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 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 INSPECTION, 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, time and attendance, face comparison, and so on.

Note

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

The complete system contains the following modules. You can install the modules according to actual needs.

Module	Introduction
System Management Service (SYS)	• Provides the unified authentication service for connecting with the clients and servers. • Provides the centralized management for the users, roles, permissions, devices, and services. • Provides the configuration interface for surveillance and management module.
Application Data Service (ADS)	Provides data storage and processing.
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.

1.3 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 Configuration, Applications, Wizard, Maintenance, License, 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.

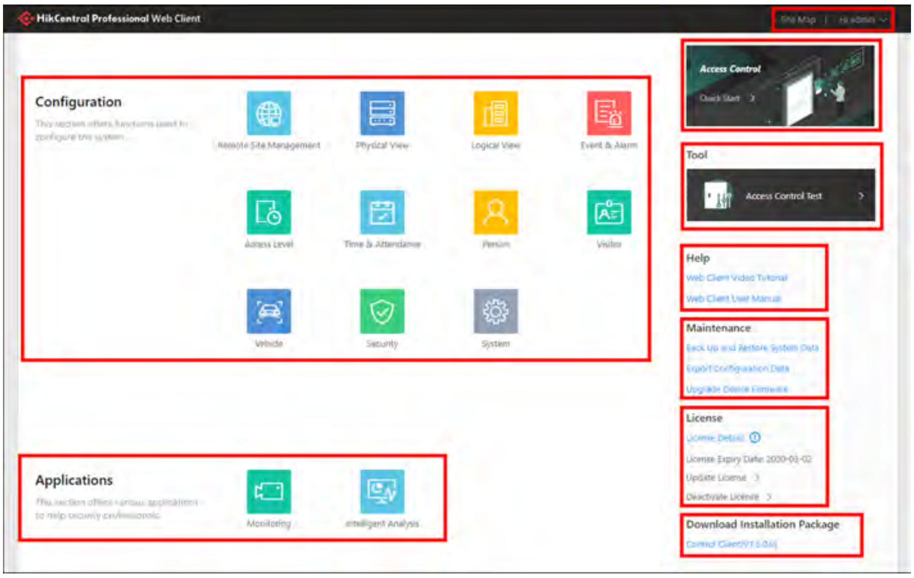


Figure 1-1 Modules on Home Page

Table 1-1 Modules on Home Page

Section	Module	Description
Configuration	Remote Site Management	The Remote Site Management (often short as RSM) module provides federation functions by adding other HikCentral Professional without RSM module to the HikCentral Professional with RSM module as the Remote Site for central management. For more details, refer to ***Manage Remote Site*** .
	Physical View	The Physical View module provides device management to manage all kinds of devices or servers in the system, such as encoding devices, access control devices, security control devices, etc. For more details, refer to ***Manage Resource*** .
	Logical View	The Logical View module provides areas to manage the added resources in different groups. You can group the resources into different areas according to the resources' locations. For more details, refer to ***Manage Area*** .
	Event & Alarm	The Event & Alarm module provides events and alarm settings as well as linkage actions settings. For more details, refer to ***Configure Event and Alarm*** .
	Access Level	The Access Level module provides defining access permissions that which persons can get access to which doors and floors during the authorized time period. For more details, refer to ***Manage Access Level*** .
	Time and Attendance	The Time and Attendance module provides tracking and monitoring when the persons start/stop work and monitor their working hours and late arrivals, early departures, time taken on breaks, and absenteeism, For more details, refer to ***Manage Time and Attendance*** .
	Person	The Person module provides adding person information to the system for further operations such as access control, face comparison, time and attendance, etc. For more details, refer to ***Manage Person List*** .
	Visitor	The Visitor module provides an entire process for visitors tour from registration to check-out. For more details, refer to ***Manage Visitor*** .

Section	Module	Description
	Vehicle	The Vehicle module provides managing vehicles in the system so that the ANPR cameras can recognize the license plate number of the detected vehicles and compare with the license plate of the vehicles in the system. It also provides entrance and exit management including managing parking lot, entrances and exits, lanes, and setting entry & exit rules so that the system can allow the vehicles to enter or exit the parking lot automatically. For more details, refer to ***Manage Entrance and Exit*** .
	Security	The Security module provides roles and users management and system security settings. For more details, refer to ***Manage Role and User*** and ***Manage System Security*** .
	System	The System module provides setting basic parameters for the system For more details, refer to ***System Configuration*** .
Applications	Monitoring	The Monitoring module provides live view, playback, and local configuration through web browser. For more details, refer to ***Monitoring*** .
	Intelligent Analysis	The Intelligent Analysis module provides BI report functions and you can use report as basis in creating decisions, addressing problems, checking tendency and comparison, etc. For more details, refer to ***Intelligent Analysis Report*** .
Access Control Quick Start		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 and elevator control in ***Flow Chart*** .
Tool	Access Control Test	A tool through which you can test whether the configurations (such as persons' credentials and access levels) are set correctly and completely and whether the devices are running properly. For more details, refer to ***Access Control Test*** .
Help	Web Client Video Tutorial	View the videos which introduce the configurations on the Web Client.

Section	Module	Description
	Web Client User Manual	Open the user manual of the Web Client for help. You can enter some keywords to search in the manual.
Maintenance	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 Database*** .
	Export Configuration Data	You can export and save configuration data to your local PC. For more details, refer to ***Export Configuration File*** .
	Upgrade Device Firmware	You can upgrade the firmware of the devices added to the system via the current Web Client or EZVIZ Cloud service. For more details, refer to ***Upgrade Device Firmware*** .
License		You can view the License details, activate, upgrade, and deactivate the License if needed. For more details, refer to ***Manage License*** .
Download Installation Package		Download the installation package of other clients, such as Control Client.
Others	Site Map	The navigation bar of the Web Client. You can access all the modules via the Site Map.
	Change Password	Change the password of the current user. For more details, refer to ***Change Password of Current User*** .
	About	Check the version information of the Web Client. View the License Agreement and Open-Source License Agreement.
	Logout	Log out of the system and back to the login page.

1.4 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 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 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 10/11 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 → Site Name** . See ***Set Site Name*** 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 **Login** and the **Change Password** window opens.
4. Set a new password and confirm the password.

   Note

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

   Caution

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

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

Result

Web Client home page displays after you successfully logging in.

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 **Login** to log in to the system.

   Note

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

Result

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

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

   Note

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

   Caution

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

5. Click **OK**.

Result

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

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 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.

5.1 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

Note

If you activate the system by the License with server distributed deployment function, you cannot switch the system to server central deployment.

1. Log in to HikCentral Professional via the Web Client. Refer to ***Login via Web Client*** .
2. Click **Online Activation** in the License area to open the License configuration window.

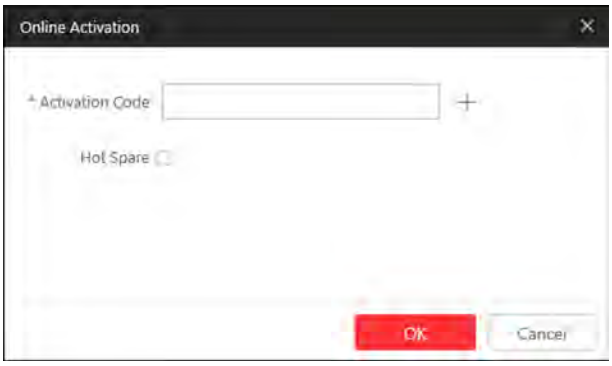


Figure 5-1 Online Activation

3. Enter the activation code received when you purchased your License.

Note

- If you have purchased more than one Licenses, you can click + and enter other activation codes.
- Up to 110 Licenses are allowed in one system.
- The activation code should contain 16 characters or 32 characters (except dashes).

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

Note

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

5. Click **OK** and the License Agreement dialog opens.
6. Read the License Agreement.
   - If you accept the terms of the License Agreement, check **I accept the terms of the agreement** and click **OK** to continue.
   - If you do not accept the agreement, click **Cancel** to cancel the activation.

   The activation will start.

5.2 Activate License - Offline

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

Steps

Note

If you activate the system by the License with server distributed deployment function, you cannot switch the system to server central deployment.

1. Log in to HikCentral Professional via the Web Client.
2. Click **Export the license request file** in the License area.

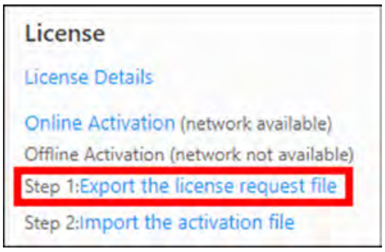

License
License Details
Online Activation (network available)
Offline Activation (network not available)
Step 1:Export the license request file
Step 2:Import the activation file

Figure 5-2 Export Request File

3. Enter the activation code received when you purchased your License.

Note

- If you have purchased more than one License, you can click + and enter other activation codes.
- Up to 110 Licenses are allowed in one system.
- The activation code should contain 16 characters or 32 characters (except dashes).

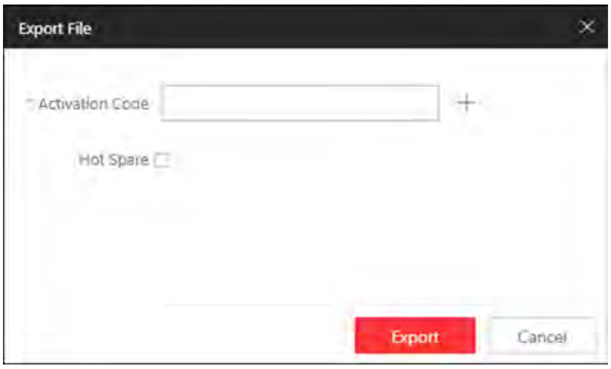


Figure 5-3 Export File

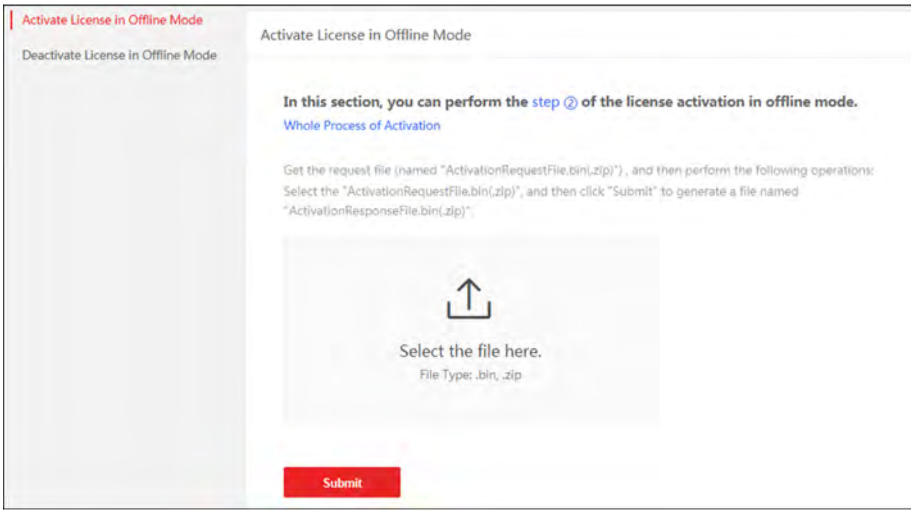
4. **Optional:** Check **Hot Spare** and enter the required parameters if you want to build a hot spare system.

Note

- The switch will be displayed if you select **Hot Spare** mode when installing the system.
- For how to build the hot spare system, please contact Hikvision's technical support engineers.

5. Click **Export**.
6. In the pop-up License Agreement window, check **I accept the terms of the agreement** and click **OK**.

   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 PC that can connect to the Internet.
8. On the PC which can connect to the Internet, enter the following website: ***https://license.hikvision.com:8443/#/active*** .
9. Click ⭱ and then select the request file downloaded in Step 6.


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 5-4 Select Request File

10. 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).

11. Copy the respond file to the proper directory of the PC that accesses HikCentral Professional via the Web Client.

12. In the License area, click **Import the activation file**.

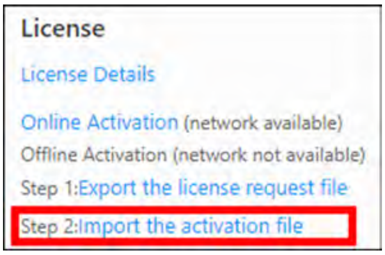

License
License Details
Online Activation (network available)
Offline Activation (network not available)
Step 1:Export the license request file
Step 2:Import the activation file

Figure 5-5 Import Respond File

13. Click ⋯ and select the respond file downloaded in Step 10.

14. Click **Import**.

5.3 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. Click **Update License** at the License area to open the update panel.
3. Enter the activation code received when you purchase your License.

Note

- If you have purchased more than one Licenses, you can click + and enter other activation codes.
- Up to 110 Licenses are allowed in one system.
- The activation code should contain 16 characters or 32 characters (except dashes).

4. Click **Update** and the License Agreement dialog opens.
5. Read the License Agreement.
   - If you accept the terms of the license agreement, check **I accept the terms of the agreement** and click **OK** to continue.
   - If you do not accept the agreement, click **Cancel** to cancel the update.

   The activation will start.

5.4 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. Click **Update License** in the License area and click **Export the license request file**.

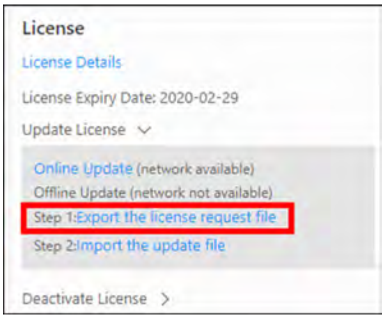

License
License Details
License Expiry Date: 2020-02-29
Update License
Online Update (network available)
Offline Update (network not available)
Step 1:Export the license request file
Step 2:Import the update file
Deactivate License

Figure 5-6 Export Request File

3. 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.
- Up to 110 Licenses are allowed in one system.
- The activation code should contain 16 characters or 32 characters (except dashes).

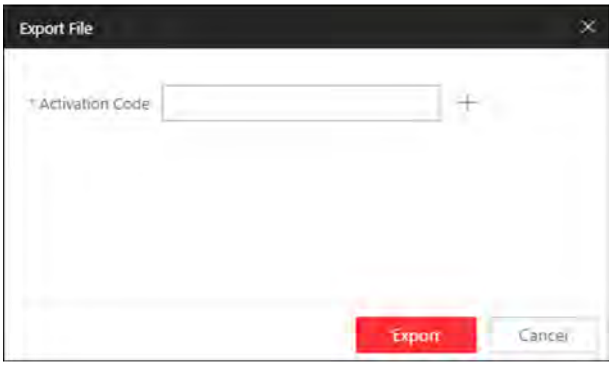
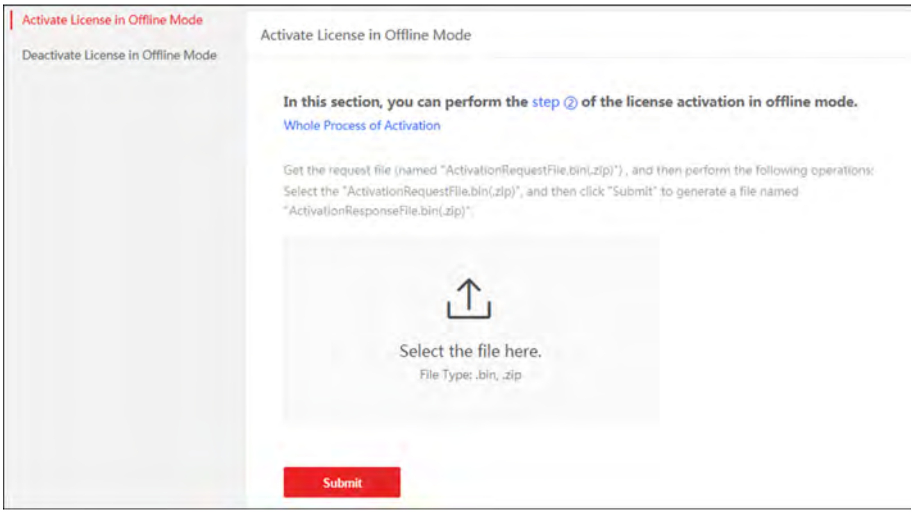


Figure 5-7 Export File

4. Click **Export**.
5. In the pop-up License Agreement window, check **I accept the terms of the agreement** and click **OK**.

   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).
6. Copy the request file to the PC that can connect to the Internet.
7. On the PC which can connect to the Internet, enter the following website: ***https://license.hikvision.com:8443/#/active*** .
8. Click ⭱ and then select the request file downloaded in Step 5.



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)".

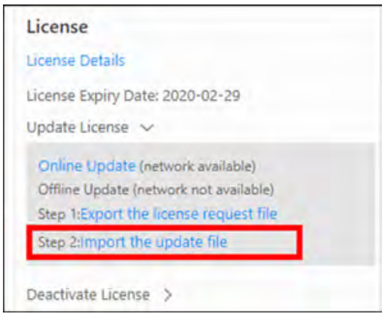
Select the file here.
File Type: .bin, .zip
Submit

Figure 5-8 Select Request File

9. 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).

10. Copy the respond file to the proper directory of the PC that accesses HikCentral Professional via the Web Client.
11. In the License area, click **Update License → Import the update file** .



License

License Details

License Expiry Date: 2020-02-29

Update License

Online Update (network available)

Offline Update (network not available)

Step 1:Export the license request file

Step 2:Import the update file

Deactivate License

Figure 5-9 Import Respond File

12. Click ··· and select the respond file downloaded in Step 9.
13. Click **Import**.

5.5 Deactivate License - Online

If you want to run the SYS on another PC 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. Click **Deactivate License** in the License area to open the deactivation panel.
3. Click **Online Deactivation** and check the activation code(s) to be deactivated.
4. Click **OK** to deactivate the license.

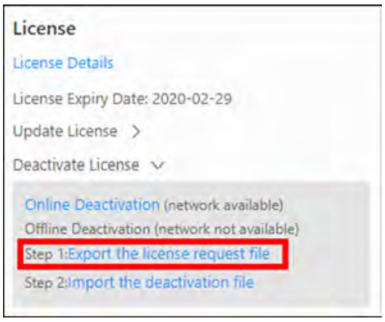
   The deactivation will start.

5.6 Deactivate License - Offline

If you want to run the SYS on another PC 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. Click **Deactivate License** in the License area and click **Export the license request file**.



License

License Details

License Expiry Date: 2020-02-29

Update License >

Deactivate License ∨

Online Deactivation (network available)

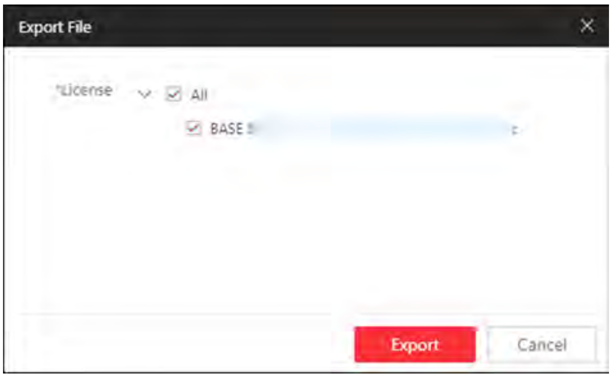
Offline Deactivation (network not available)

Step 1:Export the license request file

Step 2:Import the deactivation file

Figure 5-10 Export Request File

3. Select the activation code(s) to be deactivated.



Export File ×

*License ∨ ☑ All

☑ BASE

Figure 5-11 Select Activation Code

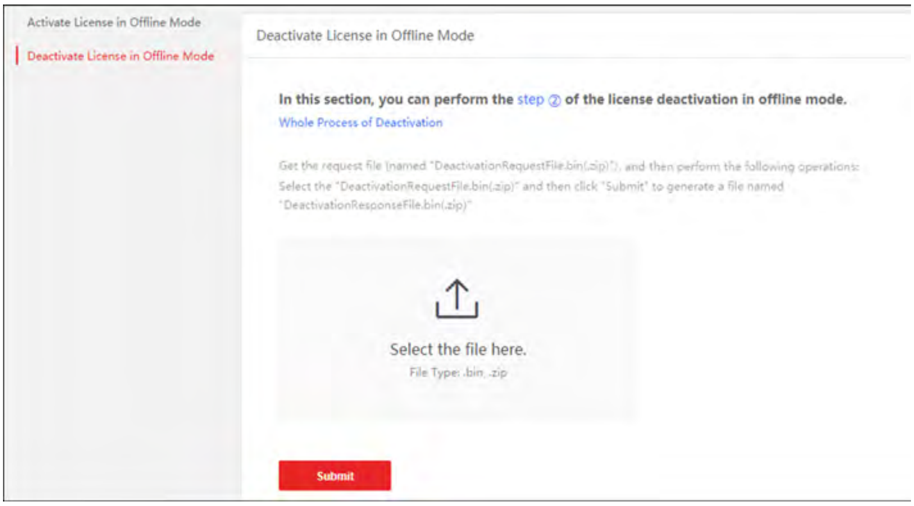
4. Click **Export**.

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

   Note

   After exporting the request file, the selected activation codes will be unavailable.

5. Copy the request file to the PC that can connect to the Internet.
6. On the PC which can connect to the Internet, enter the following website: ***https://license.hikvision.com:8443/#/deactive*** .
7. Click ⇧ and then select the request file downloaded in Step 4.


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

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

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)"

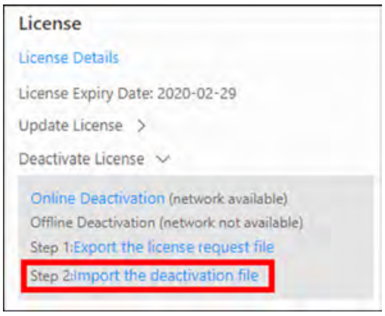
Figure 5-12 Select Request File

8. 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).

9. Copy the respond file to the proper directory of the PC that accesses HikCentral Professional via the Web Client.

10. In the License area, click **Deactivate License → Import the update file** .


License
License Details
Update License >
Deactivate License ∨
Online Deactivation (network available)
Offline Deactivation (network not available)
Step 1:Export the license request file
Step 2:Import the deactivation file

License Expiry Date: 2020-02-29

Figure 5-13 Import Respond File

11. Click ··· and select the respond file downloaded in Step 8.

12. Click **Import**.

Chapter 6 Manage Resource

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

6.1 Create Password for Inactive Device(s)

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

Before You Start

- Make sure the devices (cameras, DVR, etc.) you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the 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. Click **Physical View → Encoding Device** to enter the Encoding Device Management page.

   Note

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

The detected online devices list in the online device area.

2. View the device status (shown on Security column) and select one or multiple inactive devices.
3. Click ♡ to open the Device Activation window.
4. Create a password in the password field, and confirm the password.

⚠ **Caution**

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

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

6.2 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, change the device IP address due to the changes of the network.

Before You Start

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

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

Steps

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

Note

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

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

   Server Network

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

   Note

   The parameters may vary for different device types.
5. Click ✓ .
6. Enter device's password.
7. Click **Save**.

6.3 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,

6.3.1 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

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

   Server Network

   As the default selection, the detected online devices in the same local subnet with the 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.
3. 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.
4. In the Online Device area, select the active device to be added.
5. Click **Add to Device List** to open the Add Online 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. 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.

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 Channel 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 channels to area, select a Streaming Server to get the video stream of the channels via the server.

   Note

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

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. Click **Add**.
13. **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/thermal camera (report supported), turn to Home page, click **License Details → Configuration → Add** , 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 add multiple devices to HikCentral Professional at a time. The devices added by this method will be set as the same channel information, which you can edit later if required.

Before You Start

- Make sure the devices (cameras, DVR, etc.) you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the 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. Click **Physical View → Encoding Device** to enter the Encoding Device Management page.
2. In the Online Device area, select a network type.

   Server Network

   As the default selection, the detected online devices in the same local subnet with the 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.
3. 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.
4. In the Online Device area, check the active devices to be added.
5. Click **Add to Device List** to open the Add Online Device dialog.
6. **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.
7. **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.
8. 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.

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 Channel 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.

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

Note

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

12. Click **Add**.
13. **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/thermal camera (report supported), turn to Home page, click **License Details → Configuration → Add** , 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.

6.3.2 Add Encoding Device by IP Address or Domain Name

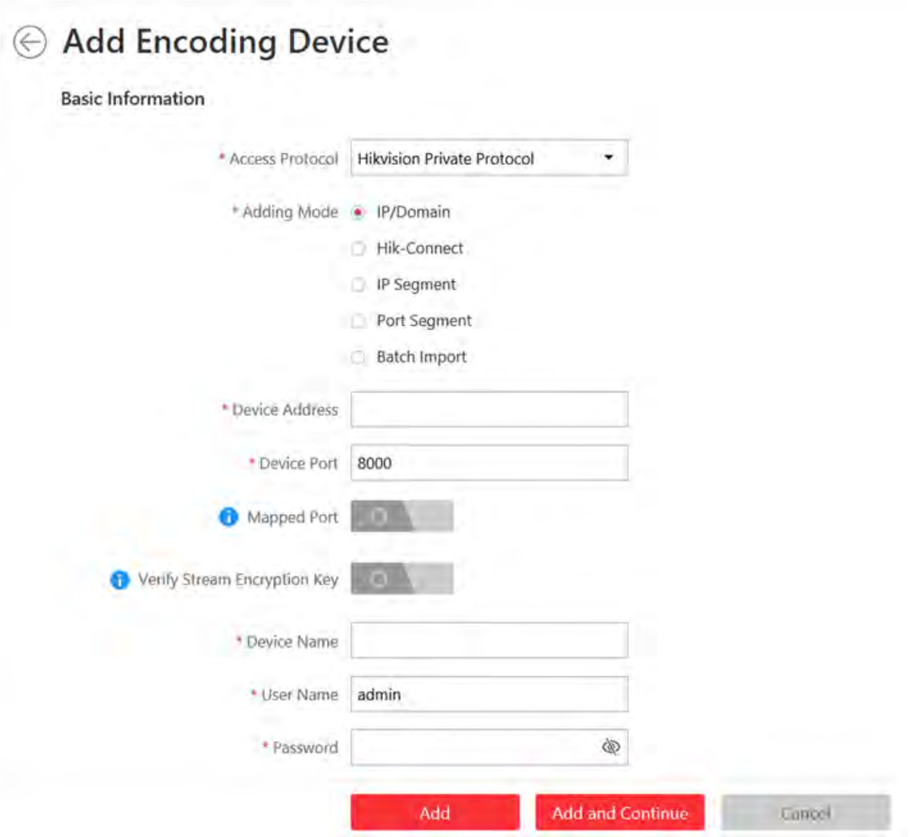
When you know the IP address or domain name of a device, you can add it to the system by specifying the IP address (or domain name), user name, password, etc.

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



Add Encoding Device

Basic Information

* Access Protocol: Hikvision Private Protocol

* Adding Mode: ● IP/Domain ○ Hik-Connect ○ IP Segment ○ Port Segment ○ Batch Import

* Device Address:

* Device Port: 8000

Mapped Port

Verify Stream Encryption Key

* Device Name:

* User Name: admin

* Password:

Figure 6-1 Add Encoding Device Page

3. 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.

4. Select **IP/Domain** as the adding mode.
5. 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.

6. **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.

7. **Optional:** Switch **Add Channel 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.

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

Note

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

9. **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.

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 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.
12. **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/thermal camera (report supported), turn to Home page, click **License Details → Configuration → Add** , 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.

6.3.3 Add Encoding Devices by IP Segment

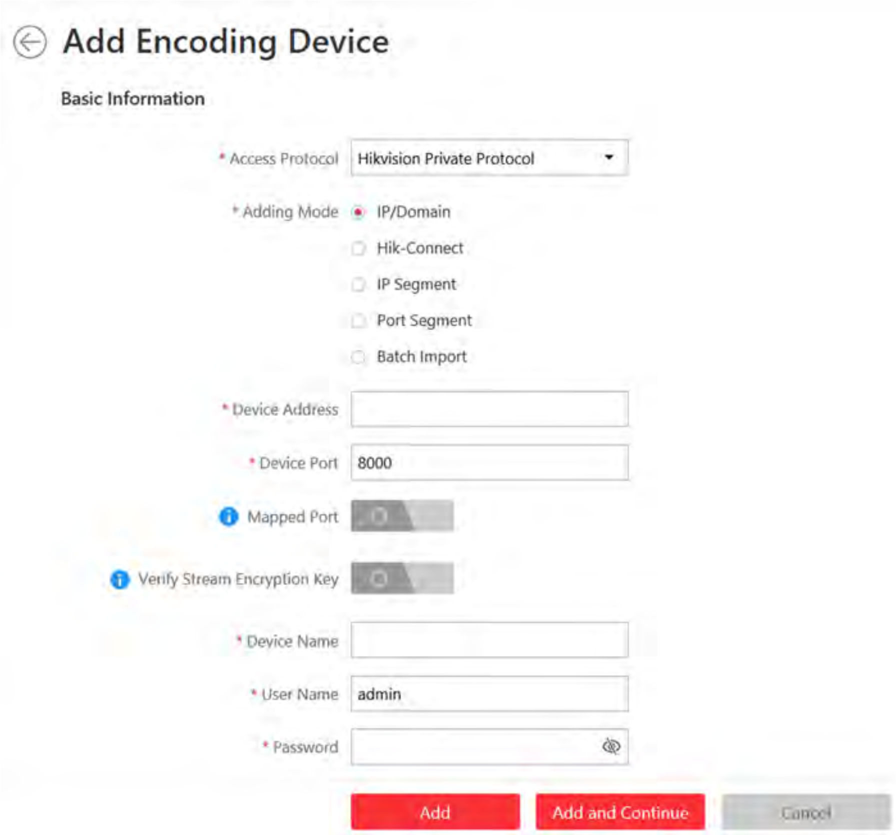
When multiple encoding devices to be added have the same port number, user name and password, but have different IP addresses within a range, you can select this adding mode, and specify the IP range where your devices are located, and other related parameters. The system will scan from the start IP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

Before You Start

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

Steps

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



Add Encoding Device

Basic Information

* Access Protocol: Hikvision Private Protocol

* Adding Mode: ● IP/Domain ○ Hik-Connect ○ IP Segment ○ Port Segment ○ Batch Import

* Device Address:

* Device Port: 8000

Mapped Port

Verify Stream Encryption Key

* Device Name:

* User Name: admin

* Password:

Figure 6-2 Add Encoding Device Page

3. 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.

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 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.

6. **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.

7. **Optional:** Switch **Add Channel 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.

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

Note

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

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

What to do next

For facial recognition camera/ANPR camera/thermal camera (report supported), turn to Home page, click **License Details → Configuration → Add** , 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.

6.3.4 Add Encoding Devices by Port Segment

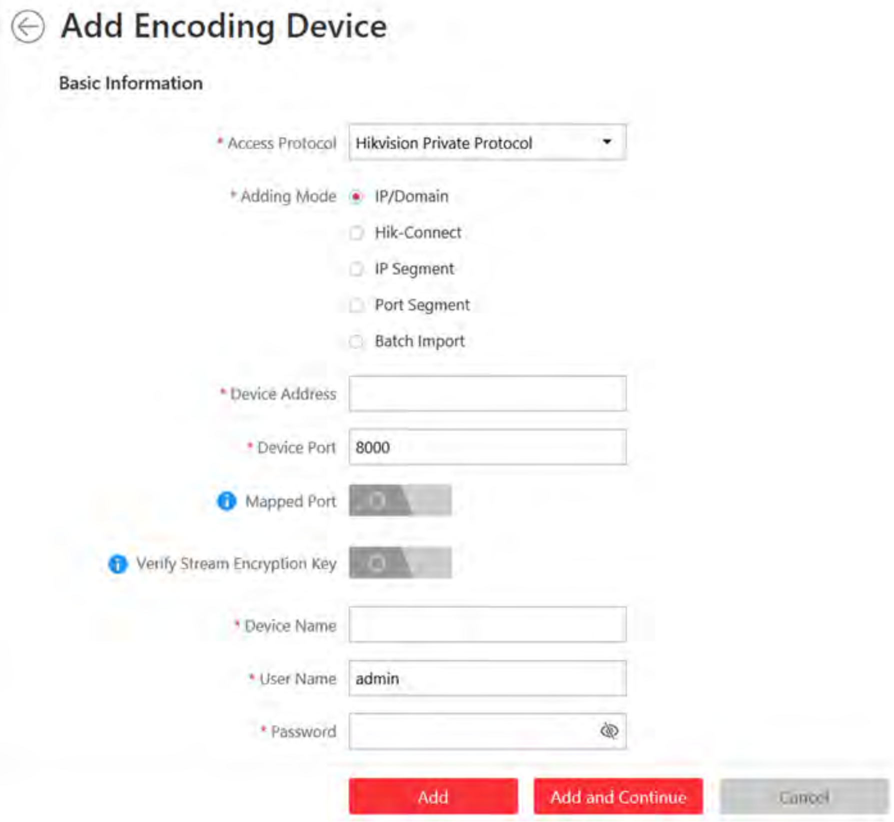
When multiple encoding devices to add have the same IP address, user name and password, but have different port numbers within a range, you can select this adding mode and specify the port range, IP address, user name, password, and other related parameters to add them.

Before You Start

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

Steps

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



Add Encoding Device

Basic Information

* Access Protocol: Hikvision Private Protocol
* Adding Mode: ● IP/Domain ○ Hik-Connect ○ IP Segment ○ Port Segment ○ Batch Import
* Device Address:
* Device Port: 8000

Mapped Port

Verify Stream Encryption Key

* Device Name:
* User Name: admin
* Password:

Figure 6-3 Add Encoding Device Page

3. 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.

4. Select **Port Segment** as the adding mode.
5. 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.

6. **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.

7. **Optional:** Switch **Add Channel 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.

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

Note

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

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

What to do next
For facial recognition camera/ANPR camera/thermal camera (report supported), turn to Home page, click **License Details → Configuration → Add** , 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.

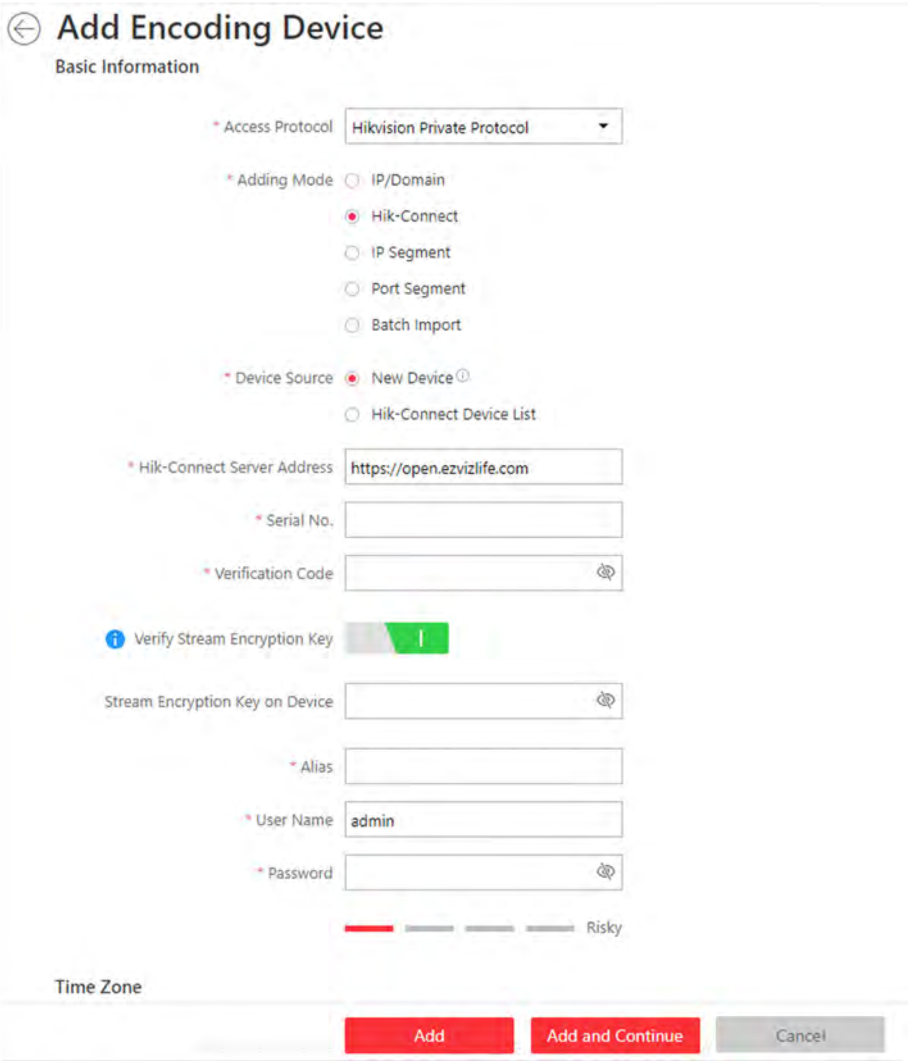
6.3.5 Add Encoding Device by Hik-Connect

With this adding mode, you can add encoding devices even if the devices do not have fixed IP addresses.

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 device by Hik-Connect.

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



Add Encoding Device

Basic Information

* Access Protocol: Hikvision Private Protocol

* Adding Mode: ○ IP/Domain ● Hik-Connect ○ IP Segment ○ Port Segment ○ Batch Import

* Device Source: ● New Device ○ Hik-Connect Device List

* Hik-Connect Server Address: https://open.ezvizlife.com

* Serial No.:

* Verification Code:

Verify Stream Encryption Key: on

Stream Encryption Key on Device:

* Alias:

* User Name: admin

* Password:

Risky

Time Zone

Figure 6-4 Add Encoding Device Page

3. Select **Hikvision Private Protocol** as the Access Protocol.
4. Select **Hik-Connect** as the adding mode.
5. **Optional:** 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.
6. 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.

7. 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.

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. Switch **Add Channel 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.

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.

    Note

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

11. **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.
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 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/thermal camera (report supported), turn to Home page, click **License Details → Configuration → Add** , 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.

6.3.6 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. Click **Physical View → Encoding Device** to enter the Encoding Device Management page.
2. Click **Add** to enter the Add Encoding Device page.
3. Select **Hikvision ISUP Protocol** as the Access Protocol.
4. Select **Device ID** as the adding mode.
5. 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.

6. **Optional:** Set **Picture Storage** switch to on to enable picture storage for the encoding device.
7. **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.
- You can not configure the storage location for the captured undercarriage pictures, which are stored on the UVSS 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:** Switch **Add Channel 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.
- 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 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.

    Note

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

11. **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.
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.

6.3.7 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. Click **Physical View → Encoding Device** to enter the Encoding Device Management page.
2. Click **Add** to enter the Add Encoding Device page.
3. Select **Hikvision ISUP Protocol** as the Access Protocol.
4. Select **Device ID Segment** as the adding mode.
5. 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.

6. **Optional:** Set **Picture Storage** switch to on to enable picture storage for the encoding device.
7. **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.
- You can not configure the storage location for the captured undercarriage pictures, which are stored on the UVSS 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:** Switch **Add Channel 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.
- 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 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.

Note

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

11. **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.
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.

6.3.8 Add Encoding Devices in a Batch

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

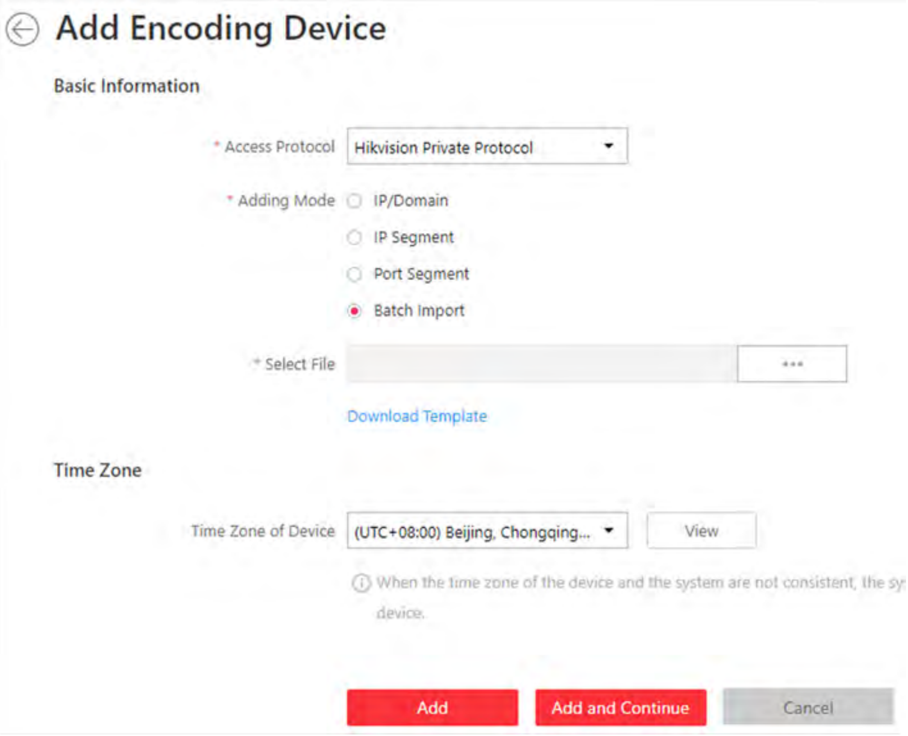
Before You Start

Make sure the devices (cameras, DVR, etc.) you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the 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. Click **Physical View → Encoding Device** to enter the Encoding Device Management page.
2. Click **Add** to enter the Add Encoding Device page.



Add Encoding Device

Basic Information

* Access Protocol: Hikvision Private Protocol

* Adding Mode: ○ IP/Domain ○ IP Segment ○ Port Segment ● Batch Import

* Select File

Time Zone

Time Zone of Device: (UTC+08:00) Beijing, Chongqing...

When the time zone of the device and the system are not consistent, the sy
device.

Figure 6-5 Add Encoding Device Page

3. 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.

4. Select **Batch Import** as the adding mode.
5. Click **Download Template** and save the predefined template (excel file) on your PC.
6. Open the exported template file and enter the required information of the devices to be added on the corresponding column.
7. Click ··· and select the edited file.
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. 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.
10. **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/thermal camera (report supported), turn to Home page, click **License Details → Configuration → Add** , 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.

6.3.9 Limit Bandwidth for Video Downloading

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

Note

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

Click **Physical View → Encoding Device** to enter the Encoding Device page and then 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).

6.3.10 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.), 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.

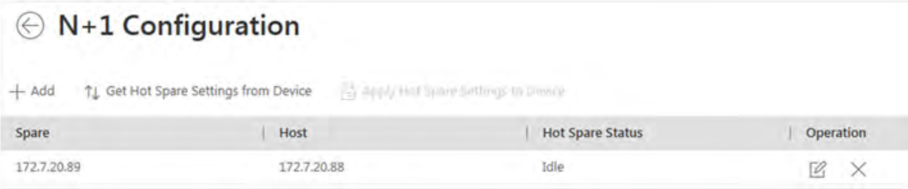
If the N+1 hot spare settings have already been configured on the NVR, click **Physical View → Encoding Device → N+1 Hot Spare → Get Hot Spare Settings from Device** to upload the hot spare settings from the device to HikCentral Professional. If the N+1 hot spare settings haven't been configured on the 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. Click **Physical View → Encoding Device → N+1 Hot Spare** to enter the N+1 Configuration page.


N+1 Configuration
+ Add
Get Hot Spare Settings from Device
Apply Hot Spare Settings to Device

Spare	Host	Hot Spare Status	Operation
172.7.20.89	172.7.20.88	Idle	✎ ×

Figure 6-6 N+1 Configuration Page

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

Note

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

6. Click **Apply Hot Spare Settings to Device** to apply the Hot Spare settings to the devices to take effect.
7. **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.

6.4 Upgrade Device Firmware

You can upgrade the firmwares of the devices added to the system via the current Web Client or EZVIZ Cloud service.

Via Current Web Client

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

Table 6-1 Device List

No.	Device Type
1	Camera
2	NVR (Network Video Recorder)
3	DVR (Digital Video Recorder)

No.	Device Type
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 EZIVZ Cloud Service

The following devices are supported to be upgraded the firmwares via EZIVZ Cloud service:

Table 6-2 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.

6.4.1 Upgrade Device Firmware via Current Web Client

You can upgrade device firmware via the current Web Client.

Steps

1. Click **Upgrade Device Firmware** on the Home page to open the Upgrade Device Firmware window.
2. Click **Via Current Web Client** tab.
3. Set the required information.

   Simultaneous Upgrade

   Set the maximum number of devices for simultaneous upgrade. For example, if you set the value to 5, up to 5 devices can be selected for batch upgrade.
4. Select a upgrade package from the local PC and then click **Next**.

   The upgradable devices will be displayed.
5. **Optional:** Filter devices by device type, device firmware version, or device model.
6. Select device(s) and then click **Next**.
7. 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).

6.4.2 Upgrade Device Firmware via EZVIZ Cloud Service

You can upgrade device firmware via EZVIZ Cloud Service, which is a cloud service provided by EZVIZ.

Steps

1. Click **Upgrade Device Firmware** on the Home page to open the Upgrade Device Firmware window.
2. Click **Via EZVIZ Cloud** tab.
3. Set the required information.

   Simultaneous Upgrade

   Set the maximum number of devices for simultaneous upgrade. For example, if you set the value to 5, up to 5 devices can be selected for batch upgrade.
4. Click **Next**.
5. 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.

6. Select device(s) and click **Next** to enter the upgrade schedule page.
7. 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).

6.5 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*** .

6.5.1 Reset Device Password

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

Before You Start

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

Steps

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

   Note

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

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

A dialog with import file and export file, password and confirm password fields opens.

3. Click **Export** to save the device file on your PC.
4. Send the file to our technical engineers.

Note

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

Caution

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

6.5.2 Restore Device's Default Password

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

Before You Start

- Make sure the devices (cameras, DVR, etc.) you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the 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. Click **Physical View → Encoding Device** to enter the Encoding Device Management page.

   The detected online devices list in the Online Device area.

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

   A dialog with security code pops up.

3. Enter the security code and restore the default password of the selected device.

Note

Contact our technical support to obtain a security code.

What to do next

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

Caution

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

6.6 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. You can also view the Remote Site's GIS location, hot spot, and hot region settings in Map module.

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.

6.6.1 Add Remote Site by IP Address or Domain Name

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

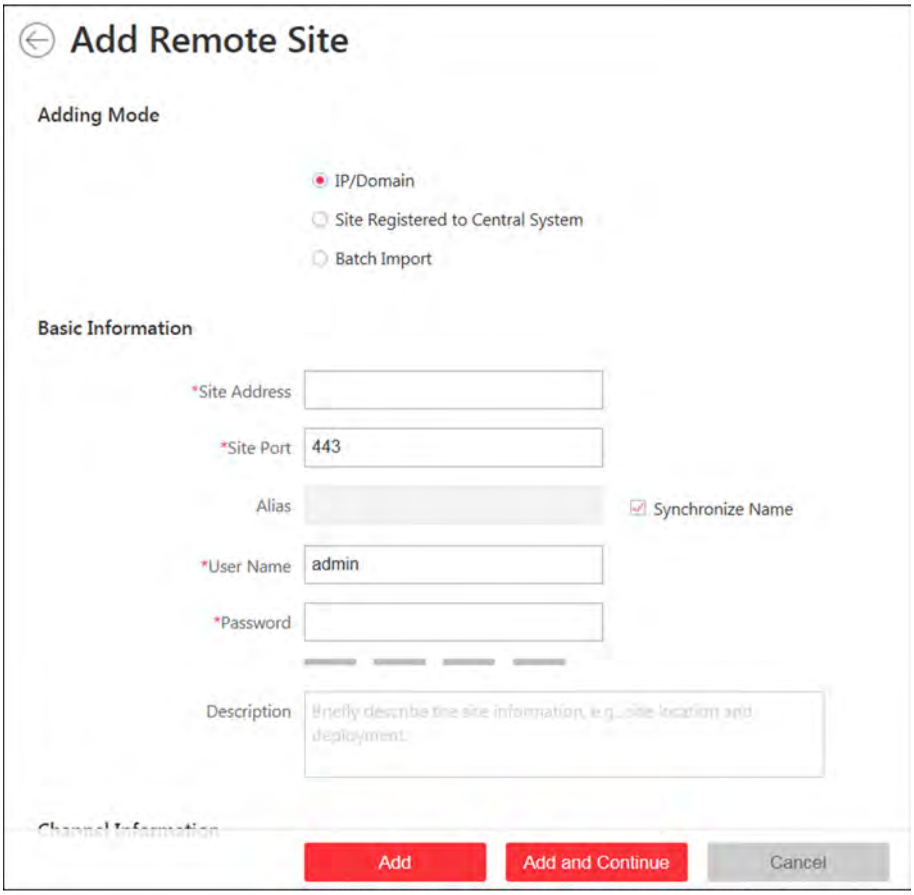
Perform this task when you need to add Remote Site by IP address or domain name.

Steps

Note

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

1. Click **Remote Site Management** on home page to open the Remote Site management page.
2. Enter the Add Remote Site page.
    - If no Remote Site added, click **Add Site** to enter the Add Remote Site page.
    - If you have already added Remote Site, click + on the left to enter the Add Remote Site page.



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

Figure 6-7 Add Remote Site Page

3. Select **IP/Domain** as the adding mode.
4. Enter the required information.

   Site Address

   The IP address or domain name of the Remote Site.

   Site Port

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

   Alias

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

   User Name

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

   Password

   The password required to access the Remote Site.

   Description

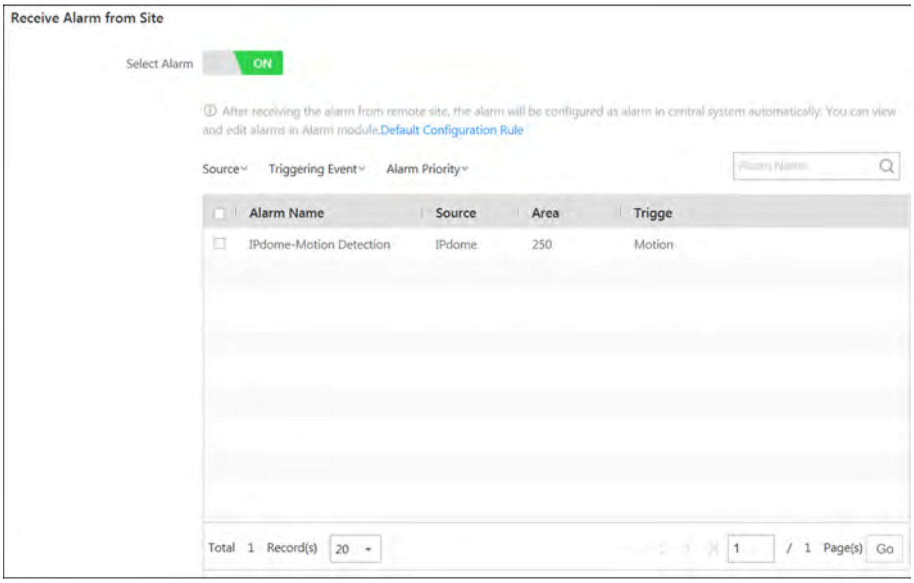
   Optionally, you can enter the descriptive information for the Remote Site, such as location and deployment.

⚠ Caution

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

□	Alarm Name	Source	Area	Trigge
□	IPdome-Motion Detection	IPdome	250	Motion

Total 1 Record(s) 20 1 / 1 Page(s) Go

Figure 6-8 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 Alarm module. For details about setting the alarm, refer to .

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.

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

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

Steps

Note

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

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

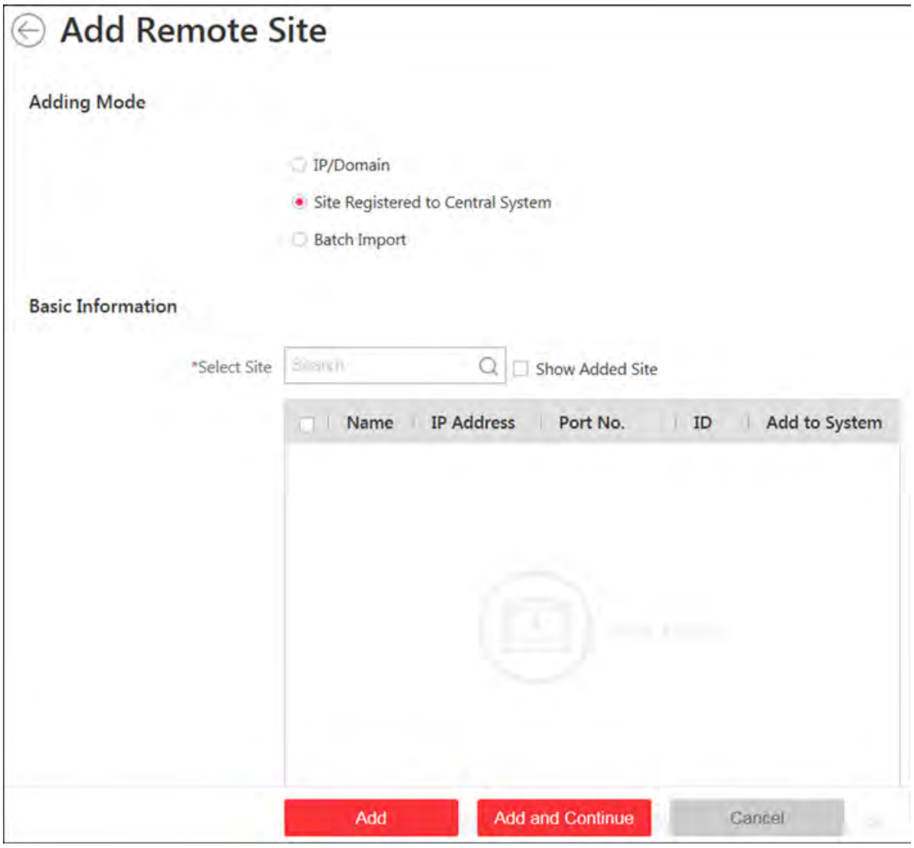


Figure 6-9 Add Remote Site Page

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.

6.6.3 Add Remote Sites in a Batch

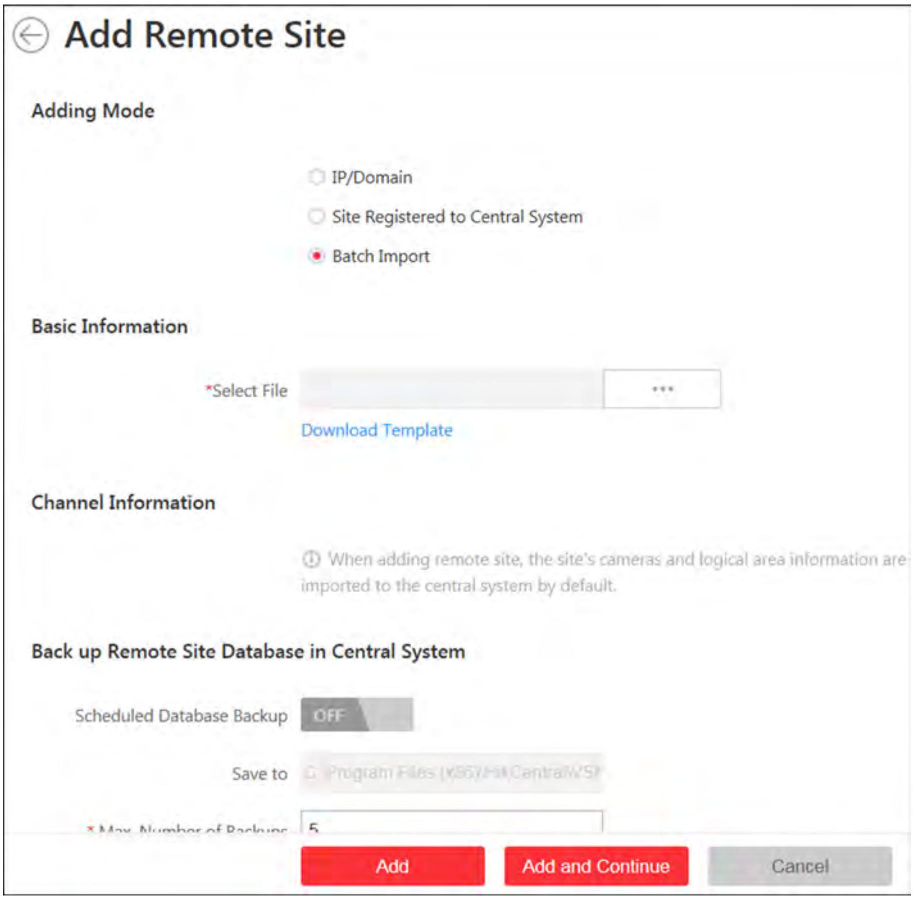
When you want to add multiple Remotes Sites at a time for convenience, you can edit the predefined template by entering the sites' parameters and import the template to the Central System to add them.

Steps

Note

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

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



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\VSP

* Max. Number of Backups 5

Figure 6-10 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.

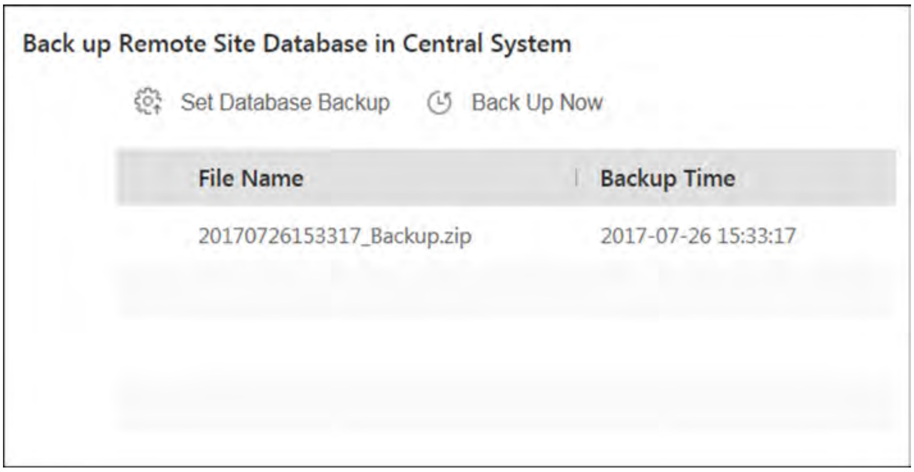
6.6.4 Back Up Remote Site's Database to Central System

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

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

Steps

1. Click **Remote Site Management** on home page to open the Remote Site management page.
2. In the site list on the left, click the Remote Site name to view its details.

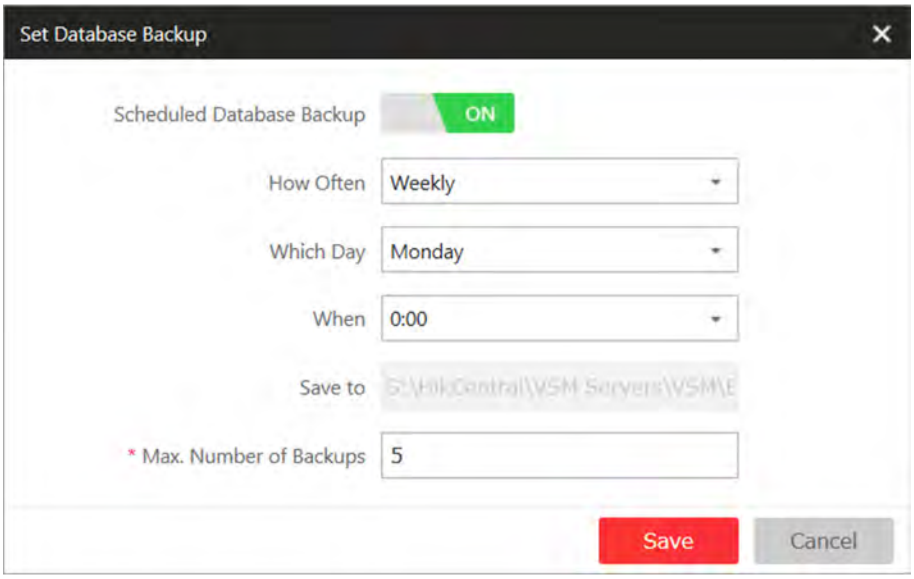


Back up Remote Site Database in Central System

File Name	Backup Time
20170726153317_Backup.zip	2017-07-26 15:33:17

Figure 6-11 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: S:\HikCentral\VSM Servers\VSM\E

* Max. Number of Backups: 5

Figure 6-12 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.

6.6.5 Edit Remote Site

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

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

Steps

1. Click **Remote Site Management** on home page to open the Remote Site management page.
2. In the site list on the left, click the Remote Site name to view its details.

3. View and edit the basic information of the Remote Site, including IP address, port, alias, etc.

Note

You cannot edit the address and port of the site registered to the Central System.

4. In the original information field, view the Remote Site's site name, system ID, system version, and GPS location.

Note

If the GPS location is not configured, click **Configuration** to set its location in Map module. See ***Manage Map*** for details.

5. **Optional:** Click **Configuration on Site** to open the Web Client of the Remote Site and log in for further configuration.

Note

The site must be online if you need to enter its Web Client.

6. Click **Save**.

6.6.6 View Remote Site's Changes

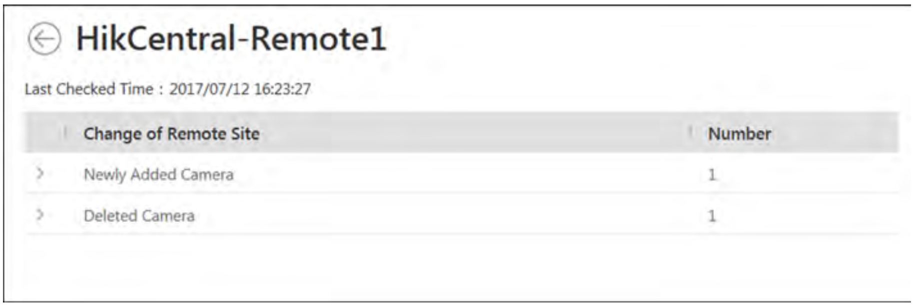
When there are changed resources on the Remote Site, such as newly added cameras, deleted cameras, and name changed cameras, you can view the changed resources and synchronize the resources in Central System with the Remote Site.

Steps

Note

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

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

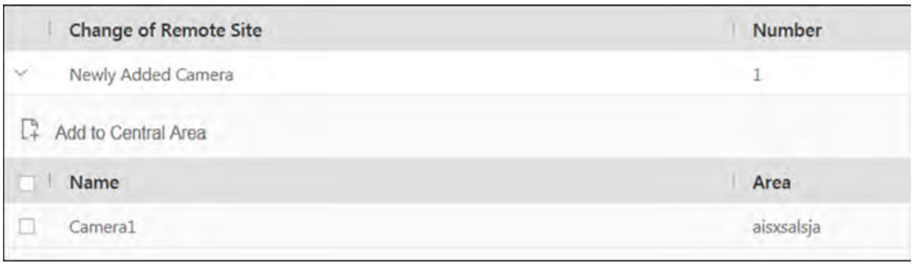
Last Checked Time : 2017/07/12 16:23:27

Change of Remote Site	Number
Newly Added Camera	1
Deleted Camera	1

Figure 6-13 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

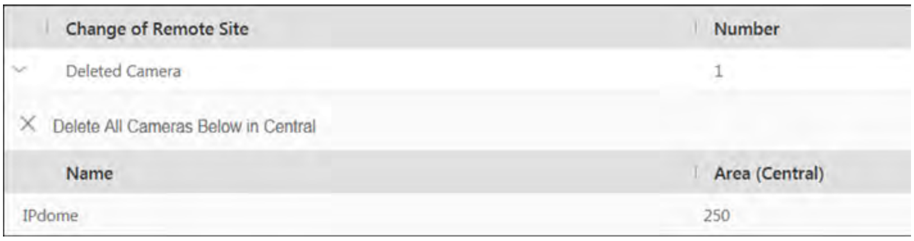
Figure 6-14 Changes of Remote Site

You can view the camera name and area name on the Remote Site.

2) Select the camera(s) and click **Add to Central Area** to synchronize the newly added cameras to the Central System.
3) Select the area in the Central System.
4) Click **Save**.

6. When there are some cameras deleted from the site, you can view the deleted cameras and remove them from Central System.

1) If there are some cameras deleted from Remote Site, click **Deleted Camera** to expand the deleted camera list.



Change of Remote Site	Number
Deleted Camera	1

× Delete All Cameras Below in Central

Name	Area (Central)
IPdome	250

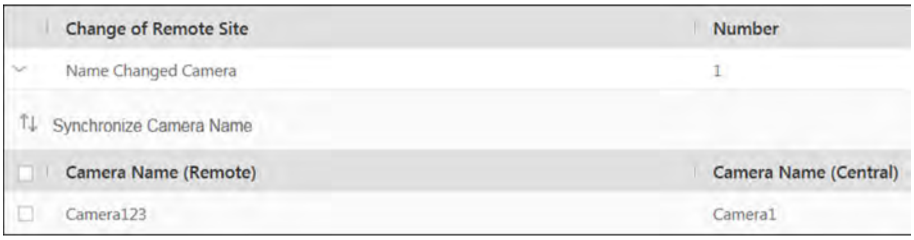
Figure 6-15 Change of Remote Site

You can view the camera name and its area in Central System.

2) Click **Delete All Cameras Below in Central** to delete the deleted cameras in Central System.

7. When there are some cameras whose names are changed on the site, you can view the name changed cameras and synchronize them to Central System.

1) If the name of camera of Remote Site is changed, click **Name Changed Camera** to expand the name changed camera list.



Change of Remote Site	Number
Name Changed Camera	1

⇅ Synchronize Camera Name

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

Figure 6-16 Name Changed Camera

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

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

6.7 Manage Application Data Server

HikCentral Professional provides distributed deployment for the two core services: System Management Service and Application Data Service. Distributed deployment can improve the system performance and the number of connectable cameras can be increased to 10,000.

Enter **Physical View → Application Data Server** to enter the application data server management page.

What is Application Data Server?

Application Data Server is the PC running the Application Data Service, which is mainly used for processing and storing the application data of the system. If the system License supports distributed deployment, you need to deploy an Application Data Server independently and add it to the system before any other operations.

What should I do before adding the Application Data Server to the system?

- Make sure the License of your system supports server distributed deployment.
- Download the installation package of Application Data Service and install it on a computer (except the computer running the System Management Service). After installation, run the Application Data Service and then the computer is an Application Data Server.
- You can add another Application Data Server as standby server for data backup redundancy if needed, which can improve the reliability and availability of the system. When the Application Data Server fails, the Application Data Standby Server will take over automatically.
- The Application Data Server, Application Data Standby Server, and the System Management Server should be in the same LAN which is secure and in the same time zone, or the system cannot run properly.
- Make sure the Application Data Server and Application Data Standby Server are online and running properly.

Encrypted Transmission

For data security, the system provides encrypted transmission for the Application Data Server, which encrypts the data transmitted between the Application Data Server and other services or clients.

Note

Only admin user can edit this function and the admin user can only edit it via the Web Client running on the SYS server.

Click **System → Security → Transfer Protocol** to check **Encrypted Transmission** to encrypt the data transmission between Application Data Server and System Management Server.

Note

- 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.

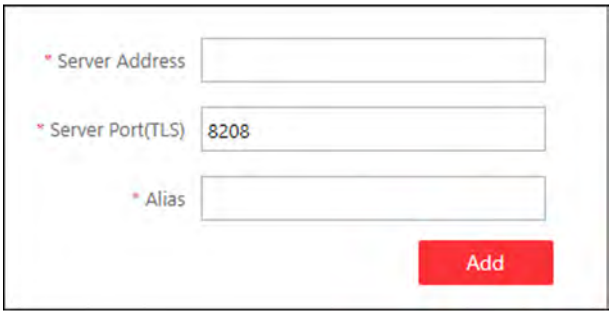
How to add an Application Data Server?

Before adding the Application Data Server, generate the security certificate on the Web Client running on the SYS server (For details, refer to ***Export Service Component Certificate***), and then enter the certificate information on the Service Manager running on the Application Data Server for authentication. Only after the authentication succeed, the Application Data Server can be added to the system.

Note

Only the admin user has the permission to add Application Data Server and Application Data Standby Server.

In the Application Data Server page, click **Add** and enter the server's IP address and port to add the server.



* Server Address	
* Server Port(TLS)	8208
* Alias	

Figure 6-17 Add Application Data Server

After adding the Application Data Server, in Application Data Server page, click **Add Standby Server** to add an Application Data Standby Server if necessary.

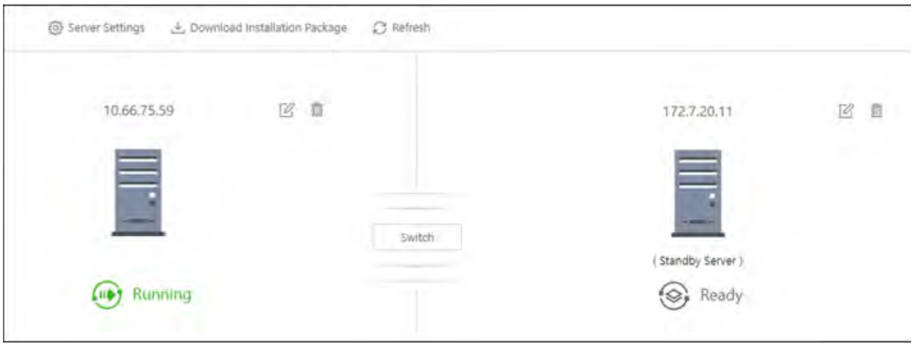


Figure 6-18 Application Data Server Management

Note

Click **Refresh** to get the latest status of the Application Data Server and Application Data Standby Server.

Set Threshold of Failure Status

If the system disconnects with the Application Data Server or Application Data Standby Server and the disconnection lasts for specified time, the system will regard the server as failure and notify the administrator to maintain it.

In Application Data Server page, click **Server Settings** and you can set the threshold in **Change Status to Failure after Disconnection of** field.

For example, if you set the threshold as 10 seconds, and the server disconnects with the system for 10 or more seconds, the server status will turn to failure.

Automatically Switch to Application Data Standby Server

If the Application Data Server fails, the Application Data Standby Server will take over automatically. After that, the original Application Data Standby Server will turn to Application Data Server, and the original Application Data Server will turn to standby server.

Once the Application Data Server and the Application Data Standby Server changes, the status will be refreshed automatically.

You can also click **Refresh** to get the latest status of the Application Data Server and Application Data Standby Server.

Maintain Server Fault

Note

Only the admin user has the permission to perform the maintenance.

After refreshing manually, if the Application Data Server or Application Data Standby Server fails, the server's status will change to failure and system will display the fault details to help you diagnose the reason. After maintenance, if the system detects the server is running properly, click **I've maintained it.** and then the servers will turn to normal status.

Manually Switch to Application Data Standby Server

Note

Only the admin user has the permission to switch to Application Data Standby Server.

If the Application Data Server fails but the system cannot detect its fault, or you need to change the server to a better one, you can manually switch the Application Data Server currently in working status to the Application Data Standby Server which is in ready status.

In Application Data Server page, click **Switch** to switch to the Application Data Standby Server and then the standby server will take over.

Note

During switching, the Application Data Server will be stopped for a while and it will resume after switching.

6.8 Manage Recording Server

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

6.8.1 Add pStor

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

Before You Start

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

Steps

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

   Address

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

   Control Port

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

   Network Port

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

   Signaling Gateway Port

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

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

   Note

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

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

Note

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

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

Caution

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

6.8.2 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. Click **Physical View → Recording Server** to enter the recording server page.

2. Click **Add** to enter the Add Recording Server page.
3. Select **Hybrid Storage Area Network**.
4. Enter the network parameters.

   Address

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

Note

The access key and secret key are used to download pictures via the Control Client. If required, you can contact our technical support to get them.

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

Caution

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

   Custom Video Copy-back

   After enabled, the video footage (if exists) recorded within the defined **Start Time** and **End Time** on cameras or NVRs managed by the Hybrid SAN will be automatically copied back to the Hybrid SAN.

Note

- The time for starting copy-back could be any time when there exists video footage which meets the above mentioned condition.
- The time period within the start time and end time should be longer than 24 hours, and the end time should NOT be later than 2 hours before.

For example, if the current time is "10:00:00, Oct. 31st", and you have enabled custom video copy-back (in which you set "2 days before copy-back" as the start time, "2 hours before copy-back" as the end time), the video footage recorded from "10:00:00, Oct. 29th" to "8:00:00, Oct. 31st" on cameras or NVRs managed by the Hybrid SAN will be backed up to the Hybrid SAN.

Video Expiration

Set the expiration time to retain the video footage stored on the Hybrid SAN.

For example, if you set 30 days as the expiration time, the video footage stored on the Hybrid SAN for longer than 30 days will be automatically deleted.

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 Storage Area Network displays. You can log in and configure the Hybrid SAN.

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

6.8.3 Add Network Video Recorder

You can add NVR (Network Video Recorder) as a Recording Server to HikCentral Professional for storing video files and 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. Click **Physical View → Recording Server** to enter the recording server page.
2. Click **Add** to enter the adding server page.
3. Select **Network Recording Server** as the server type.
4. 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.
5. 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.
6. **Optional:** If you need to access the server via WAN, set the **Enable WAN Access** switch to ON and set the corresponding parameters which are available when you access the server via WAN.
7. Enter the alias, user name, and password of the 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.
8. 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.
9. **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.

6.8.4 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 system, you should import the certificate stored in the SYS server to the Cloud Storage Server first.

Before You Start

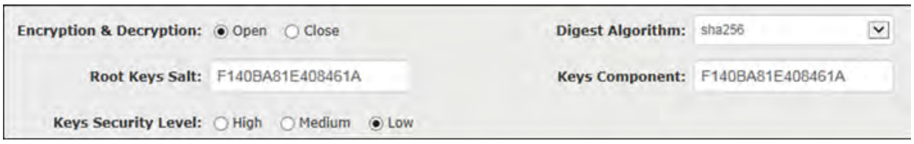
Make sure the Cloud Storage Server you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the HikCentral Professional via network.

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



Encryption & Decryption: ● Open ○ Close

Digest Algorithm: sha256

Root Keys Salt: F140BA81E408461A

Keys Component: F140BA81E408461A

Keys Security Level: ○ High ○ Medium ● Low

6. Click **Set**.

What to do next

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

Add Cloud Storage Server

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

   Address

   The server's IP address in LAN that can communicate with 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.
5. Enter the user's access key and secret key of the Cloud Storage Server for searching the video files stored in this Cloud Storage Server via the 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**).
6. **Optional:** Set the **Enable Picture Storage** switch to ON for storing pictures in this Cloud Storage Server.

   Note

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

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

⚠ **Caution**

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

6.8.5 Add pStor Cluster Service

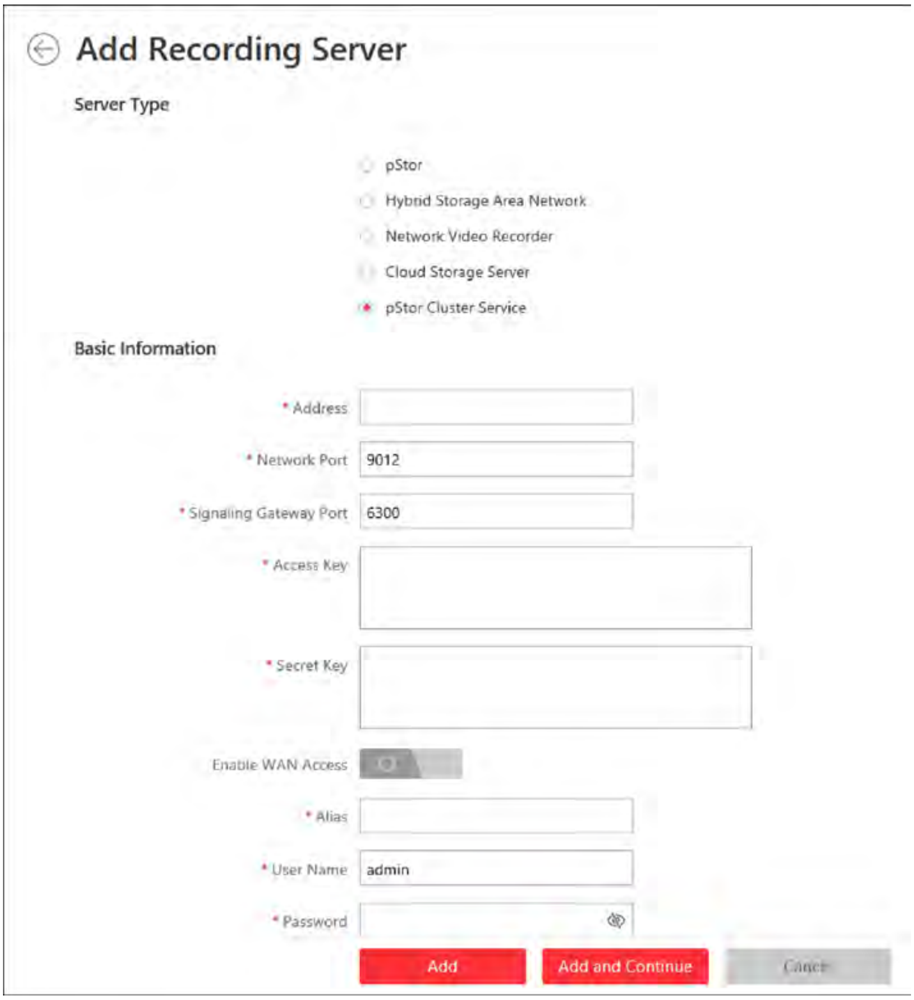
pStor Cluster Service is a service that can manage multiple pStors and the connected disks of pStors. When there are multiple pStors storing a large number of video files, you can add pStor cluster service to the HikCentral Professional for managing pStors. It is also an efficient way to add multiple 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. Click **Physical View → Recording Server** to enter the recording server page.
2. Click **Add** to enter the Add Recording Server page.
3. 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 6-19 Add pStor Cluster Service

4. 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.

5. 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.

6. **Optional:** If you need to access the server via WAN, set the **Enable WAN Access** switch to on and set the corresponding parameters which are available when you access the server via WAN.
7. Enter the 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.

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

Edit Server	Click **Name** 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.

6.8.6 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

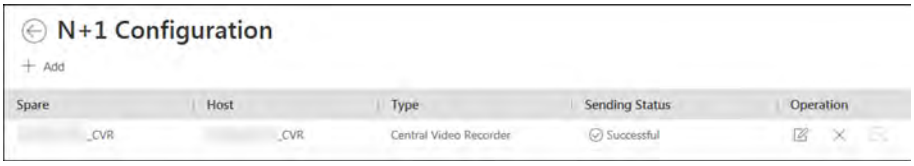
- Make sure the Hybrid Storage Area Networks you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the HikCentral Professional via network.
- At least two online 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. Click **Physical View → Recording Server → N+1 Hot Spare** to enter the N+1 Configuration page.



N+1 Configuration

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

Figure 6-20 N+1 Configuration Page

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

   Note

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

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

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

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

   Note

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

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

6.9 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.

6.9.1 Input Certificate Information to Streaming Server

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

Steps

Note

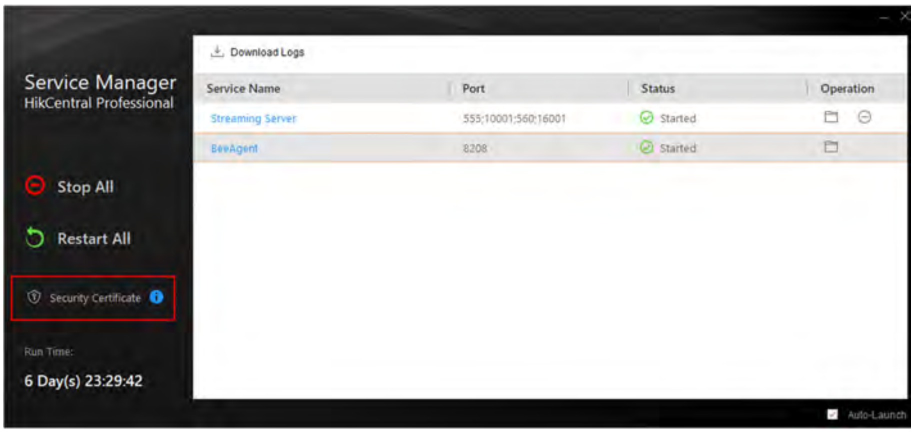
If the service component certificate is updated, you should enter the new certificate information to the Streaming Server again to update.

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

   You will enter the home page of the Web Client.
2. Enter **System → Security → Service Component Certificate** .
3. Click **Generate** beside **Certificate between Services in System** to generate the security certificate for Streaming Server verification.

   Note

   You need to enter the account password for verification to generate the security certificate.
4. On the computer which has installed with Streaming Service, open the Service Manager.
5. Click **Security Certificate**.



Service Name	Port	Status	Operation
Streaming Server	555;10001;560;16001	Started	
BeeAgent	8208	Started	

Run Time:
6 Day(s) 23:29:42

Figure 6-21 Enter Security Certificate

6. Enter the certificate information you generate in step 3.

6.9.2 Add Streaming Server

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

Steps

1. Click **Physical View → Streaming Server** to enter the Streaming Server management page.
2. Click **Add** to enter the Add Streaming Server page.
3. 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**.
4. **Optional:** If you need to access the server via WAN, set the **Enable WAN Access** switch as **ON** and set the corresponding parameters which are available when you access the server via WAN.

   Note

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

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

6.10 Manage DeepinMind Server

You can add DeepinMind Server (including behavior analysis server and facial recognition server) to the HikCentral Professional to implement intelligent functions. The behavior analysis server is used for behavior analysis, including intrusion detection, loitering detection, parking detection, etc. The facial recognition server is used for facial recognition and generate the comparison events.

6.10.1 Add Facial Recognition Server

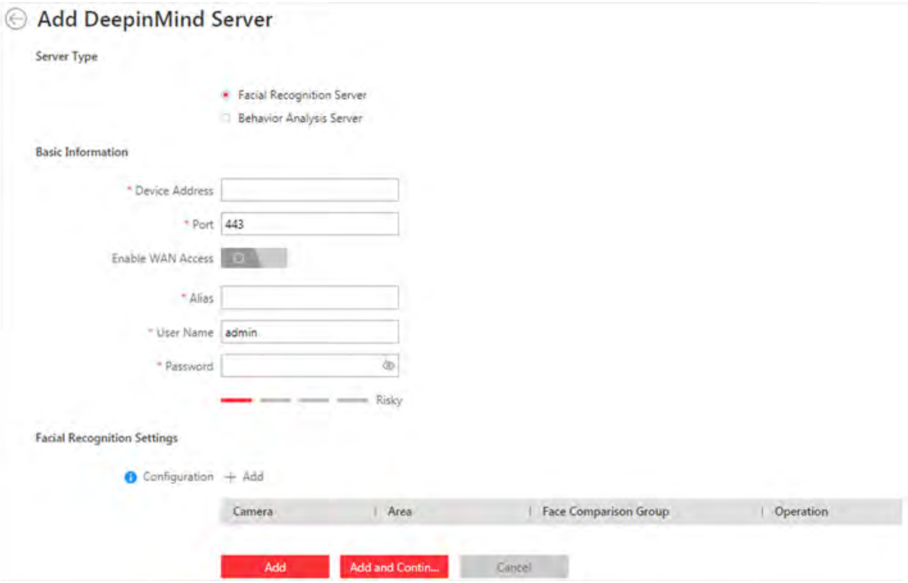
You can add a Facial Recognition Server to the HikCentral Professional for face recognition.

Before You Start

Make sure the Facial Recognition 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

1. Click **Physical View → DeepinMind Server** .
2. Click **Add** to enter the Add DeepinMind Server page.
3. Select the Server Type as **Facial Recognition Server**.



Add DeepinMind Server

Server Type

● Facial Recognition Server

○ Behavior Analysis Server

Basic Information

* Device Address

* Port 443

Enable WAN Access

* Alias

* User Name admin

* Password

Risky

Facial Recognition Settings

Configuration + Add

Camera	Area	Face Comparison Group	Operation

Figure 6-22 Add Facial Recognition Server

4. Set the required basic information such as device address, device port number, and WAN access.

   Device Address

   IP address of the facial recognition server.

   Enable WAN Access

   Enable the facial recognition 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 facial recognition server for WAN access.

5. Configure facial recognition settings to select the facial recognition camera and the face comparison group.
   1) Click **Add**.
   2) Select camera(s) from the area list or enter keywords to search camera(s).

   Note

   After adding one normal camera, the amount of cameras that can be added to the facial recognition server will decrease by 5. While after adding one facial recognition camera, the amount will decease by 1.

   3) Select face comparison group(s) for the server.
6. Finish adding the facial recognition server.

- Click **Add** to finish adding the server.
- Click **Add and Continue** to add the server and continue to add more.

6.10.2 Add Behavior Analysis Server

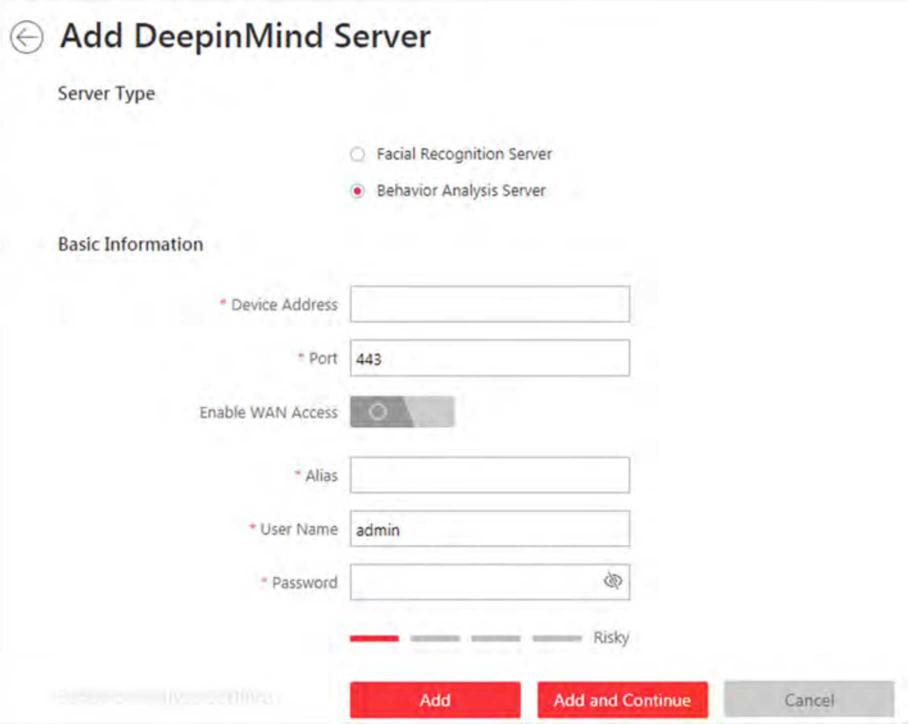
You can add the Behavior Analysis Server to the system for behavior analysis (such as intrusion detection, loitering detection, parking detection, people gathering detection), to receive the behavior analysis related alarms from the server.

Before You Start

Make sure the Behavior Analysis 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

1. Click **Physical View → DeepinMind Server** .
2. Click **Add** to enter the Add DeepinMind Server page.
3. Select the Server Type as **Behavior Analysis Server**.



Add DeepinMind Server

Server Type

○ Facial Recognition Server
● Behavior Analysis Server

Basic Information

* Device Address

* Port 443

Enable WAN Access

* Alias

* User Name admin

* Password

Risky

Figure 6-23 Add Behavior Analysis Server Page

4. Set the required basic information such as device address, device port number, and WAN access.

   Device Address

   IP address of the Behavior Analysis Server.

Device Port

The device port of the Behavior Analysis Server. By default, the port is 443, which means the security audit server access to HikCentral Professional by HTTPS.

Enable WAN Access

Enable the Behavior Analysis Server to access WAN (Wide Area Network).

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 Behavior Analysis Server.

User Name

Enter the user name that has the privilege log into the Behavior Analysis Server.

Password

Enter the password of the user that has the privilege log into the Behavior Analysis Server.

5. Configure behavior analysis settings.

1) Click **Add**.
2) Select camera(s) from the area list or enter keywords to search camera(s).

Note

You can add up to 64 cameras for one behavior analysis server.

3) Select the analysis task for the server.

6. Finish adding the Behavior Analysis Server.

- Click **Add** to finish adding the server.
- Click **Add and Continue** to add the server and continue to add more.

6.11 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

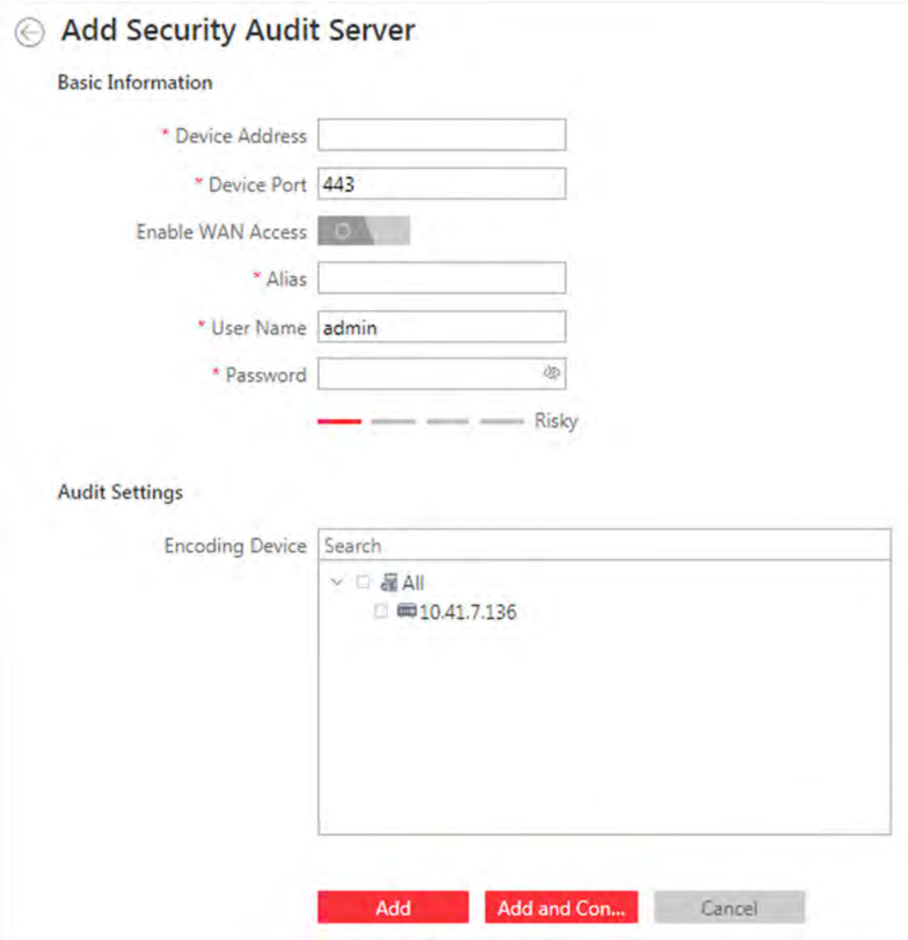
Make sure the Security Audit Server you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the HikCentral Professional via network.

Steps

Note

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. Click **Physical View → Security Audit Server** .
2. 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:

Risky

Audit Settings

Encoding Device: Search

□ All

□ 10.41.7.136

Figure 6-24 Add Security Audit Server Page

3. 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 (Wide Area Network).

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 log into the Security Audit Server.

Password

Enter the password of the user that has the privilege log into the Security Audit Server.

4. 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.

5. 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.

6.12 Manage Smart Wall

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

This mainly includes the following:

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

6.12.1 Add Decoding Device

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

Add Online Decoding Device

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

Before You Start

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

Steps

Note

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

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

   Server Network

   The detected online devices in the same local subnet with the 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.
5. Check the checkbox of the device(s) to be added.

   Note

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

   User Name

The user name for administrator account created when activating the device or the added non-admin account such as operator. When adding the device to 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. Finish adding the decoding device.
   - Click **Add** to add the decoding device and back to the decoding device list page.
   - Click **Add and Continue** to save the settings and continue to add other decoding devices.
8. **Optional:** Perform the following operations after adding the decoding device.

View Decoding Output

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

Edit Decoding Device

Click ✎ to edit the decoding device. You can modify the network location as LAN IP address or WAN IP address according to the type of the network where the device is in.

Remote Configuration

Click ⚙ to set the remote configurations of the device.

Note

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

Delete

Click × to delete the device.

Add Decoding Device by IP Address

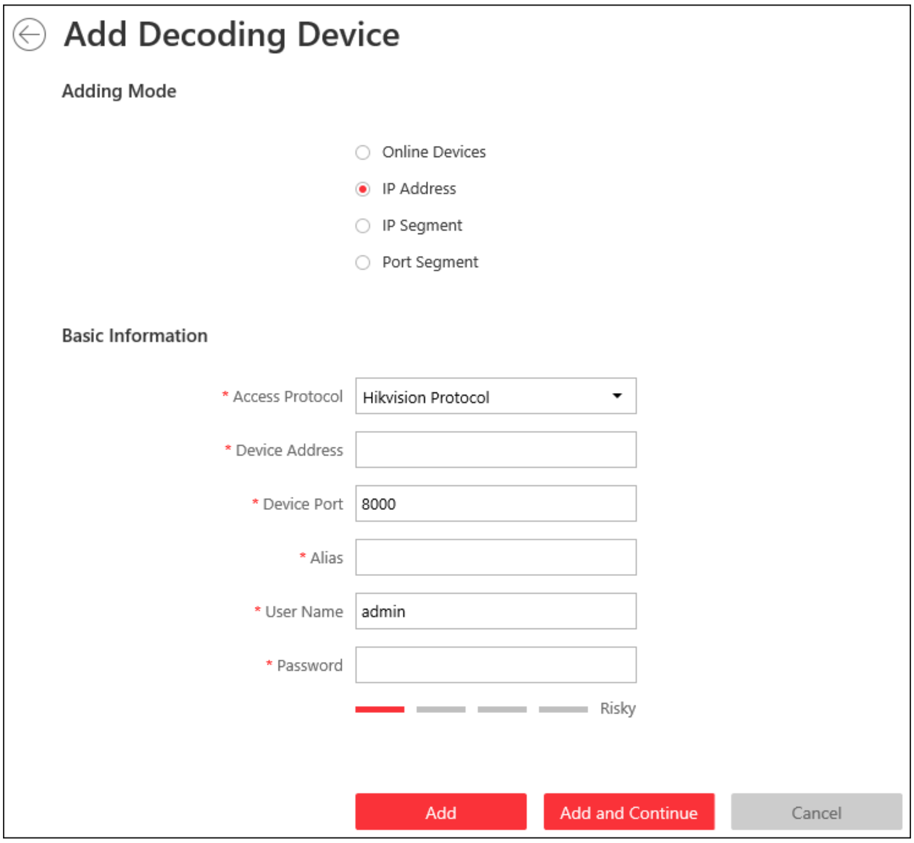
When you know the IP address of the decoding device to add, you can add the device to your system by specifying IP address, user name, password and other related parameters. This adding mode requires you to add the devices one by one, so it is a good choice if you only want to add a few devices and know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

Before You Start

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

Steps

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



Add Decoding Device

Adding Mode

○ Online Devices
● IP Address
○ IP Segment
○ Port Segment

Basic Information

* Access Protocol	Hikvision Protocol
* Device Address	
* Device Port	8000
* Alias	
* User Name	admin
* Password	

Figure 6-25 Add Decoding Device Page

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

Access Protocol

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

Device Address

The IP address of the device.

Device Port

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

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

Alias

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

User Name

The user name for administrator account created when activating the device or the added non-admin account such as operator. When adding the device to 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.

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

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

Add Decoding Devices by IP Segment

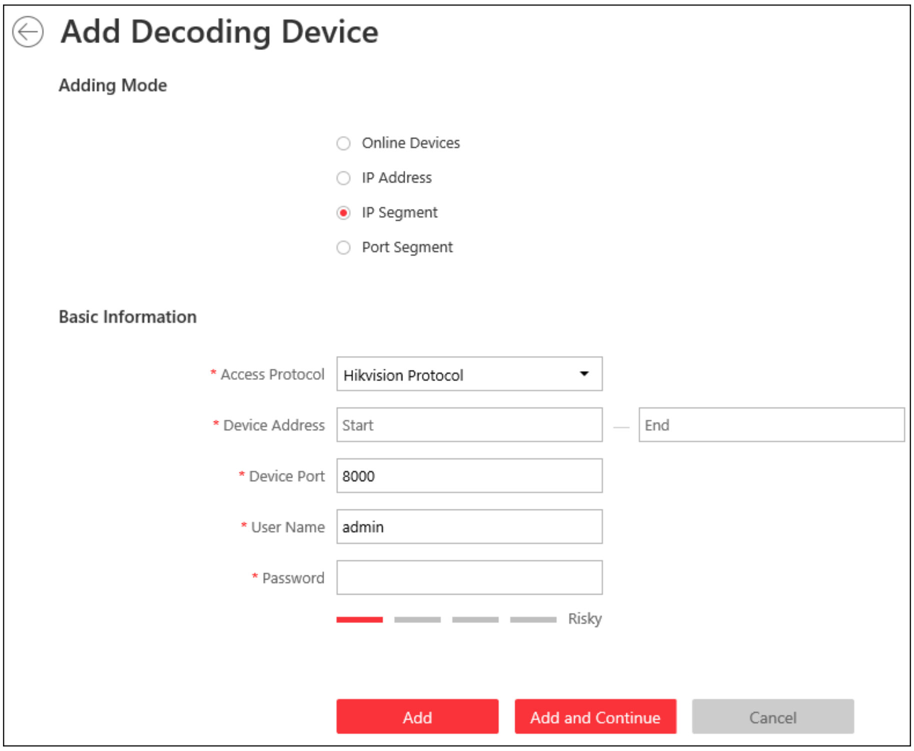
If multiple decoding devices to add have the same port number, user name and password, but have different IP addresses, which are within a range, you can select this adding mode, and specify the IP range where your devices are located, and other related parameters. The system will scan from the start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

Before You Start

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

Steps

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



Add Decoding Device

Adding Mode

○ Online Devices
○ IP Address
● IP Segment
○ Port Segment

Basic Information

* Access Protocol	Hikvision Protocol
* Device Address	Start — End
* Device Port	8000
* User Name	admin
* Password	

Figure 6-26 Add Decoding Device Page

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

   Access Protocol

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

   Device Address

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

Device Port

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

User Name

The user name for administrator account created when activating the device or the added non-admin account such as operator. When adding the device to 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.

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

View Decoding Output

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

Edit Decoding Device

Click ✎ to edit the decoding device. You can modify the network location as LAN IP address or WAN IP address according to the type of the network where the device is in.

Remote Configuration

Click ⚙ to set the remote configurations of the device.

Note

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

Delete

Click × to delete the device.

Add Decoding Devices by Port Segment

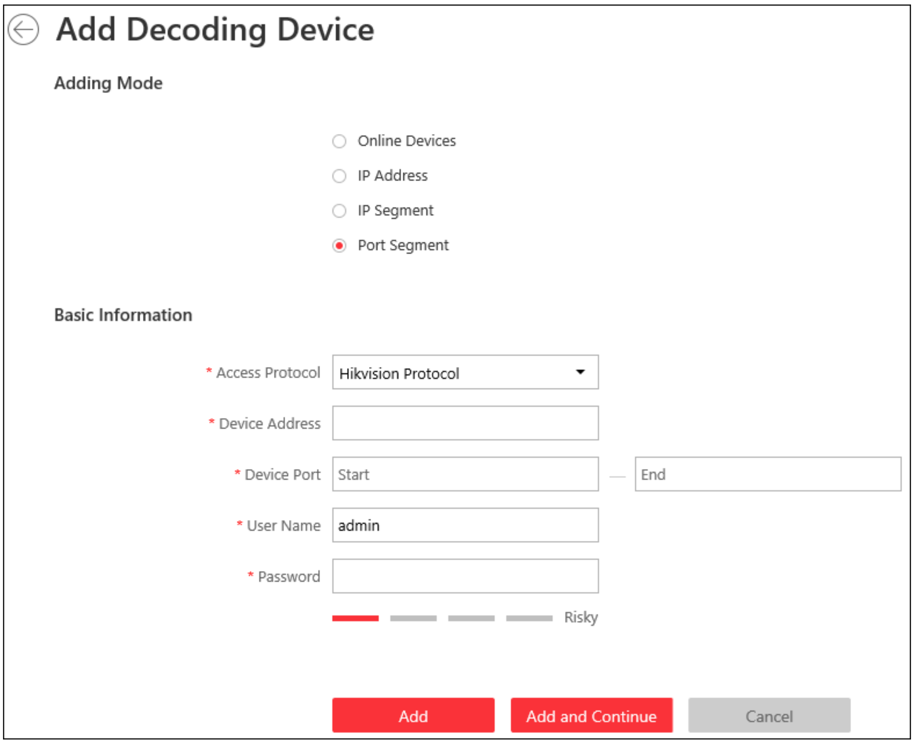
When multiple decoding devices to add have the same IP address, user name and password, but have different port numbers, which are within a range, you can select this adding mode and specify the port range, IP address, user name, password, and other related parameters to add them.

Before You Start

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

Steps

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



Add Decoding Device

Adding Mode

○ Online Devices
○ IP Address
○ IP Segment
● Port Segment

Basic Information

* Access Protocol: Hikvision Protocol
* Device Address:
* Device Port: Start — End
* User Name: admin
* Password:
Risky

Figure 6-27 Add Decoding Device Page

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

   Access Protocol

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

   Device Address

   The same IP address where the devices are located.

Device Port

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

User Name

The user name for administrator account created when activating the device or the added non-admin account such as operator. When adding the device to 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.

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

   After adding the decoding device, the device will display in the list on Decoding Device panel.
6. **Optional:** Perform the following operations after adding the decoding device.

View Decoding Output

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

Edit Decoding Device

Click ✎ to edit the decoding device. You can modify the network location as LAN IP address or WAN IP address according to the type of the network where the device is in.

Remote Configuration

Click ⚙ to set the remote configurations of the device.

Note

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

Delete

Click × to delete the device.

6.12.2 Configure Cascade

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

Before You Start

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

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

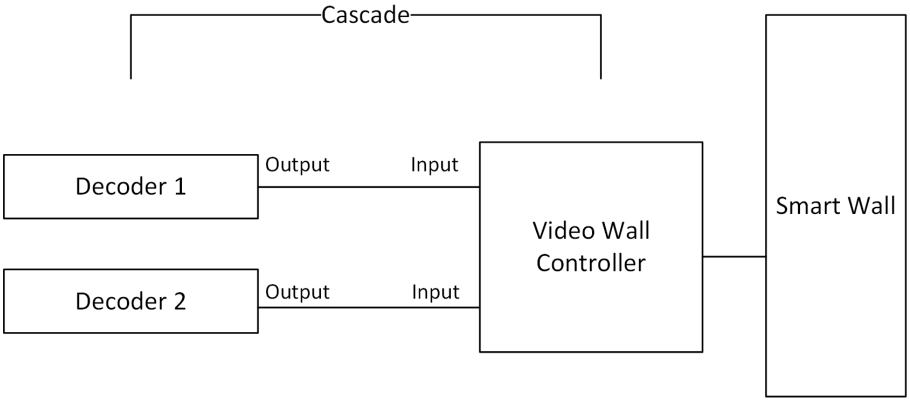


Figure 6-28 Cascade

Steps

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

   The added decoding device(s) and the added smart wall will display.

2. Click behind the added video wall controller to enter the Cascading page.

   Note

   Only video wall controller DS-C10S and DS-C10S-T can support this function.

3. Select the signal channel of the video wall controller and click .
4. Select the decoding output of the decoders to set it as the signal input of the video wall controller.

Note

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

5. Click **Save** to save the cascade.

Result

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

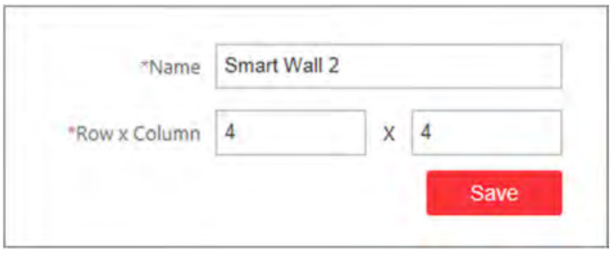
6.12.3 Add Smart Wall

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

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

Steps

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



*Name Smart Wall 2

*Row x Column 4 x 4

Figure 6-29 Add Smart Wall Dialog

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

Link Decoding Output with Window	For details about the operations, see ***Link Decoding Output with Window*** .
Edit Smart Wall	Edit the name of the smart wall.
Delete Smart Wall	Delete the smart wall.

6.12.4 Link Decoding Output with Window

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

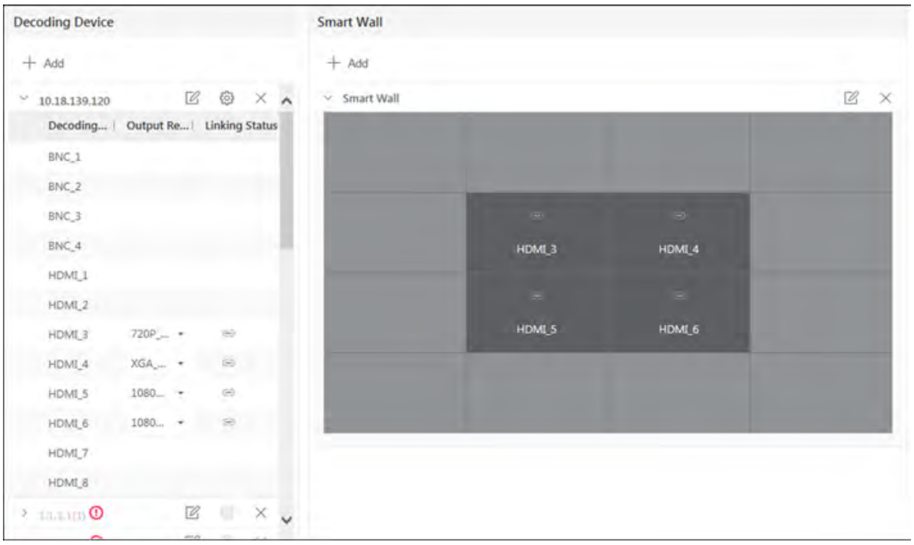
Perform this task when you need to link the decoding output to the smart wall.

Steps

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

   The added decoding device(s) and the added smart wall will display.

2. Click › in front of the decoding device to show the decoding outputs.
3. Click › in front of the smart wall to show the windows.
4. Drag the decoding output from the Decoding Device panel to the display window of the smart wall, to configure the one-to-one correspondence.



Decoding...	Output Re...	Linking Status
BNC_1		
BNC_2		
BNC_3		
BNC_4		
HDMI_1		
HDMI_2		
HDMI_3	720P_...	🔗
HDMI_4	XGA_...	🔗
HDMI_5	1080...	🔗
HDMI_6	1080...	🔗
HDMI_7		
HDMI_8		

Figure 6-30 Link Decoding Device with Window

5. **Optional:** Click ☒ to release the linkage.

Chapter 7 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.

7.1 Add Area

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

7.1.1 Add Area for Current Site

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

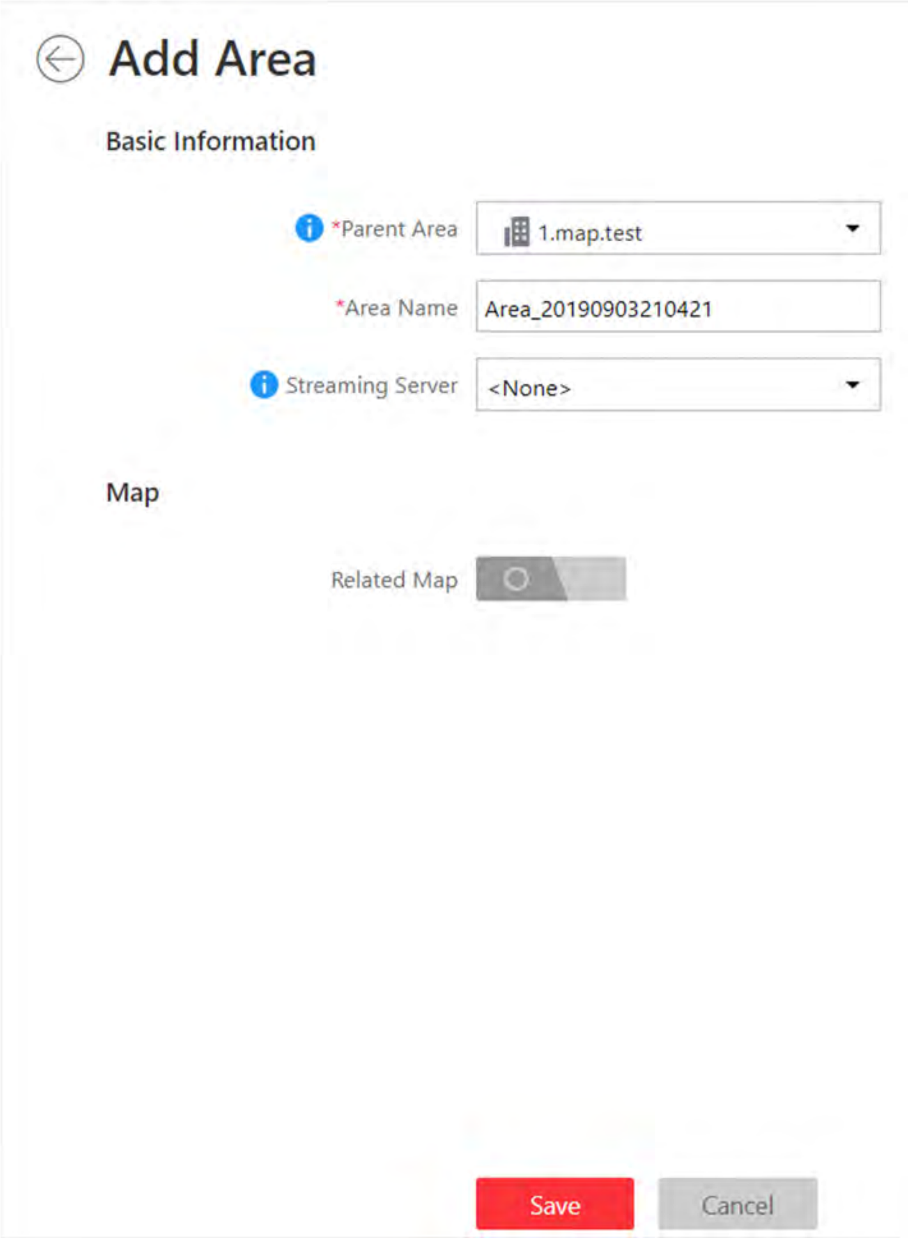
Steps

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

   Note

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

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



Add Area

Basic Information

*Parent Area: 1.map.test

*Area Name: Area_20190903210421

Streaming Server: <None>

Map

Related Map

Figure 7-1 Add Area for Current Site

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

10. Optional: After adding the area, you can do one or more of the following:

Edit Area
Click ✎ to edit the area.

Delete Area
Click 🗑 to delete 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, alarm inputs, alarm outputs, access points, and UVSSs) will be removed from the area, as well as the corresponding recording settings, event settings, and map settings.

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

7.1.2 Add Area for Remote Site

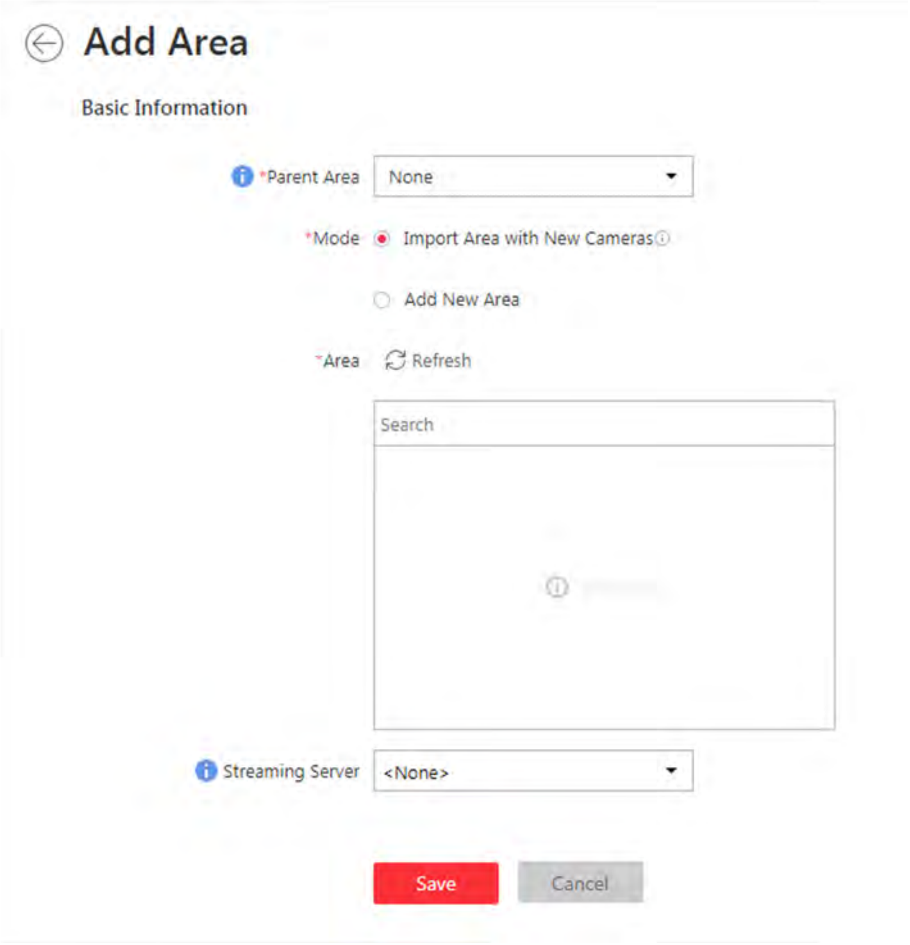
You can add an area for Remote Site to manage the devices in the Central System.

Steps

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

   > **Note**
   >
   > The icon 🌐 indicates that the site is Remote Site.

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



Add Area

Basic Information

*Parent Area: None

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

*Area: Refresh

Search

Streaming Server: <None>

Figure 7-2 Add Area for Remote Site

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

   Import Area with New Cameras

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

   Add New Area

   Add a new area to the parent area.

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

Edit Area	Click ✎ to edit the area.

Delete Area Click 🗑 to delete the selected area, 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 to search the area.

7.2 Add Element to Area

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

7.2.1 Add Camera to Area for Current Site

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

Before You Start

The devices need to be added to the HikCentral Professional for area management. Refer to ***Manage Resource*** for detailed configuration about adding devices.

Steps

Note

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

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

   Note

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

3. Select the **Cameras** tab.
4. Click **Add** to enter the Add Camera page.
5. Select the device type.
6. Select the cameras to add.
7. **Optional:** Check **Get Device's Recording Settings** to obtain the recording schedule configured on the local device and the device can start recording according to the schedule.

Note

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

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

Get Camera Name

Select the cameras and click ↑↓ **Get Camera Name** to get the cameras' names from the device in a batch.

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

Display Cameras of Child Areas

Check **Include Sub-area** to display the cameras of child areas.

7.2.2 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.

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

Steps

Note

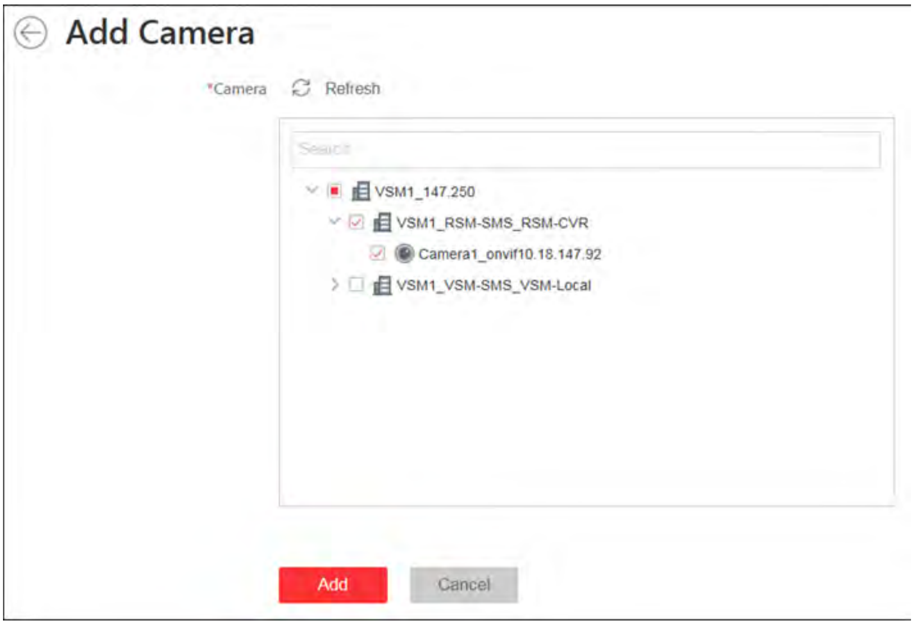
Cameras can only belong to one area. You cannot add a camera to multiple areas.

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

Note

The icon 🌐 indicates that the site is Remote Site.

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



Add Camera

*Camera Refresh

Search

- ■ VSM1_147.250
  - ☑ VSM1_RSM-SMS_RSM-CVR
    - ☑ Camera1_onvif10.18.147.92
  - □ VSM1_VSM-SMS_VSM-Local

Add Cancel

Figure 7-3 Add Camera Page

5. Select the cameras to add.

Note

Up to 64 cameras can be added to one area.

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

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

7.2.3 Add Door to Area for Current Site

You can add doors to areas for the current site for management.

Before You Start

Access control devices need to be added to the system for area management.

Steps

Note

One door can only belong to one area. You cannot add one door to multiple areas.

---

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

   Note

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

   ---

3. Select the **Doors** tab.
4. Click **Add** to enter the Add Door page.
5. Select the door(s) to add.
6. **Optional:** Check **Add to Map** to add the door to the map.
7. Click **Add**.
8. **Optional:** After adding the doors, you can do one or more of the followings.

   Get Door Name
   Select the doors and click ↑↓ **Get Door Name** to get 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.

7.2.4 Add Elevator to Area for Current Site

You should add elevator to areas for further management.

Before You Start

Elevator control devices need to be added to the system for area management.

Steps

Note

One elevator can only belong to one area. You cannot add an elevator to multiple areas.

---

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

3. Select the **Elevators** tab.
4. Click **Add** to enter the Add Elevator page.
5. In the Elevator Control Device list, all the added elevator control devices are displayed. Select the device to add the elevator to this area.
6. In the **Range of Floor No.** field, enter the start No. and end No. of the floors that you want to import to the area.

   The floors between the start No. and end No. will be imported to the area. After imported, you can manage the floors in the system, such as adding to access levels, controlling status, etc.
7. Check **Add to Map** to add the elevator to the map.
8. Click **Add**.
9. After adding the elevator, you can do one or more of the followings.

   Get Floor Name
   Select the elevator and click ↑↓ **Get Floor Name** to get the floors' names of the elevator from the device in a batch.

   Apply Floor Name
   Select the elevator and click to apply the elevator's floors names to the device in a batch.

7.2.5 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 detailed configuration about adding devices.

Steps

Note

You cannot add a radar to multiple areas.

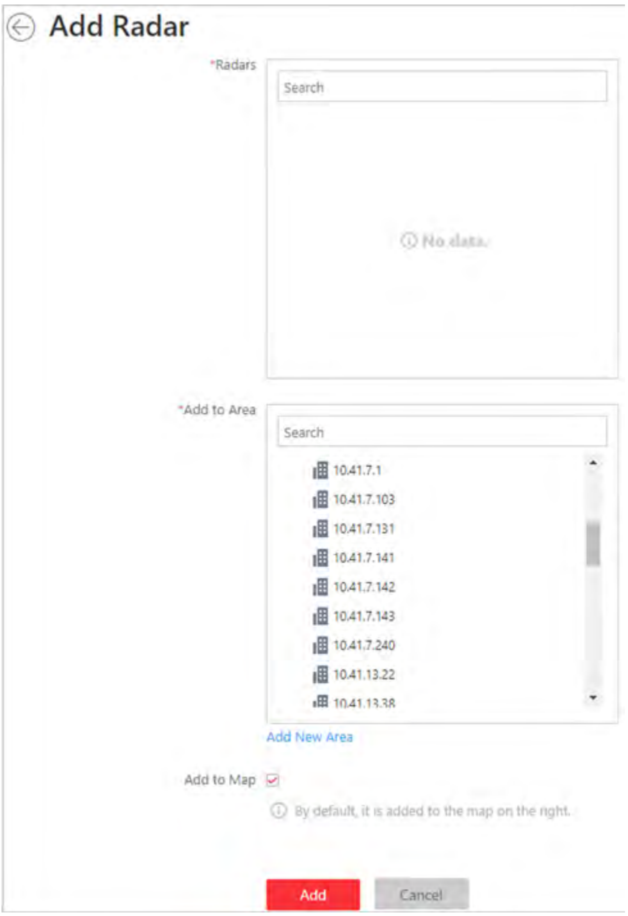
1. Click **Logical View** on the Home page to enter the Area Management page.
2. In the area list panel, select the added current site in the drop-down site list to show its areas.

   Note

   The icon indicates that the site is current site.
3. Select an area.
4. Click **Radars** tab.
5. Click **Add** to enter the Add Radar page.
6. Search a radar in the **Radar** and select a radar in the searching results.
7. Select an area in the **Add to Area** frame.

Note

You can click **Add New Area** to add a new area to the site.



Add Radar

*Radars

Search

No data.

*Add to Area

Search

10.41.7.1

10.41.7.103

10.41.7.131

10.41.7.141

10.41.7.142

10.41.7.143

10.41.7.240

10.41.13.22

10.41.13.38

Add New Area

Add to Map ☑

By default, it is added to the map on the right.

Add

Cancel

Figure 7-4 Add Radar Page

8. **Optional:** Check **Add to Map** to add the camera to the map.

Note

- You can go back to the **Radars** tab and drag the radar to another map.
- You can perform operations on the map including editing radar, deleting radar on the map, editing detection area, drawing zone, selecting related cameras, and calibrate PTZ camera. See ***Edit Radar for Current Site*** for details.

9. Click **Add**.
10. **Optional:** Check added radars in the list and click **Arm/Disarm** to arm or disarm the checked radars.

Note

An event will be triggered if anybody or an object enters an armed radar's detection area.

7.2.6 Add Alarm Input to Area

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

Before You Start

Devices need to be added to the HikCentral Professional for area management. Refer to ***Manage Resource*** for detailed configuration about adding devices.

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

Steps

Note

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

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

   Note

   - For a Central System with a Remote Site Management module, you can select the current site from the drop-down site list to show its areas.
   - The icon 🌐 indicates that the site is current site.
3. Select the **Alarm Inputs** tab.
4. Click **Add** to enter the Add Alarm Inputs page.
5. Select the device type.
6. Select the alarm inputs to add.

   Note

   For the security control device, you need to select its zones as alarm inputs to add to the area.
7. **Optional:** Check **Add to Map** to add the alarm input to the map.
8. Click **Add**.
9. **Optional:** After adding the alarm inputs, you can do one or more of the followings.

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

Display Alarm Inputs of Child Areas Check **Include Sub-area** to display the alarm inputs of child areas.

7.2.7 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

Devices need to be added to the HikCentral Professional for area management. Refer to ***Manage Resource*** for detailed configuration about adding devices.

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

Steps

Note

One alarm output can only belong to one area. You cannot add an alarm output to multiple areas.

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

   Note

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

3. Select the **Alarm Outputs** tab.
4. Click **Add** to enter the Add Alarm Outputs page.
5. Select the device type.
6. Select the alarm outputs to add.
7. **Optional:** Check **Add to Map** to add the alarm output to the map.
8. Click **Add**.
9. **Optional:** After adding the alarm outputs, you can do one or more of the followings.

Move to Other Area	Select the alarm outputs and click **Move to Other Area**. Then select the target area to move the selected alarm outputs to and click **Move**.
Display Alarm Outputs of Child Areas	Check **Include Sub-area** to display the alarm outputs of child areas.

7.2.8 Add UVSS to Area for Current Site

You can add Under Vehicle Surveillance Systems (UVSSs) to areas for the current site for management.

Perform this task when you need to add Current Site's UVSSs to areas.

Steps

Note

UVSSs can only belong to one area. You cannot add a UVSS to multiple areas.

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

   Note

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

3. Select the **Under Vehicle Surveillance Systems** tab.

   Note

   If the map function is enabled, you can click » and click **UVSSs**.

4. Click **Add** to enter the Add UVSS page.
5. Input the required information of UVSS.
6. Link cameras to the UVSS.
   1) Set **Relate Camera** switch to ON.
   2) Select the cameras.
7. Check **Add to Map** to add the UVSS on the map.
8. Click **Add**.

7.3 Edit Element in Area

You can edit the area's added elements, such as recording settings, event settings, and map settings for cameras, application settings, hardware settings, and attendance settings for doors, and so on.

7.3.1 Edit Camera for Current Site

You can edit basic information, recording settings, picture storage settings, event settings, and map settings of the camera for current site. You can also edit the face comparison group settings of the cameras which support face picture comparison.

Steps

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

Note

The icon 🌐 indicates that the site is current site.

3. Select an area.
4. Select the **Cameras** tab to show the added cameras.
5. Click a camera's name in the **Name** column to enter the Edit Camera 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 **Apply Camera Name** 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 click ▶ in the lower-right corner to switch to playback.

   Note

   The live view and playback functions in the camera details page are only supported by Internet Explorer.

8. Edit the recording settings of the camera. See ***Configure Recording*** for details.

   Note

   - If no recording settings have been configured for the camera, you can click **Configuration** to set the parameters.
   - You can also select multiple cameras and click **Get Recording Schedule** in the added cameras list page to get recording schedules of the devices in a batch.

9. **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 of devices added by ISUP protocol, this function is not available. You should click **Configuration** to edit the picture storage configuration.

10. Edit the event settings of the camera. See ***Configure Event and Alarm*** for details.

    Note

    If no event settings have been configured for the camera, you can click **Configuration** to set the parameters.

11. **Optional:** Set the face comparison.

Note

If this is supported by the license you purchased, you need to enter License Details page and click **Configuration** on Facial Recognition Camera line to add the camera as the facial recognition camera firstly. If you do not add the camera as a facial recognition camera, this function and Attendance will not show. If you did not purchase a license for Attendance, the Attendance will not show either.

1)**Optional:** Set **Link to Facial Recognition Server** switch to on and select a server.

Note

After linking to facial recognition server, the facial recognition camera no longer supports the face comparison groups on itself. For the normal camera, you must link it with a server.

2)Select the person group(s) for face comparison.

Note

You can click **Add New** to add new face comparison group and set the face comparison similarity threshold which affects the frequency and accuracy of face picture comparison alarm.

12. Add the camera to the map.

1)Set the **Add to Map** switch to on.

2)**Optional:** Check **Auto-Locating on Map** to get the GIS location information from the device and locate the camera on the map automatically.

Note

This function is only available when the map type is GIS map and should be supported by the device. The camera should have GIS function, or you should configure GIS location information for camera on the device first.

3)Select the icon style and name color for displaying the camera on the map.

13. **Optional:** Click **Configuration on Device** to set the remote configurations of the corresponding device if needed.

Note

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

14. Click **Save**.

15. **Optional:** Enter Edit Camera page again and click **Copy to** to select configuration item and copy the settings of this camera to other cameras.

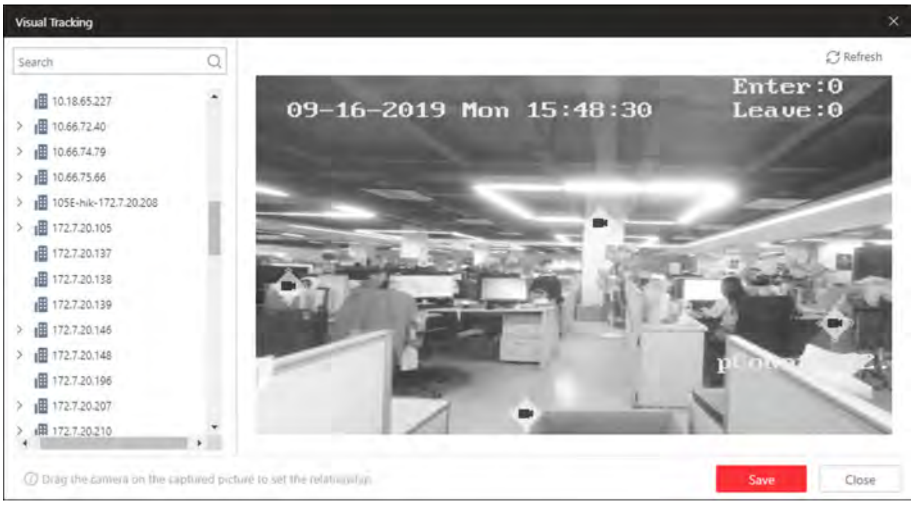
7.3.2 Configure Visual Tracking

Visual tracking allows you to track an individual (such as a suspect) across different areas without losing sight of the individual. You need to associate one camera with other cameras nearby so that you can click on the image of this camera to jump to other associated cameras' views. To associate the camera with other cameras nearby, you should create on-video overlays for a camera, thus when you click on the overlays on one camera, it will jump to other cameras during live view or playback.

Steps

1. Enter **Logical View → Cameras** to enter the camera management page.
2. Select one area on the area list and click the camera name in the **Name** column to enter the Edit Camera page.
3. In the Basic Information, click **Visual Tracking** to open the Visual Tracking settings window.

   The real-time image of the current camera will be displayed. You can click **Refresh** to get the latest image of the camera.
4. On the camera list on the left, drag cameras on the captured image of the current camera and place them according to the actual mounting positions to associate them.



Drag the camera on the captured picture to set the relationship.

Figure 7-5 Set Visual Tracking

5. **Optional:** To remove the cameras overlaid on the captured image, click the camera icon and click **Delete**.
6. Click **Save**.

Example

For example, 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 one camera respectively. You can associate camera B, C and D with camera A for visual tracking. When an individual passing by and turns to hallway B, the security personnel can click the area B on the image of camera A to jump to the image of camera B.

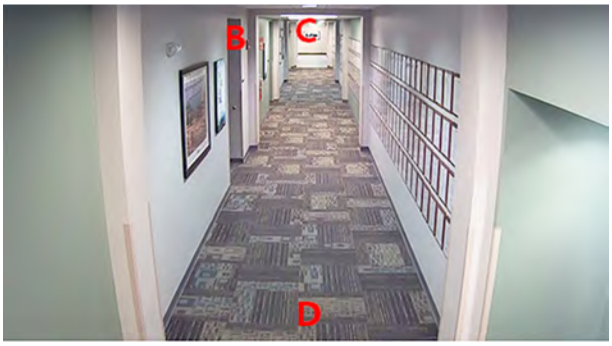


Figure 7-6 Visual Tracking in Hallway (Camera A)

7.3.3 Edit Door for Current Site

You can edit basic information, related cameras, application settings, hardware settings, access level, attendance settings, picture storage settings, event settings, and map settings of the door on current site.

Steps

1. Click **Logical View** on the Home page to enter the Area Management page.
2. In the area list panel, select the added current site from the drop-down site list to show its areas and select one area.
3. Select the **Doors** tab to show the added doors in this area.
4. Click **Name** column to enter the Edit Door page.
5. Edit the door's basic information.

Name

Edit the name for the door.

Note

If you changes the name, you can click **Apply Door Name** 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.

Dismiss Code

If you enter this code on the card reader keypad, the buzzer's beeping will be stopped. It should be different with the duress code and super password.

Door Status Settings

You can enable this function to set free access schedule and access forbidden schedule.

Free Access Schedule

During this schedule, the door remains unlocked. User can enter or exit via the access point without any credentials. For turnstile, you can set schedules for entrance and exist respectively.

Access Forbidden Schedule

During this schedule, the door remains locked. No user (except for super user) can enter or exit via the door even with credentials.

6. Link 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.

7. **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.

Note

Refer to ***Configure Storage for Uploaded Pictures*** for details.

8. Edit the application settings.

Entry & Exit Counting

You can enable this function to count the persons entering and exiting the doors in the group. For setting entry & exit counting rule, refer to ***Add Entry and Exit Counting Group*** .

Multi-Door Interlocking

You can enable the multi-door interlocking function between multiple doors of the same access control device. To unlock one of the doors, other doors must remain locked. For setting multi-door interlocking rule, refer to ***Configure Multi-Door Interlocking*** .

Anti-passback

The person should exit via the door in the anti-passback if he/she enters via the door in the anti-passback. It minimizes the misuse or fraudulent use of access credentials such as passing back card to an unauthorized person, or tailed access. For setting the anti-passback rule, refer to ***Configure Anti-Passback Rules*** .

Open Door with First Card

After swiping the first card, the door will remain unlocked or be authorized. The status depends on the card swiping times (odd or even). For odd, the door will remain unlocked or be authorized. For even, it will exit the unlocked or authorized mode.

Multi-Factor Authentication

Multi-factor authentication is an authentication method in which the access can be granted only after more than one method of authentication to verify the user's identity for access. For details about setting the multi-factor authentication rule, refer to ***Configure Multi-Factor Authentication Rules*** .

9. In the Hardware panel, set the **Card Reader** switch to on and set the card reader related parameters.

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 all the time.

Note

The card reader's access modes should be supported by the device.

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.

Note

You can add a custom schedule template and up to 3 time periods can be set for each day. See ***Set Access Schedule Template*** for details.

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)Set the **Face Recognition Terminal** switch to ON to add the face recognition terminals.
    2)Click **Add** to enter Add Face Recognition Terminal page.
    3)Select **IP Address**, **Online Devices**, or **Device ID** as the adding mode, and set the required parameters, which may vary according to different terminals.
    4)Click **Add** to link the terminal to turnstile.
11. **Optional:** Add the door to one access level. For details about access level, refer to ***Manage Access Level*** .
12. **Optional:** Set the door as attendance check point if needed and set the attendance type. All the access records on the card readers of the doors will be recorded for attendance calculation.

Check-In/Out

The access records on the card readers of this door will be calculated as check-in or check-out.

Check-In Only

All the access records on the card readers of this door will be calculated as check-in only.

Check-Out Only

All the access records on the card readers of this door will be calculated as check-out only.

13. **Optional:** View the event settings of the door. See ***Configure Event and Alarm*** for details.

Note

If no event settings have been configured for the door, you can click **Configuration** to set the parameters.

14. Add the door to the map.
    1)Set the **Add to Map** switch to ON.
    2)Select the icon style and name color for displaying the access point on the map.
15. Click **Save**.
16. **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).

7.3.4 Edit Elevator for Current Site

You can edit basic information, floor information, related cameras, hardware settings, event settings, and map settings of the elevator on current site.

Steps

1. Click **Logical View** on the Home page to enter the Area Management page.
2. In the area list panel, select the added current site from the drop-down site list to show its areas and select one area.
3. Select the **Elevators** tab to show the added elevators in this area.
4. Click **Name** column to enter the Edit Elevator page.
5. Edit the elevator's basic information.

Name

Edit the name for the elevator.

Open Duration

The time interval between the elevator door is open and closed again.

Extended Open Duration

The time interval between the elevator door is open and closed again for the person whose extended access function is enabled.

Elevator Door Open Timeout Alarm

After enabled, if the elevator has configured with event or alarm, when the elevator door 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.

Dismiss Code

If you enter this code on the card reader keypad, the buzzer's beeping will be stopped. It should be different with the duress code and super password.

6. In the Floor panel, all the imported floors will be displayed in the list. You can set the floors' status schedule, access levels, etc.

Schedule Settings

Set free access schedule and access forbidden schedule for the floor to define when the floor is accessible and not accessible.

Select the floor in the list and click **Schedule Settings** to set the schedule.

Free Access Schedule

During this schedule, all the persons can access this floor even without any credentials.

Access Forbidden Schedule

During this schedule, no person (except for super user) can access this floor even with credentials.

Access Level Settings

Add the floor to the existing access level to define the access permission that which person(s) can get access to which floor(s) during the authorized time period. For details about access level, refer to ***Manage Access Level*** .

Select the floor in the list and click **Access Level Settings** to add the floor to the access level.

Edit Floor Name

You can edit the floor name if needed.

Note

If you changes the name, you can click **Apply Floor Name** in the elevator list page to apply the new name to the device.

Reset Imported Floor No.

You can click **Reset Imported Floor No.** and enter the range of the floor No. to reset the settings of the floors, such as schedule settings, name, access level settings, etc.

7. Link cameras (such as the cameras mounted inside the elevator) to the elevator, 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 elevator.

8. In the Hardware panel, set the **Card Reader** switch to on and set the card reader related parameters.

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 all the time.

Note

The card reader's access modes should be supported by the device.

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.

Note

You can add a custom schedule template and up to 3 time periods can be set for each day. See ***Set Access Schedule Template*** for details.

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.

9. **Optional:** View the event settings of the elevator. See ***Configure Event and Alarm*** for details.

Note

If no event settings have been configured for the elevator, you can click **Configuration** to set the parameters.

10. Add the elevator to the map.
    1)Set the **Add to Map** switch to ON.
    2)Select the icon style and name color for displaying the access point on the map.
11. Click **Save**.
12. **Optional:** If needed, enter the Edit Elevator page again and click **Copy to** to apply the current settings of the elevator to other elevator(s).

7.3.5 Edit Radar for Current Site

After adding a radar to an area of the current site, you can edit the parameters of the radar, including map settings, zone settings, camera calibration, and event settings.

Before You Start

Make sure you have configured GIS map. See ***Set GIS Map and Icons*** for details about configuring GIS map.

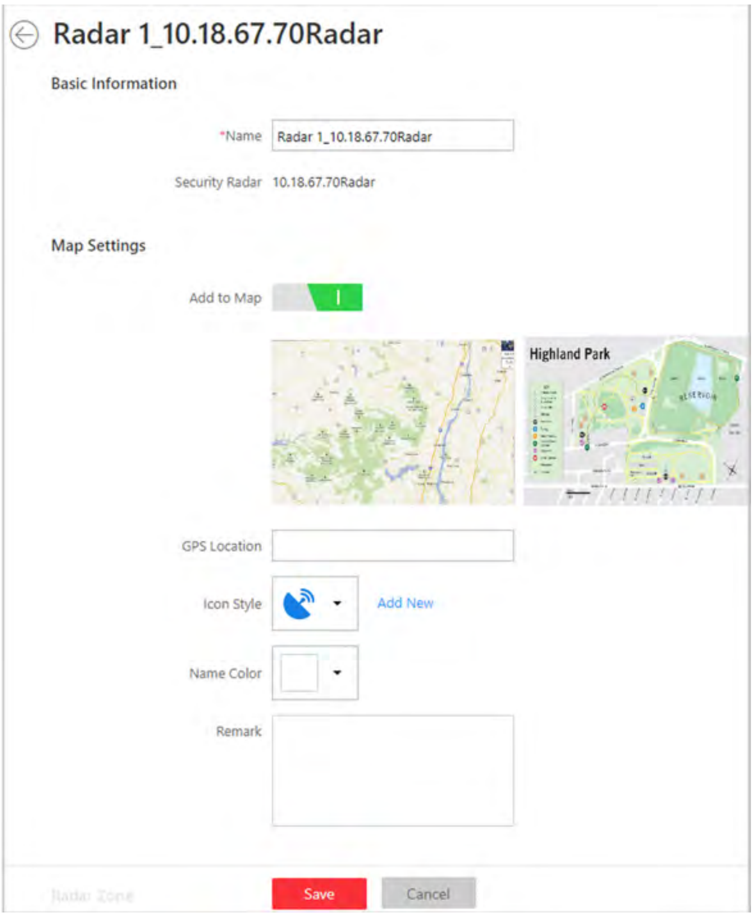
Steps

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

Note

The icon 🌐 indicates that the site is current site.

3. Select an area.
4. Select the **Radars** tab to show the added radars.
5. Click a radar's name in the **Name** column to enter the Edit Radar page.
6. Edit the radar's name in Basic Information field.
7. Edit Map Settings.



Radar 1_10.18.67.70Radar

Basic Information

*Name: Radar 1_10.18.67.70Radar

Security Radar: 10.18.67.70Radar

Map Settings

Add to Map: I

GPS Location:

Icon Style: Add New

Name Color:

Remark:

Radar Zone

Save

Cancel

Figure 7-7 Edit Radar Page

1) Enter the GPS Location for the radar.

Note

Enter a place name and the searching results will pop up. Select a result in the list.

2) Select an icon and name color on the map for the radar.

Note

You can click **Add New** to upload a new icon picture saved in your computer.

8. Configure radar zone.

1) Click the radar's icon on the map and then click **Draw Zone** to start drawing a zone.

2) Select a zone drawing method in the tool bar in the upper-left corner of the map.

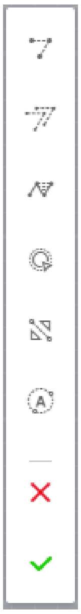


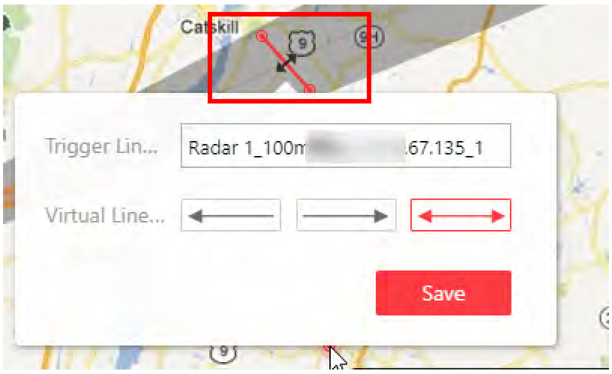
Figure 7-8 Tool Bar for Drawing Zone

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 7-9 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.

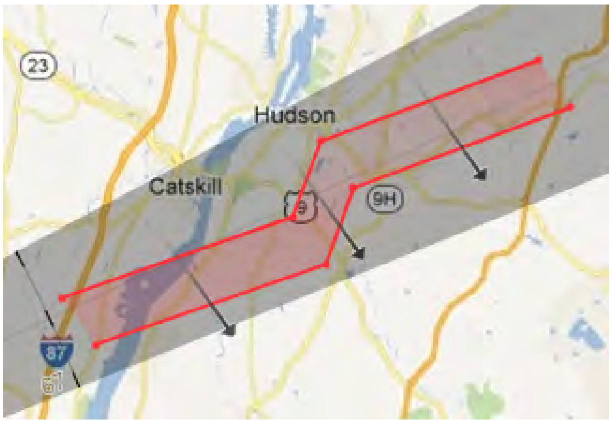


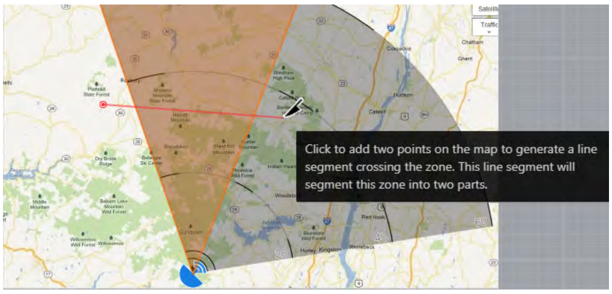
Figure 7-10 Dual-Trigger Line in the Detection Area

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.



Click to add two points on the map to generate a line segment crossing the zone. This line segment will segment this zone into two parts.

Figure 7-11 Zone Segmentation

Distance Segmentation

Split a zone into two smaller zone by an arc.

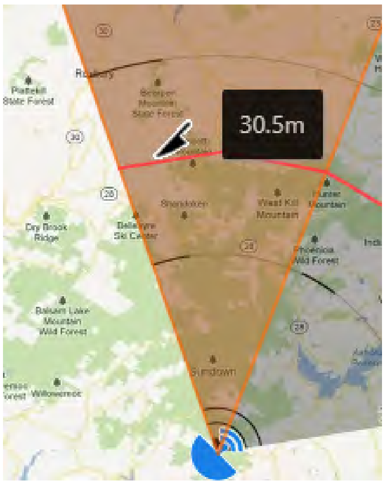


Figure 7-12 Distance Segmentation

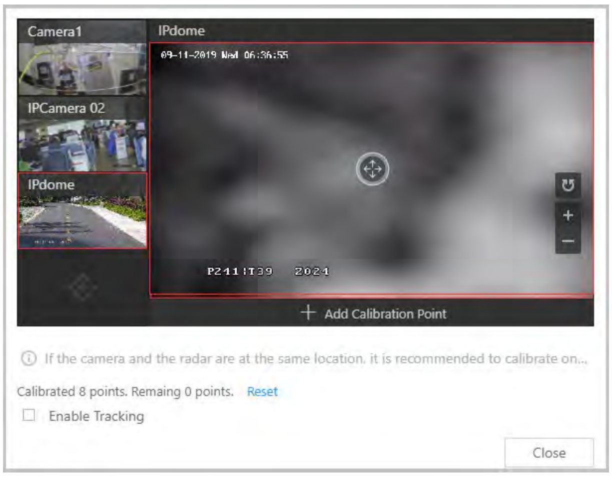
Field Assistance

Click to enable zone painting assistance function. For example, person A takes an on-site walk along the field to shape a closed figure as a zone. And then the moving path will automatically be painted as a zone on the map and a window for selecting zone type will pop up. And then Person B which operating the computer running the Web Client select a type for the zone.

9. Set related calibrated camera(s) for radar.

Note

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 calibrated camera(s) according to person A's position.



ⓘ 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

Close

Figure 7-13 Add Calibration Point Window

1) Click **Add** to select a camera in the area list.

Note

- This function needs to be supported by the device.
- Up to 4 calibrated cameras can be added.

The added cameras are displayed in a form.

2) Person A goes to the location which can be detected by one of the calibrated cameras. Person B clicks 👤 in the Operation column.

   Person A's location will appear on the map as a red point ● .
3) Click ● to open the adding calibration point window.

   The calibrated cameras' thumbnails will be displayed on the left.
4) **Optional:** Undo-check the **Enable Tracking** if you have enabled visual tracking for the calibrated cameras.
5) Click a calibrated camera's thumbnail to display its image in the window on the right.
6) Click the image to turn the camera to the position of person A until person A appears in the image.
7) Click **Add Calibration Point** to add the current image as a calibration point.

Note

- If the calibrated 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 calibrated cameras.

8) **Optional:** Check **Enable Tracking** if you have enabled visual tracking for the calibrated cameras.
9) Close the Add Calibration Point window and click ✓ to save the settings.

10. Optional: Click **Configuration** to set event for the radar. See ***Configure Event and Alarm*** for details.

11. Click **Save** to save the settings for the radar.

7.3.6 Edit Alarm Input for Current Site

You can edit basic information, event settings, and map settings of the alarm input for current site.

Perform this task when you need to edit alarm input for current site.

Steps

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

Note

The icon 🌐 indicates that the site is current site.

3. Select the **Alarm Inputs** tab to show the added alarm inputs.

4. Click Name column to enter the Edit Alarm Input page.
5. Edit the alarm input name.
6. **Optional:** For the alarm input of the security control device, select **Detector Type** and **Zone Type** according to the actual deployment.
7. Edit the event settings of the alarm input. See ***Configure Event and Alarm*** for details.

Note

If no event settings have been configured for the alarm input, you can click **Configuration** to set the parameters.

8. Add the alarm input to the map.
   1) Set the **Add to Map** switch to ON.
   2) Select the icon style and name color for displaying the alarm input on the map.
9. Click **Save**.

7.3.7 Edit Alarm Output for Current Site

You can edit basic information and map settings of the alarm output for current site.

Perform this task when you need to edit alarm output for current site.

Steps

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

Note

The icon 🌐 indicates that the site is current site.

3. Select the **Alarm Outputs** tab to show the added alarm outputs.
4. Click Name column to enter the Edit Alarm Output page.
5. Edit the alarm output name.
6. Add the alarm output to the map.
   1) Set the **Add to Map** switch to ON.
   2) Select the icon style and name color for displaying the alarm output on the map.
7. Click **Save**.

7.3.8 Edit Under Vehicle Surveillance System for Current Site

You can edit basic information, related cameras, and map settings of the Under Vehicle Surveillance System (UVSS) for current site.

Perform this task when you need to edit UVSS for current site.

Steps

1. Click **Logical View** on the Home page to enter the Area Management page.

2. In the area list panel, select the added current site from the drop-down site list to show its areas.

   Note

   The icon 🌐 indicates that the site is current site.

3. Select an area.
4. Select the **Under Vehicle Surveillance Systems** tab to show the added UVSSs.

   Note

   If the map function is enabled, you should click » and click **UVSSs**.

5. Click Name column to enter the Edit UVSS page.
6. Edit the UVSS's basic information, such as IP address, port No., and so on.
7. Link cameras to the UVSS.
   1) Set the **Relate Camera** switch to ON.
   2) Select the camera(s).
8. Add the UVSS to the map.
   1) Set the **Add to Map** switch to ON.
   2) Select the icon style and name color for displaying the UVSS on the map.
9. Click **Save**.

7.3.9 Edit Third-Party Integrated Resource for Current Site

After integrating the resources on third-party system to the HikCentral Professional via Optimus, the third-party resources are added to the areas in the **Logical View** module.

Click **Logical View** on the Home page and click **Third-Party Integrated Resource** tab.

Click the name of third-party resource to enter the details page.

You can view the basic information of the resource, such as name, device type, and manufacturer.

You can also add the resource on the map so that when an event/alarm is triggered on the resource, you can view the notification and details on the map.

Note

For details about locating resource on map, refer to ***Add Hot Spot on Map*** .

7.3.10 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. Click **Logical View** on the Home page to enter the Area Management page.

2. In the area list panel, select the added Remote Site from the drop-down site list to show its areas.

Note

The icon 🌐 indicates that the site is a Remote Site.

3. Select an area to show its added cameras.
4. Click the Name field to edit the parameters of the cameras including basic information and recording settings.

Note

For recording settings, if no recording settings have been configured for the camera, click **Configuration** to set the parameters (for details, refer to ***Configure Recording for Cameras on Remote Site***).

5. **Optional:** Click ▶ to view the live view of the camera and hover over the window and click ▶ in the lower-right corner to switch to playback.

Note

The live view and playback functions in the camera details page are only supported by Internet Explorer.

6. **Optional:** Click **Copy to** to copy the current camera's specified configuration parameters to other cameras of the Remote Site.
7. Click **Save**.
8. **Optional:** Perform one of the following operations.

Get Camera Name	Select one or multiple cameras and click **Get Camera Name** to get the cameras' names from the devices.
Edit Camera on Site	Click ⚙ in the added camera list to open the remote site configuration page of the camera to edit it.

7.4 Remove Element from Area

You can remove the added cameras, alarm inputs, alarm outputs, doors, and Under Vehicle Surveillance Systems (UVSSs) from the area.

7.4.1 Remove Element from Area for Current Site

You can remove the added cameras, alarm inputs, alarm outputs, doors, and UVSSs from the area for current site.

Steps

1. Click **Logical View** on the Home page to enter the Area Management page.

2. Select an area in the area list panel to show its added elements.

Note

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

3. Select the Cameras, Alarm Inputs, Alarm Outputs, Doors, or UVSSs tab to show the added elements.
4. Select the elements.
5. Click **Delete**.

7.4.2 Remove Element from Area for Remote Site

If the current system is a Central System with a Remote Site Management module, you can remove the added cameras from its area.

Perform this task when you need to remove the element from the area for the Remote Site.

Steps

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

Note

The icon 🌐 indicates that the site is a Remote Site.

3. Select an area to show its added cameras.
4. Select the cameras.
5. Click **Delete**.
6. **Optional:** If ⊗ appears near the camera name, it means the camera has been deleted from the Remote Site. Hover the cursor over the ⊗ and click **Delete** to delete the camera from the area.

7.5 Manage Resource Group

After adding the resources into areas for management, you can group the resources into different resources groups according to actual needs.

Currently, the system supports following types of resource groups.

Alarm Group

The alarm group is used to group the resources in certain region and provides alarm notification when the alarm occurs on the resources in the group. By grouping the resources and locating the group on the map, when an alarm occurs, the region of the group will be highlighted on the map to notify the security personnel that something happens in this region.

For details about adding an alarm group, refer to ***Add Alarm Group*** .

People Analysis Group

People analysis group is used to counting the number of people. It is separated into two types of groups:

Entry & Exit Counting Group

In access control, the entry and exit counting group is used to group the doors of certain region. 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.

For details about adding an entry & exit counting group, refer to ***Add Entry and Exit Counting Group*** .

People Counting Group

The people counting group is used to group the doors and people counting cameras of certain region. 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.

Heat Analysis Group

The heat analysis group is used to group the resources (such as doors, fisheye cameras, people counting cameras) in certain region. By grouping these resources, you can know the dwell time of the people stayed in this region, how many persons stayed in this region, and average dwell time of each people.

Pathway Analysis Group

Pathway analysis is mainly used to analyze the people counting on the pathways in the shopping malls. With the help of fisheye cameras, the system can collect the consumers data (for example,where the customers walk mostly) and translate that data onto a dashboard for mall managers. After setting the fisheye camera's pathways and their directions, the system calculates the people dwell time at each pathway and number of people walking by.

Person Feature Analysis Group

Person feature analysis is a group of cameras which supports facial recognition and feature analysis (such as gender and age group). You can group the cameras in one region into one group. After that, when generating a report, you can view the features of the persons appeared in this region, based on the data detected by the cameras in the group.

Multi-Door Interlocking Group

In access control, 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 be a problem. One group is composed of at least two doors and only one door can be opened simultaneously.

For details about adding a multi-door interlocking group, refer to ***Configure Multi-Door Interlocking*** .

Anti-Passback Group

In access control, anti-passback is designed to minimizes the misuse or fraudulent use of access credentials such as passing back card to an unauthorized person, or tailed access. It establishes a specific sequence in which cards must be used in order to grant access.

For details about adding an anti-passback group, refer to ***Configure Anti-Passback Rules*** .

Emergency Operation Group

In access control, 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 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

You can group the security control device's alarm inputs into security control partitions according to the zones on the device. You can also 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 details about adding a security control partition, refer to ***Link Alarm Inputs to Security Control Partition*** .

7.5.1 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. Click **Logical View** on the home page.

2. Choose one of the following methods to enter the area's resource group page.
   - Select one area and click ✎ to enter the editing area page.

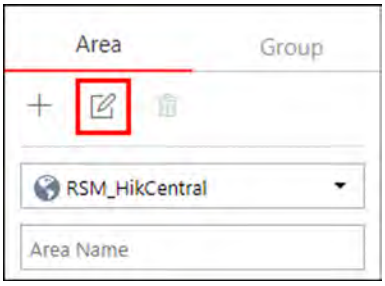


Figure 7-14 Enter Area Editing Page

   - Select **Group** tab on the left to display all the resource groups of different areas.

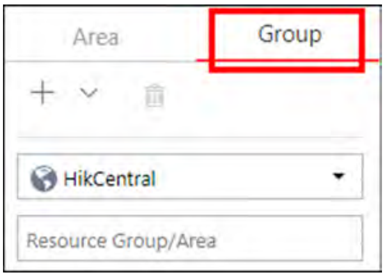
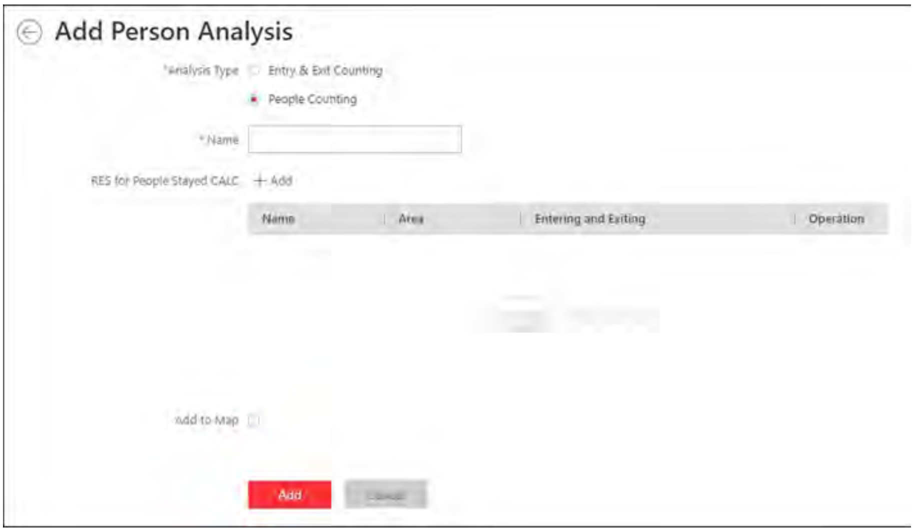


Figure 7-15 Enter Resource Group Page

3. In the People Analysis field, click **Add** to add a people analysis group.
4. In the Add Person Analysis page, select **People Counting** as the analysis type.



*Analysis Type ○ Entry & Exit Counting
● People Counting

*Name

RES for People Stayed CALC

Name	Area	Entering and Exiting	Operation

Figure 7-16 Add People Counting Group

5. Create a name for the group.
6. 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:** You can 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) Check **Add to Map**.

      The region as well as the doors and cameras in the group will be added to the map of the area on the right.
   2) Drag to draw the region according to the actual needs.
   3) Drag the icons of the doors and cameras to set the their locations on the map.
   4) Right click to finish.

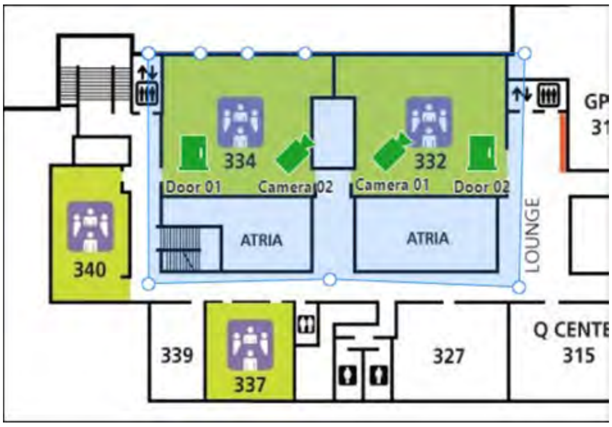


Figure 7-17 Draw People Counting Group on Map

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 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.

9. Click **Add**.

   The people counting group is added in the table and you can view the resources in the group.

7.5.2 Add Heat Analysis Group

The heat analysis group is used to group the resources (such as doors, fisheye cameras, people counting cameras) in certain region. By grouping these resources, you can know the dwell time of the people stayed in this region, how many persons stayed in this region, and average dwell time of each people. This function is mainly used to calculate and show the popularity of each stores in one shopping mall.

Steps

1. Click **Logical View** on the home page.
2. Choose one of the following methods to enter the area's resource group page.
   - Select one area and click to enter the editing area page.

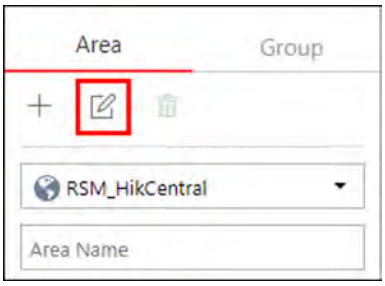


Figure 7-18 Enter Area Editing Page

   - Select **Group** tab on the left to display all the resource groups of different areas.

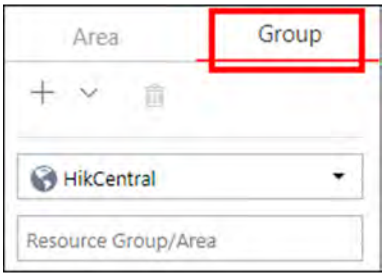


Figure 7-19 Enter Resource Group Page

3. In the Heat Analysis field, click **Add** to add a heat analysis group.

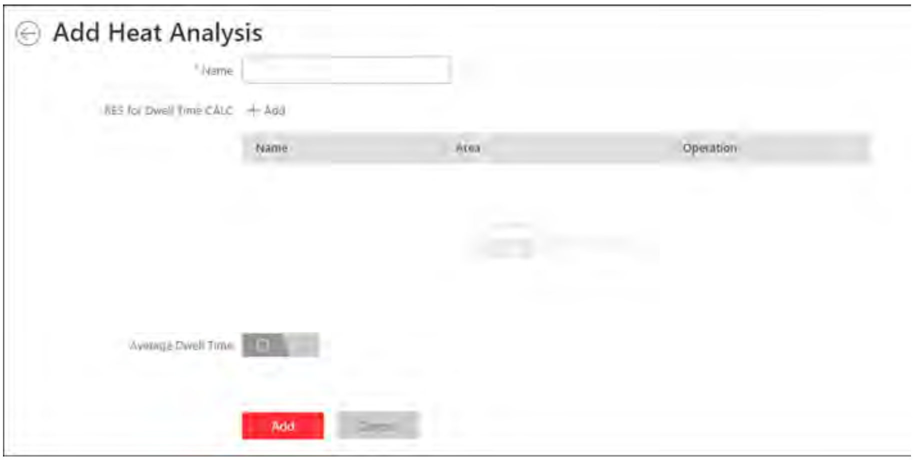


Figure 7-20 Add Heat Analysis Group

4. Create a name for the group.

5. In the **Resource for Dwell Time Calculation** field, click **Add** to select the cameras for calculating the dwell time of the people stayed in this region.
6. **Optional:** To calculate the average dwell time of each people, you need to add resources (including doors and cameras) to the group to calculate the number of people stayed in this region.

   Note

   Average Dwell Time = Total Dwell Time/Number of People in This Region

   1) Set the switch **Average Dwell Time** to on.
   2) In the **Resource for People Stayed Calculation** field, click **Add** to select the doors and camera to the group for calculating the number of people stayed in this region.
   3) 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 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.
7. Click **Add**.

   The heat analysis group is added in the table and you can view the resources in the group.

7.5.3 Add Pathway Analysis Group

Pathway analysis is mainly used to analyze the people counting on the pathways in the shopping malls. With the help of fisheye cameras, the system can collect the consumers data (for example,where the customers walk mostly) and translate that data onto a dashboard for mall managers. This helps managers analyze which areas/shops of the mall best catch a shopper's attention and which are overlooked. After setting the fisheye camera's pathways and their directions, the system calculates the people dwell time at each pathway and number of people walking by, thus helps them make decisions.

Steps

Note

This function is only supported by the second generation of fisheye cameras. You should have configured intersection analysis rule for the fisheye camera. If not, click **Configuration** to set that on the remote configuration page of the device.

1. Click **Logical View** on the home page.
2. Choose one of the following methods to enter the area's resource group page.
   - Select one area and click ✎ to enter the editing area page.

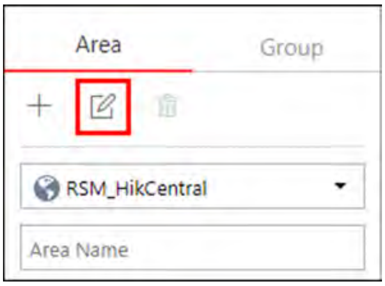


Figure 7-21 Enter Area Editing Page

   - Select **Group** tab on the left to display all the resource groups of different areas.

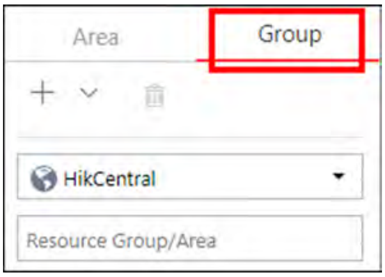


Figure 7-22 Enter Resource Group Page

3. In the Pathway Analysis field, click **Add** to add a pathway analysis group.

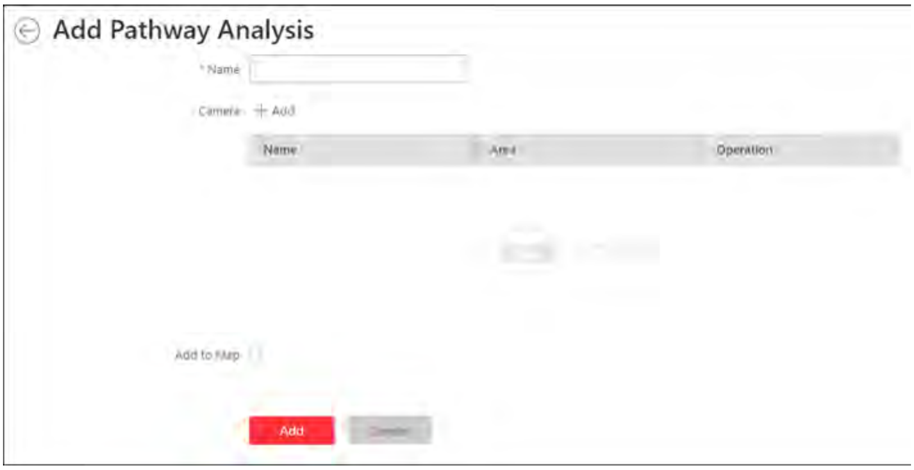


Figure 7-23 Add Pathway Analysis Group

4. Create a name for the group.
5. Click **Add** to select the fisheye cameras for calculating the number of people on different directions in specific pathway.
6. **Optional:** You can locate the pathway analysis group on the map by setting the locations of the fisheye cameras in the group and setting the directions for camera's exits.

Note

To define the camera's exits, refer to the user manual of the camera.

1) Check **Add to Map**.

   The fisheye cameras in the group will be added to the map of the area on the right.
2) Drag the icons of the cameras to set the their locations on the map.
3) Click an exit of the fisheye camera as starting point and then draw a line, indicating the direction of the pathway.
4) Enter the pathway name and select an exit for this pathway.
5) Click **Save** to save the pathway.
6) Perform the above sub-steps to draw other pathways.

   Note

   You can also draw a line to link the exits of two fisheye cameras if there are two cameras in the pathway.

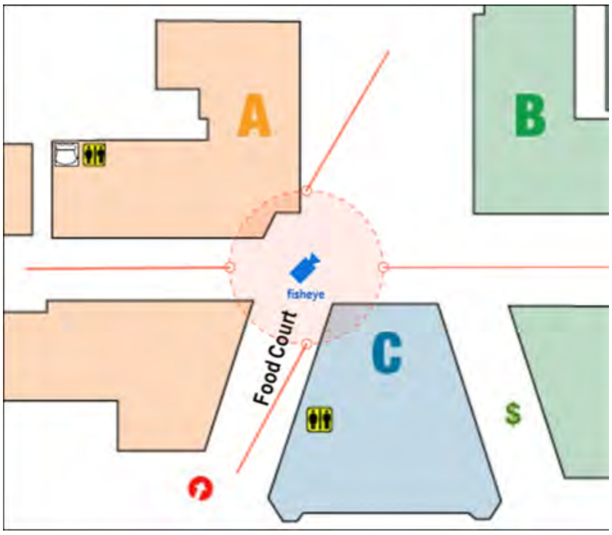


Figure 7-24 Add Pathway Analysis Group

7) **Optional:** Click the camera icon and select **Edit Direction Area** to set radius, view angle and direction.

After adding the pathway analysis group on the map, you can view the real-time number of people walking by in the Monitoring module on the Control Client.

7. Click **Add**.

The pathway analysis group is added in the table and you can view the cameras in the group.

7.5.4 Add Person Feature Analysis Group

Person feature analysis is a group of cameras which support facial recognition and feature analysis (such as gender and age group). You can group the cameras in one region into one group. After that, when generating a report, you can view the features of the persons appeared in this region, based on the data detected by the cameras in the group. For example, if there are five cameras which support facial recognition mounted in the store, the store manager can add these five cameras into one group. Then you can view features of the customers who entering the store in the Intelligent Analysis module.

Steps

1. Click **Logical View** on the home page.
2. Choose one of the following methods to enter the area's resource group page.
   - Select one area and click ✎ to enter the editing area page.

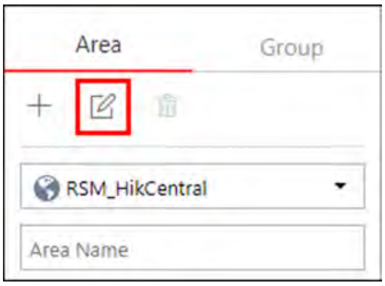


Figure 7-25 Enter Area Editing Page

   - Select **Group** tab on the left to display all the resource groups of different areas.

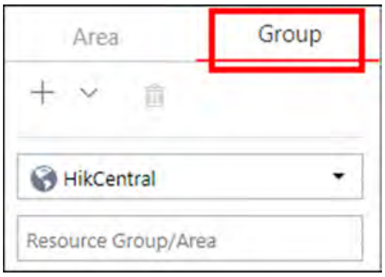


Figure 7-26 Enter Resource Group Page

3. In the Person Feature Analysis field, click **Add** to add a feature analysis group.

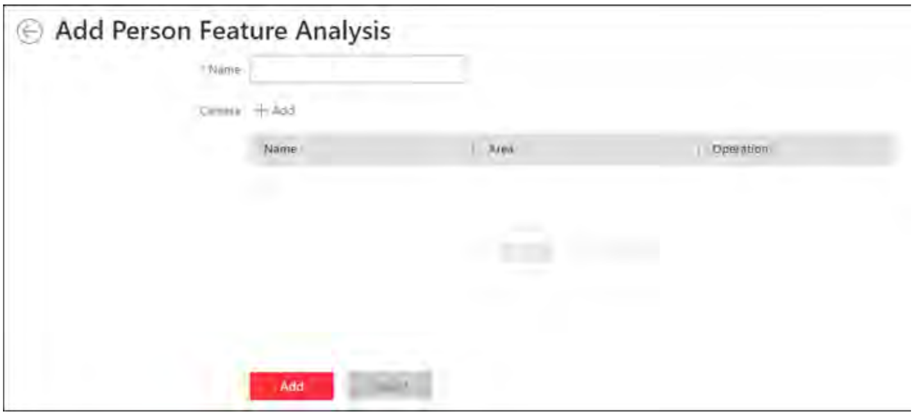


Figure 7-27 Add Person Feature Analysis Group

4. Create a name for the group.
5. In the camera field, click **Add** to select the cameras for analyzing the detected persons' age and gender.
6. Click **Add**.

   The feature group is added in the table and you can view the cameras in the group.

Chapter 8 Configure Recording

Recording settings are for defining when and how the recording starts with the pre-defined parameters. You can also configure the storage settings for storing imported pictures and uploaded pictures.

HikCentral Professional provides four storage locations (storing on encoding devices, Hybrid Storage Area Network, Cloud Storage Server, or pStor) for storing the recorded video files of the cameras.

Encoding Device

The encoding devices, including the DVRs, NVRs, and network cameras, should provide storage devices such as the HDDs, Net HDDs, and SD/SDHC cards for video files. The newly installed storage devices need to be formatted. Go to the remote configuration page of the device (**Physical View → Configuration**), click **Storage → General** , select the HDD, Net HDD or SD/ SDHC card, and click **Format** to initialize the selected storage device.

Hybrid Storage Area Network

Store the video files in the added Hybrid Storage Area Network. For details about adding Hybrid Storage Area Network, refer to ***Add Hybrid Storage Area Network*** .

Cloud Storage Server

Store the video files in the added Cloud Storage Server. For details about adding Cloud Storage Server, refer to ***Add Cloud Storage Server*** .

pStor

Store the video files in the added pStor, which is the storage access service used for managing local HDDs and logical disks. For details about adding pStor, refer to ***Add pStor*** .

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*** .

8.1 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 page.
   1) Click **Logical View → Cameras** to enter the area management page.
   2) Select an area to show its cameras.

      Note

      For Central System with Remote Site Management module, you can select the current site (marked with 🌐 icon) from the drop-down site list to show its cameras.
   3) Select a camera and click the Name field to enter the Edit Camera page.
2. Set the **Main Storage** switch to on.
3. Select the storage location for storing the recorded video file.

   Note

   If you select **Hybrid Storage Area Network**, **Cloud Storage Server**, **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.

     Note

     If you choose **Encoding Device** as the storage location, you needn't select the storage type, but configure the following parameters as real-time storage settings by default.

     Recording Schedule Template

     Set the template which defines when to record the camera's video.

     All-Day Time-Based Template

     Record the video for all-day continuously.

     All-Day Event-Based Template

     Record the video when alarm occurs.

     Add New

     Set the customized template. For details about setting customized template, refer to ***Configure Recording Schedule Template*** .

     View

     View the template details.

     Note

     The event-based recording schedule can not be configured for the **Cloud Storage Server**, and the command-based recording schedule can not be configured for the **Cloud Storage Server** and **pStor**.

Stream Type

Select the stream type as main stream, sub-stream or dual-stream.

Note

For storing on Hybrid Storage Area Network, Cloud Storage Server, 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.

- 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 in

Specify the time period to copy the recorded video files to the specified storage location during the period.

Recording for Copy-Back

Select the recorded video file type to backup.

5. **Optional:** Set the **Auxiliary Storage** switch to ON and configure another storage location for the video files.

Note

- If Cloud Storage Server, Hybrid Storage Area Network, pStor, or pStor Cluster Service is set as the auxiliary storage location, you can select **Real-Time Storage** to store recorded vide 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**.

8.2 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. Enter the recording setting page.
   1) Click **Logical View → Cameras** to enter the area management page.
   2) Select the added Remote Site form the drop-down list.

   Note

   The icon 🌐 indicates that the site is Remote Site.

   3) Select an area to show its cameras.
   4) Select a camera and click the **Name** field to enter the Edit Camera page.
   5) In the Recording Settings area, set **Storage in Central System** switch to ON to show the recording setting area.
2. 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.

3. Select the storage type and configure the required parameters.
   - Select **Real-Time Storage** as the storage type to store the recorded video files in the specified storage location at the real time.

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.

4. Click **Save**.

8.3 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 free space for picture storage.

Steps

Note

You can configure the storage only when the current Web Client is running on SYS server.

1. Click **System → Storage → Storage on SYS Server** to enter the storage on SYS server page.

   The disks of the SYS server are displayed with the free space and total capacity.
2. Select the disk to store the imported pictures.
3. **Optional:** Set the **Restrict Quota for Pictures** switch to on to allocate the quota for storing the pictures.
4. Click **Save**.

8.4 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) Click **Logical View → Cameras** to enter the area management page.
   2) Select an area to show its cameras.

   Note

   For Central System with Remote Site Management module, you can select the current site (marked with 🌐 icon) from the drop-down site list to show its cameras.

   3) Select a camera and click the Name field to enter the Edit Camera page.
2. Set the **Picture Storage** switch to on to enable the picture storage for the camera.
3. Select the storage location from the drop-down list.

Note

- If you select 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.
- You cannot configure the storage location for the captured undercarriage pictures, which are stored on the UVSS device.

4. Click **Save** to save the uploaded pictures to the specified location.

8.5 Configure Recording Schedule Template

Recording schedule is time arrangement for video recording. You can configure the recording schedules to record video in a certain period. Two default recording schedules are available: All-day Time-based Template and All-day Event-based Template. All-day Time-based Template can be used for recording videos for all day continuously, and All-day Event-based Template is for recording videos when alarm is triggered. You can also customize the recording schedule.

Perform this task when you need to customize the schedule to record the video files.

Steps

1. Click **System** on the home page and enter **Schedule → Recording Schedule Template** page.

2. Click **Add** to enter the adding recording schedule page.

Note

Up to 32 templates can be added.

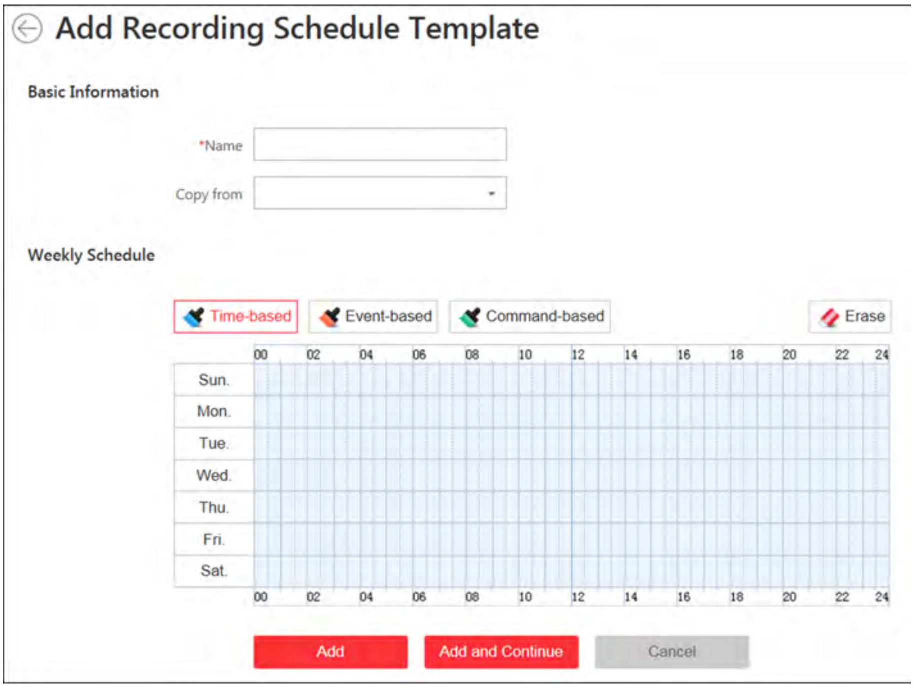


Figure 8-1 Adding Recording Schedule Template Page

3. Set the required information.

   Name

   Set a name for the template.

   Copy from

   Optionally, you can select to copy the settings from other defined templates.

4. Select a recording type and drag on the time bar to draw a time period.

   Note

   By default, the Time-based is selected.

   Time-based

   Continuous recording according to the time you arranged. The schedule time bar is marked with blue.

   Event-based

   The recording triggered by the alarm (e.g., alarm input alarm or motion detection alarm). The schedule time bar is marked with orange.

   Command-based

   The recording triggered by the ATM command. The schedule time bar is marked with green.

   Note

   Up to 8 time periods can be set for each day in the recording schedule.

5. **Optional:** Click **Erase** and click on the time bar to clear the drawn time period.
6. Finish adding the template.
   - Click **Add** to add the template and back to the recording schedule template list page.
   - Click **Add and Continue** to save the settings and continue to add other template.
7. **Optional:** Perform the following operations on the recording schedule template list page.

   View Template Details
   Click the template to check the detailed settings.

   Edit Template
   Click ✎ in the Operation column to edit template details (except the template(s) in use).

   Delete Template
   Click × in the Operation column to delete the template.

   Delete All Templates
   Click **Delete All** to delete all the schedule templates (except the default templates and the template(s) in use).

Chapter 9 Configure Event and Alarm

You can set the linkage actions for the detected events and alarms. The detailed information of the events and alarms can be received and checked via the Control Client and the Mobile Client.

Event

Events can be divided into:

System-Monitored Event

The signal that resource (e.g., camera, device, server) sends when something occurs. System can trigger linkage actions (such as recording, capturing, sending email, etc.) to record the received event for checking.

Generic Event

The signal that resource (e.g., other software, device) sends when something occurs, and can be received in the form of TCP or UDP data packages, which the system can analyze, and generate events if they match configured expression.

User-Defined Event

The user-defined event can be used to:

- The user can trigger a user-defined event manually in Monitoring and Alarm Center module on the Control Client when viewing the video or checking the alarm information.
- A user-defined event can trigger an alarm if configured.
- An alarm will be armed or disarmed when the user-defined event is triggered.
- An alarm can trigger a user-defined event as alarm actions.

Alarm

Alarm is used to notify security personnel of the particular situation which helps handle the situation promptly. An alarm can trigger a series of linkage actions (e.g., popping up window) for notification and alarm handling.

Linkage Actions

You can set linkage actions for both events and alarms.

- An event's linkage actions are used to record the event details (such as recording and capturing) and trigger basic actions (such as linking access point to lock or unlock, triggering alarm output, sending email, etc.).
- An alarm's linkage actions are used to record the alarm details and provide the recipients multiple ways to view alarm information for alarm acknowledgment and handling, such as popping up alarm window, displaying on smart wall, audible warning, etc.

9.1 About System-Related Event

System-monitored event is the signal that resource (e.g., device, camera, server) sends when something occurs. System can receive and record event for checking, and can also trigger a series of linkage actions for notification. The event can also trigger an alarm for further notification and linkage actions (such as alarm recipients, pop-up window on the Control Client, displaying on the Smart Wall, etc.). You can check the event related video and captured pictures via the Control Client if you set the recording and capturing as event linkage.

The rule of a system-monitored 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.

9.1.1 Supported System-Related Events

Currently, the system supports system-monitored events for the following types of resources:

Camera

The video exception or the events detected in the monitoring area of the camera, such as motion detection, video loss, line crossing, and so on.

Door

The access control event triggered at the doors (doors of access control devices and video intercom devices), such as access event, door status event, etc.

Elevator

The elevator control event triggered in the elevators, such as card swiping event, elevator status event, etc.

Radar

The radar arming event and the event detected by the radars, such as auto-arming event, line crossing event, etc.

Alarm Input

The event triggered by the alarm input of the resources in the system, such as a smoke detector.

ANPR

The license plate matched event and mismatched event detected by the ANPR camera or UVSS.

Person

The face matched event and mismatched event detected by the facial recognition camera.

UVSS

The event triggered by the UVSS, including getting online or offline.

Parking Lot

The event triggered by the resources in the parking lot, such as vehicle matched or mismatched which is detected at the entrance & exit.

Remote Site

The event triggered by the added Remote Site, including site getting offline.

Device Exception

The event triggered by the exception of encoding device, access control device, video intercom device, elevator control device, security control panel, dock station, and decoding device.

Resource Group

The resource group events, including person amount more/less than the threshold and its pre-alarm triggered in the people analysis group.

Server Exception

The events triggered by Recording Server, Streaming Server, DeepinMind Server, Security Audit Server, or HikCentral Professional Server.

User

The event triggered by system users, including user login and logout.

Generic Event

The event triggered by the generic event added in the system.

User-Defined Event

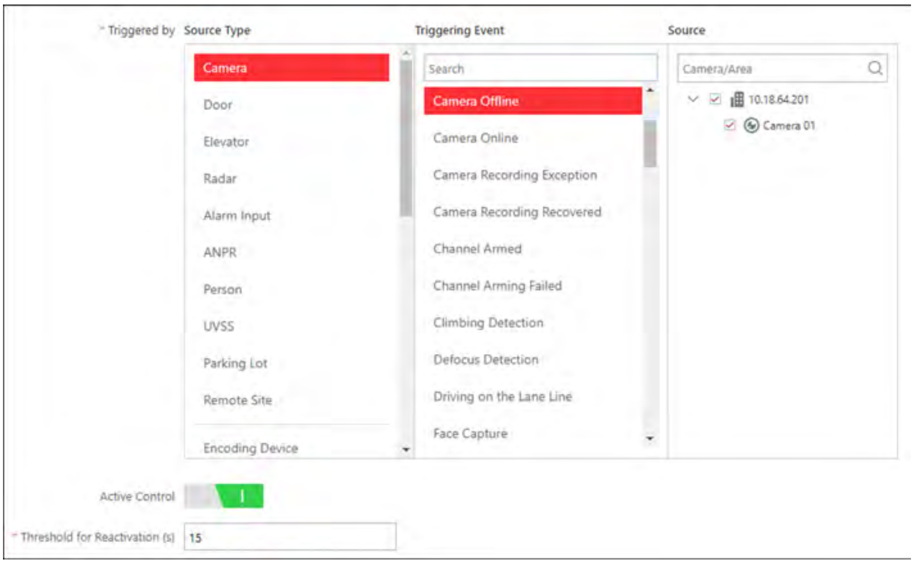
The event triggered by the user-defined event added in the system.

9.1.2 Add System-Monitored Event

Enter **Event & Alarm → System-Monitored Event** and click **Add** to add a system-monitored event.

Event Source and Triggering Event

The fields in the following image indicate two elements in the rule: "event source" and "triggering event".



* Threshold for Reactivation (s) 15

Figure 9-1 Triggering Event Occurred on Event Source

Source Type

Source

These two fields refer to **"event source"** in the rule, defining the specific entity (such as cameras, devices, servers, etc.) which can trigger this event.

Triggering Event

This field refers to **"triggering event"** in the rule. The specific event type detected on the event source will trigger a system-monitored event.

Threshold

If the source type you selected is **Resource Group**, 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 analysis group. For these two events, you need to set the threshold which determines whether the selected people analysis groups will trigger an event 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 analysis group is more than 100 or less than 10, an event will be triggered to notify the security personnel.

Active Control

Active Control is used to avoid the same event occurs frequently in a short time, which may aggravate the burden of the event center. You need to set the **Threshold for Reactivation**.

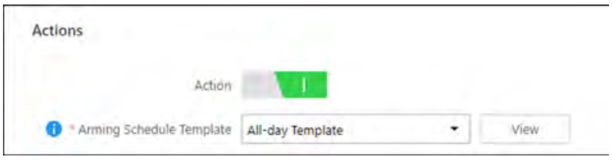
For example, if you set the **Threshold for Reactivation** as ***30 s***, the events of the same type occurred on the same camera within 30 s will be regarded as one event in the system.

Note

The **Threshold for Reactivation** is 15 s by default. You can set it from 15 s to 1800 s.

When

The field in the following image indicates one element in the rule: "when". It defines during specified time period, the linkage actions can be triggered.



* Arming Schedule Template: All-day Template

Figure 9-2 When to Trigger Actions

Arming Schedule Template

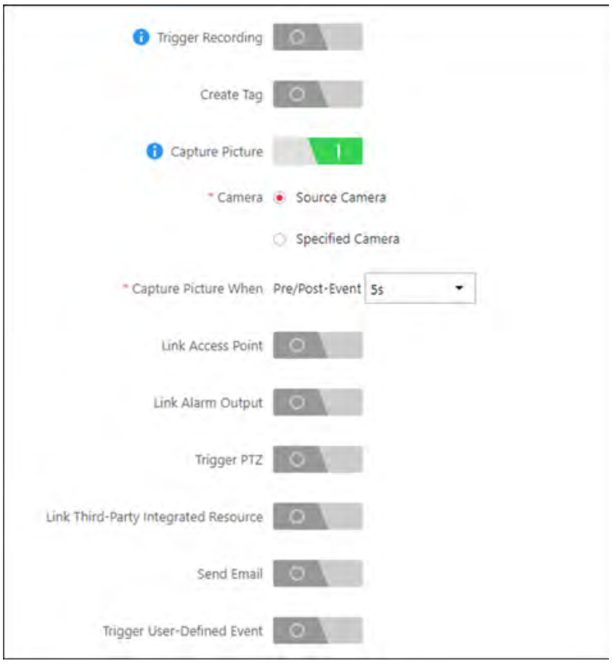
The event source is armed during the arming duration in the arming schedule and the triggering event occurred on the source during the arming duration will trigger the configured linkage actions.

Note

For setting customized template, refer to ***Configure Arming Schedule Template*** .

What to Do

The fields in the following image indicate one element in the rule: **"what to do"**. It defines what actions the system will take to record the event details and trigger basic actions.



Trigger Recording

Create Tag

Capture Picture

* Camera ● Source Camera

○ Specified Camera

* Capture Picture When Pre/Post-Event 5s

Link Access Point

Link Alarm Output

Trigger PTZ

Link Third-Party Integrated Resource

Send Email

Trigger User-Defined Event

Figure 9-3 What to Do after Event Occurs

Compared with alarm, the system monitored event's linkage actions can be 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.).

Trigger Recording

Select the cameras to record video when the event occurs and set the storage location for storing the video footage. You can play back the recorded video footage when checking events in the Alarm & Event Search of the Control Client.

- If the event source is a camera, you can set to trigger the source camera itself for recording by selecting **Source Camera**.
- To trigger other cameras, select **Specified Camera** and click **Add** to add other cameras. For example, when the camera outside the door detects suspicious person entering, you can configure to trigger the cameras inside the room to record video.

View Pre-Event Video: If the camera has recorded video before the event, you can view the video recorded from periods preceding the event. Specify the number of seconds which you want to view the recorded video for before the event starts. For example, when someone opens a door, you can view the recorded video to see what happens right before the door opened.

Post-record: Record video from periods following detected event. Specify the number of seconds which you want to record video for after the event stops.

Lock Video Files for: Set the days for protecting the video footage from being overwritten.

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 until and 10 seconds after the event. The tagged video can be searched and checked via the Control Client.

Add the description to the tagged video as needed.

Capture Picture

Select one camera to capture pictures during the event, and you can view the captured pictures when checking event in the Alarm & Event Search of the Control Client.

Note

Only one camera can be set for capturing pictures.

- If the event 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 event. After you set the number of seconds for pre/post-event, the camera will capture one picture at three time points respectively: at the configured seconds before the event starts, at the configured seconds after the event ends, and at the middle of the event (as shown in the picture below).

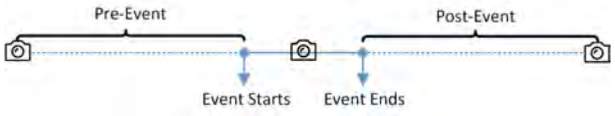


Figure 9-4 Capture Pictures

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).

Link Access Point

You can enable this function to trigger the access points (including doors and floors).

For doors, the doors can be locked, unlocked, remained locked, or remained unlocked when the event occurs.

For floors, the elevators can access the floors freely, with credentials, temporarily, or access forbidden.

For example, you can set to trigger all the doors remaining locked and all the floors access forbidden when the detecting a suspicious person entering.

- **All Access Points:** When the event occurs, the system will trigger all the doors and floors to take certain action.
- **Specified Access Point:** Click **Add** to select specified access points or emergency operation groups as the linkage targets. When the event occurs, the system will trigger these doors, floors, or doors/floors in the emergency operation groups to take certain action.

Link Alarm Output

Select the alarm output (if available) and the external device connected can be activated when the event occurs.

Note

Up to 64 alarm outputs can be selected as event linkage.

Close Alarm Output: The added alarm output(s) can be closed manually, or you can set the number of seconds in which the alarm output(s) will be closed automatically.

Trigger PTZ

Call the preset, patrol or pattern of the selected cameras when the event occurs.

Note

Up to 64 PTZ linkages can be selected as event linkage.

Link Third-Party Integrated Resource

Click **Add** to select the resources integrated from third-party platform and set the control about detailed operations that will happen when the event occurs.

Send Email

Select an email template to send the event information according to the defined email settings.

You can select **Add New** to create a new email template.

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 how many people are still in the building, their names and profiles, phone numbers, and locations of last access.

Trigger User-Defined Event

Trigger user-defined events when the system-monitored event is triggered.

You can select the pre-defined user-defined events in the event list.

You can also click **Add New** below to set a new user-defined events.

Note

- Up to 16 user-defined events can be selected as event linkage.
- For setting the user-defined event, refer to ***Configure User-Defined Event*** .

Other Operations After Adding an Event

After adding a system-monitored event, you can perform the following operations if needed.

Table 9-1 Other Operation

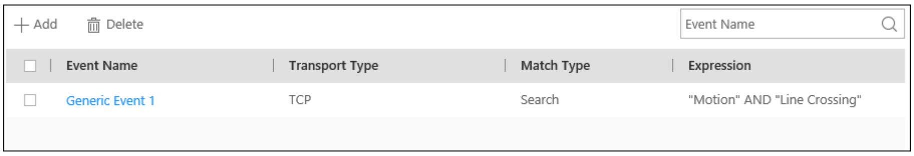
Operation	Description
Trigger Event as Alarm	Click in the Operation column of system-monitored event settings page to set the alarm properties, recipients, actions, and other parameters. **Note** For details, refer to .
Test Event	Click ◎ in the Operation column of system-monitored event settings page to trigger the event manually, and you can check whether the linkage actions take effect.
Delete Event	Select the event(s) and click **Delete** to delete the selected event(s).
Manage Invalid Event	If ⊗ appears near the event name, it means the event is not supported by the device and it is invalid. You should hover the cursor over the ⊗ and click **Delete** on the tooltip to delete the event.
Delete All Invalid Events	Click **Delete All Invalid Items** to delete all the invalid events in a batch.
Filter Event	Click ▽ to expand the filter conditions. Set the conditions and click **Filter** to filter the events according to the conditions.

9.2 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

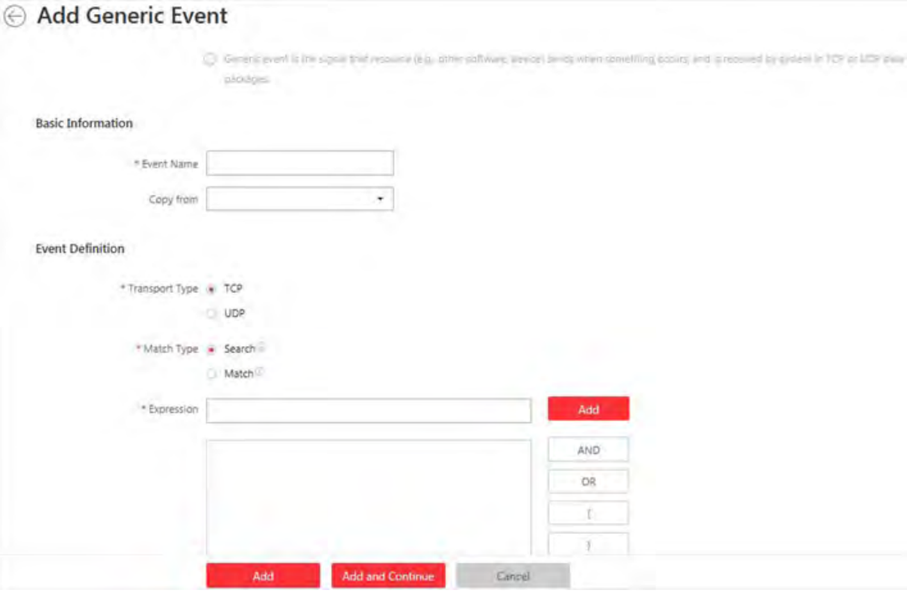
1. Click **Event & Alarm → Generic Event** to enter the generic event settings page.



☐	Event Name	Transport Type	Match Type	Expression
☐	Generic Event 1	TCP	Search	"Motion" AND "Line Crossing"

Figure 9-5 Generic Event Settings Page

2. Click **Add** to enter the Add Generic Event page.



Generic event is the signal that resource (e.g. other software, device) sends when something occurs, and is received by system in TCP or UDP data packages.

Basic Information

* Event Name

Copy from

Event Definition

* Transport Type ● TCP ○ UDP

* Match Type ● Search ○ Match

* Expression

Figure 9-6 Add Generic Event Page

3. Set a name for the event in the Event Name field.
4. **Optional:** Copy the settings from other defined generic events in the **Copy from** field.
5. Select **TCP** or **UDP** to analyze the packages using TCP or UDP protocol.
6. Select the matched type which indicating how particular your system should be when analyzing the received data packages:

   Search

   The received package must contain the text defined in the Expression field.

For example, if you have defined that the received packages should contain "Motion" and "Line Crossing", the alarm will be triggered when the received packages contain "Motion", "Intrusion" and "Line Crossing".

Match

The received package must exactly contain the text defined in the Expression field, and nothing else.

7. Define the event rule for analyzing the received package in the Expression field.

1) Enter the term which should be contained in the expression in the text field.
2) Click **Add** to add it to the expression.
3) Click parenthesis or operator button to add it to the expression.
4) To add a term, parenthesis or operator to the expression, position the cursor inside the expression field in order to determine where a new item (term, parenthesis or the operator) should be included, and click Add or one of the parenthesis or operator buttons.
5) To remove an item from the expression, position the cursor inside the field in order to determine where an item should be removed, and click × . The item immediately to the left of the cursor will be removed.

The parenthesis or operator buttons are described in the following:

AND

You specify that the terms on both sides of the AND operator must be included.

For example, if you define the rule as "Motion" AND "Line Crossing" AND "Intrusion", the term Motion, and Line Crossing as well as the term Intrusion must be all contained in the received package for the conditions to be met.

Note

In generally, the more terms you combine with AND, the fewer events will be detected.

OR

You specify that any term should be contained.

For example, if you define the rule as "Motion" OR "Line Crossing" OR "Intrusion", any of the terms (Motion, Line Crossing, or Intrusion) must be contained in the received package for the conditions to be met.

Note

In generally, the more terms you combine with OR, the more events will be detected.

(

Add the left parenthesis to the rule. Parentheses can be used to ensure that related terms are processed together as a unit; in other words, they can be used to force a certain processing order in the analysis.

For example, if you define the rule as ("Motion" OR "Line Crossing") AND "Intrusion", the two terms inside the parentheses will be processed first, then the result will be combined with the last part of the rule. In other words, the system will first search any packages containing either of the terms Motion or Line Crossing, then it search the results to look for the packages that contained the term Intrusion.

)

Add the right parenthesis to the rule.

8. Finish adding the event.
- Click **Add** to add the event and back to the event list page.
- Click **Add and Continue** to save the event settings and continue to add event.

9. 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.

Enable Receiving Generic Event
If ⊗ appears near the event name, it means the system has not enabled receiving generic event. You should hover the cursor over the ⊗ and click **Configuration** on the tooltip to enable receiving generic event for the system. For details, refer to ***Enable Receiving Generic Event*** .

Delete Event Settings
Check the event(s) and click **Delete** to delete the selected event settings.

Delete All Event Settings
Check the checkbox in the heading row, and click **Delete** to delete all the event settings.

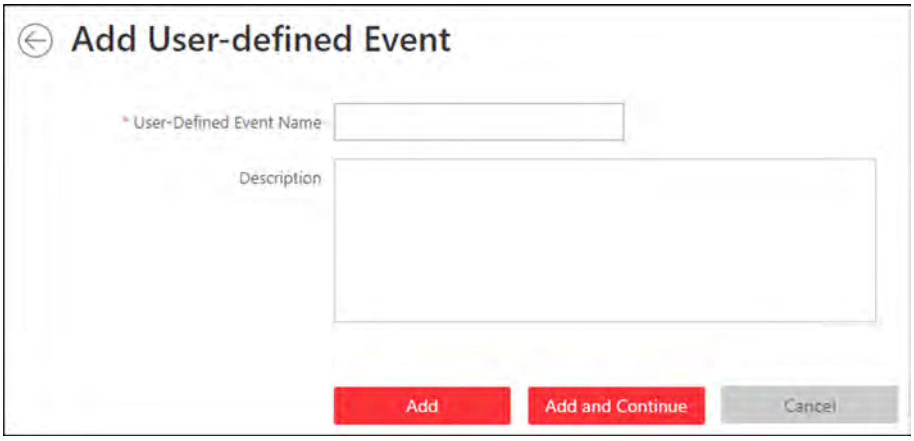
9.3 Configure User-Defined Event

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. Click **Event & Alarm → User-Defined Event** to enter the user-defined event management page.

2. Click **Add** to open the following window.



Add User-defined Event

* User-Defined Event Name

Description

Figure 9-7 Add User-Defined Event

3. Create a name for the event.
4. **Optional:** Enter the description information to describe the event details.
5. Finish adding the event.
   - Click **Add** to add the event and go back to the event list page.
   - Click **Add and Continue** to add the event and continue to add other events.

   With the customized user-defined event, it provides the following functions:

   - The user can trigger a user-defined event manually in Monitoring and Alarm Center module on the Control Client when viewing the video or checking the alarm information.
   - A user-defined event can trigger an alarm if configured.
   - You can define the arming time period by the user-defined event: An alarm's arming schedule will start or end when the user-defined event is triggered.
   - An alarm can trigger a user-defined event as alarm actions.
   - Integrate other third-party systems with 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 .
- For triggering the user-defined event on the Control Client, refer to *User Manual of HikCentral Professional Control Client*.

9.4 About 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.

9.4.1 Define Alarm Priority and Category

The system predefines several alarm priorities and alarm categories for basic needs. You can edit the predefined alarm priority and alarm category, and set customized alarm priority and alarm category according to actual needs.

Perform this task when you need to configure the alarm priority and alarm category.

Alarm Priority

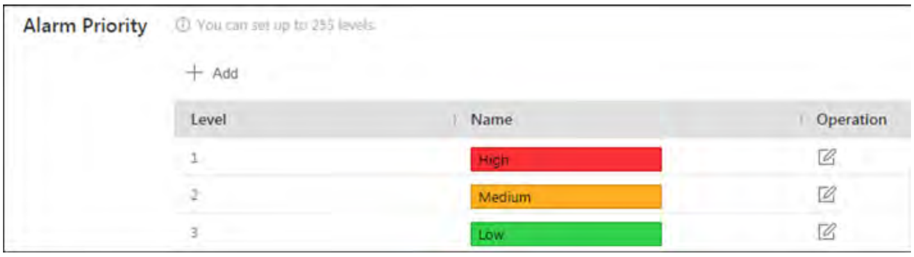
Define the priority for the alarm when add the alarm and filter alarms in the Control Client.

Alarm Category

Alarm category is used when the user acknowledges the alarm in the Control Client and 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.

Steps

1. Click **Event & Alarm → Alarm → Alarm Settings** to enter the alarm settings page.
2. Set the alarm priority according to actual needs. By default, three kinds of alarm priority exist.



Alarm Priority ⓘ You can set up to 255 levels.

+ Add

Level	Name	Operation
1	High	✎
2	Medium	✎
3	Low	✎

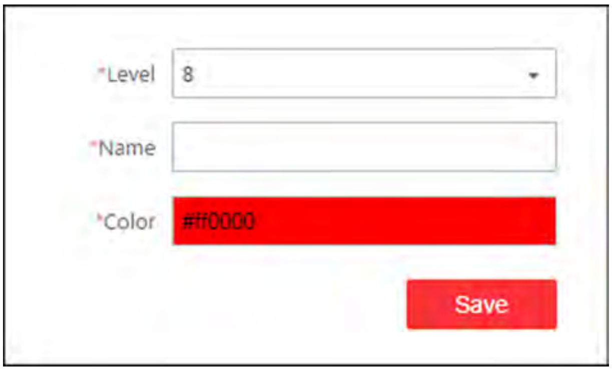
Figure 9-8 Alarm Priority Page

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:

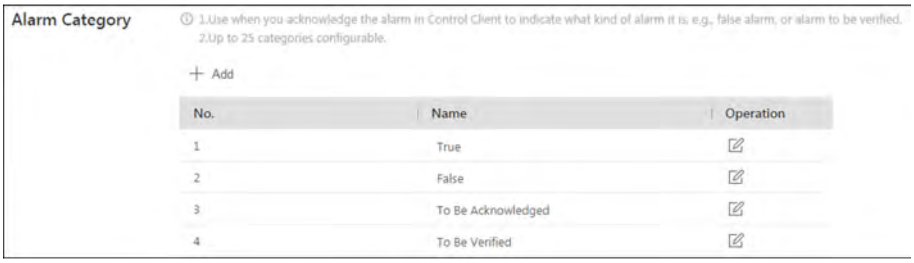
*Color: #ff0000

Figure 9-9 Alarm Priority Settings Window

5) Click **Save** to add the priority.

   The priority will be displayed on the alarm priority list.

3. Set the alarm category according to actual needs. By default, four alarm categories exist.



Alarm Category

1.Use when you acknowledge the alarm in Control Client to indicate what kind of alarm it is, e.g., false alarm, or alarm to be verified.
2.Up to 25 categories configurable.

No.	Name	Operation
1	True	✎
2	False	✎
3	To Be Acknowledged	✎
4	To Be Verified	✎

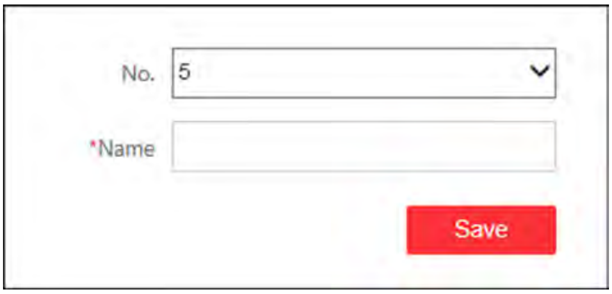
Figure 9-10 Alarm Category Page

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 9-11 Alarm Category Settings Window

4) Click **Save** to add the alarm category.

   The alarm category will be displayed on the alarm category list.

4. Perform the following operation(s) after adding alarm priority and category.

Edit	Click ✎ to edit the alarm priority and category. **Note** You cannot edit the No. of predefined alarm priorities and categories.
Delete	Click × to delete the alarm priority and category. **Note** You cannot delete the predefined alarm priorities and categories.

9.4.2 Supported Alarm

Currently, the system supports alarms for the following types of resources:

Camera

The video exception or the events detected in the monitoring area of the cameras, such as motion detection, video loss, line crossing, etc.

If the system is a Central System with Remote Site Management module, you can also set the alarm for the camera on Remote Site which has configured with alarm, so that you can receive alarms in the Central System when the alarm is triggered on devices added to Remote Sites.

Door

The alarm triggered at the doors (doors of access control devices and video intercom devices), such as access event, door status event, etc.

Elevator

The alarm triggered at the elevators, such as access event, elevator status event, etc.

Radar

The radar arming alarm and the alarm detected by the radars, such as auto-arming alarm, line crossing alarm, etc.

Alarm Input

The alarm triggered by the alarm inputs of the resources managed in the system.

ANPR

The alarm triggered when the license plate detected by the ANPR camera and UVSS matches or mismatches the vehicle information in vehicle list.

Person

The alarm triggered when the person's face detected by the face recognition device matches or mismatches the face picture in the face comparison group.

UVSS

The alarm trigger by the UVSS device, including device getting online and offline.

Remote Site

The alarm triggered by the added Remote Site, including site getting offline.

Note

Remote Site alarm is available for the system with Remote Site Management module (based on the license you purchased).

Device Exception

The alarm triggered by the exception of encoding device, access control device, video intercom device, elevator control device, security control panel, dock station, and decoding device.

Resource Group

The resource group alarms, including person amount more/less than the threshold and its pre-alarm triggered in the people analysis group.

Server Exception

The alarms triggered by Recording Server, Streaming Server, DeepinMind Server, Security Audit Server, or HikCentral Professional Server.

User

The alarm triggered by system users, including user login and logout.

User-Defined Event

The alarm triggered by the configured user-defined event.

Generic Event

The alarm triggered by the configured generic event.

9.4.3 Add Alarm

Enter **Event & Alarm → Alarm** and click **Add** to add an alarm.

Alarm Source and Triggering Event

The fields in the following image indicate two elements in the rule: "alarm source" and "triggering event".

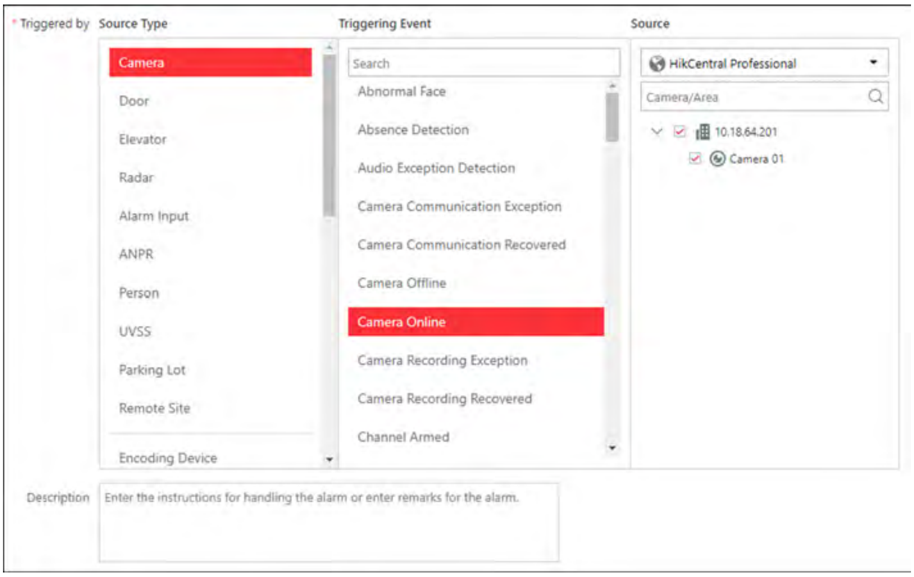


Figure 9-12 Triggering Event Occurred on Alarm Source

Source Type

Source

These two fields refer to **"alarm source"** in the rule, defining the specific entity (such as cameras, devices, servers, etc.) which can trigger this alarm.

Triggering Event

This field refers to **"triggering event"** in the rule. The specific event type detected on the event source will trigger an alarm.

Threshold

If the source type you selected is **Resource Group**, 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 analysis group. For these two alarms, you need to set the threshold which determines whether the selected people analysis 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 analysis group is more than 100 or less than 10, an alarm will be triggered to notify the security personnel.

Active Control

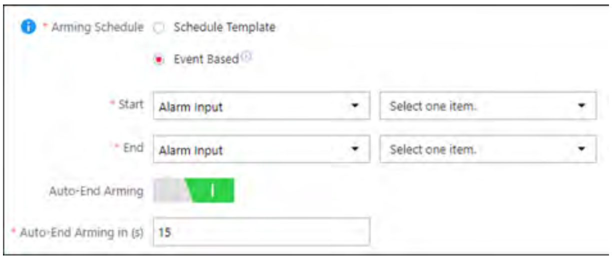
Active Control is used to avoid the same alarm being received frequently in a short time. You need to set the **Threshold for Reactivation**. For example, you have set the Threshold for

Reactivation as ***30 s***, the alarms of the same type occurred on the same camera within 30 s will be regarded as one alarm in the system.

The Threshold for Reactivation is 15 s by default. You can set it from 15 s to 1800 s.

When

The field in the following image indicates one element in the rule: "when". It defines during specified time period, the linkage actions can be triggered.



* Arming Schedule ○ Schedule Template
● Event Based

* Start: Alarm Input / Select one item.

* End: Alarm Input / Select one item.

Auto-End Arming

* Auto-End Arming in (s): 15

Figure 9-13 When Alarm Can be Triggered

Arming Schedule

The alarm source is armed during the arming schedule and the event occurred during the arming schedule will be triggered as an alarm and notify the user. The system provides two types of arming schedule:

- **Schedule Template:** Select an arming schedule template for the alarm to define when the alarm can be triggered. For setting customized template, refer to ***Configure Arming Schedule Template*** .
- **Event Based:** Specify a user-defined event or an alarm input as the start or end event of the arming schedule. When the user defined event or alarm input is triggered, the arming schedule will start or end. You can set the **Auto-End Arming** switch to on and set the specified time to automatically end arming for this alarm even if the end event does not occur.

Note

For example, you have set event A as start event, event B as end event, and set the **Auto-End Arming in** as ***60 s***, when event A occurs at T1, the alarm will be armed from T1 until event B occurs within 60 s (See the following figure Arming Schedule 1), or end arming 60 s later and event B doesn't occur (See the following figure Arming Schedule 2).

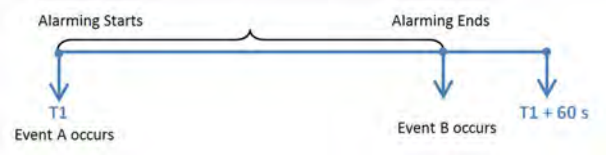


Figure 9-14 Arming Schedule 1

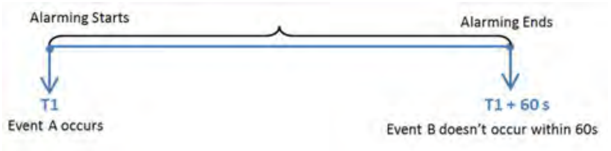


Figure 9-15 Arming Schedule 2

When A occurs at time T1, the alarm will be armed from T1, if A occurs again at time T2 but B doesn't occur, the alarm will be armed from T2 again.

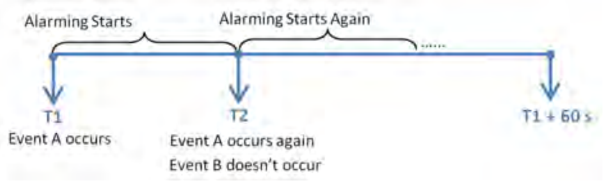
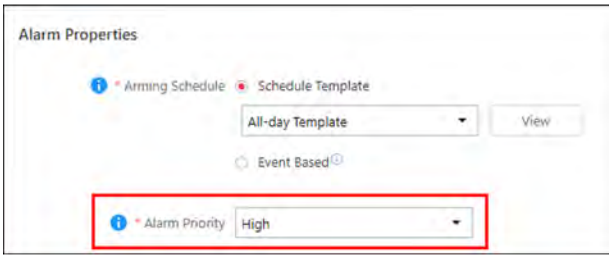


Figure 9-16 Arming Schedule 3

Priority

The field in the following image indicates one element in the rule: "recipient".



Alarm Properties

* Arming Schedule ● Schedule Template

All-day Template View

○ Event Based

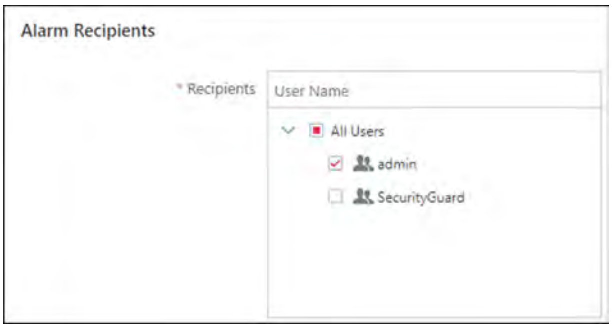
* Alarm Priority High

Figure 9-17 Alarm Priority

It defines the priority for the alarm. Priority can be used for filtering alarms in the Control Client. You can click **Add New** to set alarm priority. For setting alarm priority, refer to .

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.



Alarm Recipients

* Recipients User Name

■ All Users

☑ admin

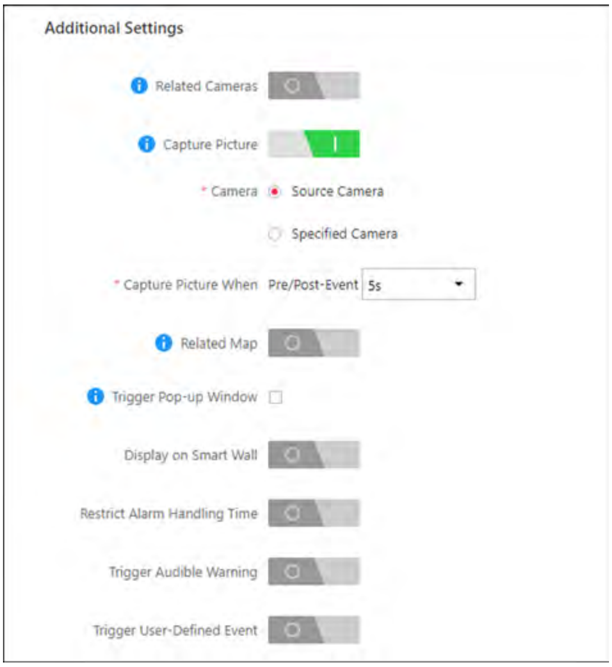
□ SecurityGuard

Figure 9-18 Alarm Recipient

Select the user to send the alarm information to and the user can receive the alarm information when he/she logs in to HikCentral Professional via the Control Client or Mobile Client.

What to Do

The fields in the following image 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.



Additional Settings

Related Cameras: Off

Capture Picture: On

* Camera: ● Source Camera ○ Specified Camera

* Capture Picture When: Pre/Post-Event 5s

Related Map: Off

Trigger Pop-up Window: □

Display on Smart Wall: Off

Restrict Alarm Handling Time: Off

Trigger Audible Warning: Off

Trigger User-Defined Event: Off

Figure 9-19 What to Do after Alarm Occurs

Related Camera

Select the related camera to record the alarm video when the alarm is triggered. You can view the live video and play back these video files in the Alarm Center of the Control Client.

- To relate the source camera itself for recording, select **Source Camera** and select the storage location for storing the video files.
- To relate other cameras, select **Specified Camera** and click **Add** to add other cameras as related cameras. Select the storage location for storing the video files.
- **View Pre-Alarm Video:** You can view the video recorded from periods preceding the alarm. Specify the number of seconds which you want to view the recorded video for before the alarm starts. For example, when someone opens a door, you can view the recorded video to see what happens right before the door opened.
- **Post-record:** Record video from periods following detected alarms. Specify the number of seconds which you want to record video for after the alarm stops.
- **Lock Video Files for:** Set the days for protecting the video file from being overwritten.
- **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).

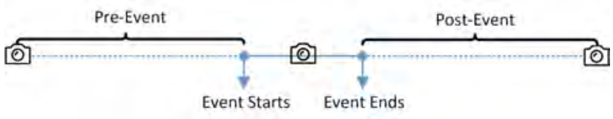


Figure 9-20 Capture Pictures

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).

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 Pop-up Window

Display the alarm window on the Control Client to show the alarm details and all the alarm related cameras' live videos and playback when alarm occurs.

Display on Smart Wall

Display the alarm video of the alarm's related camera or display the specified public view on the smart wall. You can select the added smart wall and select which window to display the alarm.

- **Alarm's Related Cameras:** Display the video of the alarm's related cameras on the smart wall. You can select to display the video on which smart wall and which window and set the alarm video's stream type.
- **Public View:** A view enables you to save the window division and the correspondence between cameras and windows as favorites to quickly access the related cameras later. If you select **Public View**, when the alarm is triggered, the system can display the selected public view on the specified smart wall and users can view the video of the cameras pre-defined in the view.
- **Wall Related to Graphic Card:** Display the alarm video on the wall which adopts graphic card of the PC that running the Control Client to decode video.
- **Wall Related to Decoding Device:** Display the alarm video on the wall which adopts decoding device (namely the wall that related to the decoding device) to decode the video.
- **Smart Wall No.:** Select the No. of smart wall window to display the alarm video.
- **Stream Type:** Select the stream type of the alarm video displaying on the smart wall.
- **Stop Displaying Alarm:** Define when the system will stop displaying the alarm on the smart wall. The system can stop displaying alarm within specified seconds, or replace the original alarm when other alarm with higher alarm priority is triggered.

Restrict Alarm Handling Time

When the alarm is triggered, you need to handle the alarm on the Control Client. Enable this function to trigger user-defined event(s) or alarm output(s) if the alarm is not handled within the configured alarm handling time.

Note

- Up to 16 user-defined events and alarm outputs can be set as the triggered event when handling alarm timed out.
- For configuring the user-defined event, refer to ***Configure User-Defined Event*** .

Trigger Audible Warning

Set the voice text for playing on the PC when alarm is triggered.

Note

You should set voice engine as the alarm sound on System Settings page of Control Client.

Trigger User-Defined Event

Trigger the user-defined event(s) when alarm is triggered.

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*** .

Other Operations After Adding an Alarm

After adding an alarm, you can perform the following operations if needed.

Table 9-2 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.

9.5 Add Alarm Group

The alarm group is used to group the resources in certain region and provides alarm notification when the alarm occurs on the resources in the group. By grouping the resources and locating the group on the map, when an alarm occurs, the region of the group will be highlighted on the map to notify the security personnel that something happens in this region.

Steps

1. Click **Logical View** on the home page.
2. Choose one of the following methods to enter the area's resource group page.
   - Select one area and click ✎ to enter the editing area page.

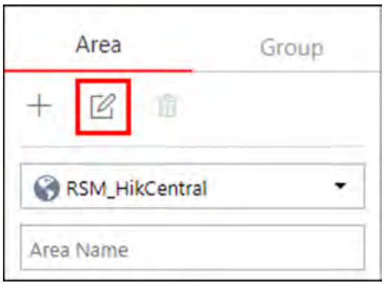


Figure 9-21 Enter Area Editing Page

- Select **Group** tab on the left to display all the resource groups of different areas.

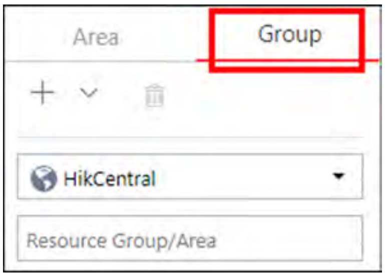
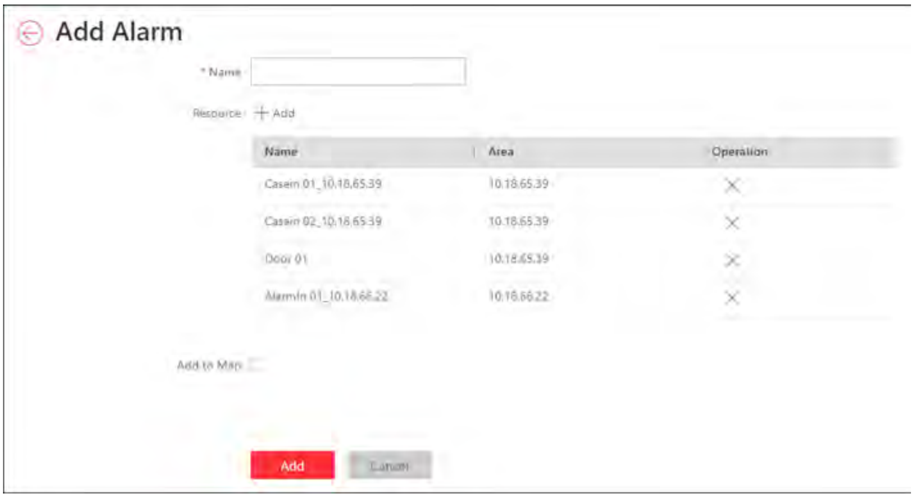


Figure 9-22 Enter Resource Group Page

3. In the Alarm field, click **Add** to add an alarm group.



Add Alarm

* Name

Resource + Add

Name	Area	Operation
Casein 01_10.18.65.39	10.18.65.39	×
Casein 02_10.18.65.39	10.18.65.39	×
Door 01	10.18.65.39	×
Alarmin 01_10.18.66.22	10.18.66.22	×

Add to Map □

Add Cancel

Figure 9-23 Add Alarm Group

4. Create a name for the group.
5. Click **Add** to select the resources for calculating the number of people stayed in this region.
6. **Optional:** You can locate the alarm group on the map by setting the locations of the resources in the group and setting the border of the region for detection.
   1) Check **Add to Map**.

      The region as well as the resources in the group will be added to the map of the area on the right.
   2) Drag to draw the region according to the actual needs.
   3) Drag the icons of the resources to set the their locations on the map.

4) Right click to finish.

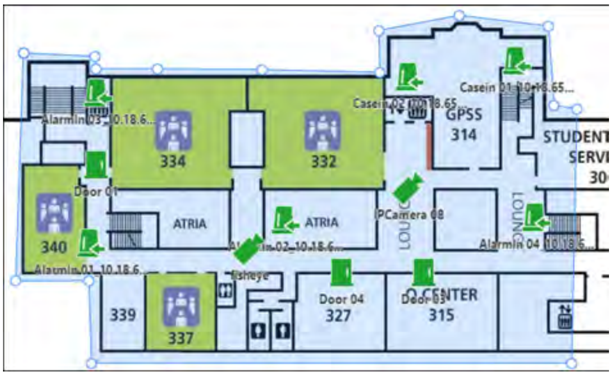


Figure 9-24 Draw Alarm Group on Map

After adding the alarm group on the map, when an alarm is triggered by the resources 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.

7. Click **Add**.

The alarm group is added in the table and you can view the resources in the group.

9.6 Configure Arming Schedule Template

When setting event and alarm, you can select the predefined arming schedule template to define when the event or alarm will be triggered. The system predefines three default arming schedule templates: All-day Template, Weekday Template, and Weekend Template. You can also add a customized template according to actual needs.

Steps

1. Click **System** on the home page.
2. Click **Schedule → Arming Schedule Template** on the left.
3. Click **Add** to enter the adding arming schedule page.

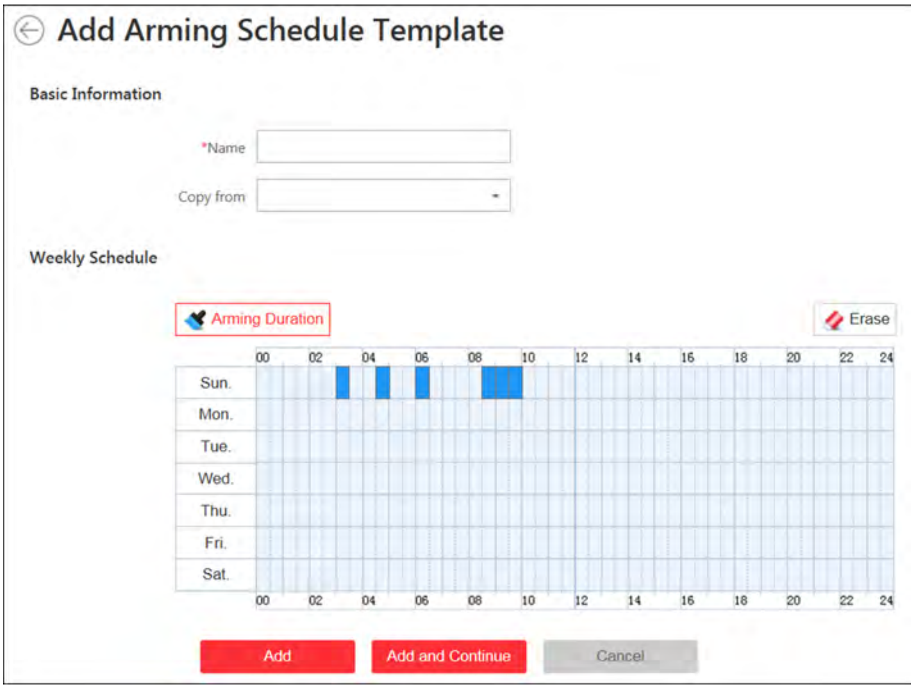


Figure 9-25 Add Arming Schedule Template Page

4. Set the required information.

   Name

   Set a name for the template.

   Copy from

   Optionally, you can select to copy the settings from other defined templates.

5. Click **Arming Duration** and drag on the time bar to set the time periods.

   Note

   Up to 4 time periods can be set for each day.

6. **Optional:** Click **Erase** and click on the drawn time period to clear the corresponding time period.
7. Finish adding the arming schedule template.
   - Click **Add** to add the template and go back to the arming schedule template list page.
   - Click **Add and Continue** to add the template and continue to add other template.

   The arming schedule template will be displayed on the arming schedule template list.
8. **Optional:** Perform the following operations after adding the arming schedule template.

View Template Details	Click the template to view its details.
Edit Template	Click ✎ in the Operation column to edit template details.
Delete Template	Click × in the Operation column to delete the template.

Delete All Templates	Click **Delete All** to delete all the added templates (except the default templates). If the added templates have been used by events or alarms, you will be asked whether or not to replace the schedule.

Chapter 10 Manage Map

Two types of map are available: GIS map and E-map. On the GIS map, you can set and view the current site, Remote Site, and element's geographic location. On the e-map, which is a static map, you can set and view the geographic locations of the installed cameras, alarm inputs, and alarm outputs, etc.

With GIS map, you can see the geographic locations of your surveillance system. This type of map uses a geographic information system to accurately show all the hot spots' (resources (e.g., camera, alarm input) placed on the map are called hot spots) geographic locations in the real world. GIS map lets you view and access cameras at multiple locations around the world in a geographically correct way. If the resources locate in multiple locations (e.g., different cities, different countries), GIS map can give you a single view to show them all and help you quickly go to each location to view video from the cameras. With the hot region, you can link to the e-map to view the detailed monitoring scenario, for example, the monitoring scenario of a building.

E-map is a static image (it does not have to be geographical maps, although they often are. Depending on your organization's needs, photos and other kinds of image files can also be used as e-maps) which gives you a visual overview of the locations and distributions of the hot spots (resources (e.g., camera, alarm input) placed on the map are called hot spots). You can see the physical locations of the cameras, alarm inputs, and alarm outputs, etc., and in what direction the cameras are pointing. With the function of hot region, e-maps can be organized into hierarchies to navigate from large perspectives to detailed perspectives, e.g., from floor level to room level.

After configuring the e-map via Web Client, you can view the live video and playback of the elements via Control Client, and get a notification message from the map via Control Client when an alarm is triggered.

10.1 Set GIS Map and Icons

This page allows you to enable GIS (Geographic Information System) map function to display the online or/and offline GIS map on the Web Client and Control Client, so that the geographic location of the resources (such as current site, Remote Sites, cameras) can be shown on the map.

Steps

1. Click **System → Normal → Map** to enter the map settings page.
2. Set the GIS Map.
   1) Set the **GIS Map** switch to on to enable the GIS map function.
   2) According to the actual requirements, select **Online** or **Offline** to set the online GIS map or offline GIS map.
      - For online GIS map, enter the GIS map API URL.

Note

The Google map API is supported currently.
Google Maps are provided by Google Inc. (Hereinafter referred to as "Google"). We only provides you the URLs to use Google Maps. You shall apply by yourself for the use of Google Maps from Google. You shall comply with Google terms and provide certain information to Google if required.

- For offline GIS map, click **Download Offline Map Configuration Guide** to refer to the guide and the interface instruction to add and configure the offline map.

3. Set the customized icons.
   1) Select hot region or hot spot as the icon type in the **Type** field.
   2) Set the icon size, including width (px) and height (px).
   3) **Optional:** Click the icon to cancel the aspect ratio.

   Note

   By default, the aspect ratio is maintained.

   4) Click **Add** in the Picture field to select a picture file from the local path.

   Note

   The icon picture format can only be PNG, JPG, or JPEG.

   The added pictures display as thumbnail preview in the Picture field.

4. Click **Save**.

Result

You can view the GIS map in the Logical View page and perform the following operations in the map area.

Filter	Click and select the object type you want to show on the map.
Full Screen	Click to show the map in full-screen mode.
Zoom In/Out	Scroll the mouse wheel or click + / − to zoom in or zoom out the map.
Adjust Map Area	Click-and-drag the map to adjust the map area for view.

10.2 Link E-Map to Area

You can add and link e-maps to the area so that the elements assigned to the area can be added to e-map.

Steps

1. Click **Logical View**.
2. Add a map for an area. Three ways are available for adding e-map.

   Add E-Map When Adding Area

   a. Click + on the area list panel.
   b. Set the parameters for adding area.
   c. Set the **Related Map** switch to ON.
   d. Hover the mouse over the Map field and link a map for the area.
      You can click **Upload Picture** and select a picture from local PC as the e-map. Or click **Existing Map** and select an existing map for linking to current area.
   e. **Optional:** Repeat the previous step to add more e-maps for the area.

   Add E-Map When Editing Area

   a. Select a map and click ✎ on the area list panel to enter the area editing page.
   b. Edit the area settings as desired.
   c. Set the **Related Map** switch to ON if it is OFF.
   d. Hover the mouse over the empty Map field and link a map for the area.
      You can click **Upload Picture** and select a picture from local PC as the e-map. Or click **Existing Map** and select an existing map for linking to current area.
   e. **Optional:** Repeat the previous step to add more e-maps for the area.

   Directly Link Map to Existing Area

   Note

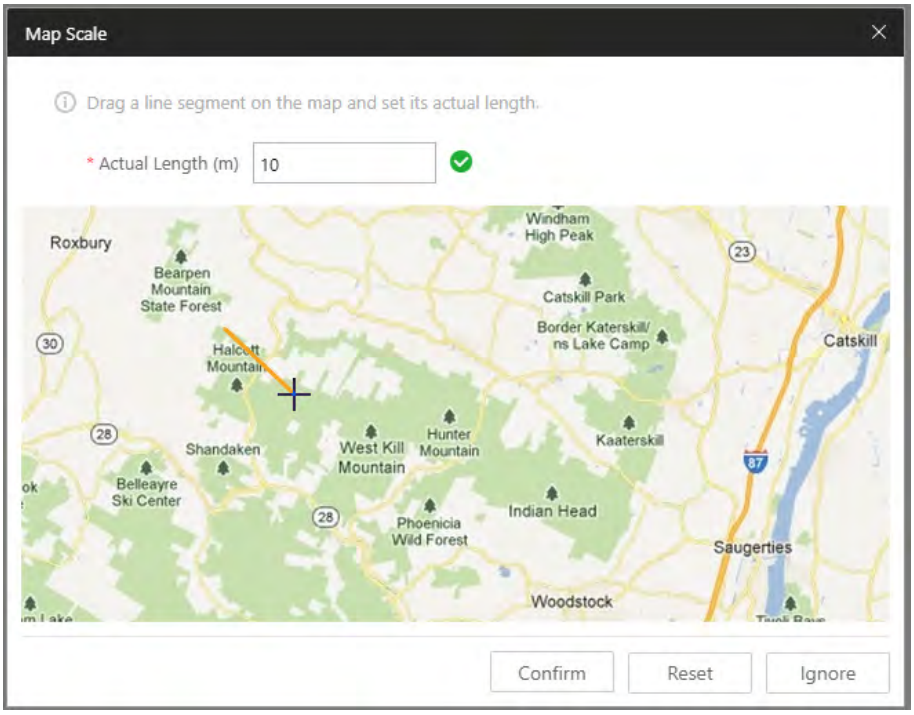
   You can adopt this way when the GIS map is not enabled.

   a. Click 🗺 to show the map area.
   b. Click **Relate Map** for adding and linking map.
   c. Select the areas for linking e-maps.
   d. Hover the mouse over the Map field and link a map for the area.
      You can click **Upload Picture** and select a picture from local PC as the e-map. Or click **Existing Map** and select an existing map for linking to current area.
   e. **Optional:** Repeat the previous step to add more e-maps for the area.

   Map Scale window will pop up.
3. **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.



Map Scale

ⓘ Drag a line segment on the map and set its actual length.

* Actual Length (m) 10 ✓

Figure 10-1 Edit Map Scale

1) Click two locations on the map to form a line.
2) Enter the real distance between the two points in the Actual Length field.
3) Click **Confirm** to finish setting the map scale.

4. **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.

5. Click **Save** to confirm the settings.
6. **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.

10.3 Search Locations

You can search the locations on the GIS map.

Before You Start
You should enable the GIS Map function and set the GIS Map API URL properly. For details, refer to ***Set GIS Map and Icons*** .

Perform this task when you need to search the locations on the GIS map.

Steps

1. Click **Logical View** on home page.
2. Click 🗺 to show the map area.
3. Enter a location name you want to search in the 🔍 field.

   The related locations display in the search field.
4. Click to select the location you want to locate from the related locations.

Result

The location will be located on the map.

10.4 Locate Sites on Map

You can set the current site's and added Remote Site's location to the GIS map.

Before You Start
You should enable the GIS Map function and set the GIS Map API URL properly. For details, refer to ***Set GIS Map and Icons*** .

Perform this task when you need to set the sites' location to the GIS map.

Steps

1. Click **Logical View** on home page.
2. Click 🗺 to show the map area.
3. Select current site or Remote Site from the drop-down list on area list panel.

   Note

   The icon 🌐 indicates that the site is current site, and 🌐 indicates Remote Site.
4. Click **Locate** on the GIS map area.

   Note

   The **Locate** button is only available when the site is not located on GIS map.
5. Operate the GIS map to find the location of the site and click on the map to locate the site on the map.

   Note

   You can use you mouse to drag, zoom in, and zoom out the map.

   After successfully located, the site icon will be displayed at the location you select.

6. **Optional:** Perform the following operations after adding the site to the GIS map.

View Site Details	Click the site icon to view the site details, including site address, location, and remark information
Edit	Click the site icon and click **Edit** to edit the site information.
Delete	Click the site icon and click **Delete** to remove the site from the map.
View Site's Resources	Click the site icon and click **View Site's Resources** to view the resources of the site.

10.5 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 or GIS 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 ***Link E-Map to Area*** or ***Set GIS Map and Icons*** for details about adding e-map or GIS map.

Steps

1. Click **Logical View** on the home page.
2. Select current site from the drop-down list on area list panel.

Note

The icon 🌐 indicates that the site is current site, you can only add current site's elements as the hot spots.

3. Three ways are available for adding hot spot.

Add Hot Spot When Adding Element to Area

a. Click the tab to enter the corresponding element page.
b. Click + in the element area.
c. Set the required parameters for adding the element to area.

Note

For details, refer to ***Add Element to Area*** .

d. Check **Add to Map** checkbox and the map area displays.
e. In the map area, click to select a map to add the hot spot to.
f. Click **Add** and you can see the adding element result in the pop-up dialog.

Drag Element to Map

Note

You can adopt this way when the element is added to the area but not added to map.

a. Click the tab to enter the corresponding element page.
b. Click to select an area so that the elements of this area display.
c. Click ◁▯ to show the map area.
d. In the map area, click to select a map to add the hot spot to.
e. Drag an element with Added to Map as No to the map.

Add Hot Spot When Editing the Element

Note

You can adopt this way when the element is added to the area but not added to map.

a. Click the tab to enter the corresponding element page.
b. **Optional:** Click to select an area so that the elements of this area can be displayed.
c. Click the Name field of the element with Added to Map as No.
d. Set the **Add to Map** switch to on.
e. Check **Auto-Locating on Map** to get the GIS location information from the device and locate the hot spot on the map automatically.

   Note

   This function should be supported by the device. For details, refer to ***Edit Camera for Current Site*** .

f. In the map area, click to select a map to add the hot spot to.
g. Configure the required settings for the hot spot.
h. Click **Save**.

4. **Optional:** Perform the following operations after adding the hot spot.

Adjust Hot Spot Location
Drag the added hot spot on the map to the desired locations.

Edit Hot Spot
Click the added hot spot icon on the map and click **Edit** to edit the detailed information (such as setting GPS location (only available when parent map is GIS map, and refer to ***Search Locations*** for details), and selecting icon style).

For camera hot spot, you can also edit the detection area, including radius, direction and angle, or drag the displayed sector on the map to directly adjust the detection area.

Delete Hot Spot
Click the hot spot icon on the map and click **Delete** to remove the hot spot from the map.

10.6 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 ***Link E-Map to Area*** or ***Set GIS Map and Icons*** for details about adding maps.

Steps

1. Click **Logical View** on the home page.
2. Select a current site in the drop-down list on area list panel.

Note

The icon 🌐 indicates that the site is current site, you can only add hot region for current site.

3. Click 🗺 in the upper-right corner to show the map area.
4. Select an added e-map or GIS map as the parent map at the bottom.
5. Click **Add Hot Region** on the top of the map and click on the spot where you want to place the hot region.

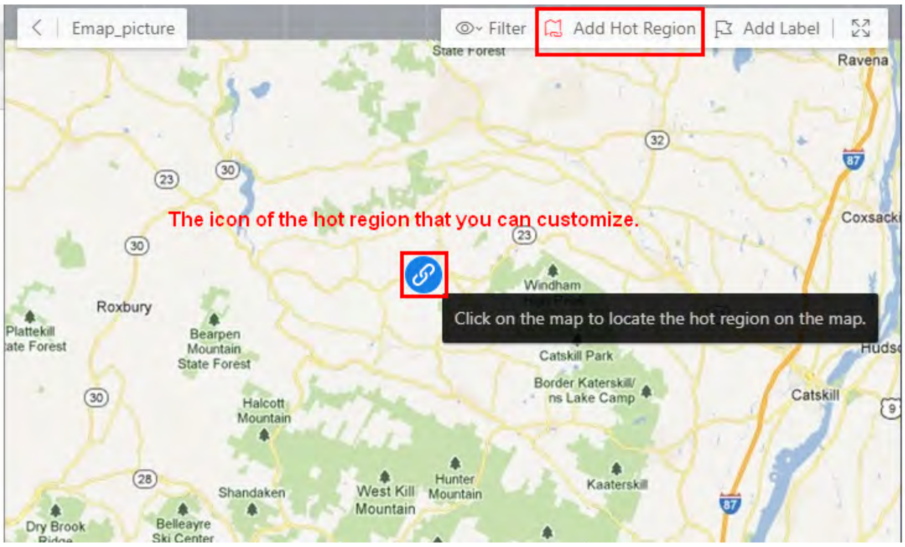


Figure 10-2 Add Hot Region on the Map

A dialog for setting child map appears.

6. Select a child map on the panel to set it as the hot region of the current map.
7. Click **Save** on dialog to add the hot region.

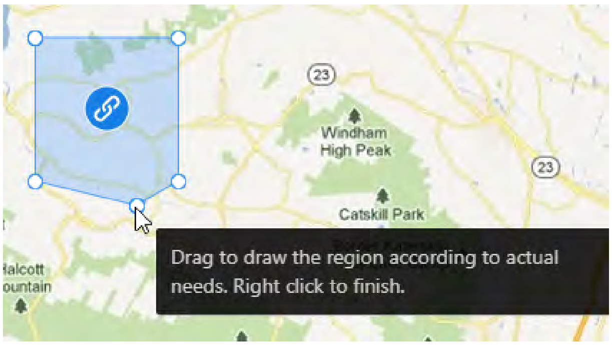
   The added hot region icon will be displayed on the parent map.
8. **Optional:** Perform the following operation(s) after adding the hot region.

Adjust Hot Region Location Drag the added hot region on the parent map to the desired locations.

Edit Hot Region Click the added hot region icon on the map to view and edit the detailed information, including GPS location (only available when parent map is GIS map, and refer to ***Search Locations*** for details), hot region name, icon style, name color, and remarks on the appearing dialog.

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.

Figure 10-3 Edit Hot Region Area

10.7 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 ***Link E-Map to Area*** or ***Set GIS Map and Icons*** for details about adding e-map or GIS map.

Perform this task when you need to add label on the map.

Steps

1. Click **Logical View** on the home page.
2. Select current site from the drop-down list on area list panel.

Note

The icon 🌐 indicates that the site is current site, you can only add label for current site.

3. Click 🗺 to show the map area.
4. Select a map to add label to.
5. Click ⚐ on the map area and click on the map where you want to place the label.
6. Customize a name for the label, and you can input content for the label as desired.
7. Click **Save**.

The added label icon will be displayed on the map.

8. **Optional:** Perform the following operation(s) after adding the label.

Adjust Label Location	Drag the added label on the map to the desired locations.
Edit Label	Click the added label icon on the map to view and edit the detailed information, including name and content on the appearing dialog.
Delete Label	Click the label icon on the map and click **Delete** on the appearing dialog to delete the label.

10.8 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:

Alarm Group

After adding the alarm group on the map, when an alarm is triggered by the resources 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 alarm group on the map, refer to ***Add Alarm Group*** .

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*** .

Pathway Analysis Group

After adding the pathway analysis group on the map, you can view the real-time number of people walking by in the Monitoring module on the Control Client.

For details about how to add a pathway analysis group on the map, refer to ***Add Pathway Analysis 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 Rules*** .

Multi-Door Interlocking

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

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*** .

Chapter 11 Manage Person List

You can add person information to the system for further operations such as access control (adding the person to access group), face comparison (adding the person to face comparison group), time and attendance (adding the person to attendance group), etc. After adding the persons, you can edit and delete the person information if needed.

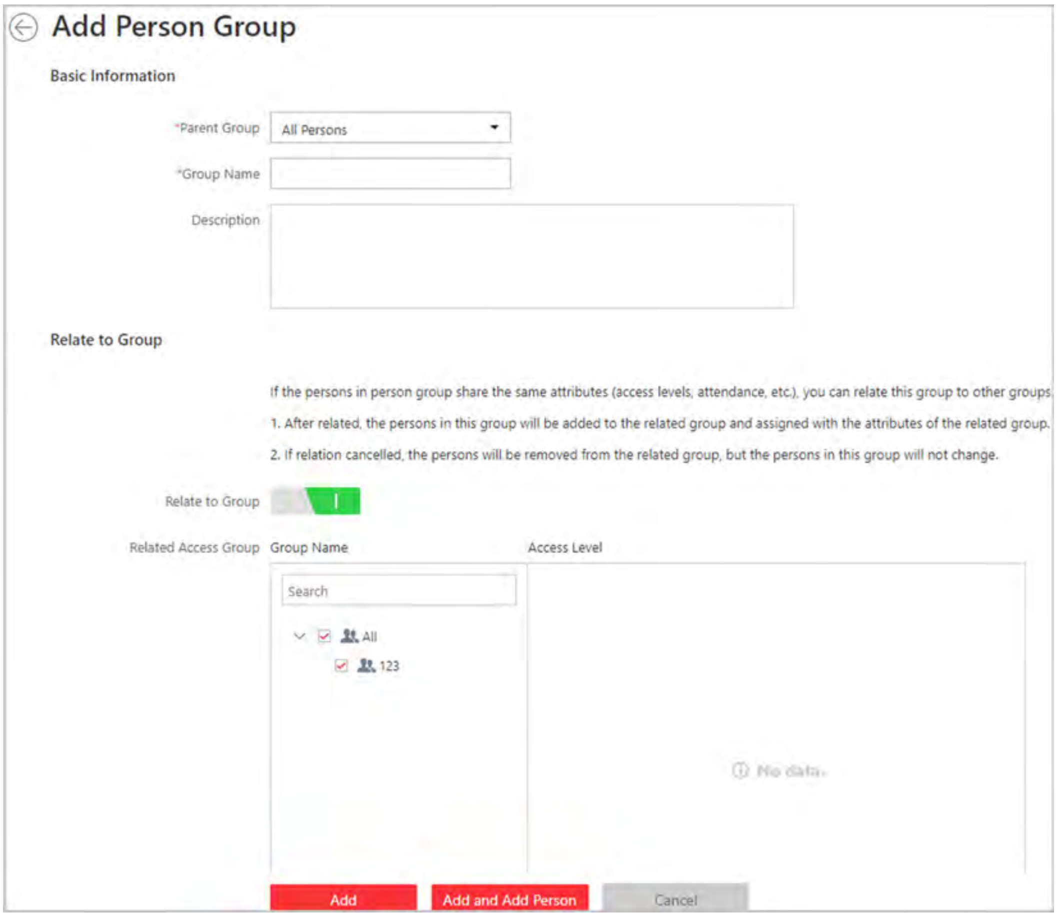
11.1 Add Person Group

When there are large amount of persons managed in the system, you can put the persons in different person groups. For example, you group employees of a company to different departments.

Steps

1. Click **Person → Person List** to enter the Person List page.

   The existing person groups will be displayed on the left panel, while all the persons will be displayed on the right panel.
2. Click + to enter the Add Person Group page.
3. Set person group information, including parent group, group name, etc.



Parent Group: All Persons

If the persons in person group share the same attributes (access levels, attendance, etc.), you can relate this group to other groups.

1. After related, the persons in this group will be added to the related group and assigned with the attributes of the related group.

2. If relation cancelled, the persons will be removed from the related group, but the persons in this group will not change.

Figure 11-1 Add Person Group Page

4. **Optional:** If the persons in the person group share the same attributes (access levels, attendance, etc.), you can relate this group to existing access group(s).
   1) Switch **Relate to Group** on.
   2) Select existing access group(s).

      After related, the persons added to this group will also be added to the related access groups and attendance groups, so that the persons will be automatically assigned with attributes of the related access groups and attendance groups.
5. Confirm to add the person group.
   - To save the person group first and add persons to this group later, click **Add** to finish this task and go back to Person List page.
   - To add persons to this person group, click **Add and Add Person** to finish this task and enter the Add Person to Person Group page to add a person to this person group.

Note

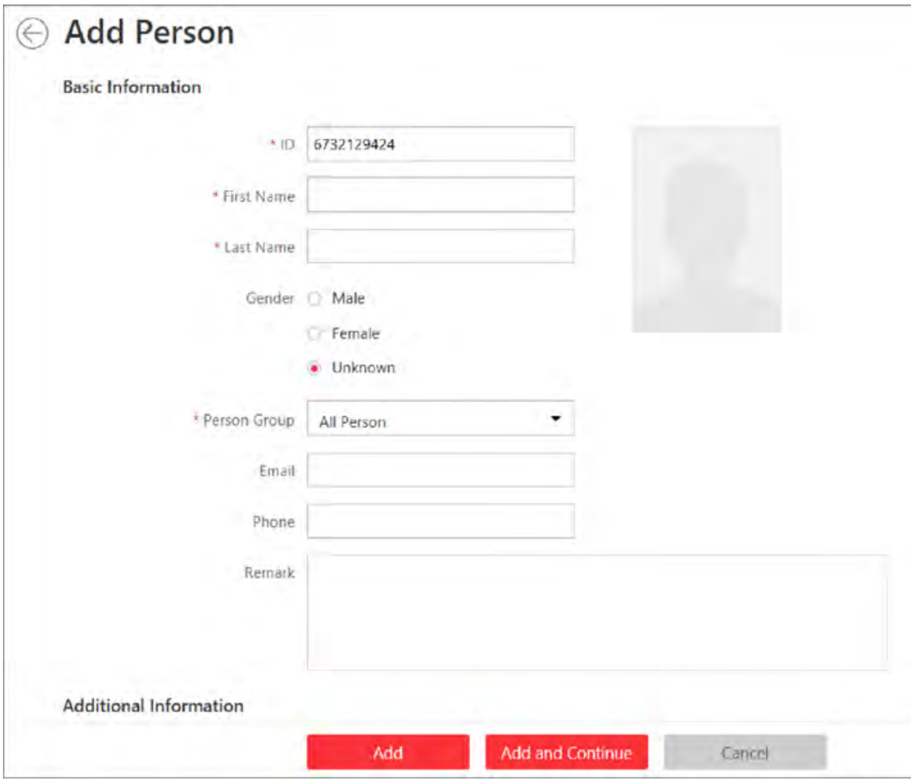
You cannot relate a person group to an access group which contains singly-added persons.

11.2 Add a Person

You can add the person information to the system one by one.

Steps

1. Click **Person → Person List** and click **Add** to enter the adding person page.



Add Person

Basic Information

* ID 6732129424

* First Name

* Last Name

Gender ○ Male ○ Female ● Unknown

* Person Group All Person

Email

Phone

Remark

Additional Information

Figure 11-2 Add a Person

2. Set the person basic information.

   ID

   The default ID is generated by the system. You can edit it if needed.

   Note

   If the person is police officer or security guard with body cameras, make sure the person ID is same with the police ID configured on the body camera.

   Person Picture

   Hover the cursor on the person picture field to show the three picture-adding modes.

   From Device

Select **Access Control Device** or **Enrollment Station** to collect the face picture. This mode is suitable for non-face-to-face scenario that the person and the system administrator are in different locations.

Note

- For access control device, only face recognition terminals (including DS-K5671, DS-K1T671, DS-K1T331, DS-K1T341, DS-K1T672, DS-K1T642, etc.) are supported.
- For enrollment station, 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** to use the PC's webcam 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 switch **Verify Face Quality by Device** to on and select a device to check its 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.

3. Select a person group for the person. See ***Add Person Group*** for details about adding a person group.
4. **Optional:** Set the person's additional information.

Note

You can customize these items according to actual needs as the person's additional information. For details, refer to ***Custom Additional Information*** .

5. **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*** .

6. **Optional:** Set the access control and time & attendance information.

Effective Period

Set the effective period for the person in access control application and time & attendance application. For example, if the person is a visitor, his/her effective period may be short and temporary.

Access Group

Add the person to the existing access group(s) which can be linked with access level(s). The linkage of access level and access group defines the access permission that which person(s) can access which access point(s) in the authorized period.

You can click the access group name to view its linked access levels.

Move the cursor to the access level to view its access point(s) and access schedule.

Note

You can click **Add New** to add a new access group. For details, refer to ***Add Access Group*** .

Super User

If the person is set as a super user, he/she will be exempted from remaining locked (credential failed) restrictions, all anti-passback rules, and first card authorization.

Note

For details about setting these functions, refer to ***Edit Door for Current Site*** .

Extended Access

When the person accessing door, grant this person more time to pass through doors which have been configured with extended open duration. Use this function for the persons with reduced mobility.

Note

You should set the door's extended open duration in Logical View. For details, refer to ***Edit Door for Current Site*** .

Attendance Group

Add the person to the existing attendance group if your need to monitor the person's working hours and absenteeism.

Note

You can click **Add New** to add a new attendance group. For details, refer to ***Add Attendance Group*** .

Note

The extended access and super user functions cannot be enabled concurrently.

7. Set the person's credential information, including PIN, face credential, card number, fingerprint, and duress credentials.

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.

Set Profile as Face Credential

If you want to use turnstile with face recognition function, you need to set the person's profile picture as her\his face credential so that the person can scan her\his face on the face recognition terminal when he/she wants to access the turnstile. Make sure you have uploaded a picture as the person profile.

Card

Issue a card to the person to assign the card number to the person. You can enter the card number manually, or swipe a card on the card enrollment station, enrollment station, or card reader to get the card number, and then issue it to the person.

a. Click **+** in the **Card** field.
b. Place the card that you want to issue to this person on the card enrollment station, enrollment station, or on the card reader and the card number will be read automatically. Or you can enter the card number manually

Note

You can click **Configuration** to set the issuing mode. For details, refer to ***Set Card Issuing Parameters*** .

123456789

Figure 11-3 Card Number Read

Note

Up to 5 cards can be issued to one person.

Fingerprint

System provides three ways to collect fingerprint: via a USB fingerprint recorder, via an enrollment station or via a fingerprint and card reader.

Click **Configuration** to set the collection mode as follows.

USB Fingerprint Recorder

Collect fingerprint via a USB fingerprint recorder connected to the PC running the Web Client, which is plug-and-play and doesn't require any settings. This mode is suitable for face-to-face scenario that the person and the system administrator are in the same location.

After connecting the fingerprint recorder to your PC, click **+**, place and lift your fingerprint on the recorder following the prompts and it will collect your fingerprint automatically.

Note

After collecting a fingerprint by a USB fingerprint recorder, the quality of the fingerprint will be displayed. A new fingerprint is required if the quality is too low.

Enrollment Station

You need to specify the device IP address, port number, user name and password to access the enrollment station. Then click **+**, place and lift your fingerprint on the device and it will enroll your fingerprint automatically.

Fingerprint and Card Reader

Collect fingerprint via the fingerprint scanner of an access control device which is managed in the system. This mode is suitable for non-face-to-face scenario that the person and the system administrator are in different locations.

Select an access control device from the managed device list and select a fingerprint and card reader.

Click **+**, place and lift your fingerprint on the selected fingerprint and card reader following the prompts and it will collect your fingerprint automatically.

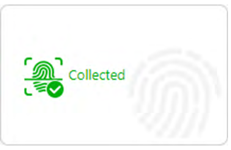


Figure 11-4 Fingerprint Recorded

Note

Up to 10 fingerprints can be added to one person.

Special Credential

Set the **Special Credential** switch to on, and select the following two usages for card or fingerprint credential.

Credential under Duress

Set the credentials (card number and fingerprint) so that when you are under duress, you can swipe the card or scan the fingerprint configured here. The door will be unlocked and the Control Client will receive a duress alarm (if configured) to notify the security personnel.

Note

When the person accesses with credentials under duress, he/she cannot be exempted from remaining locked (credential failed) restrictions, all anti-passback rules, and first card authorization. Extended access is not allowed as well.

Credential for Dismiss

Set the credentials (card number and fingerprint) so that when an alarm is triggered, you can swipe the card or scan the fingerprint configured here. The alarm will be dismissed.

8. **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

- You can click **Add New** to add a new dock station group. For details, refer to ***Add Dock Station Group*** .
- 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).

9. 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.

10. 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.

11. **Optional:** After adding the person, you can do one or more of the followings:

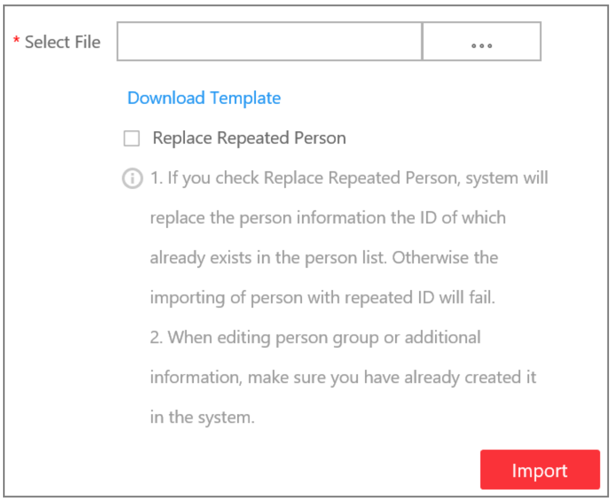
Edit Person	Click the person name to edit the person details.
Delete Person	Select the person(s) and click **Delete** to delete.
Delete All Persons	Click ⌵ near Delete button and click **Delete All** to delete all the persons in the person list.
Export Added Person Information	Click **Export All** to 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.

11.3 Batch Add Persons by Importing Person Information File

You can add the information of multiple persons to the system by importing an excel file with person information. Also, by entering the name of a person group/access group/face comparison group/attendance group/dock station group of multiple persons in the excel file, you can add them to a group in a batch.

Steps

1. Click **Person → Person List/Face Comparison Group/Access Group/Attendance Group/Dock Station Group → Import → Import an Excel File** .



* Select File ...

Download Template

□ Replace Repeated Person

ⓘ 1. If you check Replace Repeated Person, system will replace the person information the ID of which already exists in the person list. Otherwise the importing of person with repeated ID will fail.

2. When editing person group or additional information, make sure you have already created it in the system.

Import

Figure 11-5 Import Person Information

2. Click **Download Template** to save the template file in your PC.
3. In the downloaded template, enter the person information following the rules in the template.
4. **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.
5. Click **Import → Import an Excel File** to enter the Import Person Information page.
6. Select the excel file with the person information
7. Click **Import** to start importing.

Note

- The importing cannot stop once started.
- You can issue cards to persons in a batch 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.

8. **Optional:** Perform the following operation(s).

Edit Person	Click the person name to edit the person details.

Delete Person
Select one or more person 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.

11.4 Import Domain Persons

You can import the users in the AD domain in a batch to the system as persons. After importing the person information (including person name and account name) in the AD domain, you can set other information for the persons, such as credentials.

Before You Start
You should configure the active directory settings. See ***Set Active Directory*** for details.

Steps

1. Click **Person → Person List** to enter the Person List Management page.
2. Click **Import → Import Domain Persons** to enter the following page.

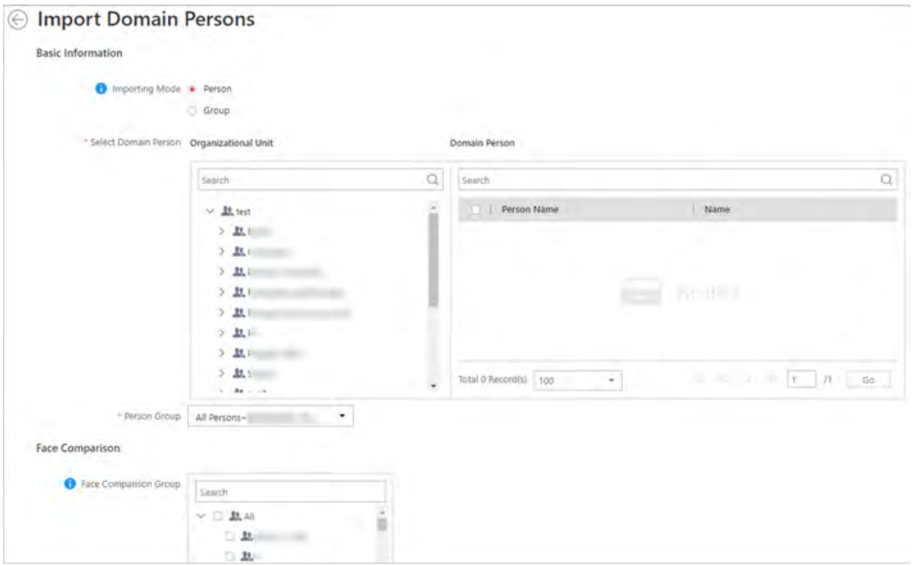


Figure 11-6 Import Domain Persons

3. Select the importing mode.

   Person

   Import the specified persons. Select the organization unit and select the persons under the organization unit which are displayed in the Domain Person list on the right. It will synchronize person information based on each person.

Group

Import all the persons in the organization unit. It will synchronize person information based on each group.

4. If you select **Person** as the importing mode, select a person group to import the persons to.
5. Add the persons to the existing face comparison group(s) which will be used for face recognition and comparison.

Note

After adding the persons to the face comparison group, you should apply the face comparison group to a device to make the settings effective. For details about applying face comparison group to the device, refer to ***Apply Face Comparison Group to Device*** .

6. Set the access control and time & attendance information.

Effective Period

Set the effective period for the person in access control application and time & attendance application. For example, if the person is a visitor, his/her effective period may be short and temporary.

Access Group

Add the persons to the existing access group(s) which can be linked with access level(s). The linkage of access level and access group defines the access permission that which person(s) can access which access point(s) in the authorized period.

You can click the access group name to view its linked access levels.

Move the cursor to the access level to view its access point(s) and access schedule.

Note

You can click **Add New** to add a new access group. For details, refer to ***Add Access Group*** .

Super User

If the persons are set as super users, they will be exempted from remaining locked (credential failed) restrictions, all anti-passback rules, and first card authorization.

Note

For details about setting these functions, refer to ***Edit Door for Current Site*** .

Extended Access

When the persons accessing access point, grant these person more time to pass through doors which have been configured with extended open duration. Use this function for the persons with reduced mobility.

Note

You should set the access point's extended open duration in Logical View. For details, refer to ***Edit Door for Current Site*** .

Attendance Group

Add the persons to the existing attendance group if your need to monitor the persons' working hours and absenteeism.

Note

You can click **Add New** to add a new attendance group. For details, refer to ***Add Attendance Group*** .

Note

The extended access and super user functions cannot be enabled concurrently.

7. Complete importing the domain persons.
   - Click **Add** to add the persons.
   - Click **Add and Continue** to save the settings and continue to add persons.
8. **Optional:** After importing the person information in the domain to the system, 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 system, the persons' profile/email will be imported to the system 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 system, 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 system, refer to ***Set Active Directory*** .

9. **Optional:** After importing the person information in the domain to the system, if the person information in domain is changed, click **Synchronize Domain Persons** to get the latest information of the persons imported to the system. If the persons are imported by group, it will synchronize the latest person information from the domain group (including added persons, deleted persons, edited persons, etc., in the group).

11.5 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. Click **Person → Person List** to enter the person list page.
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.

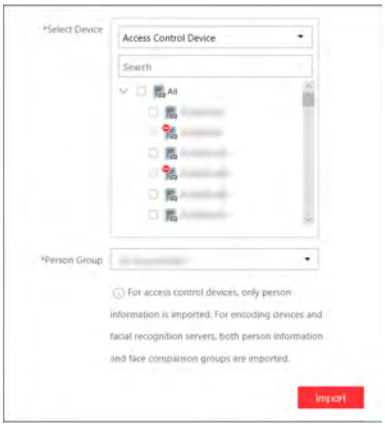
   The importing progress shows and you can check the results.
9. **Optional:** After importing profiles, click **Export Failure Details** to export the Excel file to the local PC and view the failure details including department, person name and person ID.

11.6 Import Persons from Access Control Device, Encoding Device and Facial Recognition Server

If the added access control device, encoding device, or facial recognition server has been configured with person information, you can get the person information from the device and import them to the system for further operations. The person information stored on the device, including person names, profiles, credentials (PIN codes, cards, and fingerprints), can be imported to the system.

Steps

1. Click **Person → Person List** to enter the Person List Management page.
2. Click **Import → Import from Device** to enter the following page.



*Select Device: Access Control Device

*Person Group:

For access control devices, only person information is imported. For encoding devices and facial recognition servers, both person information and face compaison groups are imported.

Figure 11-7 Import Persons from Device

3. Select the access control device(s)/encoding device(s)/facial recognition server(s) from the device list.
4. **Optional:** Select a person group to import the persons to.
5. Click **Import** to start importing.

Note

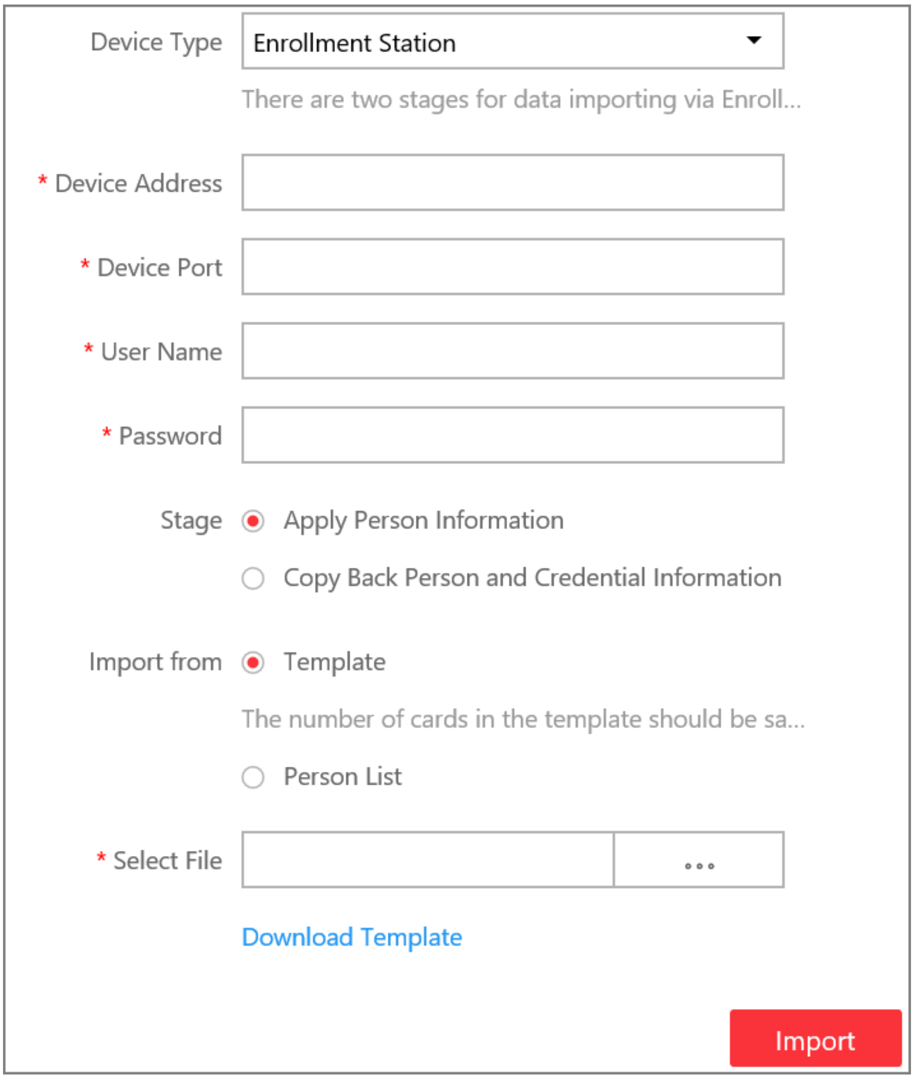
When importing, the system will compare the persons between device and system based on the person name. If the person name exists on the device but not exists in the system, the system will create a new person. If the person name exists both on the device and in the system, the person information in the system will be replaced with the data on the device.

11.7 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. Click **Person → Person List** to enter the Person List Management page.
2. Click **Import → Import from Device** .
3. Select **Enrollment Station** from the device list.



Device Type: Enrollment Station

There are two stages for data importing via Enroll...

* Device Address

* Device Port

* User Name

* Password

Stage: ● Apply Person Information ○ Copy Back Person and Credential Information

Import from: ● Template

The number of cards in the template should be sa...

○ Person List

* Select File

Figure 11-8 Import Person from Enrollment Station

4. Set device address, port, 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.

11.8 Batch Issue Cards to Persons

The system provides a convenient way to issue card to multiple persons in a batch.

Steps

Note

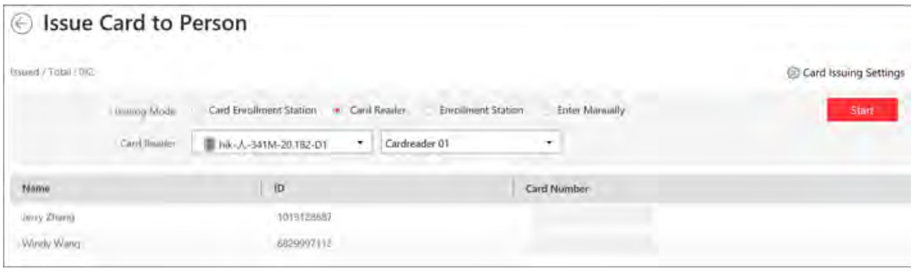
- Up to 5 cards can be issued to one person.
- You cannot issue cards to persons who have temporary card.

1. Click **Person → Person List** to enter the person list page.

   Note

   The selected persons who have less than 5 cards will be displayed.

2. Select the persons to issue the card to.
3. Click **Batch Issue Cards to Persons** to enter the following page.



Issue Card to Person

Issued / Total : 0/2

Card Issuing Settings

Issuing Mode ○ Card Enrollment Station ● Card Reader ○ Enrollment Station ○ Enter Manually

Start

Card Reader: hik-人-341M-20.182-D1 ▾ Cardreader 01 ▾

Name	ID	Card Number
Jerry Zhang	1019128687	
Windy Wang	6829997112	

Figure 11-9 Issue Card to Persons in Batch

4. Click **Card Issuing Settings** to display the area and set the 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.

  You can check **Auto Increment Card Number** and enter a start card number. Then click **Start** to issue cards with incremental numbers to the selected persons in the list.

6. Repeat the above step 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.

7. Click **Save**.

11.9 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. Click **Person** on the home page and enter the **Person List** page.
2. You can enter the card issuing parameters settings page when adding single person or issuing cards to persons in a batch.
   - For entering the card issuing parameters settings page when adding single person, refer to ***Add a Person*** .
   - For entering the card issuing parameters settings page when issuing cards to persons in a batch, refer to ***Batch Issue Cards to Persons*** .
3. Set the issuing mode and set related parameters.

   Card Enrollment Station

   Connect a card enrollment station to the PC running the Web Client. You can place the card on the card enrollment station to get the card number.

   If you select this mode, you should set the card format and card encryption function.

   Card Format

   If the card is Wiegand card, select **Wiegand**. Otherwise select **Normal**.

   Reading Frequency

If your card supports dual frequency (both IC and ID), you need to select **Dual**. Otherwise, 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**.

11.10 Report Card Loss

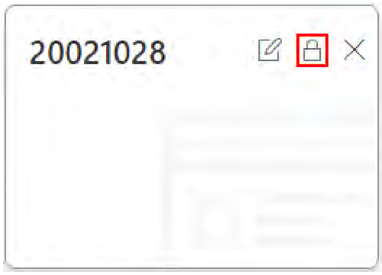
If the person cannot find his/her card, he/she should contact the card issuer as quickly as possible and the card issuer should report card loss via Web Client immediately to freeze the access level on the lost card. The card issuer can issue a temporary card with effective period and access level to 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.

11.10.1 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. Click **Person → Person List** .
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 🔒 .



20021028

Figure 11-10 Report Card Loss

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.

11.10.2 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 the card reported loss.

Steps

1. Click **Person → Person List** .
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 11-11 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 active, and their previously linked fingerprints and profiles will recover, too.

11.10.3 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 the card reported card loss and has no temporary card.

Steps

1. Click **Person → Person List** .
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 found card and click 🔓 .

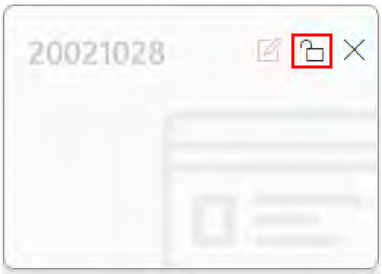


Figure 11-12 Cancel Card Loss

5. Click **OK** to confirm the operation.
6. Click **Save**.

11.11 Custom 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. Click **Person → Person List** .
2. Click ⚙ **Custom Additional Information** to enter the custom addition information page.
3. Click **Add**.
4. Create a name for this item.

   Note

   Up to 32 characters are allowed in the name.

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:** After adding the additional information, you can do one or more of the followings.

   Edit Name Click ✎ to edit its name.

   Delete Click × to delete the additional information.

   Note

   The additional information which is linked with person information in domain cannot be deleted.

Chapter 12 Manage Visitor

HikCentral Professional provides visitor management function for effective security control.

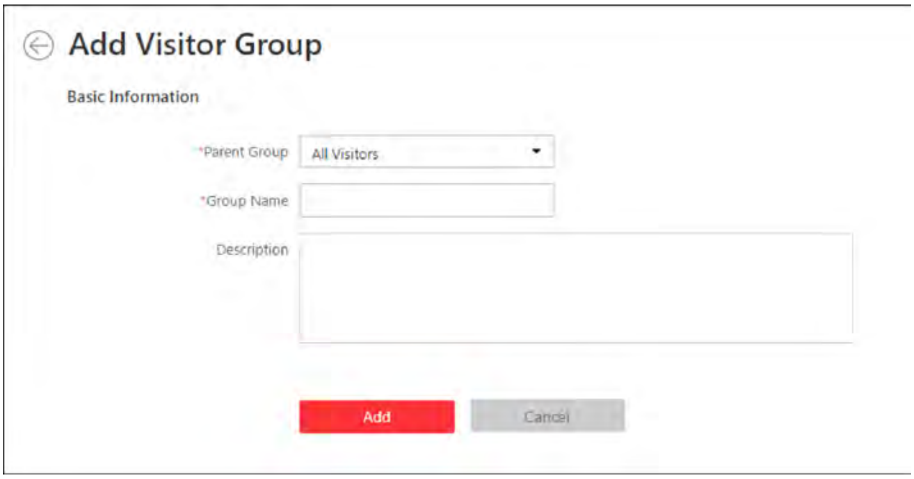
The system connects visitors and persons managed by the system together. It provides an entire process for visitors tour from registration to check-out. You can group visitors with different visiting reason to different access groups for effective management; customize the accessible area of the visitors, and the visitors can access the areas by various ways like fingerprint, face picture, and ID card.

12.1 Add a Visitor Group

You can group the added visitors for convenient management. For example, you add a business group for visitors coming for business communication, and you add a tour group for touring visitors. Then, you group the two kinds of visitors to corresponding group when you register for them.

Steps

1. Enter the Visitor module.
2. Click **Visitor List** → + to enter the Add Visitor Group page.



Add Visitor Group

Basic Information

*Parent Group: All Visitors

*Group Name:

Description:

Figure 12-1 Add Visitor Group Page

3. Select a parent group.
4. Enter information of the group.
5. Click **Add**.

   The added visitor will be displayed on the left.

Note

Up to 10 hierarchies of visitor group are supported.

6. **Optional:** Perform the following operations after adding a visitor group.

   Edit Visitor Group Click ✎ to change the visitor group's information.

   Delete Visitor Group Select a visitor group and click 🗑 , or click ⌄ to delete all added visitor groups.

12.2 Add a Visitor

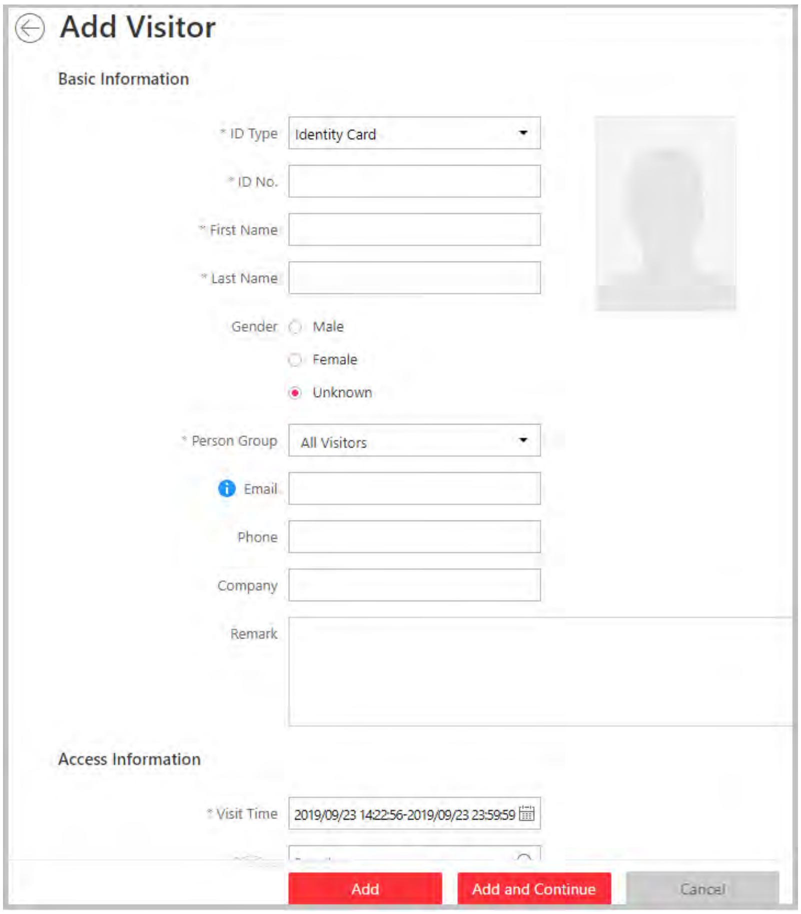
Before a visitor comes, you should register for her/him in the system by entering visitor information. Then, the visitor can check in by her/his biometrics(including fingerprint and face picture) or QR code, and will be able to access the predefined doors and floors.

Steps

1. Enter the Visitor module.
2. Click **Visitor Registration → Add** to enter the Add Visitor page.
3. Set the basic information for the visitor, including ID type, ID No., name, gender, profile, person group, email, etc.

   Note

   You can set the visitor profile by 3 different ways: collecting a face picture from device, take a picture by the camera of the running computer, and upload a picture saved in the running computer.



Add Visitor

Basic Information

* ID Type: Identity Card

* ID No.:

* First Name:

* Last Name:

Gender: ○ Male ○ Female ● Unknown

* Person Group: All Visitors

Email:

Phone:

Company:

Remark:

Access Information

* Visit Time: 2019/09/23 14:22:56-2019/09/23 23:59:59

Add | Add and Continue | Cancel

Figure 12-2 Add Visitor Page

4. Set the access information for the visitor, including visit time, visit reason, access group, etc.

Access Group

Select access groups for the visitor in the Group Name frame.

Note

If you click a group name, its access level will appear in the Access Level frame. You can hover the cursor on the access level to view the access point and schedule template of the access group.

Extended Access

If you check Extended Access, the visitor will be granted more time to pass through doors which have been configured with extended open duration when he/she accessing door. Use this function for the persons with reduced mobility.

Set Profile as Face Credential

A face picture is required to be uploaded if you check this function.

Card

Issue a card to the visitor to assign the card number to the visitor. You can enter the card number manually, or swipe a card on the card enrollment station, enrollment station, or card reader to get the card number, and then issue it to the visitor.

a. Click + in the **Card** field.
b. Place the card that you want to issue to this visitor on the card enrollment station, enrollment station, or on the card reader and the card number will be read automatically. Or you can enter the card number manually.

Note

You can click **Card Issuing Settings** to set the issuing parameters.

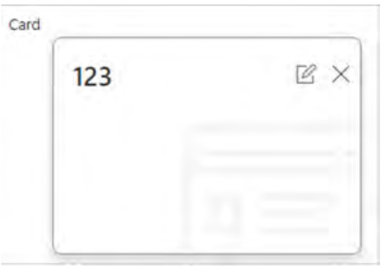


Figure 12-3 Card Number Read

Note

No more than 1 card can be issued to one visitor.

Fingerprint

System provides three ways to collect fingerprint: via a USB fingerprint recorder, via an enrollment station or via a fingerprint and card reader.

Click **Configuration** to set the collection mode as follows.

USB Fingerprint Recorder

Collect fingerprint via a USB fingerprint recorder connected to the computer running the Web Client, which is plug-and-play and does not require any settings. This mode is suitable for face-to-face scenario that the person and the system administrator are in the same location.

After connecting the fingerprint recorder to your computer, click + , place and lift your fingerprint on the recorder following the prompts and it will collect your fingerprint automatically.

Enrollment Station

You need to specify the device IP address, port number, user name and password to access the enrollment station. Then click **+**, place and lift your fingerprint on the device and it will enroll your fingerprint automatically.

Fingerprint and Card Reader

Collect fingerprint via the fingerprint scanner of an access control device which is managed in the system. This mode is suitable for non-face-to-face scenario that the person and the system administrator are in different locations.

Select an access control device from the managed device list and select a fingerprint and card reader.

Click + , place and lift your fingerprint on the selected fingerprint and card reader following the prompts and it will collect your fingerprint automatically.

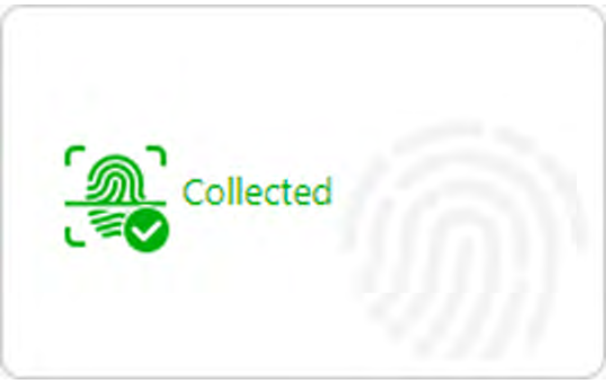


Figure 12-4 Fingerprint Recorded

Note

No more than 1 fingerprint can be collected for one visitor.

5. Click **Add** to add the visitor and go back to the Person Registration page; click **Add and Continue** to save the settings and continue to add another visitor.
6. **Optional:** Perform the following operations after adding a visitor.

Export All Visitors

Click **Export All** on the top of the registered visitor list to export all registered visitors to the computer as a file.

Note

You will be required to set a password for the exported file for security. 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.

Visitor Check-out

Click ⇥ in the Operation column to check out for the visitor.

Edit Visitor Information

Click ✎ in the Operation column to edit the added visitor's information.

Download Visitor QR Code

Click ▦ in the Operation column to download a QR code for the visitor. You can print it for the visitor's check-in.

What to do next

You can view the added visitors in the Visitor List. For details, see ***View and Delete Visitors in Visitor List*** .

12.3 Batch Add Visitors by Importing Visitor Information File

You can enter the multiple visitors' information in the predefined template to add them to the system at a time.

Steps

1. Enter the Visitor module.
2. Click **Visitor Registration → Import** .
3. Click **Download Template** to save the predefined template (a .XLSX file) in your computer.
4. Open the downloaded template file and enter the required information of the visitors to be added on corresponding columns.

   Note

   You should enter the entire path of the visitor group and separate different levels with semicolon.

5. Click ··· and select the edited file.
6. **Optional:** Check **Replace Repeated Visitor** to replace the visitor's information if the imported ID type and ID is the same with an existing visitor in the list.
7. Click **Import** to start importing the visitors into the system.
8. **Optional:** Perform the following operations after importing visitors.

   Export All Visitors
   Click **Export All** on the top of the registered visitor list to export all registered visitors to the computer as a file.

   Note

   We highly recommend you set the password of properly (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.

   Visitor Check-out
   Click 📅 in the Operation column to check out for the visitor.

   Edit Visitor Information
   Click ✎ in the Operation column to edit the added visitor's information.

   Download Visitor QR Code
   Click ▦ in the Operation column to download a QR code for the visitor. You can print it for the visitor's check-in.

12.4 View and Delete Visitors in Visitor List

You can view all registered visitors (including those who have checked out) in the visitor list and perform related operations if you need.

Enter the Visitor module and select **Visitor List**, and information of all the registered visitors will appear, including basic information, credential information, and access information. You can perform the following operations.

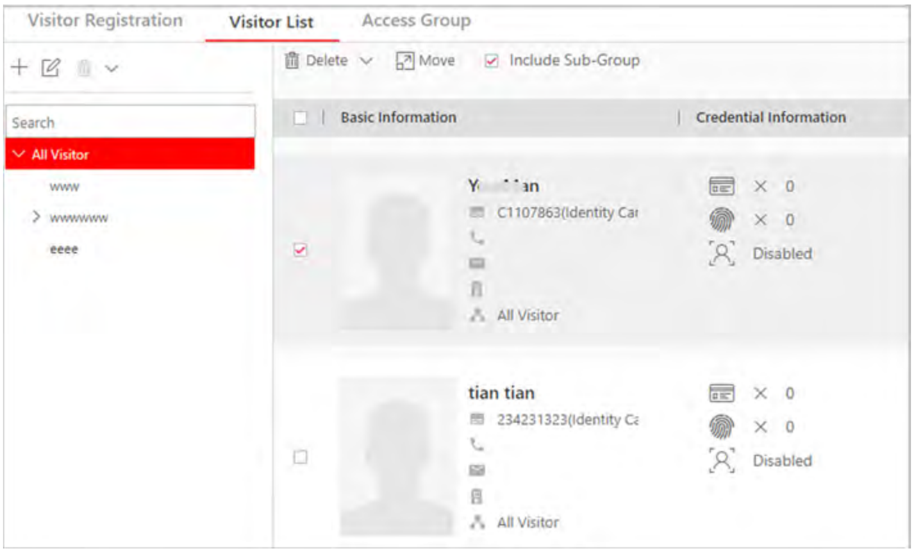


Figure 12-5 Visitor List

- Check one or more visitor and click **Delete** to delete the selected visitor(s); or click ⌵ → **Delete All** to delete all visitors.

  Note

  After deleting the visitor's personal information, you can still search the visitor's visiting records in the Visitor List.

- Check one or more visitor and click **Move** to move the selected visitor(s) into a different visitor group.
- Check **Include Sub-Group** to show visitors in both main group and sub-groups.

12.5 Add Access Group for Visitors

An access group contains access points that are accessible during certain period. If you select an access group for a visitor for registration and apply the settings to devices, he/she can access the access point(s) of the access group during authorized period with credentials.

Steps

Note

Up to 256 access groups can be added.

1. Enter the Visitor module.
2. Click **Access Group → Add** to enter the Add Access Group page.
3. Set the basic information.

   Access Level

   Select the access level(s) to link the access group to the access level(s) so that the visitors linked to the access group can access the doors and floors linked to the access level(s) during the authorized time period.

   Note

   - Up to 8 access levels can be added to an access group.
   - Move the cursor to the access level and you can view its doors, floors, and access schedule.

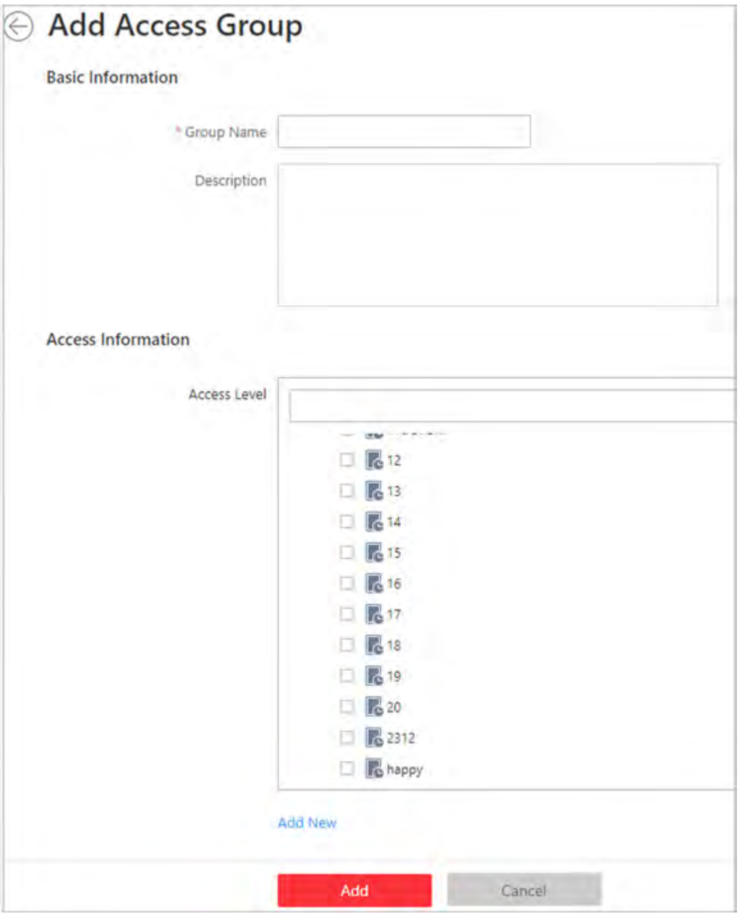


Figure 12-6 Add Access Group Page

4. Click **Add**.

The added access group will be displayed in the access group list. And you can view its accessible access points and period.

5. **Optional:** Perform the following operations after adding access group.

   View Certified Visitors
   Click access group name and the visitors who can pass the access points of the group will be displayed on the right panel.

   Edit Access Group
   Click ✎ to edit the selected access group.

   View Door's Access Template
   Click a door's access template name to view when the door is accessible for the visitor. See ***Set Access Schedule Template*** for details about setting access template.

   Delete Access Group
   Click an access group and click **Delete** to delete the selected access group; or click ⌄ → **Delete All** to delete all the access groups.

What to do next

Apply visitor's access levels to device. See ***Manually Apply Visitor's Access Levels to Device*** for details.

12.6 Manually Apply Visitor's Access Levels to Device

If you have added visitors to an access group, or deleted/edited visitors of an access group, or changed access levels of an access group, you have changed the access group's settings. You should apply the changes to its devices to make the changes take effect. If you have added new devices, you can apply the settings to all the devices.

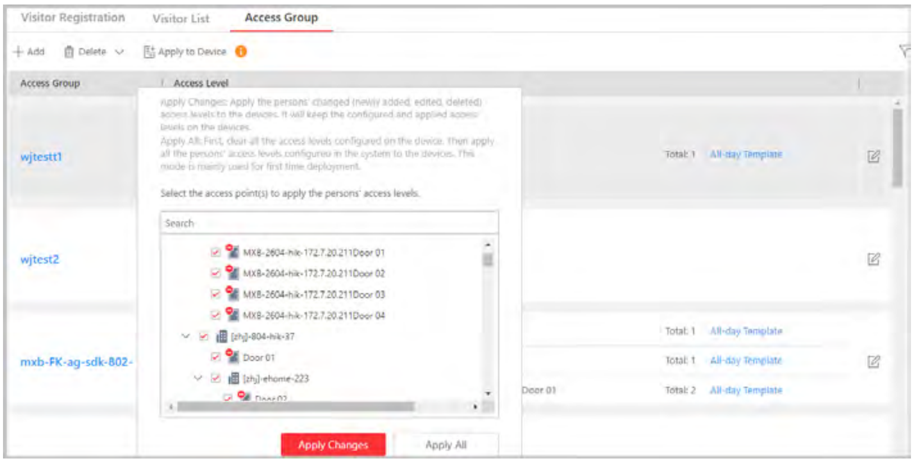
Steps

1. Enter the Visitor module and click **Access Group** tab.

   All access groups will be listed on the left panel, and the visitors of the access groups will be displayed on the right panel if you click an access group. You can check the visitors and click **Delete** or ⌄ → **Delete** on the right panel to delete the selected visitors or all visitors.

2. Select an access group, and click **Apply to Device**.

   The access level resources will be displayed in a new window.



Apply Changes: Apply the persons' changed (newly added, edited, deleted) access levels to the devices. It will keep the configured and applied access levels on the devices.

Apply All: First, clear all the access levels configured on the device. Then apply all the persons' access levels configured in the system to the devices. This mode is mainly used for first time deployment.

Select the access point(s) to apply the persons' access levels.

Figure 12-7 Apply Visitor's Access Level to Device

3. Select devices in the list, click **Apply Changes** to apply the changes of the access group to its devices, or click **Apply All** to clear all the access levels configured on the device and then apply all the access levels to the devices.

12.7 Visitor Check-Out

You should check out for the visitor before him/her leaves. After checking out, the visitor's access information will expire.

Manually Check-Out

Enter the Visitor module and click **Visitor Registration**. Find the visitor to check out and click in the Operation column.

Automatically Check-Out

The visitor will be checked out by the system automatically when the visiting duration ends if you do not manually check out for him/her.

Note

You can still view the checked-out visitor's information in Visitor List. See ***View and Delete Visitors in Visitor List*** for details.

Chapter 13 Manage Access Control and Elevator Control

The system supports access control and elevator control functions. Access control is a security technique that can be used to regulate who can get access to the specified doors and elevator control can be used to regulate who can get access to the specified floors by taking the elevator.

On the Web Client, the administrator can add access control devices & elevator control devices to the system, group resources (such as doors and elevators) into different areas, and define access permissions by creating an access level to group the doors/floors 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 and floors in the access level with their credentials during the authorized time period.

13.1 Flow Chart

The following flow chart shows the process of the configurations and operations of access control and elevator 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 configuration.

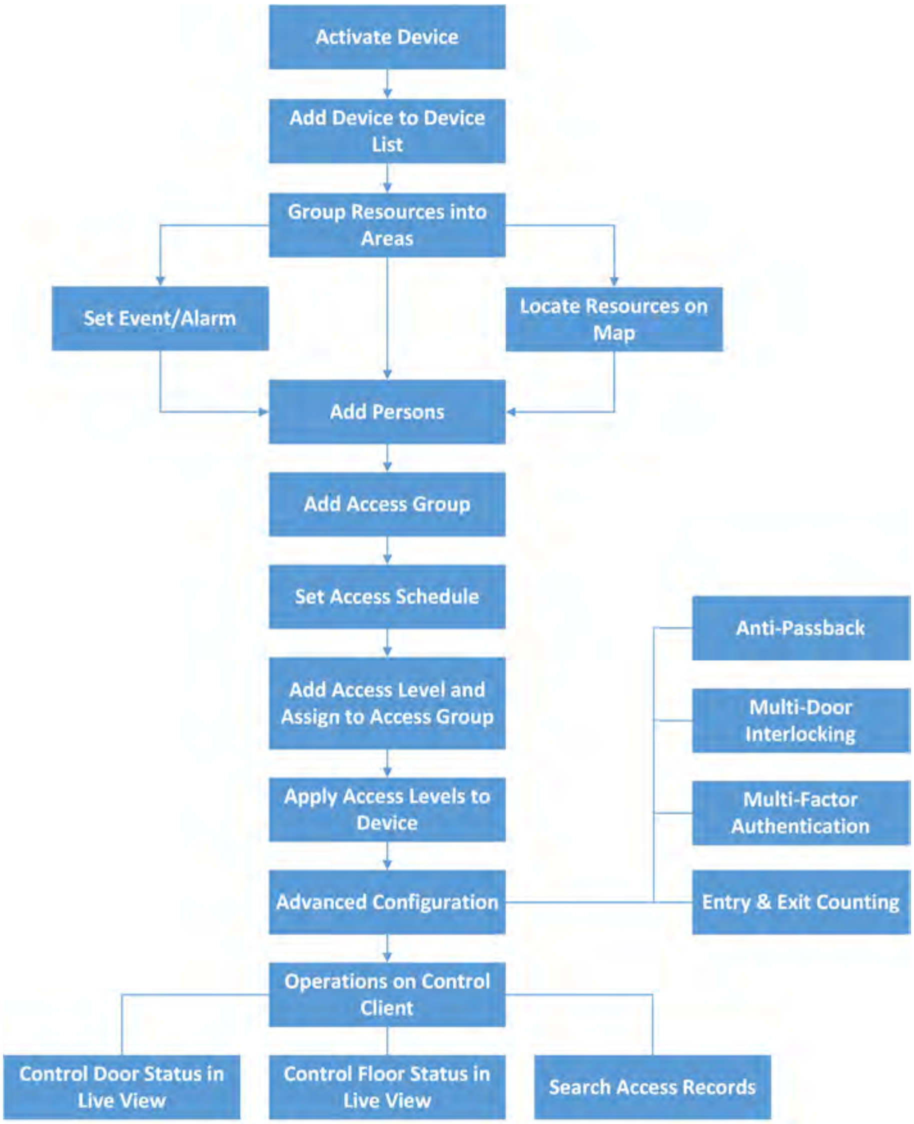

Activate Device
Add Device to Device List
Group Resources into Areas
Set Event/Alarm
Locate Resources on Map
Add Persons
Add Access Group
Set Access Schedule
Add Access Level and Assign to Access Group
Apply Access Levels to Device
Advanced Configuration
Anti-Passback
Multi-Door Interlocking
Multi-Factor Authentication
Entry & Exit Counting
Operations on Control Client
Control Door Status in Live View
Control Floor Status in Live View
Search Access Records

Figure 13-1 Flow Chart of Access Control and Elevator Control

- **Activate Device:** For the first time using the access control devices or elevator control devices, the devices are inactive. You need to activate them and create passwords for them for security purpose. For details, refer to ***Create Password for Inactive Device(s)*** .
- **Add Device to Device List:** You need to add the access control devices and elevator control devices to the system. The system provides multiple methods for adding them. For details, refer to ***Manage Access Control Device*** and ***Manage Elevator Control Device*** .
- **Group Resources into Areas:** After adding the devices to the system, you need to group the devices' resources (such as doors, elevators, alarm inputs, alarm outputs, etc.) into different areas according to the resources' locations. For details, refer to ***Manage Area*** .
- **Set Event/Alarm:** You need to pre-define the events and alarms, such as the access events occurred at the doors. The detailed event and alarm information can be received and checked via the Control Client and Mobile Client. For details, refer to ***Configure Event and Alarm*** .

- **Locate Resources on Map:** For visualization monitoring, you can locate the resources (such as doors, elevators, alarm inputs, alarm outputs, etc.) on the map. For details, refer to ***Manage Map*** .
- **Add Persons:** Add person information and set person's credentials (such as PIN, issuing a card, fingerprint, etc.). For details, refer to ***Manage Person List*** .
- **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 and floors during the same authorized time period. For details, refer to ***Add Access Group*** .
- **Set Access Schedule:** The access schedule defines when the person can open the access point with credentials. For details, refer to ***Set Access Schedule Template*** .
- **Add Access Level and Assign to Access Group:** Access level is a group of doors and floors. After assigning the access level to certain access groups, it defines the access permission that which persons can get access to which doors and floors during the authorized time period. For details, refer to ***Manage Access Level*** .
- **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 or elevator control device of the doors/floors linked to the access level to take effect. After that, the persons in the access group can access these doors/floors 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 anti-passback, multi-door interlocking, multi-factor authentication, and entry & exit counting. For details about these configurations, refer to ***Configure Anti-Passback Rules*** , ***Configure Multi-Door Interlocking*** , ***Configure Multi-Factor Authentication Rules*** , and ***Add Entry and Exit Counting Group*** .
- **Operations on Control Client:** After the above configurations on the Web Client, you can control the door/floor's status during live view, view real-time access events, search history access records, etc. For details, refer to the *User Manual of HikCentral Professional Control Client*.

13.2 Manage Access Control Device

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

13.2.1 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

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

Before You Start

- Make sure the access control devices you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the 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. Click **Physical View → Access Control Device** to enter the Access Control Device Management page.
2. In the Online Device area, select a network type.

   Server Network

   As the default selection, the detected online devices in the same local subnet with the 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.

   Note

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

3. In the Online Device area, select **Hikvision Private Protocol** or **Hikvision ISUP Protocol** to filter the detected online devices.
4. In the Online Device area, select the active device to be added.
5. Click **Add to Device List** to open the Add Online Device window.
6. Enter the required information.

   Note

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

   Caution

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

Note

- You can import all the access points or the specified access point(s) of the device to the corresponding area.
- 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 any access point to an area, you cannot perform further configurations for the access point.

9. Click **Add**.
10. **Optional:** Perform the following operations after adding the online device.

Remote Configurations

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

Note

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

Change Password

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

Note

- 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 Application Settings

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

Add Detected Online Access Control Devices in a Batch

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

Before You Start

- Make sure the access control devices you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the 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. Click **Physical View → Access Control Device** to enter the Access Control Device Management page.
2. In the Online Device area, select a network type.

   Server Network

   The detected online devices in the same local subnet with the 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.

   Note

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

3. In the Online Device area, select **Hikvision Private Protocol** or **Hikvision ISUP Protocol** to filter the detected online devices.
4. In the Online Device area, select the active devices to be added.
5. Click **Add to Device List** to open the Add Online Device window.
6. 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.

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 the **Add Channel to Area** to on to import the access points of the added devices to an area.

Note

- You can import all the access points or the specified access point(s) of the device to the corresponding area.
- 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 access points to area, you cannot perform the further operations for the access points.

9. Click **Add**.
10. Perform the following operation(s) after adding the devices.

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

Note

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

Change Password

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

Note

- 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 Application Settings

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

13.2.2 Add Access Control Device by IP Address

When you know the IP address of an access control device to add, you can add the device to the system by specifying its IP address, user name, password, etc.

Before You Start

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

Steps

1. Click **Physical View → Access Control Device** to enter the Access Control Device Management page.
2. Click **Add** to enter the Add Access Control Device page.
3. Select **Hikvision Private Protocol** as the access protocol.

4. Select **IP Address** as the adding mode.
5. Enter the required parameters.

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.

6. **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.

7. **Optional:** Switch **Add Channel to Area** to on to import the access points of the added devices to an area.

Note

- You can import all the access points or the specified access point(s) of the device to the corresponding area.
- 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 any access point to an area, you cannot perform further operations for the access point.

8. Finish adding the device.
   - Click **Add** to add the access control device and back to the access control device list page.
   - Click **Add and Continue** to save the settings and continue to add next access control device.
9. Perform the following operation(s) after adding the devices.

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

Note

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

Change Password

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

Note

- 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 Application Settings

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

13.2.3 Add Access Control Devices by IP Segment

If the access control devices share a user name and password, and their IP addresses are in an IP segment, you can add them to the system by specifying the start IP address and the end IP address, user name, password, etc.

Before You Start

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

Steps

1. Click **Physical View → Access Control Device** to enter the Access Control Device Management page.
2. Click **Add** to enter the Add Access Control Device page.

3. Select **Hikvision Private Protocol** as the access protocol.
4. Select **IP Segment** as the adding mode.
5. 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.

6. **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.

7. **Optional:** Switch **Add Channel to Area** to on to import the access points of the added devices to an area.

Note

- You can create a new area by the device name or select an existing area.
- For 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 any access point to an area, you cannot perform further operations for the access point.

8. Finish adding the device.
   - Click **Add** to add the access control device and back to the access control device list page.
   - Click **Add and Continue** to save the settings and continue to add next access control device.
9. Perform the following operation(s) after adding the devices.

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

Note

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

Change Password

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

Note

- 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 Application Settings

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

13.2.4 Add Access Control Devices by Device ID

For the access control devices supporting ISUP 5.0 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 access control device without fixed IP address by HikCentral Professional.

Before You Start

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

Steps

1. Click **Physical View → Access Control Device** to enter the Access Control Device Management page.
2. Click **Add** to enter the Add Access Control Device page.

3. Select **Hikvision ISUP Protocol** as the Access Protocol.
4. Select **Device ID** as the adding mode.
5. Enter the required the information.
6. Set the **Picture Storage** switch to on 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

   You should store face picture library and captured pictures in the different locations.
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 Channel to Area** to on to import the channels of the added devices to an area.

   Note

   - You can create a new area by the device name or select an existing area.
   - For 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 any access point to an area, you cannot perform further operations for the access point.
9. Finish adding the device.
   - Click **Add** to add the access control device and back to the access control device list page.
   - Click **Add and Continue** to save the settings and continue to add other access control devices.
10. **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.

13.2.5 Add Access Control Devices by Device ID Segment

If you need to add multiple access control devices which have no fixed IP addresses and support ISUP 5.0 protocol to HikCentral 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 access control devices you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the HikCentral Professional via network.

Steps

1. Click **Physical View → Access Control Device** to enter the Access Control Device Management page.
2. Click **Add** to enter the Add Access Control Device page.
3. Select **Hikvision ISUP Protocol** as the Access Protocol.
4. Select **Device ID Segment** as the adding mode.
5. Enter the required parameters.
6. Set the **Picture Storage** switch to on 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

   You should store face picture library and captured pictures in the different locations.
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 Channel to Area** to on to import the channels of the added devices to an area.

Note

- You can create a new area by the device name or select an existing area.
- For 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 any access point to an area, you cannot perform further operations for the access point.

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

13.2.6 Add Access Control Devices in a Batch

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

Before You Start

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

Steps

1. Click **Physical View → Access Control Device** to enter the Access Control Device Management page.
2. Click **Add** to enter the Add Access Control Device page.
3. Select **Hikvision Private Protocol** or **Hikvision ISUP Protocol** as the Access Protocol.
4. Select **Batch Import** as the adding mode.
5. Click **Download Template** and save the predefined template (excel format) in your PC.
6. Open the downloaded template file and enter the required information of the devices to be added on corresponding columns.
7. Click ••• and select the edited file.
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. 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.
10. Perform the following operation(s) after adding devices in a batch.

Remote Configurations

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

Note

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

Change Password

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

Note

- 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 Application Settings

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

13.2.7 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 parameter to communicate between the device and the third-party card readers.

Before You Start

Wire the third-party card readers to the access control device.

Steps

Note

- By default, the device disables the custom Wiegand function. If the device enables the custom Wiegand function, all wiegand interfaces in the device will use the customized wiegand protocol.
- Up to 5 custom Wiegands can be set.

1. Click **Physical View** on the Home page, and then select **Access Control Device**.
2. Click ⚙ to enter the remote configuration page.
3. Set the **Custom Wiegand** switch to on.

   The Wiegand parameters appear.
4. 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 followings:

   Odd Start, Length

   If the odd parity start bit is 1, and the length is 12, then the system 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 system 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 followings:

   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 system 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 as an 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 access control device's linkage actions for the access control device's triggered event. After that, when an event is triggered, it can trigger the alarm output, buzzer on access controller, and other actions.

Steps

Note

The function should be supported by the device.

1. Click **Physical View** on the Home page, and then select **Access Control Device**.
2. Click ⚙ to enter the remote configuration page.
3. Click **Add** on the Linkage section to enter the Linkage page.
4. Set 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 from the drop-down list besides.

   Note

   - If you select alarm input event, you should select an alarm input.
   - If you select door event, you should select a door.
   - If you select a card reader event, you should select a card reader.
5. Configure linkage target.

   Buzzing

   If the specified event is triggered, the buzzer (buzzer on the access control device or card reader) will start buzzing or stop buzzing.

   Buzzer on Controller

   ON

   If the specified event is triggered, the buzzer on the access control device will start buzzing.

   OFF

   If the specified event is triggered, the buzzer on the access control device will stop buzzing.

   No Linkage

   This linkage action is disabled. The buzzer action will not be triggered when the specified MAC address is detected.

   Buzzer on Reader

   ON

   If the specified event is triggered, the buzzer on the selected card reader will start buzzing.

   OFF

   If the specified event is triggered, the buzzer on the selected card reader will stop buzzing.

   No Linkage

This linkage action is disabled. The buzzer action will not be triggered when the specified MAC address is detected.

Capture & Recording

Check **Capture** to enable the device's linked camera to capture a picture when the specified MAC address is detected.

Check **Recording** to enable the device's linked camera to record video footage when the specified MAC address is detected.

Alarm Output

ON

If the specified event is triggered, the selected alarm output will be triggered.

OFF

If the specified event is triggered, the selected alarm output will be stopped.

No Linkage

This linkage action is disabled. The alarm output action will not be triggered when the specified MAC address is detected.

Access Point

Unlock

If the specified event is triggered, the selected door will be unlocked.

Lock

If the specified event is triggered, the selected door will be locked.

Remain Unlocked

If the specified event is triggered, the selected door will remain unlocked.

Remain Locked

If the specified event is triggered , the selected door will remain locked.

No Linkage

This linkage action is disabled. The door action will not be triggered when the specified MAC address is detected.

6. Click **Save**.
7. **Optional:** Perform the following operations after adding a linkage

Delete Linkage Settings	Select the configured linkage in the linkage list and click × to delete it.
Edit Linkage Settings	Select the configured linkage in the linkage list and click ✎ to edit the linkage.

Configure Device Actions for Card Swiping

You enable access control device's linkage actions (such as disarming a zone and triggering audio prompt) for the swiping of a specific card, In this way, you can monitor the card holder's behaviors and whereabouts.

Steps

Note

The function should be supported by the device.

1. Click **Physical View** on the Home page, and then select **Access Control Device**.
2. Click ⚙ to enter the remote configuration page.
3. Click **Add** on the Linkage section to enter the Linkage page.
4. Set the 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.
5. Configure linkage target.

   Buzzing

   If the card holder is swiping the specified card on the specified card reader, the buzzer (buzzer on the access control device or card reader) will start buzzing or stop buzzing.

   Buzzer on Controller

   ON

   If the card holder is swiping the specified card on the specified card reader, the buzzer on the access control device will start buzzing.

   OFF

   If the card holder is swiping the specified card on the specified card reader, the buzzer on the access control device will stop buzzing.

   No Linkage

   This linkage action is disabled. The buzzer action will not be triggered when the specified MAC address is detected.

   Buzzer on Reader

   ON

   If the card holder is swiping the specified card on the specified card reader, the buzzer on the selected card reader will start buzzing.

   OFF

   If the card holder is swiping the specified card on the specified card reader, the buzzer on the selected card reader will stop buzzing.

No Linkage

This linkage action is disabled. The buzzer action will not be triggered when the specified MAC address is detected.

Capture & Recording

Check **Capture** to enable the device's linked camera to capture a picture when the specified MAC address is detected.

Check **Recording** to enable the device's linked camera to record video footage when the specified MAC address is detected.

Alarm Output

ON

If the card holder is swiping the specified card on the specified card reader, the selected alarm output will be triggered.

OFF

If the card holder is swiping the specified card on the specified card reader, the selected alarm output will be stopped.

No Linkage

This linkage action is disabled. The alarm output action will not be triggered when the specified MAC address is detected.

Zone

ON

If the card holder is swiping the specified card on the specified card reader, the selected zone will be armed.

OFF

If the card holder is swiping the specified card on the specified card reader, the selected zone will be disarmed.

No Linkage

This linkage action is disabled. The zone action will not be triggered when the specified MAC address is detected.

Access Point

Unlock

If the card holder is swiping the specified card on the specified card reader, the selected door will be unlocked.

Lock

If the card holder is swiping the specified card on the specified card reader, the selected door will be locked.

Remain Unlocked

If the card holder is swiping the specified card on the specified card reader, the selected door will remain unlocked.

Remain Locked

If the card holder is swiping the specified card on the specified card reader, the selected door will remain locked.

No Linkage

This linkage action is disabled. The door action will not be triggered when the specified MAC address is detected.

6. Click **Save**.
7. **Optional:** Perform the following operations after adding a linkage

Delete Linkage Settings	Select the configured linkage in the linkage list and click × to delete it.
Edit Linkage Settings	Select the configured linkage in the linkage list and click ✎ to edit the linkage.

Configure Device Actions for Person ID

You can set the access control device's linkage actions for the specified person ID. When access control device detects the specified person ID, it can trigger the alarm output, buzzer on card reader, and other actions, so as to implement special monitoring on the specified person.

Steps

Note

The function should be supported by the device.

1. Click **Physical View** on the Home page, and then select **Access Control Device**.
2. Click ⚙ to enter the remote configuration page.
3. Click **Add** on the Linkage section to enter the Linkage page.
4. Set the 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.
5. Configure linkage target.

Buzzing

If the specified person is detected when he or she swiping card on the specified card reader, the buzzer (buzzer on the access control device or card reader) will start buzzing or stop buzzing.

Buzzer on Controller

ON

If the specified person is detected when he or she swiping card on the specified card reader, the buzzer on the access control device will start buzzing.

OFF

If the specified person is detected when he or she swiping card on the specified card reader, the buzzer on the access control device will stop buzzing.

No Linkage

This linkage action is disabled. The buzzer action will not be triggered when the specified MAC address is detected.

Buzzer on Reader

ON

If the specified person is detected when he or she swiping card on the specified card reader, the buzzer on the selected card reader will start buzzing.

OFF

If the specified person is detected when he or she swiping card on the specified card reader, the buzzer on the selected card reader will stop buzzing.

No Linkage

This linkage action is disabled. The buzzer action will not be triggered when the specified MAC address is detected.

Capture & Recording

Check **Capture** to enable the device's linked camera to capture a picture when the specified MAC address is detected.

Check **Recording** to enable the device's linked camera to record video footage when the specified MAC address is detected.

Alarm Output

ON

If the specified person is detected when he or she swiping card on the specified card reader, the selected alarm output will be triggered.

OFF

If the specified person is detected when he or she swiping card on the specified card reader, the selected alarm output will be stopped.

No Linkage

This linkage action is disabled. The alarm output action will not be triggered when the specified MAC address is detected.

Zone

ON

If the specified person is detected when he or she swiping card on the specified card reader, the selected zone will be armed.

OFF

If the specified person is detected when he or she swiping card on the specified card reader, the selected zone will be disarmed.

No Linkage

This linkage action is disabled. The zone action will not be triggered when the specified MAC address is detected.

Access Point

Unlock

If the specified person is detected when he or she swiping card on the specified card reader, the selected door will be unlocked.

Lock

If the specified person is detected when he or she swiping card on the specified card reader, the selected door will be locked.

Remain Unlocked

If the specified person is detected when he or she swiping card on the specified card reader, the selected door will remain unlocked.

Remain Locked

If the specified person is detected when he or she swiping card on the specified card reader, the selected door will remain locked.

No Linkage

This linkage action is disabled. The door action will not be triggered when the specified MAC address is detected.

6. Click **Save**.
7. **Optional:** Perform the following operations after adding a linkage

Delete Linkage Settings

Select the configured linkage in the linkage list and click × to delete it.

Edit Linkage Settings

Select the configured linkage in the linkage list and click ✎ to edit the linkage.

Configure Device Actions for MAC Address

You can set the access control device's linkage actions for the specified MAC address of mobile terminal. When access control device detects the specified MAC address, it can trigger the alarm output, host buzzer, and other actions.

Steps

Note

The function should be supported by the access control device.

1. Click **Physical View** on the Home page, and then select **Access Control Device**.
2. Click ⚙ to enter the remote configuration page.
3. Click **Add** on the Linkage section to enter the Linkage page.
4. Select **MAC Linkage** as the linkage type, and then enter the MAC address.

   Note

   MAC Address Format: AA:BB:CC:DD:EE:FF.

5. Configure linkage target.

   Buzzing

   If the specified MAC address is detected, the buzzer (buzzer on the access control device or card reader) will start buzzing or stop buzzing.

   Buzzer on Controller

   ON

   If the specified MAC address is detected, the buzzer on the access control device will start buzzing.

   OFF

   If the specified MAC address is detected, the buzzer on the access control device will stop buzzing.

   No Linkage

   This linkage action is disabled. The buzzer action will not be triggered when the specified MAC address is detected.

   Buzzer on Reader

   ON

   If the specified MAC address is detected, the buzzer on the selected card reader will start buzzing.

   OFF

   If the specified MAC address is detected, the buzzer on the selected card reader will stop buzzing.

   No Linkage

   This linkage action is disabled. The buzzer action will not be triggered when the specified MAC address is detected.

   Capture & Recording

Check **Capture** to enable the device's linked camera to capture a picture when the specified MAC address is detected.

Check **Recording** to enable the device's linked camera to record video footage when the specified MAC address is detected.

Alarm Output

ON

If the specified MAC address is detected, the selected alarm output will be triggered.

OFF

If the specified MAC address is detected, the selected alarm output will be stopped.

No Linkage

This linkage action is disabled. The alarm output action will not be triggered when the specified MAC address is detected.

Access Point

Unlock

If the specified MAC address is detected, the selected door will be unlocked.

Lock

If the specified MAC address is detected, the selected door will be locked.

Remain Unlocked

If the specified MAC address is detected, the selected door will remain unlocked.

Remain Locked

If the specified MAC address is detected , the selected door will remain locked.

No Linkage

This linkage action is disabled. The door action will not be triggered when the specified MAC address is detected.

6. Click **Save**.
7. **Optional:** Perform the following operations after adding a linkage

Delete Linkage Settings	Select the configured linkage in the linkage list and click × to delete it.
Edit Linkage Settings	Select the configured linkage in the linkage list and click ✎ to edit the linkage.

Configure Card Swiping Parameters

You can configure card swiping parameters to allow authentication by inputting card number on keypad, eanble NFC anti-cloning, and Mifare encryption.

Steps

1. Click **Physical View** on the Home page, and then select **Access Control Device**.
2. Click ⚙ to enter the remote configuration page and go to the Card Swiping section.
3. Configure card swiping parameters.

Note

The parameters vary with different models of access control devices.

Input Card Number On Keypad

If checked, visitors are allowed to input card number on keypad to authenticate their identities.

Enable NFC Card

If enabled, visitors cannot use the cloned cards for authentication.

Mifare Encryption

If enabled, only the card with the same encrypted sector can be granted by swiping the card on the card reader.

Voice Prompt

If you enable this function, the voice prompt will be enabled on the device. You can hear the voice prompt when operating on the device.

Upload Picture after linked Capture

Upload the pictures captured by the camera(s) which related to the door(s) under the access control device to the system automatically.

Note

You can relate a camera to a door in the Logical View module. For details, see ***Edit Door for Current Site*** .

Picture Storage

If checked, the captured picture(s) will be automatically saved to the storage location you configured in picture storage settings for the door(s) under the access control device.

Note

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

Picture Size

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

Picture Quality

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

Configure Other Parameters

You configure other parameters for the access control device, such as device time and facial recognition mode.

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 the Device Time field to custom time for the device.

Sync with Server Time

Synchronize the device time with that of the server of the system.

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 access control 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 should be activated after restoring.

Facial Recognition Mode

You can check **Deep Mode** to enable the function. After that, all the face credentials applied to the device will be cleared. Go to Access Group page and click **Apply to Device** to apply the data in the system to the device.

13.3 Manage Elevator Control Device

You can add the elevator control device to the system to control the elevator(s), such as assign the access authority of specified floors to person, control the elevator status on the Control Client.

13.3.1 Add Elevator Control Device by IP Address

When you know the IP address of an elevator control device to add, you can add the device to the system by specifying its IP address, user name, password, etc.

Before You Start

Make sure the elevator 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. Click **Physical View → Elevator Control Device** to enter the Elevator Control Device Management page.
2. Click **Add** to enter the Add Elevator Control Device page.
3. Select **IP Address** as the adding mode.
4. Enter the required parameters.

   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.

5. **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.

6. **Optional:** Switch **Add Channel to Area** to on to import the channels (including alarm inputs, alarm outputs and floors) of the added elevator control device to an area.

   Note

   - 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 further operations for the channels.
   - Enter the range of floor No. according to the application scene.

     Note

     You can apply the floor name according to the floor range you set in the logical view.

7. Finish adding the device.
   - Click **Add** to add the elevator control device and back to the elevator control device list page.
   - Click **Add and Continue** to save the settings and continue to add next elevator control device.
8. Perform the following operation(s) after adding the devices.

Remote Configurations

Click ⚙ to edit the time parameters, enable RS-485 communication redundancy, configure the linkage action, reboot the device, restore the device, or set other configurations of the corresponding device.

Note

- After restoring the device, you need to apply the parameters in the system to the device (click **Apply Application Settings** on Elevator Control Device Management page).
- For details about remote configuration, see the user manual of the device.

Change Password

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

Note

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

13.3.2 Add Elevator Control Device by IP Segment

If the elevator control devices share a user name and password, and their IP address are in an IP segment, you can add them to the system by specifying the start IP address and the end IP address, user name, password, etc.

Before You Start

Make sure the elevator 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. Click **Physical View → Elevator Control Device** to enter the Elevator Control Device Management page.
2. Click **Add** to enter the Add Elevator Control Device page.
3. Select **IP Segment** as the adding mode.
4. Enter the required parameters.

   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.

5. **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.

6. **Optional:** Switch **Add Channel to Area** to on to import the channels (including alarm inputs, alarm outputs and floors) of the added elevator control device to an area.

   Note

   - 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 further operations for the channels.
   - Enter the range of floor No. according to the application scene.

     Note

     You can apply the floor name according to the floor range you set in the logical view.

7. Finish adding the device.
   - Click **Add** to add the elevator control device and back to the elevator control device list page.
   - Click **Add and Continue** to save the settings and continue to add next elevator control device.
8. Perform the following operation(s) after adding the devices.

   Remote Configurations

   Click ⚙ to edit the time parameters, enable RS-485 communication redundancy, configure the linkage action, reboot the device, restore the device, or set other configurations of the corresponding device.

   Note

   - After restoring the device, you need to apply the parameters in the system to the device (click **Apply Application Settings** on Elevator Control Device Management page).
   - For details about remote configuration, see the user manual of the device.

   Change Password

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

   Note

   - 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 Application Settings

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

13.3.3 Add Elevator Control Devices in a Batch

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

Before You Start

Make sure the elevator 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. Click **Physical View → Elevator Control Device** to enter the Elevator Control Device Management page.
2. Click **Add** to enter the Add Elevator Control Device page.
3. Select **Batch Import** as the adding mode.
4. Click **Download Template** and save the predefined template (excel file) in your PC.
5. Open the exported template file and edit the required information of the devices to be added on the corresponding column.
6. Click ⋯ and select the template file.
7. **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. 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.
9. Perform the following operation(s) after adding the devices.

Remote Configurations

Click ⚙ to edit the time parameters, enable RS-485 communication redundancy, configure the linkage action, reboot the device, restore the device, or set other configurations of the corresponding device.

Note

- After restoring the device, you need to apply the parameters in the system to the device (click **Apply Application Settings** on Elevator Control Device Management page).
- For details about remote configuration, see the user manual of the device.

Change Password

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

Note

- 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 Application Settings

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

13.4 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 and floors (the doors and floors in the linked access level) during the same authorized time period. You need to assign the access level to the access group so that these persons in the access group can access the doors and floors in the access level.

Before You Start

Add person to the system. For details, refer to ***Manage Person List*** .

Steps

1. Click **Person → Access Group → Add** to enter the adding access group page.

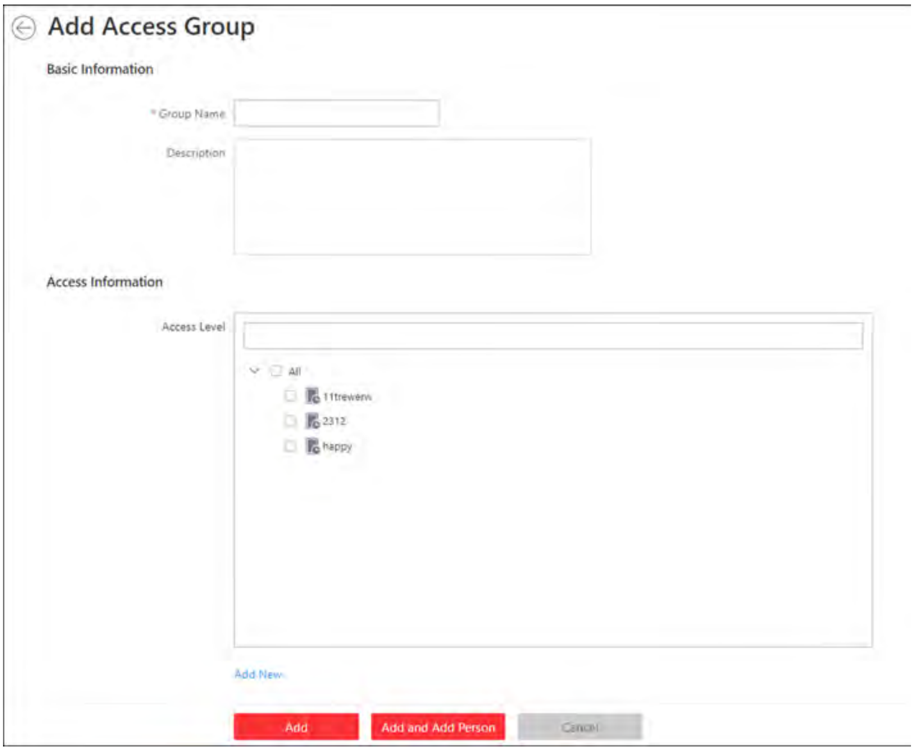


Figure 13-2 Add Access Group

2. Set the basic information.

   Group Name

   Create a name for the access group.

   Description

   Enter the descriptive information for the group. E.g., This access group is for security guards in Team A.

3. **Optional:** Select the access levels to link the access group with these access levels so that the persons in this access group can access the doors and floors in the access level(s) during the authorized time period.

   Note

   - Move the cursor to the access level and you can view its doors and floors and access schedule.
   - Up to 8 access levels can be assigned to one access group.
   - You can click **Add New** to add a new access level. For details, refer to ***Add Access Level*** .

4. **Optional:** If the persons in the existing person group share the same access level, you can enable **Relate to Person Group** to link this access group with existing person group(s).
   1) Set the **Relate to Person Group** switch to ON.
   2) Select existing person group(s) to relate the current access group to the selected person group(s).

After related, the persons in the selected person groups will be added to the current access group and assigned with the access levels of the current access group. If you add more persons to the related person groups later, these newly added persons will be added to this access group automatically. In addition, if you edit the persons in the related person groups or remove persons from the related person groups, these edited or removed persons will be edited/ removed in/from this access group automatically.

5. Confirm to add the access group.
   - To add persons to the access group, click **Add and Add Person** and perform the following steps.

     Note

     If you have enabled **Relate to Person Group** and selected person group(s) to relate, you cannot add more persons when adding this access group. If you click **Add and Add Person**, this function will be disabled.
   - To save the access group first and add persons to the access group later, click **Add** to finish this task and return to the access group list.
6. **Optional:** If you click **Add and Add Person**, you will enter the next page to add persons to this access group.
   1) In the **Add from** field, choose to add existing persons or add a new person to this group.

      Existing Person

      Add existing persons in the system to this access group.

      Add New Person

      Add a new person to this access group. The person will be added to the person list as well.
   2) **Optional:** If you select **Existing Persons**, you can select persons from the person list or other groups.

      Person List

      Filter persons in the person list by entering keywords of person name, person group name, or additional information.

      Note

      You can click **Additional Information** to enable the custom additional information as search condition.

      Access Group

      Add all the persons in the selected access group(s) to this access group.

      Attendance Group

      Add all the persons in the selected attendance group(s) to this access group.
7. Click **Add** to add the selected persons to the access group.
8. **Optional:** After adding the access group, you can do one or more of the followings.

   Edit Access Group Click ✎ in the Operation column to edit its details.

Manage Persons in Access Group

Click the added access 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 issuing cards, importing and exporting persons. For details, refer to ***Manage Person List*** .

Delete Access Group

Select one access group and click **Delete** to delete it.

Delete All Access Groups

Click **Delete All** to delete all the added access groups.

13.5 Manage Access Level

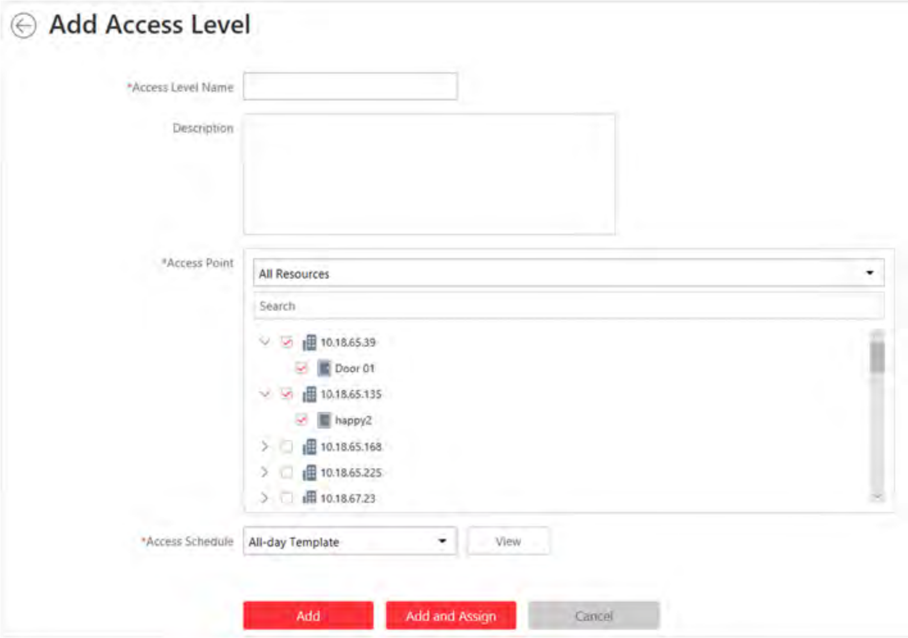
In access control, access level is a group of doors and floors. After assigning the access level to certain access groups, it defines the access permission that which persons can get access to which doors and floors during the authorized time period.

13.5.1 Add Access Level

To define the access permission, you need to add an access level first and group the access points (doors and floors).

Steps

1. Click **Access Level** on the Home page to enter the access level management page.
2. Click **Add**.



Add Access Level

*Access Level Name

Description

*Access Point: All Resources

Search

- ☑ 10.18.65.39
  - ☑ Door 01
- ☑ 10.18.65.135
  - ☑ happy2
- □ 10.18.65.168
- □ 10.18.65.225
- □ 10.18.67.23

*Access Schedule: All-day Template

Figure 13-3 Add Access Level

3. Create a name for the access level.
4. **Optional:** Enter the description for the access level.
5. Select the access point(s) to add to the access level.
   1) Select the type of access points from the drop-down list.

      All Resources

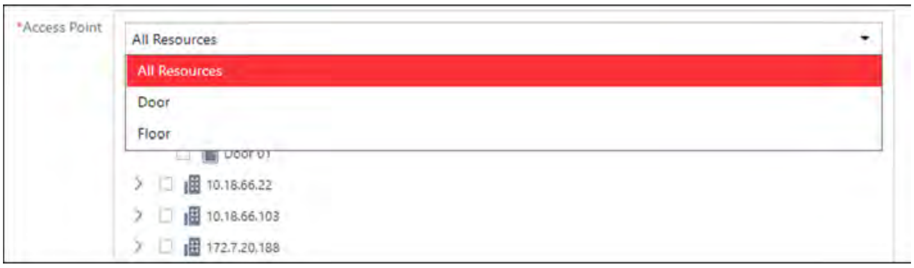
      Both doors and floors managed in the system will be display.

      Door

      Only doors will be displayed. The doors will be displayed by area.

      Floor

      Only floors will be displayed. You can set the display the floors by area or by floor No.



*Access Point: All Resources

- □ Door 01
- □ 10.18.66.22
- □ 10.18.66.103
- □ 172.7.20.188

Figure 13-4 Select Access Point Type

   2) Select the doors or floors.
6. Select the access schedule to define in which time period, the persons are authorized to access the doors and floors (selected in step 5).

Note

The default and customized access schedules are displayed in the drop-down list. You can click **Add New** to customize a new schedule. For details, refer to ***Set Access Schedule Template*** .

7. Finish adding the access level.
- Click **Add** to add the access level and return to the access level management page.
- Click **Add and Assign** to assign the access level to some access groups (including access groups for persons and access groups for visitors) so that the persons in the access groups will have the access permission to access the doors and floors selected in step 5.

  Note

  - For details about assigning the access level to the access group, refer to ***Assign Access Level to Access Group*** .
  - For setting the access group, refer to ***Add Access Group*** and ***Add Access Group for Visitors*** .

8. **Optional:** After adding the access level, you can do one or more of the followings.

Edit Access Level	Click ✎ in the Operation column to edit its details. If you want to change the assigned access group(s), or assign it to another access group, click **Configuration**.
Assign to Access Group	Click ✍ in the Operation column to assign the access level to the added access groups. For details, refer to ***Assign Access Level to Access Group*** .
Delete Access Level	Click × in the Operation column to delete the access level.
Delete All Access Levels	Click **Delete All** to delete all the added access levels.

13.5.2 Assign Access Level to Access Group

After adding the access level, you need to assign it to access group(s). After that, the persons in the access group(s) will have the permission to access the access point(s) linked to the access level.

Before You Start

Add the access group(s). For details, refer to ***Add Access Group*** .

Steps

Note

You can also link the access group to access level(s) when adding or editing the access group. The latest configured linkage will take effect. For details, refer to ***Add Access Group*** .

1. Click **Access Level** on the Home page to enter the access level management page.

2. Enter the Assign to Access Group page.

- After you setting the parameters of access level when adding, click **Add and Assign**.
- When editing the access level, click **Configuration** in the access level details page.
- Click in the Operation column.

3. In the **Assign to Access Group** field, select the access group(s) (including access groups for persons and access groups for visitors) so that the persons in the access groups will have the access permission to access the doors and floors in the access level.
4. **Optional:** Click **Add New** to add a new access group.
5. Click **Save**.

13.6 Apply Persons' Access Levels to Device

After setting the linkage between access group and access levels, or if the person's access level and access group settings are changed, you need to apply the person's access level settings to the access control device or elevator control device of the doors/floors linked to the access level to take effect. After that, the persons in the access group can access these doors/floors during the authorized time period defined by the related access level.

13.6.1 Manually Apply Persons' Access Levels to Device

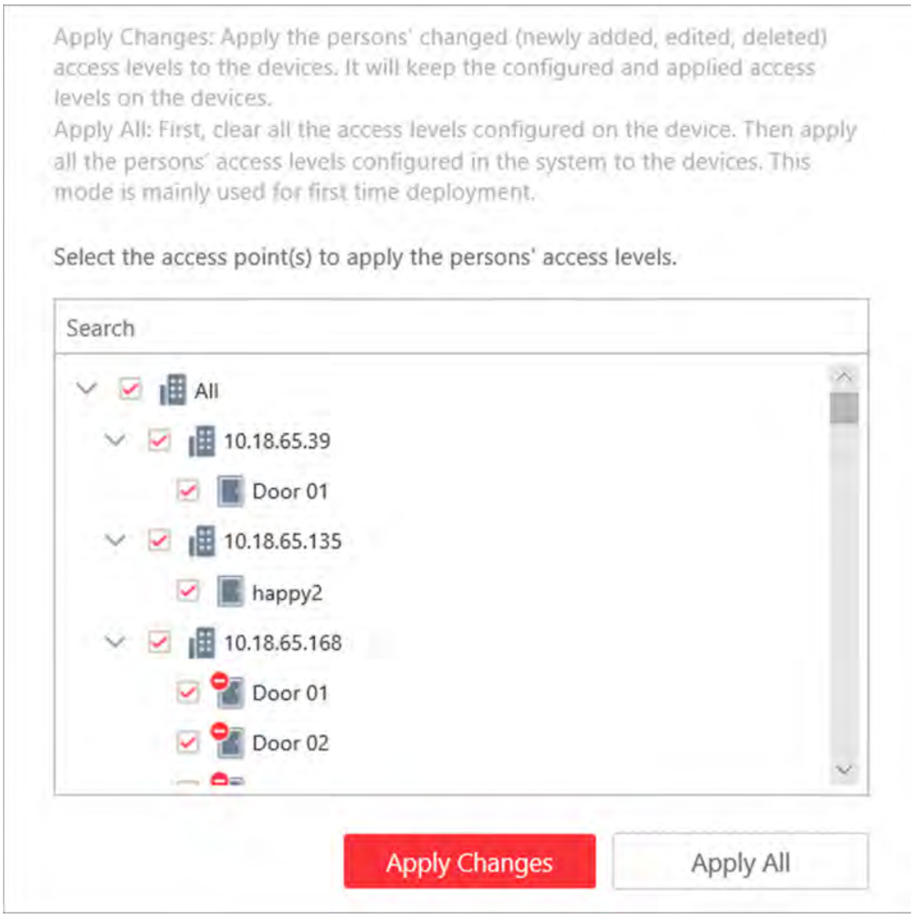
After setting the access levels and assigning access levels to access group, you should apply the relation between persons and access points to the access control device. In other words, after setting or changing the access groups and access levels, you need to apply these settings to the access control device to take effect.

Before You Start

Link the access group with access level to define the access permission. For details, refer to ***Assign Access Level to Access Group*** or ***Add Access Group*** .

Steps

1. Click **Person → Access Group** to enter the access group management page.
2. Click **Apply to Device** to open the Apply window.



Apply Changes: Apply the persons' changed (newly added, edited, deleted) access levels to the devices. It will keep the configured and applied access levels on the devices.

Apply All: First, clear all the access levels configured on the device. Then apply all the persons' access levels configured in the system to the devices. This mode is mainly used for first time deployment.

Select the access point(s) to apply the persons' access levels.

Figure 13-5 Apply to Device Manually

3. Select the access point(s) to apply the persons' access levels.

4. Select the applying mode.

Apply Changes

Apply the persons' changed (newly added, edited, deleted) access levels to the devices. It will keep the configured and applied access levels on the devices.

Apply All

First, clear all the access levels configured on the device. Then, apply all the persons' access levels configured in the system to the devices. This mode is mainly used for first time deployment.

During this process, the devices will be offline for a while, and persons cannot access via these access points.

5. Optional: If the person's access permission settings are changed (such as changes in linked access level, person credentials, etc.), the ⓘ icon will display near the **Apply to Device** icon, indicating that these new access permission settings should be applied to the device. You can hover the cursor to it to view how many persons' access levels should be applied to the device.

13.6.2 Regularly Apply Person's Access Levels to Devices

Besides manually applying to device, you can also set a schedule and the system can apply the access levels assigned to persons configured in the system to the device automatically every day.

Before You Start

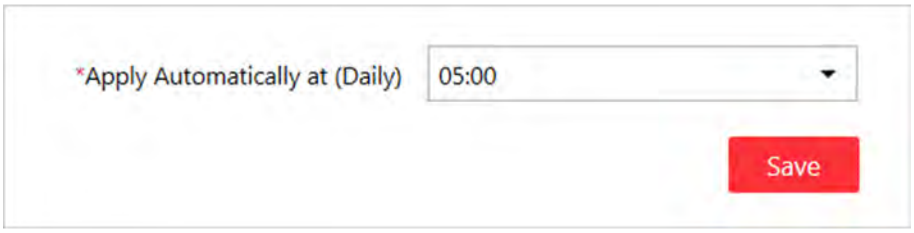
Link the access group with access level to define the access permission. For details, refer to ***Assign Access Level to Access Group*** or ***Add Access Group*** .

Steps

Note

By default, the system will apply the persons' access levels automatically to the device at 01:00 every day.

1. Click **Person → Access Group** to enter the access group management page.
2. Click **Apply to Device (Scheduled)** to open the following window.



*Apply Automatically at (Daily) 05:00

Figure 13-6 Apply to Device Regularly

3. Set a time and the system will apply the changed access levels linked with persons, as well as the applying failed access levels, to device at the configured time automatically.

   Note

   The time here is the SYS server's time.

4. Click **Save**.

13.7 Set Access Schedule Template

The access schedule defines when the person can open the access point with credentials, or when the access point remains unlocked so that person can open the access point with free access. The system predefines three default access control schedule templates: All-day Template, Weekday Template, and Weekend Template. You can also add a customized template according to actual needs.

Steps

1. Click **System** on the home page.
2. Click **Schedule → Access Schedule Template** tab on the left.
3. Click **Add** in the Access Schedule page to enter the adding access schedule template page.

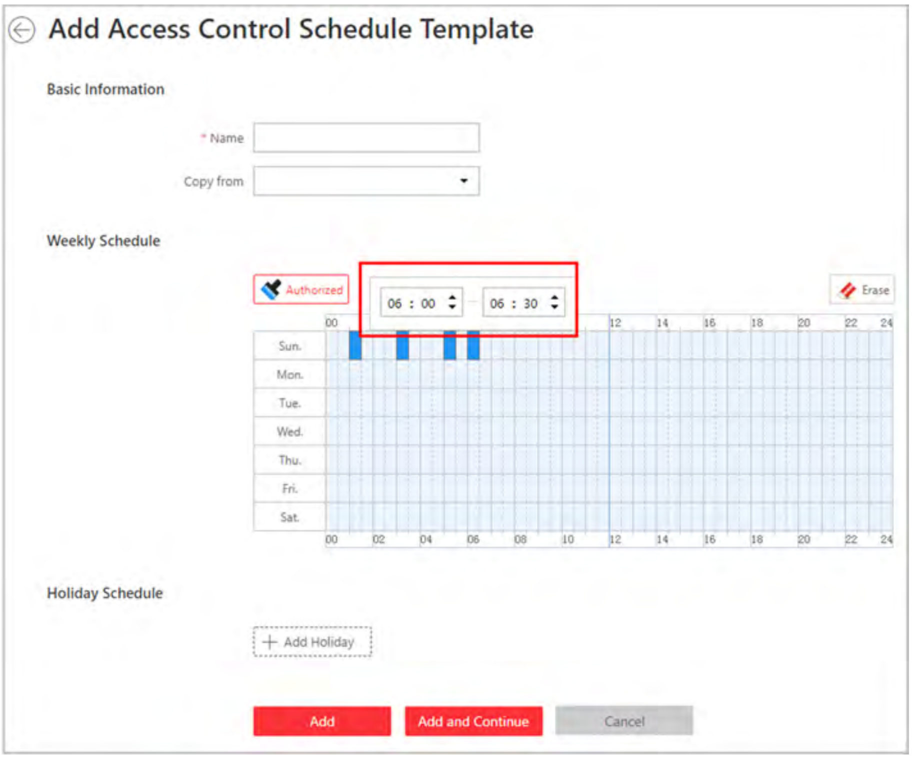


Figure 13-7 Set Access Control Schedule Template

4. Set the required information.

   Name

   Create a name for the template.

   Copy from

   Optionally, you can select to copy the settings from other defined templates.

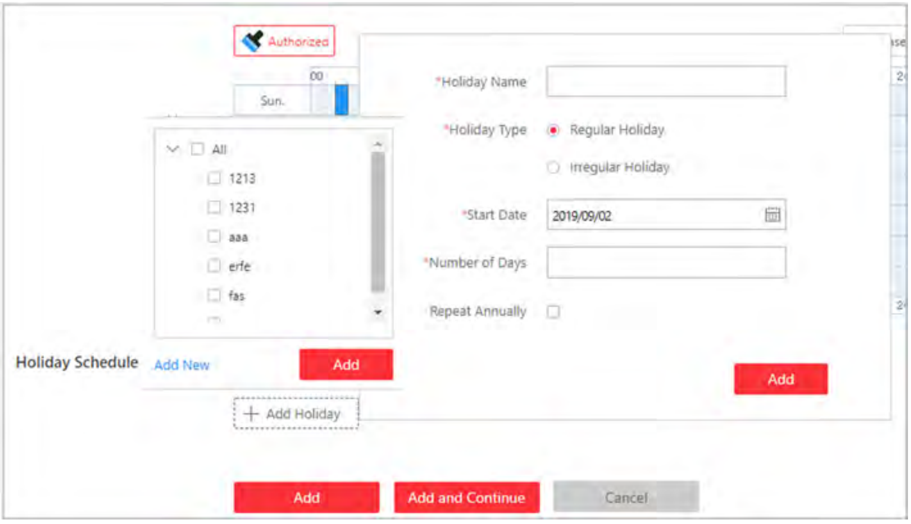
5. Click a time period on the time bar, and enter the start time and end time of the time period.

Note

Up to 8 time periods can be set for each day.

6. **Optional:** Click **Erase** and click on the drawn time period to clear the corresponding drawn time period.
7. **Optional:** Set the holiday schedule if you want to set different schedules for some special days. The priority of holiday schedule is higher than the weekly schedule which means the predefined holidays will adopt the holiday schedule rather than the weekly schedule.

   1) Click **Add Holiday**.



*Holiday Name

*Holiday Type ● Regular Holiday ○ Irregular Holiday

*Start Date 2019/09/02

*Number of Days

Repeat Annually □

Figure 13-8 Add Holiday Schedule

2) Select the predefined holiday(s), or click **Add New** to create a new holiday (see ***Set Holiday*** for details).
3) Click **Add**.
4) Draw a time period on the time bar.

Note

Up to 8 time periods can be set for each day.

5) **Optional:** Click **Erase** and click on the drawn time period to clear the corresponding drawn time period.

8. Finish adding the access schedule template.

- Click **Add** to add the template and back to the access schedule template list page.
- Click **Add and Continue** to add the template and continue to add other template.

The access schedule template will be displayed on the access schedule template list.

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

View Template Details	Click the template to view its details.
Edit Template	Click ✎ in the Operation column to edit template details.
Delete Template	Click × in the Operation column to delete the template.
Delete All Templates	Click **Delete All** to delete all the schedule templates (except the default templates and the template(s) in use).

13.8 Access Control Test

HikCentral Professional provides **Access Control Test** function. 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, elevator control, and video intercom) are set correctly and completely and whether the devices are running properly.

Click **Access Control Test** on the Home page.

Check Credential Status

Click **Credential Status** tab to view the status of the added credentials.

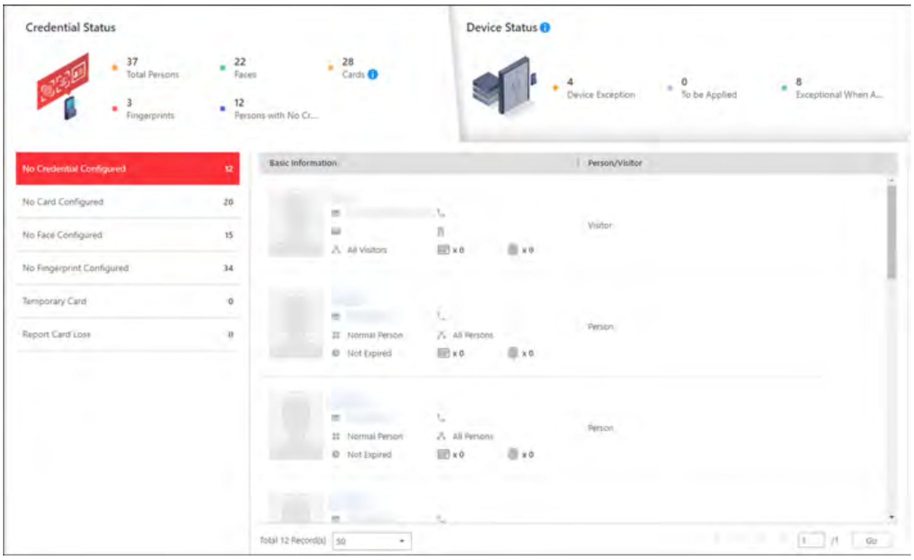


Figure 13-9 Credential Status

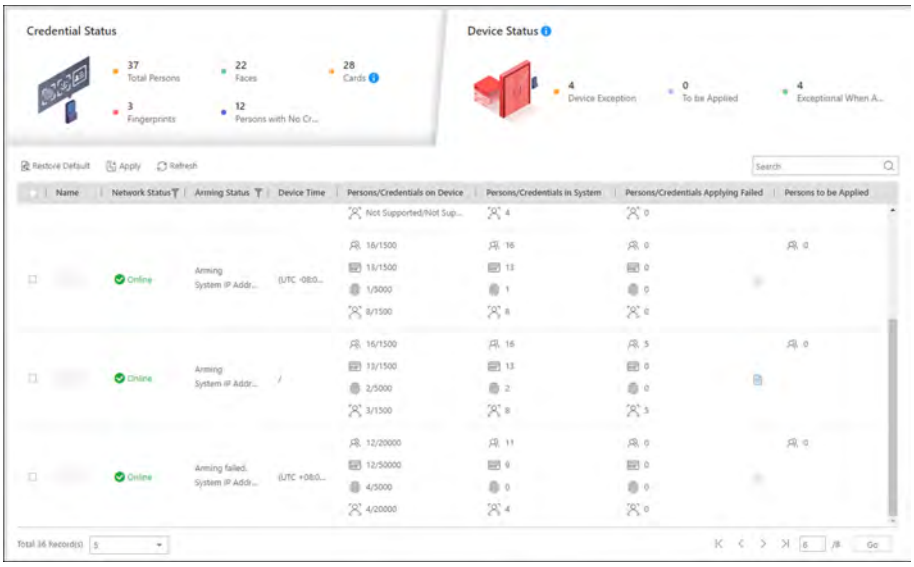
There are six types of exceptions about credential settings in the system. The numbers after these exception types indicate the number of persons and visitors whose credential settings are exceptional.
Click these exception types to view the information of the persons and visitors.
You can click the name to edit the credentials if necessary.

Check Device Status

Click **Device Status** tab to view the status of the devices (including access control devices, elevator control devices, and video intercom devices), and you can check the person information and credential information that are already applied to the devices, configured in the system, applying to devices failed, and persons to be applied to the devices.

Note

Only the status of the devices which have been configured with access levels will be displayed here.



Credential Status

37	Total Persons
22	Faces
28	Cards
3	Fingerprints
12	Persons with No Cr...

Device Status

4	Device Exception
0	To be Applied
4	Exceptional When A...

	Name	Network Status	Arming Status	Device Time	Persons/Credentials on Device	Persons/Credentials in System	Persons/Credentials Applying Failed	Persons to be Applied
					Not Supported/Not Sup...	4	0	
□		Online	Arming System IP Addr...	(UTC -08:0...	16/1500 13/1500 1/5000 8/1500	16 13 1 8	0 0 0 0	0
□		Online	Arming System IP Addr...	/	16/1500 13/1500 2/5000 3/1500	16 13 2 8	5 0 0 5	0
□		Online	Arming failed. System IP Addr...	(UTC +08:0...	12/20000 12/50000 4/5000 4/20000	11 9 0 4	0 0 0 0	0

Figure 13-10 Device Status

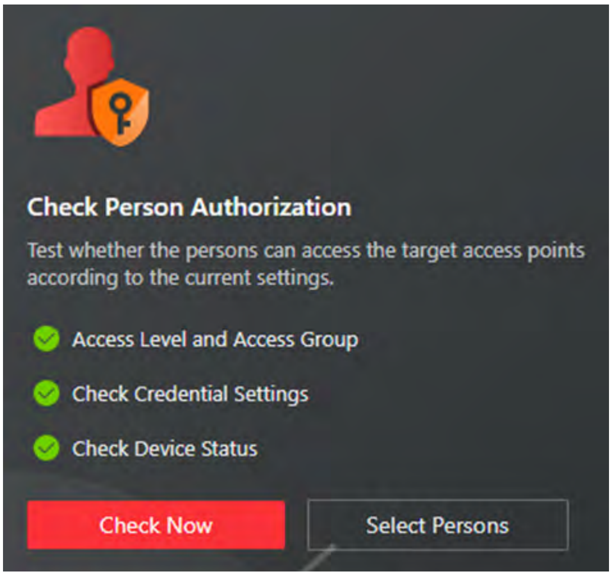
In the **Persons/Credentials Applying Failed** column, click 🗎 to view the detailed person information whose credentials fail to apply to the device and which credential fails.

You can select the device(s) and click **Apply** to apply the person information and credential settings to these devices again.

You can also select the device(s) and click **Restore Default** to restore the settings on the devices to the default value.

Check Authorization Settings of Persons/Visitors

You can check the authorization settings (such as access levels and access group settings, credential settings, and applying status) of specified persons or visitors in the system. This function helps you to test whether the persons can access the target access points according to the current settings.



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 13-11 Check Authorization Settings

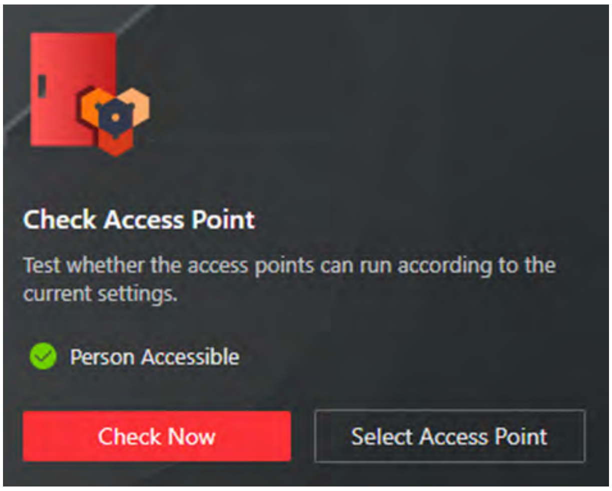
Click **Check Now** to test the authorization settings of all the existing persons and visitors.
Click **Select Persons** to select the persons or visitors you want to test and click **Check Now** to test the authorization settings of the selected persons or visitors.

Note

The persons who are not added to any access groups will not be checked.

Check Access Point Settings

You can test whether the persons can access the access points according to the settings in the system.



Check Access Point

Test whether the access points can run according to the current settings.

✓ Person Accessible

Figure 13-12 Check Access Point Settings

Click **Check Now** to test the settings of all the existing access points in the system.
Click **Select Access Points** to select the access points you want to test and 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.

13.9 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. Click **Logical View** on the Home page.
2. Choose one of the following methods to enter the area's resource group page.
   - Select one area and click ✎ to enter the editing area page.

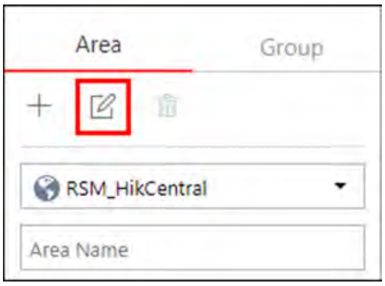


Figure 13-13 Enter Area Editing Page

   - Select **Group** tab on the left to display all the resource groups of different areas.

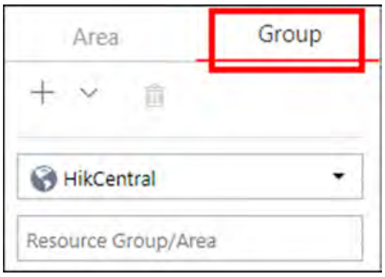


Figure 13-14 Enter Resource Group Page

3. In the Emergency Operation field, click **Add** to add an emergency operation group.

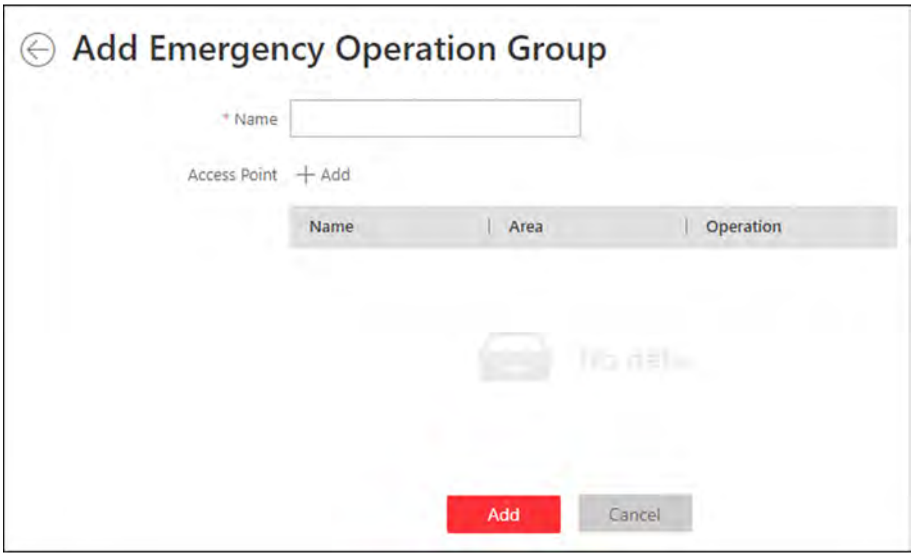


Figure 13-15 Add Emergency Operation Group

4. Create a name for the group.
5. Click **Add** to select the access points to add them to the group.

Note

You can add doors of access control devices, doors of video intercom devices, and floors of elevator control 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.

13.10 Configure Anti-Passback Rules

The anti-passback feature is designed to minimizes the misuse or fraudulent use of access credentials such as passing back card to an unauthorized person, or tailed access. The anti-passback function establishes a specific sequence in which cards must be used in order to grant access. The person should exit via the 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. Click **Logical View** on the home page.
2. Choose one of the following methods to enter the area's resource group page.
   - Select one area and click ✎ to enter the editing area page.

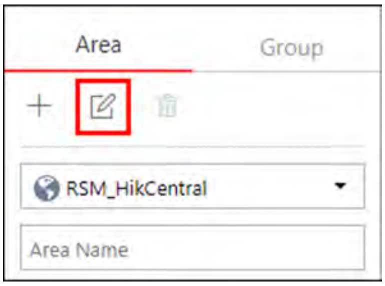


Figure 13-16 Enter Area Editing Page

   - Select **Group** tab on the left to display all the resource groups of different areas.

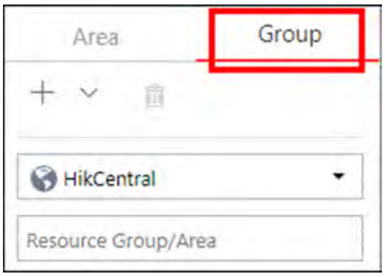


Figure 13-17 Enter Resource Group Page

3. In the Anti-Passback field, click **Add** to add an anti-passback group.

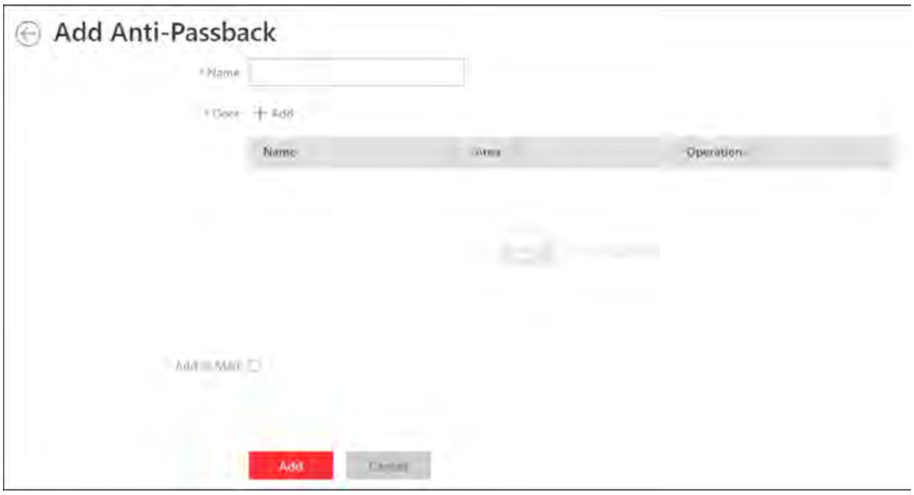


Figure 13-18 Add Anti-Passback Group

4. Create a name for the group.
5. Click **Add** to select the doors to add them to the group.
6. **Optional:** You can locate the anti-passback group on the map by setting the locations of the doors in the group and setting the border of the region for detection.
    1) Check **Add to Map**.

       The region as well as the doors in the group will be added to the map of the area on the right.
    2) Drag to draw the region according to the actual needs.
    3) Drag the icons of the doors to set the their locations on the map.
    4) Right click to finish.

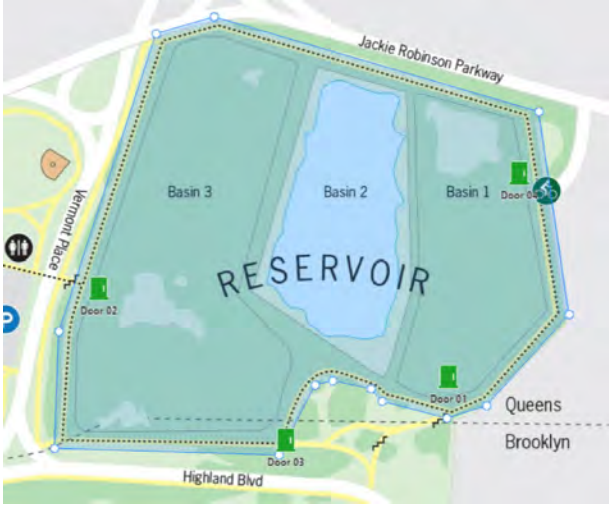


Figure 13-19 Draw Anti-Passback Group on Map

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.

7. Click **Add**.

   The anti-passback group is added in the table and you can view the doors in the group.

13.11 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 be a problem. 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. Click **Logical View** on the home page.
2. Choose one of the following methods to enter the area's resource group page.
   - Select one area and click ✎ to enter the editing area page.

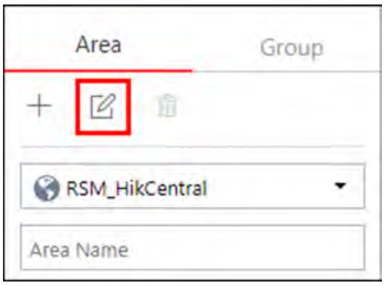


Figure 13-20 Enter Area Editing Page

   - Select **Group** tab on the left to display all the resource groups of different areas.

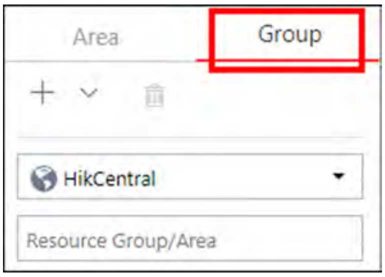


Figure 13-21 Enter Resource Group Page

3. In the Multi-Door Interlocking field, click **Add** to add a multi-door interlocking group.

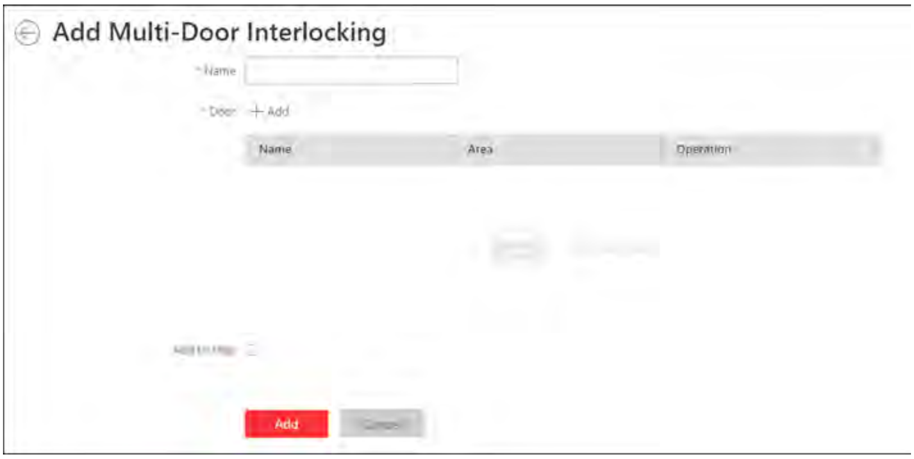


Figure 13-22 Add Multi-Door Interlocking Group

4. Create a name for the group.
5. In the **Door** field, click **Add** to select the doors to add them to the group. Among the added doors, only one door can be opened simultaneously.
6. **Optional:** You can locate the multi-door interlocking group on the map by setting the locations of the doors in the group and setting the border of the region for detection.
    1) Check **Add to Map**.

       The region as well as the doors in the group will be added to the map of the area on the right.
    2) Drag to draw the region according to the actual needs.
    3) Drag the icons of the doors to set the their locations on the map.
    4) Right click to finish.

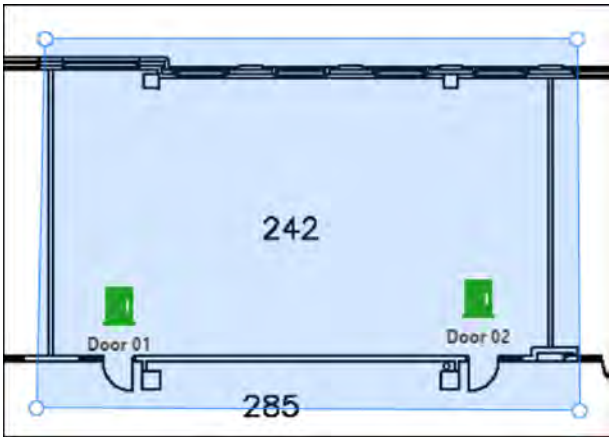


Figure 13-23 Draw Multi-Door Interlocking Group on Map

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.

7. Click **Add**.

The multi-door interlocking group is added in the table and you can view the doors in the group.

13.12 Configure Multi-Factor Authentication Rules

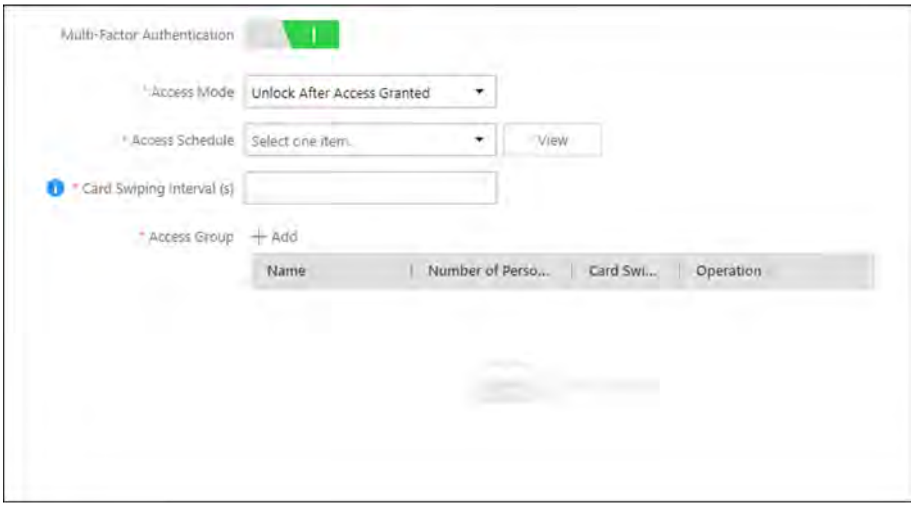
In access control, multi-factor authentication is an authentication method in which the door will unlock only after multiple persons present authenticating multiple credentials in turn. This method is mainly used for locations with high security requirements, such as bank vault. With the mutual supervision 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. Enter **Logical View** on the Home page to enter the Area Management page.
2. In the area list, select the current site from the drop-down site list to show its areas and select one area.
3. Select the **Doors** tab to show the added doors in this area.
4. Click **Name** column to enter the Edit Door page.
5. In the **Application**, set the **Multi-Factor Authentication** switch to on to enable this function.



Multi-Factor Authentication

*Access Mode: Unlock After Access Granted

*Access Schedule: Select one item. View

*Card Swiping Interval (s)

*Access Group + Add

Name	Number of Perso...	Card Swi...	Operation

Figure 13-24 Set Multi-Factor Authentication

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**.

13.13 Add Entry and Exit Counting Group

The entry and exit counting group is used to group the doors of certain region. You can set some doors as the region border. Only the persons accessing these doors are calculated, 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 available for certain emergency scene. For example, during a fire escape, the number of the stayed persons and name list are required for rescue.

Before You Start

Add the access points into different areas first. 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 calculate the number of people who still in the region and view who enters/exits this region.

1. Click **Logical View** on the home page.
2. Choose one of the following methods to enter the area's resource group page.
   - Select one area and click ☑ to enter the editing area page.

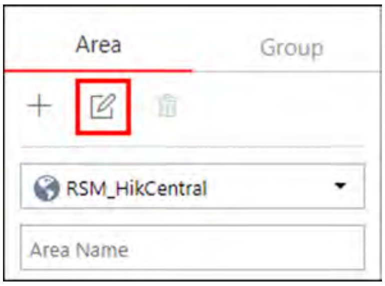


Figure 13-25 Enter Area Editing Page

   - Select **Group** tab on the left to display all the resource groups of different areas.

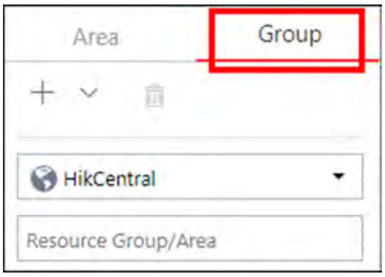
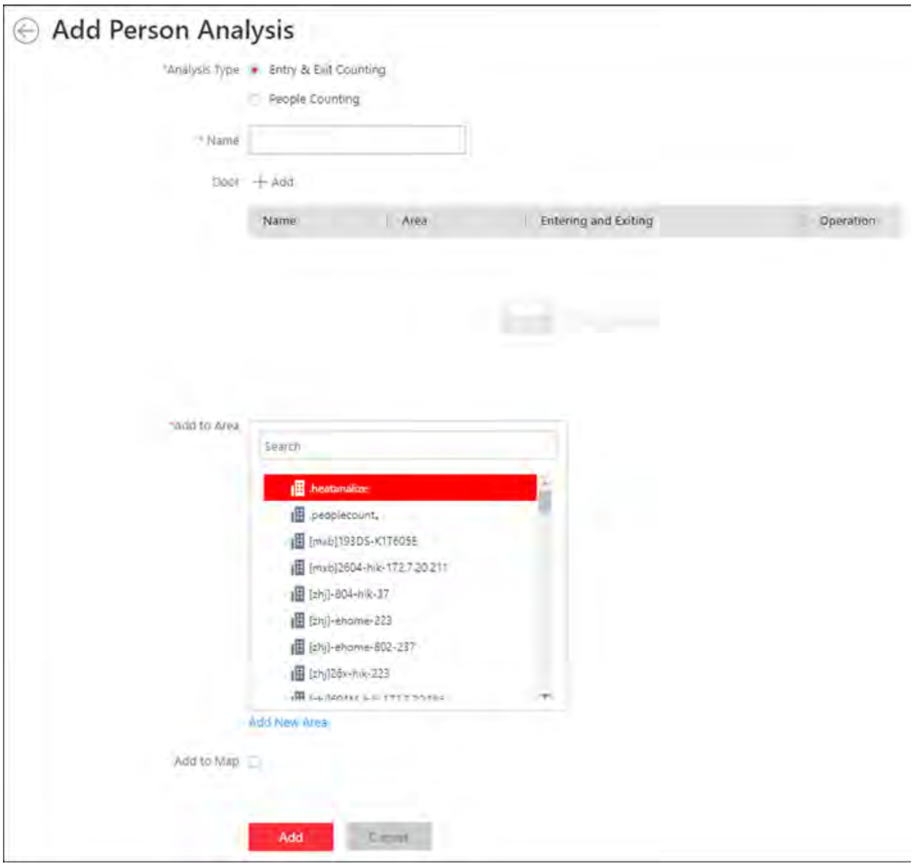


Figure 13-26 Enter Resource Group Page

3. In the People Analysis field, click **Add** to add a people analysis group.
4. In the Add Person Analysis page, select **Entry & Exit Counting** as the analysis type.



Add Person Analysis

*Analysis Type ● Entry & Exit Counting

○ People Counting

* Name

Door + Add

Name	Area	Entering and Exiting	Operation

*Add to Area

Search

- .heatanalize
- .peoplecount,
- [mxb]193DS-K1T605E
- [mxb]2604-hik-172.7.20.211
- [zhj]-804-hik-37
- [zhj]-ehome-223
- [zhj]-ehome-802-237
- [zhj]26x-hik-223

Add New Area

Add to Map □

Figure 13-27 Add Entry & Exit Counting Group

5. Create a name for the group.
6. Click **Add** to select the doors.
7. Set the entering or exiting direction of the card readers of the selected 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.
8. **Optional:** You can locate the entry &exit counting group on the map by setting the locations of the doors in the group and setting the border of the region for detection.
   1) Check **Add to Map**.

      The region as well as the doors in the group will be added to the map of the area on the right.
   2) Drag to draw the region according to the actual needs.
   3) Drag the icons of the doors to set the doors locations on the map.
   4) Right click to finish.

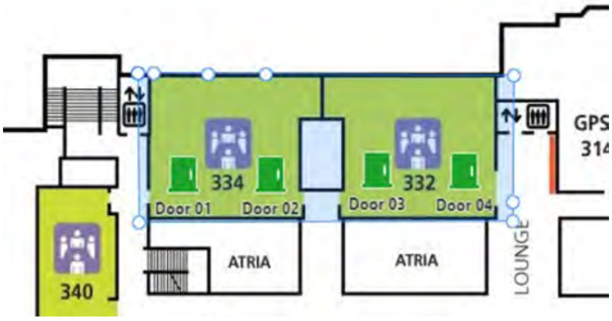


Figure 13-28 Draw Entry & Exit Counting Group on Map

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.

9. Click **Add**.

   The entry & exit counting group is added in the table and you can view the doors in the group.

13.14 Set Working Mode of DS-K5600 Series

In access control, if you adopt DS-K5600 face recognition series (such as DS-K5603-Z) in actual application, you need to set the working mode for these devices after adding them to the system according to actual needs.

Enter **System → Advanced → Working Mode** .

If the DS-K5600 series device is applied with our turnstile, select **Face Recognition Terminal** mode to form a turnstile with face recognition function. The persons can access the turnstile by scanning their faces with the DS-K5600 series device after setting the face credentials and access levels.

If the DS-K5600 series device is applied with other third-party turnstile, select **Access Control Terminal** mode and you can set access levels in the system to define the access permissions.

Chapter 14 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.

14.1 Flow Chart

For the first time, you can follow the flow chart to perform configurations and operations.

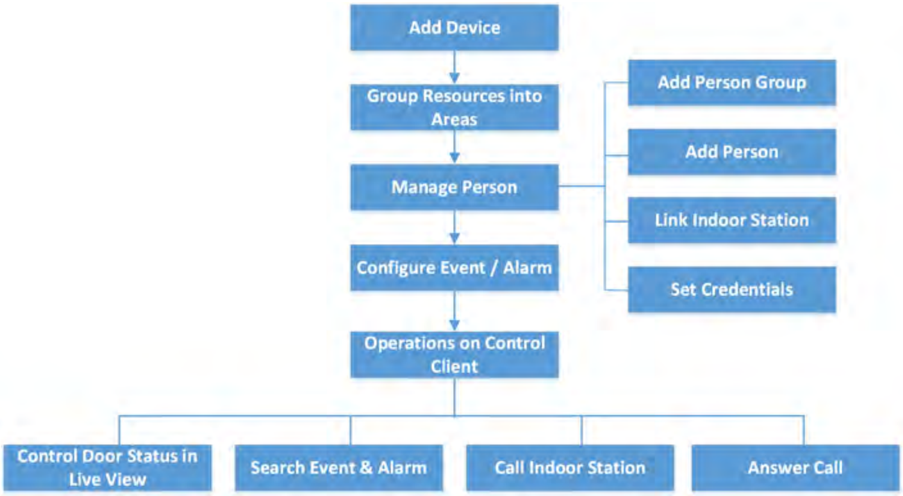


Figure 14-1 Flow Chart of Video Intercom

- **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 List*** .

- **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*** .

14.2 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.

14.2.1 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 in 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

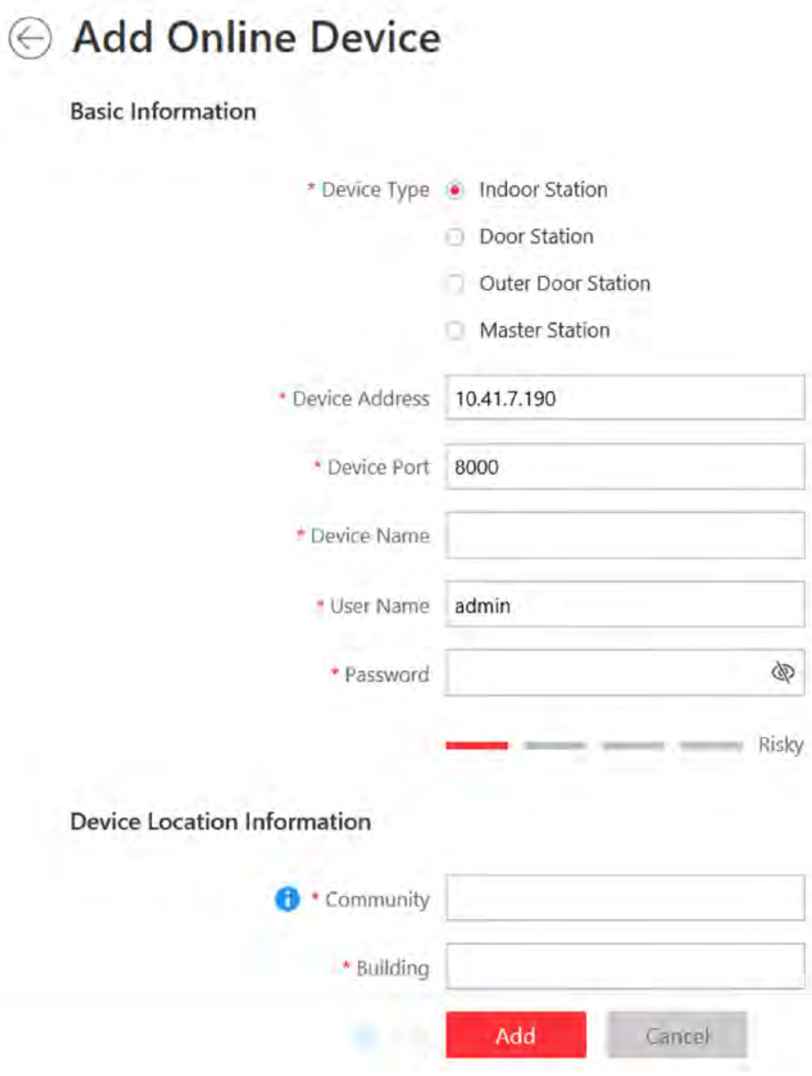
1. Click **Physical View → Video Intercom Device** to enter the video intercom device management page.
2. In the Online Device area, select a network type.

   Server Network

   As the default selection, the detected online devices in the same local subnet with the 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.
3. In the Online Device area, select the active device to be added.
4. Click 🗋 in the **Operation** Column to open the Add Online Device window.
5. Select **Indoor Station** as the device type.



Add Online 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:

Figure 14-2 Add Online Indoor Station

6. 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.

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 Channel to Area** to on to import the channels 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 channels 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. 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).

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, 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 **Apply Device Settings**. Click **Apply Device Settings** to apply the current settings in system to the device(s).

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. Click **Physical View → Video Intercom Device** to enter the video intercom device management page.
2. In the Online Device area, select a network type.

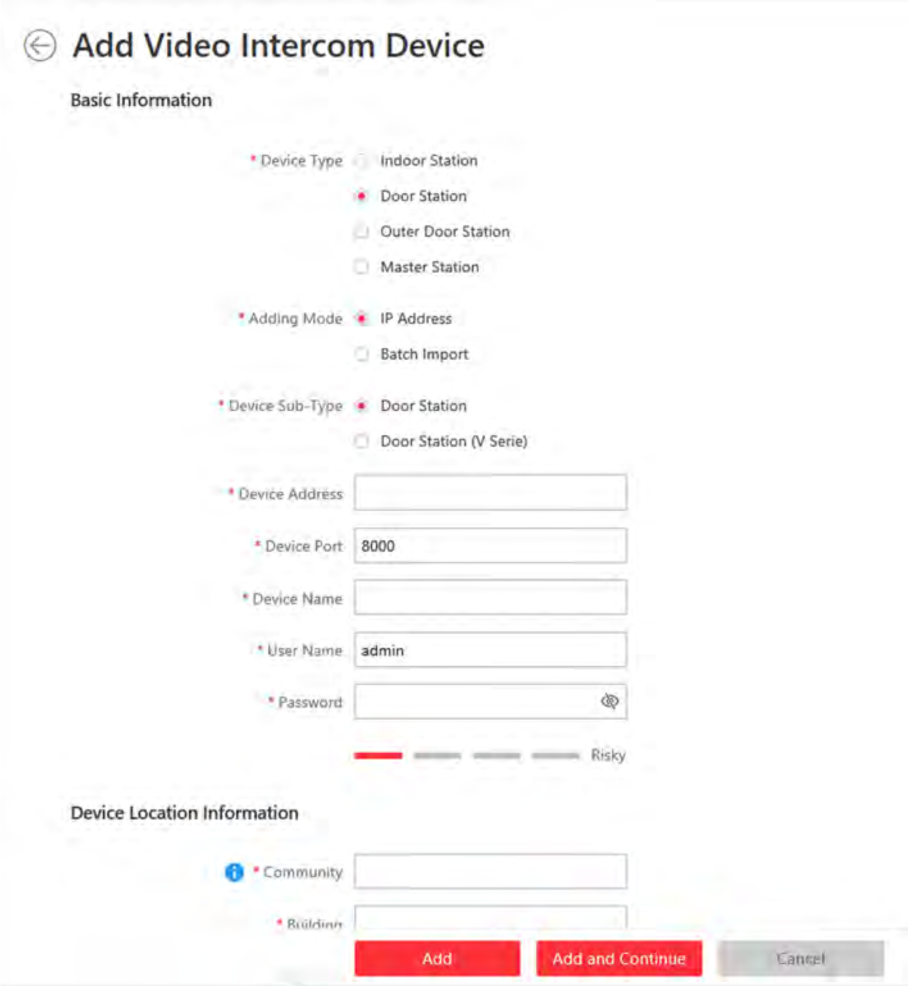
   Server Network

   As the default selection, the detected online devices in the same local subnet with the 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.
3. In the Online Device area, select the active device to be added.

4. Click 🗋 in the **Operation** Column to open the Add Online Device window.
5. 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)

* Device Address

* Device Port 8000

* Device Name

* User Name admin

* Password

Risky

Device Location Information

* Community

* Building

Add | Add and Continue | Cancel

Figure 14-3 Add Online Door Station

6. Select **Door Station** or **Door Station (V Serie)** as the device sub-type.
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 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 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 Channel to Area** to on to import the channels of the added devices to an area.

Note

- You can import all the channels (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 channels to area, you cannot perform further operations such as such as live view, playback, etc., for the cameras.

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).

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 **Apply Device Settings**. Click **Apply Device Settings** to apply the current settings in system to the device(s).

Add a Detected Online Outer 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 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

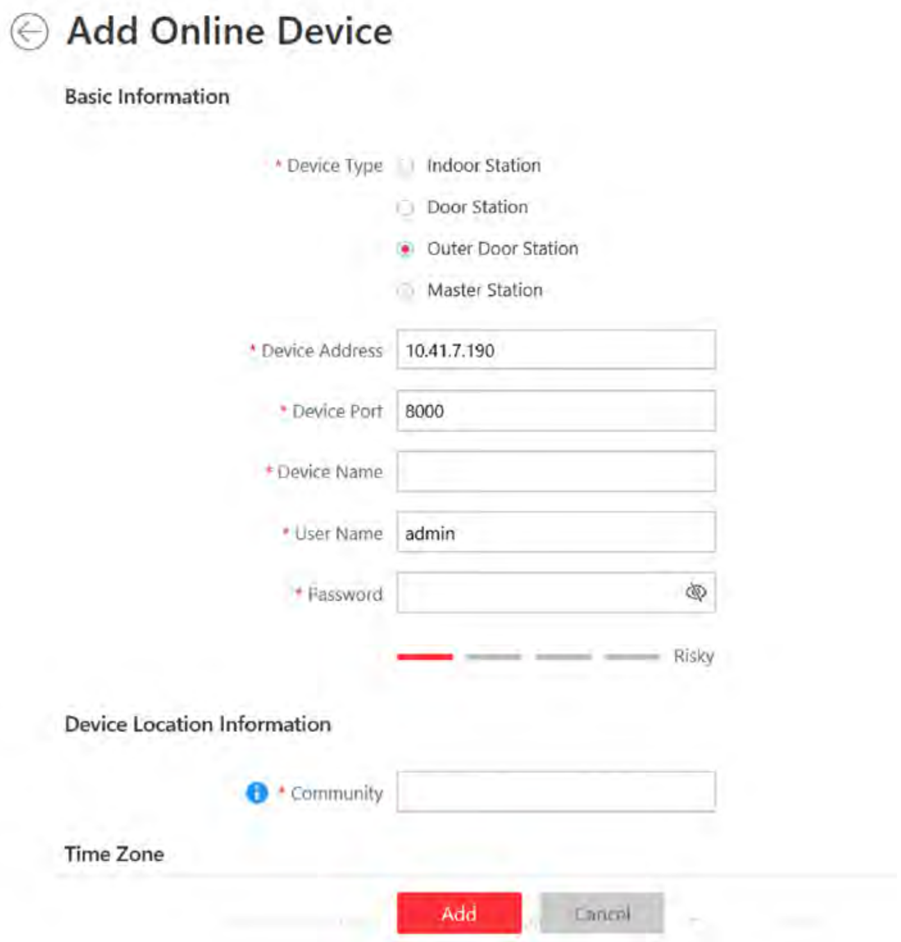
1. Click **Physical View → Video Intercom Device** to enter the video intercom device management page.
2. In the Online Device area, select a network type.

   Server Network

   As the default selection, the detected online devices in the same local subnet with the 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.
3. In the Online Device area, select the active device to be added.
4. Click in the **Operation** Column to open the Add Online Device window.
5. Select **Outer Door Station** as the device type.



Add Online 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

Figure 14-4 Add Outer Door Station

6. 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.

7. 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.

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 Channel to Area** to on to import the channels of the added devices to an area.

   Note

   - You can import all the channels (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 channels to area, you cannot perform further operations such as live view, playback, etc., for the cameras.

10. Click **Add**.
11. 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 **Apply Device Settings**. Click **Apply Device Settings** to apply the current settings in system to the device(s).

Add a Detected Online Master 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 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

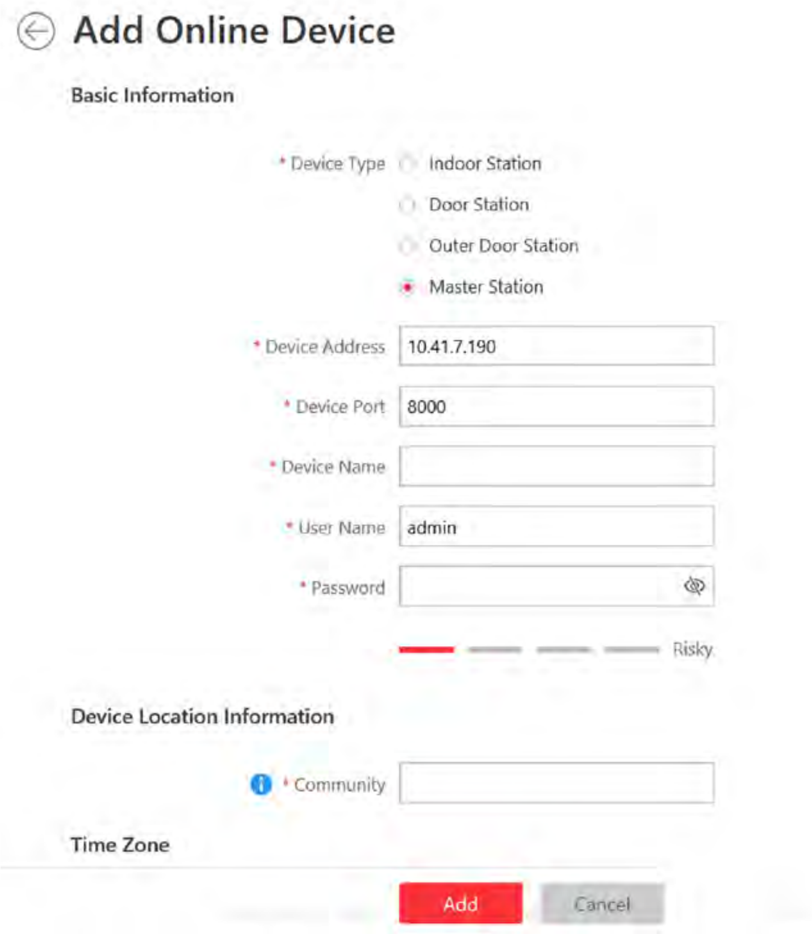
1. Click **Physical View → Video Intercom Device** to enter the video intercom device management page.
2. In the Online Device area, select a network type.

   Server Network

   As the default selection, the detected online devices in the same local subnet with the 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.
3. In the Online Device area, select the active device to be added.
4. Click ⊕ in the **Operation** Column to open the Add Online Device window.
5. Select **Master Station** as the device type.



Add Online 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

Figure 14-5 Add Online Master Station

6. 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.

7. 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.

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. Click **Add**.
10. 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 **Apply Device Settings**. Click **Apply Device Settings** to apply the current settings in system to the device(s).

14.2.2 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.

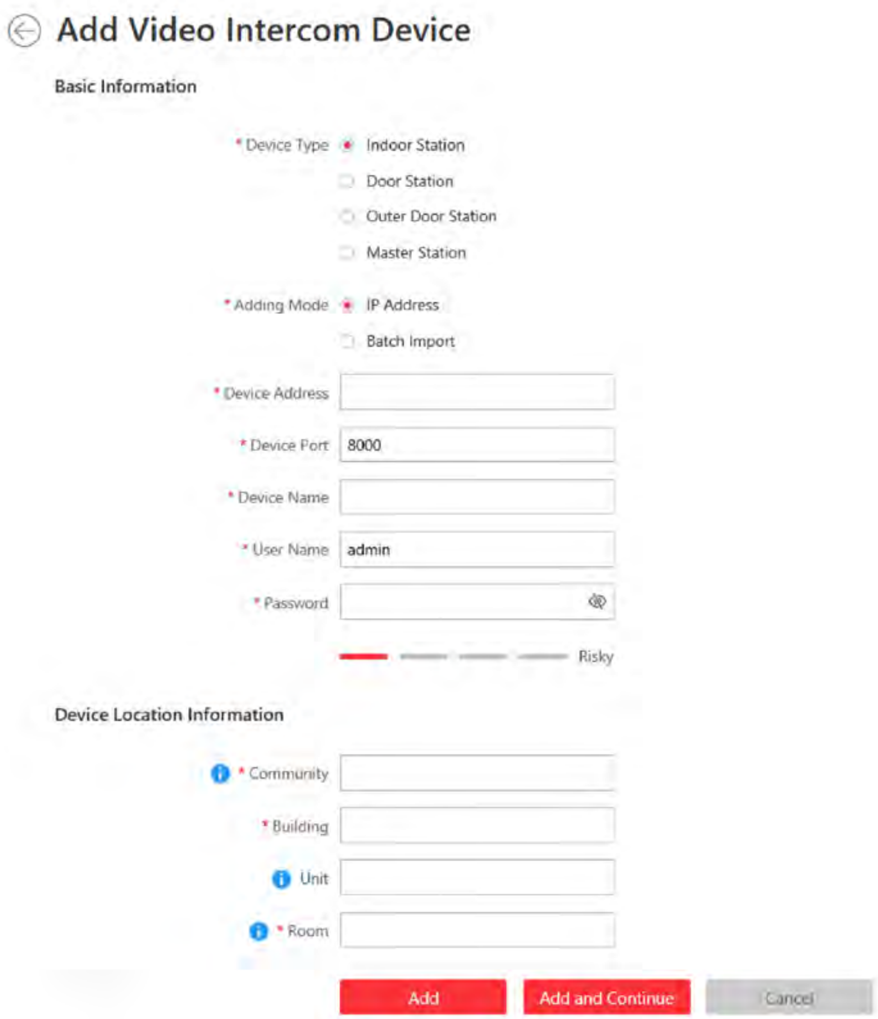
Before You Start

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. Click **Physical View → Video Intercom Device** to enter the video intercom device management page.
2. Click **Add** to enter Add Video Intercom Device page.
3. 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	

Figure 14-6 Add Indoor Station

4. Select **IP Address** as the adding mode.
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.

⚠ **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. 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.

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 Channel to Area** to on to import the channels 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 channels to area, you cannot perform further operations for the alarm inputs.

9. 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.

10. 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.
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.

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 ⓘ will be displayed on the right side of the **Apply Device Settings**. Click **Apply Device Settings** to apply the current settings in system to the device(s).

14.2.3 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.

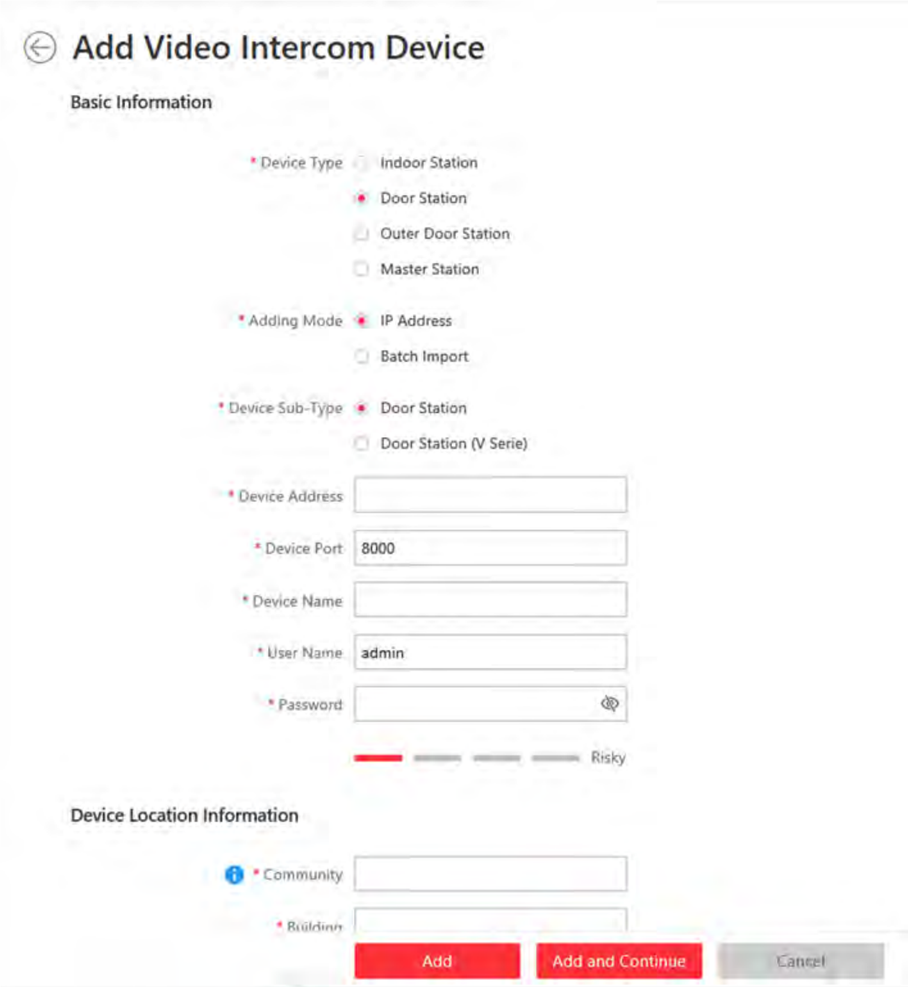
Before You Start

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. Click **Physical View → Video Intercom Device** to enter the video intercom device management page.
2. Click **Add** to enter Add Video Intercom Device page.
3. 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)

* Device Address

* Device Port: 8000

* Device Name

* User Name: admin

* Password

Risky

Device Location Information

* Community

* Building

Figure 14-7 Add Door Station

4. Select **IP Address** as the adding mode.
5. Select **Door Station** or **Door Station (V Serie)** as the device sub-type.
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.

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 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.

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 Channel to Area** to on to import the channels of the added devices to an area.

Note

- You can import all the channels (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 channels to area, you cannot perform further operations such as such as live view, playback, etc., for the cameras.

10. 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.
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 **Apply Device Settings**. Click **Apply Device Settings** to apply the current settings in system to the device(s).

14.2.4 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.

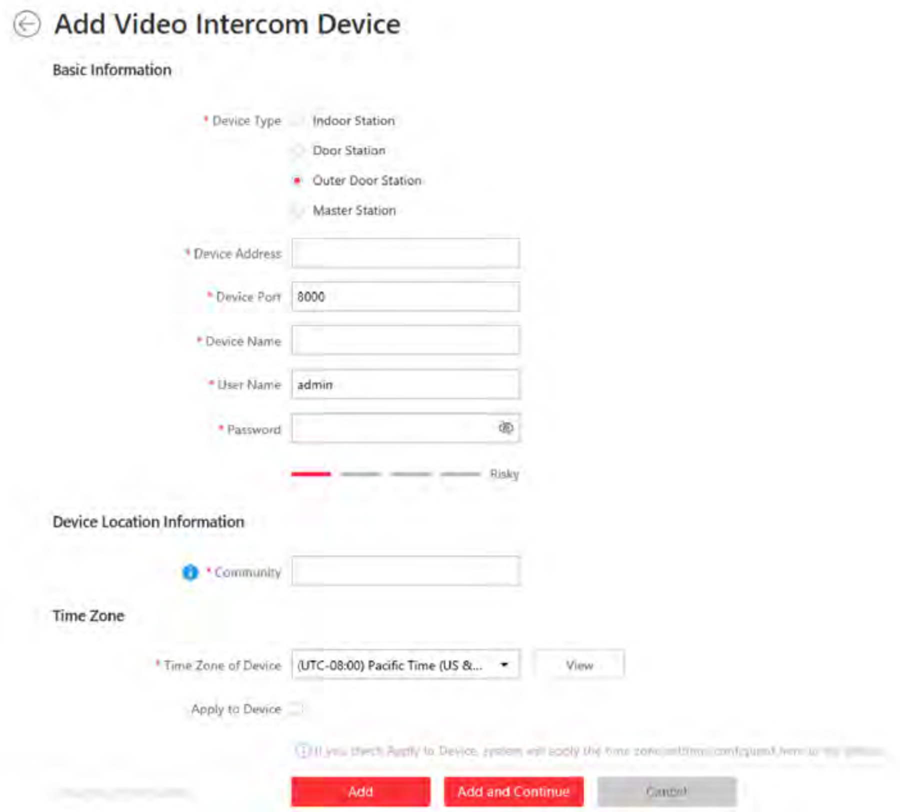
Before You Start

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. Click **Physical View → Video Intercom Device** to enter the video intercom device management page.
2. Click **Add** to enter Add Video Intercom Device page.
3. 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 &...

Apply to Device □

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

Figure 14-8 Add Outer Door Station

4. 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.

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. 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.

6. **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.

7. **Optional:** Switch **Add Channel to Area** to on to import the channels of the added devices to an area.

Note

- You can import all the channels (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 channels to area, you cannot perform further operations such as live view, playback, etc., for the cameras.

8. 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.
9. 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 **Apply Device Settings**. Click **Apply Device Settings** to apply the current settings in system to the device(s).

14.2.5 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.

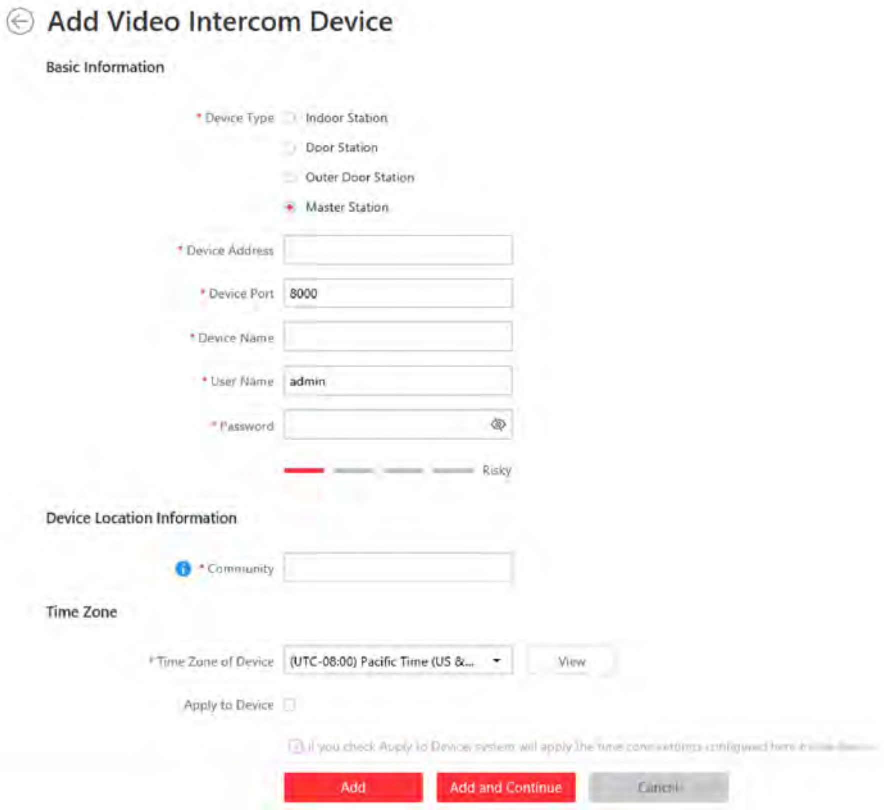
Before You Start

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. Click **Physical View → Video Intercom Device** to enter the video intercom device management page.
2. Click **Add** to enter Add Video Intercom Device page.
3. 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 14-9 Add Master Station

4. 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.

⚠ **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. 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.

6. **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.

7. 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.
8. 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 a red icon ❗ will display on the right side of the **Apply Device Settings**. Click **Apply Device Settings** to apply the current settings in system to the device(s).

14.2.6 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. Click **Physical View → Video Intercom Device** to enter the video intercom device management page.
2. Click **Add** to enter Add Video Intercom Device page.
3. Select **Indoor Station** or **Door Station** as the device type.
4. Click **Batch Import** as the adding mode.
5. Click **Download Template** to save the predefined template (Excel file) on your PC.
6. Open the exported template file and enter the required information of the devices to be added.
7. Click ··· and select the template file.
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. 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.

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.

Add Related Camera

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

14.2.7 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.

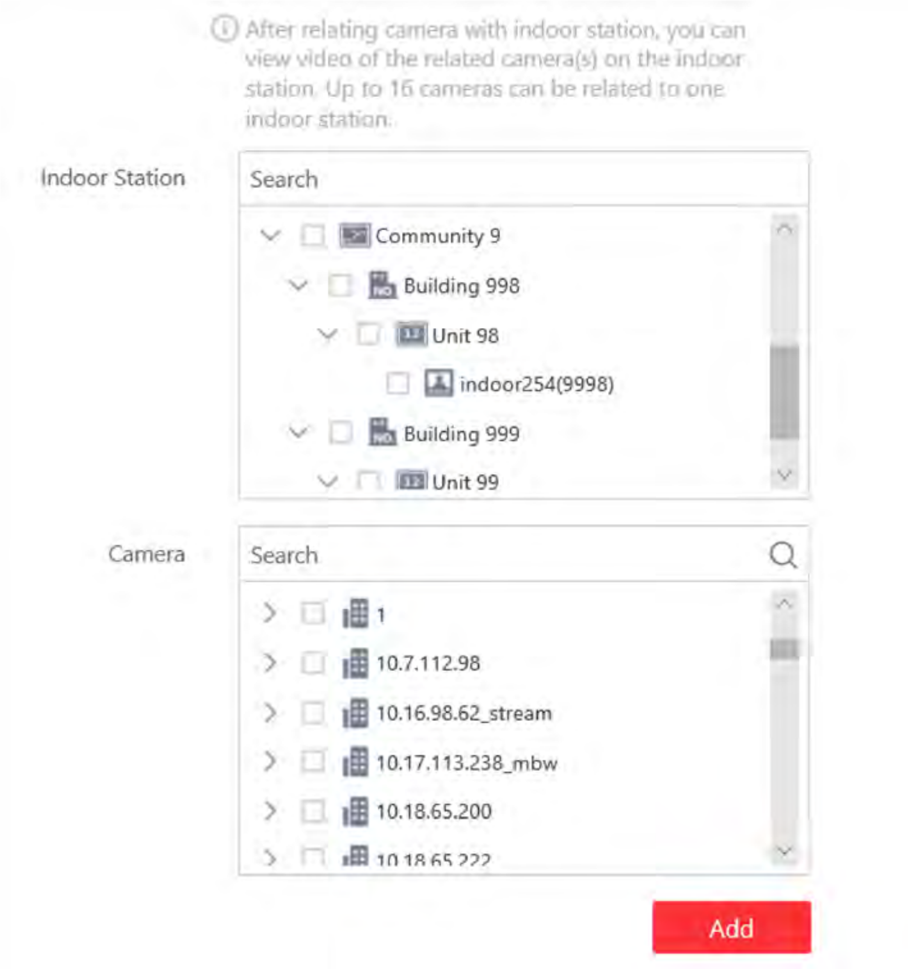
Before You Start

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. Click **Physical View → Video Intercom Device** to enter the video intercom device management page.
2. Select an indoor station in the video intercom device list.
3. Click 📷 to add the related camera(s).



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

- □ Community 9
  - □ Building 998
    - □ Unit 98
      - □ indoor254(9998)
  - □ Building 999
    - □ Unit 99

Camera

Search

- □ 1
- □ 10.7.112.98
- □ 10.16.98.62_stream
- □ 10.17.113.238_mbw
- □ 10.18.65.200
- □ 10.18.65.222

Add

Figure 14-10 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*** .

4. In the Indoor Station list, check one or more indoor station(s).

Note

You can enter a keyword to search the target indoor station(s). And the keyword of corresponding device(s) will be displayed in red.

5. In the Camera list, check one or more cameras.

Note

You can enter a keyword to search the target camera(s). And the keyword of corresponding camera(s) will be displayed in red.

6. Click **Add**.

Note

You can delete the related camera(s) in the configuration page of the indoor station.

14.3 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

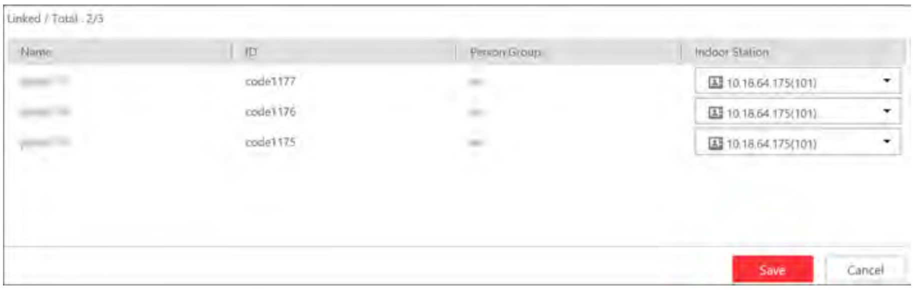
Note

For more details about linking single person with an indoor station, refer to ***Add a Person*** .

1. Click **Person → Person List** to enter person management page.
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	--	10.18.64.175(101)
[redacted]	code1176	--	10.18.64.175(101)
[redacted]	code1175	--	10.18.64.175(101)

Figure 14-11 Batch Link Persons with Indoor Station(s)

6. Click **Save**.

   The linked person information will be applied to the indoor station(s).

14.4 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 15 Manage Time and Attendance

After adding the persons to the person list, if you want to track and monitor when the persons start/stop work and monitor their working hours and late arrivals, early departures, time taken on breaks, and absenteeism, you can add the person to the attendance group and assign a shift schedule (a rule for the attendance defining how the schedule repeats, the shift type, break settings, and the card swiping rule.) to the attendance group to define the attendance parameters for the persons in the attendance group.

15.1 Flow Chart

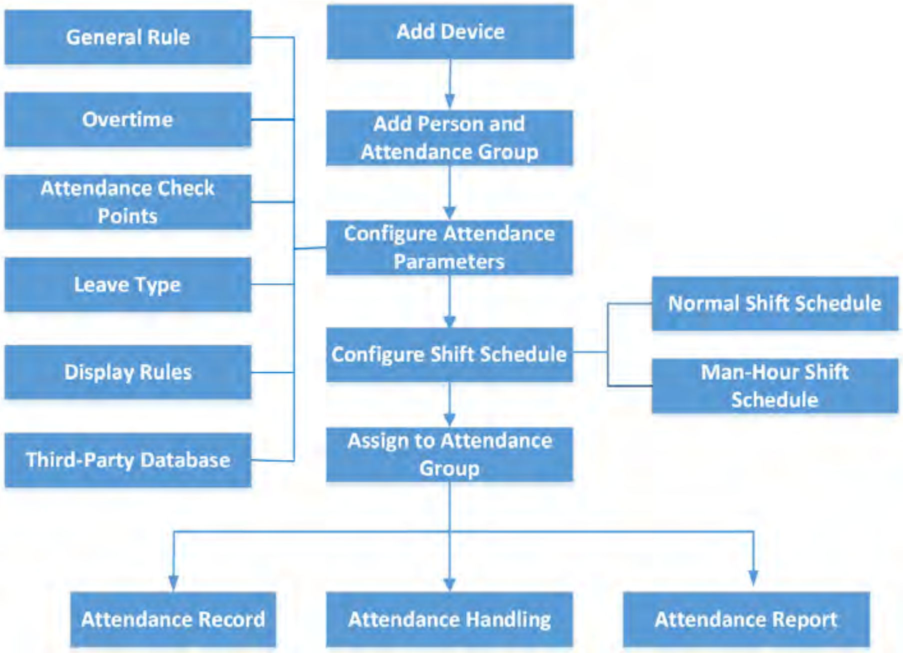


Figure 15-1 Flow Chart of Time and Attendance

- **Add Device**: Add devices (e.g., access control devices, facial recolonization cameras, etc.) to Web Client. For more details, refer to ***Manage Access Control Device*** or ***Manage Encoding Device*** .
- **Add Person and Attendance Group**: Add persons and attendance group, and group the persons to group. For more details, refer to ***Manage Person List*** and ***Add Attendance Group*** .
- **Configure Attendance Parameters**: Configure general rules, overtime, attendance check points, leave type, display rules for report, third-party database. For more details, refer to ***Configure Attendance Parameters*** , ***Set Display Rules for Attendance Report*** and ***Synchronize Card Swiping Records to Third-Party Database*** .
- **Configure Shift Schedule**: Add normal shift schedule or man-hour shift schedule. For more details, refer to ***Add Normal Shift Schedule*** or ***Add Man-Hour Shift Schedule*** .

- **Assign to Attendance Group**: Assign the added shift schedule to attendance group. For more details, refer to ***Assign Shift Schedule to Attendance Group*** .
- **Attendance Record**, **Attendance Handling**: Search and correct attendance record, apply leave, get device's attendance record, manually calculate attendance results, etc. For more details, refer to ***Manage Attendance Record*** .
- **Attendance Report**: Export attendance report in local PC. For more details, refer to ***Export Attendance Report*** .

15.2 Add Attendance Group

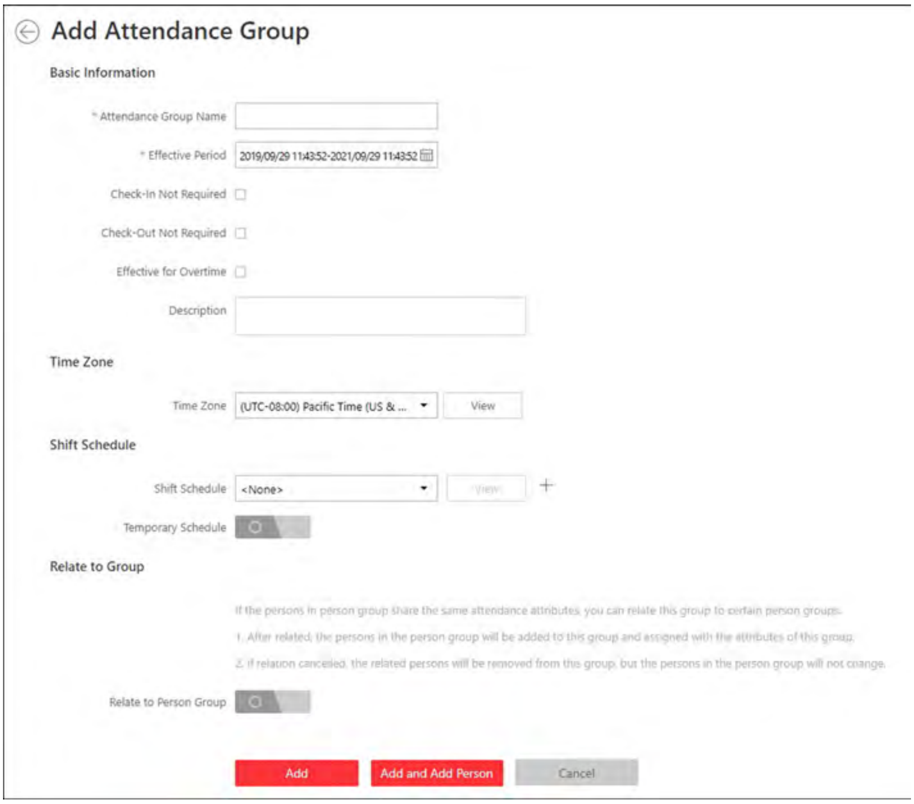
After adding the persons, you can group the persons into different attendance groups. The persons in the same attendance group are assigned with the same shift schedule.

Steps

Note

For each person, he/she can be added to up to one attendance group.

1. Click **Person → Attendance Group → Add** to enter the adding attendance group page.



Add Attendance Group

Basic Information

* Attendance Group Name

* Effective Period 2019/09/29 11:43:52-2021/09/29 11:43:52

Check-In Not Required □

Check-Out Not Required □

Effective for Overtime □

Description

Time Zone

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

Shift Schedule

Shift Schedule <None>

Temporary Schedule

Relate to Group

If the persons in person group share the same attendance attributes, you can relate this group to certain person groups.

1. After related, the persons in the person group will be added to this group and assigned with the attributes of this group.

2. If relation canceled, the related persons will be removed from this group, but the persons in the person group will not change.

Relate to Person Group

Figure 15-2 Add Attendance Group

2. Set the basic information of the group.

   Group Name

Create a name for the attendance group.

Effective Period

Set the effective period for this attendance group.

Check-In Not Required

Persons in this attendance group do not need to check-in when they come to work.

Check-Out Not Required

Persons in this attendance do not need to check-out when they end work.

Effective for Overtime

For persons in this attendance group, their overtime will be recorded.

Description

Enter the descriptive information for the group. E.g., This attendance group is for security guards in Team A.

3. **Optional:** Select a time zone for the attendance group in drop-down list of **Time Zone** when the persons are in the different time zones.

Note

The default time zone is where the SYS server is located. For certain across-timezone scene, such as the attendance persons in different time zones, you need to set the time zone for them.

4. **Optional:** Set the shift schedule for the persons in the group so that they need to attend according to this shift schedule.

Shift Schedule

Select a shift schedule from the drop-down list. The persons in the group should attend according to this shift schedule.

Note

Click **Add New** to add a new shift schedule. For details, refer to ***Add Normal Shift Schedule*** .

Temporary Schedule

You can also set a temporary schedule for the persons in this group. During the effective period of the temporary schedule, the persons should attend according to the temporary schedule.

For example, according to the general shift schedule, the security guards should check-in at 6:00 am and check out at14:00 pm. You can add a temporary schedule for special days that they should check-in at 3:00 am and 14:00 pm.

5. **Optional:** If the persons in the existing person group share the same shift schedule, you can enable **Relate to Person Group** to link this attendance group with existing person group(s).
   1) Set the **Relate to Person Group** switch to ON.
   2) Select existing person group(s) to relate the current attendance group to the selected person group(s).

After related, the persons in the selected person groups will be added to the current attendance group. If you add more persons to the related person groups later, these newly added persons will be added to this attendance group automatically. In addition, if you edit the persons in the related person groups or remove persons from the related person groups, these edited or removed persons will be edited/removed in/from this attendance group automatically.

6. Confirm to add the attendance group.
   - To add persons to the attendance group, click **Add and Add Person** and perform the following steps.

     Note

     If you have enabled **Relate to Person Group** and select person group(s) to relate, you cannot add more persons when adding this attendance group. If you click **Add and Add Person**, this function will be disabled.
   - To save the attendance group first and add persons to the attendance group later, click **Add** to finish this task and return to the attendance group list.
7. **Optional:** If you click **Add and Add Person**, you will enter the next page to add persons to this attendance group.
   1) In the **Add from** field, choose to add existing persons or add a new person to this group.

      Existing Person

      Add existing persons in the system to this attendance group.

      Add New Person

      Add a new person to this attendance group. The person will be added to the person list as well.
   2) **Optional:** If you select **Existing Person**, you can select persons from the person list or other groups.

      Person List

      Filter persons in the person list by entering keywords of person name, person group name, or additional information.

      Note

      You can click **Additional Information** to enable the custom additional information as search condition.

      Access Group

      Add all the persons in the selected access group(s) to this attendance group.

      Attendance Group

      Add all the persons in the selected attendance group(s) to this attendance group.
8. Click **Add** to add the selected persons to the attendance group.
9. **Optional:** After adding the attendance group, you can do one or more of the followings.

Edit Attendance Group	Click ✎ in the Operation column to edit its details.

Manage Persons in Attendance Group	Click the added attendance 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 issuing cards, importing and exporting persons. For details, refer to ***Manage Person List*** .
Delete Attendance Group	Select one attendance group and click **Delete** to delete it.
Delete All Attendance Groups	Click **Delete All** to delete all the added attendance groups.

15.3 Add Normal Shift Schedule

A normal shift schedule defines the scheduled work time (e.g.,start-work time, end-work time, late rule, valid check-in/out time break time, etc.) and how it repeats. You can add a normal shift and assign the attendance group(s) to it. The assigned persons in the attendance group(s) will have the same attendance rules.

Steps

1. Click **Time & Attendance → Shift Schedule** to enter the shift schedule management page.
2. Click **Add**.
3. Set the shift schedule's basic information, including a custom name and the description.
4. **Optional:** Select another shift schedule from the drop-down list of **Copy from** field to copy the schedule information to the current schedule. You can edit the schedule settings on this basis.
5. Set the schedule's repeating mode.

   Week

   The schedule will repeat every 7/14 days based on the week. If you select two weeks, you need to set the start week.

   Day(s)

   You can customize the number of days in one period. You should set a start date of one period for reference which can define how the schedule repeats.

   Note

   The number of days should be between 1 to 30.
6. Select **Normal Shift** as the schedule type.
7. Draw the scheduled work time on the timeline and in the pop-up window, set the detailed schedule rules.
   1) Set the required parameters.

      Scheduled Work Time

      The range of the scheduled work time, including start-work time and end-work time.

Min. Work Hours

The employee must work for more than this period calculated as the work duration.

Flexible Mode

Allow Late/Early Leave

The scheduled start-work time and end-work time is fixed. The employees need to check in before the start-work time and check out after the end-work time.

For this mode, you need to set the allowable minutes for late and early leave. If the employee checks in/out within the period after the start-work time or before the end-work time, the status will be **Normal**.

For example, if the start-work time is set as 09:00, and the late allowable duration is 30 min, if the employee checks in at 09:15, the attendance status will be **Normal**.

Flexible Period

Flexible period allows employees to extend their start-work time and end-work time.

For flexible schedule, set the flexible duration, which defines the extended duration for both start-work and end-work time. During this flexible schedule, the check-in/out will be recorded and the status will be **Normal**.

For example, if the required work time is set as 09:00 to 18:00, and the flexible duration is 30 min, if the employee checks in at 09:15, and checks out at 18:15, the attendance status will be **Normal**.

2) Set the break duration such as lunch time.

Auto Deduct

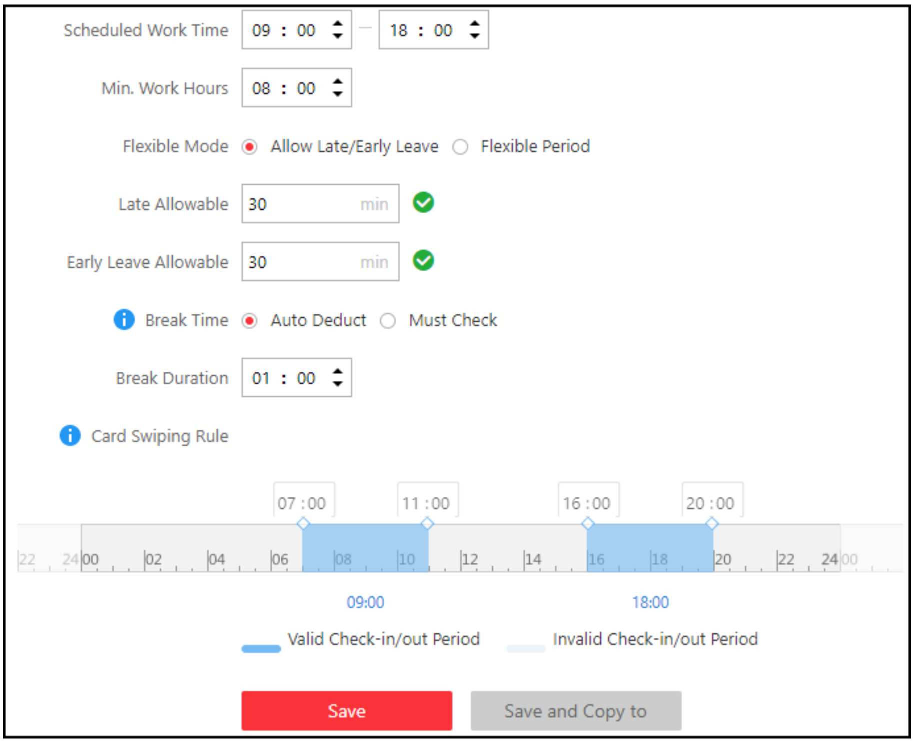
The fixed break duration will be excluded from work hours.

Must Check

The break duration will be calculated and excluded from work hours according to actual check-in and check-out time.

3) **Optional:** View and edit the valid check-in/out period on the timeline. If the employee checks in/out during the valid check-in/out period, the check-in/out will be recorded and the attendance status will not be absent.
4) Click **Save**. You can click **Save and Copy to** to copy the schedule to other days.

Example



Scheduled Work Time 09 : 00 — 18 : 00

Min. Work Hours 08 : 00

Flexible Mode ● Allow Late/Early Leave ○ Flexible Period

Late Allowable 30 min ✓

Early Leave Allowable 30 min ✓

Break Time ● Auto Deduct ○ Must Check

Break Duration 01 : 00

Card Swiping Rule

Figure 15-3 Set Detailed Schedule Rules for Normal Shift Schedule

In the above image, if you set the parameters as above, if the employee checks in during 07:00 to 09:00, the check-in will be normal. If the employee checks in during 09:00 to 9:30, the check-in will be normal. If the employee checks in during 09:30 to 11:00, the check-in will be valid but whether late or absent according to the absence rule.

If the employee checks out during 18:00 to 20:00, the check-out will be normal. If the employee checks out during 17:30 to 18:00, the check-out will be normal. If the employee checks in during 16:00 to 17:30, the check-out will be valid but whether late or absent according to the absence rule.

If the employee checks in after 11:00, the check-in will be invalid and he/she will be marked as absent or late for a period according to the absence rule.

If the employee checks out before 16:00, the check-out will be invalid and he/she will be marked as absent or late for a period according to the absence rule.

Note

For more details about absence rule, refer to ***Define Absence*** .

8. Select the calculation mode.

First In & Last Out

The first check-in time is recorded as start work time and the last check-out time is recorded as the end-work time.

Each Check-In/Out

Each check-in time and check-out time is valid and the sum of all periods between adjacent check-in and check-out time will be recorded as the valid work hours. You need to set **Min. Interval** for this calculation method. For example, if the interval between card swiping of the same card is less than the set value, the period is not be calculated.

9. **Optional:** Set **Enable T&A Status on Device** switch to on to calculate according to attendance status on the device.

   Note

   Make sure the device supports this function.

10. Select the holidays on which days the shift schedule will not be effective.

    Note

    For setting the holiday, refer to ***Set Holiday*** .

11. Finish adding the shift schedule.
    - Click **Add** to add the shift schedule and go back to the shift schedule management page.
    - Click **Add and Assign** to add the shift schedule and assign it to the attendance group. For details, refer to ***Assign Shift Schedule to Attendance Group*** .

15.4 Add Man-Hour Shift Schedule

Man-hour shift schedule is usually used for the attendance with irregular time schedule. It does not requires the strict check-in time and check-out time and only requires the staffs' work hours (from the start time you set) is equal to or larger than the predefined minimum work hours. The man-hour shift schedule defines the rules and how it repeats. You can add a man-hour shift and assign the attendance group(s) to it. The assigned persons in the attendance group(s) will have the same attendance rules.

Steps

1. Click **Time & Attendance → Shift Schedule** to enter the shift schedule management page.
2. Click **Add**.
3. Set the shift schedule's basic information, including a custom name and the description.
4. **Optional:** Select another shift schedule from the drop-down list of **Copy from** field to copy the schedule information to the current schedule. You can edit the schedule settings on this basis.
5. Set the schedule's repeating mode.

   Week

   The schedule will repeat every 7/14 days based on the week. If you select two weeks, you need to set the start week.

   Day(s)

   You can customize the number of days in one period. You should set a start date of one period for reference which can define how the schedule repeats.

Note

The number of days should be between 1 to 30.

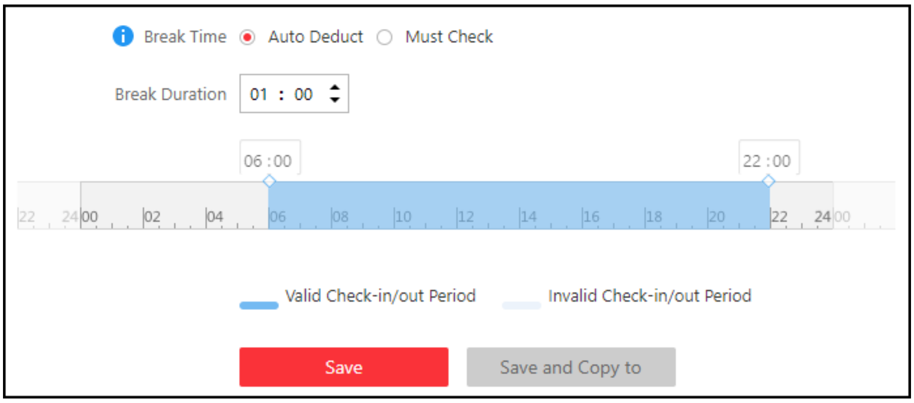
6. Select **Man-Hour Shift** as the schedule type.
7. Draw the scheduled work time on the timeline as valid check-in/out period and in the pop-up window, set the detailed schedule rules.
   1) Set the break duration such as lunch time.

      Auto Deduct

      The fixed break duration will be excluded from work hours.

      Must Check

      The break duration will be calculated and excluded from work hours according to actual check-in and check-out time.
   2) **Optional:** View and edit the valid check-in/out period on the timeline. If the employee checks-in/out during the valid check-in/out period, the check-in/out will be recorded and the attendance status will not be absent.
   3) Click **Save**. You can click **Save and Copy to** to copy the schedule to other days.



Break Time ● Auto Deduct ○ Must Check

Break Duration 01 : 00

Figure 15-4 Set Detailed Schedule Rules for Man-Hour Shift Schedule

8. Set **Min. Work Hours**. Only when the employee's work hours reach the value, her/his attendance status is normal.
9. Select the calculation mode.

   First In & Last Out

   The first check-in time is recorded as start work time and the last check-out time is recorded as the end-work time.

   Each Check-In/Out

   Each check-in time and check-out time is valid and the sum of all periods between adjacent check-in and check-out time will be recorded as the valid work hours. You need to set **Min. Interval** for this calculation method. For example, if the interval between card swiping of the same card is less than the set value, the period is not be calculated.
10. **Optional:** Set **Enable T&A Status on Device** switch to on to calculate according to attendance status of the device.

Note

Make sure the device support this function.

11. Select the holidays on which days the shift schedule will not be effective.

Note

For setting the holiday, refer to ***Set Holiday*** .

12. Finish adding the shift schedule.
    - Click **Add** to add the shift schedule and go back to the shift schedule management page.
    - Click **Add and Assign** to add the shift schedule and assign it to the attendance group. For details, refer to ***Assign Shift Schedule to Attendance Group*** .

15.5 Assign Shift Schedule to Attendance Group

After setting the shift schedule, you need to assign it to the attendance group so that it will calculate the attendance records for persons in the attendance group according to this shift schedule.

Before You Start

- Add a shift schedule and set the rule. For details, refer to ***Add Normal Shift Schedule*** .
- Add an attendance group. For details, refer to ***Add Attendance Group*** .

Perform this task to assign a shift schedule to attendance group(s).

Steps

1. Click **Time & Attendance → Shift Schedule** to enter the shift schedule management page.
2. Enter the Assign to Attendance Group page.
    - After you set the parameters of shift schedule when adding, click **Add and Assign**.
    - When editing the shift schedule, click **Configuration** in the shift schedule details page.
    - Click ✎ in the Operation column.
3. In the Assign to Attendance Group field, select the attendance group(s) you want to assign the shift schedule to.

Note

Only the attendance groups which haven't been linked to a shift schedule will display.

4. **Optional:** Click **Add New** to add a new attendance group.
5. Click **Save**.

15.6 Configure Attendance Parameters

You can configure the attendance parameters, including the weekends, absence rule, overtime parameters, attendance check point, leave type, etc.

15.6.1 Define Weekends

The days of weekends may vary in different countries and regions. HikCentral Professional provides weekends definition function. You can select one or more days as the weekends according to actual requirements, to set different attendance rules for weekends from workdays.

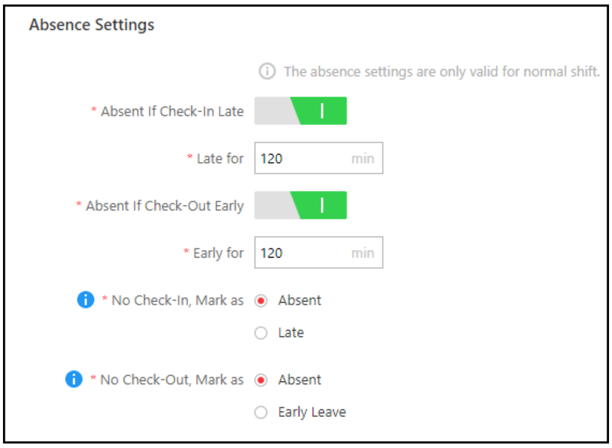
Click **Time & Attendance → Attendance Settings → General Rule** and in the Weekend Settings area, select the date(s) from Monday to Sunday . The attendance data of the selected date(s) will be calculated as the weekends' rule.

15.6.2 Define Absence

You can define the global rules about absence. When the employee's attendance conforms to rules, the attendance record will be marked as absent or other defined status.

Click **Time & Attendance → Attendance Settings → General Rule** and in the Absence Settings area, you can define the absence rules. There are four rules provided for absence as follows.

- Enable **Absent If Check-In Late** function and set the period. When the employee's check-in time is late for the period or longer, her/his attendance status on that day will be marked as absent.
- Enable **Absent If Check-Out Early** function and set the period. When the employee's check-out time is early for the period or longer, her/his attendance status on that day will be marked as absent.
- If no check-in record found for the person on one day, her/his attendance status on that day will be marked as absent or late for certain period according to your settings.
- If no check-out record found for the person on one day, her/his attendance status on that day will be marked as absent or early leave for certain period according to your settings.



Absence Settings

The absence settings are only valid for normal shift.

* Absent If Check-In Late: On

* Late for: 120 min

* Absent If Check-Out Early: On

* Early for: 120 min

* No Check-In, Mark as: ● Absent ○ Late

* No Check-Out, Mark as: ● Absent ○ Early Leave

Figure 15-5 Define Absence

15.6.3 Configure Overtime Parameters

Overtime is the amount of time someone works beyond normal work hours. It is generally used for the pay received for this time, applying overtime exchange holiday, etc. You can configure the overtime parameters for workday, weekends and holiday, including work hour rate, overtime level, attendance status for overtime, etc.

Steps

1. Click **Time & Attendance → Attendance Settings → Overtime** to enter the overtime settings page.
2. Set **Work Hour Rate** for every overtime level.

   Example

   Work Hour Rate is used to calculate work hours by multiplying it by overtime. When you work for certain period after end-work time on workday, you will reach different overtime level: overtime level 1, overtime level 2 and overtime level 3. You can set different work hour rates for three overtime levels. For example, your valid overtime is one hour (in overtime level 1), and the work hour rate of overtime level 1 is set as 2, so the work hours in the period will be calculated as 2 hours.
3. Set **Calculate Overtime** switch to on and set required information.

   By Total Work Hours

   The overtime of this calculation mode is calculated according to the additional work hours which exceed the required work hours.

   You need to set a period as the valid overtime rule. The additional work hour longer than this period is valid.

   For example, if you set it as 60 minutes, then if the employee works for 59 minutes more than the required work hours, the overtime is calculated as 0. If the employee works for 61 minutes more than the required work hours, the overtime is calculated as 61.

   By Time Points

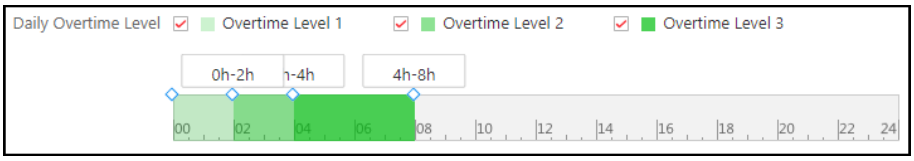
   The overtime of this calculation mode is calculated according to the additional work hours which is earlier than start-work time point and later than end-work time point in one day.

   You can enable **Count Early Check-In as OT** and **Count Late Check-Out as OT** and set one period for each. The overtime is valid when the employee works earlier than start-work time or later than end-work time for a period.

   For example, if you set **Earlier than Check-In Time for 60 min Mark as Valid Overtime**, and the start-work time is 9:00, then when the employee's check-in time is 8:00, the valid overtime is 0. When the employee's check-in time is 7:59, the valid overtime is 61 minutes.

   Daily Overtime Level

Check the overtime level and drag on the time bar to set the time range for selected overtime level(s). The total work hours will be calculated according to the work hour rate of the overtime level.



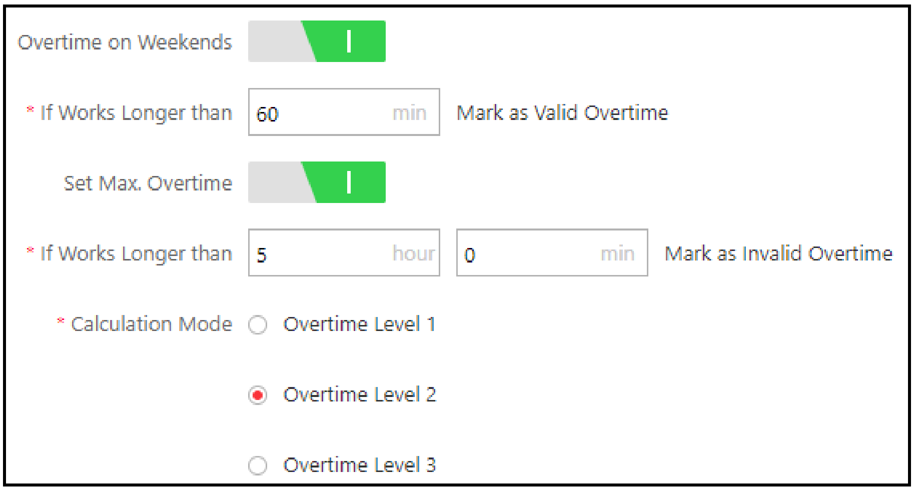
Daily Overtime Level ☑ 🟩 Overtime Level 1 ☑ 🟩 Overtime Level 2 ☑ 🟩 Overtime Level 3

Figure 15-6 Set Daily Overtime Level

Overtime on Weekends

You can set the rule for overtime on weekends and select the calculation mode. The work hour within one period range should be valid.

For example, If you set the parameters as follows, then when the employee's work hour is less than 60 minutes, her/his valid overtime is 0.



Overtime on Weekends: On

* If Works Longer than 60 min Mark as Valid Overtime

Set Max. Overtime: On

* If Works Longer than 5 hour 0 min Mark as Invalid Overtime

* Calculation Mode ○ Overtime Level 1
● Overtime Level 2
○ Overtime Level 3

Figure 15-7 Set Overtime on Weekends

4. Set overtime rule for holidays.

Note

You can set the period for valid or invalid overtime on holiday and select the overtime level as calculation mode for added holidays. The work hour within one period range should be valid. Refer to description about overtime on weekends in step 3 for details.

5. Click **Save**.

15.6.4 Add Attendance Check Point

You should set the doors or cameras which support facial recognition (such as DeepinView series camera, and the camera connected with DeepinMind series NVR) as attendance check points, so that the check-in/out by credentials (such as swiping card on the door's card reader, or face detected by the camera) will be valid and will be recorded.

Steps

1. Click **Time & Attendance → Attendance Settings → Attendance Check Point** to enter the attendance check point management page.
2. Click **Add**.
3. Select type for attendance check point to set as check-in only, check-out only, or check in & out.

   Check-In&Out

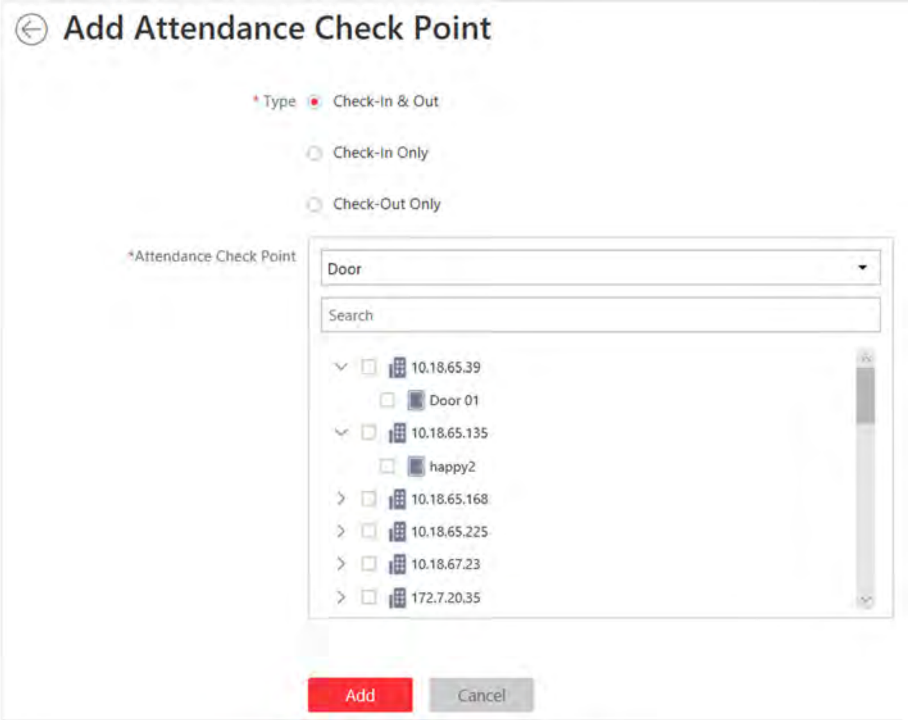
   The attendance records of check-in or check-out on the attendance check point are valid.

   Check-In Only

   The attendance records of swiping card or face recognition on the attendance check point will be only calculated as check-in. The users cannot check out on this check point.

   Check-Out Only

   The attendance records of swiping card or face recognition on the attendance check point will be only calculated as check-out. The users cannot check in on this check point.
4. Select **Door** or **Camera** from drop-down list.



Add Attendance Check Point

*Type ● Check-In & Out
○ Check-In Only
○ Check-Out Only

*Attendance Check Point: Door

Figure 15-8 Add Attendance Check Point

All the doors or cameras which haven't been set as attendance check point will be displayed.

5. Select the door(s) or camera(s) to be added.
6. Click **Add**.

   The selected resource(s) will be displayed in the attendance check point list.

7. Perform the following operations.

Change Check Point's Type
For the added attendance check points, you can select one or more items and click **Set as Check-In Only**, **Set as Check-Out Only**, or **Set as Check-In/Out** from drop-down list to change the current type to another.

Delete Check Point
To delete the added attendance check point, select the added attendance check point(s) and click **Delete**.

Note

If the attendance check point is deleted, the attendance records on this attendance check point will be deleted as well, and it will affect the persons' attendance results for the days on which the attendance data haven't been calculated.

15.6.5 Manage Leave Type

Leave type means the reason for a period of time that the employee is away from one's common work place. It is generally used for attendance management of the company. You can customize the leave type (major leave type and minor leave type) according to actual needs. You can also edit or delete the leave type.

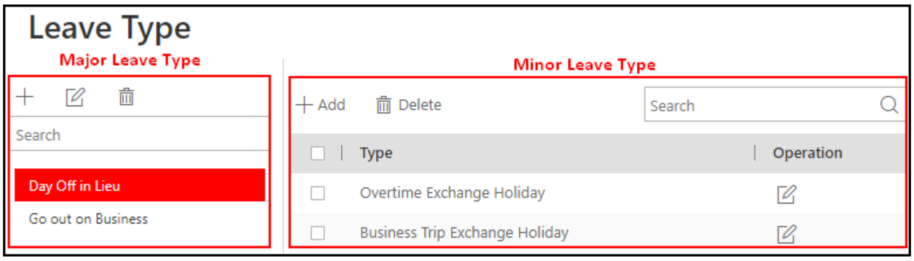
Click **Time & Attendance → Attendance Settings → Leave Type** to enter leave type management page.

In the Major Leave Type area, you can add, edit or delete the major leave types.

- Add Major Leave Type: Click + and enter the leave type name to save a new major leave type.
- Edit/Delete Major Leave Type: Select a major leave type and click ✎ or × to edit or delete the selected major leave type.

Select a major leave type, the minor leave types belonging to the major leave type display in the Minor Leave Type area. You can add, edit or delete the minor leave types.

- Add Minor Leave Type: Click **Add** and enter leave type name to add a new minor leave type.
- Edit Minor Leave Type: Click ✎ on the Operation column to edit the major leave type.
- Delete Minor Leave Type: Select the minor leave type(s) and click **Delete** to delete the selected major leave type.



□	Type	Operation
□	Overtime Exchange Holiday	✎
□	Business Trip Exchange Holiday	✎

Figure 15-9 Manage Leave Type

15.7 Manage Attendance Record

The persons' attendance records will be recorded and stored in the system. You can search the records by setting the search conditions to view the attendance details and view the person's attendance report. You can also correct check-in/out time for the exceptional records according to actual needs.

15.7.1 Search Attendance Record

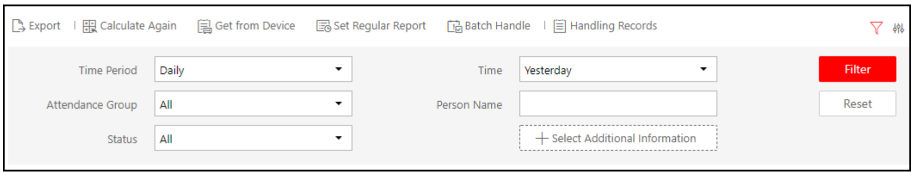
You can search the attendance records to view the person's attendance status by setting the search conditions.

Before You Start

- Make sure the person information is not expired.
- Make sure the person's attendance group is not expired. Or the attendance records will not be recorded. For setting the attendance group's effective period, refer to ***Add Attendance Group*** .

Steps

1. Click **Time & Attendance → Records and Handling** to enter the attendance record page.
2. In the filter panel, set the search conditions.



Time Period: Daily

Time: Yesterday

Attendance Group: All

Person Name:

Status: All

Figure 15-10 Set Search Condition

Time Period / Time

Set the time range of the attendance records you want to search. You can set one year's time range at most and search the persons' attendance records recorded within three years.

Attendance Group

Select the attendance group or person to view the attendance report. By default, it will search all.

Status

You can search the attendance record for certain status. For example, if you want to view the late arrival record, you can select **Late** to search.

Select Additional Information

You can search the attendance record by more custom condition(s). Click **Select Additional Information** to select the additional search condition(s).

Note

For more details for adding additional condition, refer to ***Custom Additional Information*** .

3. Click **Filter** to filter the attendance records according to the search conditions.
4. **Optional:** Perform the following operations.

View Person's Attendance Records

Click the person name to view the person's attendance records.

Note

Hover the cursor on the date to view the detailed work time, including scheduled work time and actual work time.

Select Display Items

Click and select the items displayed in the search result.

Export Attendance Records

Click **Export** to export the filtered attendance records and save in your PC.

Note

For more details, refer to ***Export Attendance Records*** .

Handle Attendance / View Handling Records

You can also correct the check-in/out or apply for leave for the exceptional attendance status if necessary. You can also view the handling records for that. For details, refer to ***Correct Attendance Record for Single Person*** , ***Apply for Leave for Multiple Persons*** and ***View Attendance Handling Records*** .

Set Regular Report

Click **Set Regular Report** to pre-define the report content and the report will be sent automatically to the email address you configured. Refer to ***Send Attendance Report Regularly***

15.7.2 Correct Attendance Record for Single Person

After searching the person's attendance record, you can correct one person's check-in/out time according to actual needs.

Steps

1. Click **Time & Attendance → Attendance Record** to enter the attendance record page.
2. Search the attendance records.

Note

For details, refer to ***Search Attendance Record*** .

3. If you set **Daily** as time period, perform one of the followings to enter the correcting check-in/out time page. If you select other time periods, you can only perform the second choice to enter the correcting check-in/out time page.
   - Click 📅 in the Operation column.
   - Click the name in the list of attendance records, hover the cursor over the date and click **Handle**.
4. Select **Correct Check-in/out**.
5. Set the correction type and time.
6. **Optional:** Enter the remarks, such as correction reason.
7. Click **Save**.

15.7.3 Correct Check-In/Out for Multiple Persons

You can correct multiple persons' check-in/out time in a batch according to actual need (e.g., the employees forgot to check in or check out).

Steps

1. Click **Time & Attendance → Record and Handling** to enter the attendance record page.
2. Click **Batch Handle**.
3. Select **Correct Check-in/out**.
4. Choose one of the following operations for handing.
   - Select Persons: Select one or multiple persons in attendance group(s), and set corrected type and time.

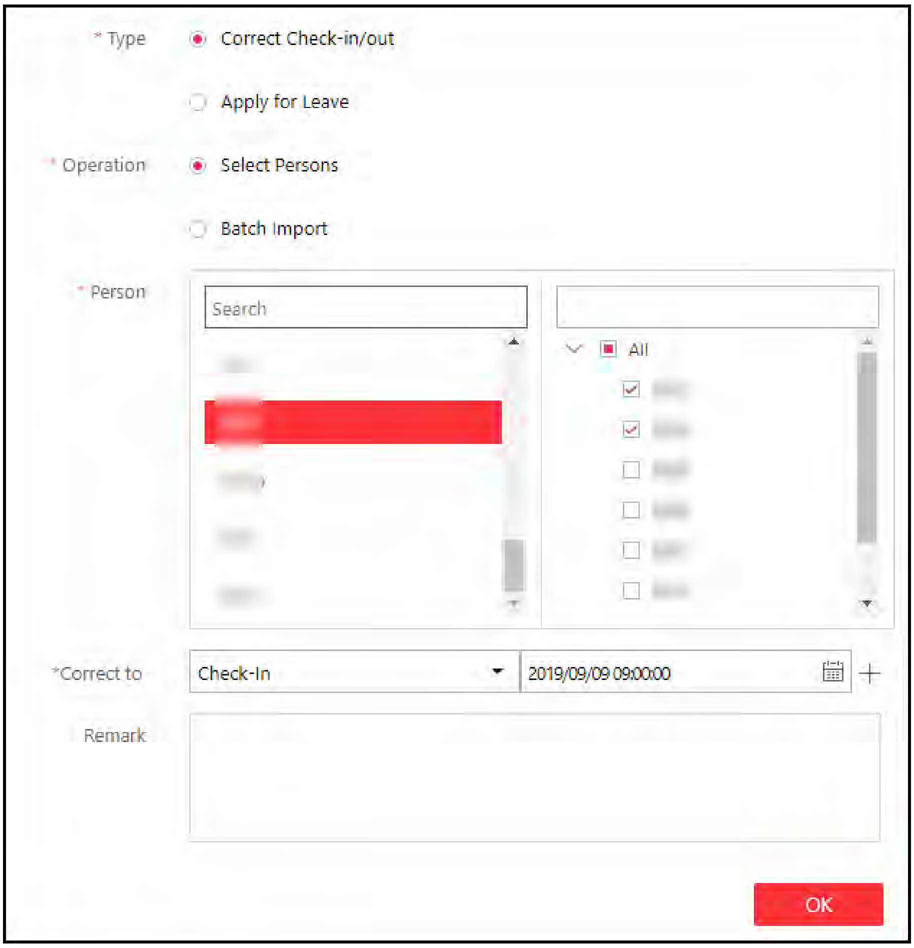
     Note

     Up to 10,000 persons can be selected at a time.

   - Batch Import: Click **Download Template** and edit the related information in the downloaded template, then click ··· and import the template with the corrected attendance records.

     Note

     If failed, you can export the wrong information, and import the edited information again.



* Type ● Correct Check-in/out

○ Apply for Leave

* Operation ● Select Persons

○ Batch Import

* Person

*Correct to Check-In 2019/09/09 09:00:00

Remark

Figure 15-11 Batch Correct Check-In/Out by Selecting Persons

5. Click **OK**.

Note

The system will recalculate the attendance results according to the imported attendance records.

15.7.4 Apply for Leave for Single Person

After searching the person's attendance record, you can apply for leave according to actual needs.

Steps

1. Click **Time & Attendance → Attendance Record** to enter the attendance record page.
2. Search the attendance records.

Note

For details, refer to ***Search Attendance Record*** .

3. If you set **Daily** as time period, perform one of the followings to enter the applying for leave page. If you select other time periods, you can only perform the second choice to enter the applying for leave page.
   - Click in the Operation column.
   - Click the name in the list of attendance records, hover the cursor over the date and click **Handle**.
4. Select **Apply for Leave**.
5. Set the leave type and time.
6. **Optional:** Enter the remarks, such as leave reason.
7. Click **Save**.

15.7.5 Apply for Leave for Multiple Persons

You can apply for leave for multiple persons when they want to ask for leave or go on a business trip.

Before You Start

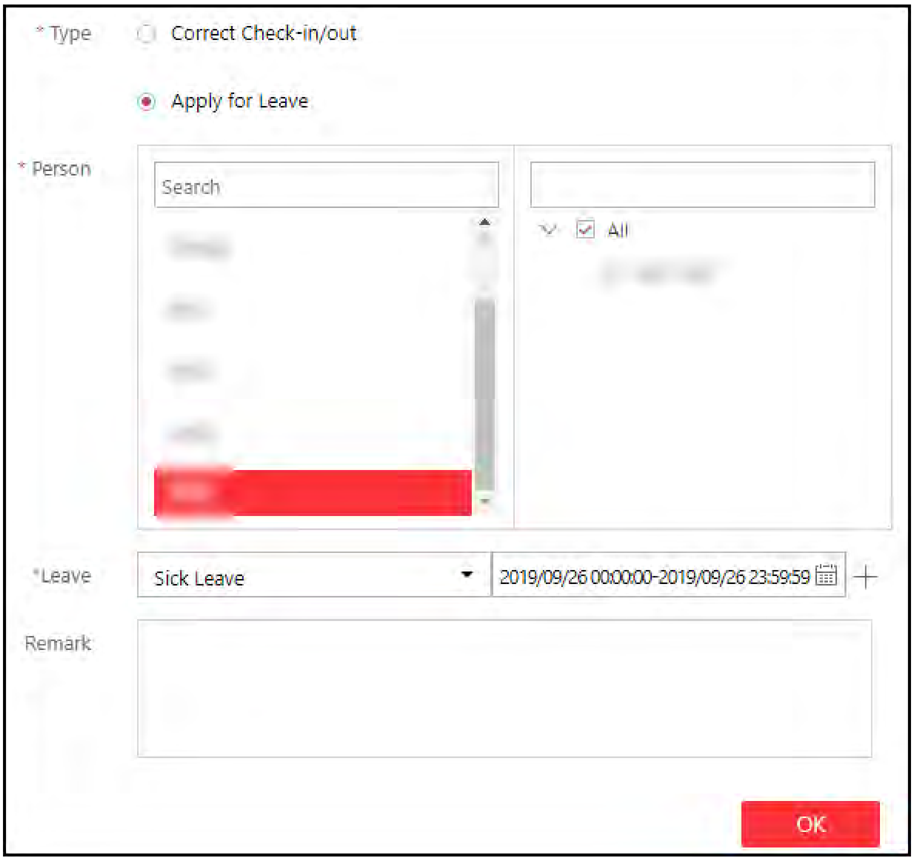
Make sure the required leave type have been defined. For more details, refer to ***Manage Leave Type*** .

Steps

1. Click **Time & Attendance → Attendance Record and Handling** to enter the attendance record page.
2. Click **Batch Handle**.
3. Select **Apply for Leave**.
4. Select one or multiple persons in attendance group(s), and set leave type and time.

   Note

   Up to 10,000 persons can be selected at a time.
5. **Optional:** Enter some words as remark, such as leave reason.



* Type ○ Correct Check-in/out

● Apply for Leave

* Person

Search

☑ All

*Leave Sick Leave 2019/09/26 00:00:00-2019/09/26 23:59:59

Remark

Figure 15-12 Apply for Sick Leave

6. Click **OK**.

Note

The system will recalculate the attendance results according to the imported attendance records.

15.7.6 Manually Calculate Attendance Results

If attendance group or shift schedule changes, abnormal attendance is handled, etc. you can calculate the attendance data manually according to the latest settings. After calculating, the original data will be replaced by new attendance data.

Steps

Note

HikCentral Professional can calculate the attendance data automatically at the fixed time (4 o'clock by default) every day. You can edit the time point in **Time & Attendance → General Rule** .

1. Click **Time & Attendance → Records and Handling** .

2. Click **Calculate Again** to open the calculation settings window.
3. Set the start time and end time as the **Time Period** for attendance data.
4. Select **All Persons** or **Specified Persons** for attendance calculation.
5. Click **Calculate**.

Note

It can only calculate the attendance data within three months.

15.7.7 Export Attendance Records

The attendance records can be exported in Excel, PDF, or CSV format and be saved in the local PC. You can select the items to display in the exported file.

Before You Start

- Make sure the person information is not expired.
- Make sure the person's attendance group is not expired. Or the attendance records will not be recorded. For setting the attendance group's effective period, refer to ***Add Attendance Group*** .

Steps

1. Click **Time & Attendance → Records and Handling** to enter the attendance record page.
2. In the filter panel, set the search conditions to filter attendance records.

   Note

   For more details, refer to ***Search Attendance Record*** .

3. Click **Export** and select the format and items to export the filtered attendance records and save in your PC.

   Note

   The exported file is in Excel, PDF, or CSV format. If the file is larger than 50 MB, the file will be compressed to a ZIP package.

15.7.8 Get Attendance Records from Device

Some causes (such as abnormal running status and offline devices) may lead to asynchronous attendance data between HikCentral Professional and the devices. You can use this function to get the latest attendance records from the devices.

Click **Time & Attendance → Records and Handing** . Click **Get from Device** and select door(s) to get attendance data from the device(s).

15.7.9 View Attendance Handling Records

Attendance handling records show the added attendance handling information, including check-in/out correction and leave application. You can view the handling details, cancel the handling operation or export the record here.

Click **Time & Attendance → Records and Handling** .

Click **Handling Record** to view the attendance handling records. You can perform the following operations.

- Filter Handling Record: Click ▽ and set conditions (e.g., Name, ID, Time, etc.) to filter the handling records.
- Undo Handing Operations: Select the handling record(s) and click **Undo** to cancel the handling operations. The correction records will be deleted in the page and the previous attendance status will also be restored.
- Export Handling Record: Click **Export** to save the handling records in CSV or Excel format in the local PC.

15.8 Configure Attendance Report

Attendance report is the statistics of the attendance results of the specific attendance group(s) or person(s) in a certain time period. For example, the employer or related persons can view the employees' attendance via attendance report and make it as the standard of performance evaluation or pay. You can define the display rules on the report, and manually export report.

15.8.1 Set Display Rules for Attendance Report

You can configure the contents displayed in the attendance report, such as the company name, logo, date format, time format, and marks of different attendance status.

Click **Time & Attendance → Attendance Report → Report Display** to set the following display rules.

Company Information

The company information (including company name and logo) will be displayed on the cover page of the attendance report. You can customize the company name. You can also upload a picture for the logo.

Format of Date and Time

The formats of date and time may vary for the persons in different countries or regions. You can set the date format and time format according to the actual needs.

Marks of Different Status

In the report, different marks indicate different attendance status respectively. You can customize these marks according to actual needs.

Weekend Mark in Report

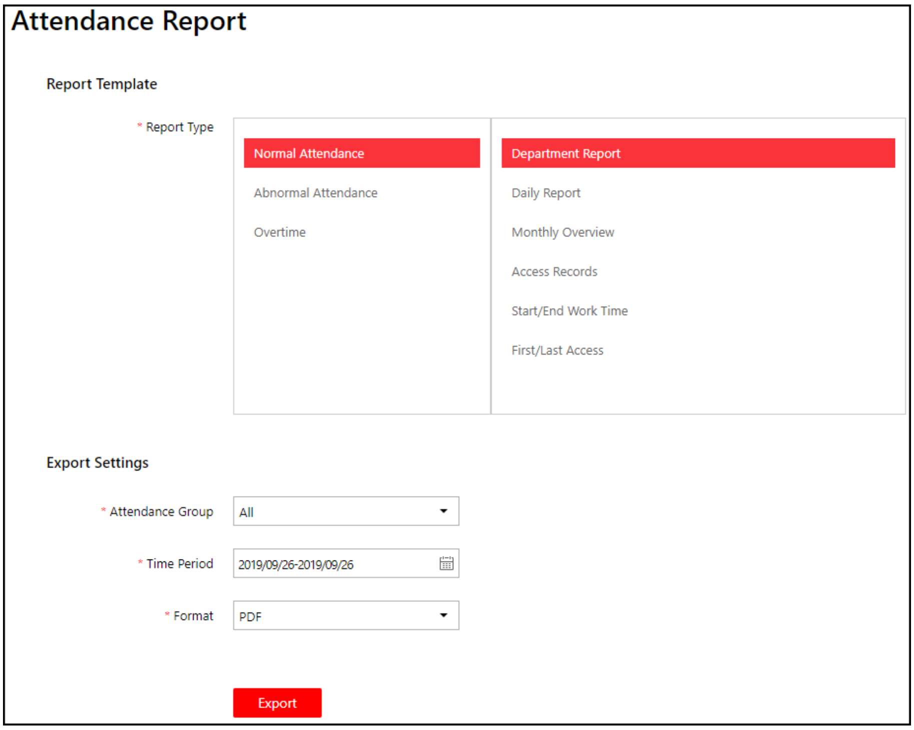
In the report, the weekends will be marked with special marks.

15.8.2 Export Attendance Report

HikCentral Professional supports multiple report types and you can export a series of attendance reports manually to view the employees' attendance data.

Steps

1. Click **Time & Attendance → Attendance Report → Export Report** to enter the attendance report page.



Attendance Report

Report Template

* Report Type: Normal Attendance; Department Report

Export Settings

* Attendance Group: All

* Time Period: 2019/09/26-2019/09/26

* Format: PDF

Figure 15-13 Export Attendance Report

2. Select a report type.
3. Select the attendance group or person for exporting the attendance report.
4. Set the start time and end time during which the attendance data will be displayed in the report.
5. Select report format.
6. Click **Export**.

   The report will be generated in the format and save in local PC.

Chapter 16 Manage Entrance and Exit

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 pre-define 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.

16.1 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.

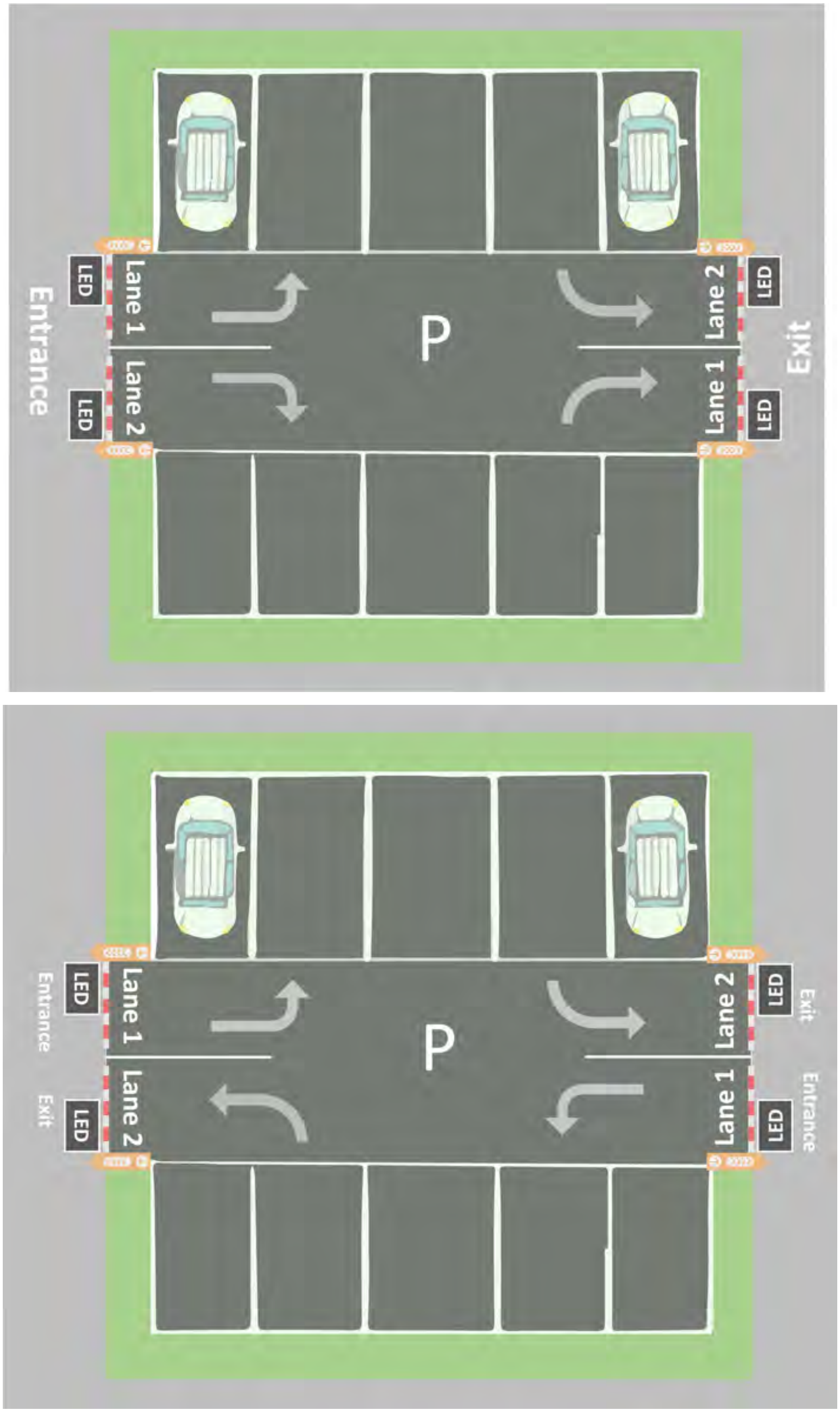


Figure 16-1 Parking Lot

16.1.1 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. On the Home Page, click **Vehicle** to enter the Vehicle module.
2. Click **Create Parking Lot** to open the Create Parking Lot window.

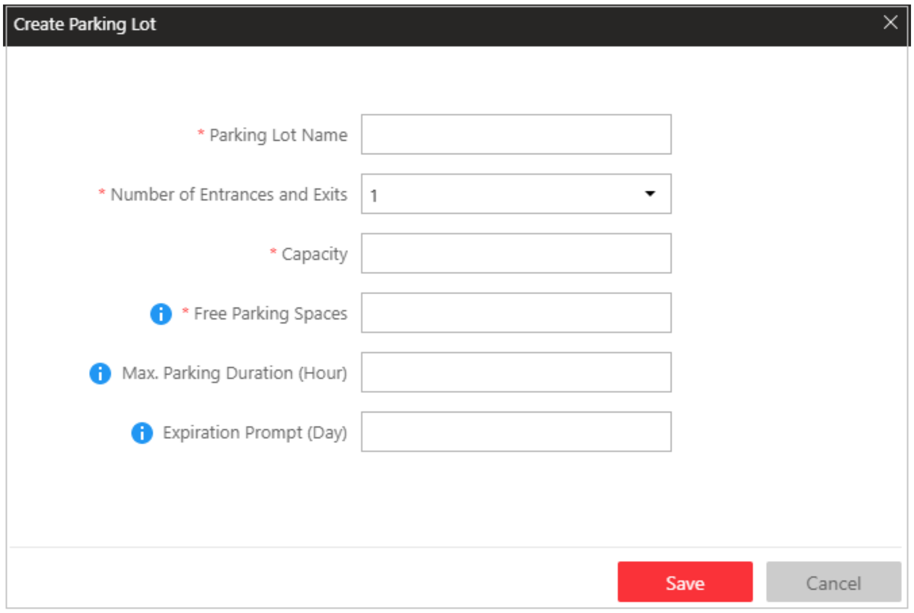


Figure 16-2 Create Parking Lot Window

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.

Free 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/free parking spaces/Max. parking duration/expiration prompt.

      Example

      Free Parking Spaces: if the free parking space amount is not the same with the actual amount, you can edit it here.
   3) Click **Save**.

16.1.2 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 blacklist 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. On the Home page, click **Vehicle → Parking Lot → +** to open the add entrance and exit window.
2. Enter the entrance and exit name.
3. Click **Save**.

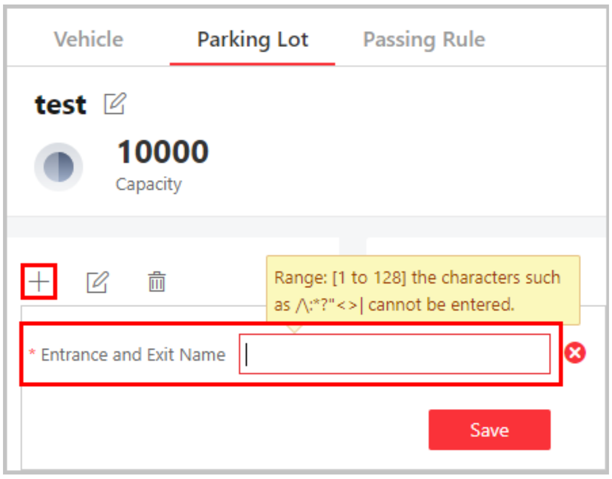


Figure 16-3 Enter Entrance and Exit Name

What to do next

Add lane for the entrance and exit. See ***Add Lane*** for details.

16.1.3 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 blacklist; the access control device/video intercom device cannot control the barrier without swiping a card specialized for the parking lot.

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. On the Home page, click **Vehicle → Parking Lot →** + to enter the Add Lane page.
2. Select the lane type as **Entrance** or **Exit**.
3. Enter the lane name.

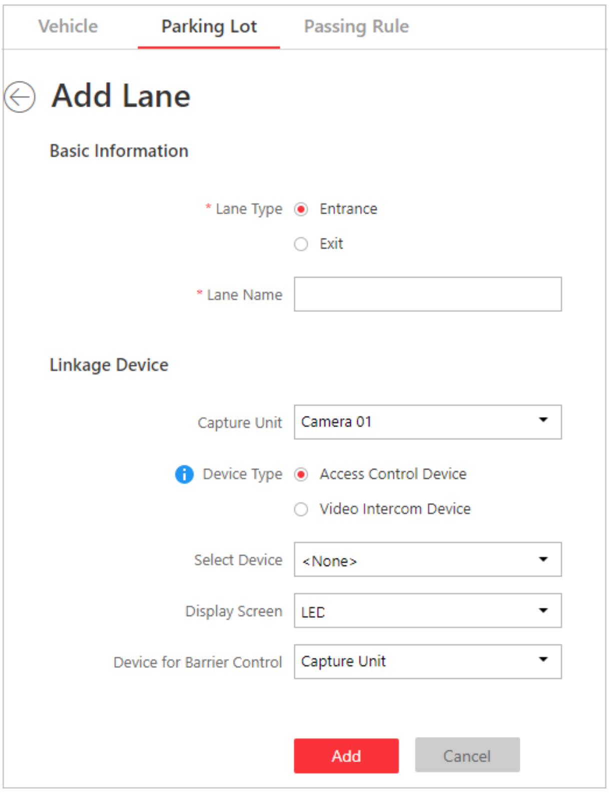


Figure 16-4 Add Lane Page

4. **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 blacklist. See ***Manage Entry & Exit Rule*** for details about setting an entry & exit rule.

   2) Select the device type for swiping card or video intercom when entering/exiting the parking lot as access control device or video intercom device.
   3) Select a device for swiping card or video intercom in 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.

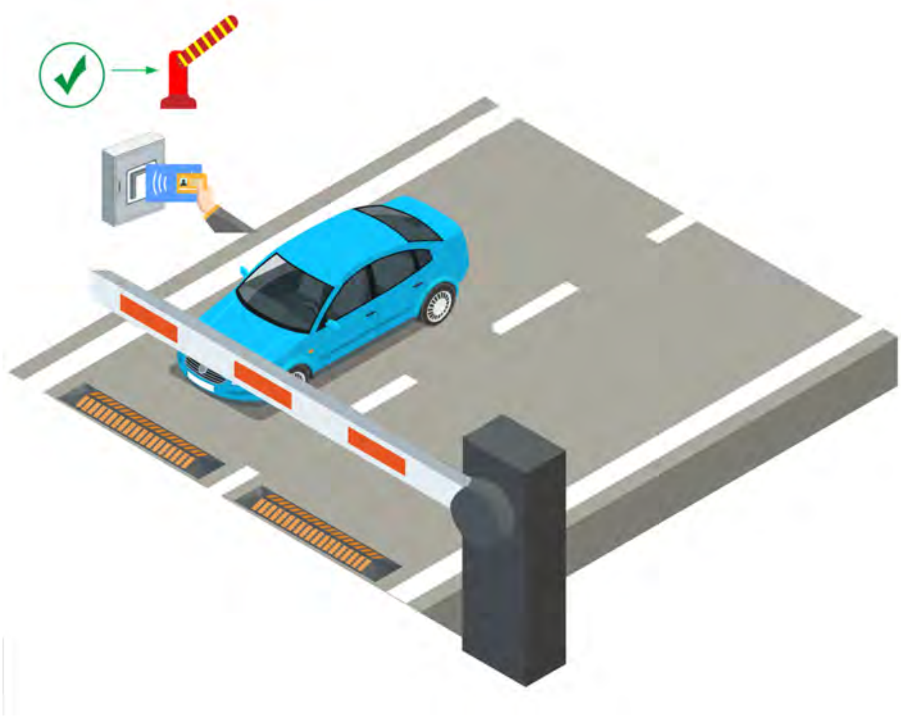


Figure 16-5 Opening Barrier by Card Swiping

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.

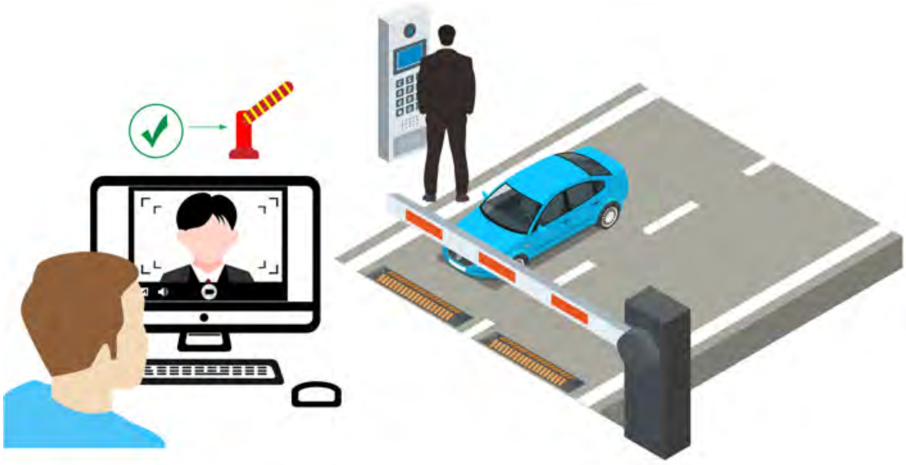


Figure 16-6 Opening Barrier by Video Intercom

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.

5. Click **Add**.

16.1.4 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.

Click **Physical View → Display Screen → 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.

16.1.5 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.

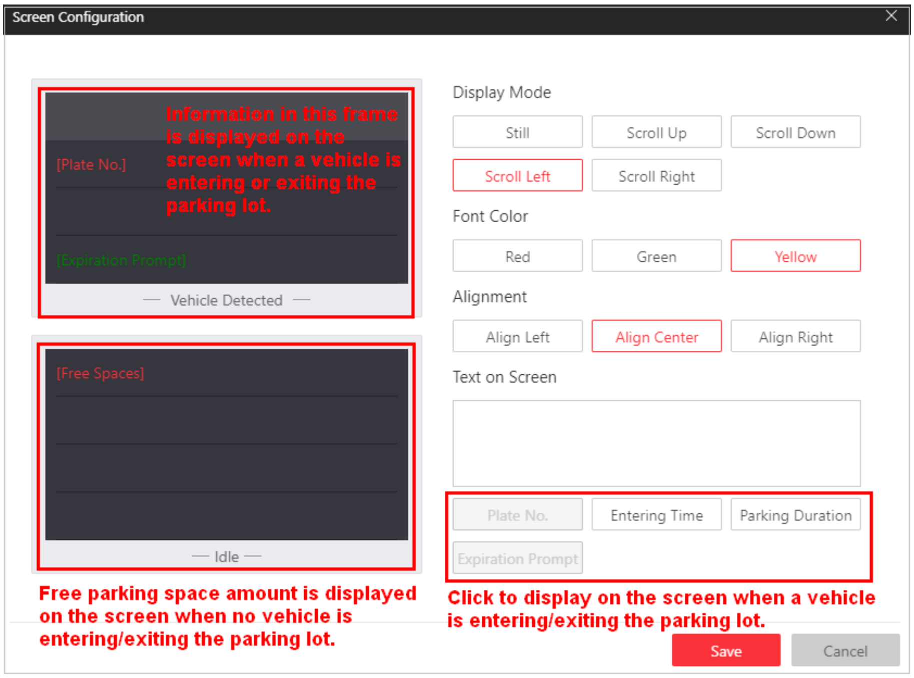
Before You Start

Make sure you have linked a display screen to a lane.

Steps

1. On the Home page, click **Vehicle → Parking Lot** .
2. Select an entrance and 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.

16.2 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 import the vehicle information to the system. You can 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. For entrance and exit control, you can set entry & exit rules for the vehicles managed in the system to define whether to allow the vehicles to enter or exit.

16.2.1 Add Vehicle List

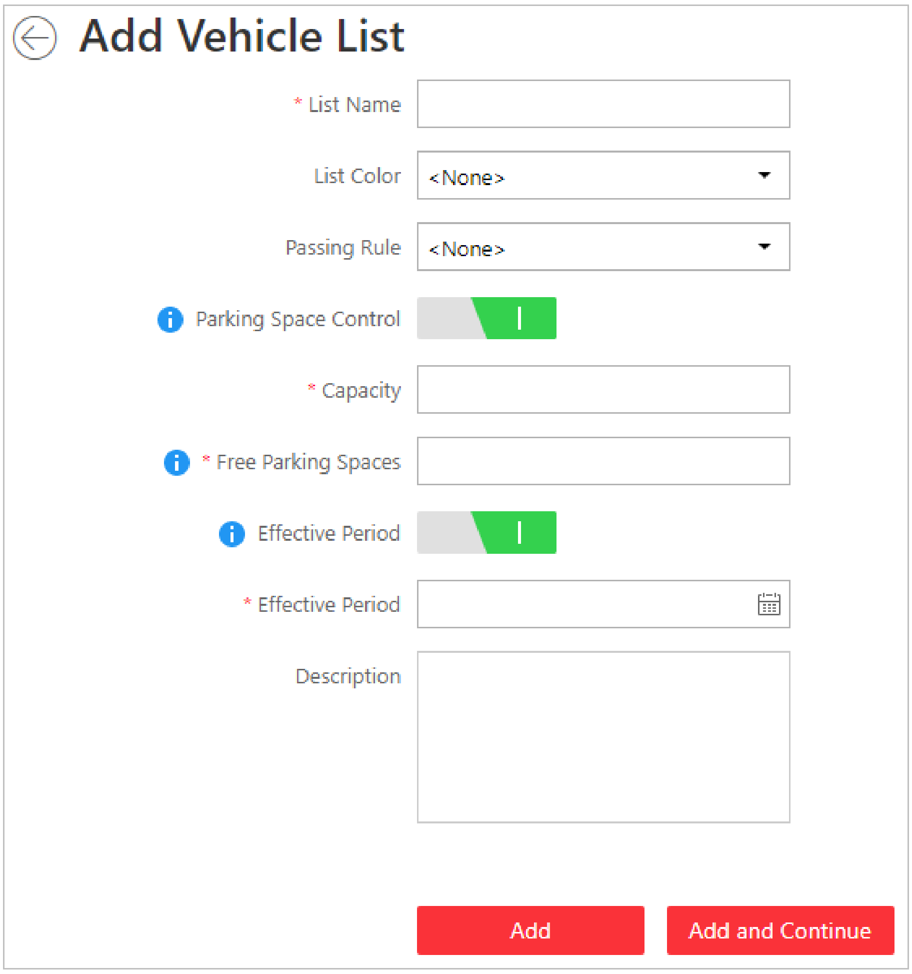
To add vehicle information to the system, you should create a vehicle list first. When you are adding a vehicle list, you configure an entry & exit rule (when and how to open the barrier for entry & exit), set parking space information, and effective period for it. Vehicle list helps you manage the different vehicles. For example, you add a list for VIP vehicles that enjoy certain privileges, or add a blacklist 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. Click **Vehicle** to enter the Vehicle Management page.
2. Click **Vehicle →** + to enter the add vehicle list page.



Add Vehicle List

* List Name

List Color <None>

Passing Rule <None>

Parking Space Control

* Capacity

* Free Parking Spaces

Effective Period

* 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 free 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 free parking spaces of the parking lot.

Note

Vehicles will not be allowed to enter the parking lot if there is no free 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.

16.2.2 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. Click **Vehicle** to enter the Vehicle Management page.
2. Click **Vehicle** tab and select a vehicle list.
3. Click **Import** to open the Import window.

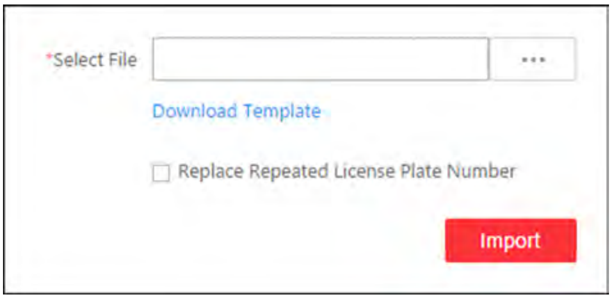


Figure 16-9 Import Window

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.

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

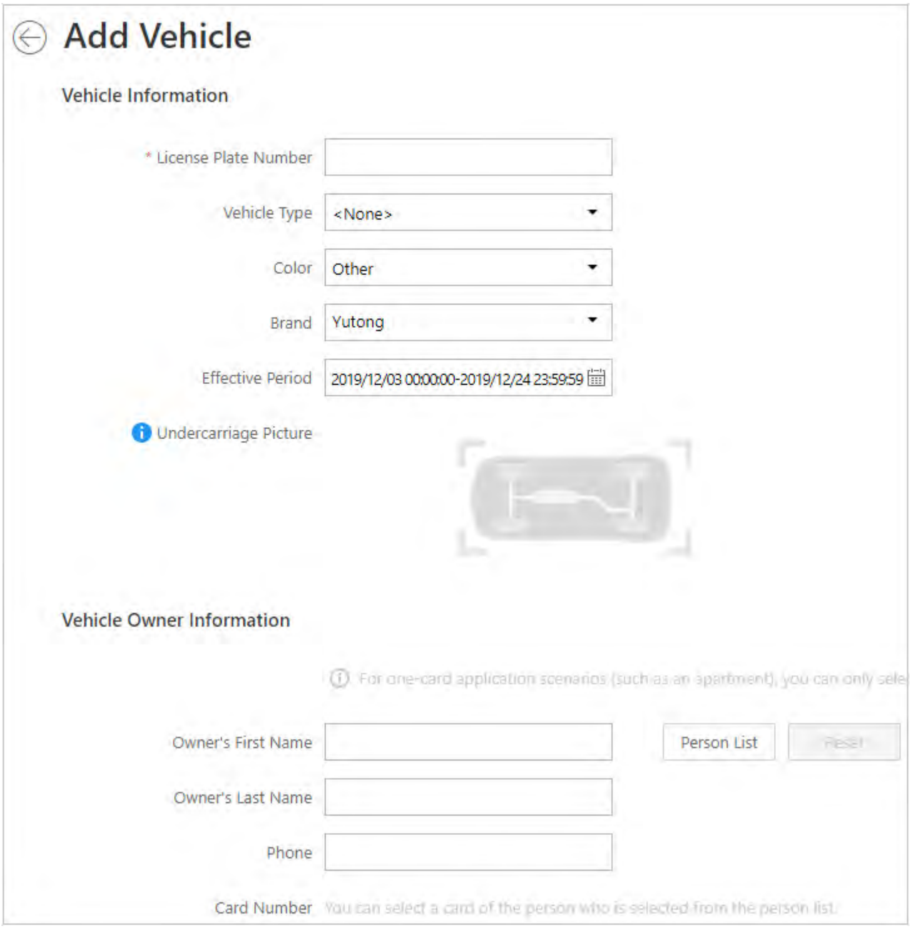
You can add single vehicle information manually.

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. Click **Vehicle** to enter the Vehicle Management page.
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 Other

Brand Yutong

Effective Period 2019/12/03 00:00:00-2019/12/24 23:59:59

Undercarriage Picture

Vehicle Owner Information

For one-card application scenarios (such as an apartment), you can only sele

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. **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.

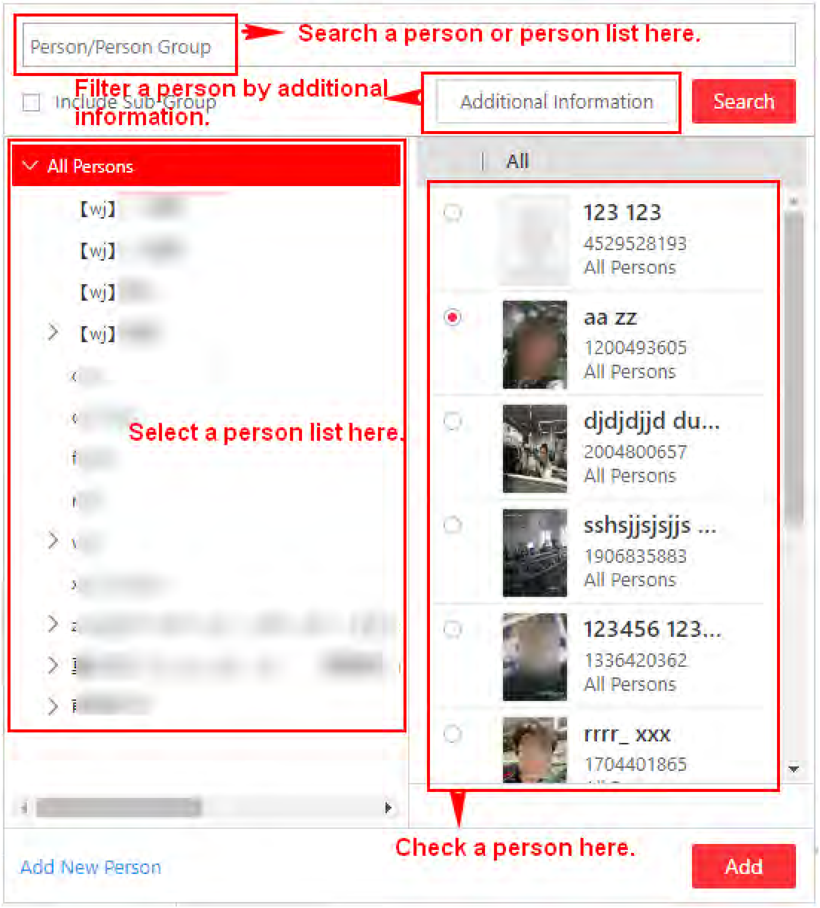


Figure 16-11 Add Person in Person List as Vehicle Owner

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.

6. 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.

7. **Optional:** Perform the following operations after importing the vehicle information.

Edit Vehicle Information	Click the plate number in License Plate Number column to edit the vehicle information
Edit Effective Period	Select the vehicle(s) and click **Edit Effective Period** to edit the effective period of the selected vehicle(s) in a batch. If the license plate number is expired, it cannot trigger an event or alarm when license plate number matched if license plate number matched event/alarm is configured.
Delete Vehicle Information	Check the vehicle information and click **Delete** to delete the selected vehicle information
Export Vehicle Information	Click **Export All** to save the vehicle information of the list (CSV file) to your PC, which can be imported to other vehicle list.

16.3 Manage Entry & Exit Rule

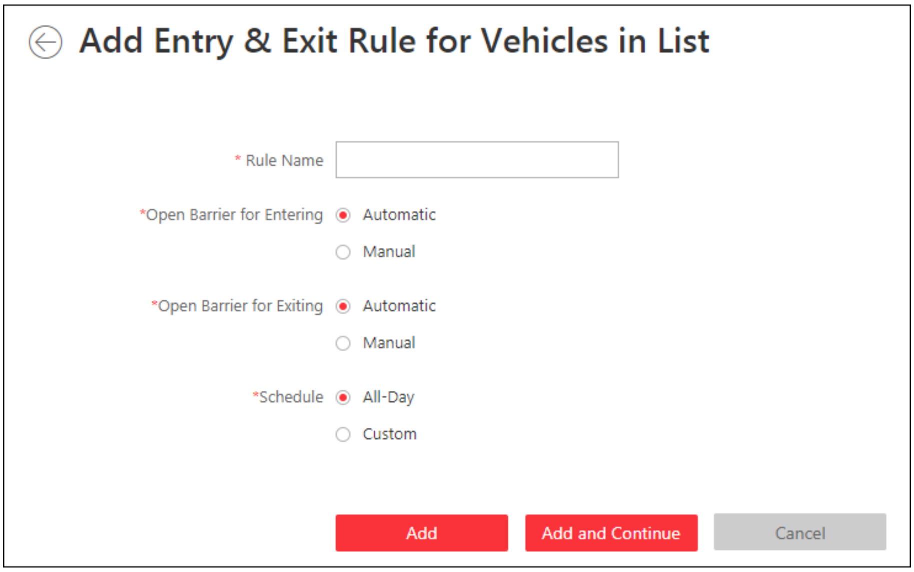
An entry & exit rule defines how to open barrier when the system detects a vehicle at the lane. The system can open the barrier automatically when detects a vehicle, or you can also open it manually by clicking **Allow** button on the Control Client after verifying its identity.

You can set entry & exit rules for vehicles in the vehicle lists and temporary vehicles which are not in any vehicle lists.

16.3.1 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.

Enter **Vehicle → Entry & Exit Rule → Rule for Vehicles in List** , and 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 "blacklist" 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 "blacklist" 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.

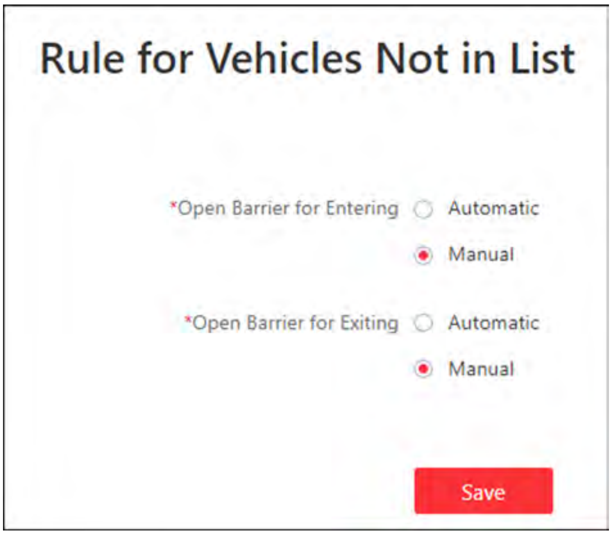
You can click **Erase** and click on the drawn time period to clear the corresponding drawn time period.

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*** .

16.3.2 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.

Enter **Vehicle → Entry & Exit Rule → Rule for Vehicles Not in List** , and click **Add** to add an entry & exit rule for vehicles in vehicle 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 Vehicle 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.

Chapter 17 Manage Facial Comparison

HikCentral Professional supports facial recognition and comparison functions. After adding devices which support facial 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 list, 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.

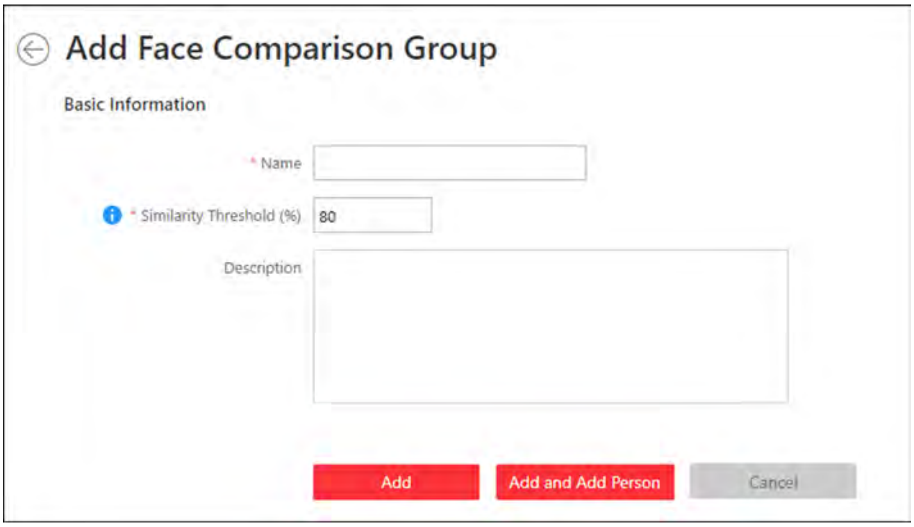
When a person's face is detected and it matches or mismatches the person information in the face comparison group, an event/alarm (if configured) will be triggered to notify the security personnel and you can view the face comparison information during live view on the Control Client.

17.1 Add Face Comparison Group

After adding the person(s), you can add a face comparison group and add person(s) to the group for face comparison.

Steps

1. Click **Person → Face Comparison Group → Add** to enter the adding face comparison group page.



Add Face Comparison Group

Basic Information

* Name

* Similarity Threshold (%) 80

Description

Figure 17-1 Add Face Comparison Group

2. Create a name for the face comparison group.
3. Set the face comparison similarity threshold which affects the frequency and accuracy of face picture comparison alarm. When the face comparison similarity is higher than the configured threshold, the camera will regard the person as matched.
4. **Optional:** Enter the description information if needed.

5. Confirm to add the face comparison group.
   - To add persons to the face comparison group, click **Add and Add Person** and perform the following steps.
   - To save the face comparison group first and add persons to the face comparison group later, click **Add** to finish this task and return to the face comparison group list.
6. **Optional:** If you click **Add and Add Person**, you will enter the next page to add persons to this face comparison group.
   1) In the **Add from** field, choose to add existing persons or add a new person to this group.

      Existing Person

      Add existing persons in the system to this face comparison group.

      Add New Person

      Add a new person to this face comparison group. The person will be added to the person list as well.
   2) **Optional:** If you select **Existing Person**, you can filter persons in the person list by entering keywords of person name, person group name, or additional information.

      Person List

      Filter persons in the person list by entering keywords of person name, person group name, or additional information.

      Note

      You can click **Additional Information** to enable the custom additional information as search condition.

      Face Comparison Group

      Add all the persons in the selected face comparison group(s) to this face comparison group.
7. **Optional:** After adding the persons to the face comparison group, you can do one or more of the followings.

   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 issuing cards, importing and exporting persons. For details, refer to ***Manage Person List*** .

   Edit Face Comparison Group

   Click ✎ in the Operation column to edit its details and edit the cameras that it is applied to.

   Delete Face Comparison Group

   Select one face comparison group and click **Delete** to delete it.

   Delete All Face Comparison Groups

   Click **Delete All** to delete all the added face comparison groups.

What to do next

After adding the face comparison group and configuring the persons in the group, you should apply the group to the camera which supports face comparison to take effect. For details, refer to ***Apply Face Comparison Group to Device*** .

17.2 Apply Face Comparison Group to Device

After setting the face comparison group and adding person(s) to the group, you need to apply the group settings to the camera which supports face picture comparison so that the camera can compare the detected faces with the face pictures in the face comparison group and trigger alarms (if configured). After applying the face comparison group to the device, if the data in the group are changed (such as adding a person to the group, removing person from the group, etc.), the system will automatically apply the data in the group to the device to take effect.

Before You Start

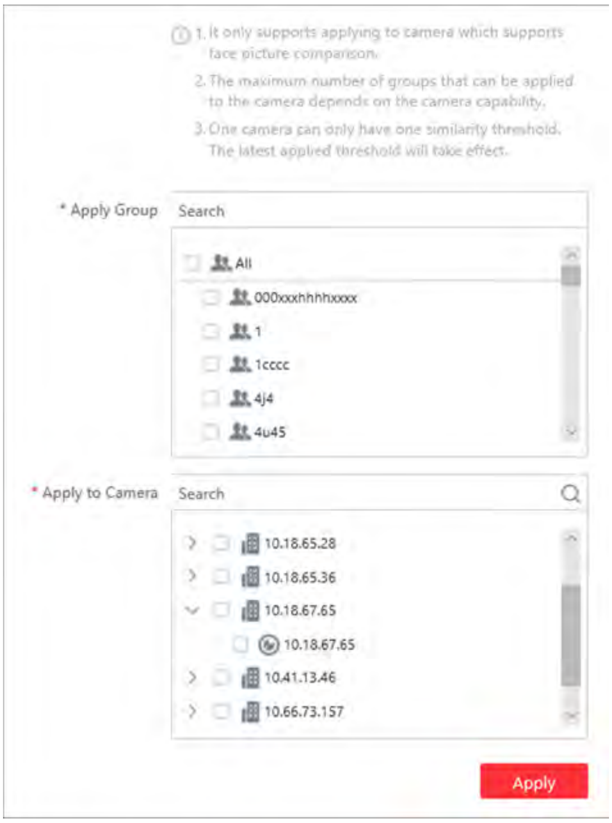
Add camera which supports face picture comparison to the system.

Steps

Note

- Currently it only supports applying to camera which supports face picture comparison.
- The maximum number of groups that can be applied to the camera depends on the camera capability.
- Make sure your license supports facial recognition function, or turn to Home page, click **License Details → Configuration → Add** and then select the added cameras as facial recognition cameras. Otherwise, facial recognition function cannot perform normally in the system.

1. Click **Person → Face Comparison Group** to enter the face comparison group management page.
2. Click **Apply to Device**.



1. It only supports applying to camera which supports face picture comparison.

2. The maximum number of groups that can be applied to the camera depends on the camera capability.

3. One camera can only have one similarity threshold. The latest applied threshold will take effect.

Figure 17-2 Apply Face Comparison Group to Device

3. Select the face comparison group(s) to be applied.
4. Select the camera(s) to apply the selected face comparison group(s) to.
5. Click **Apply** to start applying.

   The applying progress will display in the Operation column.

6. **Optional:** If there exists applying failed face comparison group, the ⓘ icon will display near the group name. Hover the cursor to the icon to check the prompt.

Note

You can click **Retry** to apply this group to the linked camera(s) again. Click **Details** to view the exception details.

Chapter 18 Dock Station

The dock station is a data collector which can automatically detect and back up law-enforcement data and evidence 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*.

18.1 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.

18.1.1 Add Dock Station by IP/Domain

When you know the IP address or domain name of the to-be-added dock station, 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 access control devices you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the HikCentral Professional via network.

Steps

1. Click **Physical View → Dock Station** to enter the dock station management page.
2. Select **IP/Domain** as the adding mode.
3. 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.

4. **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.
5. Configure the dock station group.

   Note

   Dock station group is a group of persons (usually policemen or policewomen). Only when the persons are added to the dock station, can the data in their body cameras be backed up to the dock station.

   - Click **Add New** in the **Dock Station Group** drop-down list to add a new dock station group.

     Note

     For details about adding dock station group, see ***Add Dock Station Group*** .
   - Select a dock station group from the **Dock Station Group** drop-down list.
6. Finish adding the dock station.
   - 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.
7. **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.

18.1.2 Add Dock Stations by IP Segment

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

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. Click **Physical View → Dock Station** to enter the dock station management page.
2. Click **Add** to enter the Add Dock Station page.
3. Select **IP Segment** as the adding mode.
4. 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***.

5. **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.
6. 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.
7. **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.

18.1.3 Add Dock Stations by Port Segment

When multiple to-be-added dock stations have the same IP address, user name and password, but have different port numbers, which are within a range, you can select this adding mode and specify the port range, IP address, user name, password, and other related parameters to add them at a time.

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. Click **Physical View → Dock Station** to enter the dock station management page.
2. Click **Add** to enter the Add Dock Station page.
3. Select **Port Segment** as the adding mode.
4. 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.

5. **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.
6. 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.
7. **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.

18.1.4 Add Dock Stations in Batch

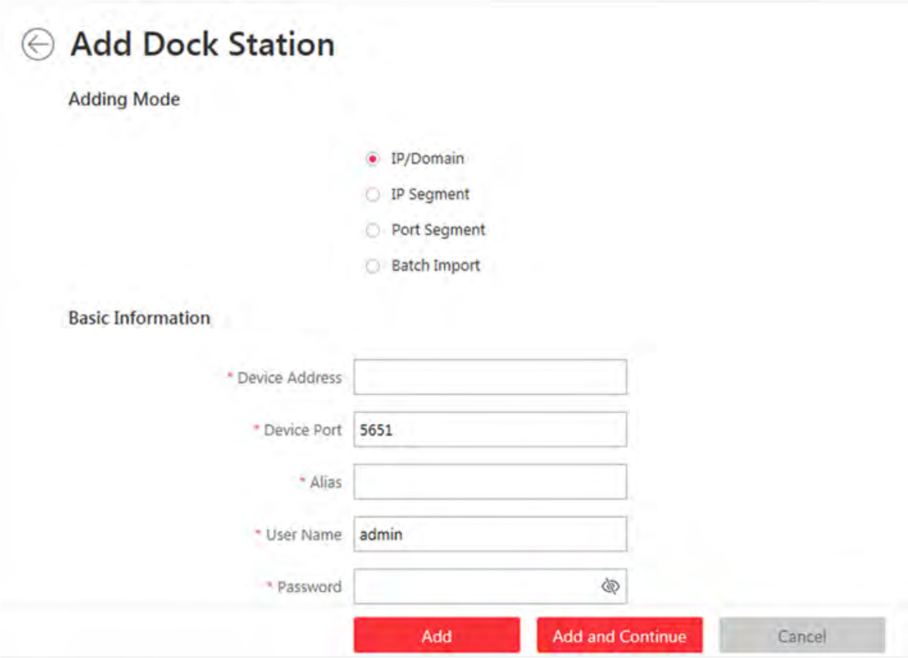
When there are multiple dock stations need to be added to HikCentral Professional, you can download a predefined template and fill in the required information about the dock stations, and then import the template to the system to add multiple dock stations at a time.

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. Click **Physical View → Dock Station** to enter the dock station management page.
2. Click **Add** to open the Add Dock Station page.



Add Dock Station

Adding Mode

● IP/Domain

○ IP Segment

○ Port Segment

○ Batch Import

Basic Information

* Device Address	
* Device Port	5651
* Alias	
* User Name	admin
* Password	

Figure 18-1 Add Dock Station Page

3. Select **Batch Import** as the adding mode.
4. Click **Download Template** and save the predefined template (CSV file) on your PC.
5. Open the template file and enter the required information of the devices to be added on the corresponding column.
6. Click ••• and select the template file.
7. **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.
8. 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.
9. **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.

18.2 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. Click **Person → Dock Station Group → Add** to enter the adding dock station group page.

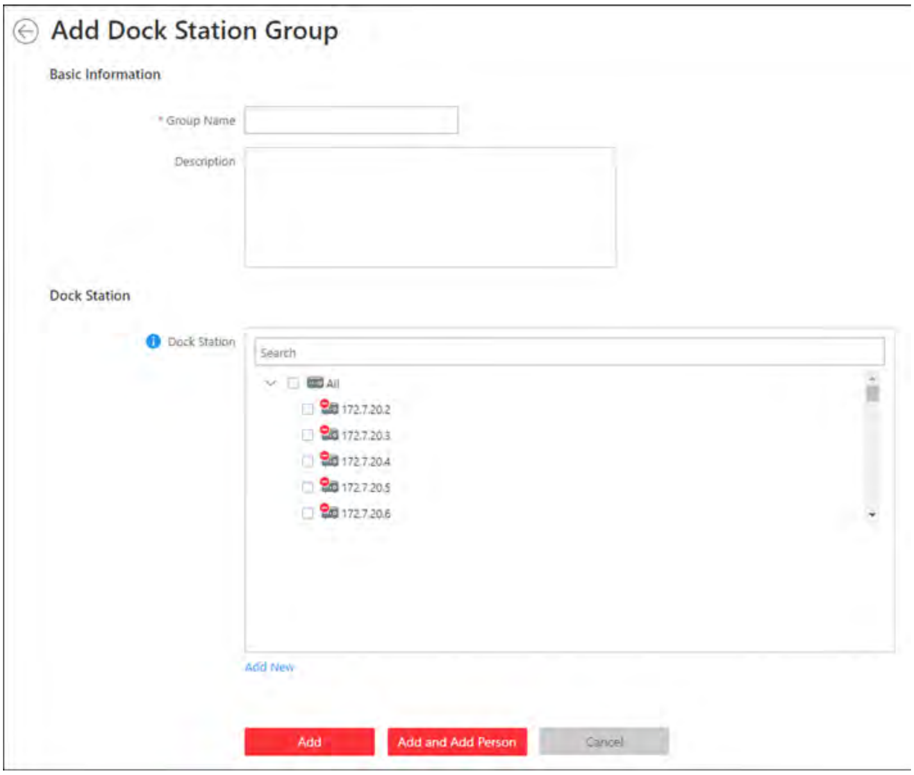


Figure 18-2 Add Dock Station Group

2. Set the basic information.

   Group 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.

3. Select the dock station(s) to link them to the selected persons.

   Note

   You can click **Add New** to add a new dock station to the system. For details, refer to ***Manage Dock Station*** .

4. Confirm to add the dock station group.
   - To add persons to the dock station group, click **Add and Add Person** and perform the following steps.

- To save the dock station group first and add persons to the dock station group later, click **Add** to finish this task and return to the dock station group list.

5. **Optional:** If you click **Add and Add Person**, you will enter the next page to add persons to this dock station group.

Note

Up to 20 persons can be added to one dock station group.

1) In the **Add from** field, choose to add existing persons or add a new person to this group.

Existing Person

Add existing persons in the system to this dock station group.

Add New Person

Add a new person to this dock station group. The person will be added to the person list as well.

2) **Optional:** If you select **Existing Person**, you can filter persons in the person list by entering keywords of person name, person group name, or additional information.

Note

You can click **Additional Information** to enable the custom additional information as search condition.

6. Click **Add** to add the selected persons to the dock station group.
7. **Optional:** After adding the dock station group, you can do one or more of the followings.

Edit Dock Station Group	Click ✎ in the Operation column to edit its details.
Manage Persons in Dock Station Group	Click the added dock station 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 issuing cards, importing and exporting persons. For details, refer to ***Manage Person List*** .
Delete Dock Station Group	Select one dock station group and click **Delete** to delete it.
Delete All Dock Station Groups	Click **Delete All** to delete all the added dock station groups.

Chapter 19 Manage Security Control

A security control device detects people, vehicles, etc., entering a pre-defined 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.

19.1 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.

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

   Server Network

   As the default selection, the detected online devices in the same local subnet with the 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.
3. In the Online Device area, select **Hikvision Private Protocol** or **Hikvision ISUP Protocol** to filter the detected online devices.
4. In the Online Device area, select the active device to be added .
5. Click 🗋 to open the Add Online Device window.
6. 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.

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 Channel to Area** switch to ON to import the channels (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 channels to area, you cannot perform the further configurations for the channels.

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

   Server Network

   The detected online devices in the same local subnet with the 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.
3. In the Online Device area, select **Hikvision Private Protocol** or **Hikvision ISUP Protocol** to filter the detected online devices.
4. In the Online Device area, select the active devices to be added.
5. Click 🗋 to open the Add Online Device window.
6. 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.
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 Channel to Area** switch to on to import the channels (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 channels to area, you cannot perform the further configurations for the channels.

9. Click **Add**.
10. **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.

19.1.2 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. Click **Physical View → Security Control Device** to enter the Security Control Device Management page.
2. Click **Add** to enter the Add Security Control Device page.
3. Select **Hikvision Private Protocol** as the Access Protocol.
4. Select **IP Address** as the adding mode.
5. 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.

6. **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.

7. **Optional:** Set the **Add Channel to Area** switch to on to import the channels (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 channels to area, you cannot perform further operations for the channels.
   - 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.

8. 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.

9. 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.

19.1.3 Add Security Control Device by Hik-Connect

You can add the security control devices which have been added to the Hik-Connect account to the system.

Before You Start

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

Steps

1. Click **Physical View → Security Control Device** to enter the Security Control Device Management page.
2. Click **Add** to enter the Add Security Control Device page.
3. Select **Hikvision Private Protocol** as the Access Protocol.
4. Select Hik-Connect as the adding mode.
5. 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.

6. 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 new device, enter the serial No. of the device.

Verification Code

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

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 Channel to Area** switch to on to import the channels (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 channels to area, you cannot perform the further configurations for the channels.

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. **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.

19.1.4 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. Click **Physical View → Security Control Device** to enter the Security Control Device Management page.
2. Select **Hikvision Private Protocol** as the Access Protocol.
3. Click **Add** to enter the Add Security Control Device page.
4. Select **IP Segment** as the adding mode.
5. Enter the required the information.

   Note

   By default, the device port No. is 8000.

   Caution

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

7. **Optional:** Set the **Add Channel to Area** switch to on to import the channels (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 channels to area, you cannot perform the further configurations for the channels.

8. 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.
9. 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.

19.1.5 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. Click **Physical View → Security Control Device** to enter the Security Control Device Management page.
2. Click **Add** to enter the Add Security Control Device page.
3. Select **Hikvision Private Protocol** as the Access Protocol.
4. Select **Port Segment** as the adding mode.
5. 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.

6. **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.

7. **Optional:** Set the **Add Channel to Area** switch to on to import the channels (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 channels to area, you cannot perform the further configurations for the channels.

8. 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.
9. 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.

19.1.6 Add Security Control Device by Device ID

For the security control devices supporting ISUP Protocol, you can add them by specifying a predefined device ID, key, 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.

Steps

1. Click **Physical View → Security Control Device** to enter the Security Control Device Management page.
2. Click **Add** to enter the Add Security Control Device page.
3. Select **Hikvision ISUP Protocol** as the Access Protocol.
4. Select **Device ID** as the adding mode.
5. Enter the required information, including device ID, key, and device name.
6. **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.
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 Channel to Area** switch to on to import the channels (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 channels to area, you cannot perform the further configurations for the channels.

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.

19.1.7 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 Protocol 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.

Steps

1. Click **Physical View → Security Control Device** to enter the Security Control Device Management page.
2. Click **Add** to enter the Add Security Control Device page.
3. Select **Hikvision ISUP Protocol** as the Access Protocol.

4. Select **Device ID Segment** as the adding mode.
5. Enter the required information, including the start device ID and the end device ID, and the key.
6. **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.
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 Channel to Area** switch to on to import the channels (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 channels to area, you cannot perform the further configurations for the channels.

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.

19.1.8 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 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. Click **Physical View → Security Control Device** to enter the Security Control Device Management page.
2. Click **Add** to enter the Add Security Control Device page.
3. Select **Hikvision Private Protocol** or **Hikvision ISUP Protocol** as the Access Protocol.
4. Select **Batch Import** as the adding mode.
5. Click **Download Template** and save the predefined template (excel file) in your PC.
6. Open the exported template file and edit the required information of the devices to be added on the corresponding column.
7. Click ··· and select the template file.
8. **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 video.

   Note

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

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 other devices.
11. 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.

19.2 Link Alarm Inputs to Security Control Partition

After adding the security control device's zones to the system (called "alarm inputs" after added to the system), you should link them to different security control partitions in the system according to the relation between zones and partitions configured on the device.

Before You Start

Make sure the security control device's zones are added to the system and grouped into areas. For details, refer to ***Add Alarm Input to Area*** .

Steps

1. Click **Logical View** on the home page.
2. Choose one of the following methods to enter the area's resource group page.
   - Select one area and click ✎ to enter the editing area page.

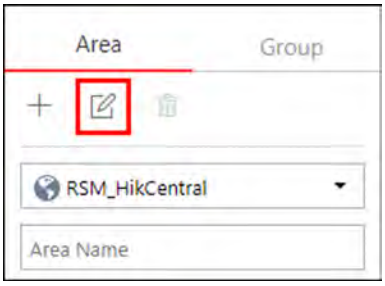


Figure 19-1 Enter Area Editing Page

   - Select **Group** tab on the left to display all the resource groups of different areas.

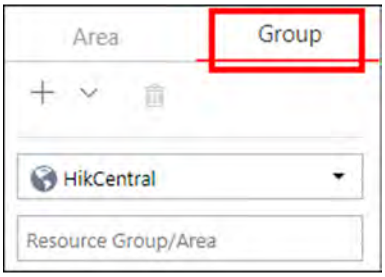


Figure 19-2 Enter Resource Group Page

3. In the Security Control Partition field, click **Add**.
4. Create a name for the security control partition.
5. In the drop-down list of Alarm Input field, select a security control device.

The alarm inputs of the security control device added to this area and haven't been added to any security control partitions are displayed.

6. Select the alarm inputs which you want to add to the security control partition.
7. Select a security control partition No. in the drop-down list which is gotten from the device you selected in Step 5.
8. **Optional:** Set a defense schedule for this partition, which defines how and when to arm the alarm inputs in the security control partition.

Note

For setting a new defense schedule, refer to ***Configure Defense Schedule Template*** .

9. Click **Add**.
10. **Optional:** Perform one or more of the following operations after linking alarm inputs to security control partition.

Edit Security Control Partition

Click ✎ to edit the partition settings. You can uncheck the alarm input(s) to remove the added alarm input(s) from the security control partition.

Note

After removing the alarm input(s) from the security control panel, the zones will be removed from this partition on the device, too.

Delete Security Control Partition

Click × to delete the added security control partition.

19.3 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 arming, instant arming, or away arming in one week. The system predefines two default defense schedule templates: All-day Template and Weekday Template. You can also add a customized template according to actual needs.

Steps

1. Click **System** on the home page and enter **Schedule → Defense Schedule Template** page.
2. Click **Add** to enter the adding defense schedule template page.
3. Set the required information.

Name

Set a name for the template.

Copy from

Optionally, you can select to copy the settings from other defined templates.

4. Select an arming mode and drag on the time bar to draw a time period.

Note

By default, the Time-based is selected.

Instant Arming

It is used when people leave the detection area. The zone will be immediately triggered when it detects event or alarm with no delay and notify the security personnel.

Away Arming

It is used when people leave the detection area. Event or alarms will be activated when the zone is triggered or tampered. For delayed zone, the alarm will not be activated when the zone detects triggering event during entry/exit delay.

Stay Arming

It is used when people stay inside the detection area. During stay arming, all the perimeter burglary detections (such as perimeter detector, magnetic contacts, curtain detector in the balcony) will be turned on. Meanwhile, the detectors inside the detection area are bypassed (such as PIR detectors). People can move inside the area and not trigger an event or alarm.

Note

Up to 8 time periods can be set for each day.

5. **Optional:** Click **Erase** and click on the drawn time period to clear the corresponding drawn time period.
6. Finish adding the defense schedule template.
   - Click **Add** to add the template and back to the defense schedule template list page.
   - Click **Add and Continue** to add the template and continue to add other template.

   The defense schedule template will be displayed on the defense schedule template list.
7. **Optional:** Perform the following operations after adding the template.

   View Template Details Click the template to view its details.

   Edit Template Click ✎ in the Operation column to edit template details (except the template(s) in use).

   Delete Template Click × in the Operation column to delete the template.

   Delete All Templates Click **Delete All** to delete all the schedule templates (except the default templates and the template(s) in use).

Chapter 20 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.

20.1 Add Role

You can assign the permissions to the roles as required, and the users can be assigned with different roles to obtain different permissions.

Steps

1. Click **Security → Roles** to enter the Role Management page.

   Note

   The system pre-defines two default roles: administrator and operator. You can click the role name to view the details and operations. But you cannot edit or delete the two default roles.

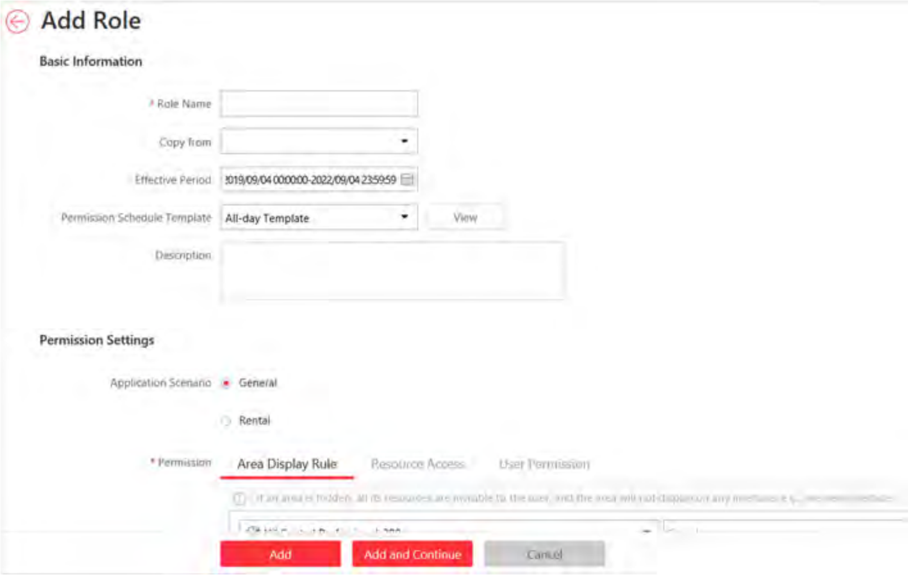
   Administrator

   The role that has all the permission of the system.

   Operator

   The role that has all the permission for operating the Control Client and has the permission for operating the Applications (Live View, Playback, and Local Configuration) on the Web Client.

2. Click **Add** to enter the Add Role page.



Add Role

Basic Information

*Role Name

Copy from

Effective Period: 019/09/04 00:00:00-2022/09/04 23:59:59

Permission Schedule Template: All-day Template

Description

Permission Settings

Application Scenario: ● General ○ Rental

*Permission

Figure 20-1 Add Role Page

3. Set the role name, effective period, permission schedule template, and description as desired.

   Effective Period

   The date that this role takes effective and turns invalid.

   Permission Schedule Template

   Set the authorized time period when the role's permissions are valid. Select **All-day Template/ Weekday Template/Weekend Template** as the permission schedule of the role, or click **Add New** customize a permission schedule for the role.

Note

- The role's permissions will expire when the current time is not in the authorized time period of the permission schedule.
- When the permissions expire, the role will be logged out and not allowed to login.
- The permission schedule's time zone is consistent with that of the system.
- If the role's permissions are invalid after editing the permission schedule, the role will be forced to login to the system again.
- By default, the role will be linked with All-day Template after updating the system.
- The permission schedule also goes for RSM client and OpenSdk client.

4. Set the permission for the role.
   - Select the default or pre-defined role from the **Copy from** drop-down list to copy the permission settings of selected role.
   - Select Application Scenario for the role. If you select **General**, you need to assign the permissions to the role; if you select **Rental**, you need to select access groups for the rental so that the role can be verified by the devices of the selected access groups.

Note

For a rental role, only Person module, person list, and access group are available.

Area Display Rule

Show or hide the specific area(s) for the role. If the area is hidden, the user with the role cannot view and access the area and its resources on any interface.

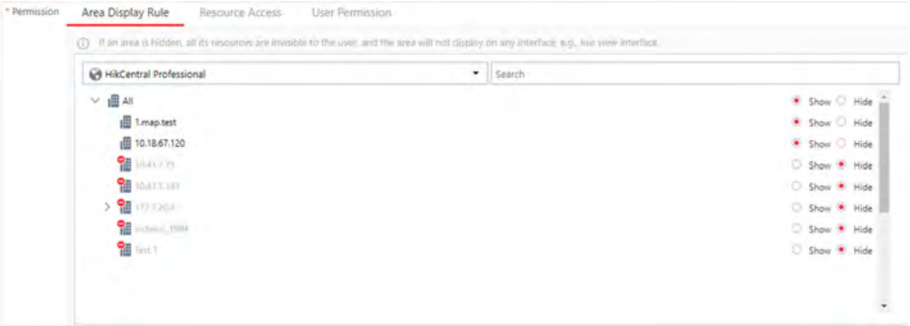


Figure 20-2 Area Display Rule

Resource Access Permission

Select the functions from the left panel and select resources from right panel to assign the selected resources' permissions to the role.

Note

If you do not check the resources, the resource permission cannot be applied to the role.

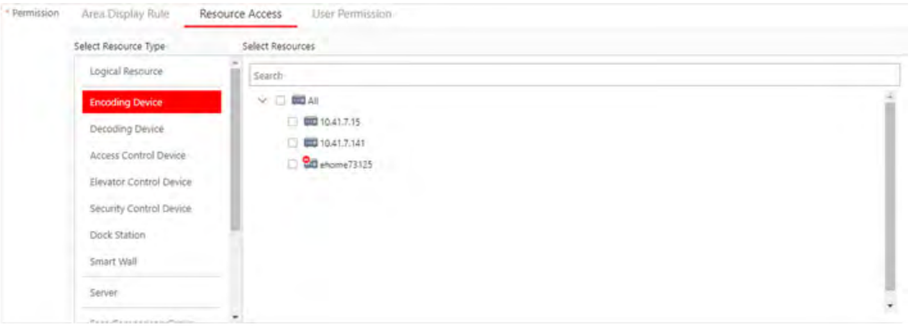


Figure 20-3 Resource Access Permission

User Permission

Assign the resource permissions, configuration permissions on the Web Client, and the control permissions on the Control Client to the role.

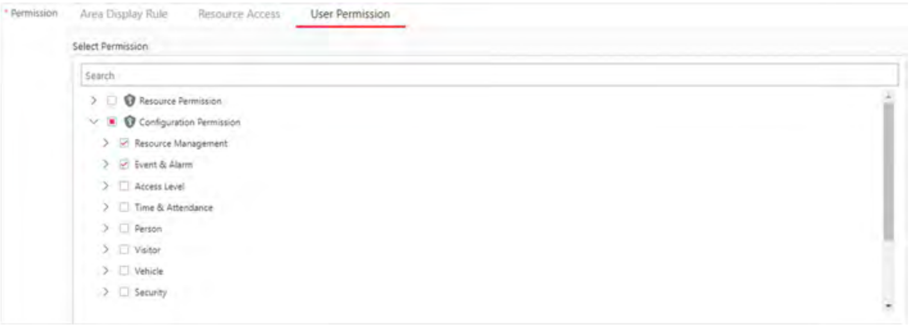


Figure 20-4 User Permission

5. Complete adding the role.
   - Click **Add** to add the role.
   - Click **Add and Continue** to save the settings and continue to add roles.
6. **Optional:** After adding the role, you can do one or more of the following:

Edit Role Click the **Name** field to edit the settings of the role.

Refresh Role Click **Refresh All** to get the latest status of the roles.

Delete Role Click **Delete** to delete the role.

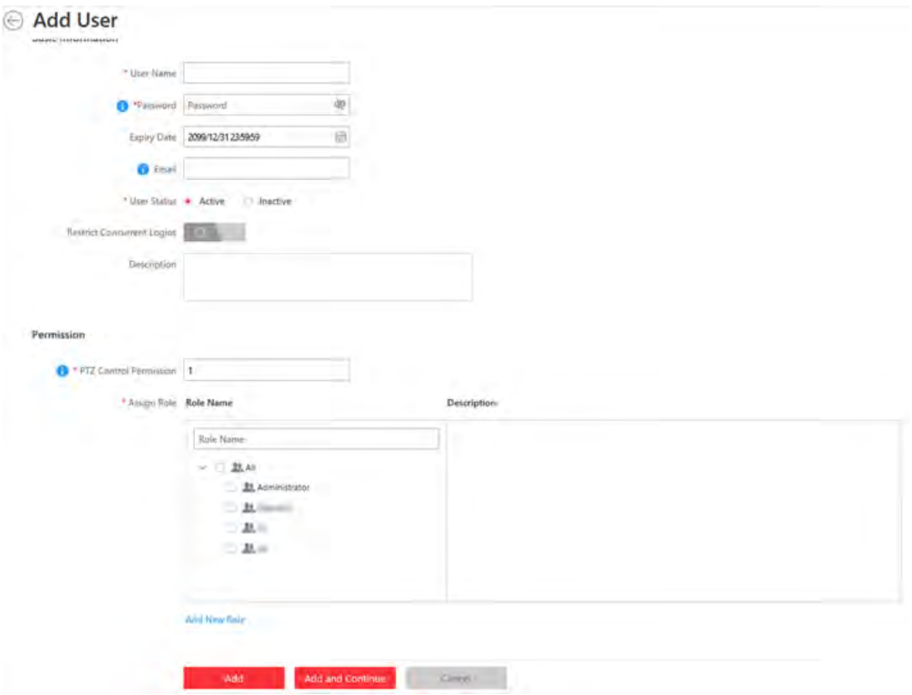
Filter Role Click ▽ to expand the filter conditions. Set the conditions and click **Filter** to filter the roles according to the set conditions.

20.2 Add Normal User

You can add normal users for accessing the system and assign role to the normal user. Normal users refer to all the users except the admin user.

Steps

1. Click **Security → Users** to enter the User Management page.
2. Click **Add** to enter the Add User page.



Add User

* User Name

*Password Password

Expiry Date 2099/12/31 235959

Email

* User Status ● Active ○ Inactive

Restrict Concurrent Logins

Description

Permission

* PTZ Control Permission 1

* Assign Role

Role Name	Description
□ All □ Administrator	

Figure 20-5 Add User Page

3. Set the required parameters.

User Name

For user name, only letters(a-z, A-Z), digits(0-9), and "-" can be contained.

Password

Create an initial password for the user which should be changed by the user for first time login.

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 this user account becomes invalid.

Email

The system can notify user by sending an email to the email address. If the normal user forget his/her password, he/she can reset the password via email.

Note

The email address of the admin user can be edited by the user with the role of administrator.

User Status

Two kinds of status are available. If you select freeze, the user account is inactive until you set the user status to active.

Restrict Concurrent Logins

If necessary, switch **Restrict Concurrent Logins** to on and enter the maximum number of concurrent logins.

4. Set the permission level (1-100) for PTZ control in PTZ Control Permission.

Note

The larger the value is, the higher permission level the user has. The user with higher permission level has the priority to control the PTZ unit.

Example

When user1 and user 2 control the PTZ unit at the same time, the user with higher PTZ control permission level will take the control of the PTZ movement.

5. Check the existing roles to assign the role(s) for the user.

Note

- If no role has been added, two default roles are selectable: administrator and operator.
  Administrator
  The role that has all permissions of the system.

  Operator
  The role that has all permissions of the system Control Client.
- If you want to add customized roles, you can click **Add New Role** to quickly enter the Add Role page. See ***Add Role*** for details.

6. Complete adding the user.
   - Click **Add** to add the user.
   - Click **Add and Continue** to save the settings and continue to add users.

Note

You will be asked to change the password when logging in for first time. See ***First Time Login for Normal User*** for details.

7. **Optional:** Perform the following operations after adding the normal user.

Edit User	Click the **Name** field of the user to edit the information
Reset Password	In the Edit User page, click **Reset** to enter 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 changing the password, refer to ***Change Password for Reset User*** .

Delete User
Select one or multiple users and click **Delete** to delete the selected user(s).

Force Logout
You can also select the online user and click **Force Logout** to log out the online user.

Inactive/ Active User
The admin user or user with administrator permission can perform the following operations to inactive or activate the non-admin users in a batch.

- Select one or multiple active users and click **Inactive** to inactivate the user(s)
- Select one or multiple inactive users and click **Active** to activate the user(s)

Refresh All
Click **Refresh All** to get the latest status of the users.

Filter User
Click ▽ to expand the filter conditions. Set the conditions and click **Filter** to filter the users according to the set conditions.

Note

The administrator user named admin was pre-defined by default. It cannot be edited ,deleted, or forced to log out.

20.3 Import Domain Users

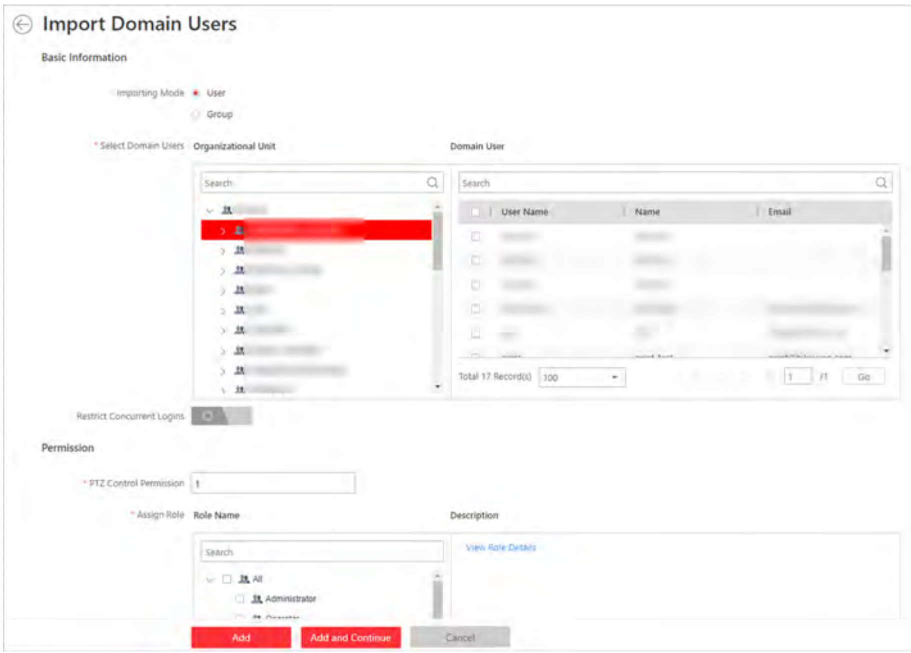
You can import the users in the AD domain in a batch to the system (including user name, real name, and email) and assign roles to the domain users.

Before You Start

You should configure the active directory settings. See ***Set Active Directory*** for details.

Steps

1. Click **Security → Users** to enter the User Management page.
2. Click **Import Domain Users** to enter the Import Domain Users page.



Import Domain Users

Basic Information

Importing Mode ● User ○ Group

*Select Domain Users: Organizational Unit / Domain User

Total 17 Record(s) 100 · 1 /1 Go

Restrict Concurrent Logins

Permission

*PTZ Control Permission: 1

*Assign Role: Role Name / Description

Figure 20-6 Import Domain Users

3. Select the importing mode.

   User

   Import the specified users. Select the organization unit and select the user accounts under the organization unit which are displayed in the Domain User list on the right.

   Group

   Import all the users in the group.

4. **Optional:** Set **Restrict Concurrent Logins** switch to ON and enter the maximum number of concurrent logins.
5. Set the permission level (1-100) for PTZ control in PTZ Control Permission.

   Note

   The larger the value is, the higher permission level the user has. The user with higher permission level has the priority to control the PTZ unit.

   Example

   When user1 and user2 control the PTZ unit at the same time, the user who has the higher PTZ control permission level will take the control of the PTZ movement.

6. Check the existing roles to assign the role(s) for the selected domain user.

   Note

   - If no role has been added, two default roles are selectable: administrator and operator.
     Administrator

The role that has all permissions of the HikCentral Professional.

Operator

The role that has all permissions of the HikCentral Professional Control Client.

- If you want to add customized roles, you can click **Add New Role** to quickly enter the Add Role page. See ***Add Role*** for details.

7. Complete importing the domain user.
   - Click **Add** to add the user.
   - Click **Add and Continue** to save the settings and continue to add users.
8. **Optional:** After importing the user information in the domain to the system, if the user information in domain is changed, click **Synchronize Domain Users** to get the latest information of the users imported to the system. If the users are imported by group, it will synchronize the latest user information from the domain group (including added users, deleted users, edited users, etc., in the group).

Result

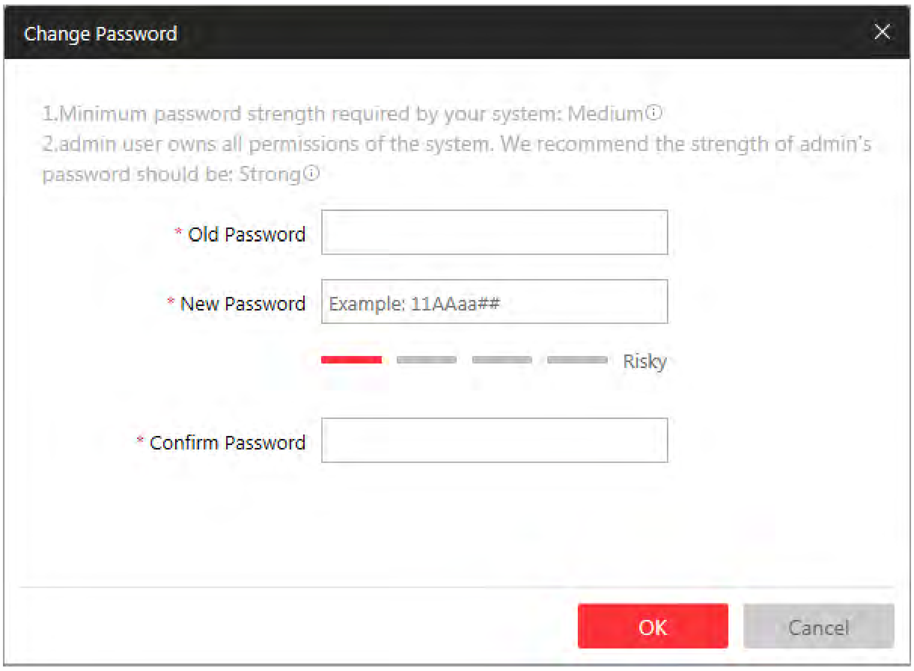
After successfully adding the domain users, the users can log in to the HikCentral Professional via the Web Client, Control Client and Mobile Client by their domain account and password.

20.4 Change Password of Current User

When you log in via Web Client, you can change your password as desired.

Steps

1. Move the cursor on the name of the current user at the top-right corner of the system.
2. From the drop-down list, select **Change Password** to open the Change Password dialog.



Change Password

1.Minimum password strength required by your system: Medium

2.admin user owns all permissions of the system. We recommend the strength of admin's password should be: Strong

* Old Password

* New Password: Example: 11AAaa##

Risky

* Confirm Password

Figure 20-7 Change Password Dialog

3. Enter the old password, new password, and confirm password.

Caution

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

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

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

20.5 Reset Password for Admin User

When you forgot the password of admin user, you can reset the password and set a new password for admin user.

Steps

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

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

A login page will pop up.

2. **Optional:** When you log in via current Internet Explorer browser for the first time, you should install the plug-in before you can access the functions.

Note

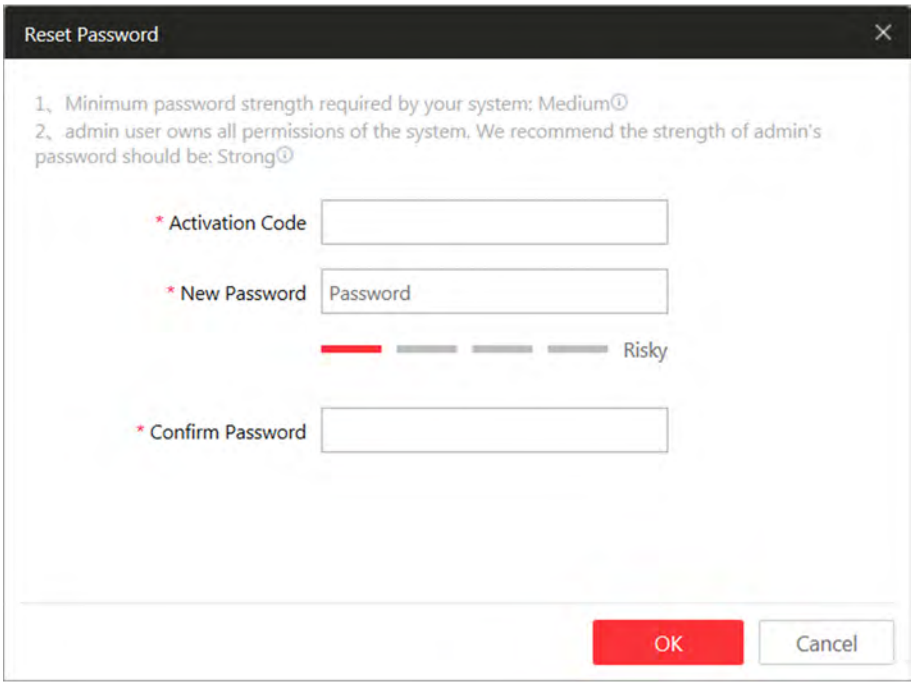
If a new version of plug-in is detected, you should update it to ensure the proper usage and better user experience.

1) Click **OK** in the pop-up dialog to install the plug-in. Or click **Download Plug-in** to download it.
2) Save the plug-in file to your PC and close the web browser.
3) Find the plug-in that stores on your PC and install the plug-in according to the prompt.
4) Re-open the web browser and log in to the SYS (step 1).

Note

Please allow the browser to run the plug-in in the pop-up prompt.

3. Input ***admin*** in the User Name field.
4. Click **Forgot Password** to open the Reset Password dialog.



Reset Password

1、Minimum password strength required by your system: Medium

2、admin user owns all permissions of the system. We recommend the strength of admin's password should be: Strong

* Activation Code

* New Password: Password

Risky

* Confirm Password

Figure 20-8 Reset Password

5. Enter the required parameters in the pop-up dialog, including activation code, new password, and confirm password.

Note

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

Caution

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

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

6. Click **OK** to reset the admin password.

Note

If you forgot the password of other users, contact the administrator user to reset the password and then change the password for login.

20.6 Reset Password for Normal User

If the user forgot the password, he/she can contact the users with administrator role to reset the password.

Steps

Note

The admin user can reset the passwords of all the other users. Other users with administrator role can reset the passwords of the users without administrator role. See ***Add Normal User*** for details about user's role settings.

1. Click **Security** to enter the Security Management page.
2. Click **Users** on the left.
3. Select one user and click the **Name** field to enter the user details page.
4. Click **Reset** to enter a new password of the user.

20.7 Configure Permission Schedule

The permission schedule defines when the role's permissions are valid. During the authorized time periods, the permissions will be valid. In unauthorized time periods, the user with the role will be forced to logout and he/she cannot login again. The system predefines three default permission schedule templates: All-day Template, Weekday Template, and Weekend Template. You can also add a customized template according to actual needs.

Steps

1. Click **System** on the home page.
2. Click **Schedule → Permission Schedule Template** tab on the left.
3. Click **Add** in the Permission Schedule page to enter the adding permission schedule template page.
4. Set the required information.

   Name

   Create a name for the template.

   Copy from

   Optionally, you can select to copy the settings from other defined templates.
5. Draw a time period on the time bar.

Note

Up to 8 time periods can be set for each day.

6. **Optional:** Click **Erase** and click on the drawn time period to clear the corresponding drawn time period.
7. **Optional:** Set the holiday schedule. The priority of holiday schedule is higher than the weekly schedule which means the predefined holidays will adopt the holiday schedule rather than the weekly schedule.
   1) Click **Add Holiday**.
   2) Select the predefined holiday(s), or click **Add New** to create a new holiday (see ***Set Holiday*** for details).
   3) Click **Add**.
   4) Draw a time period on the time bar.

      Note

      Up to 8 time periods can be set for each day.
   5) **Optional:** Click **Erase** and click on the drawn time period to clear the corresponding drawn time period.
8. Finish adding the permission schedule template.
   - Click **Add** to add the template and back to the permission schedule template list page.
   - Click **Add and Continue** to add the template and continue to add other template.

   The permission schedule template will be displayed on the permission schedule template list.
9. **Optional:** Perform the following operations after adding the template.

View Template Details	Click the template to view its details.
Edit Template	Click ✎ in the Operation column to edit template details.
Delete Template	Click × in the Operation column to delete the template.
Delete All Templates	Click **Delete All** to delete all the schedule templates (except the default templates and the template(s) in use).

Chapter 21 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.

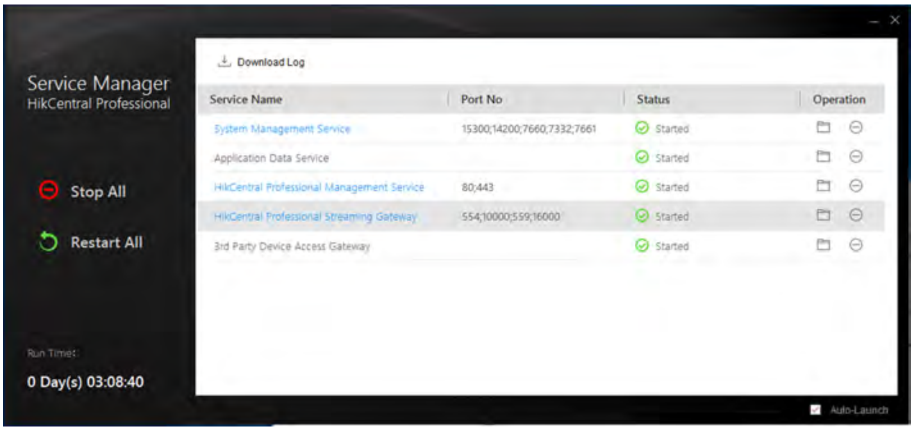
You can also export the system's configuration data and save it to the local PC.

21.1 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	

Figure 21-1 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.

21.2 Set System Data Backup

For purpose of restoring the original system data after a data loss event or recovering data from an earlier time, you can manually back up the data in the system, or configure a schedule to run the backup task regularly. The system data includes data configured in the system, pictures configured in the system, received events and alarms, face comparison data, card swiping data, maintenance data, etc.

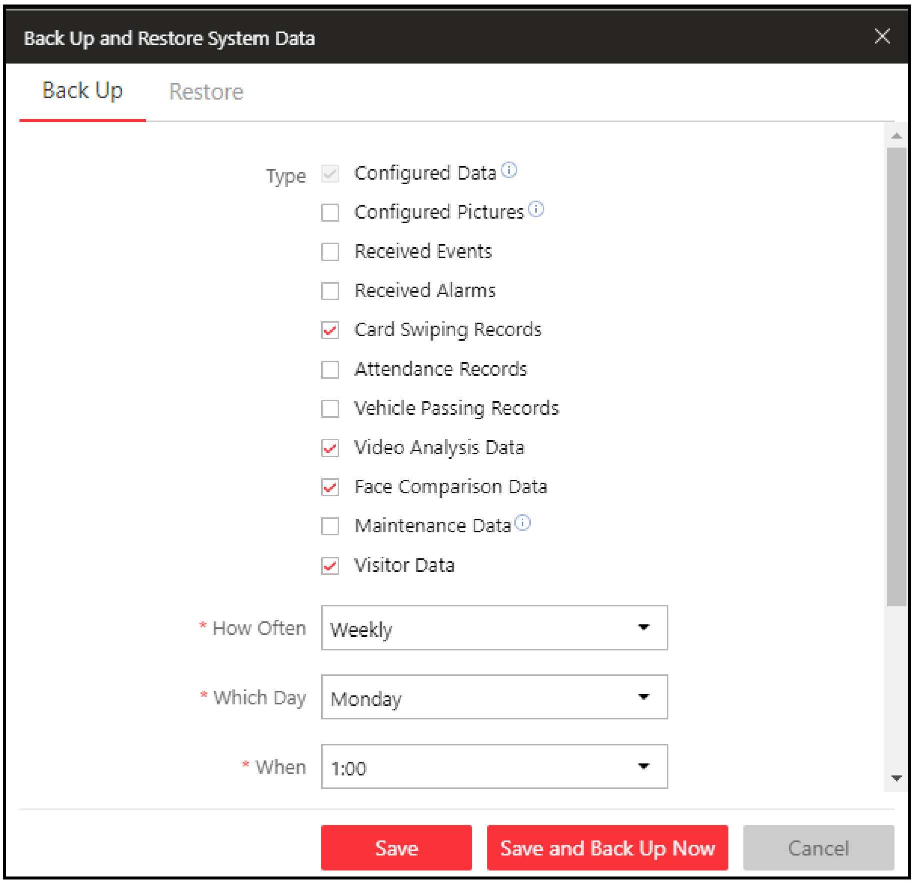
Perform this task when you need to configure the schedule to run the system data backup task regularly or manually back up the data.

Steps

Note

The backups are stored in the SYS server. If you want to edit the default saving path, you should enter Back Up and Restore System Data page via the Web Client running on the SYS server.

1. Click **Back Up and Restore System Data** on the home page.
2. Click **Back Up**.



Back Up and Restore System Data

Type ☑ Configured Data
□ Configured Pictures
□ Received Events
□ Received Alarms
☑ Card Swiping Records
□ Attendance Records
□ Vehicle Passing Records
☑ Video Analysis Data
☑ Face Comparison Data
□ Maintenance Data
☑ Visitor Data

* How Often: Weekly

* Which Day: Monday

* When: 1:00

Figure 21-2 Set System Data Backup

3. Select the system data type for backup.

Configured Data

The data configured via the Web Client, including physical resources, logical resources, user permissions, etc. It is selected by default.

Configured Pictures

The pictures uploaded when setting maps, persons, vehicles, etc.

Maintenance Data

The maintenance data includes service's logs, cameras' online/offline status, recording status, encoding devices' online/offline status, etc.

4. Set the backup schedule to run backup regularly.

1) Select the frequency to back up the system data.

Note

- If you select the data type besides configured data, you cannot set the frequency as **Daily**.
- If you select **Weekly** or **Monthly** for running the backup task, select which day to run.

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

3) Set the **Max. Number of Backups** to define the maximum number of backup files available on the system.

Note

The value ranges from 1 to 5.

5. **Optional:** Click **Save and Back Up Now** if you need to perform the backup immediately.
6. Click **Save**.

21.3 Restore Database

When an exception occurs, you can restore the database if you have backed up the database.

Before You Start

You should have backed up the database. Refer to ***Set System Data Backup*** for details.

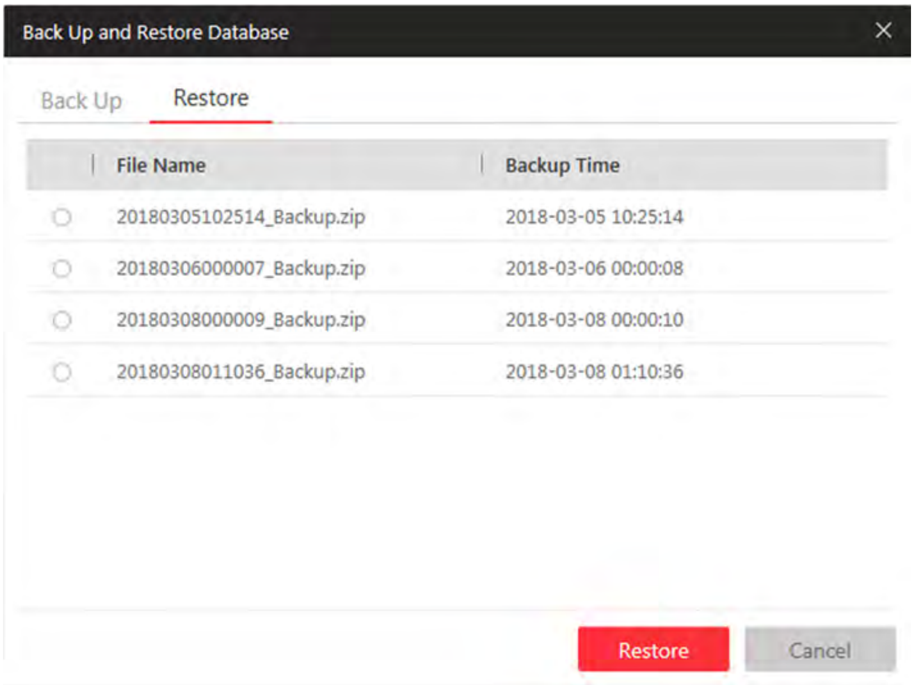
Perform this task when you need to restore the database.

Steps

Note

Database recovery will restore the database to an earlier state. Thus the data added after that state will be lost.

1. Click **Back Up and Restore Database** on the home page.
2. Click **Restore** in the pop-up dialog to enter the database restore page.
3. Select a backup file to restore the database to an earlier state.



	File Name	Backup Time
○	20180305102514_Backup.zip	2018-03-05 10:25:14
○	20180306000007_Backup.zip	2018-03-06 00:00:08
○	20180308000009_Backup.zip	2018-03-08 00:00:10
○	20180308011036_Backup.zip	2018-03-08 01:10:36

Figure 21-3 Database Restore

4. Click **Restore** to confirm the database recovery.

What to do next

After restoring the database, you must reboot the SYS service via Service Manager and log in again via Web Client.

21.4 Export Configuration File

You can export and save configuration data to the local PC, including Remote Site, recording settings and etc.

Perform this task when you need to export configuration data.

Steps

1. Click **Export Configuration Data** on the home page to open the Export Configuration Data dialog.
2. Select the configuration data type to export.
3. Click **Export** to save the data to your local PC.

Note

- You can set the saving path by following the prompt of the browser.
- The configuration data file is in CSV format.

Chapter 22 Manage System Security

System security is crucial for your system and property, you can set the password strength and lock IP address to prevent malicious attacks, and set other security policies to increase the security of the system.

Perform this task to set the minimum password strength, IP address locking, and other security policy settings to prevent malicious attacks.

Steps

1. Click **Security → Security Settings** to open the Security Settings page.
2. Set **Lock IP Address** switch to ON and the number of failed login attempts is limited.
   1) Select the allowable login attempts for accessing 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.
3. Select the **Minimum Password Strength** to define the minimum complexity requirements that the password should meet.
4. Set the maximum password age.
   1) Set **Enable Maximum Password Age** switch as ON to force user to change the password when password expires.
   2) Set the maximum number of days that the password is valid.

   Note

   After this number of days, you will have to change the password. You can select the pre-defined time length or customize the time length.
5. Configure the settings to automatically lock the Control Client after a time period of inactivity on the Control Client.
   1) Set **Auto Lock Control Client** switch to ON to lock the Control Client after a time period of inactivity on Control Client.
   2) Select time period for user inactivity. You can select the pre-defined time period or customize the time period.
6. Click **Save**.

Chapter 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 Site Name

You can set a name for the current system.

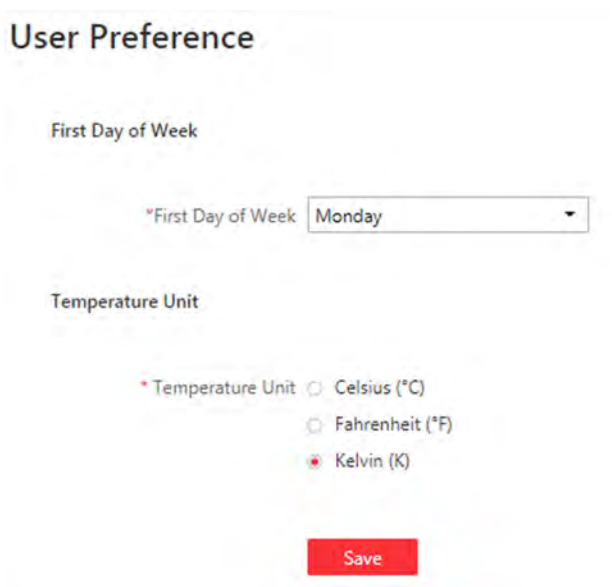
Steps

1. Click **System → Normal → Site Name** on home page.
2. Edit the site name for the current system.
3. Click **Save**.

23.2 Set User Preference

Due to the difference of nation, region, culture and enterprise background, the user preference might be different. You can set the user preference according to the actual scene, including the first day of week and the unit of temperature.

Click **System → Normal → User Preference** to enter the setting user preference page.



User Preference

First Day of Week

*First Day of Week: Monday

Temperature Unit

* Temperature Unit: ○ Celsius (°C) ○ Fahrenheit (°F) ● Kelvin (K)

Figure 23-1 User Preference

Set the following parameters:

First Day of Week

Set the first day of week according to the custom of the actual scene.

Note

The first day of week is used in the intelligent analysis report generation, live view and playback, attendance settings, etc.

Temperature Unit

Set the temperature unit according to the custom of the actual scene.

Note

The temperature unit is used in the temperature analysis report generation, etc.

23.3 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. Click **System → Normal → Server Usage Thresholds** on the home page.
2. Drag the △ to adjust the CPU and RAM threshold value.
3. Define the duration in the **Notify if Value Exceeds for (s)** field for CPU Usage and RAM Usage.

Example

- If you set warning threshold as 60%, and set 20 in the **Notify if Value Exceeds for (s)** field of CPU Usage, you can view the CPU status changes to Waring in Health Monitoring in Control Client when the CPU usage reaches the warning threshold and lasts for 20 seconds.
- If you set 60% as the warning threshold, and set 20 in the **Notify if Value Exceeds for (s)** field of CPU Usage, and set an alarm for CPU Warning (see), the alarm will be triggered when the CPU usage reaches the warning threshold and lasts for 20 seconds.

23.4 Set NTP

You can set the NTP server for syncing 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 system's.

1. Click **System → Network → NTP Settings** .
2. Set the **Time Synchronization** switch to ON to enable the NTP function.
3. Set the NTP server address and NTP port.
4. Enter the interval for the auto time synchronization.
5. **Optional:** Click **Test** to test the communication between the SYS and NTP server.
6. Click **Save**.

23.5 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

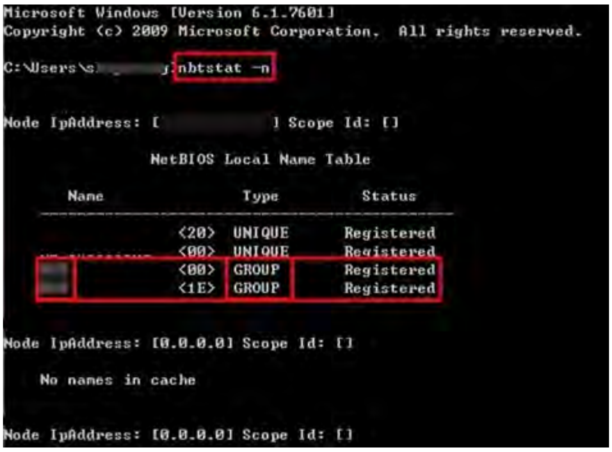
1. Click **System → Network → Active Directory** on the home page.
2. Configure the basic information parameters to connect to the AD domain controller.

   Domain Name

      The domain name of the AD domain controller.

Note

- 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.

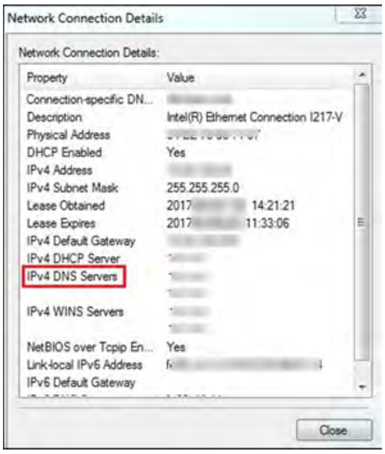


```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\s[redacted]>nbtstat -n

Node IpAddress: [[redacted]] Scope Id: []

                NetBIOS Local Name Table

       Name               Type         Status
    ---------------------------------------------
    [redacted]       <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]
IPv4 WINS Servers	[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 ***Custom Additional Information***) are displayed in the Person Information area by default. You can set the link relationship for those or add new person information items as you desired.
   2) **Optional:** Click **Add New** to add a person information item you concerned.

      Note

      - You needn't add the basic person information items, including ID, First Name, Last Name, Phone, and Remark) manually, which has the default link relationship with the domain.
      - The new person information item is also displayed on Custom Additional Information page, where you can edit or delete the items. Refer to ***Custom Additional Information*** for details.
      - The person information item is case-sensitive.
   3) **Optional:** Click + to show the person information items stored in the domain.
   4) Check the checkbox in the domain to link it to the added person information items when importing the domain persons.
   5) **Optional:** Hover over the linked person information in domain and click × to remove the relationship. You can also change the link relationship among each other by clicking and dragging the one item to anther.
4. Click **Save**.

   After the configuration, the organization unit and domain user information will be displayed when you click **Import Domain User** on User Management page.

   If the Link Person Information function is enabled, the corresponding person information in the system will match the linked person information in the domain and cannot be edited.

23.6 Enable Receiving Generic Event

After creating a generic event to analyze the received TCP and/or UDP data packages from a very wide range of external systems, you can enable the receiving generic event function so that the system can receive the configured generic events.

Steps

1. Click **System → Network → Receiving Generic Event** .
2. Check **Receiving Generic Event** to enable this function.
3. Click **Save**.

Note

You can configure the system's port No. for generic event: Open Service Manager (installed on the PC running SYS service), and click **HikCentral Professional System Management Service** to edit.

23.7 Allow for Remote Site Registration

This page allows the system with Remote Site Management module (as we called 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.

Before You Start

If a remote site needs to register to the Central System, it should open the Remote Site's Web Client and enter **Registering to Central System** to configure the Central System's parameters. See ***Register to Central System*** for details.

Steps

Note

Allowing for Remote Site registration is only available for the system with Remote Site Management module.

1. Click **System → Network → Receiving Site Registration** .
2. Check **Receiving Site Registration** to enable this function.
3. Click **Save**.

23.8 Register to Central System

This page allows the system without Remote Site Management module (as we called Remote Site) to register to the Central System. Central System is the system that has Remote Site Management module and can join multiple Remote Sites together 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.

Before You Start

For Central System, it should enable the receiving site registration function so that it can receive the Remote Site registration. See ***Allow for Remote Site Registration*** for details.

Steps

Note

Registering to Central System is only available for the system without Remote Site Management module.

1. Click **System → Network → Registering to Central System** .
2. Set the **Registering to Central System** switch to ON to enable this function.
3. Enter the IP address and port No. of Central System.

   Note

   Open Service Manager (installed on the PC running central system's SYS service), and click **HikCentral Professional System Management Service** if you need to view or edit the Central System's port.
4. Click **Save**.

23.9 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.

Click **System → Network → Device Access Protocol** to enter the Device Access Protocol page.

Check **Allow ISUP of Earlier Version**.

Click **Save**.

Note

The device may be attacked when accessing the system by ISUP of earlier versions.

23.10 Set WAN Access

In 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 server via WAN (Wide Area Network). For example, if the SYS server is in a local area network, and you need to visit the system via the Web Client or Control Client running in WAN, you should enable WAN access and set a static IP address or domain name and ports for HikCentral Professional.

Steps

1. Click **System → Network → WAN Access** .
2. Set the **WAN Access** switch to ON to enable the WAN access function.
3. Enter a static IP address or domain name of the server for WAN access.
4. Set the following ports, including HTTP, HTTPS, RTSP (Real Time Streaming Port), video file streaming port, and WebSocket port.

   Client Communication Port

   Used for Web Client and Control Client to access the system in HTTP protocol. By default, it is 80.

   Client SSL Communication Port

   Used for Web Client and Control Client to access the system 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 to receiving the TCP and/or UDP data packages.

   Note

   For setting the generic event, refer to ***Configure Generic Event*** .
6. **Optional:** For the system 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 in ISUP protocol, you can set the ports for these ISUP devices such as registration port, alarm receiving port, streaming port, etc.
8. Click **Save**.

23.11 Set Network Timeout

Network timeout duration refers to the default waiting time for the configurations on the Web Client. The configuration will be regarded as failure if no response within the configured timeout time.

The minimum default waiting time of the interactions between the configurations and 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.

23.12 Set Device Access Mode

Device Access Mode page allows you to define how the system accesses all the added encoding devices and decoding devices.

Perform this task to define how the system accesses all the added encoding devices and decoding devices.

Steps

1. Click **System → Network → Device Access Mode** .
2. Set the device access mode as automatically judge or proxy mode.

   Automatically Judge

   The system will automatically judge the condition of network connection and then set the device access mode accordingly as accessing directly or accessing via Streaming Gateway and Management Service.

   Proxy

   The system will access the device via Streaming Gateway and Management Service. It is less effective and less efficient than accessing directly.
3. Click **Save** to confirm the settings.

   System accesses all the added encoding devices and decoding devices via the selected mode.

23.13 Set Server NIC

You can select the NIC of the current SYS server so that the system can receive the alarm information of the device connected via ONVIF protocol.

Steps

1. Click **System → Network → Server NIC** .
2. Select the currently used NIC name of SYS in the drop-down list.

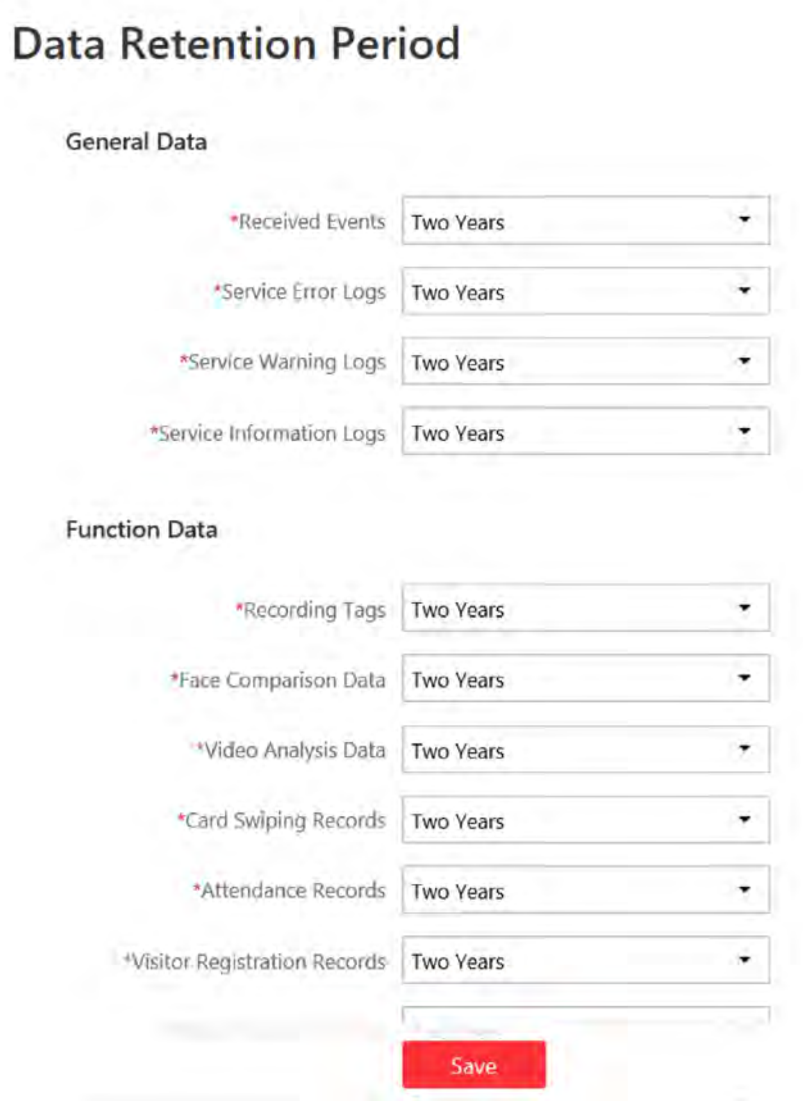
   The NIC information including description, MAC address, and IP address will display.
3. Click **Save**.

23.14 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. Click **System → 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

*Attendance Records: Two Years

*Visitor Registration Records: Two Years

Figure 23-4 Set Data Retention Period

Note

The card swiping records are saved as the configured period. The user with the permission can search the persons' swiping records and view related information during this period, even if the searched persons have been deleted from the SYS server.

3. Click **Save**.

23.15 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.
Click **System → Schedule → 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.
Click **System → Schedule → 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**.

23.16 Set Email Template

You should set the email template properly before sending the event message to the designate email account(s) as email linkage. The email template can also be used when sending report to the designate recipients.

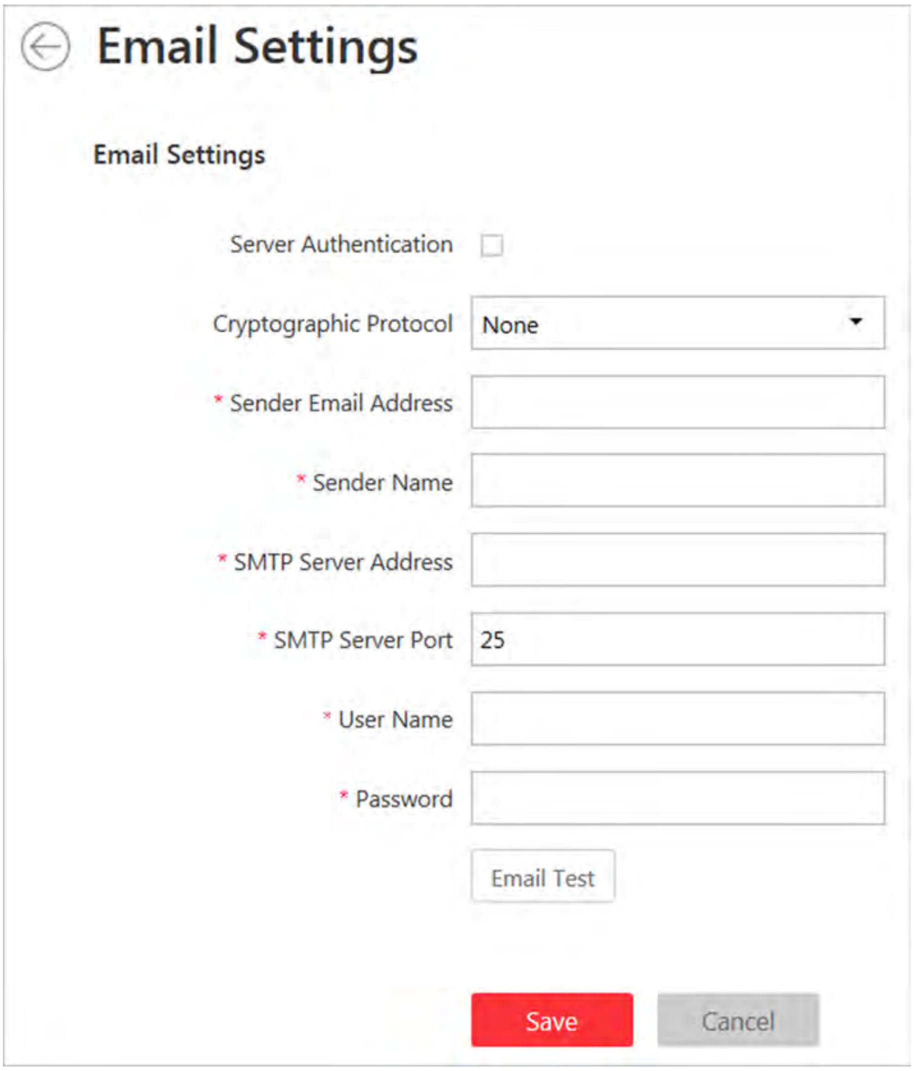
23.16.1 Configure Email Account

You should configure the parameters of sender's email account before the system can send the message to the designate email account(s) as email linkage.

Perform this task when you need to configure the sender's email account.

Steps

1. Click **System → Email** to enter the email page.
2. Click **Email Settings** to enter the Email Settings page.



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

3. Configure the parameters according to actual needs.

   Server Authentication (Optional)

   If your mail server requires authentication, check this checkbox to use authentication to log in to this server.

   Cryptographic Protocol

   Select the cryptographic protocol of the email to protect the email content if required by the SMTP server.

   SMTP Server Address

   The SMTP Server IP address or host name (e.g., smtp.263xmail.com).

   SMTP Server Port

   The default TCP/IP port used for SMTP is 25.

4. Click **Email Test**to test whether the email settings work or not.

The corresponding attention message box will pop up.

5. Click **Save**.

23.16.2 Add Email Template

You can set email templates including specifying the recipient, email subject, and content, so that the system can send the information to the designate recipient according to the pre-defined email template.

Before You Start

Before adding the email template, you should set the sender's email account first. See ***Configure Email Account*** for details.

Perform this task when you need to add a new email template.

Steps

1. Enter **System → Email** to enter the email page.
2. Click **Add** to enter the Add Email Template page.
3. Enter the required parameters.

   Name

   Create a name for the template.

   Recipients

   Click **Add User** and select the person's email as the recipient, which is configured when adding the person.

   Click **Add Email** and enter the recipient(s) email address to send the email to.

   Note

   You can enter multiple recipients and separate them by ";".

   Subject

   Enter the email subject as desired. You can also click the button in the lower part of the window to add the related information to the subject.

   Content

   Define the event information to be sent. You can also click the button in the lower part of the window to add the related information to the content.

   Note

   If you select to add the event time to the email subject or content, and the email application (such as Outlook) and the system are in different time zones, the displayed evnet time may have some deviations.

4. **Optional:** Check **Attach Image** to send email with image attachment.
5. Finish adding the email template.

- Click **Add** to add the template and go back to the email template list page.
- Click **Add and Continue** to add the template and continue to add other templates.

The email template will be displayed on the email template list.

6. Perform the following operation(s) after adding the email template:

Edit Template Click ✎ in the Operation column to edit template details.

Delete Template Click × in the Operation column to delete the template.

Delete All Templates Click **Delete All** to delete all the added templates.

23.17 Send Report Regularly

Reports are essential documents in order to submitting performance to users to make business run smoothly and effectively. Users can use reports as basis in creating decisions, addressing problems, checking tendency and comparison, etc. HikCentral Professional provides report functions that the system can send reports automatically and regularly to target users by emails, showing the occurred events and alarms, number of passing vehicles, people counting, queue management, and temperature status during specified time period, attendance report, etc.

23.17.1 Send Event Report Regularly

You can set a regular report rule for specified system-monitored events, and the system can send an email with a report attached to the target recipients daily or weekly, showing the details of specified system-monitored events triggered in the day or the week.

Before You Start

- Set the email template with recipient information, subject, and content. For details, refer to ***Set Email Template*** .
- Set the email settings such as sender address, SMTP server address and port, etc. For details, refer to ***Configure Email Account*** .

Steps

Note

One report can contain up to 10,000 event records in total.

1. Click **System** on the home page and enter **Report** page.
2. Select the report category as **Event**.
3. Create a name for the report.
4. Set the system-monitored event(s) contained in the report.
   1) In the Report Target field, click **Add**.

      All the added system-monitored events are displayed.
   2) (Optional) Filter the events by event source type and triggering event.
   3) Select the event(s).

Note

Up to 32 events can be added in one report rule.

4) Click **Add**.

5. Set the report type as **Daily** or **Weekly** and set the sending time.

   Daily Report

   Daily report shows data on a daily basis. The system will send one report at the sending time every day, which contains information of the events triggered on the day (24 hours) before the current day.

   For example, if you set the sending time as 20:00, the system will send a report at 20:00. every day, containing details of all the events triggered between 00:00. and 24:00. before the current day.

   Weekly Report

   As compared to daily report, weekly report can be less time-consuming, since it is not to be submitted every day. The system will send one report at the sending time every week, which contains information of the events triggered on the last 7 days before the sending date.

   For example, if you set the sending time as 6:00 on Monday, the system will send a report at 6:00 in the morning on every Monday, containing details of all the events triggered between last Monday and Sunday.

6. Select the email template from the drop-down list to define the recipient information and email format.

   Note

   You can click **Add New** to add a new email template. For setting the email template, refer to ***Set Email Template*** .

7. Select Excel or PDF as the report format.
8. Finish adding the report.
   - Click **Add** to add the report and go back to the report list page.
   - Click **Add and Continue** to add the report and continue adding other reports.

23.17.2 Send Alarm Report Regularly

You can set a regular report rule for specified alarms, and the system can send an email with a report attached to the target recipients daily or weekly, showing the details of specified alarms triggered in the day or the week.

Before You Start

- Set the email template with recipient information, subject, and content. For details, refer to ***Set Email Template*** .
- Set the email settings such as sender address, SMTP server address and port, etc. For details, refer to ***Configure Email Account*** .

Steps

Note

One report can contain up to 10,000 alarm records in total.

1. Click **System** on the home page and enter **Report** page.
2. Select the report category as **Alarm**.
3. Create a name for the report.
4. Set the alarm(s) contained in the report.
   1) In the Report Target field, click **Add**.

      All the added alarms are displayed.
   2) (Optional) Filter the alarms by alarm source type, triggering event, and alarm priority.
   3) Select the alarm(s).

      Note

      Up to 32 alarms can be added in one report rule.
   4) Click **Add**.
5. Set the report type as **Daily** or **Weekly** and set the sending time.

   Daily Report

   Daily report shows data on a daily basis. The system will send one report at the sending time every day, which contains information of the alarms triggered on the day (24 hours) before the current day.

   For example, if you set the sending time as 20:00, the system will send a report at 20:00 every day, containing details of all the alarms triggered between 00:00 and 24:00 before the current day.

   Weekly Report

   As compared to daily report, weekly report can be less time-consuming, since it is not to be submitted every day. The system will send one report at the sending time every week, which contains information of the alarms triggered on the last 7 days before the sending date.

   For example, if you set the sending time as 6:00 on Monday, the system will send a report at 6:00 in the morning on every Monday, containing details of all the alarms triggered between last Monday and Sunday.
6. Select the email template from the drop-down list to define the recipient information and email format.

   Note

   You can click **Add New** to add a new email template. For setting the email template, refer to ***Set Email Template*** .
7. Select Excel or PDF as the report format.
8. Finish adding the report.
   - Click **Add** to add the report and go back to the report list page.

- Click **Add and Continue** to add the report and continue adding other reports.

23.17.3 Send Attendance Report Regularly

You can set a regular report rule for specified attendance groups, and the system can send an email with a report attached to the target recipients daily, weekly, or monthly, showing the attendance records of the persons during the specified time periods in these attendance groups.

Before You Start

- Set the email template with recipient information, subject, and content. For details, refer to ***Set Email Template*** .
- Set the email settings such as sender address, SMTP server address and port, etc. For details, refer to ***Configure Email Account*** .

Steps

Note

- One report can contain up to 10,000 records in total.
- The report will be an Excel file.

1. Click **System → Report** to enter the report setting page.
2. Select the report category as **Attendance**.
3. Create a name for the report.
4. Click **Add** to select the attendance group for this report.

   The attendance records of the persons in the selected attendance group will be calculated in this report.
5. Select a report type.
6. Set the report time 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 persons' attendance records 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 persons' attendance records 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 persons' attendance records detected between last Monday and Sunday.

Note

The system will calculate the attendance records of the previous day at 4 a.m. every day. For accuracy of the report time, you cannot set to send the report between 0 a.m. to 4:59 a.m.

7. Select the email template from the drop-down list to define the recipient information and email format.

   Note

   You can click **Add New** to add a new email template. For setting the email template, refer to ***Set Email Template*** .

8. Finish adding the report.
   - Click **Add** to add the report and go back to the report list page.
   - Click **Add and Continue** to add the report and continue adding other reports.

23.17.4 Send Device Log Report Regularly

You can set a regular report rule for specified encoding devices, and the system can send an email with a report attached to the target recipients daily, weekly, or monthly, showing the device logs of the devices during the specified time periods.

Before You Start

- Set the email template with recipient information, subject, and content. For details, refer to ***Set Email Template*** .
- Set the email settings such as sender address, SMTP server address and port, etc. For details, refer to ***Configure Email Account*** .

Steps

Note

- One report can contain up to 10,000 records in total.
- The report will be an Excel file.

1. Click **System → Report** to enter the report setting page.
2. Select the report category as **Device Logs**.
3. Create a name for the report.
4. Select the Report Target as **All Encoding Devices** or **Specified Device**.
5. **Optional:** Select **Encoding Device Online/Offline Status** as Report Content.
6. 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 recorded 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 encoding devices' logs recorded 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 encoding devices' logs recorded 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 encoding devices' logs recorded between last Monday and Sunday.

7. Select the email template from the drop-down list to define the recipient information and email format.

Note

You can click **Add New** to add a new email template. For setting the email template, refer to ***Set Email Template*** .

8. Finish adding the report.
   - Click **Add** to add the report and go back to the report list page.
   - Click **Add and Continue** to add the report and continue adding other reports.

23.17.5 Send Resource Log Report Regularly

You can set a regular report rule for specified camera resources, and the system can send an email with a report attached to the target recipients daily, weekly, or monthly, showing the logs of the resources during the specified time periods.

Before You Start

- Set the email template with recipient information, subject, and content. For details, refer to ***Set Email Template*** .
- Set the email settings such as sender address, SMTP server address and port, etc. For details, refer to ***Configure Email Account*** .

Steps

Note

- One report can contain up to 10,000 records in total.
- The report will be an Excel file.

1. Click **System → Report** to enter the report setting page.
2. Select the report category as **Resource Logs**.
3. Create a name for the report.
4. Select the Report Target as **All Cameras** or **Specified Cameras**.

5. **Optional:** Select **Camera Online/Offline Status** and **Recording Status** as Report Content.
6. 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 recorded 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 cameras' logs recorded 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 cameras' logs recorded 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 cameras' logs recorded between last Monday and Sunday.
7. Select the email template from the drop-down list to define the recipient information and email format.

   Note

   You can click **Add New** to add a new email template. For setting the email template, refer to ***Set Email Template*** .
8. Finish adding the report.
   - Click **Add** to add the report and go back to the report list page.
   - Click **Add and Continue** to add the report and continue adding other reports.

23.18 Enable Evidence Collection

Only when evidence collection is enabled, can the operators save specific video footage as evidence and search the saved evidence on the Control Client. Evidence collection can help to settle issues such as traffic disputes and criminal cases.

Before You Start

You should have configured a SFTP (Secure File Transfer Protocol) server.

Steps

Note

Operator is the role that has all the permission for operating the Control Client and the permission for operating the Applications (Live View, Playback, and Local Configuration) on the Web Client. For details about configuring users and roles, see ***Manage Role and User*** .

1. Click **System → Evidence Collection** to enter the Evidence Collection page.
2. Set the **Evidence Collection** switch to ON.

   The required information for enabling evidence collection will be displayed.
3. Set the required SFTP parameters.

   SFTP Address

   Enter the IP address of the SFTP server.

   Port

   Enter the port number of the SFTP server.

   User Name

   Enter the user name of the SFTP server.

   Password

   Enter the password of the SFTP server.
4. Set other required parameters for the evidence.

   Evidence Type

   Define the evidence types that the operators can select when they edit evidence information on the Control Client.

   Organization on Site

   Define the type(s) of organization on site that the operators can select when they edit the evidence information on the Control Client.

   Organization on site refers to the organization or personnel (e.g., police, fire department) on the site of the accident or criminal incident.

   Result/Conclusion

   Define the evidence-related incidents' results or conclusions that the operators can select when they edit evidence information on the Control Client.
5. Click **Save** to enable evidence collection.

23.19 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. For system with distributed deployment License, you can also enable encrypted transmission to encrypt the data transmission between Application Data Server and System Management Server, thus enhancing the system security.

Steps

Note

Setting transfer protocol is only available when accessing the Web Client on the SYS server locally.

1. Click **System → 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. **Optional:** Check **Encrypted Transmission** to encrypt the data transmission between Application Data Server and System Management Server.

Note

This field will show when the system's License support server distributed deployment.

5. 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.

23.20 Set Camera ID

When displaying live view on smart wall, you may use a keyboard for convenience operations such as starting live view on smart wall, PTZ control, etc. If you want to display certain camera's live view on smart wall, you should press the camera's identifier number on the keyboard, which is called **Camera ID**. As a result, HikCentral Professional provides this module for you to set a unique ID for each camera.

Click **System → Advanced → Camera ID** to enter the camera ID settings page.

You can filter the cameras by setting the site and area, or entering keywords of camera name or camera ID.

The system provides a default ID for each camera. You can edit the default value for the cameras if needed.

Note

The camera ID should be unique in the system.

23.21 Export Service Component Certificate

For data security, before adding the Streaming Server, Application Data 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 or the Application Data 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 or the Application Data 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. Click **System → Security → Service Component Certificate** .
2. Click **Generate** beside **Certificate between Services in System** to generate the security certificate for Streaming Server verification and Application Server verification.

   Note

   On the Service Manager of the Streaming Server or the Application Data Server you want to add, input the certificate information you generate. For the following operations, see ***Manage Application Data Server*** and ***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*** .

23.22 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.

Click **System → Security → Database Password** .

Enter the password and then click **Verify** to generate the verification code and enter the verification code.

23.23 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 on the Control Client, 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.

Enter **System → Advanced → 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, elevator 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

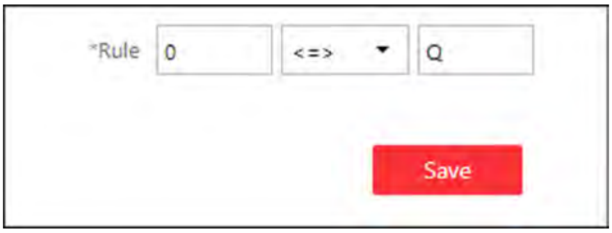
- **Device Capabilities:** Set how often the system gets the managed devices' capabilities. After disabled, the system will not update the capability changes of all the managed devices. You need to refresh manually to get the latest status.
- **Recording:** Set how often the system checks the camera's 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.

23.24 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. Enter **System → Advanced → Plate Fuzzy Search** .
2. Click **Add**.



*Rule 0 <=> Q

Figure 23-6 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.

23.25 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. Click **System → 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**.

23.26 Set Third-Party Integration

HikCentral Professional supports integrating third-party resources (such as camera, door, etc.) via Optimus. Also, the system provides open platform to integrate the third-party system. By the Open APIs (application programming interface) provided on the open platform, the third-party system can obtain some functions (such live view, playback, alarm, etc.) of HikCentral Professional, to develop more customized features.

Click **System → Advanced → Third-Party Integration** .

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.

Open Platform

Note

Setting open platform is only available when you access the Web Client on the SYS server locally.

Turn **Open API** to ON, set the IP address of the open platform, management port of the open platform and select the partner user.

Note

- The open platform should be deployed in the same network with the SYS server.
- The third-party system integrates the HikCentral Professional by the partner user(s) you select, which defines the permission(s) of resources and operations in the HikCentral Professional.

Click **Test** to test the service availability of the open platform.
Click **Save** to save the settings.

23.27 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.

23.27.1 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. Click **System → Advanced → Data Interchange** to enter the Data Interchange page.
2. Set **Data Synchronization** switch to on to enable synchronization 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 attendance data will be written to the third-party database.

23.27.2 Dump Card Swiping Records to Third-Party Database

The card swiping records of specified resources can be dumped as a CSV file and the third-party system will read the CSV file (instead of accessing database and mapping the table fields) for further applications, such as attendance calculation and pay calculation.

Before You Start

- You need to log into the Web Client running on SYS server.
- The third-party system should be installed in the same server with HikCentral Professional to read the CSV file directly in the local disk.

Steps

1. Click **System → Advanced → Data Interchange** to enter the Data Interchange page.
2. Set **Data Synchronization** switch to on to enable synchronization 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 which the card swiping records are dumped as.

Saving Path

The path where the CSV file is saved.

Content

The display items and data in the dumped CSV file.

Dump Every

The frequency for dumping card swiping records.

6. Click **Save**.

23.28 Reset Device Network Information

When system network domain changes (such as server migration), you must reset the network information of the added device to adapt to the new network environment. Otherwise the device live view, playback and other functions will be affected.

Perform this task when you need to reset the network information of the added device.

Steps

1. Click **System → Advanced → Reset Network Information** .
2. Click **Reset** to one-touch reset the device network information.

23.29 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.

Click **System → Advanced → SUP Upgrade Prompt** .

Turn **Upgrade Prompt** to ON, and 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.

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).

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).

Click **Save** to save the settings.

Chapter 24 Monitoring

The HikCentral Professional provides functionalities of live view, playback, and local configuration through web browser.

Note

- If the SYS's transfer protocol is HTTPS, the Monitoring 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.

24.1 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.

24.1.1 Start Live View

After adding the cameras into areas, you can start live view to view the camera's live video, and perform some basic operations via the Web Client.

Before You Start

An area with cameras assigned to is required to be defined for live view.

Steps

1. Click **Monitoring → Live View** on home page to enter the Live View page.
2. Select a site from the drop-down list.

   The area and cameras of the selected site is displayed.
3. **Optional:** Enter a keyword of camera name or area name in the search field and click **Search in All Sites** or **Search in Current Site** to search the cameras or areas.

   All the search results display.

   Note

   You can move the cursor to the camera name to view the image thumbnail.

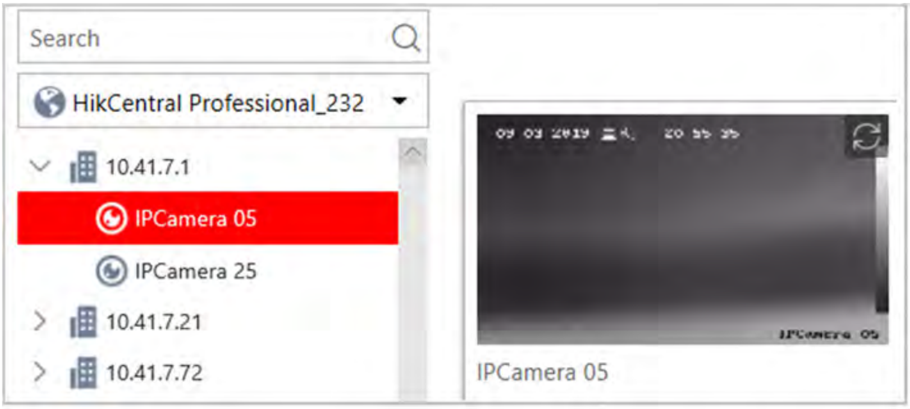


Figure 24-1 Thumbnail

4. **Optional:** Click ⊞ on the live view toolbar, and select a window division mode.

Note

Up to16-window mode is available when you access the Web Client via the Google Chrome, Firefox, Internet Explorer, or Safari.

5. Drag a camera/area to the display window, or double-click a camera/area name after selecting the display window to start the live view. The selected window is outlined in red.

Note

- If the system is Central System with Remote Site Management module, you can also view the live video of the cameras imported from remote site. For managing remote site's cameras in areas, refer to ***Add Camera to Area for Remote Site*** .
- You can also double-click the area name to start the live view of cameras in the area. The display windows adapt to the number of cameras in the area.

6. **Optional:** Move the cursor over the display window during live view, and you can perform some operations, such as digital zoom, instant playback, two-way audio, fisheye dewarping, and PTZ control, etc.

24.1.2 PTZ Control

Cameras with the pan/tilt/zoom functionality can be controlled through the web browser. You can also set the preset, patrol, and pattern for the cameras.

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 image position which contains configuration parameters for pan, tilt, zoom, focus and other parameters. You can also set a virtual preset after enabling digital zoom.

Steps

1. Click **Monitoring → Live View** on the home page to enter the live view page.
2. Start live view of camera.

Note

See ***Start Live View*** for details about how to start live view.

3. Click on the live view toolbar to open the PTZ control panel.
4. Click to enter the PTZ preset configuration panel.

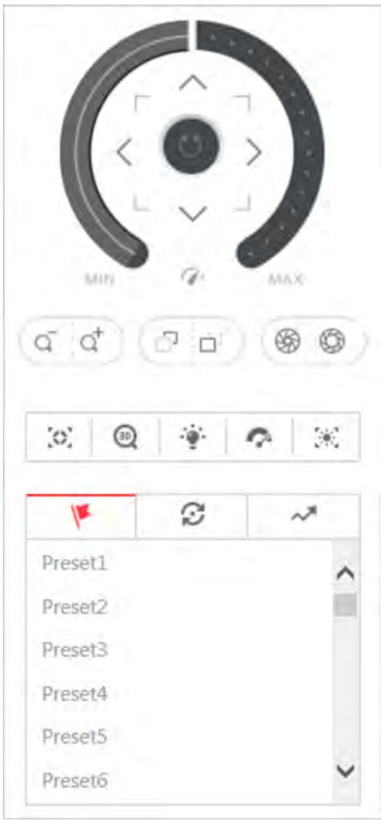


Figure 24-2 Configure Preset

5. Click the direction buttons to move the camera to the desired view or zoom in/out the view.

Note

You can also scroll the mouse wheel to zoom in or zoom out the view.

6. Select a PTZ preset number from the preset list and click .
7. Create a name for the preset.

8. Click **OK** to save the settings.

Note

- Up to 256 presets can be added.
- The unconfigured preset is gray.
  The configured preset is highlighted.

9. **Optional:** After setting the preset, you can do one or more of the followings:

   Call Preset Double-click the configured preset in the list, or select the preset and click ▶ to call the preset.

   Edit Preset Select the configured preset from the list and click ✎ to edit it.

   Delete Preset Select the configured preset from the list and click × to delete it.

Configure Patrol

A patrol is a scanning track specified by a group of user-defined presets (including virtual presets), with the scanning speed between two presets and the dwell time of the preset separately programmable.

Before You Start

Two or more presets for one PTZ camera need to be added.

Note

See ***Configure Preset*** for details.

Steps

1. Click **Monitoring → Live View** on the home page.
2. Start live view of camera.

   Note

   See ***Start Live View*** for details about how to start live view.

3. Click ⛭ on the live view toolbar to open the PTZ control panel.
4. Click ⟳ to enter the patrol configuration panel.

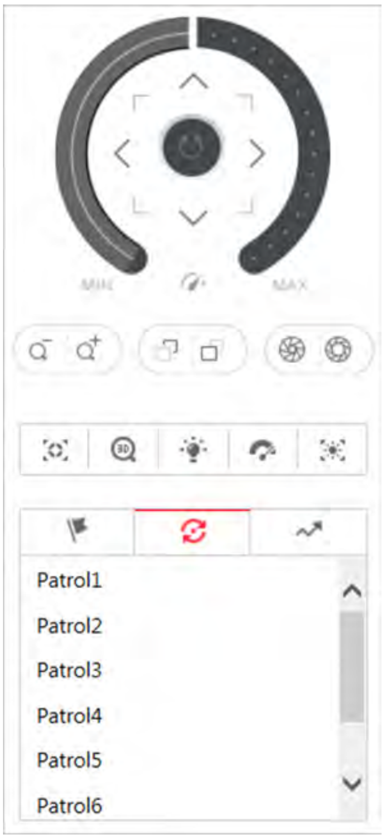


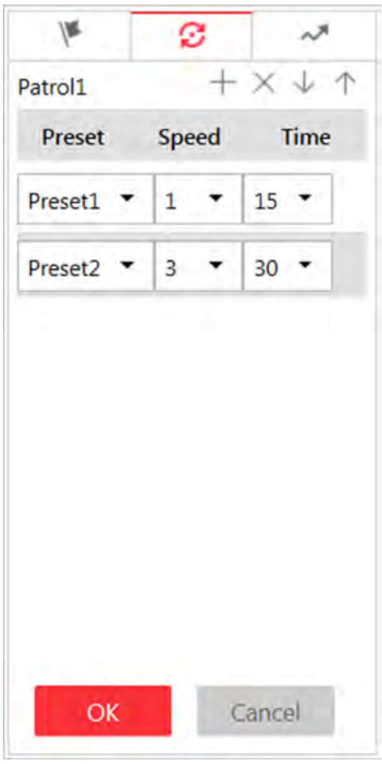
Figure 24-3 Configure Patrol

5. Select a patrol and click ✎ .
6. Click + to add a configured preset, and set the dwell time and the patrol speed.

Note

- The preset dwell time ranges from 15 to 30s.
- The patrol speed ranges from 1 to 40.
- The unconfigured patrol is gray.
  The configured patrol is highlighted.

7. Repeat the above step to add other presets to the patrol.



Preset	Speed	Time
Preset1	1	15
Preset2	3	30

Figure 24-4 Add Preset to Patrol

8. **Optional:** Perform the following operations after adding the preset.

Remove Preset from Patrol	Select the added preset and click ✕ to remove the preset from the patrol.
Adjust Preset Sequence	Select the added preset and click ↑ ↓ to adjust the preset sequence.

9. Click **OK** to save the patrol settings.

Note

Up to eight patrols can be configured.

10. **Optional:** Perform the following operations after setting the patrol.

Call Patrol	Click ▶ to start the patrol.
Stop Calling Patrol	Click ■ to stop the patrol.

Configure Pattern

You can set patterns to record the movement of the PTZ.

Steps

1. Click **Monitoring → Live View** on the home page to enter the Live View page.

2. Start live view of the camera.

Note

See ***Start Live View*** for details about how to start live view.

3. Click on the live view toolbar to open the PTZ control panel.
4. Click ↗ to enter the PTZ pattern configuration panel.

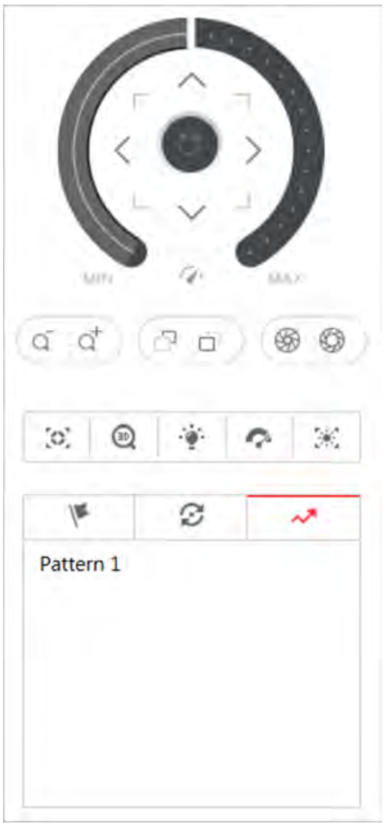


Figure 24-5 Configure Pattern

5. Click ▶ to start recording movement pattern path.
6. Click the direction buttons and other buttons to control the PTZ movement.
7. Click ■ to stop and save the pattern recording.

Note

Only one pattern can be configured each time, and the newly-defined pattern will overwrite the previous pattern.

8. **Optional:** Perform the following operations after setting the pattern.

Call Pattern	Click ▶ to call the pattern.
Stop Calling Pattern	Click ⊙ to stop calling the pattern.
Delete Pattern	Click × to delete the pattern.

24.2 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.

24.2.1 Search Video File

You can search the video footage of cameras and filter the searched video footage by video type or by storage location.

Steps

1. Click **Monitoring → Playback** on home page to open the Playback page.
2. **Optional:** Enter a keyword of camera name or area name in the search field and click **Search in All Sites** or **Search in Current Site** to search the cameras or areas.

   All the search results display.

   Note

   You can move the cursor to the camera name to view the image thumbnail.

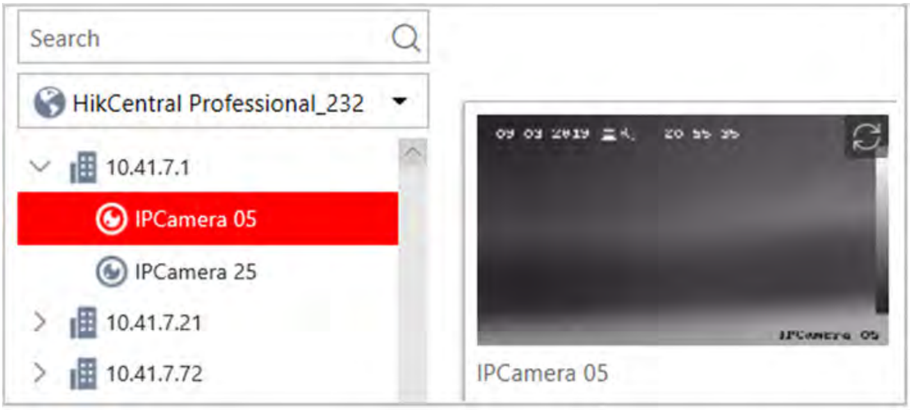
   

   Figure 24-6 Thumbnail

3. Drag the camera to the display window, or double-click the camera to start the playback.

   Note

   If the system is central system with Remote Site Management module, you can also play back the recorded video of the cameras imported from remote site. For managing remote site's cameras in areas, refer to ***Manage Area*** .

4. **Optional:** Click the date and time on the toolbar to select the date and time to search the video files.

Note

- In the calendar panel, the date with video files will be marked with a triangle.
- The calendar is not supported by cameras on remote site.

5. **Optional:** Click ▽ on the playback toolbar to select the video file type for playback.
6. **Optional:** Select the storage location and the stream type of the video files for playback.

For camera configured with auxiliary storage: Select the storage location of the video files for playback.

For camera configured with dual-stream recording: Select the stream type of the video files for playback.

Note

For setting the storage location of recording, refer to ***Configure Recording*** .

24.2.2 Play Video File

After searching the video footage, the playback starts. You can control the video playback via timeline. The timeline indicates the time duration for the video footage.

Steps

1. Click **Monitoring → Playback** on home page to open the Playback page.
2. Search the video file of cameras for playback. For details, refer to ***Search Video File*** .

   The playback starts.
3. Click the icons on the toolbar to control the playback.
4. Click on the timeline or drag the timeline to play back the video of the specific time.
5. **Optional:** Click ⊞ or ⊟ or use the mouse wheel to scale up or scale down the timeline bar.
6. **Optional:** Move the cursor to the display window in playback to access further functions, including capture, clipping, and other functions.

Open Digital Zoom Click 🔍 to enable the digital zoom function and draw a rectangle on the video. Click again to disable the function.

Note

When in software decoding mode, you can also capture the zoomed in picture after enabling digital zoom function.

Camera Status Click to show the camera's recording status, signal status, connection number, etc.

Stream Switch Click , , or (if supported) to switch the live view stream to main stream, sub-stream, or smooth stream (if supported).

Note

The smooth stream will show if the device supports smoothing function. You can switch to smooth stream if in low bandwidth situation to make live view more fluent.

Audio Control

Click 🔊 or 🔇 to turn off/on the sound.

Note

You can adjust the volume when moving the cursor on 🔊 .

24.3 Local Configuration

HikCentral Professional provides live view and playback functions via the Web Client. You can set the related network transmission parameters (such as hardware decoding, stream type, etc.) for the performance of live view and playback via the current Web Client. You can also view the saving path of video files and captured pictures on your current PC.

Steps

Note

The parameters in Local Configuration only affect the current Web Client.

1. Click **Monitoring → Local Configuration** on home page to enter the Local Configuration page.
2. Click **Network Transmission** tab on the left.
3. Set the following parameters as desired.

GPU Hardware Decoding

Enable the GPU decoding for live view and playback to save CPU resources.

Note

- Your PC must support GPU hardware decoding.
- After enabling GPU hardware decoding, restart live view and playback to take effect.
- If the client shows a blurred screen after enabling GPU hardware decoding, disable it.

Global Stream

The default stream type for global usage in the current Web Client.

If the device doesn't support smooth stream, it will use sub-stream. If the device doesn't support sub-stream, it will use main stream.

If the network is in good condition, select main stream or sub-stream. If the network is in poor condition, select smooth stream.

Threshold for Main/Sub-Stream

If a window's proportion of the displaying area is larger than the configured threshold, the stream type will be main stream. If the proportion is smaller than the threshold, it will be switched to sub-stream.

For example, if you set the threshold as ¼, when the window division turns to 5-window, the camera's stream type will be switched from main-stream to sub-stream.

Note

This parameter is only available when the **Global Stream** is set as **Main Stream**.

Network Timeout

The default waiting time for the operations in Applications on the current Web Client. The operations will be regarded as failure if no response within the configured time.

The minimum default waiting time of the interactions between the Applications and SYS server is 60s, the minimum time between SYS server and devices is 5s, and the minimum time between the Applications and devices is 5s.

Video Caching

Video caching should be determined based on network performance, computer performance, and bit rate. You can set is as **Small (1 Frame)**, **Medium (6 Frames)**, or **Large (15 Frame)**. Larger frame caching will result in better video performance.

Picture Format

Set the file format for the captured pictures during live view or playback. Currently it supports **BMP** and **JPEG** formats.

Device Access Mode

Restore Default

Restore the device access mode as configured in the **System → Device Access Mode** on Web Client.

Automatically Judge

Judge the device access mode according to the current network.

Directly Access

Access the device directly, not via HikCentral Professional Streaming Service.

Proxy

Access the device via HikCentral Professional Streaming Gateway and HikCentral Professional Management Service.

Note

By default, the system will judge the device access mode according to the current network. If you change to other mode, it only affects the client you logged in currently.

4. **Optional:** Click **Default Value** to restore the defaults of the settings.
5. Click **Save**.

6. **Optional:** Click **Saving Path** on the left to view the saving path of the recorded or clipped video files and captured pictures during live view or playback in your local PC.

Chapter 25 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.

25.1 Customize Report Dashboard

The report dashboard provides an at-a-glance view for the reports supported by the system, such as people counting report, vehicle analysis report, and queue analysis report. You can customize the report dashboard as required.

Steps

1. Click **Intelligent Analysis** to enter the report dashboard page.
2. **Optional:** Add dashboard(s).
   - Click + on the report dashboard page to add a new dashboard.
   - Click ⊞ → + to add a new dashboard.

   Note

   You can add up to 200 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 enter the dashboard management page.
   2) Move the cursor to the name of a dashboard, and then click ✎ to edit the dashboard name, or click 🗑 to delete the dashboard.
   3) Click **Back** to go back to the report dashboard page.
4. Add report(s) to a dashboard and edit the report(s).
   1) Select a report type and generate the report.
   2) Click **Add to Dashboard** on the report page to add the report to dashboard.

      The report appears on the selected dashboard.

      And ⊕ appears on the lower-right of the report dashboard page. You can click the icon to add more reports.
   3) Perform the following operations.
      - Add More Reports: Click ⊕ 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 Name**.
- Delete Report from Dashboard: Click ··· and then click **Delete**.

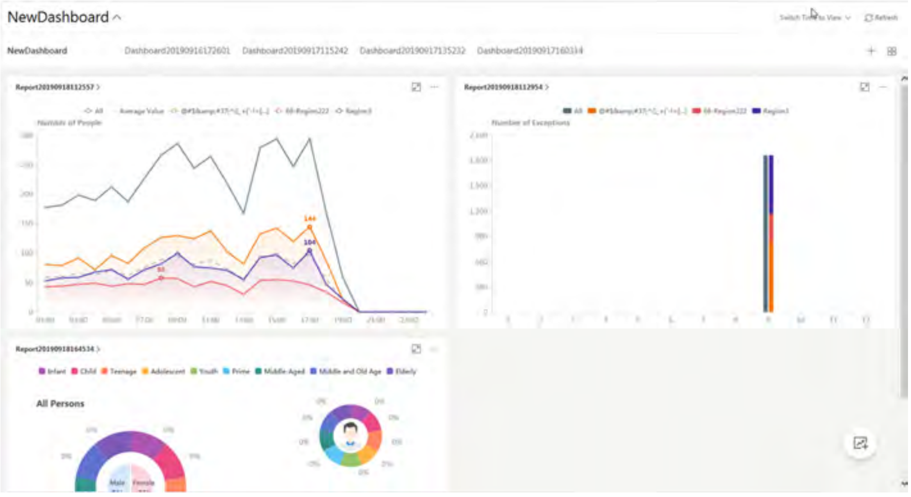


Figure 25-1 Report Dashboard

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) Perform one of the following operations.

- 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.
- Click **View** to view the reports in the dashboard on the basis of the time you set in the previous sub step.

25.2 People Counting Report

People counting report shows the number of line crossing people counted by people counting cameras or obtained from the card swiping records of access control devices in a specific area and within a certain time period. The report lets you know the number of persons who stay in a specific region, which can be used for certain commercial or emergency scenarios. For example, during the peak time of a shopping mall, the shopping mall manager may need the people counting report to determine whether to limit the number of customers staying in the mall or not for security reasons.

Before generating a people counting report, you can add people counting group(s) to group the doors and people counting cameras of certain region so as to define region border. After that, you can set a regular report rule for the specified cameras which support people counting or people counting groups, and the system will send emails with reports attached to the target recipients daily, weekly, or monthly. You can also manually generate a people counting report at any time to view the data if required.

For details about adding a people counting group, refer to ***Add People Counting Group*** .

25.2.1 Generate People Counting Report

You can manually generate a people counting report to view the people counting statistics in a line chart or histogram, and generate reports for exporting the detailed data to local storage.

Before You Start

Properly configure the camera with a people counting rule for the required area. To configure the people counting rule, please refer to user manual of people counting camera.

Steps

1. Click **Intelligent Analysis** on the Home page and then select **People Counting** on the navigation panel on the left to enter the People Counting page.
2. Set the analysis type.

   People Counting for One Camera

   A people counting report based on the data from the cameras you select will be generated. You can compare the data of different cameras.

   People Counting in One Region

   A people counting report based on the data from the people counting groups you select will be generated. You can compare the data of different groups.

   Note

   You should have added people counting groups. See ***Add People Counting Group*** for details.
3. Select people counting camera(s) or people counting group(s) based on the analysis type you set in the previous step.
   1) Click .
   2) Select a current site or Remote Site from the drop-down site list to show its people counting cameras or people counting groups.

   Note

   Only people counting cameras and people counting groups will be displayed here.

   3) Check the people counting camera(s) or people counting group(s) for statistics.

   The selected item(s) will appear in the camera list or people counting group list.
4. Select item(s) for the report in the camera list or people counting group list.

Note

Up to 20 people counting cameras can be selected for statistics at the same time.

5. Set the report type to 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 people 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 people in each day of one 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 people 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 statistics of all the selected item(s) are displayed in the right panel.

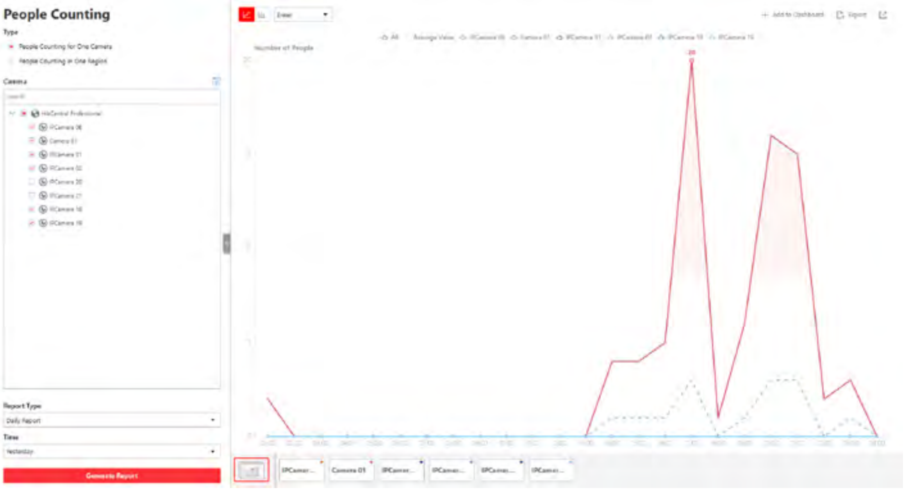


Figure 25-2 People Counting Report

8. **Optional:** Perform the following operation(s) after generating the people counting report.

Show/Hide Certain Data	Click the legend to show or hide the data of certain element, such as certain camera.
View Entered/ Exited/Both Entered and Exited Statistics	Select **Enter**, **Exit**, or **Enter and Exit** from the drop-down list. The total statistics and all the selected cameras' statistics are displayed and marked with different colors.
View Both Entered and Exited Statistics of Single Camera	Click the camera name on the page below to view the chart of single camera.
Switch Between Line Chart and Histogram	Select **Time** or **Item for Comparison** on the upper-right corner to switch the between line chart (displaying the trend for the number of people on different time points) or histogram (for comparison).
Play Linked Video	For line chart, if the selected report type is daily report, weekly report, or monthly report, click the line on the line chart to play the linked video. For histogram, if the selected report type is daily report, click the rectangle on the histogram to play the linked video.

25.2.2 Send People Counting Report Regularly

You can set a regular report rule for specified people counting cameras or specified resource groups, and the system can send an email with a report attached to the target recipients daily, weekly, or monthly, showing the number of people entered or exited detected by people counting cameras, or the number of people remained calculated by the people counting cameras and doors in the same region.

Before You Start

- Set the email template with recipient information, subject, and content. For details, refer to ***Set Email Template*** .
- Set the email settings such as sender address, SMTP server address and port, etc. For details, refer to ***Configure Email Account*** .

Steps

Note

- One report can contain up to 10,000 records in total.
- The report will be an Excel file.

1. Click **System** on the home page and enter **Report** page.
2. Select the report category as **People Counting**.
3. Create a name for the report.
4. Select the People Counting Type.

People Counting for One Camera

The report contains the number of people entered and exited detected by the people counting camera(s). You need to select the camera(s) as the Report Target.

For example, if you select the people counting type as **People Counting for One Camera** and select two people counting cameras as the **Report Target**, the system will generate two of the cameras respectively, including the number of people entered and exited detected by the two cameras.

People Counting for One Region

The report contains the number of people remained in one region, which is calculated by the detected people from the people counting camera(s) and the statistic people from the doors in the region. You need to select the resource group(s) as the Report Target.

Note

For more details about resource group, refer to ***Add People Counting Group*** .

5. Set the people counting camera(s) contained in the report.
   1) In the Report Target field, click **Add**.
   2) Select the people counting camera(s) or resource group(s).
   3) Click **Add**.
6. Set the report type as **Daily**, **Weekly**, or **Monthly** and set the sending time.

Daily Report

Daily report shows data on a daily basis. The system will send one report at the sending time every day, which contains data detected on the day (24 hours) before the current day.

For example, if you set the sending time as 20:00, the system will send a report at 20:00 every day, containing the number of people detected between 00:00 and 24:00 before the current day.

Weekly Report and Monthly Report

As compared to daily report, weekly report and monthly report can be less time-consuming, since they are not to be submitted every day. The system will send one report at the sending time every week or every month, which contains the number of people detected on the last 7 days or last month before the sending date.

For example, for weekly report, if you set the sending time as 6:00 on Monday, the system will send a report at 6:00 in the morning on every Monday, containing number of people detected between last Monday and Sunday.

7. After setting the report type, set how the report will present the data detected in the specified time period.

Example

For example, if you select the report type as **Daily**, you can select **Calculate by Hour** or **Calculate by Minute**. There will be 24 or 24×60 records for each camera respectively in the report, showing the number of people detected in each hour or each minute for one camera.

8. Set the sending time according to the report type.
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 ***Set Email Template*** .

10. 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.

25.3 Queue Analysis Report

Queue analysis report shows the number of queue exceptions and number of persons in each queue, and show the queue status including waiting duration and queue length. It is helpful for allocating resources for retailers.

You can set a regular report rule for the specified cameras, and the system will send emails with queue analysis reports attached to the target recipients daily, weekly, or monthly. You can also manually generate a queue analysis report at any time to view the data if required.

25.3.1 Generate Queue Analysis Report

For cameras which support queue management, you can generate a report to show the number of queue exceptions and number of persons in each queue, and show the queue status including waiting duration and queue length.

Before You Start

Add a camera which supports queue management to the system and configure queue regions. To configure the queue region, refer to user manual of the camera.

Steps

1. Click **Intelligent Analysis** on the Home page and then select **Queue Analysis** on the navigation panel on the left to enter the Queue Analysis page.
2. Select 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 cameras.

    Note

    Only cameras which support queue management will be displayed here.

    3) Check the camera(s) for statistics.

    The cameras will be added to the camera list.

3. Select the queue regions configured on the camera and the system will collect the queue data in these queue regions.

Note

For configuring the queue, refer to the user manual of the camera.

4. Select the report type as daily report, weekly report, monthly report, or annual report.

Daily Report

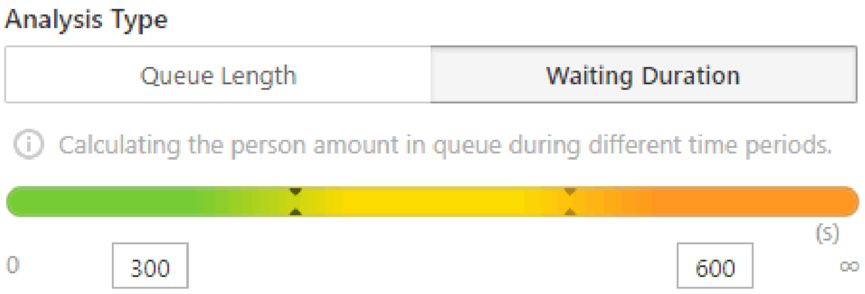
Daily report shows data on a daily basis. The system will calculate the queue data detected in each hour of one day.

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 queue data detected in each day of way week, in each day of one month, and in each month of one year.

5. Set the time or time period in the Time field for statistics.
6. **Optional:** Select the analysis type and set the report range for daily report, weekly report, or monthly report.

Waiting Duration



Analysis Type

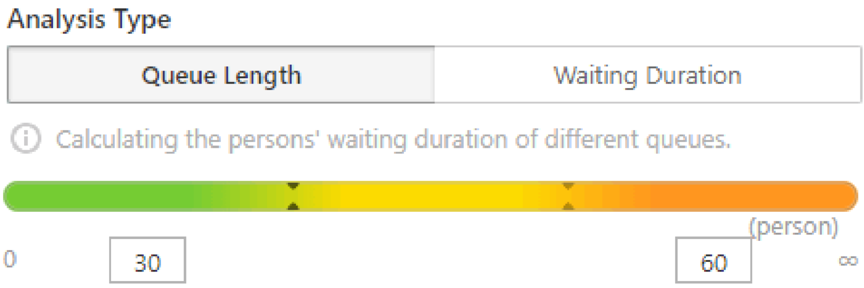
Calculating the person amount in queue during different time periods.

Figure 25-3 Set Range for Waiting Duration

The report can show the number of persons in each queue who have waited for specified duration at different time points.

For example, if you set the report range as 300s and 600s, the report will show that in each queue, how many persons have waited for less than 300s, how many persons have waited for 300 to 600s, and how many persons have waited for more than 600s.

Queue Length



Analysis Type

Queue Length | Waiting Duration

Calculating the persons' waiting duration of different queues.

Figure 25-4 Set Range for Queue Length

The report will show how many seconds each queue status (number of persons in different ranges) lasts.

For example, if you set the report range as 5 persons and 10 persons, the report will show that in each queue, how many seconds the status lasts when there are less then 5 persons, how many seconds the status lasts when there are 5 to 10 persons, and how many seconds the status lasts when there are more than 10 persons.

7. Click **Generate Report**.

A chart are displayed in the right panel, showing the number of exceptions (waiting timeout or people amount exceeding) of different queues.

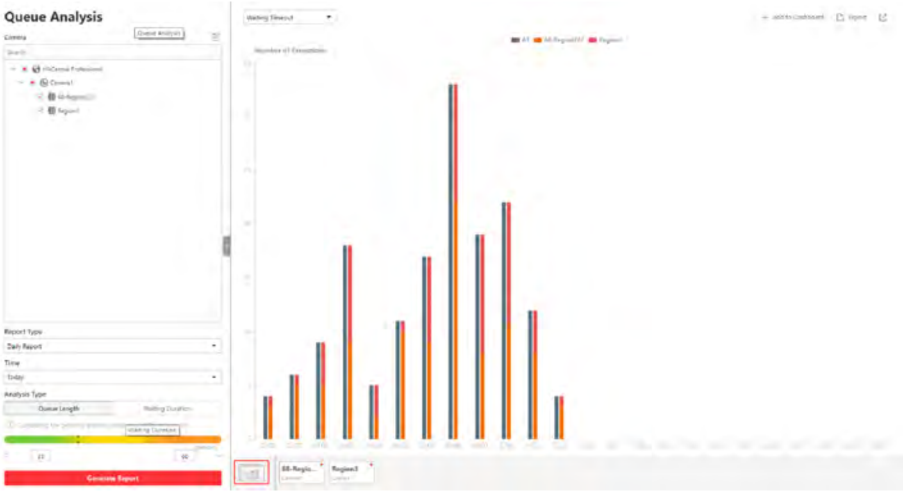


Figure 25-5 Queue Analysis Report

8. Optional: Perform the following operation(s) after generating the report.

Show/Hide Certain Data Click the legend to show or hide the data of certain element, such as queue.

View Queue Analysis Report of Single Queue Click the queue icon on the page below to view the report of the single queue, including the number of exceptions, number of people in the queue, and waiting durations .

Switch Between Number of Exceptions, Number of People, and Queue Length

Click 📊 on the page below to view the report of all the selected queues.

If you select the report type as **Daily Report**, **Weekly Report**, or **Monthly Report**, and set the analysis type as **Waiting Duration**, click the drop-down list to view the number of waiting timeout exceptions, or number of people in different and all queues.

If you select the report type as **Annual Report**, and set the analysis type as **Waiting Duration**, click the drop-down list to view the number of waiting timeout exceptions or number of people in all queues.

If you select the report type as **Daily Report**, **Weekly Report**, or **Monthly Report** and set the analysis type as **Queue Length**, click the drop-down list to view the number of people amount exceeding exceptions or queue length of different queues.

If you select the report type as **Annual Report**, and set the analysis type as **Queue Length**, the people amount exceeding exceptions will show.

25.3.2 Send Queue Analysis Report Regularly

You can set a regular report rule for specified cameras which support queue management, and the system can send an email with a report attached to the target recipients daily, weekly, or monthly, showing queue exceptions, number of persons in the queue, and queue status including waiting duration and queue length, detected by these people counting cameras during the specified time periods.

Before You Start

- Set the email template with recipient information, subject, and content. For details, refer to ***Set Email Template*** .
- Set the email settings such as sender address, SMTP server address and port, etc. For details, refer to ***Configure Email Account*** .

Steps

Note

- One report can contain up to 10,000 records in total.
- The report will be an Excel file.

1. Click **System** on the home page and enter **Report** page.
2. Select the report category as **Queue**.
3. Create a name for the report.
4. Set the camera(s) which support queue management contained in the report.
   1) In the Report Target field, click **Add**.

Note

Only cameras which support queue management will be displayed here.

2) Select the camera(s) for statistics.
3) Click **Add**.

The report will show the data of all the queues configured on the cameras.

Note

For configuring the queue, refer to the user manual of the camera.

5. Set the report type as **Daily**, **Weekly**, or **Monthly**.

Daily Report

Daily report shows data on a daily basis. The system will send one report at the sending time every day, which contains data detected on the day (24 hours) before the current day.

For example, if you set the sending time as 20:00, the system will send a report at 20:00 every day, containing queue data detected between 00:00 and 24:00 before the current day.

Weekly Report and Monthly Report

As compared to daily report, weekly report and monthly report can be less time-consuming, since they are not to be submitted every day. The system will send one report at the sending time every week or every month, which contains the queue data detected on the last 7 days or last month before the sending date.

For example, for weekly report, if you set the sending time as 6:00 on Monday, the system will send a report at 6:00 in the morning on every Monday, containing queue data detected between last Monday and Sunday.

6. Set the content in the report.

Queue Exception

The number of exceptions (people amount exceeding and waiting timeout duration) of each queue, including the number of persons in the queue exceeds the configured threshold and the waiting duration for persons in the queue exceeds the configured threshold.

Person Amount in Queue

The number of persons in each queue.

Queue Status

The status of each queue, including persons' waiting duration and number of persons in the queue.

If you select **Queue Status**, you should select the **Analysis Type** as waiting duration or queue length, and set the range.

Waiting Duration

The report will show the number of persons in each queue who have waited for specified duration.

For example, if you set the report range as ***Range 1 < 300 ≤ Range 2 ≤ 600 < Range 3***, the report will show that in each queue, how many persons have waited for less than 300s, how many persons have waited for 300 to 600s, and how many persons have waited for more than 300s.

Queue Length

The report will show how many seconds each queue status (number of persons in different ranges) lasts.

For example, if you set the report range as ***Range 1 < 5 ≤ Range 2 ≤ 10 < Range 3***, the report will show that in each queue, how many seconds the status lasts when there are less then 5 persons, how many seconds the status lasts when there are 5 to 10 persons, and how many seconds the status lasts when there are more than 10 persons.

7. Set the sending time according to the report type.
8. Select the email template from the drop-down list to define the recipient information and email format.

Note

You can click **Add New** to add a new email template. For setting the email template, refer to ***Set Email Template*** .

9. Finish adding the report.
   - Click **Add** to add the report and go back to the report list page.
   - Click **Add and Continue** to add the report and continue adding other reports.

25.4 Heat Analysis Report

Heat analysis report shows data with a heat map, which is a graphical representation of data represented by colors. The heat map function of the camera is usually used to track the consumers movements (where the customers walk, and what items they stop to touch and pick up) and analyze the visit times and dwell time in a configured area. This report is mainly used for store managers or retailers to see which part of the store got the most attention from consumers and which got least. Knowing where customers move is useful for retailers. They can optimize store layouts, for example, where to place popular and unpopular goods.

Before using heat analysis report, you can add a heat analysis group to define the region for heat analysis. After that, you can set a regular report rule for the specified cameras or the specified heat analysis groups, and the system will send emails with heat analysis reports attached to the target recipients daily, weekly, or monthly. You can also manually generate a heat analysis report at any time to view the data if required.

For details about adding a heat analysis group, refer to ***Add Heat Analysis Group*** .

25.4.1 Generate Heat Analysis Report

You can generate a heat analysis report to track consumer movements and analyze the visit times and dwell time in a configured area.

Before You Start

- Add a heat map network camera to the system and properly configure the camera with heat map rule for the required area. To add a heat map network camera, please refer to the *User Manual of HikCentral Professional Web Client*. To configure the heat map rule, please refer to the user manual of heat map network camera.
- Add the camera to a static map. For details about how to add a camera to the static map, refer to *User Manual of HikCentral Professional Web Client*.

Steps

1. Click **Intelligent Analysis** on the Home page and then select **Heat Analysis** on the navigation panel on the left to enter the Heat Analysis page.
2. Select analysis type.

   Heat Analysis for One Camera

   A heat analysis report based on the data from the selected cameras will be generated. The data of different cameras will be displayed and you can compare the data of different cameras.

   Heat Analysis in One Region

   A heat analysis report based on the data from the selected heat analysis groups will be generated. The data of different groups will be displayed and you can compare the data from different groups.

   Note

   You should have added heat analysis group(s). For details, see ***Add Heat Analysis Group*** .
3. Select heat analysis camera(s) or heat analysis group(s) for statistics.
   1) Click .

   Note

   Only heat analysis camera or heat analysis group will be displayed here.

   2) Check the heat analysis camera(s) or heat analysis group(s) for statistics.
4. Select camera(s) for the report in the camera list.

   Note

   Up to 20 heat analysis cameras can be selected for statistics at the same time.
5. Set the report type to 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 people or people dwell time 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 people or people dwell time 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 people or people dwell time in each day or month of the custom time interval.

6. **Optional:** 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. Set the analysis type.

Dwell Time

The minutes that the people stay at the same location during each time period for each camera.

People Amount

The number of people detected during each time period for each camera.

Note

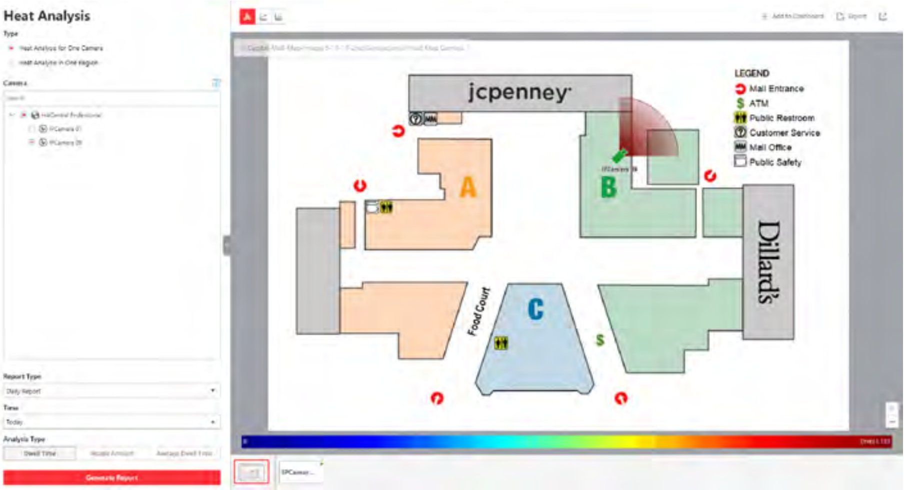
This analysis type is only supported by the second generation of heat analysis cameras.

Average Dwell Time

The average dwell time for the each person stay at the same location during each time period for each camera.

8. Click **Generate Report**.

The static maps of the selected cameras will appear.



Heat Analysis

Type

● Heat Analysis for One Camera

○ Heat Analysis in One Region

Camera

HikCentral Professional

IPCamera 01

IPCamera 09

Report Type

Daily Report

Time

Today

Analysis Type

Dwell Time | People Amount | Average Dwell Time

Generate Report

Figure 25-6 Static Map of selected Cameras

9. Click the map to view the detailed heat data of the cameras on the map. You can view each camera's field of view, and the fields are color coded. The red color block (255, 0, 0) indicates the most welcome region (most persons detected or longest dwell time), and blue color block (0, 0, 255) indicates the less-popular region (least persons detected or shortest dwell time).

Note

Move the cursor to the field of view to view the detected value, including people amount or dwell time.

10. **Optional:** Click the camera icon on the page below to view heat analysis of single camera.

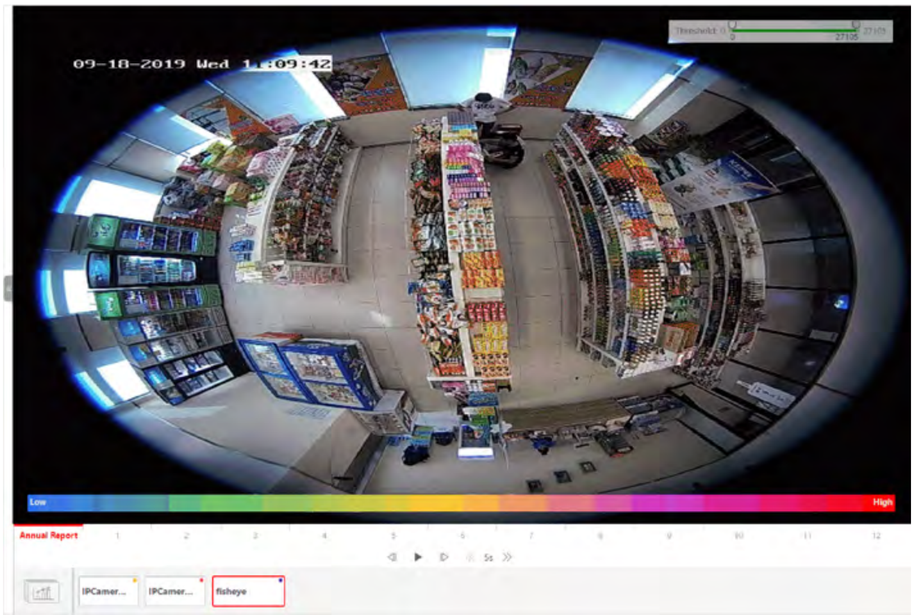


Figure 25-7 Heat Map of Single Camera

The image of the camera is color coded. The red color block (255, 0, 0) indicates the most welcome region (most persons detected or longest dwell time), and blue color block (0, 0, 255) indicates the less-popular region (least persons detected or shortest dwell time).

You can drag the slider on the upper-right to adjust the range of the heat value. The heat data out of the range will not be displayed.

11. **Optional:** Click 🟥 to switch among heat map, histogram, line chart to view the details.

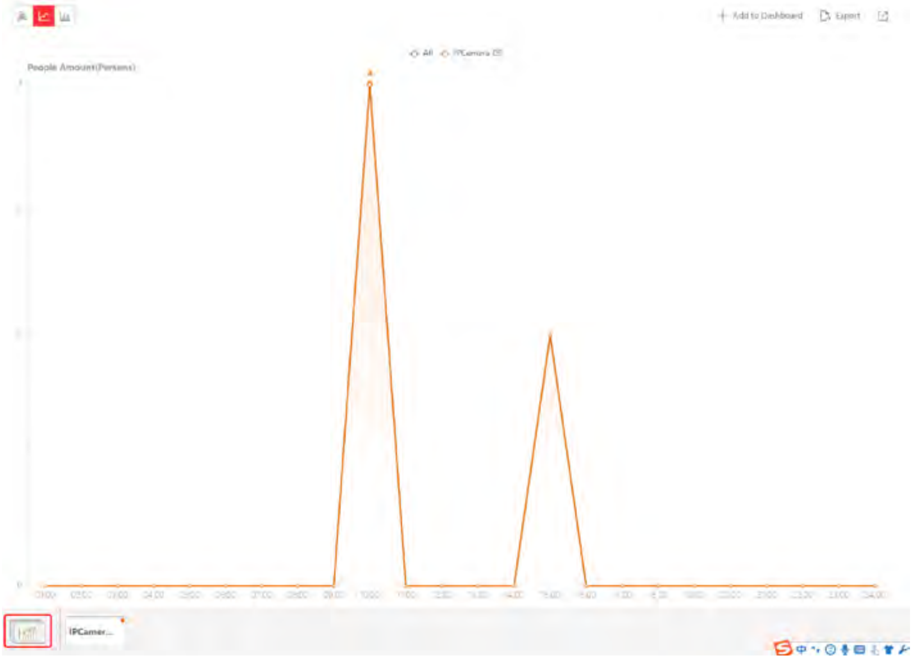


Figure 25-8 Line Chart of Heat Analysis

25.4.2 Send Heat Analysis Report Regularly

You can set a regular report rule for specified heat map cameras, and the system can send an email with a report attached to the target recipients daily, weekly, or monthly, showing the heat map data (people dwell time at each location and number of people detected) during the specified time periods.

Before You Start

- Set the email template with recipient information, subject, and content. For details, refer to ***Set Email Template*** .
- Set the email settings such as sender address, SMTP server address and port, etc. For details, refer to ***Configure Email Account*** .

Steps

ℹ **Note**

- One report can contain up to 10,000 records in total.
- The report will be an Excel file.

1. Click **System → Report** to enter the report settings page.
2. Click **Add** to open the Add Report page.
3. Select **Heat Analysis** as the report category.
4. Select heat analysis type.

   Heat Analysis for One Camera

   Analyze people dwell time and number of people detected by the specified camera(s).

   Heat Analysis in One Region

   Analyze people dwell time and number of people detected by the cameras in the specified heat analysis group(s).

   ℹ **Note**

   For details about adding heat analysis group, see ***Add Heat Analysis Group*** .
5. Create a name for the report.
6. Select the report target.
   1) Click **Add** and then select camera(s) or a heat analysis group(s) from the Resource Group/ Area list.

   ℹ **Note**

   If you select **Heat Analysis for One Camera** in step 4， you should select camera(s). If you select **Heat Analysis in One Region**, you should select heat analysis group(s).

   2) Click **Add**.
   3) **Optional:** Click × to delete a camera or a heat analysis group, or click **Delete All** to delete all selected item(s).
7. Set the report type as **Daily**, **Weekly**, or **Monthly**.

   Daily Report

   Daily report shows data on a daily basis. The system will send one report at the sending time every day, which contains data detected on the day (24 hours) before the current day.

   For example, if you set the sending time as 20:00, the system will send a report at 20:00 every day, containing the heat map data detected between 00:00 and 24:00 before the current day.

   Weekly Report and Monthly Report

   As compared to daily report, weekly report and monthly report can be less time-consuming, since they are not to be submitted every day. The system will send one report at the sending time every week or every month, which contains the heat map data detected on the last 7 days or last month before the sending date.

For example, for weekly report, if you set the sending time as 6:00 on Monday, the system will send a report at 6:00 in the morning on every Monday, containing heat map data detected between last Monday and Sunday.

8. After setting the report type, set how the report will present the data detected in the specified time period.

   Example

   For example, if you select the report type as **Weekly**, you can select **Calculate by Day** or **Calculate by Hour**. There will be 7 or 7×24 records for each camera respectively in the report, showing the people amount or dwell time detected on each day or each hour for one camera.

9. Set the content in the report.

   Dwell Time

   The minutes that the people stay at the same location during each time period for each camera.

   People Amount

   The number of people detected during each time period for each camera.

   Average Dwell Time

   The average time that each people stay at a same location during each time period for each camera. The value is calculated by dividing the dwell time by the number of people who appear at the location.

   Note

   - The Number of People who Appear at a Location= The Number of People who Stay at the Location at the End of Previous Time Period + The Number of People who Visit the Location at the Current Time Period.
   - The number of people who appears at a location refers to the number of people who visits the location from 00:00:00 to 23:59:59.

10. Set the sending time according to the report type.
11. 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*** .

12. 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.

25.5 Pathway Analysis Report

Pathway analysis is mainly used to analyze the people counting on the pathways in the shopping malls. With the help of fisheye cameras, the system can collect the consumers data (for example,where the customers walk mostly) and translate that data onto a dashboard for mall managers. This helps managers analyze which areas/shops of the mall best catch a shopper's attention and which are overlooked.

Before using pathway analysis, you should add pathway analysis groups first, which define the region for pathway analysis. After that, you can set a regular report rule for the specified pathway analysis group, and the system will send emails with pathway analysis reports attached to the target recipients daily, weekly, or monthly. You can also manually generate a pathway analysis report at any time to view the data if required.

For details about adding a pathway analysis group, refer to ***Add Pathway Analysis Group*** .

25.5.1 Generate Pathway Analysis Report

Pathway analysis is mainly used to analyze the people counting on the pathways in the shopping malls. With the help of fisheye cameras, the system can collect the consumers data (for example, where the customers walk mostly) and translate that data onto a dashboard for mall managers. This helps managers analyze which areas/shops of the mall best catch a shopper's attention and which are overlooked. After setting the fisheye camera's pathways and their directions, the system calculates the people dwell time at each pathway and number of people walking by, thus helps them make decisions.

Before You Start

- Properly add the camera to a static map and set its pathways on the map via the Web Client first. For details about adding camera to map and set pathways, refer to the *User Manual of HikCentral Professional Web Client*.
- You should have added pathway analysis groups. For details, see ***Add Pathway Analysis Group*** .

Steps

Note

This function is only supported by the second generation of fisheye cameras.

1. Click **Intelligent Analysis** on the Home page and then select **Pathway Analysis** on the navigation panel on the left to enter the Pathway Analysis page.
2. Select path analysis group(s) from the Resource Group list for statistics.
3. 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 people or people dwell time 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 people or people dwell time 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 people or people dwell time in each day or month of the custom time interval.

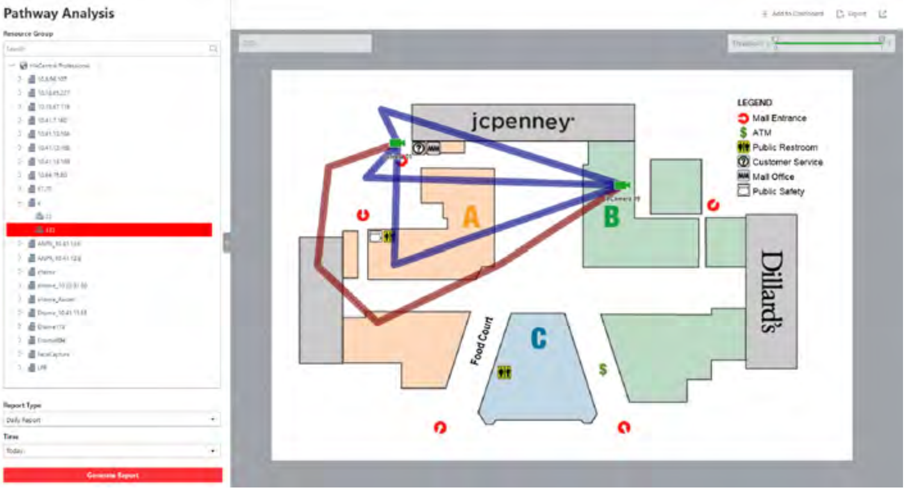
4. **Optional:** Set the time or time period in the Time field for statistics.

Note

For custom time interval report, you need to set the start time and end time to specify the time period.

5. Click **Generate Report**.

The static map with the cameras and pathways color coded on the map will be displayed. The red color block (255, 0, 0) indicates the most welcome pathway (most persons detected or longest dwell time), and blue color block (0, 0, 255) indicates the less-popular pathway (least persons detected or shortest dwell time).



Pathway Analysis

Resource Group

Report Type

Daily Report

Time

Today

Figure 25-9 Pathway Analysis Report

6. Move the cursor to the camera hot spot to view the line chart or heat map of the people amount and people dwell time in the pathways during this time period.

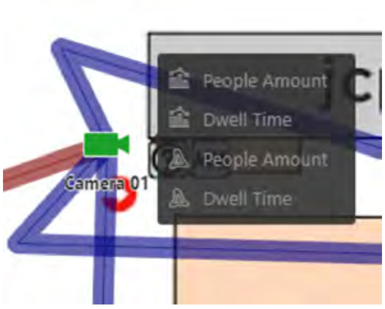


Figure 25-10 View Heat Map or Line Chart

25.5.2 Send Pathway Report Regularly

You can set a regular report rule for specified fisheye cameras which support pathway analysis, and the system can send an email with a report attached to the target recipients daily, weekly, or monthly, showing the people counting data (people dwell time at each location and number of people) on the configured pathways, detected by these fisheye cameras, during the specified time periods.

Before You Start

- Set the email template with recipient information, subject, and content. For details, refer to ***Set Email Template*** .
- Set the email settings such as sender address, SMTP server address and port, etc. For details, refer to ***Configure Email Account*** .

Steps

Note

- One report can contain up to 10,000 records in total.
- The report will be an Excel file.

1. Click **System** on the home page and enter **Report** page.
2. Select the report category as **Pathway**.
3. Create a name for the report.
4. Set the fisheye camera contained in the report, which support pathway analysis.
    1) In the Report Target field, click **Add**.

       All the fisheye cameras added to the current site which support pathway analysis are displayed.
    2) Select one fisheye camera.
    3) Click **Add**.
5. Set the report type as **Daily**, **Weekly**, or **Monthly**.

   Daily Report

Daily report shows data on a daily basis. The system will send one report at the sending time every day, which contains data detected on the day (24 hours) before the current day.

For example, if you set the sending time as 20:00, the system will send a report at 20:00 every day, containing people amount and dwell time 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 heat map data detected on the last 7 days or last month before the sending date.

For example, for weekly report, if you set the sending time as 6:00 on Monday, the system will send a report at 6:00 in the morning on every Monday, containing people amount and dwell time detected between last Monday and Sunday.

6. After setting the report type, set how the report will present the data detected in the specified time period.

   Example

   For example, if you select the report type as **Weekly**, you can select **Calculate by Day** or **Calculate by Hour**. There will be 7 or 7×24 records for each camera respectively in the report, showing the people amount and dwell time detected on each day or each hour for one camera.
7. Set the sending time according to the report type.
8. Select the email template from the drop-down list to define the recipient information and email format.

   Note

   You can click **Add New** to add a new email template. For setting the email template, refer to ***Set Email Template*** .
9. Finish adding the report.
   - Click **Add** to add the report and go back to the report list page.
   - Click **Add and Continue** to add the report and continue adding other reports.

25.6 Person Feature Analysis Report

Person feature analysis report shows the proportion of persons with different features detected by cameras which support facial recognition. The person features refers to the gender and age group of the detected persons, such as male, female, child, the elderly, and teenager.

You can add a person feature analysis group before generating a report to define the region for person feature analysis by grouping the cameras which support facial recognition and feature analysis. After that, you can set a regular report rule for the specified cameras or specified person feature analysis groups, and the system will send emails with reports attached to the target recipients daily, weekly, or monthly. You can also manually generate a person feature analysis report at any time to view the data if required.

For details about adding a person feature analysis group, refer to ***Add Person Feature Analysis Group*** .

25.6.1 Generate Person Feature Analysis Report

The system supports saving features (including age and gender) of recognized human faces and generating reports in various time periods. The reports tells the percentage and number of people of different gender and age groups in different time period. It can be used in places such as shopping mall to analyze interests of people in different gender and age.

Before You Start

Make sure you have added a person feature analysis group if you want to perform feature analysis in one region. See ***Add Person Feature Analysis Group*** for details about adding a person feature analysis group.

Steps

1. Click **Intelligence Analysis →** to enter the Person Feature Analysis page.
2. Select analysis type.

   Feature Analysis for One Camera

      Compare percentage and number of people of different gender and age groups detected by specified camera(s).

   Feature Analysis in One Region

      Compare percentage and number of people of different gender and age groups detected by the cameras in specified person feature analysis group(s) of multiple regions.

3. Select camera(s)/resource group(s).

   Note

   - Up to 20 cameras/resource groups can be selected for statistics at the same time.
   - The system supports selecting one resource group of a remote site.

4. Select the report type as daily report, weekly report, monthly report, annual report, or customize the time interval for a report, and the system will generate statistics of the selected camera(s)/resource group(s) of the current day/week/month/year or the customized period.
5. 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.

6. Click **Generate Report**.

Note

The statistics of all the selected cameras/resource groups are displayed on the right panel.

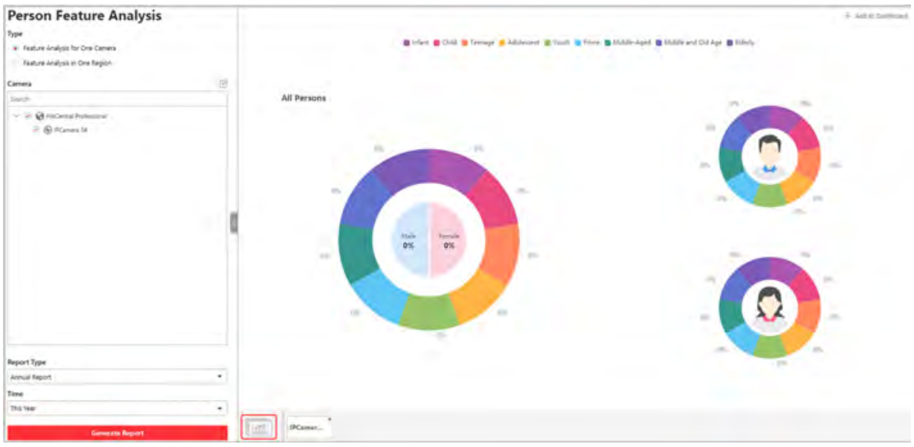


Figure 25-11 Person Feature Analysis

7. **Optional:** Click **Add to Dashboard** to display the report on the Dashboard.

25.6.2 Send Person Feature Analysis Report Regularly

You can set a regular report rule for specified cameras of person feature analysis, and the system can send an email with a report attached to the target recipients daily, weekly, or monthly, showing the percentage and number of people of different genders and ages during the specified time periods.

Before You Start

- Set the email template with recipient information, subject, and content. For details, refer to ***Set Email Template*** .
- Set the email settings such as sender address, SMTP server address and port, etc. For details, refer to ***Configure Email Account*** .

Steps

1. Click **System → Report** to enter the report settings page.
2. Click **Add** to open the Add Report page.
3. Select **Person Feature Analysis** as the report category.
4. Select person feature type.

   Feature Analysis for One Camera

   Compare percentage and number of people of different gender and age groups detected by specified camera(s).

   Feature Analysis in One Region

   Compare percentage and number of people of different gender and age groups detected by the cameras in specified person feature analysis group(s) of multiple regions.

5. Create a name for the report.
6. Select the report target.
    1) Click **Add** and then select camera(s) or person feature analysis group(s) from the Resource Group/Area list.

    Note

    If you select **Feature Analysis for One Camera** as person feature type, you should select camera(s). If you select **Feature Analysis in One Region**, you should select feature analysis group(s).

    2) Click **Add**.
    3) **Optional:** Click × to delete a camera or a person feature group, or click **Delete All** to delete all item(s).
7. Set the report type as **Daily**, **Weekly**, or **Monthly**.

    Daily Report

    Daily report shows data on a daily basis. The system will send one report at the sending time every day, which contains data detected on the day (24 hours) before the current day.

    For example, if you set the sending time as 20:00, the system will send a report at 20:00 every day, containing the person feature data detected between 00:00 and 24:00 before the current day.

    Weekly Report and Monthly Report

    As compared to daily report, weekly report and monthly report can be less time-consuming, since they are not to be submitted every day. The system will send one report at the sending time every week or every month, which contains the person feature data detected on the last 7 days or last month before the sending date.

    For example, for weekly report, if you set the sending time as 6:00 on Monday, the system will send a report at 6:00 in the morning on every Monday, containing person feature data detected between last Monday and Sunday.
8. After setting the report type, set how the report will present the data detected in the specified time period.

    Example

    For example, if you select the report type as **Weekly**, you can select **Calculate by Day** or **Calculate by Hour**. There will be 7 or 7×24 records for each camera respectively in the report, showing the percentage and number of people of different gender and age groups detected on each day or each hour for one camera.
9. Set the sending time according to the report type.
10. 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*** .

11. 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.

25.7 Temperature Analysis Report

Temperature analysis report show the number of exceptions (temperature too high or too low) and maximum/minimum temperature of different thermometry points on different presets.

You can set a regular report rule for the specified thermal cameras and the system will send emails with reports attached to the target recipients daily, weekly, or monthly. You can also manually generate a temperature analysis report at any time to view the data if required.

25.7.1 Generate Temperature Report

For thermal cameras, you can generate a report to show the number of exceptions (temperature too high or too low) and maximum/minimum temperature of different thermometry points on different presets.

Steps

1. Click **Intelligent Analysis** on the Home page and then select **Temperature Analysis** on the navigation panel on the left to enter the Tempeature Analysis page.
2. Select thermal 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 thermal cameras.

      Note

      Only thermal cameras will be displayed here.
   3) Check the thermal camera(s) for statistics.

      The cameras will be added to the camera list.
3. Select the preset(s) configured on the camera and the system will collect the data on the thermometry point in these presets.

   Note

   For configuring the thermometry point with temperature measurement rules, refer to the user manual of the thermal camera.
4. 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 temperature data detected 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 temperature data detected 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 temperature data detected in each day or month of the custom time interval.

5. 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.

6. Click **Generate Report**.

   The temperature statistics of all the selected presets are displayed in the right panel.

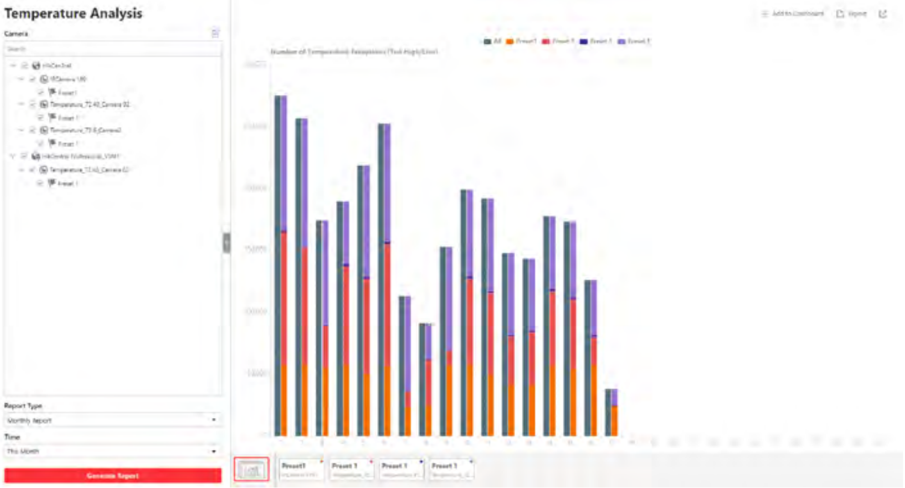


Figure 25-12 Temperature Report

7. **Optional:** Perform the following operation(s) after generating the temperature report.

Show/Hide Certain Data

Click the legend to show or hide the data of certain element, such as certain preset or thermometry point.

View Temperature Report of Single Preset

Click the preset icon on the page below to view the report in the single preset.

View Temperature Report of Single Thermometry Point

a. Click the preset icon on the page below to view the report in the single preset.

b. In the **Item for Comparison** field, select one thermometry point.

c. In the **Item for Comparison** field, select the indicator you want to view in the chart.

High/Low Temperature

Shows the number of exceptions that the temperature at this thermometry point is higher or lower than the pre-defined temperature.

Max. Temperature

Shows the maximum temperature at this thermometry point during the set time period.

The temperature is displayed in line chart, indicating the trend.

Min. Temperature

Shows the minimum temperature at this thermometry point during the set time period.

The temperature is displayed in line chart, indicating the trend.

25.7.2 Send Temperature Report Regularly

You can set a regular report rule for specified thermal cameras, and the system can send an email with a report attached to the target recipients daily, weekly, or monthly, showing temperature exceptions or min./max. temperature, detected by these thermal cameras during the specified time periods.

Before You Start

- Set the email template with recipient information, subject, and content. For details, refer to ***Set Email Template*** .
- Set the email settings such as sender address, SMTP server address and port, etc. For details, refer to ***Configure Email Account*** .

Steps

Note

- One report can contain up to 10,000 records in total.
- The report will be an Excel file.

1. Click **System** on the home page and enter **Report** page.
2. Select the report category as **Temperature Analysis**.
3. Create a name for the report.
4. Set the thermal camera(s) and presets contained in the report.
   1) In the Report Target field, click **Add**.

All the thermal camera(s) added to the current site are displayed.

2) Select the thermal camera(s) and preset.
3) Click **Add**.

The report will show the temperature exceptions (including temperature too high or too low) or maximum and minimum temperature of different thermometry points on these presets.

5. Set the report type as **Daily**, **Weekly**, or **Monthly** and set the sending time.

Daily Report

Daily report shows data on a daily basis. The system will send one report at the sending time every day, which contains data detected on the day (24 hours) before the current day.

For example, if you set the sending time as 20:00, the system will send a report at 20:00 every day, containing the temperature exceptions or min./max. temperature detected between 00:00 and 24:00 before the current day.

Weekly Report and Monthly Report

As compared to daily report, weekly report and monthly report can be less time-consuming, since they are not to be submitted every day. The system will send one report at the sending time every week or every month, which contains the temperature exceptions or min./max. temperature detected on the last 7 days or last month before the sending date.

For example, for weekly report, if you set the sending time as 6:00 on Monday, the system will send a report at 6:00 in the morning on every Monday, containing temperature exceptions or min./max. temperature detected between last Monday and Sunday.

6. After setting the report time, set how the report will present the data detected in the specified time period.

Example

For example, if you select the report type as **Daily**, you can select **Calculate by Hour** or **Calculate by Minute**. There will be 24 or 24×60 records for each thermometry point respectively in the report, showing the temperature exceptions or min./max. temperature detected in each hour or each minute.

7. Set the content in the report.

Temperature Exception

The number of exceptions on temperature (temperature too high or too low) of each thermometry point.

Temperature Status

The maximum temperature and minimum temperature of each thermometry point.

8. Select the email template from the drop-down list to define the recipient information and email format.

Note

You can click **Add New** to add a new email template. For setting the email template, refer to ***Set Email Template*** .

9. Finish adding the report.
   - Click **Add** to add the report and go back to the report list page.
   - Click **Add and Continue** to add the report and continue adding other reports.

25.8 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.

25.8.1 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. Click **Intelligent Analysis** on the Home page and then select **Vehicle Analysis** on the navigation panel on the left to enter the Vehicle Analysis page.
2. 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.
3. 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.
4. 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.

5. 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.

6. Click **Generate Report**.

   The passing vehicles statistics detected by all the selected cameras are displayed in the right panel.

25.8.2 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 ***Set Email Template*** .
- Set the email settings such as sender address, SMTP server address and port, etc. For details, refer to ***Configure Email Account*** .

Steps

Note

- One report can contain up to 10,000 records in total.
- The report will be an Excel file.

1. Click **System** on the home page and enter **Report** page.
2. Select the report category as **Vehicle Analysis**.
3. Create a name for the report.
4. Set the ANPR camera(s) contained in the report.
   1) In the Report Target field, click **Add**.

      All the ANPR camera(s) added to the current site are displayed.
   2) Select the ANPR camera(s).
   3) Click **Add**.

5. Set the report type as **Daily**, **Weekly**, or **Monthly** and set the sending time.

   Daily Report

   Daily report shows data on a daily basis. The system will send one report at the sending time every day, which contains data detected on the day (24 hours) before the current day.

   For example, if you set the sending time as 20:00, the system will send a report at 20:00 every day, containing the number of passing vehicles detected between 00:00 and 24:00 before the current day.

   Weekly Report and Monthly Report

   As compared to daily report, weekly report and monthly report can be less time-consuming, since they are not to be submitted every day. The system will send one report at the sending time every week or every month, which contains the number of passing vehicles detected on the last 7 days or last month before the sending date.

   For example, for weekly report, if you set the sending time as 6:00 on Monday, the system will send a report at 6:00 in the morning on every Monday, containing number of passing vehicles detected between last Monday and Sunday.

6. After setting the report time, set how the report will present the data detected in the specified time period.

   Example

   For example, if you select the report type as **Daily**, you can select **Calculate by Hour** or **Calculate by Minute**. There will be 24 or 24×60 records for each camera respectively in the report, showing the number of passing vehicles detected in each hour or each minute for one camera.

7. Select the email template from the drop-down list to define the recipient information and email format.

   Note

   You can click **Add New** to add a new email template. For setting the email template, refer to ***Set Email Template*** .

8. Finish adding the report.
   - Click **Add** to add the report and go back to the report list page.
   - Click **Add and Continue** to add the report and continue adding other reports.

Chapter 26 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	7660 (TCP)	Used for receiving registration from ISUP device.
SYS	7661 (TCP)	Used for getting stream from ISUP device via Streaming Server
SYS	30051 (HTTP)	Used for communication between SYS and ADS in server distributed deployment.
SYS	30053 (HTTPS)	Used for communication between SYS and ADS in server distributed deployment, after encrypted transmission enabled.
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	Used for getting the status of Streaming Gateway.

Destination	Port No.	Description
Streaming Gateway	6678	Used for setting the certificate.
Keyboard Proxy Service (KPS)	8910 (HTTP)	Used for network keyboard to access the Keyboard Proxy Service.
NTP Service	123 (UDP)	NTP port used for time synchronization.
PostgreSQL	5432 (TCP)	Used for database access. **Note** This port is available in distributed deployment.
Application Data Service (ADS) Port		
ADS	30054 (HTTPS)	Used for communication between SYS and ADS in server distributed deployment, after encrypted transmission enabled.
ADS	30052 (HTTP)	Used for communication between SYS and ADS.
ADS	19999 (HTTP)	Used for communication between SYS's NGINX and ADS.
ADS	19443 (HTTPS)	Used for communication between SYS's NGINX and ADS.
WDS	6208 (WebSocket)	Listen port for Service Manager.
WDS	8208 (WebSocket over TLS)	Listen port for Service Manager after encrypted transmission enabled.
PostgreSQL	5432 (TCP)	Used for real-time data synchronization between Application Data Server and Application Data Standby Server. **Note** This port is available in distributed deployment.
Streaming Service Port		
Streaming Service	554 (RTSP)	Used for Streaming Service to get stream (real time streaming port).
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).

Destination	Port No.	Description	
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	Used for security certificate authentication.	
Streaming Service	6678	Used for setting the certificate.	
pStor Cluster Service			
pStor Cluster Service	9012	Used for accessing the pStor Cluster Service via Web Browser.	
pStor Cluster Service	6300	Used for signaling gateway.	
OpenAPI			
OpenAPI Service	443	Used for third-party system accessing OpenAPI service.	
OpenAPI Service	8208	Listen port for Service Manager after encrypted transmission enabled.	

See Far, Go Further