HikCentral Professional

Quick Start Guide

Contents

Chapter 1 Guide Content

This guide briefly explains how to install your HikCentral Professional as well as how to configure some of its basic features.

To ensure the properness of usage and stability of the HikCentral Professional, please refer to the contents below and read the guide carefully before installation and operation.

Chapter 2 Administrator Rights

When you install and run the service modules, it is important that you have administrator rights on the PCs or servers that should run these components. Otherwise, you cannot install and configure the system.

Consult your IT system administrator if in doubt about your rights.

If you access the system via HikCentral All-In-One Server, you can log in to the **operating system** with the following default administrator user name and password at the first boot.

- Default User Name: ***Administrator***
- Default Password: ***Abc12345***

It is recommended that you change the default administrator password immediately after entering the system for data security.

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.

Chapter 3 System Requirements

3.1 System Requirements for Servers

Server without Remote Site Management (RSM) Module

- **Operating System:** Microsoft® Windows 7 SP1 (64-bit), Windows 8.1 (64-bit), Windows 10 (64-bit), Windows Server 2008 R2 SP1 (64-bit), Windows Server 2012 (64-bit), Windows Server 2012 R2 (64-bit), Windows Server 2016 (64-bit), Windows Server 2019 (64-bit).

Note

For Windows 8.1 and Windows Server 2012 R2, make sure it is installed with the rollup (KB2919355) undated in April, 2014.

- **CPU:** Intel® Core i3-4590 @ 3.3 GHz.
- **Memory:** 8 GB.
- **HDD:** Enterprise-class SATA disk with 601 GB storage capacity. When running the SYS service, there should be at least 1 GB free space.
- **Network Controller:** RJ45 Gigabit self-adaptive Ethernet interfaces.

Server with Remote Site Management (RSM) Module

- **Operating System:** Microsoft® Windows 7 SP1 (64-bit), Windows 8.1 (64-bit), Windows 10 (64-bit), Windows Server 2008 R2 SP1 (64-bit), Windows Server 2012 (64-bit), Windows Server 2012 R2 (64-bit), Windows Server 2016 (64-bit), Windows Server 2019 (64-bit).

Note

For Windows 8.1 and Windows Server 2012 R2, make sure it is installed with the rollup (KB2919355) undated in April, 2014.

- **CPU:** Intel® Xeon® E5-2620 V4 @ 2.10 GHz.
- **Memory:** 16 GB.
- **HDD:** Enterprise-class SATA disk with 601 GB storage capacity. When running the SYS service, there should be at least 1 GB free space.
- **Network Controller:** RJ45 Gigabit self-adaptive Ethernet interfaces.

3.2 System Requirements for Control Client

- **Operating System:** Microsoft® Windows 7 SP1 (32/64-bit), Windows 8.1 (32/64-bit), Windows 10 (64-bit), Windows Server 2008 R2 SP1 (64-bit), Windows Server 2012 (64-bit), Windows Server 2012 R2 (64-bit), Windows Server 2016 (64-bit), Windows Server 2019 (64-bit).

Note

For Windows 8.1 and Windows Server 2012 R2, make sure it is installed with the rollup (KB2919355) undated in April, 2014.

- **CPU:** Intel® Core™ i5-4590 @ 3.3 GHz and above.
- **Memory:** 8 GB and above.
- **Video Card:** NVIDIA® Geforce GTX 970 and above.
- **HDD:** When running the Control Client, there should be at least 1 GB free space.

Chapter 4 Centralized Deployment and Distributed Deployment

HikCentral Professional provides centralized or distributed deployment for the two core services: System Management Service and Application Data Service.

- **System Management Service (SYS):** It provides unified authentication service for connecting with the clients and servers. It also provides centralized management for the users, roles, permissions, resources, and services.
- **Application Data Service (ADS):** It is mainly used for processing and storing the application data of the system.

Centralized Deployment

The SYS and ADS are deployed on the same server. In centralized deployment, up to 3,000 cameras, 128 access points, 1,024 IP addresses can be managed in one site.

Distributed Deployment

The SYS and ADS are deployed on different servers. Distributed deployment can improve the system performance and the number of connectable cameras can be increased to 10,000. Up to 10,000 cameras, 512 access points, 2,500 video devices, 500 access control devices can be managed in one site.

The whole process of distributed deployment is shown as follows:

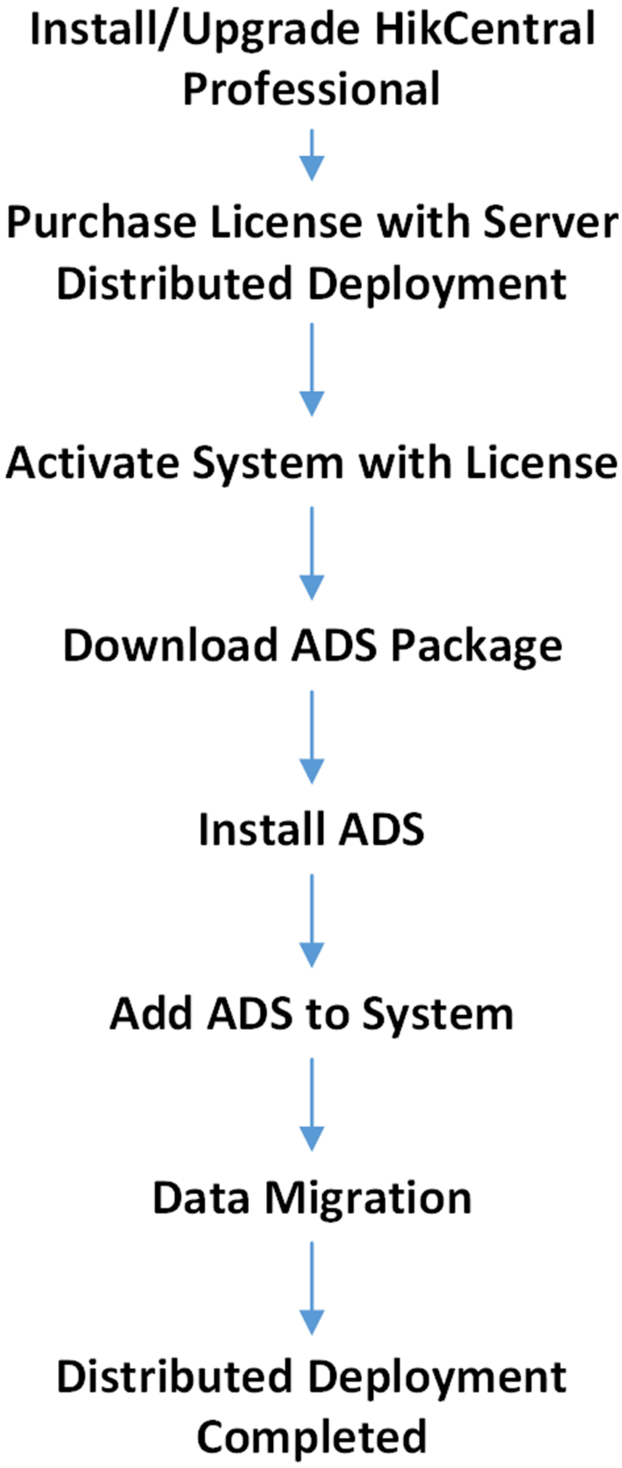

Install/Upgrade HikCentral Professional
Purchase License with Server Distributed Deployment
Activate System with License
Download ADS Package
Install ADS
Add ADS to System
Data Migration
Distributed Deployment Completed

Figure 4-1 Process of Distributed Deployment

- **Install/Upgrade HikCentral Professional:** Install or upgrade the HikCentral Professional with the installation package **HikCentral_Professional_V1.4.0**. For details about the installation, refer to ***Installation*** .
- **Purchase License with Server Distributed Deployment:** Purchase a License with server distributed deployment. You can contact our technical support for details.
- **Activate System with License:** Active the HikCentral Professional with the License you purchased. For details about activation, refer to ***Manage License*** .
- **Download ADS Package:** Download the installation package of ADS from the home page of the Web Client.
- **Install ADS:** Install the ADS with the downloaded ADS installation package on another server. Following the instructions during the installation to complete the installation.
- **Add ADS to System:** Add the ADS server to the HikCentral Professional. For details, refer to ***Manage Application Data Server*** .
- **Data Migration:** After adding the ADS to the system, the data in the SYS server will be migrated to the ADS server automatically.

Chapter 5 Installation

Install the service modules on your servers or PCs to build your HikCentral Professional.

Two installation packages are available for building your system.

Basic Installation Package

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

Control Client Installation Package

Contains the Control Client module only.

Note

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

5.1 Install Module

Two installation methods are available for building the modules.

Typical Mode

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

Custom Mode

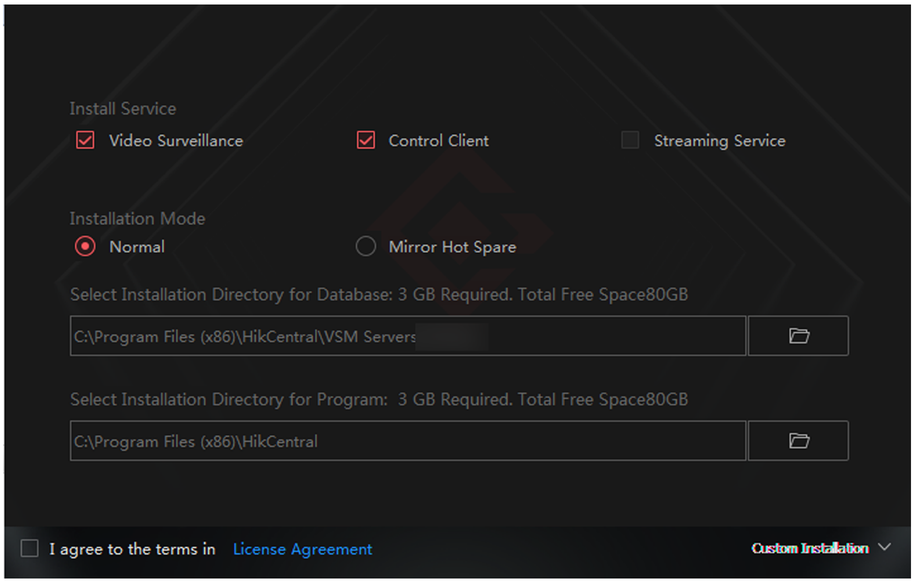
Select the installation directory and modules to be installed as desired.

5.1.1 Install Service Module in Custom Mode

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

Steps

1. Double-click (HikCentral Professional) to enter the Welcome panel of the InstallShield Wizard.
2. Click **I agree to the terms in License Agreement** and read the License Agreement.
3. Select **Custom Installation** as setup type.
4. Select the module(s) you want to install and click **Next**.



Install Service

☑ Video Surveillance ☑ Control Client □ Streaming Service

Installation Mode

● Normal ○ Mirror Hot Spare

Select Installation Directory for Database: 3 GB Required. Total Free Space80GB

C:\Program Files (x86)\HikCentral\VSM Servers[redacted]

Select Installation Directory for Program: 3 GB Required. Total Free Space80GB

C:\Program Files (x86)\HikCentral

□ I agree to the terms in License Agreement

Figure 5-1 Select Modules to Install

Note

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

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

5. **Optional:** Select the hot spare mode if you select to install Video Surveillance Service in the previous step.
   - Select **Normal** if you do not need to build a hot spare system.
   - Select **Mirror Hot Spare** to build a mirror hot spare system. There are two HikCentral servers in the hot spare system: host server and spare server. When the host server works, the data in host server is copied to the spare server in real time. When the host server fails, the spare server switches into operation without interruption, thus increasing the reliability of the system.

Note

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

6. **Optional:** Select a proper directory as desired to install the program module(s) and the database.
7. Click **Custom Installation** again to return to the Welcome panel.
8. Click **Install Now** to begin the installation.

   A panel indicating progress of the installation will display.
9. Click **Finish** to complete the installation.

5.1.2 Install Service Module in Typical Mode

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

Steps

1. Double-click (HikCentral Professional) to enter the welcome panel of the InstallShield Wizard.
2. Click **I agree to the terms in License Agreement** and read the License Agreement.
3. Click **Install Now** to begin the installation.

   A panel indicating progress of the installation will display.
4. Click **Finish** to complete the installation.

5.2 Install Control Client

You must install HikCentral Professional Control Client on your computer before you can access the system via Control Client. You can get the installation package from Hikvision's official site, or download from HikCentral Professional Web Client's Home page (32-bit).

Steps

Note

We provide an installation package of Control Client in MSI format. For scenario with Active Directory Domain Services (AD DS), you can install/upgrade the Control Clients on the PCs in the AD domain in a batch by Windows® Group Policy. Click ***here*** to visit the official site of Microsoft® and you can view details and instructions about Windows® Group Policy.

1. Double-click (HikCentral Professional_Client) to enter the welcome panel of the InstallShield Wizard.
2. **Optional:** Select a proper directory on your computer to install the Control Client.
3. Click **Install Now** to begin the installation.

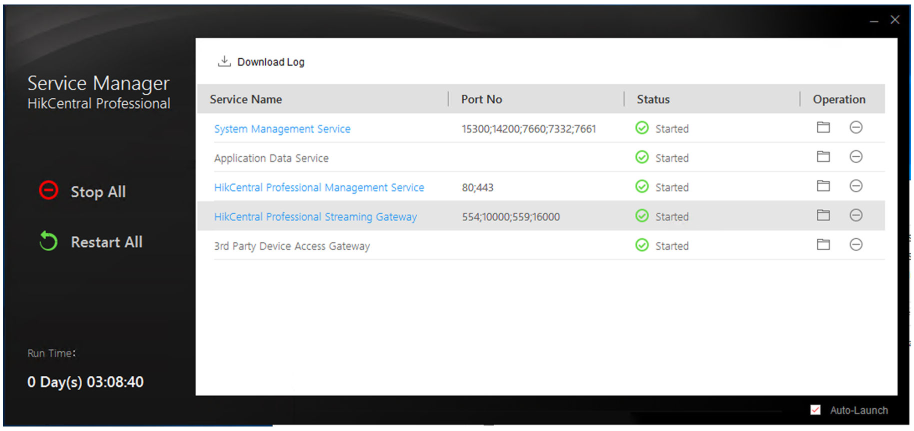
   A panel indicating progress of the installation will display.
4. Click **Finish** to complete the installation.

5.3 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 5-2 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.

Chapter 6 Log into the Web Client

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

6.1 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.

6.2 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.

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

⚠ **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.

Chapter 7 Manage License

After you install 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 system to access more functions and manage more devices. If you do not want to activate the system now, you can skip this chapter and perform this operation later.

Two types of License are available for HikCentral Professional:

- **Base:** You need to purchase at least one basic License to activate 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 the hardware server to be activated has been activated before, please make sure the network card used for previous activation is still in use. Otherwise, the activation may fail.
- If you encounter any problems during activation, update, and deactivation, please send the server logs to Hikvision's technical support engineers.
- For other License operation, refer to *User Manual of HikCentral Professional Web Client*.

7.1 Activate License - Online

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

Steps

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

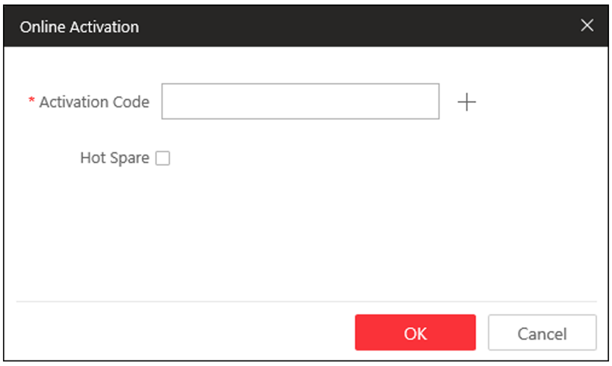


Figure 7-1 Online Activation

3. Enter the activation code.

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.

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.

7.2 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.
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.

Chapter 8 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, 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.

This section only addresses the addition of device via an IP address or domain name. For other methods, please refer to the *User Manual of HikCentral Professional Web Client*.

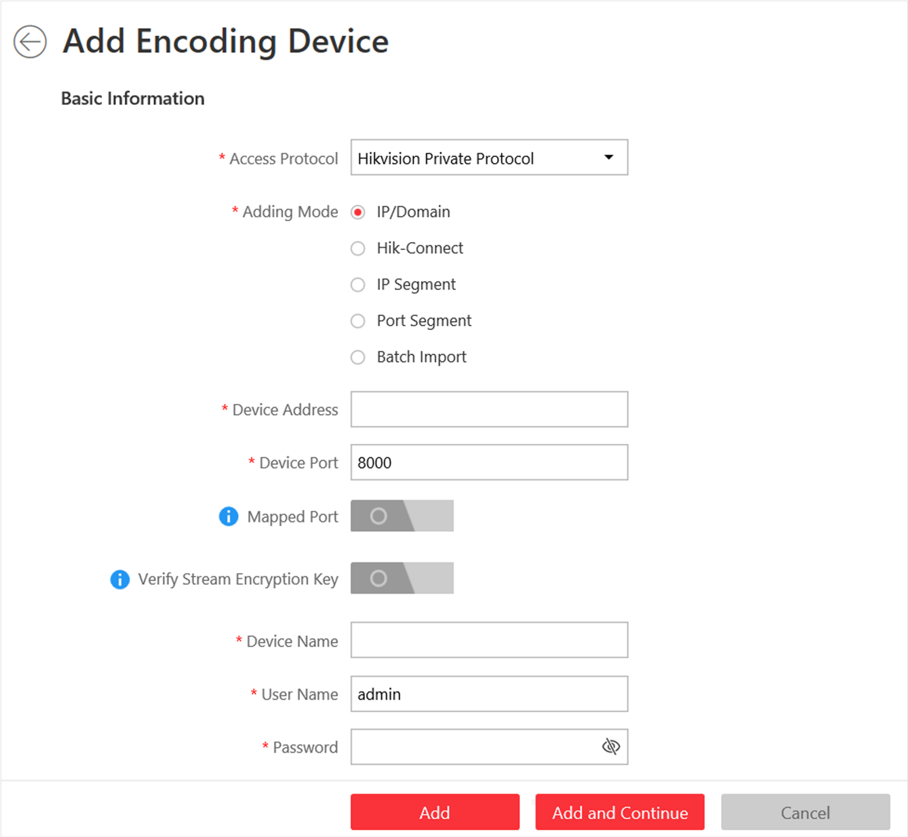
8.1 Add Encoding Device by IP Address or Domain Name

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: off

Verify Stream Encryption Key: off

* Device Name:

* User Name: admin

* Password:

Figure 8-1 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, 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.

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.
10. 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.

What to do next

For facial recognition camera/ANPR camera, 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 and plate recognition) cannot be performed normally in the system.

8.2 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.

8.3 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.

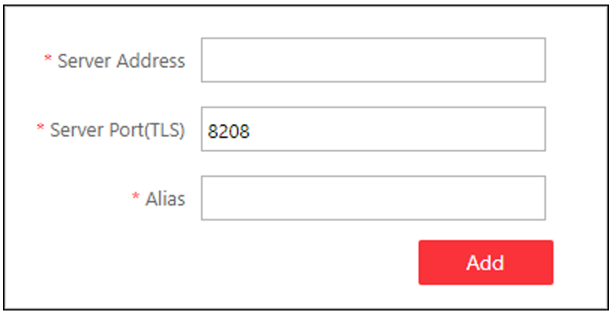
How to add an Application Data Server?

Before adding the Application Data Server, generate the security certificate on the Web Client running on the SYS server, 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 8-2 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.

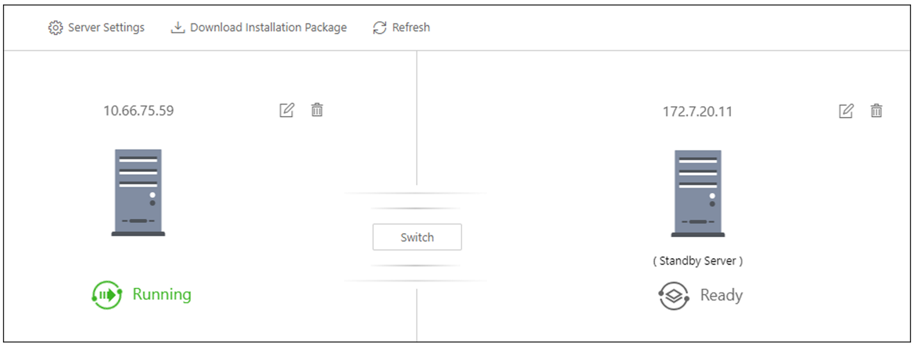


Figure 8-3 Application Data Server Management

ℹ **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

ℹ **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

ℹ **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.

8.4 Manage Area

The system provides areas to manage the added resources in different groups. You can group the resources into different areas according to the resources' locations.

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.

8.4.1 Add an Area

You can add an area to manage the resources of the added 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.
3. Click + on the area list panel to open the Add Area window.

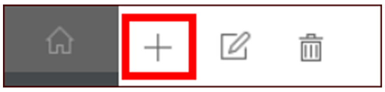


Figure 8-4 Adding Area Icon

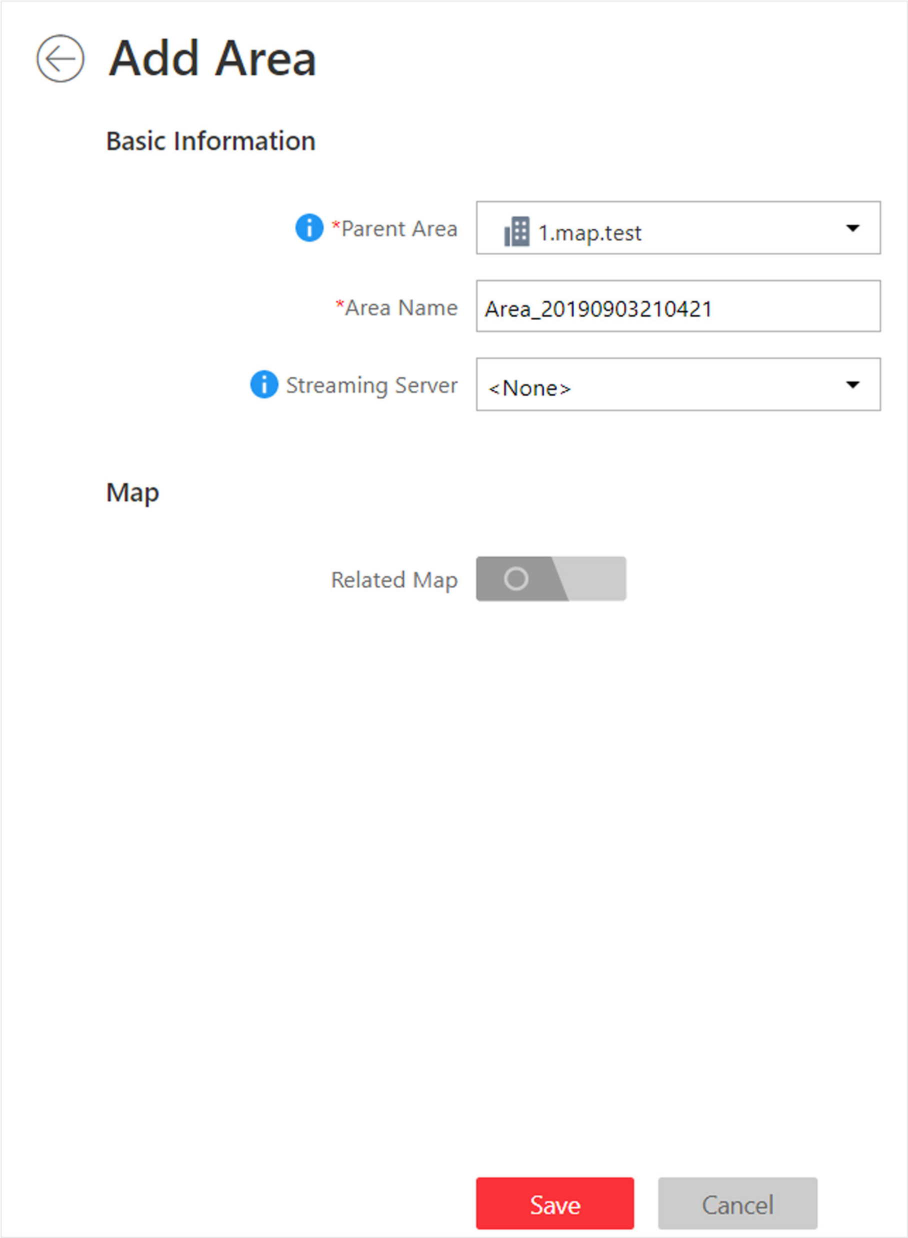


Figure 8-5 Add an Area

4. Select the parent area to add a sub area.
5. Create a name for the area.
6. Click **Save**.

8.4.2 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.

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.
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. Click **Add**.

8.4.3 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. Click **Add**.

Chapter 9 Configure Event and Alarm

You can set the linkage actions for the detected events and alarms. The information of the alarms can be received by the Control Client and the Mobile Client, and you can check the details via the Control Client and the Mobile Client.

System-monitored event is 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.

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.

Note

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.

In this document, we will introduce setting camera alarm as an example. For the settings of other event types (e.g., alarm input, encoding device exception, server alarm), refer to the *User Manual of HikCentral Professional Web Client*.

9.1 About System-Monitored Event

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

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-Monitored Events

Supported Types of System-Monitored 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.

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 and zones of a security control panel.

Vehicle Features

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

Person

The event detected by facial recognition camera or temperature screening cameras, such as face matched event, face mismatched event, rarely appeared event, abnormal skin-surface temperature, no mask event, etc.

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, security control device, dock station, decoding device, and network transmission 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

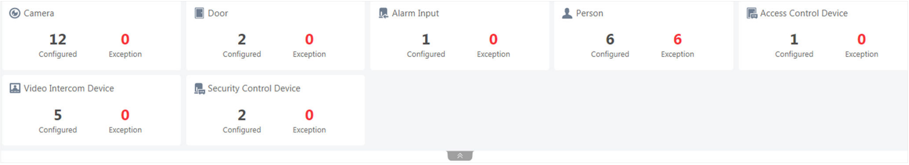
The event triggered by the generic event added in the system.

User-Defined Event

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

Dashboard of Configured Event Rules

On the System-Monitored Event page, HikCentral Professional provides a dashboard, displaying the number of configured system-monitored event rules of each type of event sources as well as the number of abnormal ones.



	Configured	Exception
Camera	12	0
Door	2	0
Alarm Input	1	0
Person	6	6
Access Control Device	1	0
Video Intercom Device	5	0
Security Control Device	2	0

Figure 9-1 Dashboard of System-Monitored Event Rules

You can click the numbers to quickly filter out the existing or exceptional event rules of the corresponding event source types.

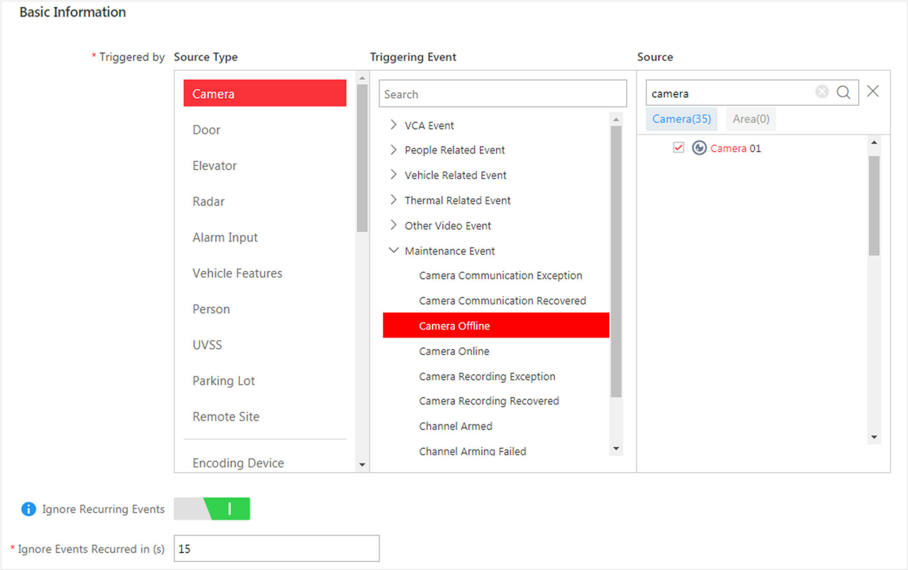
If you do not want to view the dashboard, click ⌃ to fold it.

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".



* Triggered by: Camera; Camera Offline; ☑ Camera 01 (search: camera)

Ignore Recurring Events: on

* Ignore Events Recurred in (s): 15

Figure 9-2 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.

When setting a thermal related event for thermal cameras, you can select areas, points, or lines as event sources.

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.

Card No.

If the source type you selected is **Person** and the triggering event is **Card Number Matched Event**, you need to select cards from the Person List so that when someone presents these cards on the card readers of the event sources, an event will be triggered.

For example, if the card of one resident is stolen, you can set a card number matched event for this card. If someone punches this card on the card readers to gain access, an event will be triggered and you can quickly locate the suspect.

Frequency

If the source type you selected is **Parking Lot** and the triggering event is **Frequently Appeared Vehicle**, you can pre-define the frequency.

For example, if you set the frequency to daily 3 times, when the devices in the source parking lot detect the license plate numbers of the vehicles in the selected vehicle list for more than 3 times in one day, an event will be triggered.

Vehicle Type

If the source type you selected is **Vehicle Features** and the triggering event is **Vehicle Type Matched Event**, you need to specify the vehicle type(s). When the source camera detects a vehicle the type of which matches with the one(s) you selected here, a vehicle type matched event will be triggered.

For example, if oil tank truck is not allowed on one road, you can set a vehicle type matched event for the camera mounted on this road and set the vehicle type as **Oil Tank Truck**. When the camera detects an oil tank truck, an event will be triggered.

Ignore Recurring Events

This function 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 **Ignore Events Recurred in (s)** which is the threshold of the recurring events.

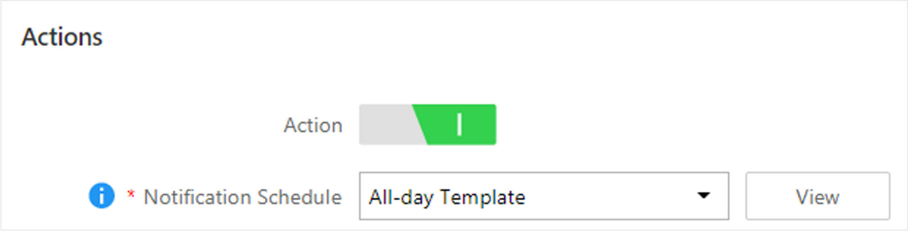
For example, if you set the **Ignore Events Recurred in (s)** to ***30 s***, the events of the same type occurred on the same camera within 30 s will be regarded as one event.

Note

The **Ignore Events Recurred in (s)** 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.


Actions

Action: I

* Notification Schedule: All-day Template

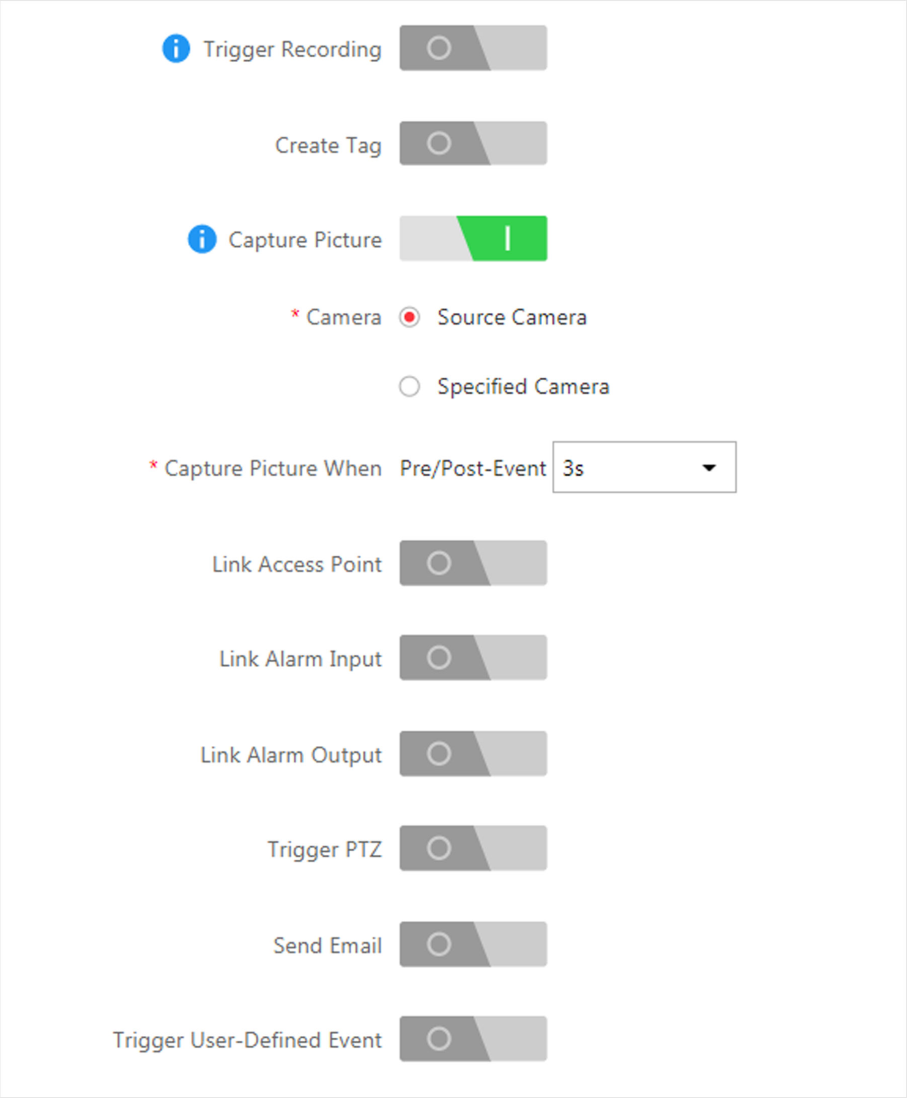
Figure 9-3 When to Trigger Actions

Notification Schedule

In the notification duration in the notification schedule, when the source detects the triggering event, an event will be triggered and link the configured linkage actions.

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: I

* Camera: ● Source Camera ○ Specified Camera

* Capture Picture When: Pre/Post-Event 3s

Link Access Point: ○

Link Alarm Input: ○

Link Alarm Output: ○

Trigger PTZ: ○

Send Email: ○

Trigger User-Defined Event: ○

Figure 9-4 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 locking or unlocking access point, 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 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 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 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 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).

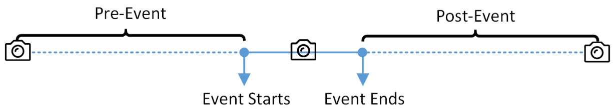


Figure 9-5 Capture Pictures

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 stores the video in the Recording Server (Cloud Storage Server, Hybrid SAN, or pStor).

Link Access Point

You can enable this function to trigger the doors.

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

For example, you can trigger all the doors remaining locked when intrusion of a suspicious person is detected.

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

Link Alarm Input

Select alarm inputs and these alarm inputs will be armed or disarmed when the event occurs.

For example, when adding an intrusion alarm of camera A, which is mounted at the entrance of the building, you can link the alarm input B, C, and D to arm them, which are PIR detectors mounted in different rooms in the building and are disarmed usually. When camera A detects intrusion alarm, these PIR detectors will be armed and trigger other events or alarms (if rules configured) when they detect new motions, so that the security personnel will get to known where the suspect goes.

Link Alarm Output

Select alarm output (if available) and the external device connected can be activated when the 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 time period(unit: s) after which the alarm output(s) will be closed automatically.

When the source you selected for this event rule is resource group, the alarm output can also be closed automatically when the amount of people stayed is less than the threshold you configured here.

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.

Send Email

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

Attach with Entry & Exit Counting

If the source type you selected is **Alarm Input**, you can select an entry & exit counting group from the drop-down list to attach a report of entry & exit counting in the sent email.

For example, if the fire alarm input detects fire in the building, the security personnel will receive a file, which contains the information such as the number of people still in the building, their names and profiles, phone numbers, and locations of last access.

Link Printer

If the source type you selected is **Alarm Input**, you can link to print the entry & exit counting report of certain entry & exit counting group.

For example, if the fire alarm input detects fire in the building, the platform will automatically send the entry & exit counting report to all the printers configured in the system so that they can get the information such as the number of people stuck 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.

Note

Up to 16 user-defined events can be selected as event linkage.

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.
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 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.

9.2.1 Supported Alarm

Supported Types of Alarms

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.

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, such as a smoke detector and zones of a security control panel.

Vehicle Features

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

Person

The alarm triggered by facial recognition camera or temperature screening cameras, such as face matched event, face mismatched event, rarely appeared event, abnormal skin-surface temperature, no mask event, etc.

UVSS

The alarm triggered by the UVSS device, including device getting online and offline.

Parking Lot

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

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, security control device, dock station, decoding device, and network transmission 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

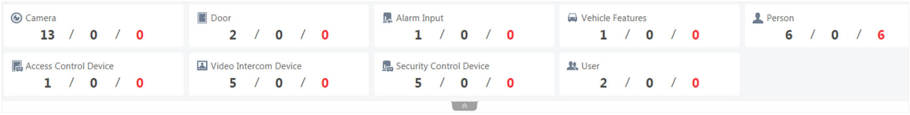
The alarm triggered by the configured user-defined event.

Generic Event

The alarm triggered by the configured generic event.

Dashboard of Configured Alarm Rules

On the Alarm page, HikCentral Professional provides a dashboard, displaying the number of configured alarm rules of each type of event sources, the number of disabled rules, as well as the number of abnormal ones.



Camera 13 / 0 / 0

Door 2 / 0 / 0

Alarm Input 1 / 0 / 0

Vehicle Features 1 / 0 / 0

Person 6 / 0 / 6

Access Control Device 1 / 0 / 0

Video Intercom Device 5 / 0 / 0

Security Control Device 5 / 0 / 0

User 2 / 0 / 0

Figure 9-6 Dashboard of Alarm Rules

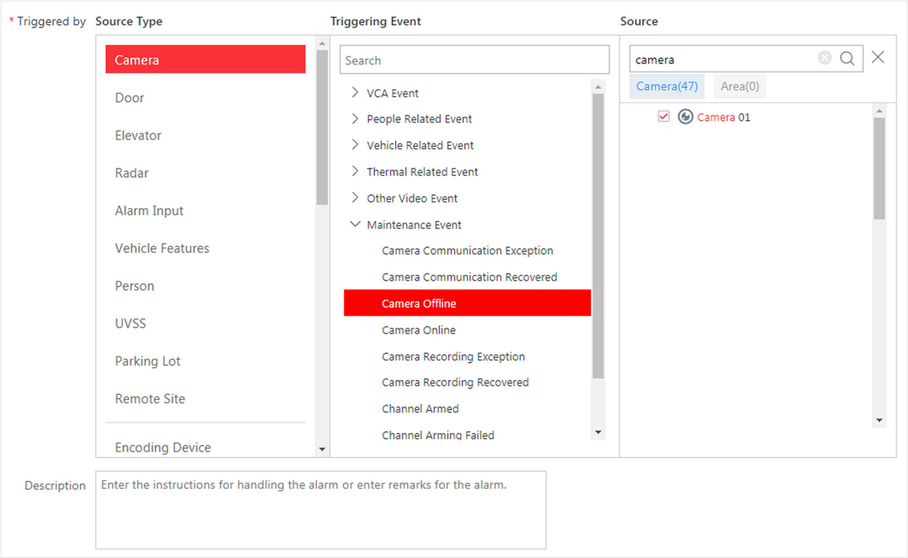
You can click the numbers to quickly filter out the existing, disabled, or exceptional alarm rules of the corresponding event source types.
If you do not want to view the dashboard, click ︽ to fold it.

9.2.2 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".



* Triggered by

Source Type

- Camera
- Door
- Elevator
- Radar
- Alarm Input
- Vehicle Features
- Person
- UVSS
- Parking Lot
- Remote Site
- Encoding Device

Triggering Event

Search

- VCA Event
- People Related Event
- Vehicle Related Event
- Thermal Related Event
- Other Video Event
- Maintenance Event
  - Camera Communication Exception
  - Camera Communication Recovered
  - Camera Offline
  - Camera Online
  - Camera Recording Exception
  - Camera Recording Recovered
  - Channel Armed
  - Channel Arming Failed

Source

camera

Camera(47) Area(0)

☑ Camera 01

Description

Enter the instructions for handling the alarm or enter remarks for the alarm.

Figure 9-7 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.

When setting a thermal related alarm for thermal cameras, you can select areas, points, or lines as alarm sources.

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.

Card No.

If the source type you selected is **Person** and the triggering event is **Card Number Matched Event**, you need to select cards from the Person List so that when someone presents these cards on the card readers of the alarm sources, an alarm will be triggered.

For example, if the card of one resident is stolen, you can set a card number matched alarm for this card. If someone punches this card on the card readers to gain access, an alarm will be triggered and you can quickly locate the suspect.

Frequency

If the source type you selected is **Parking Lot** and the triggering event is **Frequently Appeared Vehicle**, you can pre-define the frequency.

For example, if you set the frequency to daily 3 times, when the devices in the source parking lot detect the license plate numbers of the vehicles in the selected vehicle list for more than 3 times in one day, an alarm will be triggered.

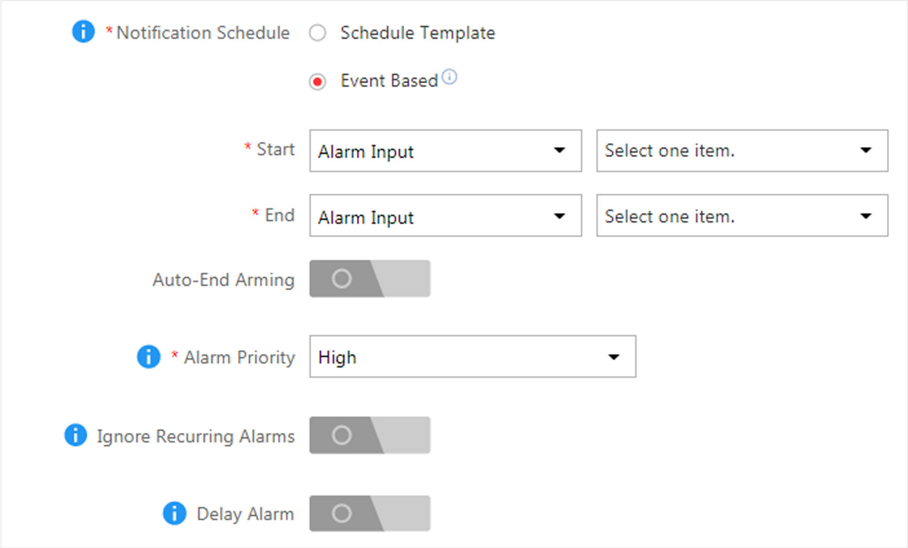
Vehicle Type

If the source type you selected is **Vehicle Features** and the triggering event is **Vehicle Type Matched Event**, you need to specify the vehicle type(s). When the source camera detects a vehicle the type of which matches with the one(s) you selected here, a vehicle type matched alarm will be triggered.

For example, if oil tank truck is not allowed on one road, you can set a vehicle type matched alarm for the camera mounted on this road and set the vehicle type as **Oil Tank Truck**. When the camera detects an oil tank truck, an alarm will be triggered.

When

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



*Notification Schedule ○ Schedule Template
● Event Based

* Start: Alarm Input | Select one item.

* End: Alarm Input | Select one item.

Auto-End Arming

* Alarm Priority: High

Ignore Recurring Alarms

Delay Alarm

Figure 9-8 When Alarm Can be Triggered

Notification Schedule

The alarm source is armed during the notification schedule and when the source detects the triggering event, an alarm will be triggered and link the configured linkage actions. The system provides two types of notification schedule:

- **Schedule Template:** Select a notification schedule template for the alarm to define when the alarm can be triggered.
- **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, assume that you have set event A as the start event, event B as the end event, and set the value of **Auto-End Arming in** to ***60 s***. Under these peconditions, when event A occurs at T1, if event B occurs within 60 s, the arming schedule ends at the occurrence of event B (see the following figure Arming Schedule 1); if not, ends at 60 s after the occurrence of event A (see the following figure Arming Schedule 2).

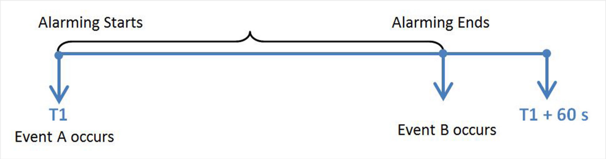


Figure 9-9 Notification Schedule 1

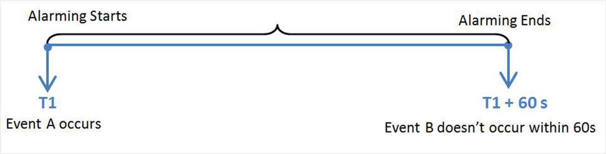


Figure 9-10 Notification Schedule 2

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.

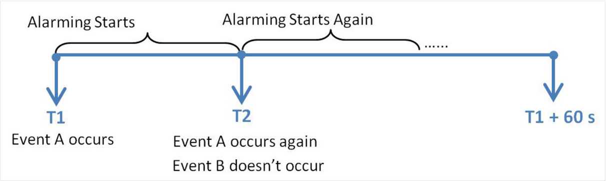


Figure 9-11 Notification Schedule 3

Ignore Recurring Alarms

This function is used to avoid the same alarm occurs frequently in a short time. You need to set the **Ignore Alarms Recurred in (s)** which is the threshold of the recurring alarms.

For example, if you set **Ignore Alarms Recurred in (s)** to ***30 s***, the alarms of the same type occurred on the same camera within 30 s will be regarded as one alarms.

Note

The **Ignore Alarms Recurred in (s)** is 15 s by default. You can set it from 15 s to 1800 s.

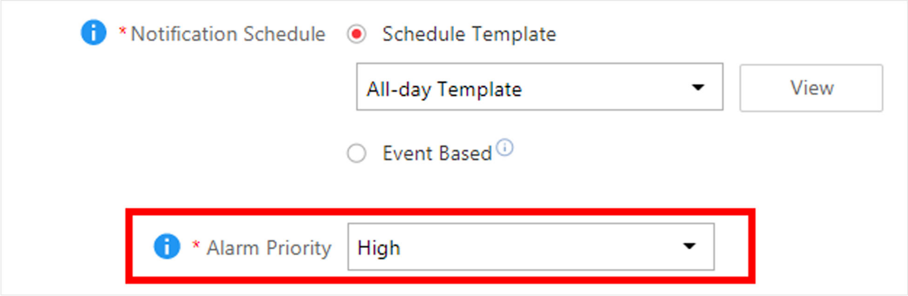
Delay Alarm

If the source type you selected is **Camera** and the triggering event is **Camera Offline**, you can enable this function and set a delay duration. During the delay duration, when the source detects the triggering event, the triggering event will not be uploaded to the system. After this duration, if the source still detects this triggering event, the triggering event will be uploaded to the system and trigger an alarm.

With this function, when the system detects that the camera is offline, if the camera gets online again within the delay duration, it will not trigger a camera offline alarm. Thus the maintainers can focus on the cameras which are truly disconnected.

Priority

The field in the following image indicates one element in the rule: "recipient".



* Notification Schedule ● Schedule Template

All-day Template ▾ View

○ Event Based

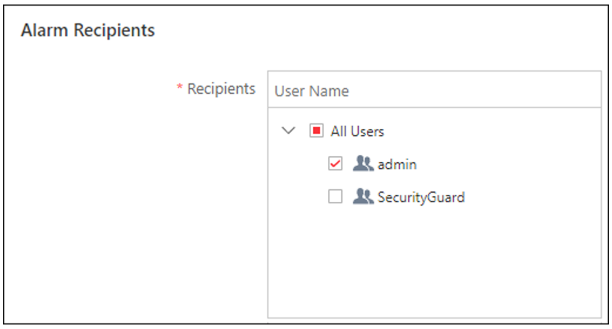
* Alarm Priority High ▾

Figure 9-12 Alarm Priority

It defines the priority for the alarm. Priority can be used for filtering alarms in the Control Client.

Recipient

The field in the following image indicates one element in the rule: "recipient". It defines when the alarm is triggered, which users can receive the alarm notification and check the alarm details.



Alarm Recipients

* Recipients User Name

■ All Users

☑ admin

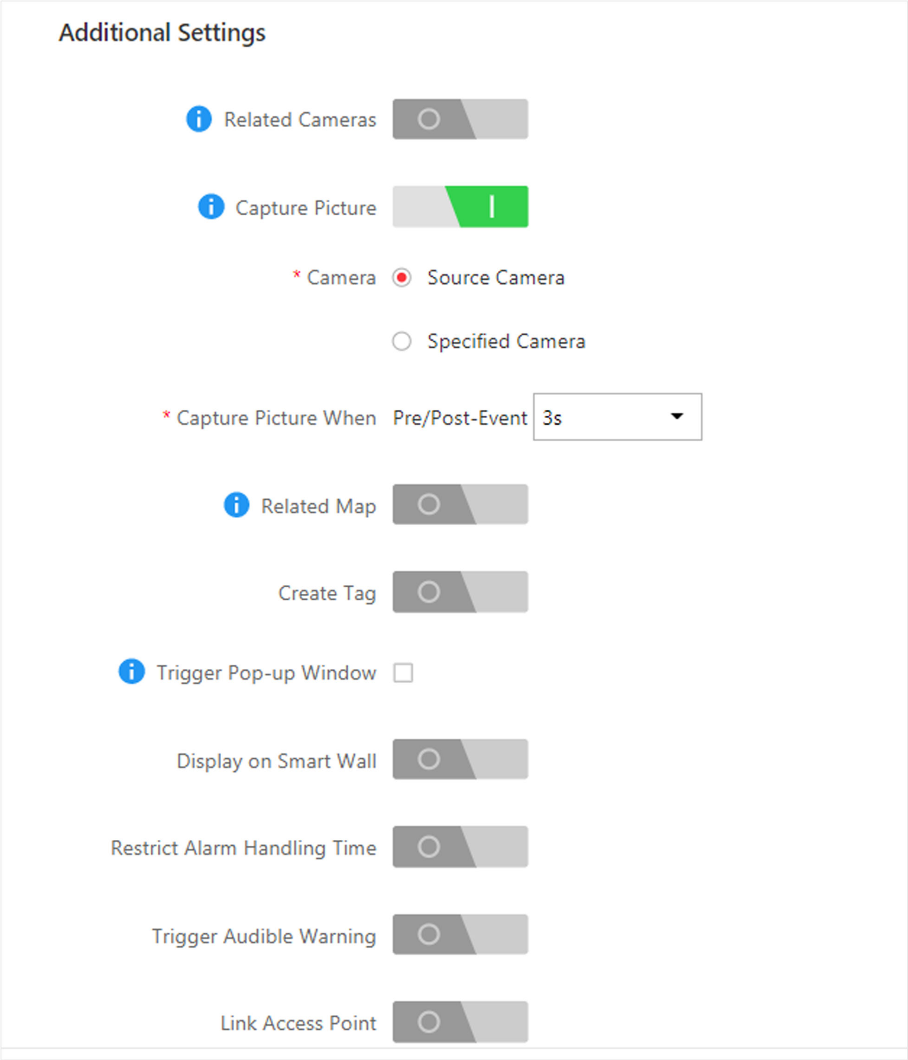
□ SecurityGuard

Figure 9-13 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 Additional Settings indicate one element in the rule: "what to do". It defines what actions the system will take to record the alarm details and notify security personnel.



Additional Settings

Related Cameras

Capture Picture

* Camera ● Source Camera

○ Specified Camera

* Capture Picture When Pre/Post-Event 3s

Related Map

Create Tag

Trigger Pop-up Window □

Display on Smart Wall

Restrict Alarm Handling Time

Trigger Audible Warning

Link Access Point

Figure 9-14 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 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).

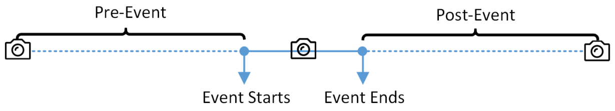


Figure 9-15 Capture Pictures

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 stores 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. You can check the map in the Alarm Center and Alarm & Event Search of the Control Client.

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 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 record the tagged video started from 5 seconds before the event and lasted until 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.

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.

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.

Link Access Point

You can enable this function to trigger the doors.

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

For example, you can trigger all the doors remaining locked when intrusion of a suspicious person is detected.

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

Link Alarm Input

Select alarm inputs and these alarm inputs will be armed or disarmed when the alarm occurs.

For example, when adding an intrusion alarm of camera A, which is mounted at the entrance of the building, you can link the alarm input B, C, and D to arm them, which are PIR detectors mounted in different rooms in the building and are disarmed usually. When camera A detects intrusion alarm, these PIR detectors will be armed and trigger other events or alarms (if rules configured) when they detect new motions, so that the security personnel will get to known where the suspect goes.

Link Alarm Output

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

Note

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

Close Alarm Output: The added alarm output(s) can be closed manually, or you can set the time period(unit: s) after which the alarm output(s) will be closed automatically.

When the source you selected for this alarm rule is resource group, the alarm output can also be closed automatically when the amount of people stayed is less than the threshold you configured here.

Trigger PTZ

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

Note

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

Send Email

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

Attach with Entry & Exit Counting

If the source type you selected is **Alarm Input**, you can select an entry & exit counting group from the drop-down list to attach a report of entry & exit counting in the sent email.

For example, if the fire alarm input detects fire in the building, the security personnel will receive a file, which contains the information such as the number of people still in the building, their names and profiles, phone numbers, and locations of last access.

Link Printer

If the source type you selected is **Alarm Input**, you can link to print the entry & exit counting report of certain entry & exit counting group.

For example, if the fire alarm input detects fire in the building, the platform will automatically send the entry & exit counting report to all the printers configured in the system so that they can get the information such as the number of people stuck in the building, their names and profiles, phone numbers, and locations of last access.

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.

Note

Up to 16 user-defined events can be selected as alarm linkage.

Chapter 10 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), etc. After adding the persons, you can edit and delete the person information if needed.

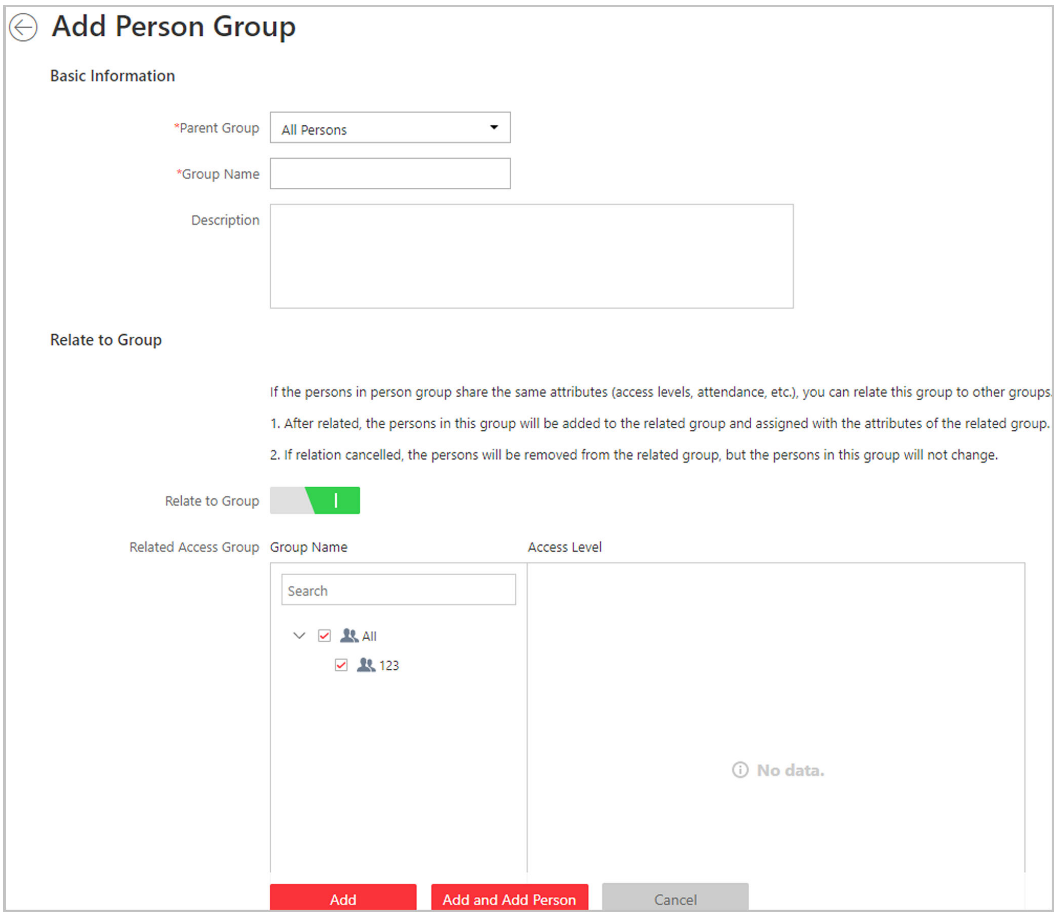
10.1 Add Person Group

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.



Add Person Group

Basic Information

*Parent Group: All Persons

*Group Name

Description

Relate to Group

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.

Relate to Group: on

Related Access Group

Group Name	Access Level
Search ☑ All ☑ 123	No data.

Figure 10-1 Add Person Group Page

4. **Optional:** If the persons in the person group share the same attributes (access levels, 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, so that the persons will be automatically assigned with attributes of the related access 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

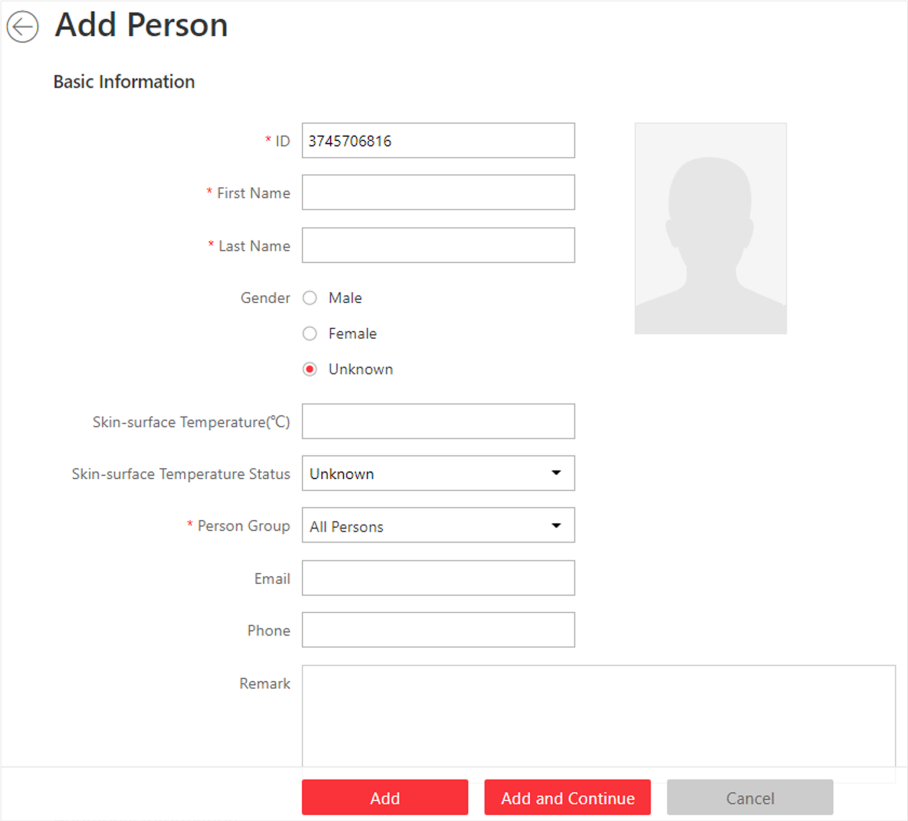
You cannot relate a person group to an access group which contains singly-added persons.

10.2 Add a Person

You can add a person to the system by entering her/his information and set more configurations for the person.

Steps

1. Click **Person → Person List** .
2. Click **Add** to enter the adding person page.



Add Person

Basic Information

* ID	3745706816
* First Name	
* Last Name	
Gender	○ Male ○ Female ● Unknown
Skin-surface Temperature(℃)	
Skin-surface Temperature Status	Unknown
* Person Group	All Persons
Email	
Phone	
Remark	

Figure 10-2 Add a Person

3. Set basic information for the person.

   ID

   The default ID is generated by the system. You can edit it if needed.

   Note

   If the person is a police officer or a security guard with body cameras, make sure the person ID is same as the police ID configured on the body camera.

   Person Picture

   Hover the cursor on the person picture field, and you can select from three modes to add a picture:

From Device

Select **Access Control Device**, **Video Intercom Device**, or **Enrollment Station** to collect the face picture. This mode is suitable for non-face-to-face scenario when the person and the system administrator are in different locations.

Note

- For access control devices, only face recognition terminals (including DS-K5671, DS-K1T671, DS-K1T331, DS-K1T341, DS-K1T672, DS-K1T642, etc.) are supported.
- For video intercom devices, door stations and outer door stations are supported.
- For enrollment stations, you need to set related parameters, including device address, port, user name, password, face anti-spoofing, and security level.

Take a Picture

Click **Take a Picture** and select one of the PC's webcam(s) to take a picture.

Upload Picture

Click **Upload Picture** to select a picture in your PC.

Note

- It is recommended that the face in the picture should be in full-face view directly facing the camera, without a hat or head covering.
- You can drag the picture to change its position or zoom in/out before cutting it.
- You can set **Verify Profile Quality** switch to on and select a device to check profile quality. Click **Save** to start checking. You will be informed if the picture is not qualified, while the cut picture will be put in the profile position if it is qualified.

4. **Optional:** Enter the person's skin-surface temperature and select the corresponding temperature status.

   Example

   For example, if a person's skin-surface temperature is 37℃, then you can select her/his temperature status as normal.
5. Select a person group for the person.
6. **Optional:** Set the person's additional information.
7. **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.
8. **Optional:** Set the access control information.

   Effective Period

Set the effective period for the person in access control application. For example, if the person is a visitor, his/her effective period may be short and temporary.

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.

Super User

If the person is set as a super user, he/she will be exempted from remaining locked (credential failed) restrictions, all anti-passback rules, and first card authorization.

Extended Access

When the person accesses the door, grant this person more time to pass through doors which have been configured with extended open duration. Use this function for the persons with reduced mobility.

Note

You should set the door's extended open duration in Logical View.

Note

The extended access and super user functions cannot be enabled concurrently.

9. 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.

123456789

Figure 10-3 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 when 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 or a video intercom 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 or a video intercom device from the managed device list.

Click **+**, place and lift your fingerprint on the selected fingerprint and card reader following the prompts and it will collect your fingerprint automatically.

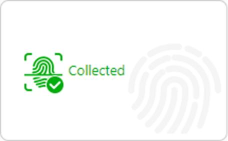


Figure 10-4 Fingerprint Recorded

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.

10. **Optional:** Add the person to the existing dock station group(s) and set the login password which is used for the dock station(s) in the group to log into the body cameras.

Note

By default, the login password is 123456.

The videos and pictures stored on the person's body camera can be copied to the person's linked dock station(s).

11. 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.

12. 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.

Chapter 11 Manage Access Control

The system supports access control function. Access control is a security technique that can be used to regulate who can get access to the specified doors.

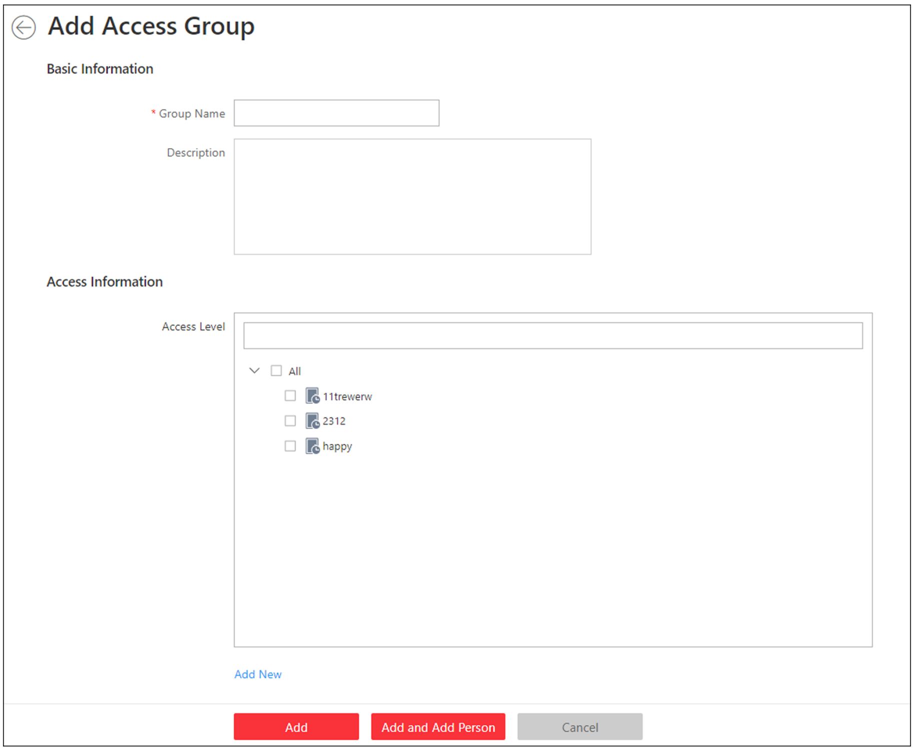
On the Web Client, the administrator can add access control devices to the system, group resources (such as doors) into different areas, and define access permissions by creating an access level to group the doors and an access group to group the persons. After assigning the access level to the access group, the persons in the access group will be authorized to access the doors in the access level with their credentials during the authorized time period.

11.1 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 (the doors 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 in the access level.

Steps

1. Click **Person → Access Group → Add** to enter the adding access group page.



Add Access Group

Basic Information

* Group Name

Description

Access Information

Access Level

☐ All

☐ 11trewerw

☐ 2312

☐ happy

Figure 11-1 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 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 access schedule.
- Up to 8 access levels can be assigned to one access group.

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.

Access Group

Add all the persons in the selected access group(s) to this access group.

7. Click **Add** to add the selected persons to the access group.

11.2 Manage Access Level

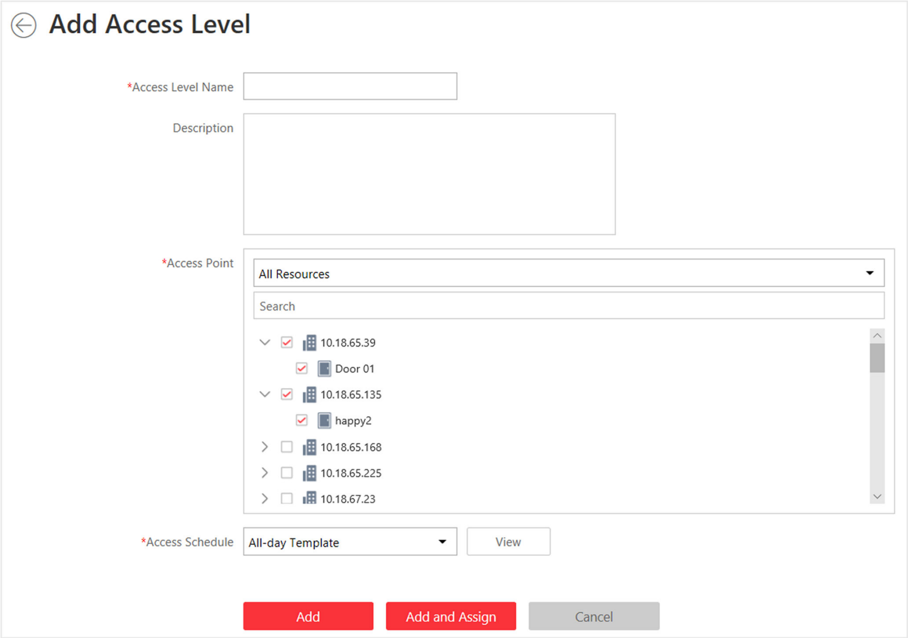
In access control, access level is a group of doors. After assigning the access level to certain access groups, it defines the access permission that which persons can get access to which doors during the authorized time period.

11.2.1 Add Access Level

To define the access permission, you need to add an access level first and group the doors.

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

- ☑ 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 11-2 Add Access Level

3. Create a name for the access level.

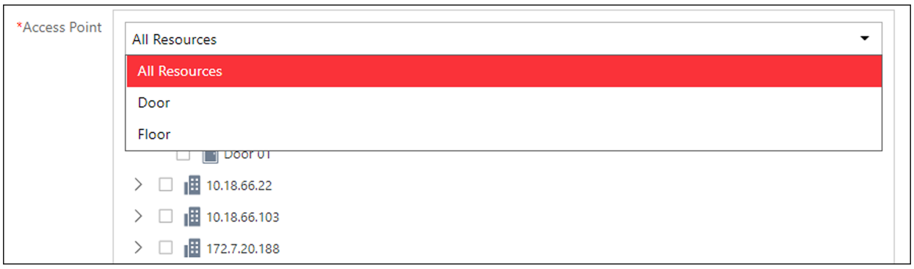
4. **Optional:** Enter the description for the access level.
5. Select the access point(s) to add to the access level.
   1) Select the type of access points from the drop-down list.

      All Resources

      Both doors managed in the system will be display.

      Door

      Only doors will be displayed. The doors will be displayed by area.



*Access Point: All Resources

Figure 11-3 Select Access Point Type

   2) Select the doors.
6. Select the access schedule to define in which time period, the persons are authorized to access the doors (selected in step 5).
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 so that the persons in the access groups will have the access permission to access the doors selected in step 5.

11.2.2 Assign Access Level to Access Group

After adding the access level, you need to assign it to access group(s). After that, the persons in the access group(s) will have the permission to access the 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) so that the persons in the access groups will have the access permission to access the doors in the access level.
4. **Optional:** Click **Add New** to add a new access group.
5. Click **Save**.

Chapter 12 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.

12.1 Add Role

You can assign 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. The two default roles cannot be edited or deleted.

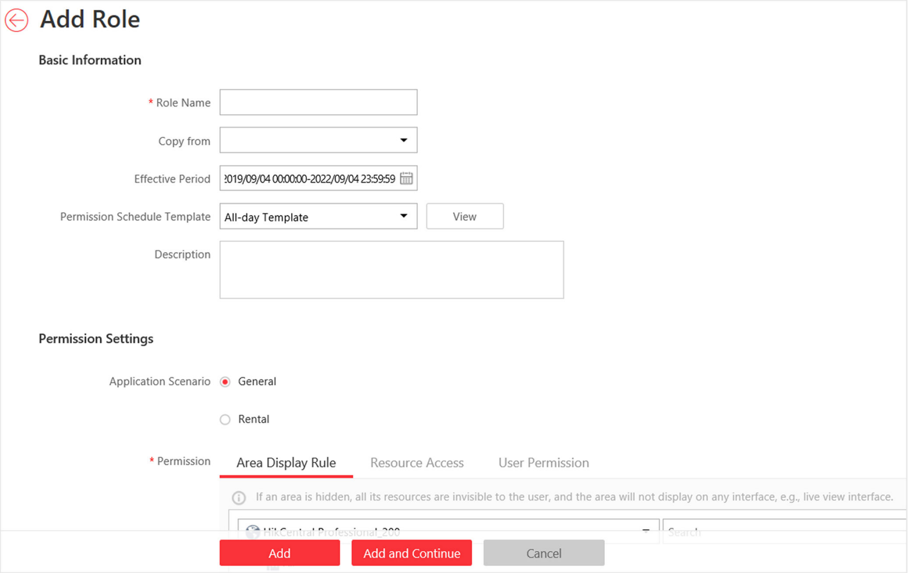
   Administrator

   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: 2019/09/04 00:00:00-2022/09/04 23:59:59

Permission Schedule Template: All-day Template

Description

Permission Settings

Application Scenario: ● General ○ Rental

* Permission: Area Display Rule | Resource Access | User Permission

If an area is hidden, all its resources are invisible to the user, and the area will not display on any interface, e.g., live view interface.

HikCentral Professional_200

Figure 12-1 Add Role Page

3. Set the basic information of the role, including role name, effective period, permission schedule template, role status, etc.

Effective Period

The date that this role takes effect.

Permission Schedule Template

Set the authorized time period when the role's permission is valid. Select **All-day Template**/ **Weekday Template**/**Weekend Template** as the permission schedule of the role, or click **Add New** to customize a new permission schedule template for the role.

Note

- The role's permission will expire when the current time is not in the authorized time period of the permission schedule.
- When the permission expires, the role will be logged out and not be allowed to login.
- The permission schedule's time zone is consistent with that of the system.
- If the role's permission is invalid after editing the permission schedule, the role will be forced to exit the system.
- 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.

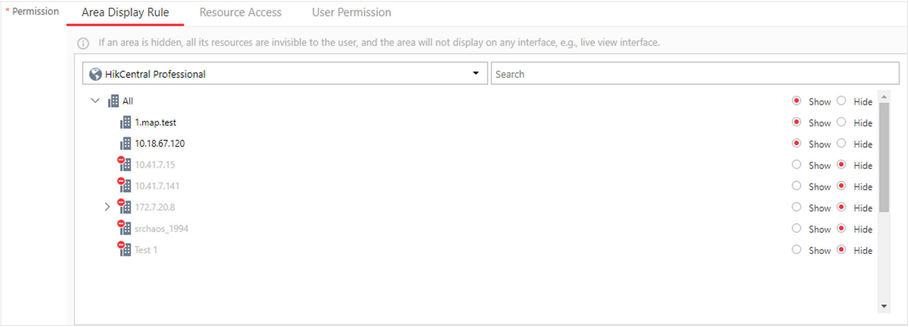
- Select the default or pre-defined role from the **Copy from** drop-down list to copy the permission settings of selected role.
- Select Application Scenario for the role. If you select **General**, you need to assign the permissions to the role; if you select **Rental**, you need to select access groups 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.



If an area is hidden, all its resources are invisible to the user, and the area will not display on any interface, e.g., live view interface.

All	● Show ○ Hide
1.map.test	● Show ○ Hide
10.18.67.120	● Show ○ Hide
10.41.7.15	○ Show ● Hide
10.41.7.141	○ Show ● Hide
172.7.20.8	○ Show ● Hide
srchaos_1994	○ Show ● Hide
Test 1	○ Show ● Hide

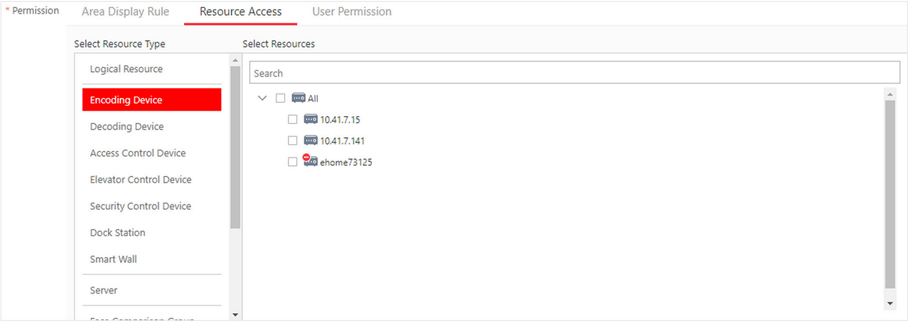
Figure 12-2 Area Display Rule

Resource Access Permission

Select the functions from the left panel and select resources from right panel to assign the selected resources' permission to the role.

Note

If you do not check the resources, the resource permission cannot be applied to the role.



- □ All
  - □ 10.41.7.15
  - □ 10.41.7.141
  - □ ehome73125

Figure 12-3 Resource Access Permission

User Permission

Assign the resource permissions, configuration permissions and operation permissions to the role.

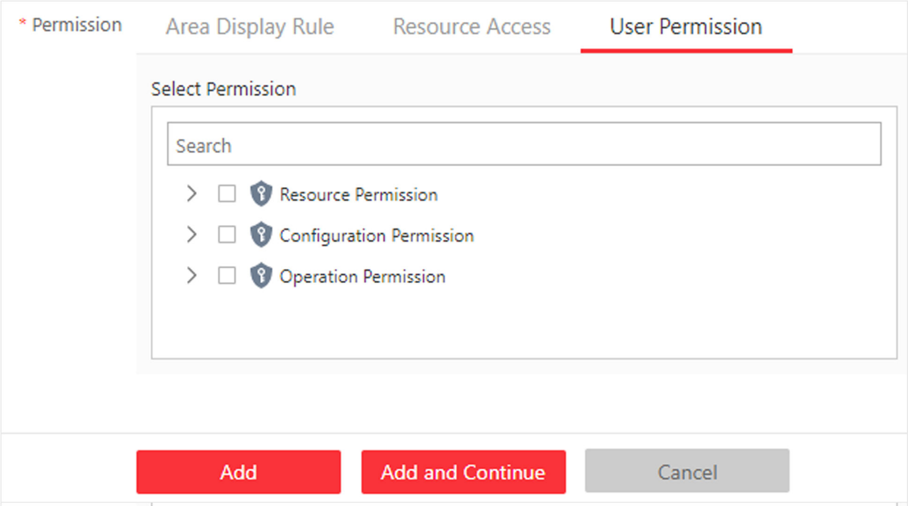


Figure 12-4 User Permission

Note

In **Resource Permission**, you can set time restriction for video playback permission. After that, the role's permission of viewing and downloading video playback will be restricted within the configured time period. For example, if you set restricting for recent video for 6 minutes, the role can only view video playback of the camera that he/she has permission to for 6 the recent minutes.

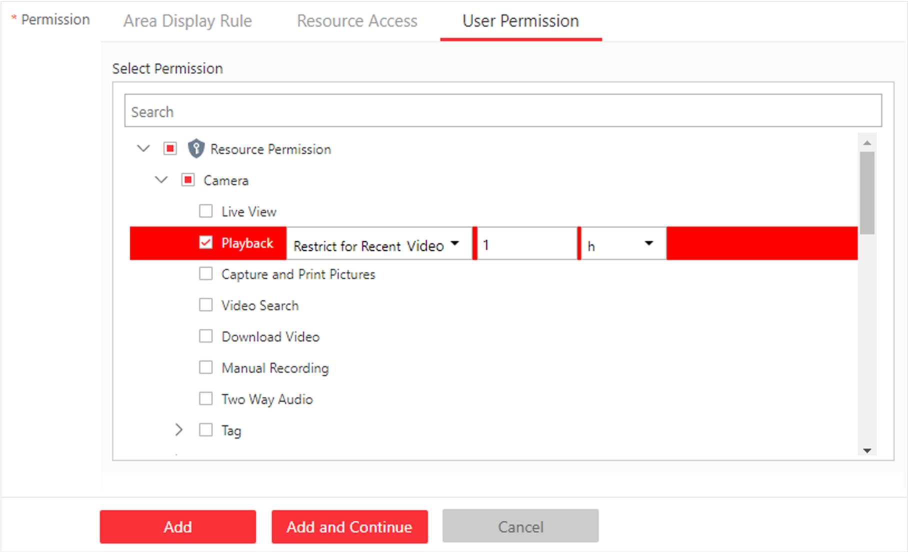


Figure 12-5 Playback Permission

5. Complete adding the role.

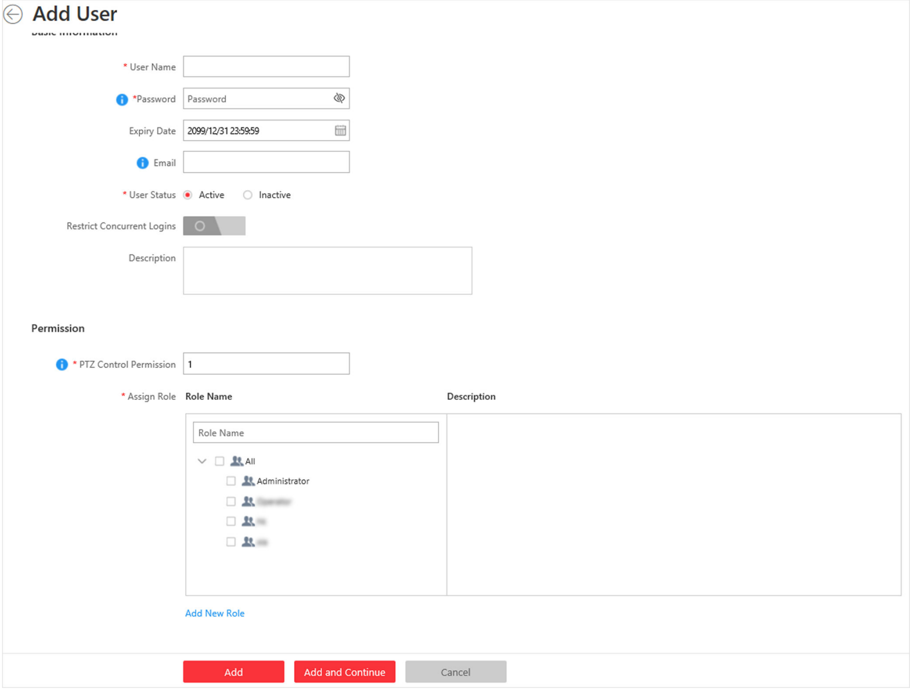
- Click **Add** to add the role.
- Click **Add and Continue** to save the settings and continue to add roles.

12.2 Add Basic User

You can add basic users for accessing the system and assign role to the basic user. Basic 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 23:59:59

Email

* User Status: ● Active ○ Inactive

Restrict Concurrent Logins

Description

Permission

* PTZ Control Permission: 1

* Assign Role

Role Name	Description
Role Name □ All □ Administrator □ □ □	

Figure 12-6 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.
6. Complete adding the user.
   - Click **Add** to add the user.
   - Click **Add and Continue** to save the settings and continue to add users.

See Far, Go Further