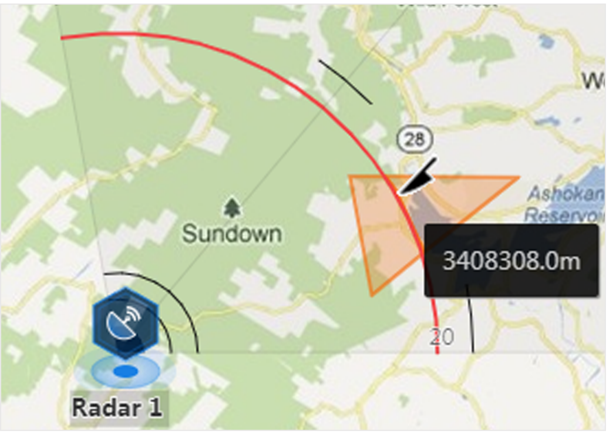


Figure 21-6 Distance Segmentation

4. Right click to finish drawing and open a configuration window.
5. Set parameters for the drawn trigger line or zone.
6. Click **Save**.
7. Right click to exit the zone or trigger line drawing mode.

21.8.3 Relate Calibrated Camera to Radar

This operation requires two persons' teamwork: person A walks into the radar's detection area (the person's position will be displayed on the map as a red point), while person B who operates the computer running the Web Client adds calibration points by PTZ control of the camera(s) according to person A's position.

Before You Start

A radar has been added to the area and map. Refer to ***Add Radar to Area for Current Site*** and ***Add Hot Spot on Map*** for details.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **Map** → **Map Settings** .
2. Click the radar's icon on the map and then select **Relate Calibrated Camera** from the drop-down list to relate cameras.
3. Click **Resource** on the Map Settings panel and drag camera(s) to the map.

Note

- This function needs to be supported by the device.
- Up to 4 calibrated cameras can be added.

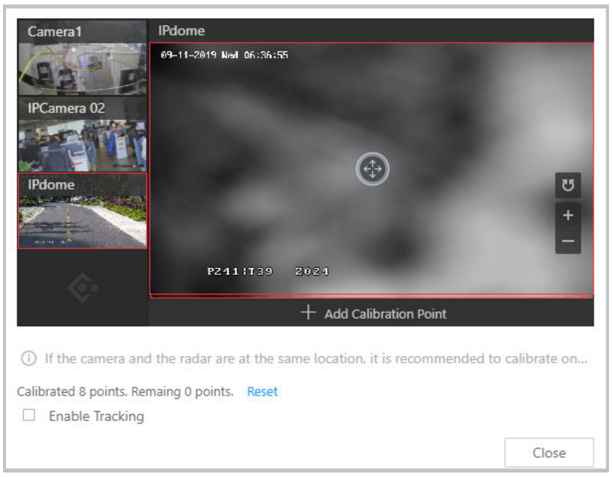
4. Click the radar's icon first, and then click camera icon(s) to relate the camera(s) with the radar.

Note

You can right click to finish relating cameras or it will automatically finish when no camera can be related.

5. Click the radar's icon on the map and then select **Calibrate PTZ Camera** from the drop-down list to enter the camera calibration settings page.
6. Person A goes to the location which can be detected by one of the cameras.

   Person A's location will appear on the map as a red point 🔴 .
7. Person B clicks 🔴 on the map to open the adding calibration point window.



ⓘ If the camera and the radar are at the same location, it is recommended to calibrate on...

Calibrated 8 points. Remaing 0 points. Reset

□ Enable Tracking

Figure 21-7 Add Calibration Point

   The cameras' thumbnails will be displayed on the left of the window.
8. **Optional:** Undo-check the **Enable Tracking** if you have enabled visual tracking for the calibrated cameras.
9. Click a camera's thumbnail to display its image in the window on the right.
10. Click the image to turn the camera to the position of person A until person A appears in the image.
11. Click **Add Calibration Point** to add the current image as a calibration point.

Note

- If the camera locates above or under the radar vertically, only 1 calibration point is enough; if not, at least 4 calibration points are required.
- Up to 8 calibration points can be added for one cameras.

12. **Optional:** Check **Enable Tracking** if you have enabled visual tracking for the calibrated cameras.
13. Close the Add Calibration Point window and click ✓ to save the settings.

21.8.4 Perform Arming Control

You can arm or disarm the hot spots via the arming control function. After arming the device, the current Control Client can receive the triggered alarm information from the hot spot.

Before You Start

Configure the map settings via the Web Client. For details, see ***Manage Map*** .

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **Map** → **Map Monitoring** .
2. Click **Select Map** on the top left to display the map(s) of an area.
3. **Optional:** If an area has multiple maps, click to select a map.
4. Click the hot spot.

   A window on which the related functions of the hot spot display is opened.
5. Click **Arm**/**Disarm** to arm/disarm the hot spot.

21.8.5 View History Alarm

When an alarm is triggered, it will be recorded in the system. You can check the history log related to an alarm, including the alarm source details, alarm category, alarm triggered time, etc.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **Map** → **Map Monitoring** .
2. Click the hot spot.

   A dialog pops up on which the related functions of the hot spot display.
3. Click to enter the event and alarm search page.
4. Search history alarms of the hot spot. See ***Search Event/Alarm Logs*** for details.

21.9 Preview 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

Configure the map settings via the Web Client. For details, see ***Manage Map*** .

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **Map** → **Map Monitoring** .
2. Click **Select Map** on the top left to display the map(s) of an area.
3. **Optional:** If an area has multiple maps, click a map to select it.
4. Click a hot region on the map to enter the map of the hot region.

21.10 Preview Resource Group

During displaying map, you can view locations and regions of the resource groups, including people counting group, multi-door interlocking group, and anti-passback group. You can also perform further operations on the resources in the group.

Note

Make sure you have configured the required resource group and map settings via the Web Client. For details, see ***Manage Map*** .

In the top left corner of Home page, select ≡ → **All Modules** → **Map** → **Map Monitoring** .

- People Counting Group: You can view the real-time number of people entered, exited the region, or stayed in the region. Meanwhile, when an alarm is triggered in the region (such as people amount more/less than threshold), the region of the group will be highlighted on the map to notify the user on the Control Client.
- Pathway Analysis Group: You can view the real-time number of people walking by in the Monitoring module on the Control Client.
- Anti-Passback Group: When an anti-passback alarm is triggered by the doors in the group, the region of the group will be highlighted on the map and you can view the real-time alarms triggered in the region in the Monitoring module on the Control Client.
- Multi-Door Interlocking Group: When multi-door interlocking alarm is triggered by the doors in the group, the region of the group will be highlighted on the map and you can view the real-time alarms triggered in the region in the Monitoring module on the Control Client.
- Entry & Exit Counting Group: You can view the real-time number of people entered, exited the region, or stayed in the region in the Monitoring module on the Control Client. Meanwhile, when an alarm is triggered in the region (such as people amount more/less than threshold), the client will notify the user by highlighting the region on the map.

21.11 Operate Map

After opening map, you can perform one or more operations of the followings, such as zooming in or out map, selecting resource(s) on map, adding label, printing map, displaying map in full screen mode, and so on.

Zoom in/Zoom out Map

Use the mouse wheel or click + or − to zoom in or zoom out on the map.

Filter

Click 👁 and select the object type you want to show on the map.

Add Label

Click to add a label with description to the map.

Search Location

By the search bar on the top of the map, you can search hot spots/hot regions on the e-map by entering keyword(s).

Chapter 22 Maintenance

The system provides Service Manager to manage the installed services on the SYS server. You can check the service's running status, edit the service port, start/stop service via the Service Manager.

The system also 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.

22.1 Health Monitoring

Health monitoring provides both near-real-time and history information about the status of the SYS server and added resources. It is critical to multiple aspects of operating the servers or devices and is especially important for maintenance. When a resource exception occurs, you can enter this module to check the resource status and find out the abnormal device(s) and view the exception details.

In the top left corner of Home page, select ≡ → **All Modules** → **Maintenance** → **Health Monitoring** to enter the health monitoring page.

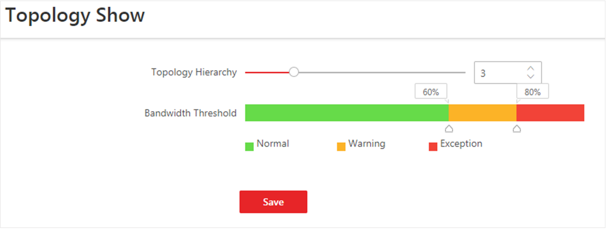
22.1.1 Set Topology Show Parameters

You can set parameters in the topology of health monitoring module, including topology hierarchy and bandwidth threshold.

Note

For details about health monitoring, see ***Health Monitoring*** .

In the top left corner of Home page, select ≡ → **All Modules** → **Maintenance** → **Health Monitoring** → **Basic Settings** → **Topology Show** to enter the Topology Show page.



Topology Show

Topology Hierarchy: 3

Bandwidth Threshold: 60% 80%

🟩 Normal 🟧 Warning 🟥 Exception

Figure 22-1 Topology Show Settings

Topology Hierarchy

If the devices connection hierarchy is complicated, you can set the topology hierarchy to display the primary devices.

Note

After setting the topology hierarchy, the topology will be generated again.

Bandwidth Threshold

When the bandwidth usage exceeds the threshold, the cable on the topology will turns to the corresponding color.

22.1.2 Set Health Check Frequency

The SYS server will perform health check to the resources managed in the system, including devices, servers, and configurations. The system will display the health check results in the Health Monitoring module, including the devices' online/offline status, recording status, etc. You can set the frequency which controls how often the system gets the latest status of the devices, servers, and configurations.

In the top left corner of Home page, select ≡ → **All Modules** → **Maintenance** → **Basic Settings** → **Health Check Frequency** .

Device Health Status

You can set the health check frequency for the devices managed in the system, including encoding devices, access control devices, video intercom devices, security control devices, and dock stations. It controls how often the system pings these devices to determine if they're online.
After disabled, the system will not update the status of the managed devices. You need to refresh manually to get the latest status.

Server Health Status

You can set the health check frequency for the managed Recording Servers and facial recognition servers. It controls how often the system pings these servers to determine if they're online.
After disabled, the system will not update the status of the managed servers. You need to refresh manually to get the latest status.

Others

- **Device Capabilities:** Set how often the system gets the managed devices' capabilities. After disabled, the system will not update the capability changes of all the managed devices. You need to refresh manually to get the latest status.
- **Recording:** Set how often the system checks the camera's recording status. After disabled, the system will not update the cameras' recording status.
- **Alarm/Event Enabled or Not:** Set how often the system checks whether the events and alarms are enabled or not. After disabled, the system will not update the configured event and alarm rules status.
- **Remote Alarm Enabled or Not:** Set how often the system checks whether the events and alarms configured on the Remote Sites are enabled or not. After disabled, the system will not update the configured alarm rules status configured on the Remote Sites.

22.1.3 Real-Time Overview (Resource Health Status Overview)

In Health Monitoring module, you can view the real-time health status of the devices, servers, and resources managed in the system. If there is no network transmission devices added, the Real-Time Overview provides an at-a-glance view of the health status with charts and basic data of resource status.

In the top left corner of Home page, select ≡ → **All Modules** → **Maintenance** → **Health Monitoring** → **Real-Time Overview** to enter the Real-Time Overview page.

Select **Real-Time Overview** in the upper area to open the real-time overview page.

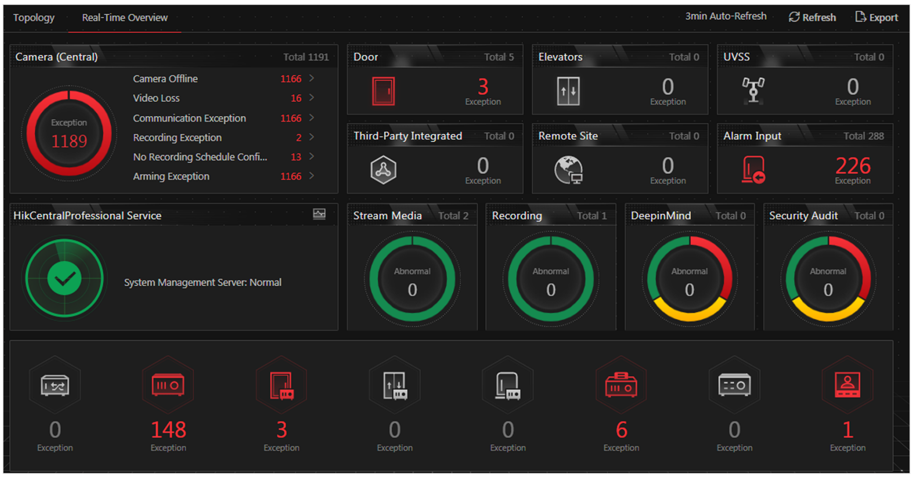


Figure 22-2 Real-Time Overview

View Status Information

You can view the overall status of the resources managed in the system, such as the cameras managed in the Central System, the access points, servers, devices, etc.

Note

You can go to **Maintenance** → **Basic Settings** → **Health Check Frequency** to set the interval for automatically refreshing the status of the resources.

You can click the numbers and status types on the chart to enter the corresponding status page to view the details.

- For HikCentral Professional service, you can click to open the System Management Server window to view the followings.
  - **CPU**: The real-time CPU usage.
  - **RAM**: The real-time RAM usage.
  - **Network**: The real-time network traffic sent and received.

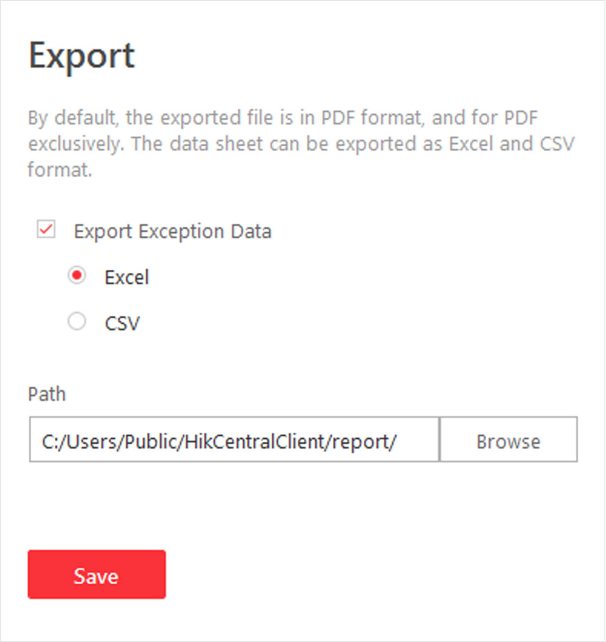
- **Streaming Gateway**: The incoming or outgoing streaming situation of the Streaming Gateway running on SYS server.
- **Picture Storage**: The real-time usage of picture storage.

- The Remote Site status is only available for the Central System with Remote Site Management module (based on the license you purchased).

Export Data

You can perform the following task to export the Real-Time Overview page as a PDF file to the local PC.

1. Click **Export** to open the Export panel.



Export

By default, the exported file is in PDF format, and for PDF exclusively. The data sheet can be exported as Excel and CSV format.

☑ Export Exception Data

● Excel

○ CSV

Path

C:/Users/Public/HikCentralClient/report/

Figure 22-3 The Export Panel

2. Select a saving path for the to-be-exported data.
3. Click **Save**.

You can also perform the following task to export the abnormal data to the local PC.

1. Click **Export** to open the Export panel.
2. Check **Export Exception Data**.
3. Select **CSV** or **Excel** as the format of the to-be-exported data.
4. Click **Save**.

22.1.4 Real-Time Overview (Topology Management)

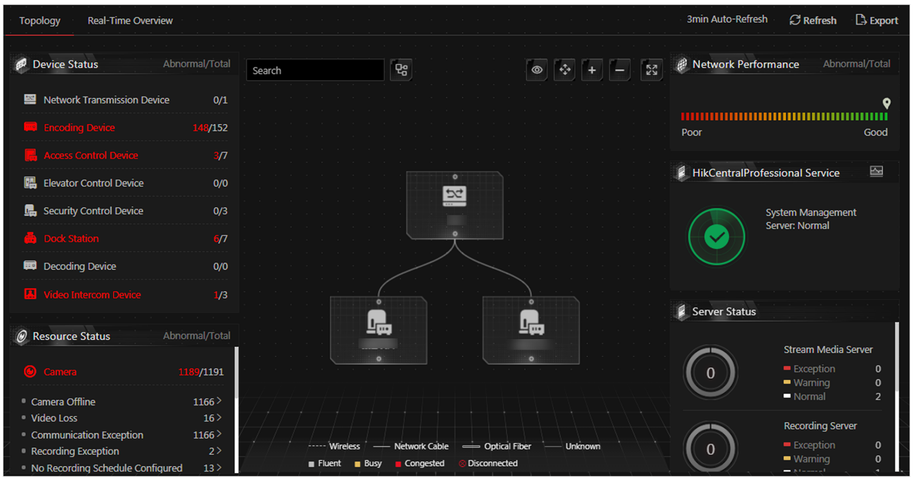
In the Health Monitoring module, you can view the real-time health status of the devices, servers, and resources managed in the system. If there are network transmission devices managed in the system, Real-Time Overview provides a topology of the managed devices. Topology is a figure that displays the connection relation of network transmission devices, surveillance devices, etc. It is mainly used for network maintenance.

In the top left corner of Home page, select ≡ → **All Modules → Maintenance → Health Monitoring → Real-Time Overview** to enter the Real-Time Overview page.

Select **Topology** in the upper area to open the topology page.

Topology

Display the abnormal data of different devices (e.g. Recording Server, HikCentral Professional server, access control device or security control device). Click the number of Exception or Warning to locate the exceptional device in the topology or view resource real-time status.



Device Status	Abnormal/Total
Network Transmission Device	0/1
Encoding Device	148/152
Access Control Device	3/7
Elevator Control Device	0/0
Security Control Device	0/3
Dock Station	6/7
Decoding Device	0/0
Video Intercom Device	1/3

Resource Status	Abnormal/Total
Camera	1189/1191
Camera Offline	1166 >
Video Loss	16 >
Communication Exception	1166 >
Recording Exception	2 >
No Recording Schedule Configured	13 >

Stream Media Server	
Exception	0
Warning	0
Normal	2

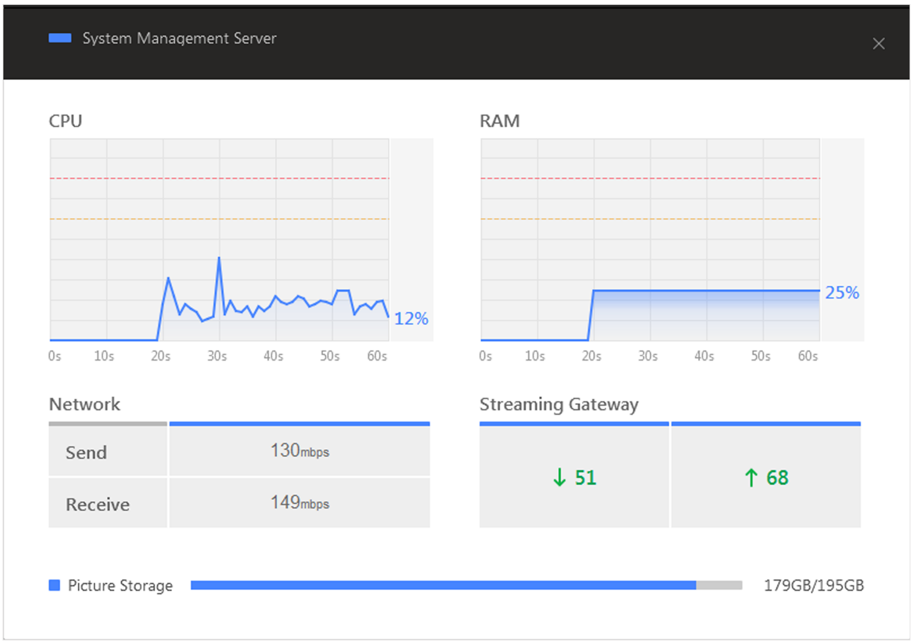
Recording Server	
Exception	0
Warning	0

System Management Server: Normal

Figure 22-4 Topology

System Management Server Status

View the network health status and server running status. Click on the right side of HikCentral Professional Server to view the running status of the server, including CPU usage, RAM usage, etc.



Network

Send	130mbps
Receive	149mbps

Streaming Gateway

↓ 51 ↑ 68

Picture Storage 179GB/195GB

Figure 22-5 System Management Server Status

Topology Overview

If there are network transmission devices managed in the system, the topology of devices will be displayed in the Real-Time Overview page, to display the hierarchical relationship of the devices, device information, link status and alarm information, etc.

In the top left corner of Home page, select ≡ → **All Modules** → **Maintenance** → **Health Monitoring** → **Real-Time Overview** .

Select **Topology** in the upper area to open the topology page, and then click **Refresh** → **Generate Topology Again** to draw the network topology again.

Note

- Make sure the network transmission devices have been added to the system.
- For the added online device, the displayed device alias is the same as the device IP address.
- If the network transmission device can not be recognized by the system, it will be displayed as unknown device.

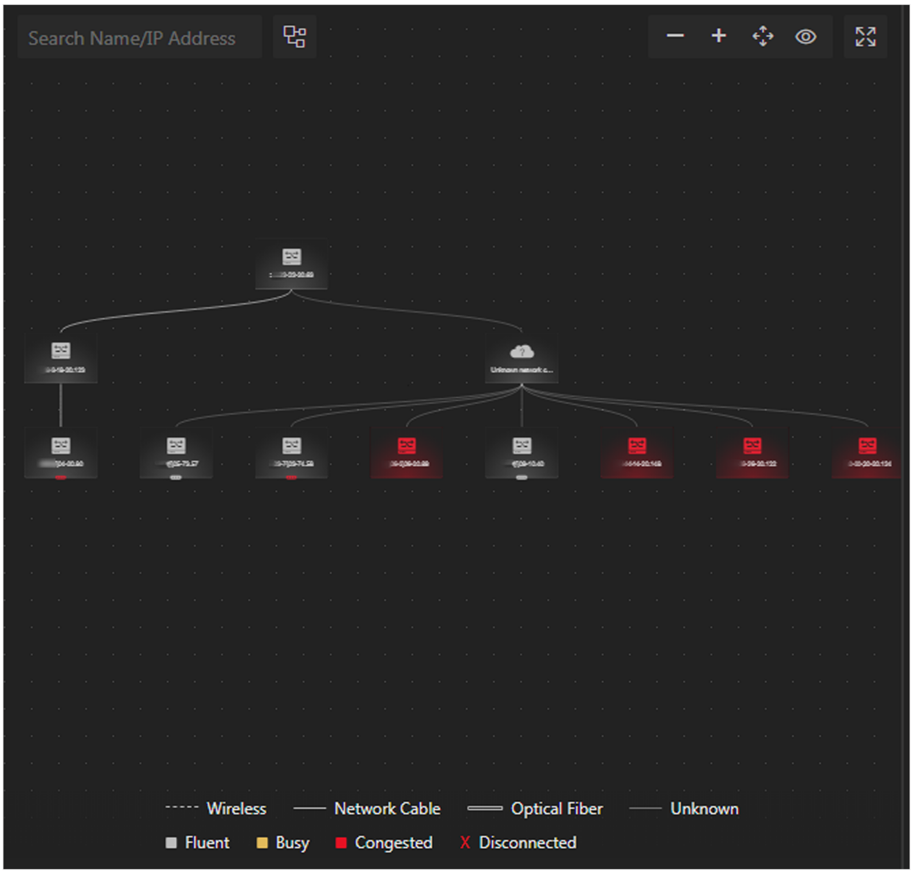


Figure 22-6 Topology Overview

Device Node

- **Display Device Type:** The device nodes are displayed by icons, including HikCentral Professional server, Recording Server, network transmission device, encoding device, access control device, video intercom device, network bridge, fiber converter, etc.
- **Display Information:** Display the device name, IP address in the topology.

Note

- When the device information (device name, IP address, online/offline status) changes, you should manually refresh to generate the topology again or set auto-refresh.
- When the device hierarchy or physical connection changes, you should manually refresh to generate the topology again.

- **Zoom In/Zoom Out:** Click + or — to zoom in or zoom out the device node(s) and the subsidiary device node(s). You can scroll the mouse wheel to zoom in or zoom out the topology.
- **Adjust Topology:** Left click the background of the topology to move the topology in up, down, right, or left direction.
- **Search:** By entering device name or IP address in the search box, you can quickly locate the device on the topology.

Cable Introduction

The color of cable indicates the network bandwidth utilization rate (red: congested, yellow: busy, gray: fluent).
The shape of cable indicates the cable type (wireless, network cable, optical fiber).

Note

If the node icon is displayed in red, it indicates the device is abnormal or alarms happen. You can view the abnormal reason or alarm details. For more details, refer to ***View Device Details*** .

View Device Details

You can view the device details, including basic information, device usage, device panel status and port information.

In the top left corner of Home page, select ≡ → **All Modules** → **Maintenance** → **Health Monitoring** → **Real-Time Overview** .

Select **Topology** in the upper area to open the topology page, and then click the device icon in the topology and click **Details** in the pop-up window.

Note

The device details might be different for different device models.

Basic Information

View the device name, IP address and device model.

Device Usage

View the device network status, RAM usage, CPU usage, PoE power, etc.

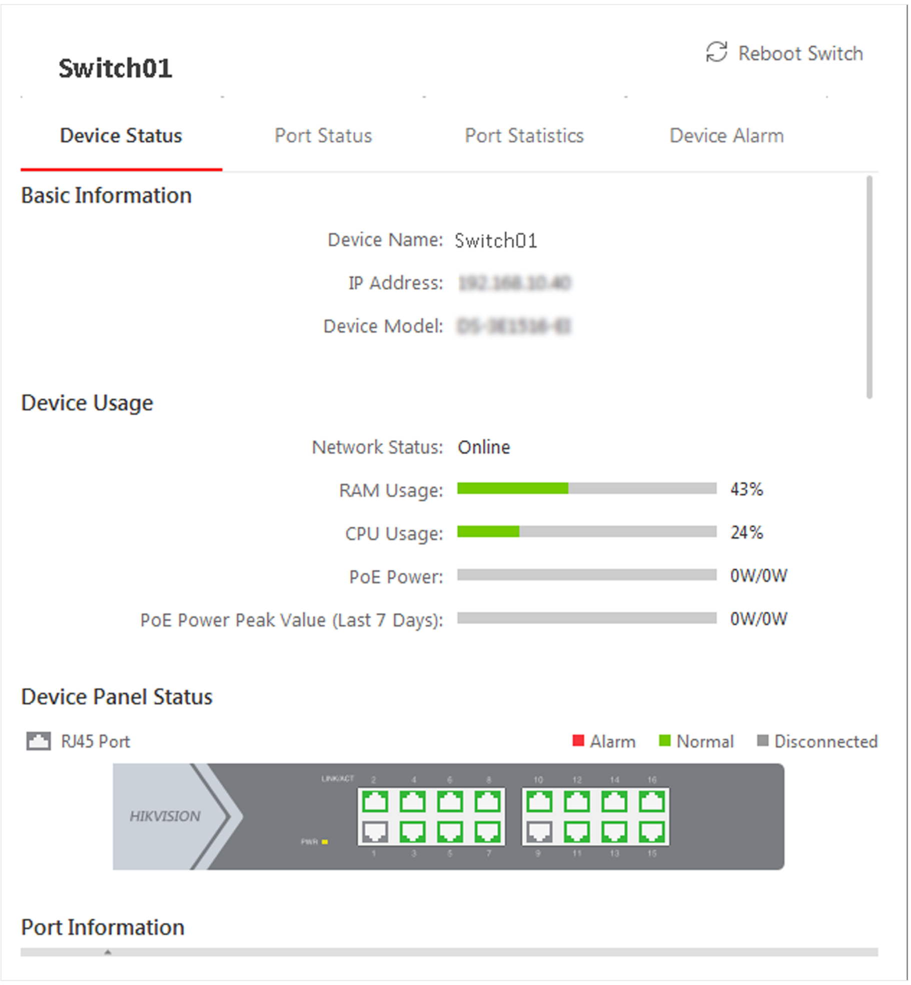
- For the encoding device, you can view the arming status and disk array.
- If the device is linked with camera, you can view the camera's monitoring video. If the camera is linked with entrance & exit, you can view the linked lane name, entrance direction, entrance & exit name. Manually controlling the barrier is also supported.
- For the access control device, you can view the door details, including door status and card reader status.

Device Panel Status

View the ports and ports usage on the panel.

Port Information

View the port name, and peer device type, peer device IP address and peer device name.



Switch01

Reboot Switch

Device Status | Port Status | Port Statistics | Device Alarm

Basic Information

Device Name: Switch01

IP Address: [redacted]

Device Model: [redacted]

Device Usage

Network Status: Online

RAM Usage: 43%

CPU Usage: 24%

PoE Power: 0W/0W

PoE Power Peak Value (Last 7 Days): 0W/0W

Device Panel Status

RJ45 Port

🟥 Alarm 🟩 Normal ▨ Disconnected

Port Information

Figure 22-7 Device Details

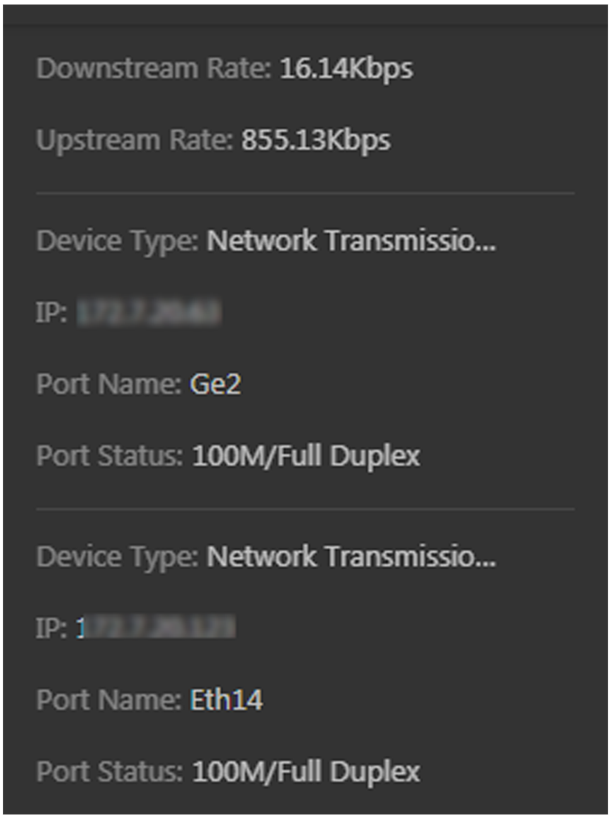
View Link Details

You can view the link details, including stream rate, connected device type and port information, etc.

In the top left corner of Home page, select ≡ → **All Modules** → **Maintenance** → **Health Monitoring** → **Real-Time Overview** .

Select **Topology** in the upper area to open the topology page, move the cursor to the link between nodes in the topology, to display the link details.

You can view the upstream rate and downstream rate to judge whether the network status is normal or not. You can also view the connected device type, IP address, port name and port status.



Downstream Rate: 16.14Kbps

Upstream Rate: 855.13Kbps

Device Type: Network Transmissio...

IP: [redacted]

Port Name: Ge2

Port Status: 100M/Full Duplex

Device Type: Network Transmissio...

IP: [redacted]

Port Name: Eth14

Port Status: 100M/Full Duplex

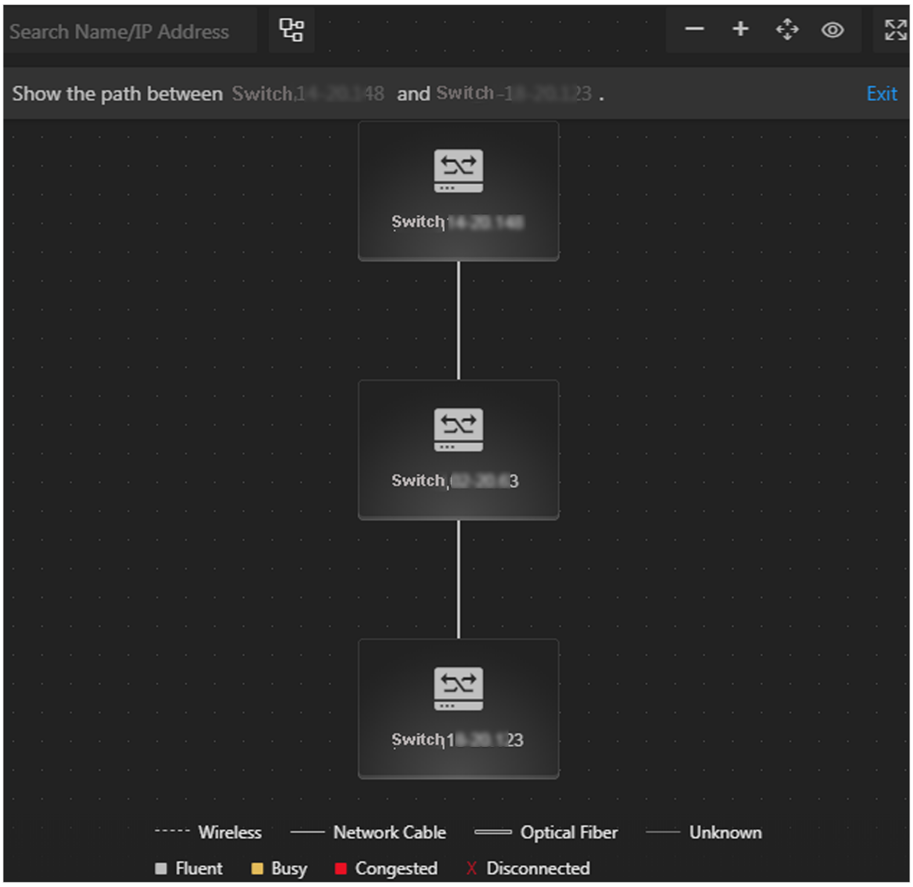
Figure 22-8 View Link Details

View Connection Path

If there is data transmission failure between the devices, you can view the connection path to judge which link is disconnected, to maintain the link efficiently.

In the top left corner of Home page, select ≡ → **All Modules** → **Maintenance** → **Health Monitoring** → **Real-Time Overview** .

Select **Topology** in the upper area to open the topology page. Click the node to be viewed, and then select **Show Connection Path**. According to the hint information on the upper side, click **Please select nodes.** to select the peer node, and then click **OK**. After that, the connection link path between the two nodes will be displayed.



Show the path between Switch.1[redacted]48 and Switch-1[redacted]23 .

Figure 22-9 Device Connection Path

Export Real-Time Status Overview Report

You can export the real-time status overview page in PDF format, or export the exception data in Excel/CSV format.

In the top left corner of Home page, select ≡ → **All Modules** → **Maintenance** → **Health Monitoring** → **Real-Time Overview** .

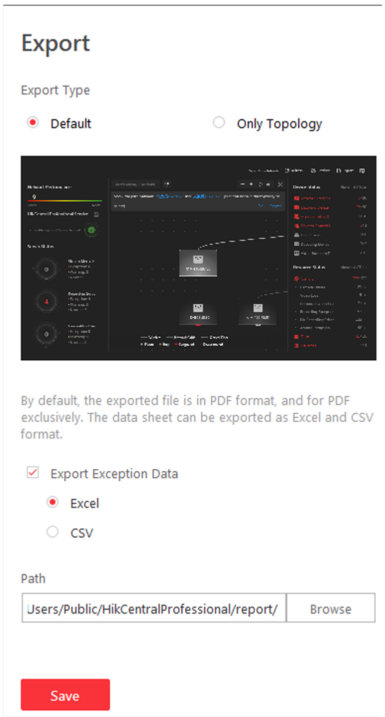
Select **Topology** in the upper area to open the topology page, and then click **Export** in the upper-right corner. Select the export type as **Default** or **Only Topology**.

Default

By default, the whole displaying information on the Real-Time Overview page will be exported.

Only Topology

If you select **Only Topology**, only the topology will be exported.



Export

Export Type

● Default ○ Only Topology

By default, the exported file is in PDF format, and for PDF exclusively. The data sheet can be exported as Excel and CSV format.

☑ Export Exception Data

● Excel

○ CSV

Path

Users/Public/HikCentralProfessional/report/ Browse

Save

Figure 22-10 Export Report

More Functions

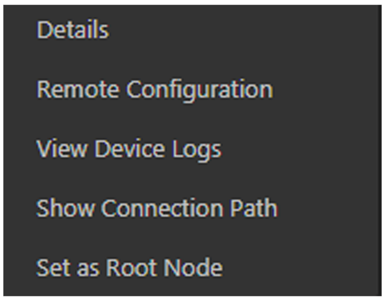
In the topology, more functions are supported, including the entrance of device remote configuration, viewing device logs, setting device as root node, to manage the network conveniently.

Note

The functions might be different for different device models.

In the top left corner of Home page, select ≡ → **All Modules** → **Maintenance** → **Health Monitoring** → **Real-Time Overview** .

Select **Topology** in the upper area to open the topology page. Click one device node in the topology to view more functions.



Details

Remote Configuration

View Device Logs

Show Connection Path

Set as Root Node

Figure 22-11 More Functions

Remote Configuration

Configure the device parameters, including system settings, network and port configuration. You can configure the network parameters and device port according to the network usage. For details, refer to the user manual of the device.

View Device Logs

When a device failure happens or trouble shooting is required, you can view the device logs to know the alarms, notifications, operations and events of the device.
Enter the Device Logs page, and the set the filter condition to search the device logs.

Set as Root Node

When you need to adjust the topology structure, you can set the node as the root node.

Note

Only switch, wireless network bridge and fiber converter can be set as root node.

Others

Click ⛶ on the upper-right corner of the topology to display the topology in full-screen. Click 👁 on the upper-right corner of the topology to display the thumbnail of the whole topology, to help you know the topology hierarchy quickly.

22.1.5 History Overview

You can view the overview of history resource online rate, device online rate, and recording integrity rate.

In the top left corner of Home page, select ≡ → **All Modules** → **Maintenance** → **Health Monitoring** → **History Overview** to enter the History Overview page.

You can select a time period from the drop-down list for filtering data.

You can also click **Export** to export the history overview to the local PC. For details, see ***Export Data*** .

Resource Online Rate

On the line chart, you can perform the following operations.

- Move the cursor on the line chart to view the camera online rate and the number of offline cameras at specific time points.
- Click the a dot on the line to go to Resource Log page to view the detailed network status of cameras at that time point.

On the doughnut chart, you can perform the following operations.

- Move the cursor to red part of the doughnut chart to view the number of the cameras which once were offline and the offline rate during the time period you select.
- Move the cursor to the green part of the doughnut chart to view the number of the cameras which stay online and the online rate during the time period you select.

On the table, you can do one of the followings.

- Click **Total Offline Duration** to rank the cameras in terms of total offline duration within the time period you select.
- Click **Offline Times** to rank the cameras in terms of offline times within the time period you select.

Device Online Rate

On the line chart, you can do one of the followings.

- Move the cursor on the line chart to view the device online rate and the number of offline devices at specific time points.
- Click the a dot on the line to go to Device Log page to view the detailed network status of devices at that time point.

On the doughnut chart, you can perform the following operations.

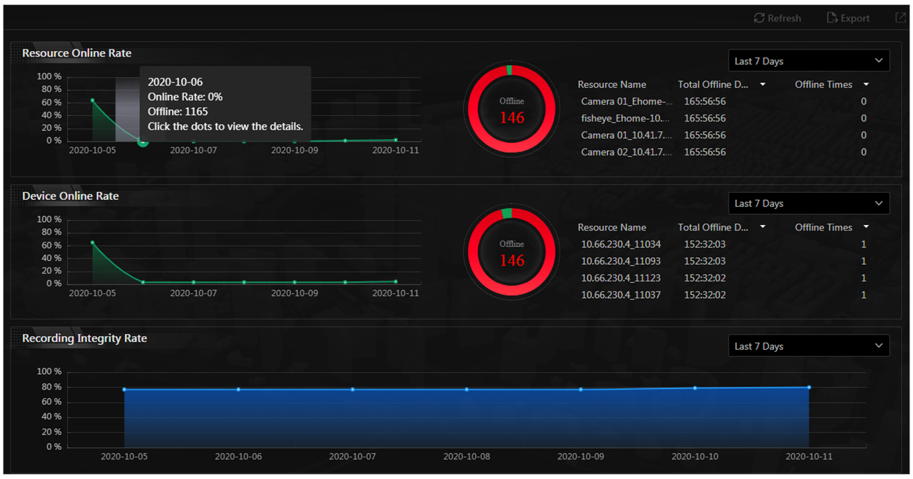
- Move the cursor to red part of the doughnut chart to view the number of the devices which once were offline and the offline rate during the time period you select.
- Move the cursor to the green part of the doughnut chart to view the number of the devices which stay online and the online rate during the time period you select.

On the table, you can do one of the followings.

- Click **Total Offline Duration** to rank the devices in terms of total offline duration within the time period you select.
- Click **Offline Times** to rank the devices in terms of offline times within the time period you select.

Recording Integrity Rate

On the line chart, you can move the cursor to view the recording integrity rate at specific time points. Click the a dot on the line to go to Device Log page to view the detailed resource status of devices at that time point.



2020-10-06
Online Rate: 0%
Offline: 1165
Click the dots to view the details.

Resource Name	Total Offline D...	Offline Times
Camera 01_Ehome-...	165:56:56	0
fisheye_Ehome-10....	165:56:56	0
Camera 01_10.41.7....	165:56:56	0
Camera 02_10.41.7....	165:56:56	0

Resource Name	Total Offline D...	Offline Times
10.66.230.4_11034	152:32:03	1
10.66.230.4_11093	152:32:03	1
10.66.230.4_11123	152:32:02	1
10.66.230.4_11037	152:32:02	1

Figure 22-12 History Overview

22.2 Resource Status

You can monitor the near-real time status of the added resources, such as Recording Servers, Streaming Servers, and encoding devices, to find out and maintain the abnormal resources in time, ensuring the smooth running of the system to the greatest extent.

On the top left corner of Home page, select ≡ → **All Modules** → **Maintenance** → **Resource Status** , and select a resource type on the navigation panel on the left.

The resource status will be automatically refreshed in a specified interval. You can also click **Refresh** to refresh all the resource status manually.

Note

For details about specifying the interval for refreshing resource status, see ***Set Topology Show Parameters*** .

You can perform the following operations for different resource types.

- Check **Include Sub-area** to display the cameras of child areas.
- Check the check box beside the drop-down list on the upper-right and then select an abnormal type (such as **Camera Offline** and **Video Loss** to filter data.
- Click **Export** to export the status data as CSV or Excel to the local PC.

Camera Status

On the camera status page, you can view camera status such as network status, arming status, and recording status.
You can also perform the following operations.

- Click the camera name to view its status and basic information.
- Click the IP address to view the status of the device to which the camera is connected to.

- Click in the Operation column to view the online/offline records of the camera. For details, see ***Search Online/Offline Logs of Resource*** .
- Click in the Operation column to view the recording status of the camera. For details, see ***Search Recording Status of Resource*** .
- Click in the Operation column to go to the HikCentral Professional Web Client to configure the camera parameters.

Note

Contact the admin user to edit the exceptional configuration of camera's event or alarm via the Web Client if an icon ⓘ appears near the camera name.

Door Status

On the door status page, you can view the information such as the network status of the access control device and the door status.

Note

For the door linked to the video intercom device, the door status is not available to be displayed.

You can click in the Operation column to go to the HikCentral Professional Web Client to configure the door parameters.
You can click the door status icon in the Operation column to control the door status.

Unlock

When the door is locked, unlock the door and it will be open. After the open duration (configured via the Web Client), the door will be closed and locked again automatically.

Lock

When the door is unlocked, lock the door and it will be closed. The person who has the access permission can access the door with credentials.

Remain Unlocked

The door will be unlocked (no matter closed or open). All the persons can access the door with no credentials required (free access).

Note

For the door linked to video intercom device, setting its status to remain unlocked is not available.

Remain Locked

The door will be closed and locked. No person can access the door even if he/she has the authorized credentials, except the super users.

Remote Site Status

You can view the remote site status such as network status and default stream.

You can click 🌐 or 🌐 in the Operation column to switch the mode for accessing the resources on Remote Site between Automatically Judge mode and 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.

You can click **Restore All Network Connections** to restore the connection mode of all the added Remote Site's resources to Automatically Judge mode.

The **Default Stream** in the table refers to the default stream type for accessing the resources on the Remote Site. You can select the Remote Site(s) and click **Switch Stream** to switch the stream type. When starting live view of the Remote Site's resources in Central System, the Control Client will get this default stream to start live view.

- **Main Stream:** Main stream provides higher quality video, higher resolution, but brings about higher bandwidth usage.
- **Sub-Stream:** Sub stream can save on bandwidth, but the video quality is lower than main stream.
- **Smooth Stream:** This stream type is usually used in low-bandwidth situation. After switching to smooth stream, the live view and playback will be smoother in slow network performance, but the image quality will be lower accordingly.
- **Default Stream Type:** If you select **Default Stream Type**, the stream type for accessing the selected Remote Site's resources will be restored to the global stream type you set in **System → General** .

Alarm Input Status

You can view the alarm input status including resource usage status (online or offline), arming status, bypass status, fault status, alarm status, detector connection status, battery status, etc.

Streaming Server Status

You can view the streams via each added Streaming Server (including incoming streams and outgoing streams), and view the hardware status such as network status, CPU usage, and RAM usage.

Recording Server Status

Click the status in **Recording Status** column to view the recording status of the channels configured to store the video files in this Recording Server.

Click the status in **Hardware Status** or **HDD Status** column to view the hardware status and HDD exception details if the status is exceptional.

DeepinMind Server Status

You can view the network status, CPU usage, and RAM usage, etc., of the DeepinMind servers.

Security Audit Server Status

You can view the HDD status, network status, and first added time, etc., of the audit server.

Encoding Device Status

You can view the encoding device status including recording status, HDD usage, default stream, etc. In the Operation column, you can perform the following operations.

- Click in the Operation column to view the online/offline records of the encoding device. For details, see ***Search Online/Offline Logs of Device*** .
- Click in the Operation column to go to the HikCentral Professional Web Client to configure the device parameters.

Click the status in **Recording Status** column to view the recording status of the channels configured to store the video files in this Recording Server.
Click **Switch Device Access Mode** to switch the access mode for the Control Client to access the devices.

- **Restore Default**: Restore the device access mode as configured in the **System → Device Access Mode** on the Web Client.
- **Automatically Judge**: Judge the device access mode according to the current network.
- **Directly Access**: Access the device directly, not via HikCentral Professional Streaming Service.

> **Note**
>
> When the encoding device is in the same LAN with the SYS server, the Direct Access mode is not available.

- **Proxy**: Access the device via HikCentral Professional Streaming Gateway and HikCentral Professional Management Service. It is less effective and less efficient than accessing directly.

The **Default Stream** in the table refers to the default stream type for accessing the resources of the encoding device. You can select the encoding device(s) and click **Switch Stream** to switch the stream type. When starting live view, the Control Client will get this default stream to start live view of the encoding device's resources.

- **Main Stream:** Main stream provides higher quality video, higher resolution, but brings about higher bandwidth usage.
- **Sub-Stream:** Sub stream can save on bandwidth, but the video quality is lower than main stream.
- **Smooth Stream:** This stream type is usually used in low-bandwidth situation. After switching to smooth stream, the live view and playback will be smoother in slow network performance, but the image quality will be lower accordingly.
- **Default Stream Type:** If you select **Default Stream Type**, the stream type for accessing the selected encoding device(s) will be restored to the global stream type you set in **System → General** .

Access Control Device Status

You can view the network status and battery status of the added access control devices.
If the device is turnstile, you can view the status of master lane controller, slave lane controller, and component.

Click 🖥 in the Operation column to go to the HikCentral Professional Web Client to configure the device parameters.

Security Control Panel Status

You can view the managed devices' network status and battery status.
Click 🖥 in the Operation column to go to the HikCentral Professional Web Client to configure the device parameters.

Dock Station Status

You can view the network status and HDD status of the added dock station.
Click 🖥 in the Operation column to go to the HikCentral Professional Web Client to configure the dock station parameters.

Decoding Device Status

You can view the status information such network status, first added time, and checking time.

Video Intercom Device Status

You can view the status information of the video intercom device such as network status, arming status, and the status of calling center from device.

Calling Center from Device

Whether the device is able to call the surveillance center of the system.

You can perform the following operations:

- Filter Device Type: Click **All Devices** and then select a type a video intercom device to display the selected type only.
- Configure Device Parameter: Click 🖥 in the Operation column to go to the HikCentral Professional Web Client to configure the device parameters.

22.3 Log Search

Three types of log files are provided: server logs, device logs, and resource logs. The server logs refer to the logs files stored in the SYS server on the Current Site and the Remote Site; The device logs refer to the log files stored on the connected devices, such as encoding device and security control device; The resource logs refers the logs about camera recording status and online status. You can search the log files, view the log details and backup the log files.

22.3.1 Search Server Logs for Current Site

You can search for server logs of the current site, which contain error logs, warning logs and information logs. Server logs contain historical user and server activities. You can search for the logs and then check the details.

Follow the steps to search for the server logs in your current site.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **Maintenance** → **Audit Trail** .
2. Select **Server Logs** on the left.

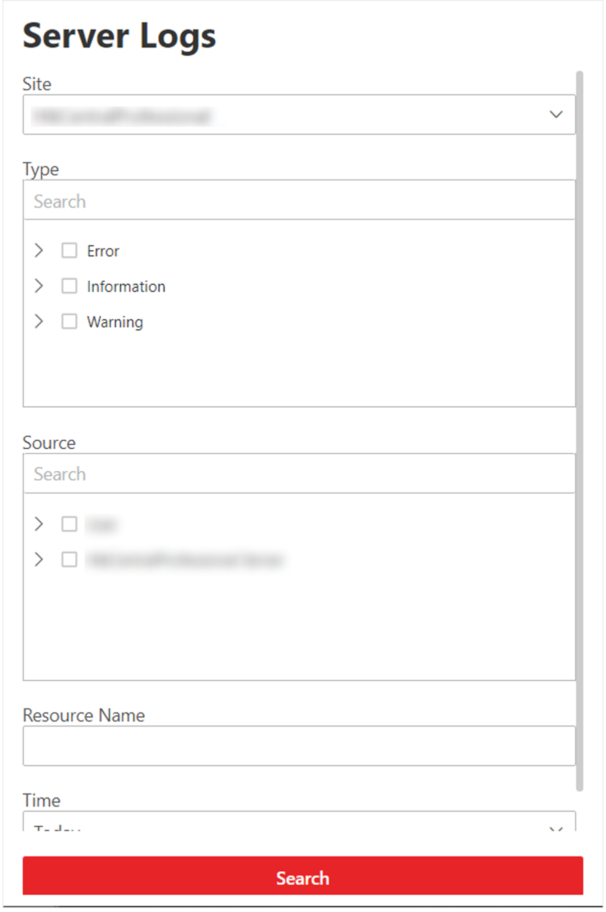


Figure 22-13 Search for Server Logs

3. In **Site**, select the current site.
4. In **Type**, select one or multiple log types and sub types.

Note

Error logs record failures or errors. Warning logs record license expiration events. Information logs refer to other general logs which record successful or unknown operation results.

5. In **Source**, select user and server to set the source of the logs that you want to search for.
6. **Optional:** In **Resource Name**, enter the name of a resource to search the logs of the resource.
7. In **Time**, select the time range of this search.

Note

You can select **Custom Time Interval** to set a precise start time and end time.

8. Click **Search**.

All matched logs are listed with details on the right.

22.3.2 Search Server Logs for Remote Site

You can search for server logs of a remote site, which contain error logs, warning logs and information logs. Server logs contain historical user and server activities. You can search for the logs and then check the details.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **Maintenance** → **Audit Trail** .
2. Select **Server Logs** on the left.
3. In **Site**, select a remote site.
4. In **Type**, select one or multiple log types and sub types.

Note

- Error logs record failures or errors. Warning logs record license expiration events. Information logs refer to other general logs which record successful or unknown operation results.
- For some earlier versions of remote site, only information logs can be searched.

5. In **Source**, select user and server to set the source of the logs that you want to search for.
6. **Optional:** In **Resource Name**, enter the name of a resource to search the logs of the resource.
7. In **Time**, select the time range of this search.

Note

You can select **Custom Time Interval** to set a precise start time and end time.

8. Click **Search**.

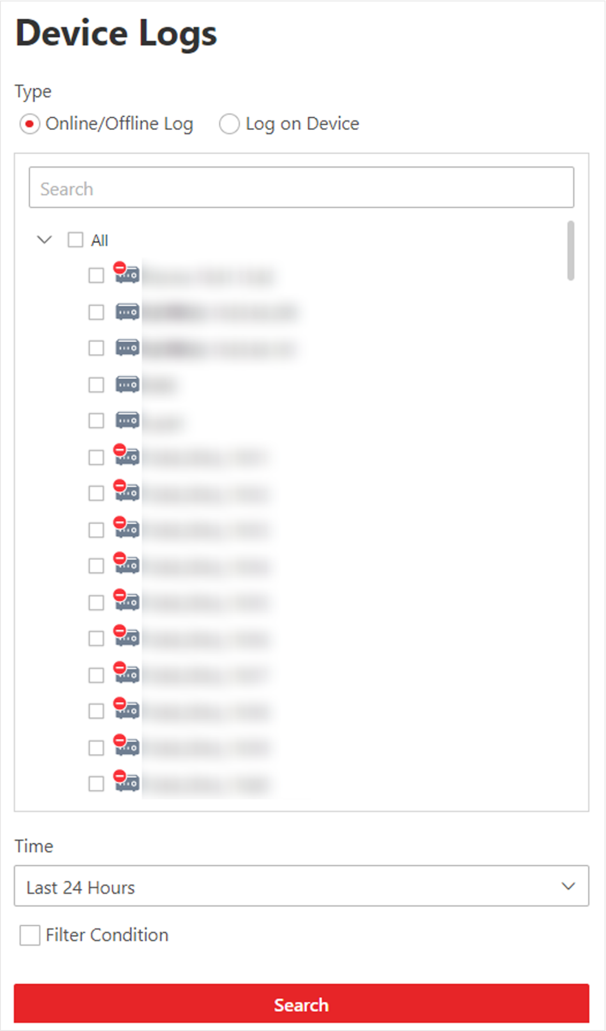
All matched logs are listed on the right with details.

22.3.3 Search Online/Offline Logs of Device

You can search the online/offline logs of encoding devices. The online/offline logs provide information on current device status (online or offline), latest offline time, total offline duration, etc.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **Maintenance** → **Audit Trail** .
2. Select **Device Logs** on the left.
3. In **Type**, select **Online/Offline Log** as the log type.



Device Logs

Type

● Online/Offline Log ○ Log on Device

Time

Last 24 Hours

□ Filter Condition

Figure 22-14 Search for Device Online/Offline Logs

4. In the device list, select the devices to be searched.
5. In **Time**, specify the time range of this search.

Note

You can select **Custom Time Interval** to set a precise start time and end time.

6. **Optional:** If there are a large number of devices, check **Filter Condition** to set a range of total offline times during the specified time range to filter the devices.
7. Click **Search**.

   The offline/online log of each device are listed on the right. You can check the name, IP address, current status (online/offline), latest offline time, total offline times, and total offline duration of each device.
8. **Optional:** Perform further operations after searching for device logs.

View Offline History

Click on device name to view history online duration (displayed as a line chart) and status (displayed as a list) of the device.

You can perform the following operations.

- Filter Data: Select a time period and a status (online, offline or all) from the drop-down lists respectively to filter the data.
- View Details: Move the cursor to the line chart to view the detailed offline and online duration at each time point.

View Device Logs

Click in the Operation column to view the logs on the device.

Export Logs

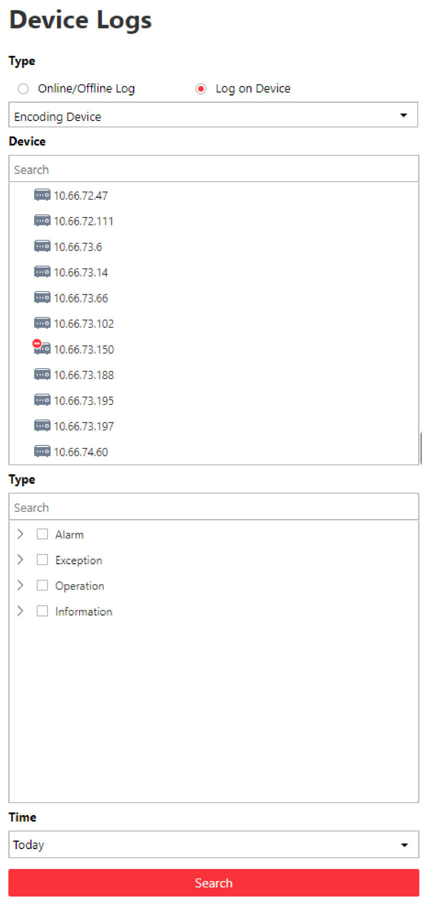
Click **Export** and then select a file format to download the searched logs as a single file to your local PC.

22.3.4 Search Device Logs

You can search the logs stored on encoding devices, security control devices, decoding device, and access control devices.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **Maintenance** → **Audit Trail** .
2. Select **Device Logs** on the left.
3. Select **Log on Device** as the log type.



Device Logs

Type

○ Online/Offline Log ● Log on Device

Encoding Device

Device

Search

10.66.72.47
10.66.72.111
10.66.73.6
10.66.73.14
10.66.73.66
10.66.73.102
10.66.73.150
10.66.73.188
10.66.73.195
10.66.73.197
10.66.74.60

Type

Search

□ Alarm
□ Exception
□ Operation
□ Information

Time

Today

Search

Figure 22-15 Search for Logs on Device

4. Select a device type and the device you want to search.
5. Select one or multiple log types and sub types to search for.
6. Specify the time range of this search.

Note

You can select **Custom Time Interval** to specify a precise start time and end time.

7. Click **Search**.

   All matched logs are listed with details on the right.

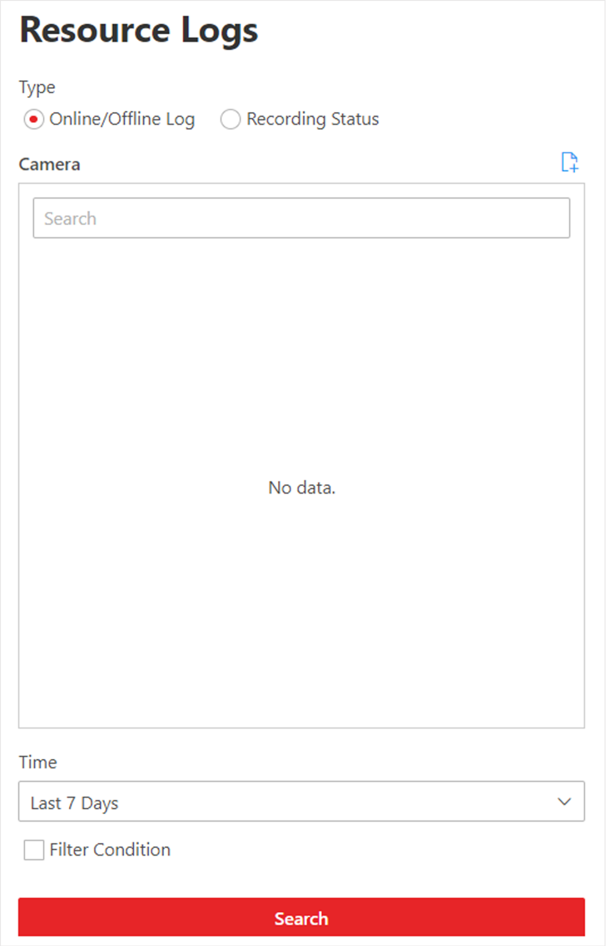
22.3.5 Search Online/Offline Logs of Resource

You can search the online/offline logs of cameras. The online/offline logs provide information on current device status (online or offline), latest offline time, total offline duration, etc.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **Maintenance** → **Audit Trail** .
2. Select **Resource Logs** on the left.

3. In **Type**, select **Online/Offline Log**.



Resource Logs

Type

● Online/Offline Log ○ Recording Status

Camera

Search

No data.

Time

Last 7 Days

□ Filter Condition

Figure 22-16 Search for Resource Online/Offline Logs

4. Click to show the area list and then select the cameras you want to search in the list.

   Selected cameras are added to the **Apply to Camera** list.

5. **Optional:** Modify your selection in the **Apply to Camera** list.

Remove a Camera	Click of a camera to remove the camera from the list.
Remove All Cameras	Click to remove all cameras in the list.

6. In **Time**, specify the time range of this search.

Note

You can select **Custom Time Interval** to set a precise start time and end time.

7. **Optional:** If there are a large number of resources, check **Filter Condition** to set a range of total offline times during the specified time range to filter the resources.
8. Click **Search**.

The offline/online log of each resource are listed on the right. You can view the name, IP address, current status (online/offline), latest offline time, total offline times, and total offline duration of each resource.

9. **Optional:** Perform further operations after searching fro resource logs.

View Offline History

Click resource name to view history online duration (displayed as a line chart) and status (displayed as a list) of the resource.

You can perform the following operations.

- Filter Data: Select a time period and a status (online, offline or all) from the drop-down lists respectively to filter data.
- View Details: Move the cursor to the line chart to view the detailed offline and online duration at each time point.

View Device Online/ Offline Logs

Click the IP address to view the online/offline logs of the device where the resource is linked.

Export Logs

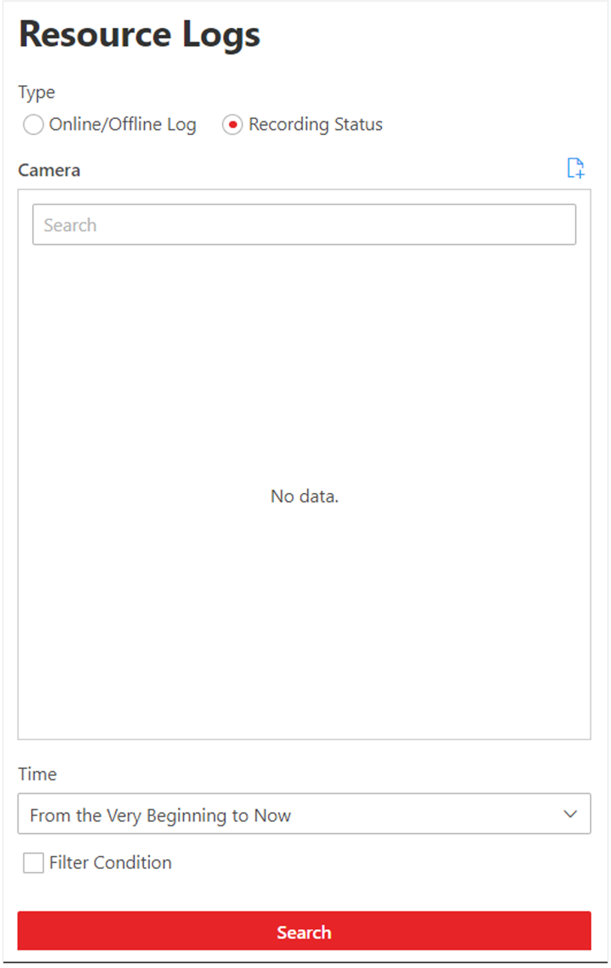
Click **Export** and then select a file format to download the searched logs as a single file to your local PC.

22.3.6 Search Recording Status of Resource

You can search the recording status of cameras. The recording status includes recording integrity rate, total time length abnormal recording, times of recording interruptions, etc.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **Maintenance** → **Audit Trail** .
2. Select **Resource Logs** on the left.
3. In **Type**, select **Recording Status**.



Resource Logs

Type

○ Online/Offline Log ● Recording Status

Camera

Search

No data.

Time

From the Very Beginning to Now

□ Filter Condition

Search

Figure 22-17 Search for Resource Recording Status

4. Click to show the area list and then select the cameras you want to search in the list.

   Selected cameras are added to the **Apply to Camera** list.

5. **Optional:** Modify your selection in the **Apply to Camera** list.

   Remove a Camera Click and then click to remove a camera from the list.

   Remove All Cameras Click and then click to remove all cameras in the list.

6. In **Time**, specify the time range of this search.

   Note

   You can select **Custom Time Interval** to set a precise start time and end time.

7. **Optional:** If there are a large number of resources, check **Filter Condition** and set the filter conditions.

   Retention Duration (Days)

   Set a range of the retention duration of the recorded video footage to filter the cameras.

Recording Integrity Rate

Set a range of the recording integrity rate to filter cameras. The recording integrity rate refers to the percentage obtained from dividing the actual recording duration by the scheduled recording time.

Note

For details about recording schedule, refer to ***Configure Recording Schedule Template*** .

8. Click **Search**.

   Recording status of each camera are listed on the right, including camera name, camera IP address, area where the camera belong, video storage type, etc.

   Start Time

   The time when the camera started recording.

   End Time

   The latest time when the camera was recording.

   Retention Duration (Days)

   The retention duration (unit: day) of the recorded video footage refers to the duration between **Start Time** and **End Time**.

   Total Length

   The total time length of video storage.

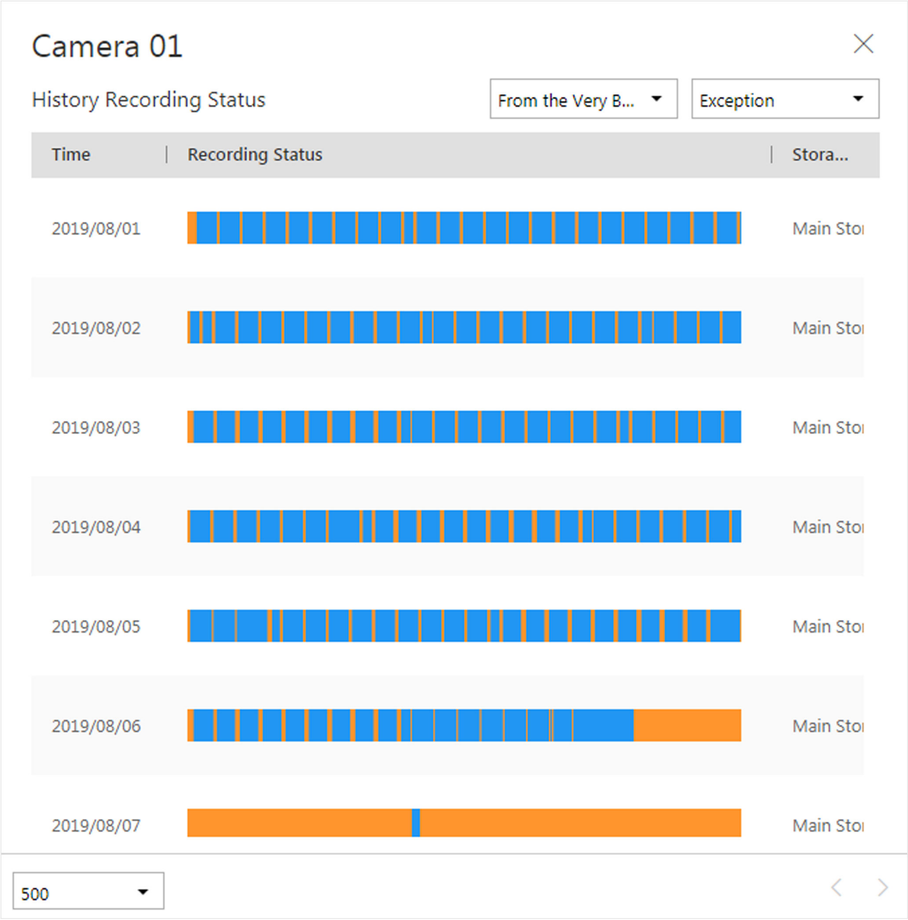
   Abnormal Total Length

   The total time length of the video loss within the scheduled time.

   Recording Interruption

   The total times of recording interruption within the scheduled time.

9. **Optional:** Check history recording status.
   1) Click camera name to open the History Recording Status panel.



Camera 01

History Recording Status

From the Very B... ▾ Exception ▾

Time	Recording Status	Stora...
2019/08/01		Main Sto
2019/08/02		Main Sto
2019/08/03		Main Sto
2019/08/04		Main Sto
2019/08/05		Main Sto
2019/08/06		Main Sto
2019/08/07		Main Sto

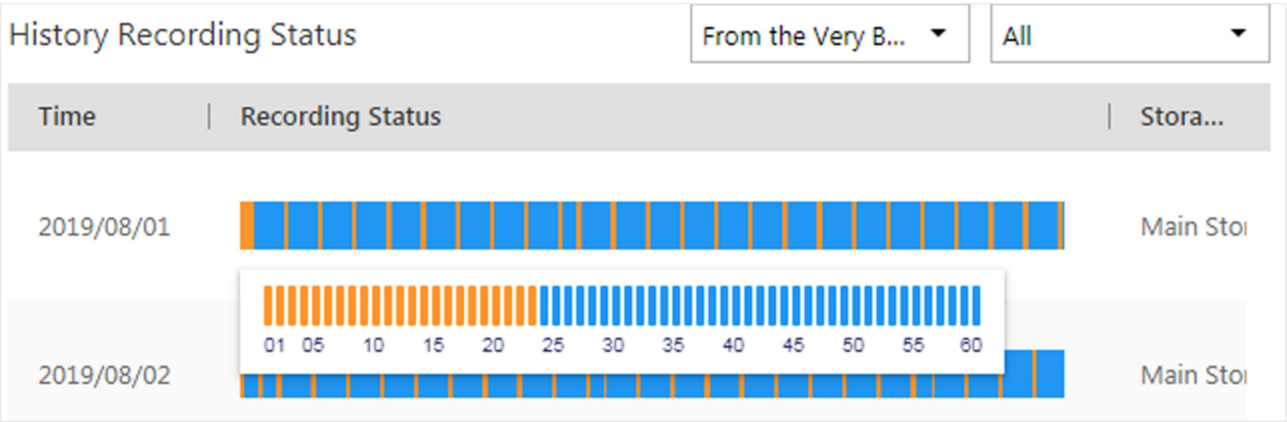
500 ▾

Figure 22-18 History Recording Status

Note

The blue parts on the time bars represent the time periods during which video footage were recorded. The orange parts on the time bars represent the time periods during which video loss occurred or the time periods during which no recording schedule exists.

2) Select a time period and a status (exception or all) from the drop-down lists respectively to filter data.
3) **Optional:** Select the number of records displayed on each page of the History Recording Status panel from the drop-down list at the lower-left corner of the panel.
4) **Optional:** Move the cursor to the time bar to show the 24 hours on it, and click one hour to view recording status details within the hour.



History Recording Status

From the Very B... ▼ | All ▼

Time	Recording Status	Stora...
2019/08/01		Main Stoı
2019/08/02		Main Stoı

Figure 22-19 Recording Status Details within One Hour

22.3.7 Back Up Logs

After searching for logs, you can export the matched logs into a log file and save to local storage for backup.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **Maintenance** → **Audit Trail** .
2. Search for logs.
3. Click **Export** in the top-right corner.
4. In Export panel, select **Excel** or **CSV** as the format of the log file.
5. Click **Save** to download the log file.

22.4 Send Report Regularly

You can configure the platform to send device and resource log reports to you regularly via email. Device log reports contain information on device online/offline status. Resource log reports contain resource online/offline status and recording status.

22.4.1 Send Device Log Report Regularly

You can set report sending rules for encoding devices, and the system can send emails with device log reports to you daily, weekly, or monthly.

Before You Start

- Make sure you have set an email template with recipient information, subject, and content. For details, refer to ***Set Email Template*** .
- Make sure you have configured 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 is an Excel file.

1. In the top left corner of Home page, select ≡ → **All Modules** → **Maintenance** → **Basic Settings** .
2. Select **Timing Report Configuration** on the left.
3. Click + to create a new report rule.
4. In **Report Category**, select **Device Logs**.
5. Edit the report rule.

   Report Name

   Create a name for the report.

   Report Target

   Specify the devices that you want to add into the report.

   Report Content

   Select the log content to be included in the report.

   Report Type

   Select the generation frequency of the report. You can set a sending time in **Send At**.

   Daily

   Daily report shows data on a daily basis. The system will send a report at the sending time every day, which contains logs recorded during the day (24 hours) prior to the sending date.

   For example, if you set the sending time as 20:00, the system will send a report at 20:00 every day. The report contains the logs recorded between 00:00 and 24:00 of the previous day.

   Weekly/Monthly

   The system will send a report at the sending time every week or every month, which contains logs recorded during the past 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. The report contains logs recorded between last Monday and Sunday.

   Send At

   Set a report sending time.

   Email Template

   Select an email template to define the recipient information and content.

Note

You can click **Add New** to add a new email template. For setting email template, refer to ***Set Email Template*** .

Report Language

Select a report language.

6. Click **Add** to save the report rule.

22.4.2 Send Resource Log Report Regularly

You can set report sending rules for camera resources, and the platform can send emails with resource log reports to you daily, weekly, or monthly.

Before You Start

- Make sure you have set an email template with recipient information, subject, and content. For details, refer to ***Set Email Template*** .
- Make sure you have configured 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 is an Excel file.

1. In the top left corner of Home page, select ≡ → **All Modules** → **Maintenance** → **Basic Settings** .
2. Select **Timing Report Configuration** on the left.
3. Click + to create a new report rule.
4. In **Report Category**, select **Resource Logs**.
5. Edit the report rule.

   Report Name

   Create a name for the report.

   Report Target

   Specify the resources that you want to add into the report.

   Report Content

   Select the log content to be included in the report.

   Report Type

   Select the generation frequency of the report. You can set a sending time in **Send At**.

   Daily

Daily report shows data on a daily basis. The platform will send a report at the sending time every day, which contains logs recorded during the day (24 hours) prior to the sending date.

For example, if you set the sending time as 20:00, the platform will send a report at 20:00 every day. The report contains the logs recorded between 00:00 and 24:00 of the previous day.

Weekly/Monthly

The platform will send a report at the sending time every week or every month, which contains logs recorded during the past 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 platform will send a report at 6:00 in the morning on every Monday. The report contains logs recorded between last Monday and Sunday.

Send At

Set a report sending time.

Email Template

Select an email template to define the recipient information and content.

Note

You can click **Add New** to add a new email template. For setting email template, refer to ***Set Email Template*** .

Report Language

Select a report language.

6. Click **Add** to save the report rule.

22.5 Set Warning Threshold for Server Usage

You can enable the system to trigger an alarm if the SYS 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.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **Maintenance** → **Basic Settings** → **Server Usage Thresholds** .
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 Event and Alarm***), the alarm will be triggered when the CPU usage reaches the warning threshold and lasts for 20 seconds.

22.6 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.

In top left corner of Home page, select ≡ → **All Modules** → **Maintenance** → **Basic Settings** → **Network Timeout** .

The minimum default waiting time of the interactions between the configurations and SYS server is 60s, the minimum time between SYS server and devices is 5s, and the minimum time between the configurations and devices is 5s.

Note

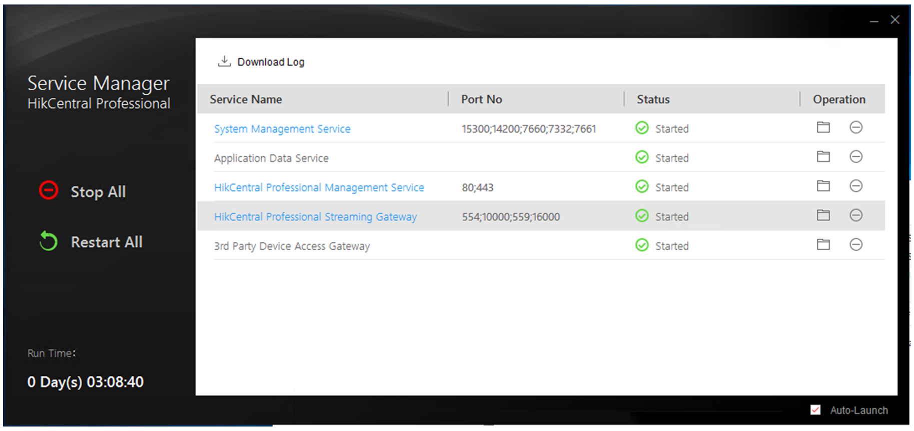
This parameter affects all the Web Clients accessing the current SYS server.

22.7 Service Manager

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

Steps

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



Service Name	Port No	Status	Operation
System Management Service	15300;14200;7660;7332;7661	Started	
Application Data Service		Started	
HikCentral Professional Management Service	80;443	Started	
HikCentral Professional Streaming Gateway	554;10000;559;16000	Started	
3rd Party Device Access Gateway		Started	

Run Time:

0 Day(s) 03:08:40

Figure 22-20 Service Manager Main Page

Note

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

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

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

   Restart All
   Click **Restart All** to run all the services 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.

22.8 Set System Data Backup

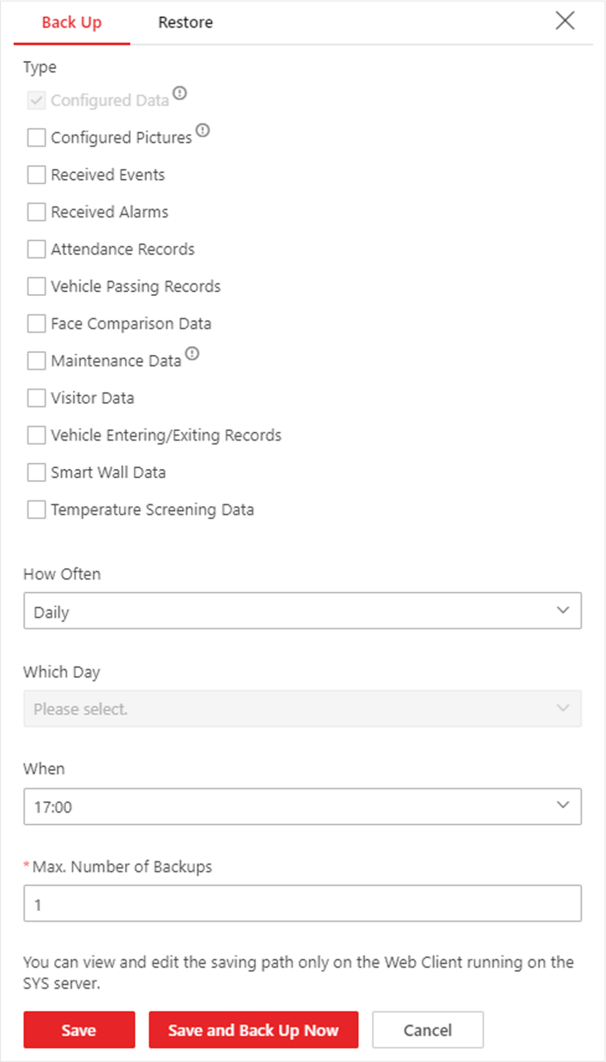
For purpose of restoring the original system data after a data loss event or recovering data from an earlier time, you can manually back up system data, or configure a schedule to back up regularly. System data includes data configured in the system, pictures, received events and alarms, face comparison data, card swiping data, maintenance data, etc.

Steps

Note

The backups are stored in the SYS server. You can edit the saving path only on the Web Client running on the SYS server.

1. In the top right of the client, click **Maintenance and Management → Back Up and Restore System Data** .
2. Select the **Back Up** tab.



Type

☑ Configured Data

□ Configured Pictures

□ Received Events

□ Received Alarms

□ Attendance Records

□ Vehicle Passing Records

□ Face Comparison Data

□ Maintenance Data

□ Visitor Data

□ Vehicle Entering/Exiting Records

□ Smart Wall Data

□ Temperature Screening Data

How Often: Daily

Which Day: Please select.

When: 17:00

*Max. Number of Backups: 1

You can view and edit the saving path only on the Web Client running on the SYS server.

Figure 22-21 Set System Data Backup

3. In **Type**, select the system data that you want to back up.

Configured Data

Data configured via the Web Client, including resources, user permissions, etc. It is selected by default.

Configured Pictures

Pictures uploaded when configuring maps, persons, vehicles, etc.

Maintenance Data

Maintenance data includes received events/alarms, etc.

Note

- Person access records are the access records on the card readers of doors with credentials.
- Device recorded data includes the data recorded by the access control devices, video intercom devices, and alarm inputs of these devices, and other records except access records on the doors.

4. Set a backup schedule to run backup regularly.
   1) In **How Often**, select the frequency to back up the system data.
   2) In **Which Day** and **When**, specify which time to back up.
   3) In **Max. Number of Backups**, set the maximum number of backup files. Old backup files will be automatically deleted.

   Note

   The value ranges from 1 to 5.
5. Save the settings.
   - Click **Save** to save the backup schedule.
   - Click **Save and Back Up Now** if you need to back up the system data immediately.

22.9 Restore System Data

When an exception occurs, you can restore the system data if you have backed up system data before.

Before You Start

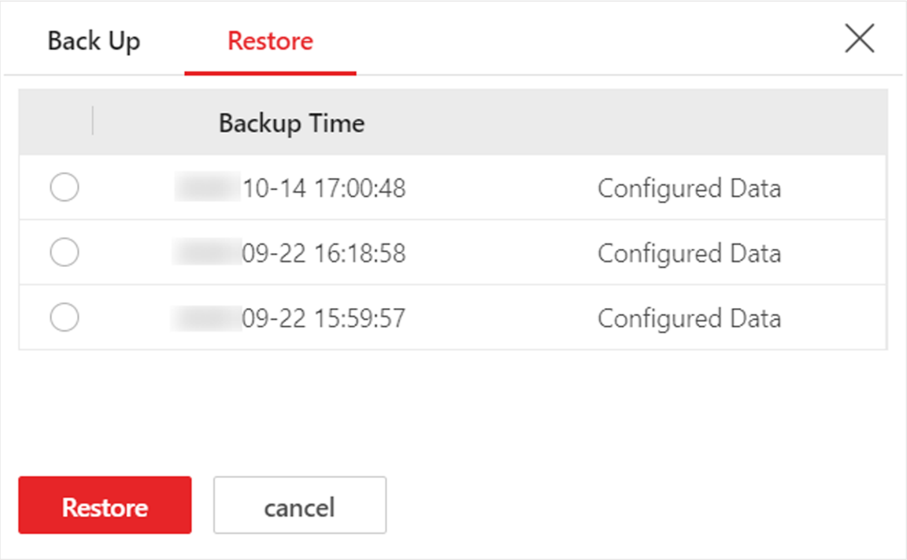
Make sure you have backed up system data. Refer to ***Set System Data Backup*** for details.

Steps

Note

System data recovery will restore the system to an earlier state, and thus the data added after backup date will be lost.

1. In the top right of the client, click **Maintenance and Management → Back Up and Restore System Data** .
2. Select the **Restore** tab.
3. Select a backup file to be restored.



	Backup Time	
○	[redacted]10-14 17:00:48	Configured Data
○	[redacted]09-22 16:18:58	Configured Data
○	[redacted]09-22 15:59:57	Configured Data

Figure 22-22 Restore System Data

4. Click **Restore** to confirm the system data recovery.

What to do next

After restoring the system data, you must reboot the SYS service via Service Manager and log in to Web Client again.

22.10 Export Configuration File

You can export and save configuration data to local disk, including remote site configurations, recording settings and resource configurations.

Steps

1. In the top right of the client, click **Maintenance and Management → Export Configuration Data** .
2. Select the configuration data types that you want to export.
3. Click **Export** to download the data to your local disk.

Note

The configuration data file is in CSV format.

Chapter 23 System Configuration

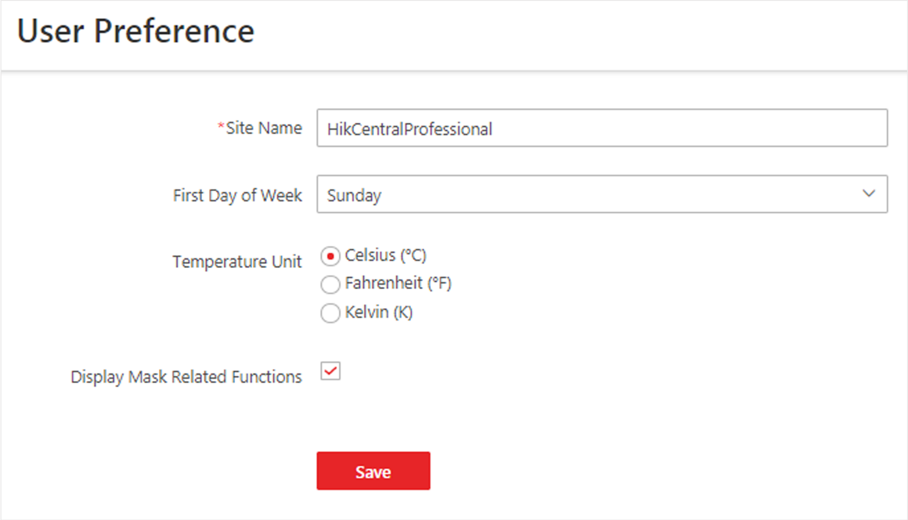
The System page allows you to set basic parameters for the system, such as defining a customized name for your site, setting the WAN IP address for allowing to access your system via WAN (Wide Area Network), and configuring NTP (Network Time Protocol) settings to synchronizing the time between the system and the NTP server.

- For the system with Remote Site Management module, you can enable it to receive the registration from Remote Site.
- For the system without Remote Site Management module, you can set to register it to the Central System as a Remote Site.

23.1 Set User Preference

For different nations, regions, cultures and enterprise backgrounds, the user preference might be different. You can set the user preference according to the actual scene, including the first day of a week and the temperature unit.

In the top left corner of Home page, select ≡ → **All Modules** → **General** → **System Configuration** → **Normal** → **User Preference** to enter the User Preference page.



User Preference

*Site Name: HikCentralProfessional

First Day of Week: Sunday

Temperature Unit: ● Celsius (°C) ○ Fahrenheit (°F) ○ Kelvin (K)

Display Mask Related Functions: ☑

Figure 23-1 User Preference

Set the following parameters:

Site Name

Set the name of current site.

First Day of Week

Set the first day of a week as Sunday, Monday, Tuesday, etc., according to the custom of the actual scene.

Note

This parameter is used in the intelligent analysis report generation, live view and playback, etc.

Temperature Unit

Set the temperature unit according to the custom of the actual scene.

Note

This parameter is used in the temperature analysis report generation, etc.

Display Mask Related Functions

Set whether to display mask related functions. Check the box to display the functions about masks on Control Client, Web Client and Mobile Client. Otherwise these functions will be hidden.

Note

This parameter is mainly used in temperature screening module.

23.2 Set Printer

You can set printer(s) for the system, which can be used to print the stranded person list in some urgent evacuation scenario, such as fire hazard.

Note

Make sure the printer(s) are installed in the same network with the SYS server.

In the top left corner of Home page, select ≡ → **All Modules** → **General** → **System Configuration** → **Normal** → **Printer Settings** .

Click **Add** to select the printer(s) detected by the HikCentral Professional.

Note

After setting printer(s) for the system, you can link printer when configuring alarm/event whose source type is alarm input. For details, refer to ***Add Event and Alarm*** .

You can also click × in the Operation column to delete the printer.

23.3 Set NTP

You can set the NTP server for synchronizing the time between the SYS and the NTP server.

Steps

Note

For devices added via ONVIF protocol, time synchronization will fail. Please configure the time on the device locally and make sure the device's NTP settings are the same with the platform's.

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **System Configuration** → **Network** → **NTP** .
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 SYS and NTP server.
6. Click **Save**.

23.4 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 HikCentral Professional conveniently.

Perform this task when you need to set active directory.

Steps

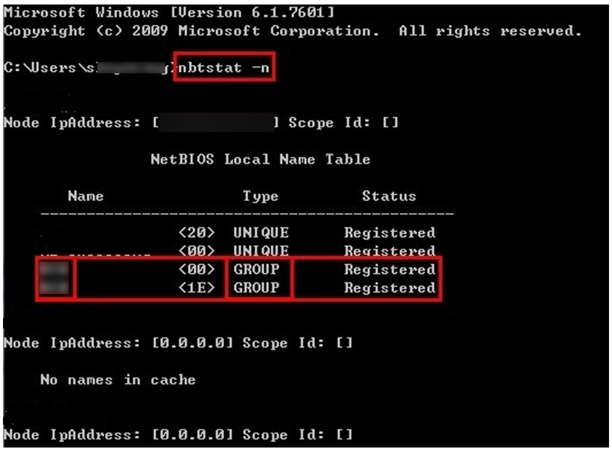
1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **System Configuration** → **Network** → **Active Directory** to enter the Active Directory page.
2. Configure the basic information parameters to connect to the AD domain controller.

   Domain Name

   The domain name of the AD domain controller.

   Note

   - HikCentral Professional 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.

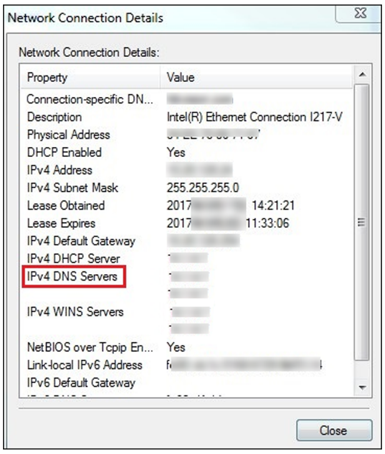


```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\s[redacted]>nbtstat -n

Node IpAddress: [[redacted]] Scope Id: []

                NetBIOS Local Name Table

       Name               Type         Status
    ---------------------------------------------
                   <20>  UNIQUE      Registered
                   <00>  UNIQUE      Registered
    [redacted]     <00>  GROUP       Registered
                   <1E>  GROUP       Registered

Node IpAddress: [0.0.0.0] Scope Id: []

    No names in cache

Node IpAddress: [0.0.0.0] Scope Id: []
```

Figure 23-2 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	f[redacted]
IPv6 Default Gateway	

Figure 23-3 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 default and custom additional information items (see ***Customize 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 ***Customize 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.

23.5 Device Access Protocol

Before adding devices supporting ISUP 2.6/4.0 protocol to the system, you need to set related configuration to allow these devices to access the system.

In the top left corner of Home page, select ≡ → **All Modules** → **General** → **System Configuration** → **Network** → **Device Access Protocol** to enter the Device Access Protocol page.

Enable the **Allow ISUP Registration** function.

Check **Allow ISUP of Earlier Version**.

Click **Save**.

Note

The device may be attacked when accessing the system by ISUP of earlier versions.

23.6 Set WAN Access

In some complicated network environments, you need to set a static IP address or a domain name and ports for HikCentral Professional to enable it to access the SYS via WAN (Wide Area Network). For example, if the SYS is in a local area network, and you need to visit the platform via the Web Client or Control Client running in WAN, you should enable WAN access and set a static IP address or domain name and ports for HikCentral Professional.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **System Configuration** → **Network** → **WAN Access** to enter the WAN Access page.
2. Set the **WAN Access** switch to ON to enable the WAN access function.
3. Enter a static IP address or domain name of the server for WAN access.
4. Set the following ports.

   Client Communication Port

   Used for Web Client and Control Client to access the platform in HTTP protocol. By default, it is 80.

   Client SSL Communication Port

   Used for Web Client and Control Client to access the platform in HTTPS protocol. By default, it is 443.

   Real Time Streaming Port

   Used for getting stream for live view via Control Client. By default, it is 554.

   Video File Streaming Port

   Used for getting stream for playback via Control Client. By default, it is 10000.

   Web Client Streaming Port

   Used for getting stream via Web Client (for web browser of Google Chrome, Firefox, or Safari). By default, it is 559.
5. **Optional:** If you adopts generic event to integrate HikCentral Professional with external sources, you need to set the TCP port and UDP port for receiving the TCP and/or UDP data packages.

   Note

   For setting the generic event, refer to ***Configure Generic Event*** .

6. **Optional:** For the platform with Remote Site Management module, 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. **Optional:** If you need to manage devices accessing via ISUP account, you can set the ports for these ISUP devices, such as registration port, alarm receiving port.

   ISUP Registration Port

   Used for the ISUP devices registering to the platform. By default, it is 7660.

   ISUP Alarm Receiving Port (TCP)

   Used for receiving alarms from ISUP devices in TCP protocol. By default, it is 7332.

   ISUP Alarm Receiving Port (UCP)

   Used for receiving alarms from ISUP devices in UCP protocol. By default, it is 7334.

   ISUP Streaming Port (via VAG)

   Used for getting stream from ISUP devices via VAG server. By default, it is 7661.

   ISUP Streaming Port (via Plugin)

   Used for getting stream from ISUP devices via Plugin. By default, it is 16000.

   Note

   If the ISUP ports are disabled on the SYS, the ISUP related ports will not be displayed in the WAN Access page.

8. Click **Save**.

23.7 Set IP Address for Receiving Device Information

You can select the NIC of the current SYS so that the platform can receive the alarm information of the device connected via ISUP account, and to perform live view and playback for the devices connected via ISUP account.

Before You Start

Make sure the server's ports ranging from 8087 to 8097 are available.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **System Configuration** → **Network** → **Address for Receiving Device Info** .
2. Select **Get from NIC** or **Enter Manually**.

   Get from NIC

   Usually, you can select **Get from NIC** to get IP address from the NIC of SYS.

Select the currently used NIC name of SYS in the drop-down list. The NIC information including description, MAC address, and IP address will display.

Enter Manually

If you have configured hot spare for the SYS. Manually enter the IP address for receiving device information.

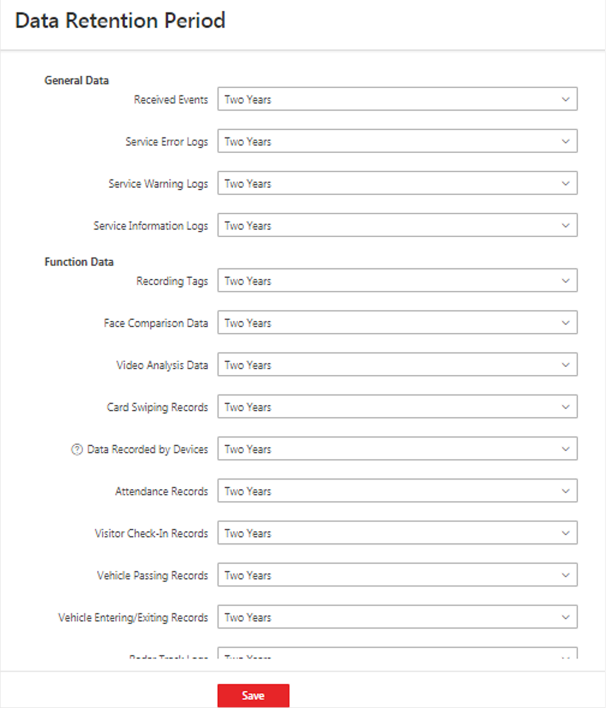
3. Click **Save**.

23.8 Set Data Retention Period

The data retention period specifies how long you can keep the events, logs, and some records SYS server, such as recording tags, face comparison data, vehicle entering/exiting records, etc.

Steps

1. On the top left corner of Home page, select ≡ → **All Modules** → **General** → **System Configuration** → **Storage** → **Data Retention Period** .
2. Set the data retention period from the drop-down list for the required data types.



Data Retention Period

General Data

Received Events: Two Years

Service Error Logs: Two Years

Service Warning Logs: Two Years

Service Information Logs: Two Years

Function Data

Recording Tags: Two Years

Face Comparison Data: Two Years

Video Analysis Data: Two Years

Card Swiping Records: Two Years

Data Recorded by Devices: Two Years

Attendance Records: Two Years

Visitor Check-In Records: Two Years

Vehicle Passing Records: Two Years

Vehicle Entering/Exiting Records: Two Years

Radar Track Logs: Two Years

Figure 23-4 Set Data Retention Period

Note

- The person access records are the access records on the card readers of doors by credentials.
- The data recorded by devices includes the data recorded by the access control devices, video intercom devices, and alarm inputs of these devices, and other records except access records on the doors.
- The person access records and data recorded by devices are saved as the configured period. The user with the permission can search the persons' access records and the data recorded by devices, even if the searched persons have been deleted from the SYS server.

3. Click **Save**.

23.9 Set Holiday

You can add the holiday to define the special days that can adopt different shifts schedule or access schedule. You can set regular holiday and irregular holiday according to the actual scene.

Add Regular Holiday

Regular holiday is suitable for the holiday that has fixed date. For example, the Christmas is in December 25th of each year.
In the top left corner of Home page, select ≡ → **All Modules** → **General** → **System Configuration** → **Normal** → **Holiday Settings** → **Add** to open the adding holiday dialog. Select the Holiday Type as **Regular Holiday**.
Set the parameters as the following instructions:

Start Date

The start date of the holiday.

Number of Days

The lasting days of the holiday.

Repeat Annually

If selected, the system will generate date of holiday according to the date of the VSM server.

Add Irregular Holiday

Irregular holiday is suitable for the holiday that is calculated by the weekdays, and specified date might be different in different year. For example, the Mother's Day is in the second Sunday of each May.
In the top of top left corner of Home page, select ≡ → **All Modules** → **General** → **System Configuration** → **Normal** → **Holiday Settings** → **Add** to open the adding holiday dialog. Select the Holiday Type as **Irregular Holiday**..
Set the parameters as the following instructions:

Start Date

The start date of the holiday.

For example, select **May**, **Second** and **Sunday** for Mother's Day.

Number of Days

The lasting days of the holiday.

Repeat Annually

If selected, the system will generate date of holiday according to the date of the SYS server.

Note

If you select **Repeat Annually**, the specified date of this holiday will be generated automatically according to the current year of the SYS server.
For example, the Mother's Day in 2019 and 2020 is on 12th, May, 2019 and on 10th, May, 2020. The the system will automatically set these two days as holidays for Mother's Day if you have selected **Repeat Annually**.

23.10 Set Email Template

Before sending report or sending event message to the designate email account(s) as email linkage, you should set the email template properly. The email templates include template for sending report and template for sending event message as linkage action when the event is triggered. The email template specifies the recipient, email subject, and content.

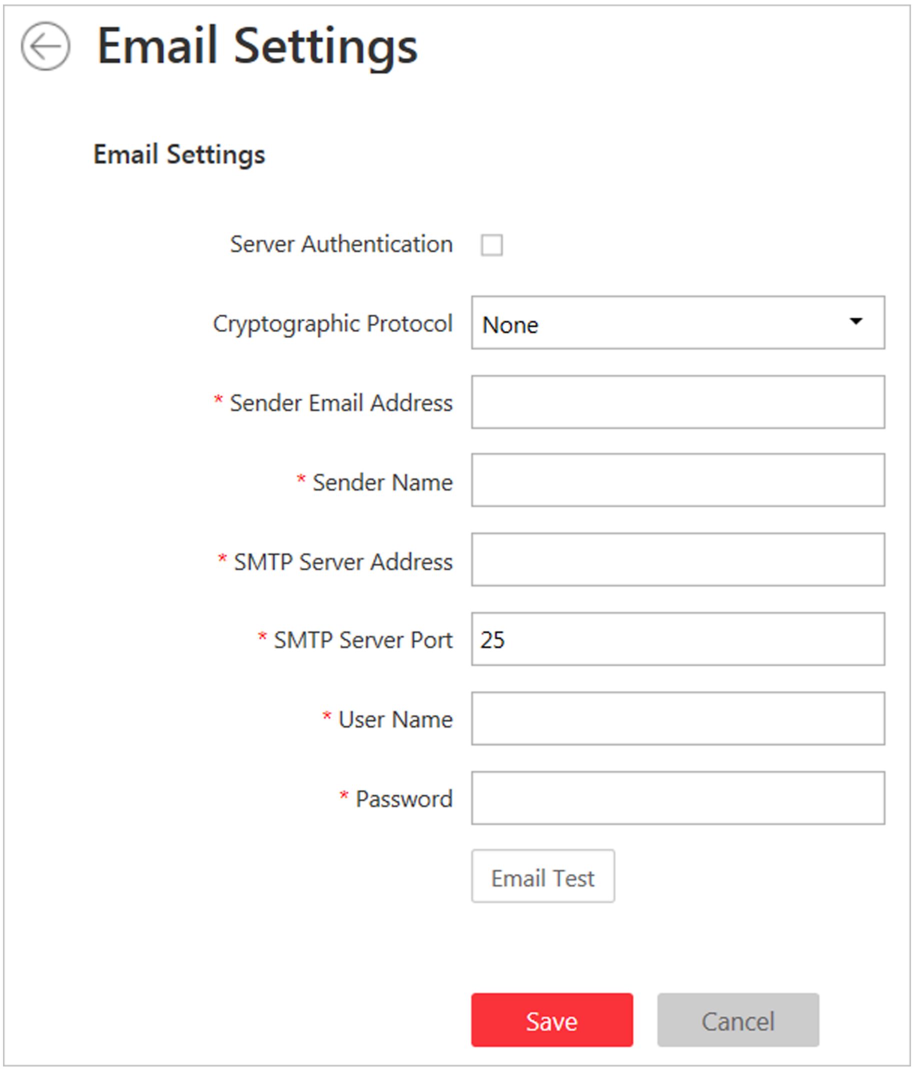
23.10.1 Configure Email Account

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. In the top of top left corner of Home page, select ≡ → **All Modules** → **General** → **System Configuration** → **Email** → **Email Settings** .



Email Settings

Email Settings

Server Authentication □

Cryptographic Protocol: None

* Sender Email Address

* Sender Name

* SMTP Server Address

* SMTP Server Port: 25

* User Name

* Password

Figure 23-5 Email Settings

2. 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.

3. Click **Email Test**to test whether the email settings work or not.

The corresponding attention message box will pop up.

4. Click **Save**.

23.10.2 Add Email Template for Sending Report Regularly

You can set email templates (including specifying the recipient, email subject, and content) for sending report regularly, so that the platform can send report as email attachment to the designate recipient regularly according to the predefined 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.

Steps

1. In the top of top left corner of Home page, select ≡ → **All Modules** → **General** → **System Configuration** → **Email** → **Email for Receiving Reports** .
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 report content to be sent. You can also click buttons below the **Content** parameter to add the related information to the content.

   Note

   If you add the time period to the email subject or email content, and the email application (such as Outlook) and the platform are in different time zones, the displayed time period 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.

23.10.3 Add Email Template for Event and Alarm Linkage

You can set email templates (including specifying the recipient, email subject, and content) for event and alarm linkage. When the event or alarm is triggered, the platform can send email as the linkage action to the designate recipient regularly according to the predefined 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.

Steps

1. In the top of top left corner of Home page, select ≡ → **All Modules** → **General** → **System Configuration** → **Email** → **Email for Event/Alarm Linkage** .
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 or alarm information to be sent. You can also click buttons below the **Content** parameter to add the related information to the content.

Note

If you add the event time to the email subject or content, and the email application (such as Outlook) and the platform are in different time zones, the displayed event 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.

23.11 Set Transfer Protocol

You can set the SYS server's transfer protocol to define the access mode for the SYS (via Web Client, Control Client, or Mobile Client) as HTTP or HTTPS. The HTTPS protocol provides higher data security.

Steps

Note

Setting transfer protocol is only available when accessing the Web Client on the SYS server locally.

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **System Configuration** → **Security** → **Transfer Protocol** .
2. In the **Clients and SYS Transfer** field, select **HTTP** or **HTTPS** as the transfer protocol between the clients (Web Client, Control Client, and Mobile Client) and the SYS servers.
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 SYS server will reboot automatically after changing the clients and SYS server transmission settings.
   - All the users logged in will be forced logout during reboot. The reboot takes about one minute and after that, the users can login again.

23.12 Export Service Component Certificate

For data security, before adding the Streaming Server or Cloud Storage Server to the system, you should generate the service component certificate stored in the SYS server and input the certificate information to the Streaming Server you want to add, or export the service component certificate stored in the SYS and import the certificate to the Cloud Storage Server, so that the certificates of the Streaming Server, Cloud Storage Server and SYS server are the same.

Steps

Note

Exporting SYS server's service component certificate is only available when you access the Web Client on the SYS server locally.

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **System Configuration** → **Security** → **Service Component** .
2. Click **Generate** beside **Certificate between Services in System** to generate the security certificate for Streaming Server verification.

   Note

   On the Service Manager of the Streaming Server you want to add, input the certificate information you generate. For the following operations, see ***Add Streaming Server*** for details.
3. Click **Export** beside **Certificate between System and Recording Server** to export the service component certificate in XML format and save it in the local PC.

   Note

   On the Cloud Storage Server you want to add, import the service component certificate you export. For more details, see ***Manage Cloud Storage Server*** .

23.13 Set Database Password

You can set the database password of the system on the Web Client running on the SYS server.

Note

Setting database password is only available when you access the Web Client on the SYS server locally.

In the top left corner of Home page, select ≡ → **All Modules** → **General** → **System Configuration** → **Security** → **Database Password** .

Enter the password and then click **Verify** to generate the verification code and enter the verification code.

23.14 Configure System Hot Spare

A hot spare is used as a failover mechanism to provide reliability for your system. If you build the hot spare system when installing the SYS service, you can enable the hot spare function and configure the hot spare property of the current SYS 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.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **System Configuration** → **Advanced** → **Hot Spare** .
2. Set the **Hot Spare Configuration** switch to ON to enable the hot spare function.

   The current SYS 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**.

23.15 Set Third-Party Integration

HikCentral Professional supports integrating third-party resources (such as camera, door, etc.) via Optimus.

In the top left corner of Home page, select ≡ → **All Modules** → **General** → **System Configuration** → **Third-Party Integration** .

Note

- Setting open platform is only available when you access the Web Client on the SYS server locally.
- Only admin/administrator users have the permission to perform this function.

Turn **Integrate via Optimus** to ON.

Configure related parameters in the Optimus software. For details, refer to the *User Manual of Optimus*.

The default icons of resources integrated from the third-party will be displayed. Click **Edit** to change the resource icons according to your need.

23.16 Data Interchange

The card swiping data recorded in HikCentral Professional can be used by the third-party system for pay calculation or other applications. You can apply the card swiping records or dump the records as CSV files for data synchronization with the third-party system.

23.16.1 Synchronize Card Swiping Records to Third-Party Database

You can enable synchronization function to apply the card swiping records of specified resources from HikCentral Professional to the third-party database automatically.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **System Configuration** → **Third-Party Integration** → **Data Interchange** .
2. Set **Data Interchange** switch to on to enable data interchange function.
3. Click **Add** and select the resource(s) for card swiping records synchronization.

Note

You can click 🗑 on Operation column to delete the resource or click **Delete All** to delete all added resources.

4. Select **Database Synchronization**.
5. Set the required parameters of the third-party database, including database type, server IP address, server port, database name, user name and password.
6. Click **Test Connection** to test whether database can be connected.
7. Set table parameters of database table and table fields according to the actual configurations.
   1) Enter the table name of the third-party database.
   2) Set the mapped table fields between the HikCentral Professional and the third-party database.
8. Click **Save**.

   The data will be written to the third-party database.

23.16.2 Dump Access Records to Third-Party Database

The access records of specified resources can be dumped as a CSV file or TXT file and the third-party system will read the dumped file (instead of accessing database and mapping the table fields) for further applications, such as attendance calculation and pay calculation.

Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **System Configuration** → **Third-Party Integration** → **Data Interchange** .
2. Set **Data Interchange** switch to on to enable data interchange function.
3. Click **Add** and select the resource(s) for card swiping records synchronization.

Note

You can click 🗑 on Operation column to delete the resource or click **Delete All** to delete all added resources.

4. Select **Access Record Dump**.
5. Set the required parameters.

File Name

The name of CSV file or TXT file which the access records are dumped as.

Storage Location

Local Storage

The access records can be dumped as a file and saved in local disk of SYS server. Then you need to copy this file from the server to your PC with the third-party system installed to read the dumped file.

Note

- You need to log into the Web Client running on SYS server to configure related settings of local storage.
- You need to set **Saving Path**, which is the path where the CSV file or TXT file is saved.

SFTP Storage

You can access SFTP server as the storage location for saving dumped file by setting SFTP address, port, user name, and password. And you can enter the path to save the dumped file in the folder on SFTP server or leave it empty to save that in root directory.

Note

The third-party system should be installed in the SFTP server to read the dumped file.

Content

The display items and data in the dumped file.

Min. Length of Person ID

For some scenarios, the person IDs need to be dumped as certain fixed length.

You can set the switch to on and set the value of **Length**. If the length of person ID is short than the value, zero(s) will be added before the ID to make it equal to the value. If the length is longer than the value, the person IDs will be dumped according to the actual length.

File Format

Two formats are supported, including CSV and TXT.

Dump Frequency

The frequency for dumping card swiping records.

Dump Time

The time when dumping card swiping records is started.

6. Click **Save**.

23.17 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.

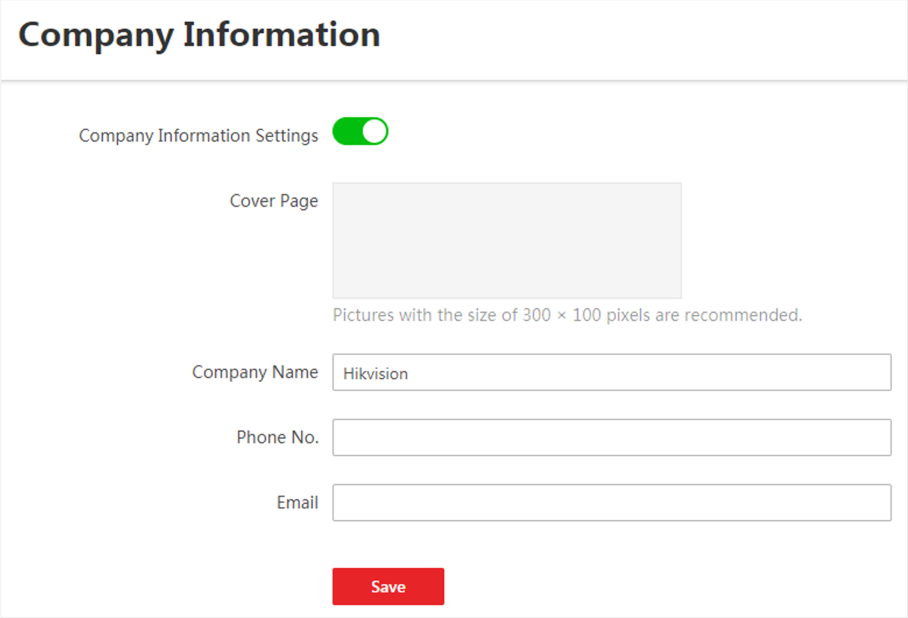
Steps

1. In the top left corner of Home page, select ≡ → **All Modules** → **General** → **System Configuration** → **Advanced** → **Reset Network Information** .
2. Click **Reset** to one-touch reset the device network information.

23.18 Set Company Information

You can configure and show the company information on the Web Client for customization requirements.

In the top left corner of Home page, select ≡ → **All Modules** → **General** → **System Configuration** → → **Company Information** to enter the Company Information Settings page.



Company Information

Company Information Settings: ●

Cover Page

Pictures with the size of 300 × 100 pixels are recommended.

Company Name: Hikvision

Phone No.:

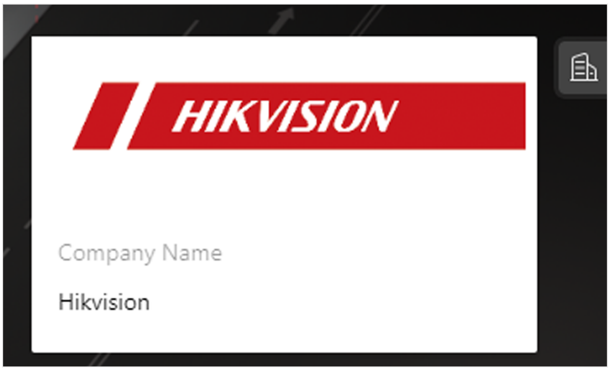
Email:

Save

Figure 23-6 Company Information Settings

Switch on **Company Information Settings** to enable displaying company information on the Web Client. And then set the information (cover page, company name, etc.) as needed and click **Save**.

An icon 🏢 appears at right of the Web Client and keeps displaying. You can click the icon to view the company information.



Company Name

Hikvision

Figure 23-7 Company Information Displayed on Web Client

Chapter 24 Important Ports

HikCentral Professional 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.

Destination	Port No.	Description
System Management Service (SYS) Port		
NGINX	80 (HTTP/WebSocket)	Used for web browser access in HTTP protocol.
NGINX	443 (HTTPS/ WebSocket over TLS)	Used for web browser access in HTTPS protocol.
SYS	14200 (HTTP/HTTPS)	Used for Remote Site registration to central system.
SYS	15300 (TCP and UDP)	Used for receiving generic event.
SYS	7332 (TCP)	Used for receiving alarms from ISUP device.
SYS	7334 (UDP)	Used for receiving alarms from ISUP device.
SYS	7660 (TCP)	Used for receiving registration from ISUP device.
SYS	7661 (TCP)	Used for getting stream from ISUP device via Streaming Server
Streaming Gateway	554 (RTSP)	Used for getting stream (real time streaming port).
Streaming Gateway	559 (WebSocket)	Used for getting stream for Google Chrome or Firefox (WebSocket port).
Streaming Gateway	10000 (TCP)	Used for getting stream for playback (video file streaming port).
Streaming Gateway	16000 (TCP)	Used for getting stream from ISUP device via plugin.
Streaming Gateway	6001 (SNMP)	Used for getting the status of Streaming Gateway.
Streaming Gateway	6678 (HTTPS)	Used for setting the certificate.
NTP Service	123 (UDP)	Used for time synchronization.
Streaming Service Port		
Streaming Service	554 (RTSP)	Used for Streaming Service to get stream (real time streaming port).

Destination	Port No.	Description	
Streaming Service	559 (WebSocket)	Used for getting stream for Google Chrome or Firefox (WebSocket port).	
Streaming Service	10000 (TCP)	Used for Streaming Service to get stream for playback (video file streaming port).	
Streaming Service	6001 (TCP)	Used for getting the status of Streaming Service.	
Streaming Service	16000 (TCP)	Used for getting stream from ISUP device via plugin.	
Streaming Service	8208 (WebSocket over TLS)	Used for security certificate authentication.	
Streaming Service	6678 (HTTPS)	Used for setting the certificate.	
pStor Cluster Service Port			
pStor Cluster Service	9012 (HHTP)	Used for accessing the pStor Cluster Service via Web Browser.	
pStor Cluster Service	6300 (HTTP)	Used for signaling gateway.	

See Far, Go Further

UD22917B