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 HikCentral 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:

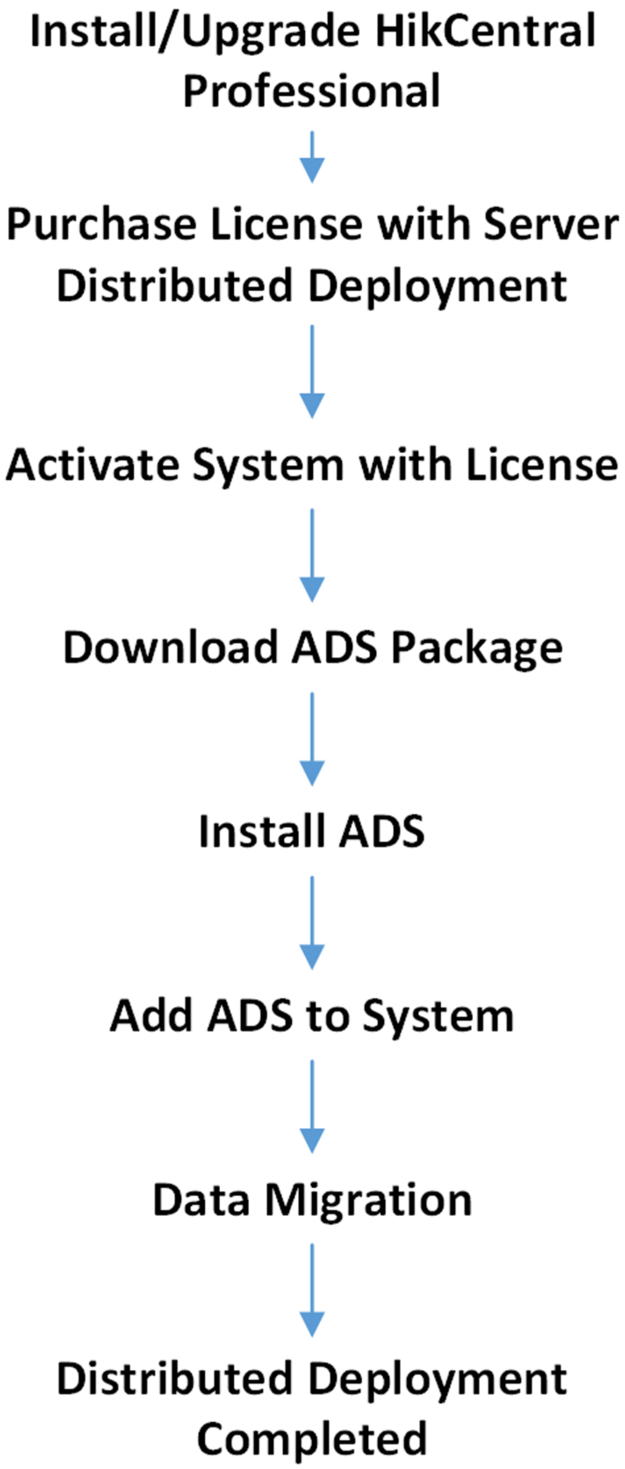

Install/Upgrade HikCentral Professional
Purchase License with Server Distributed Deployment
Activate System with License
Download ADS Package
Install ADS
Add ADS to System
Data Migration
Distributed Deployment Completed

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 HikCentral Professional Service, Streaming Service, and Control Client.

Control Client Installation Package:

Contains the Control Client module only.

Note

The HikCentral Professional 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

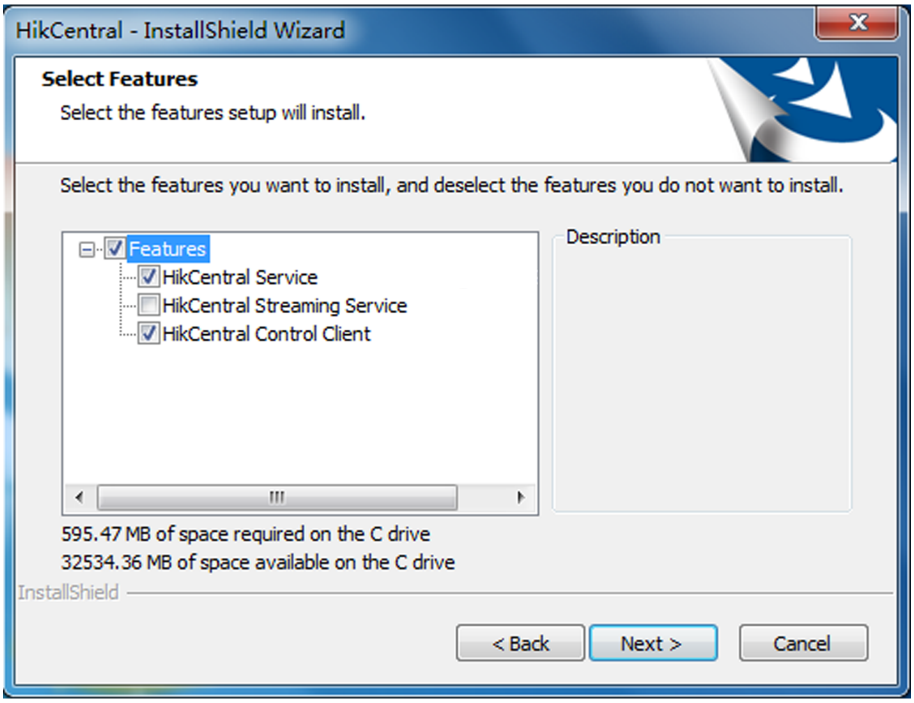
Select the installation directory and modules to be installed as desired.

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



HikCentral - InstallShield Wizard

Select Features

Select the features setup will install.

Select the features you want to install, and deselect the features you do not want to install.

- ☑ Features
  - ☑ HikCentral Service
  - □ HikCentral Streaming Service
  - ☑ HikCentral Control Client

595.47 MB of space required on the C drive

32534.36 MB of space available on the C drive

Figure 5-1 Select Modules to Install

Note

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

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

8. **Optional:** Select the hot spare mode if you select to install HikCentral 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.
   - Select **Shared Storage Hot Spare** to build a shared storage hot spare system. There are two HikCentral servers and one HDD (installed on another server) in the hot spare system: host server, spare server, and the selected HDD. When the host server works, the data is stored in the HDD. When the host server fails, the spare server switches into operation and will take over the HDD to use the same data file.

Note

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

9. Click **Install**.

   A panel indicating progress of the installation will display.

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

Note

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

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 **Next** to start the InstallShield Wizard.
3. Read the License Agreement.
   - Click **I accept the terms of the license agreement** and continue.
   - Click **I do not accept the terms of the license agreement** to cancel the installation.
4. Select **Typical** as setup type and click **Next**.
5. **Optional:** Click **Change...** and select a proper directory as desired to install the module.
6. Click **Next** to continue.
7. **Optional:** Select the hot spare mode.
   - 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 SYS servers in the hot spare system: host server and spare server. When the host server works, the data in host server is copied to the spare server in real time. When the host server fails, the spare server switches into operation without interruption, thus increasing the reliability of the system.
   - Select **Shared Storage Hot Spare** to build a shared storage hot spare system. There are two SYS servers and one HDD (installed on another server) in the hot spare system: host server, spare server, and the selected HDD. When the host server works, the data is stored in the HDD. When the host server fails, the spare server switches into operation and will take over the HDD to use the same data file.

   Note

   For building the hot spare system, contact our technical support engineer.
8. Read the pre-install information, and click **Install** to begin the installation.

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

Note

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

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. Click **Next** to start the InstallShield Wizard.
3. **Optional:** Click **Browse** and select a proper directory on your computer to install the Control Client.
4. Click **Next** to continue.
5. Read the pre-install information and click **Install** to begin the installation.

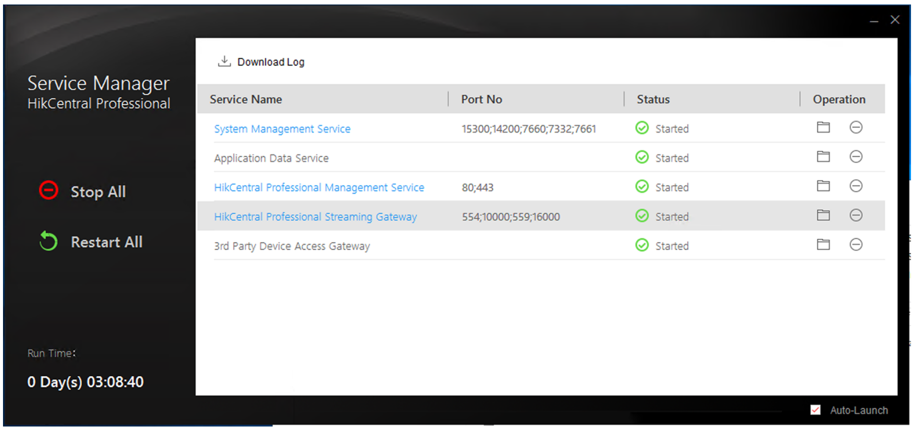
   A panel indicating progress of the installation will display.
6. Read the post-install information and click **Finish** to complete the installation.

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	

Run Time:
0 Day(s) 03:08:40

☑ Auto-Launch

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

Steps

Note

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

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

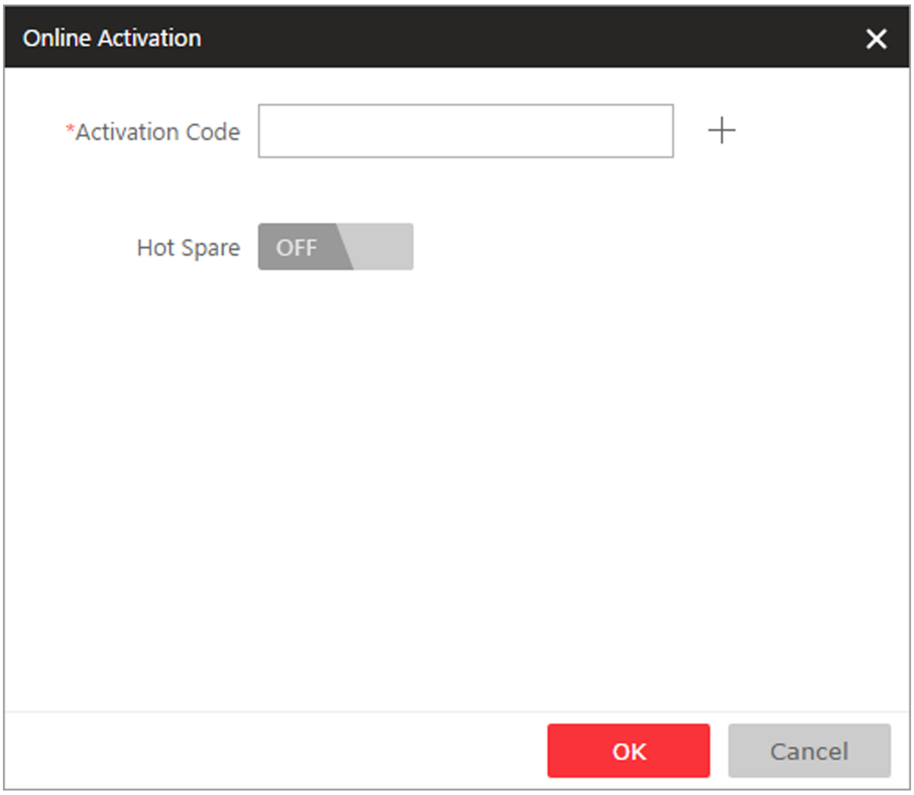


Figure 7-1 License Configuration Window

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

Note

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

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

Note

- You must select Hot Spare mode when you install the system.
- For 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.

Result

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

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 system 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 License, you can click + and enter other activation codes.

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.

Result

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

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, time and attendance management, etc., add Remote Site for central management of multiple systems, add Recording Server for storing the videos, add Streaming Server for getting the video data stream from the server, and add Smart Wall for displaying decoded video on smart wall.

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

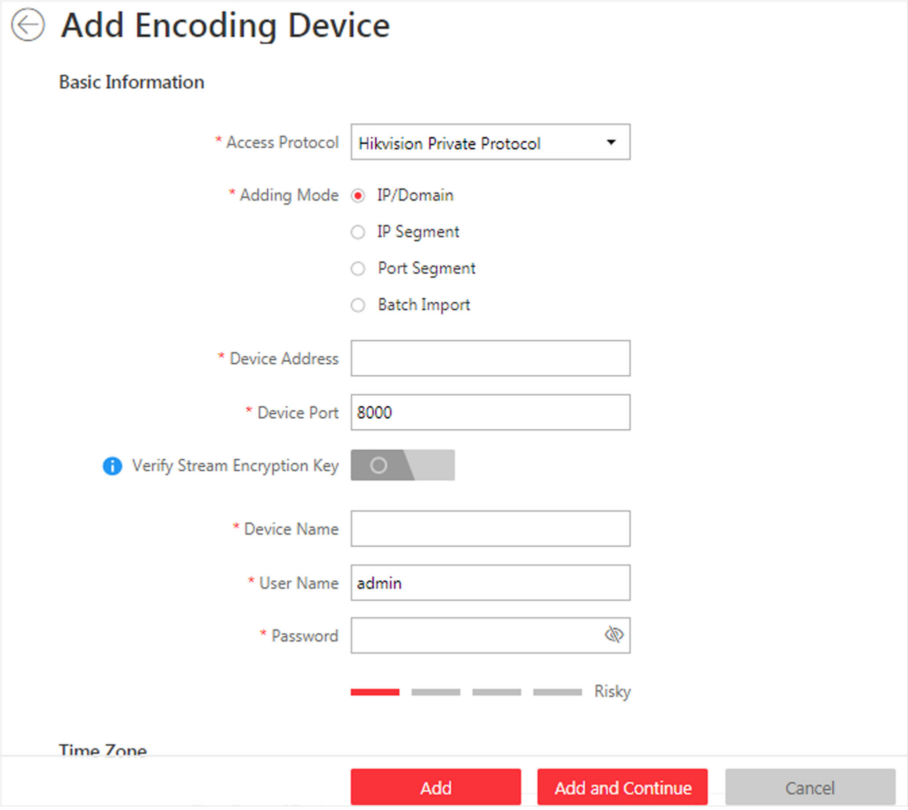
8.1 Add Encoding Device by IP Address or Domain Name

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 ○ IP Segment ○ Port Segment ○ Batch Import

* Device Address:

* Device Port: 8000

Verify Stream Encryption Key: ○

* Device Name:

* User Name: admin

* Password:

Risky

Time Zone

Figure 8-1 Add Encoding Device Page

3. Select **Hikvision Private Protocol/Hikvision EHome Protocol** to add a Hikvision device and 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.

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.

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

What to do next

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

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 VSM server will reboot automatically after changing the clients and VSM server transmission settings.
- All the users logged in will be forced logout during reboot. The reboot takes about one minute and after that, the users can login again.

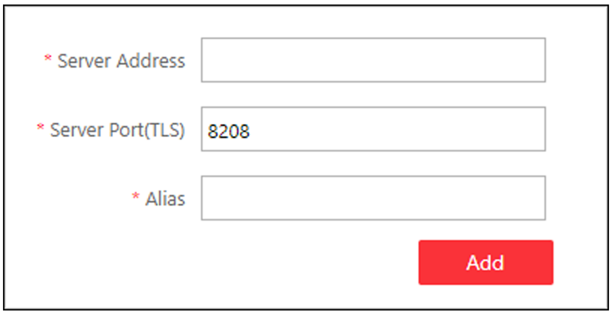
How to add an Application Data Server?

Before adding the Application Data Server, generate the security certificate on the Web Client running on the SYS server (For details, refer to), 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.

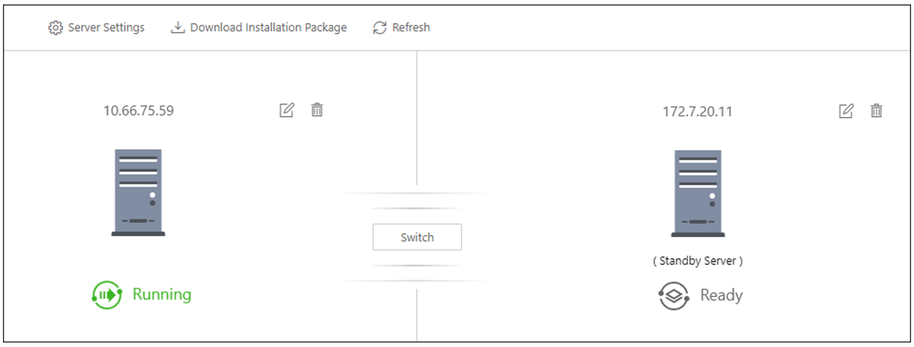


Figure 8-3 Application Data Server Management

Note

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

Set Threshold of Failure Status

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

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

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

Automatically Switch to Application Data Standby Server

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

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

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

Maintain Server Fault

Note

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

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

Manually Switch to Application Data Standby Server

Note

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

If the Application Data Server fails but the system cannot detect its fault, or you need to change the server to a better one, you can manually switch the Application Data Server currently in working status to the Application Data Standby Server which is in ready status.
In Application Data Server page, click **Switch** to switch to the Application Data Standby Server and then the standby server will take over.

Note

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

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.

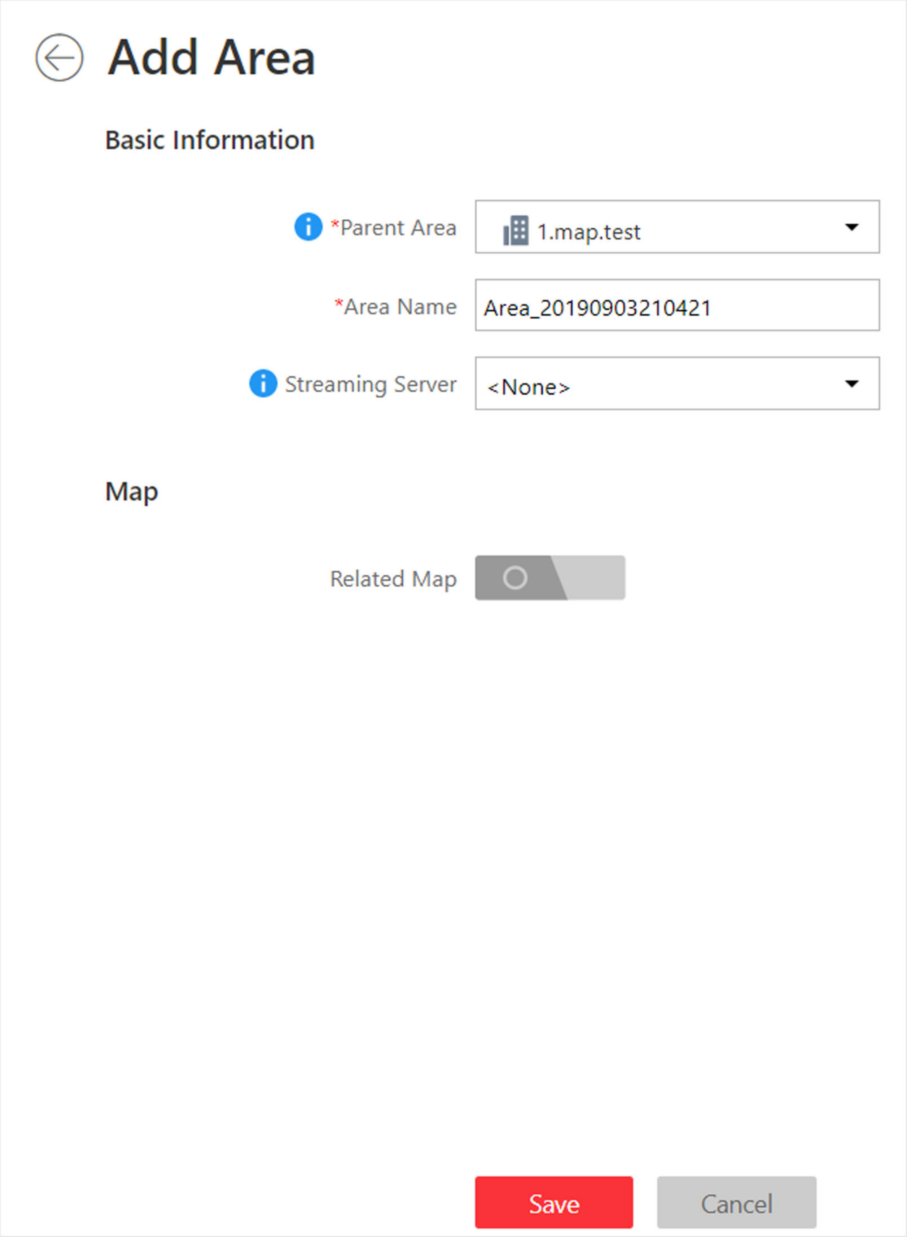
Example
On the 1st floor, there mounted 64 cameras, 16 access points, 64 alarm inputs, and 16 alarm outputs. You can organize these resources into one area (named 1st Floor) for convenient management. You can get the live view, play back the video files, and do some other operations of the devices after managing the resources by areas.

8.4.1 Add Area for Current Site

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

Steps

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



Add Area

Basic Information

*Parent Area: 1.map.test

*Area Name: Area_20190903210421

Streaming Server: <None>

Map

Related Map

Figure 8-4 Add Area for Current Site

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**.

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.

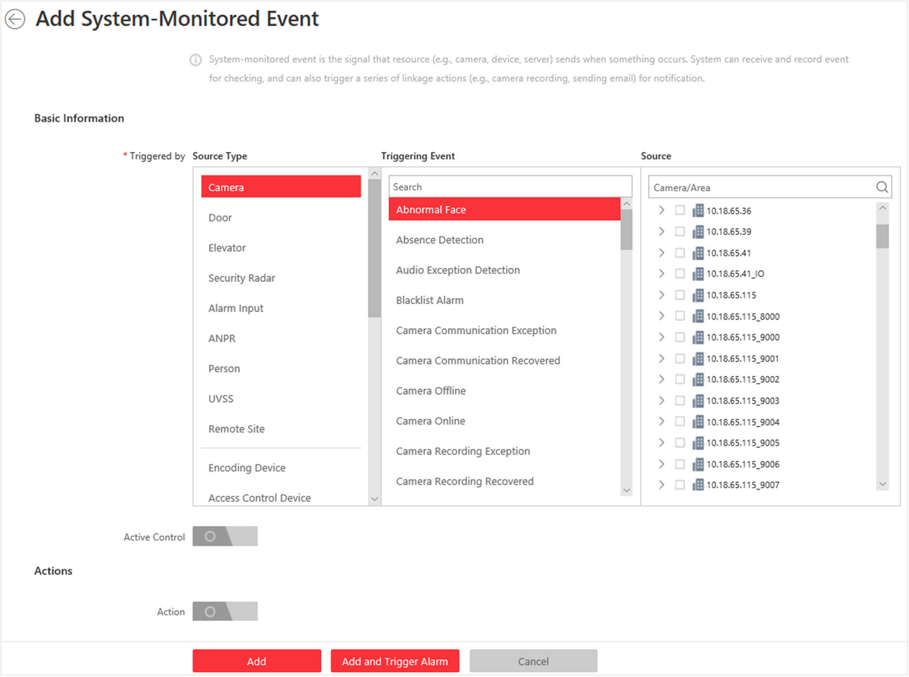
In this document, we will introduce setting camera alarm as an example. For the settings of other event types (e.g., alarm input, encoding device exception, server alarm), refer to the *User Manual of HikCentral Professional Web Client*.

9.1 Add Event for Camera

You can add an event for the cameras on the current site. When the event is triggered on the camera, system can receive and record event for checking and trigger a series of linkage actions (e.g., sending email) for notification.

Steps

1. Click **Event & Alarm → System-Monitored Event → Add** to enter the event adding page.



Add System-Monitored Event

System-monitored event is the signal that resource (e.g., camera, device, server) sends when something occurs. System can receive and record event for checking, and can also trigger a series of linkage actions (e.g., camera recording, sending email) for notification.

Figure 9-1 Add a System-Monitored Event

2. Configure the event's basic information, including source type, triggering event, and event source.

   Source Type

   Select the source type as **Camera**.

   Triggering Event

   The event detected on the camera will trigger a system-monitored event in the system.

   Source

   The specific camera(s) which can trigger this event.

3. **Optional:** Set the **Active Control** switch to on, and then set the Threshold for Reactivation.

   Note

   - Active Control is used to avoid the same event occurs frequently in a short time, which may aggravate the burden of HikCentral Professional event center. You need to set the Threshold for Reactivation. For example, you have set the Threshold for Reactivation as **30 s**, the same events from the same camera within 30 s will be regarded as one event on the HikCentral Professional.
   - The Threshold for Reactivation is 15 s by default. You can set it from 15 s to 1800 s.

4. **Optional:** Set the **Action** switch to on to set the linkage actions for the event.

   Arming Schedule Template

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

Trigger Recording

Select the camera to record video when the event occurs. You can play back the recorded video files when checking events in the Alarm & Event Search of the Control Client.

- To trigger the source camera itself for recording, select **Source Camera** and select the storage location for storing the video files.
- To trigger other cameras, select **Specified Camera** and click **Add** to add other cameras. Select the storage location for storing the video files. 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 files before the event, you can view the video recorded from periods preceding the event. Specify the number of seconds which you want to view the recorded video for before the event starts. For example, when someone opens a door, you can view the recorded video to see what happens right before the door opened.

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

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

Create Tag

Select the camera(s) to record video when the event occurs and add tag to the event triggered video. The tagged video can be searched and checked via the Control Client.

- To trigger the source camera itself for tagged recording, select **Source Camera** and select the storage location for storing the video files.
- To trigger other cameras for tagged recording, select **Specified Camera** and click **Add** to add other cameras. Select the storage location for storing the video files.

You can enter the tag name as desired. You can also click the button below to add the related information to the name.

Set the time range to define the tagged video length. For example, you can set to record the tagged video started from 5 seconds before the event and lasted until and 10 seconds after the event. The tagged video can be searched and checked via the Control Client.

Add the description to the tagged video as needed.

Capture Picture

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

- To trigger the source camera itself for capturing pictures, select **Source Camera**.
- To trigger other camera for capturing pictures, select **Specified Camera** and select one camera for capturing pictures.

Note

Only one camera can be set for capturing pictures.

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

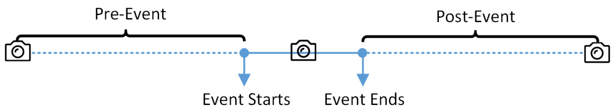


Figure 9-2 Capture Pictures

Note

The pre-event picture is captured from the camera's recorded video files. This pre-event capture function is only supported by the camera which is set to store the video files in the Recording Server (Cloud Storage Server, Hybrid SAN, or pStor).

Link Access Point

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

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

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

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

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

Link Alarm Output

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

Note

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

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

Trigger PTZ

Call the preset, patrol or pattern of the selected camera(s) when the event occurs.

Note

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

Send Email

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

Trigger User-Defined Event

Trigger user-defined event(s) when the system-monitored event is triggered.

You can select the pre-defined user-defined event(s) in the event list.

5. Finish adding the event.
   - Click **Add** to add the event and back to the event list page.
   - Click **Add and Trigger Alarm** to trigger this event as an alarm for further notification.

   After adding the event, it displays on the event list, and you can view the event name, event source, and triggering event.

9.2 Add Alarm for Camera on Current Site

You can set alarms for added cameras on current site and configure a series of linkage actions (e.g., triggering pop-up window on the Control Client) for notification when alarm is triggered.

Steps

1. Click **Event & Alarm → Alarm → Add** to enter the Add Alarm page.
2. Set the source type as **Camera** in the **Source Type** field.
3. Select a triggering event as the source for triggering the alarm.
4. In the site drop-down list, select the current site.
5. Select a specific camera for triggering the alarm.
6. **Optional:** Enter the instructions for handling the alarm or enter remarks for the alarm.
7. Set the required information.

   Arming Schedule

   The camera is armed during the arming schedule and the event occurred during the arming schedule will be triggered as alarm and notify the user. It provides two types of arming schedule:

   - **Schedule Template:** Select an arming schedule template for the alarm to define when the alarm can be triggered.
   - **Event Based:** Specify a user-defined event or an alarm input as the start or end event of the arming schedule. When the user defined event or alarm input is triggered, the arming schedule will start or end. You can set the **Auto-End Arming** switch to on and set the specified time to automatically end arming for this alarm even if the end event does not occur.

Note

For example, you have set event A as start event, event B as end event, and set the **Auto-End Arming in** as ***60 s***, when event A occurs at T1, the alarm will be armed from T1 until event B occurs within 60 s (See the following figure Arming Schedule 1), or end arming 60 s later and event B doesn't occur (See the following figure Arming Schedule 2).

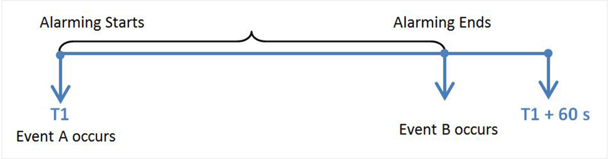


Figure 9-3 Arming Schedule 1

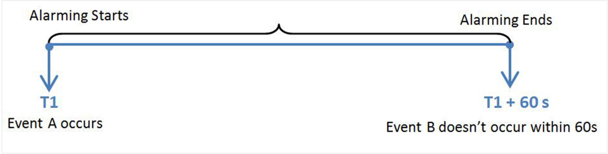


Figure 9-4 Arming Schedule 2

When A occurs at time T1, the alarm will be armed from T1, if A occurs again at time T2 but B doesn't occur, the alarm will be armed from T2 again.

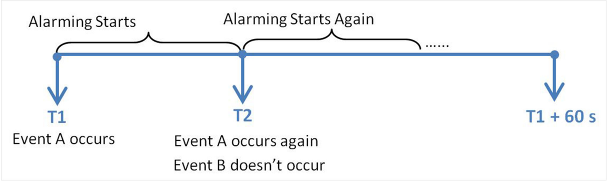


Figure 9-5 Arming Schedule 3

Alarm Priority

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

Active Control

Active Control is used to avoid the same alarm being received frequently in a short time. You need to set the Threshold for Reactivation. For example, you have set the Threshold for Reactivation as ***30 s***, the same alarms from the same camera within 30 s will be regarded as one alarm on the system.

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

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.

8. **Optional:** Set the alarm's additional settings such as alarm related cameras and map, and alarm linkage actions.

Related Camera

Select the related camera to record the alarm video when the alarm is triggered. You can view the live video and play back these video files in the Alarm Center of the Control Client.

- To relate the source camera itself for recording, select **Source Camera** and select the storage location for storing the video files.
- To relate other cameras, select **Specified Camera** and click **Add** to add other cameras as related cameras. Select the storage location for storing the video files.
- **View Pre-Alarm Video:** You can view the video recorded from periods preceding the alarm. Specify the number of seconds which you want to view the recorded video for before the alarm starts. For example, when someone opens a door, you can view the recorded video to see what happens right before the door opened.
- **Post-record:** Record video from periods following detected alarms. Specify the number of seconds which you want to record video for after the alarm stops.
- **Lock Video Files for:** Set the days for protecting the video file from being overwritten.
- **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.

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.

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.

Trigger Audible Warning

Set the voice text for playing on the PC when alarm is triggered.

Note

You should set voice engine as the alarm sound on System Settings page of Control Client.

Trigger User-Defined Event

Trigger the user-defined event(s) when alarm is triggered.

You can select the pre-defined user-defined event(s) in the event list.

9. Finish adding the alarm.
- Click **Add** to add the alarm and back to the alarm list page.
- Click **Add and Continue** to add the alarm and continue to add other alarm.

The alarm will be displayed on the alarm list and you can view the alarm name and alarm status.

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), time and attendance (adding the person to attendance group), etc. After adding the persons, you can edit and delete the person information if needed.

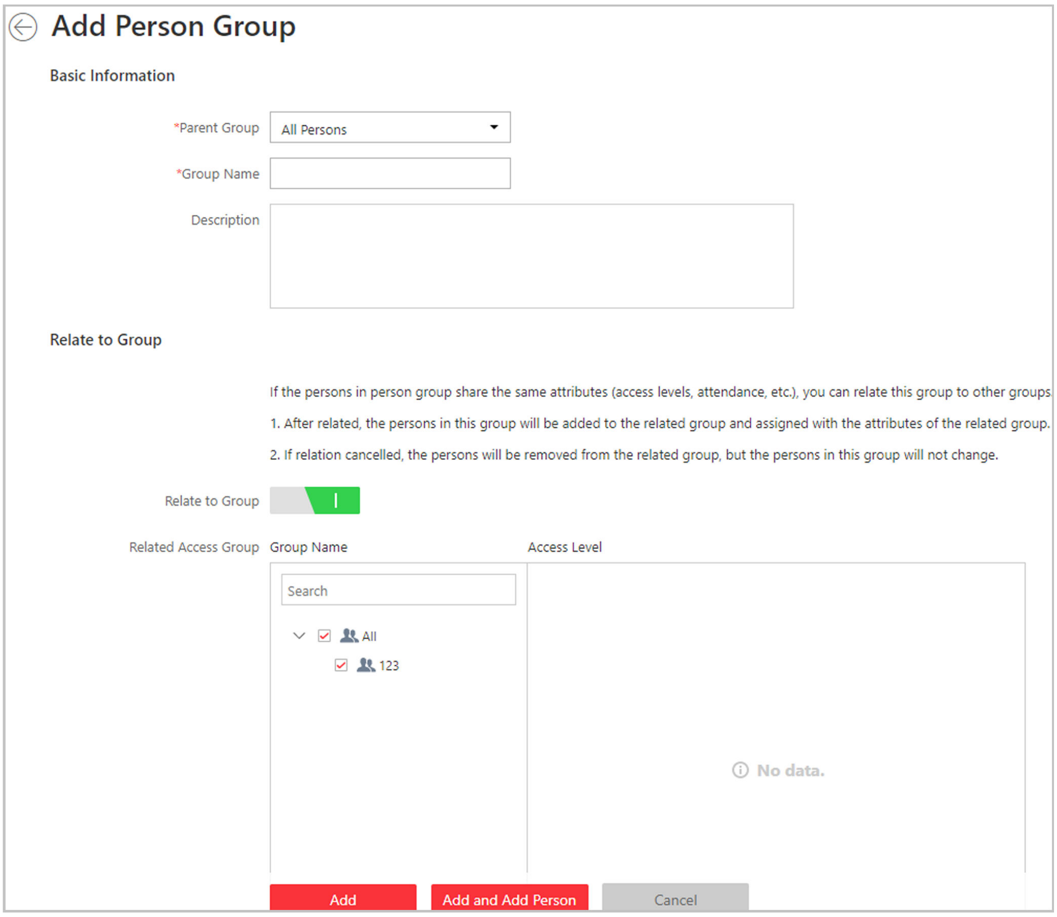
10.1 Add Person Group

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, attendance, etc.), you can relate this group to existing access group(s).
   1) Switch **Relate to Group** on.
   2) Select existing access group(s).

      After related, the persons added to this group will also be added to the related access groups and attendance groups, so that the persons will be automatically assigned with attributes of the related access groups and attendance groups.
5. Confirm to add the person group.
   - To save the person group first and add persons to this group later, click **Add** to finish this task and go back to Person List page.
   - To add persons to this person group, click **Add and Add Person** to finish this task and enter the Add Person to Person Group page to add a person to this person group.

Note

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

10.2 Add a Person

You can add the person information to the system one by one.

Steps

1. Click **Person → Person List** and click **Add** to enter the adding person page.
2. Set the person basic information.

   ID

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

   Note

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

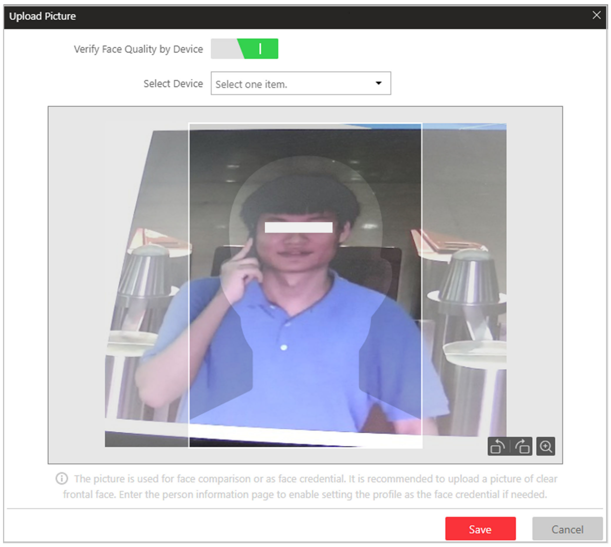
   Person Picture

   Hover the cursor on the person picture field to show the three picture-adding modes.

   - Click **Collect by Device** to open the Collect by Device window. Select a face recognition terminal 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.

     Note

     Collect by Device mode only supports face recognition terminal (including DS-K5603-Z, DS-K1T604, DS-K1T605, DS-K1T606, DS-K1T607, etc.).



Upload Picture

Verify Face Quality by Device

Select Device: Select one item.

The picture is used for face comparison or as face credential. It is recommended to upload a picture of clear frontal face. Enter the person information page to enable setting the profile as the face credential if needed.

Figure 10-2 Collect by Device Window

   - Click **Take a Picture** to use the PC's webcam to take a picture.
   - Click **Upload Picture** to select a picture in your PC.

Note

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

3. Select a person group for the person.
4. **Optional:** Set the person's additional information.
5. **Optional:** Set the access control and time & attendance information.

Effective Period

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

Access Group

Add the person to the existing access group(s) which can be linked with access level(s). The linkage of access level and access group defines the access permission that which person(s) can access which access point(s) in the authorized period.

You can click the access group name to view its linked access levels.

Move the cursor to the access level to view its access point(s) and access schedule.

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

Note

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

6. Set the person's credential information, including PIN, face credential, card number, fingerprint, and duress credentials.

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 or card reader to get the card number, and then issue it to the person.

a. Click **+** in the **Card** field.
b. Place the card that you want to issue to this person on the card enrollment station or on the card reader and the card number will be read automatically. Or you can enter the card number manually

123456789

Figure 10-3 Card Number Read

Note

Up to 5 cards can be issued to one person.

Fingerprint

System provides two ways to collect fingerprint: via a USB fingerprint recorder connected to the PC running the Web Client or via a fingerprint and card reader of the access control device managed in the system.

Click **Configuration** to set the collection mode as **USB Fingerprint Recorder** or **Fingerprint and Card Reader**.

USB Fingerprint Recorder

Collect fingerprint via a USB fingerprint recorder connected to the PC running the Web Client, which is plug-and-play and doesn't require any settings. This mode is suitable for face-to-face scenario that the person and the system administrator are in the same location.

After connecting the fingerprint recorder to your PC, click **+**, place and lift your fingerprint on the recorder following the prompts and it will collect your fingerprint automatically.

Fingerprint and Card Reader

Collect fingerprint via the fingerprint scanner of an access control device which is managed in the system. This mode is suitable for non-face-to-face scenario that the person and the system administrator are in different locations.

Select an access control device from the managed device list and select a fingerprint and card reader.

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

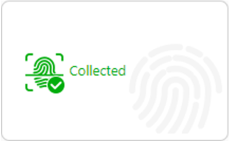


Figure 10-4 Fingerprint Recorded

Note

Up to 10 fingerprints can be added to one person.

Credential under Duress

Set the credentials (card number and fingerprint) so that when you are under duress, you can swipe the card or scan the fingerprint configured here. The door will be unlocked and the Control Client will receive a duress alarm (if configured) to notify the security personnel.

Note

When the person accesses with credentials under duress, he/she cannot be exempted from remaining locked (credential failed) restrictions, all anti-passback rules, and first card authorization. Extended access is not allowed as well.

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.

7. Finish adding the person.
- Click **Add** to add the person and return the person list.
- Click **Add and Continue** to add the person and continue to add other persons.

The person will be displayed in the person list and you can view the details.

Chapter 11 Manage Access Control

The system supports access control and elevator control functions. Access control is a security technique that can be used to regulate who can get access to the specified doors and elevator control can be used to regulate who can get access to the specified floors by taking the elevator.

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

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 and floors (the doors and floors in the linked access level) during the same authorized time period. You need to assign the access level to the access group so that these persons in the access group can access the doors and floors in the access level.

Steps

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

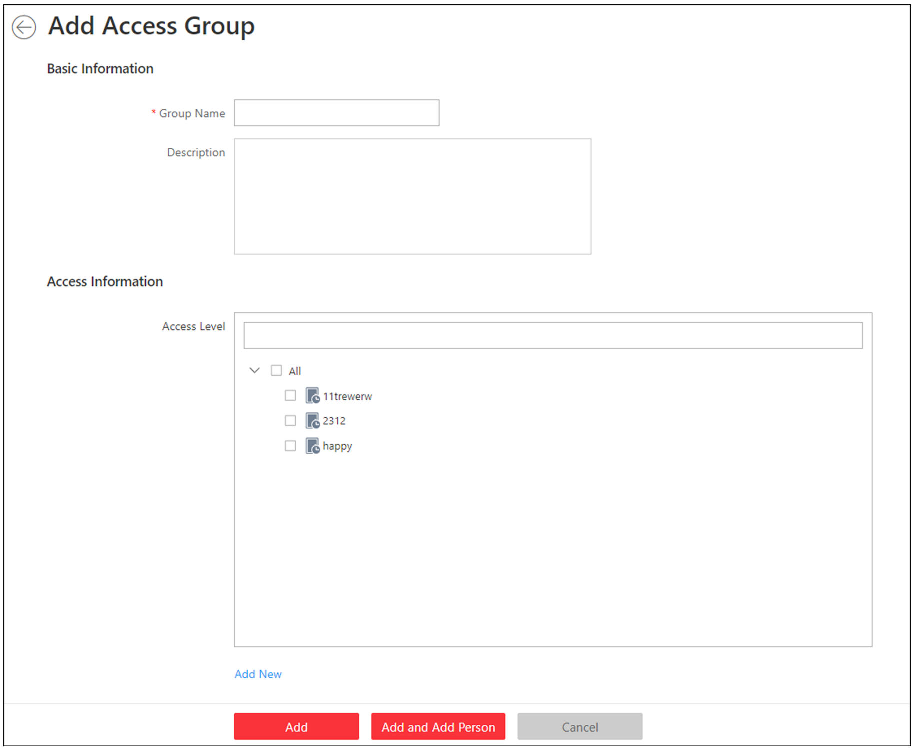


Figure 11-1 Add Access Group

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 and floors in the access level(s) during the authorized time period.

Note

- Move the cursor to the access level and you can view its doors and floors and access schedule.
- Up to 8 access levels can be assigned to one access group.

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.

   Attendance Group

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

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

11.2 Manage Access Level

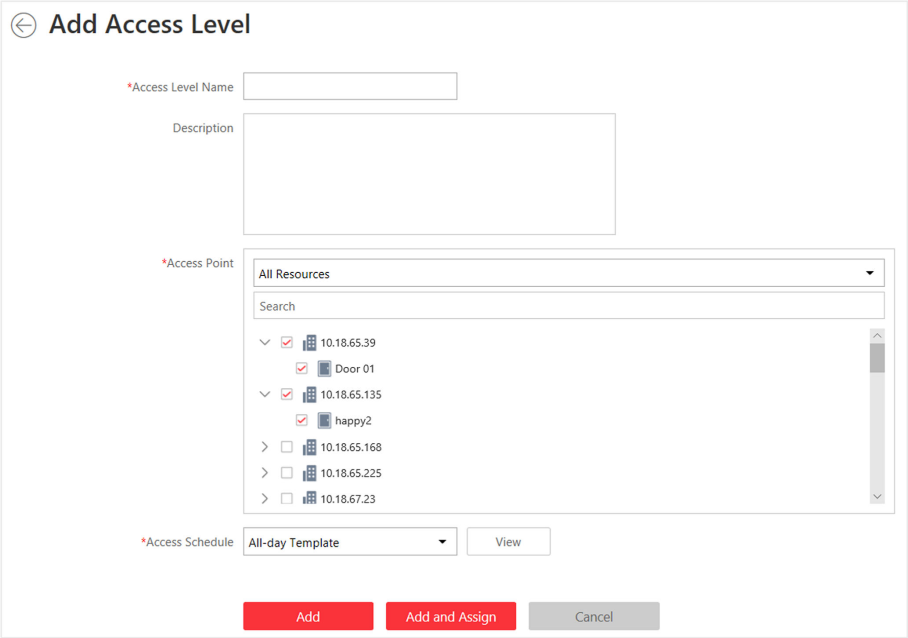
In access control, access level is a group of doors and floors. After assigning the access level to certain access groups, it defines the access permission that which persons can get access to which doors and floors during the authorized time period.

11.2.1 Add Access Level

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

Steps

1. Click **Access Level** on the Home page to enter the access level management page.
2. Click **Add**.



*Access Point: All Resources

*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 and floors managed in the system will be display.

      Door

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

      Floor

         Only floors will be displayed. You can set the display the floors by area or by floor No.

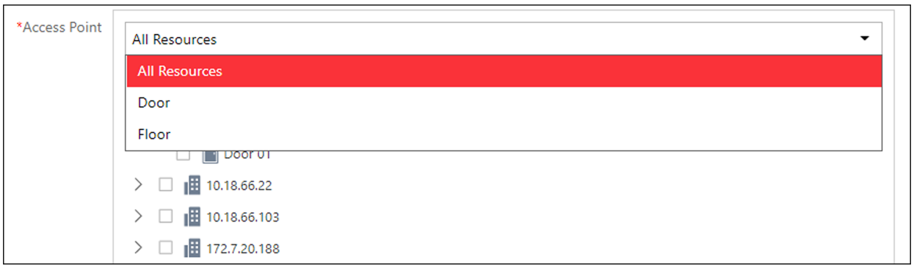


Figure 11-3 Select Access Point Type

2) Select the doors or floors.

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

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.

Steps

1. Click **Access Level** on the Home page to enter the access level management page.
2. Enter the Assign to Access Group page.
   - After you setting the parameters of access level when adding, click **Add and Assign**.
   - When editing the access level, click **Configuration** in the access level details page.
   - Click in the Operation column.
3. In the **Assign to Access Group** field, select the access group(s) (including access groups for persons and access groups for visitors) so that the persons in the access groups will have the access permission to access the doors and floors in the access level.
4. 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 the permissions to the roles as required, and the users can be assigned with different roles to obtain different permissions.

Steps

1. Click **Security → Roles** to enter the Role Management page.

   Note

   The system pre-defines two default roles: administrator and operator. You can click the role name to view the details and operations. But you cannot edit or delete the two default roles.

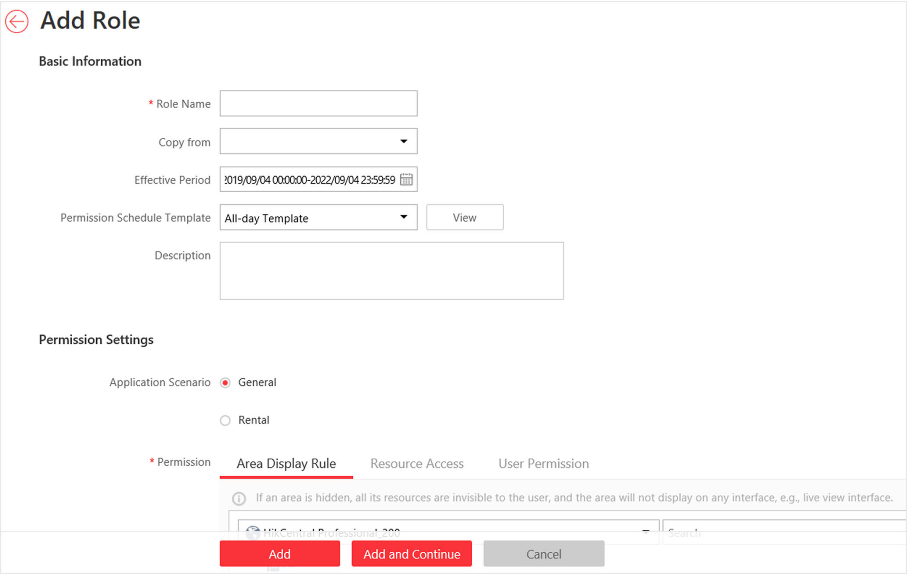
   Administrator

   The role that has all the permission of the system.

   Operator

   The role that has all the permission for operating the Control Client and has the permission for operating the Applications (Live View, Playback, and Local Configuration) on the Web Client.

2. Click **Add** to enter the Add Role page.



Add Role

Basic Information

* Role Name

Copy from

Effective Period 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.

Figure 12-1 Add Role Page

3. Set the role name, effective period, permission schedule template, and description as desired.

Effective Period

The date that this role takes effective and turns invalid.

Permission Schedule Template

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

4. Set the permission for the role.

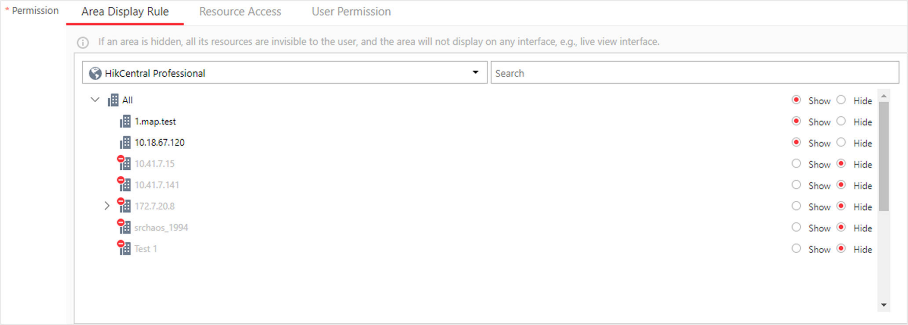
- Select the default or pre-defined role from the **Copy from** drop-down list to copy the permission settings of selected role.
- Select Application Scenario for the role. If you select **General**, you need to assign the permissions to the role; if you select **Rental**, you need to select access groups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

HikCentral Professional | Search

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

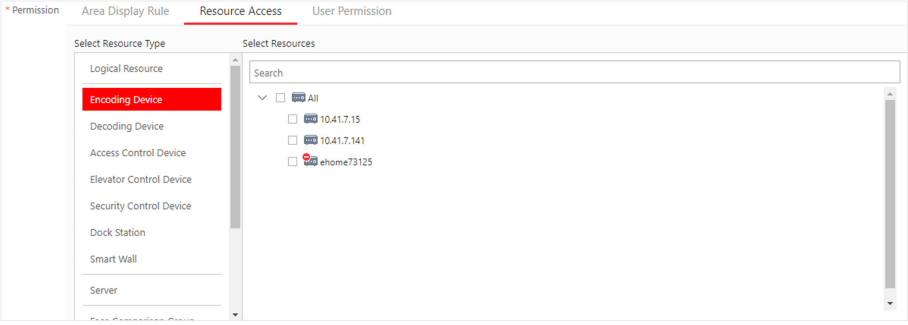
Figure 12-2 Area Display Rule

Resource Access Permission

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

Note

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

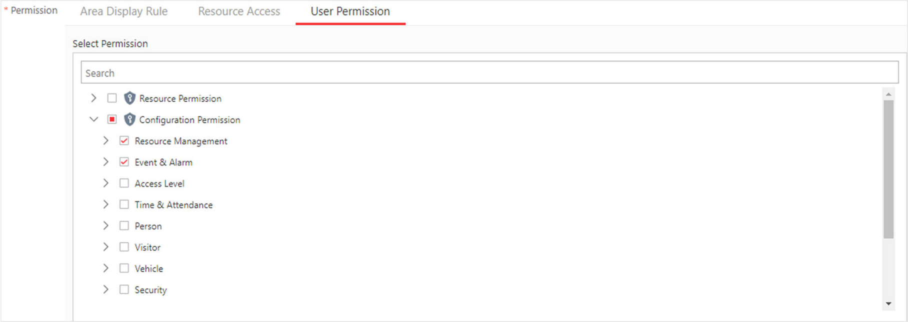


□ All
- □ 10.41.7.15
- □ 10.41.7.141
- □ ehome73125

Figure 12-3 Resource Access Permission

User Permission

Assign the resource permissions, configuration permissions on the Web Client, and the control permissions on the Control Client to the role.



- □ Resource Permission
- ■ Configuration Permission
  - ☑ Resource Management
  - ☑ Event & Alarm
  - □ Access Level
  - □ Time & Attendance
  - □ Person
  - □ Visitor
  - □ Vehicle
  - □ Security

Figure 12-4 User Permission

5. Complete adding the role.

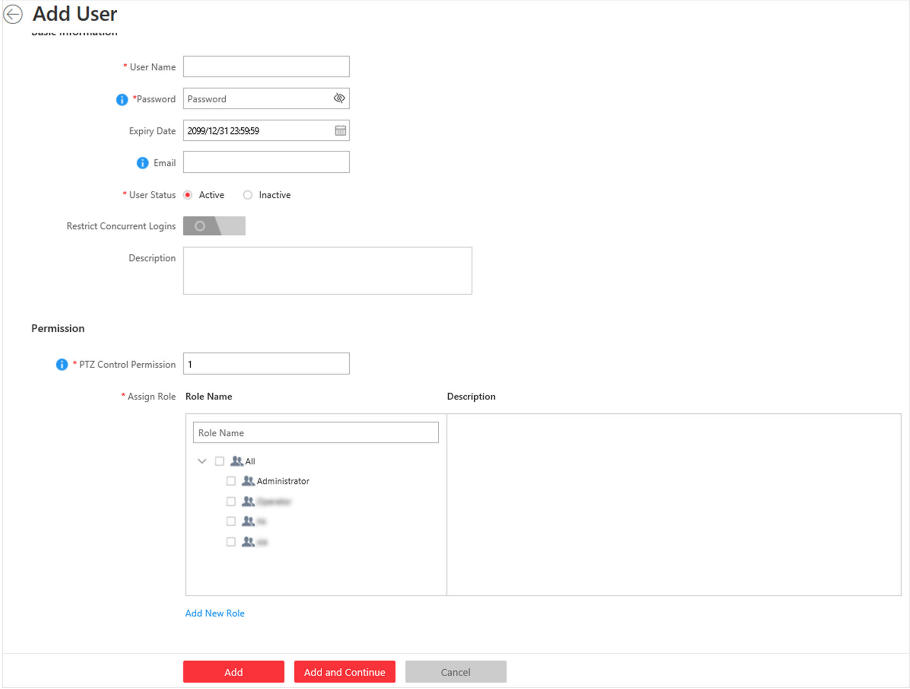
- Click **Add** to add the role.
- Click **Add and Continue** to save the settings and continue to add roles.

12.2 Add Normal User

You can add normal users for accessing the system and assign role to the normal user. Normal users refer to all the users except the admin user.

Steps

1. Click **Security → Users** to enter the User Management page.
2. Click **Add** to enter the Add User page.



Add User

* User Name	
*Password	Password
Expiry Date	2099/12/31 23:59:59
Email	
* User Status	● Active ○ Inactive
Restrict Concurrent Logins	
Description	

Permission

* PTZ Control Permission	1
* Assign Role	Role Name

Figure 12-5 Add User Page

3. Set the required parameters.

   User Name

   For user name, only letters(a-z, A-Z), digits(0-9), and "-" can be contained.

   Password

   Create an initial password for the user which should be changed by the user for first time login.

   Note

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

Expiry Date

The date when this user account becomes invalid.

Email

The system can notify user by sending an email to the email address. If the normal user forget his/her password, he/she can reset the password via email.

Note

The email address of the admin user can be edited by the user with the role of administrator.

User Status

Two kinds of status are available. If you select freeze, the user account is inactive until you set the user status to active.

Restrict Concurrent Logins

If necessary, switch **Restrict Concurrent Logins** to on and enter the maximum number of concurrent logins.

4. Set the permission level (1-100) for PTZ control in PTZ Control Permission.

Note

The larger the value is, the higher permission level the user has. The user with higher permission level has the priority to control the PTZ unit.

Example

When user1 and user 2 control the PTZ unit at the same time, the user with higher PTZ control permission level will take the control of the PTZ movement.

5. Check the existing roles to assign the role(s) for the user.
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