HikCentral Professional

Quick Start Guide

Contents

Chapter 1 Guide Content 1

Chapter 2 Administrator Rights 2

Chapter 3 System Requirements 3

3.1 System Requirements for Servers 3

3.2 System Requirements for Control Client 3

Chapter 4 Centralized Deployment and Distributed Deployment 5

Chapter 5 Installation 8

5.1 Install Module 8

5.1.1 Install Service Module in Custom Mode 8

5.1.2 Install Service Module in Typical Mode 10

5.2 Install Control Client 11

5.3 Service Manager 11

Chapter 6 Log into the Web Client 13

6.1 Recommended Running Environment 13

6.2 Login for First Time for admin User 13

Chapter 7 Manage License 15

7.1 Activate License - Online 15

7.2 Update License - Online 17

Chapter 8 Manage Resource 18

8.1 Add Encoding Device by IP Address or Domain Name 18

8.2 Add Access Control Device by IP Address 21

8.3 Manage Application Data Server 22

8.4 Manage Area 24

8.4.1 Add Area for Current Site 24

8.4.2 Add Camera to Area for Current Site 25

Chapter 9 Configure Event and Alarm 27

9.1 Add Event for Camera 27
9.2 Add Alarm for Camera on Current Site 30
Chapter 10 Manage Access Control 33
10.1 Add Access Group 33
10.2 Manage Access Level 35
10.2.1 Add Access Level 35
10.2.2 Assign Access Level to Access Group 36
Chapter 11 Manage Role and User 37
11.1 Add Role 37
11.2 Add Normal User 38

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 reset your password regularly, especially in the high security system, resetting 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).

  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).

  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).

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:

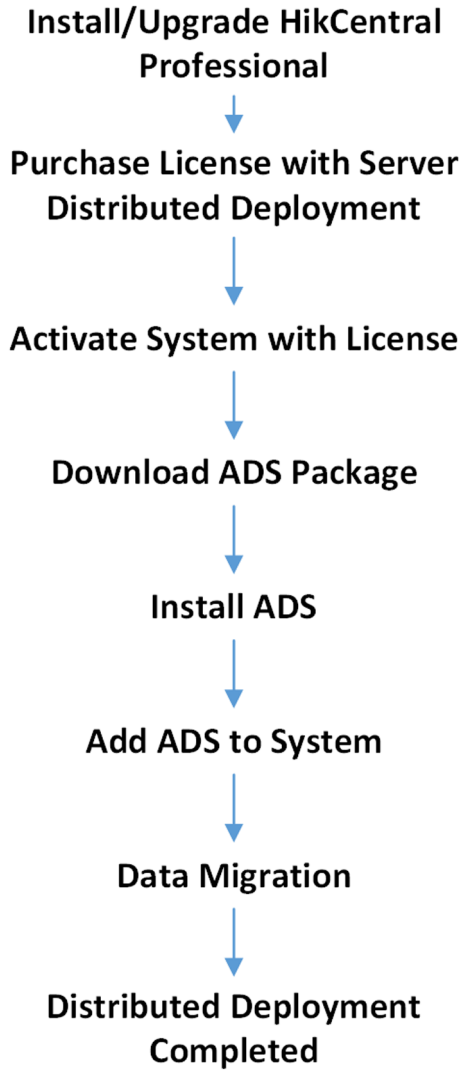

Figure 4-1 Process of Distributed Deployment

- **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**.

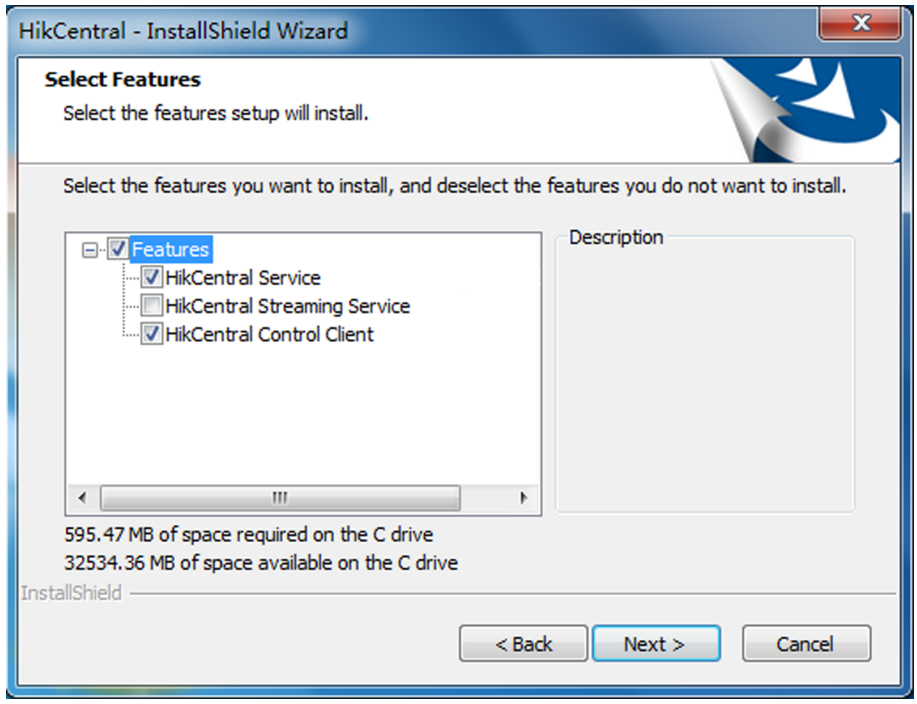

Figure 5-1 Select Modules to Install

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.

Steps

Note

The installation package downloaded from the Web Client is 32-bit.

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.

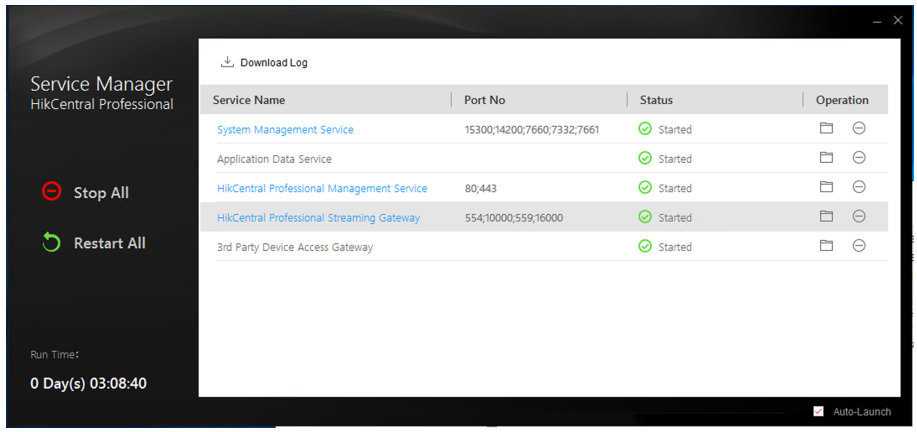

Figure 5-2 Service Manager Main Page

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 (32-bit), Firefox 57 and above (32-bit), Google Chrome 61 and above (32-bit), 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 reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.
Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

3. Click **OK**.

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

Result

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

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.

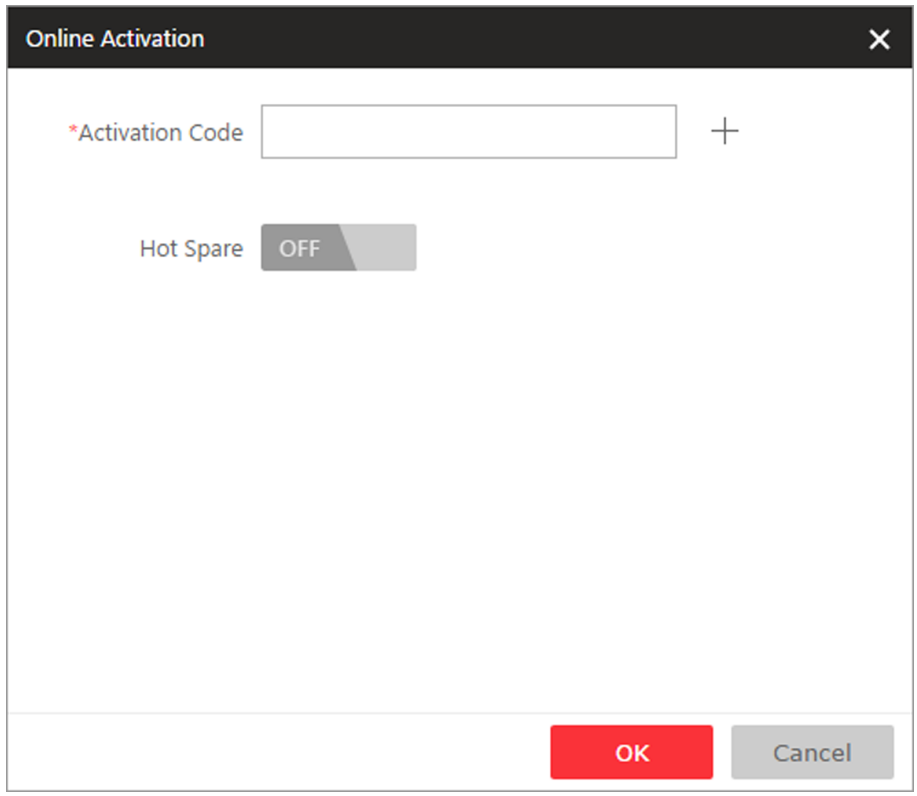

Figure 7-1 License Configuration Window

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.

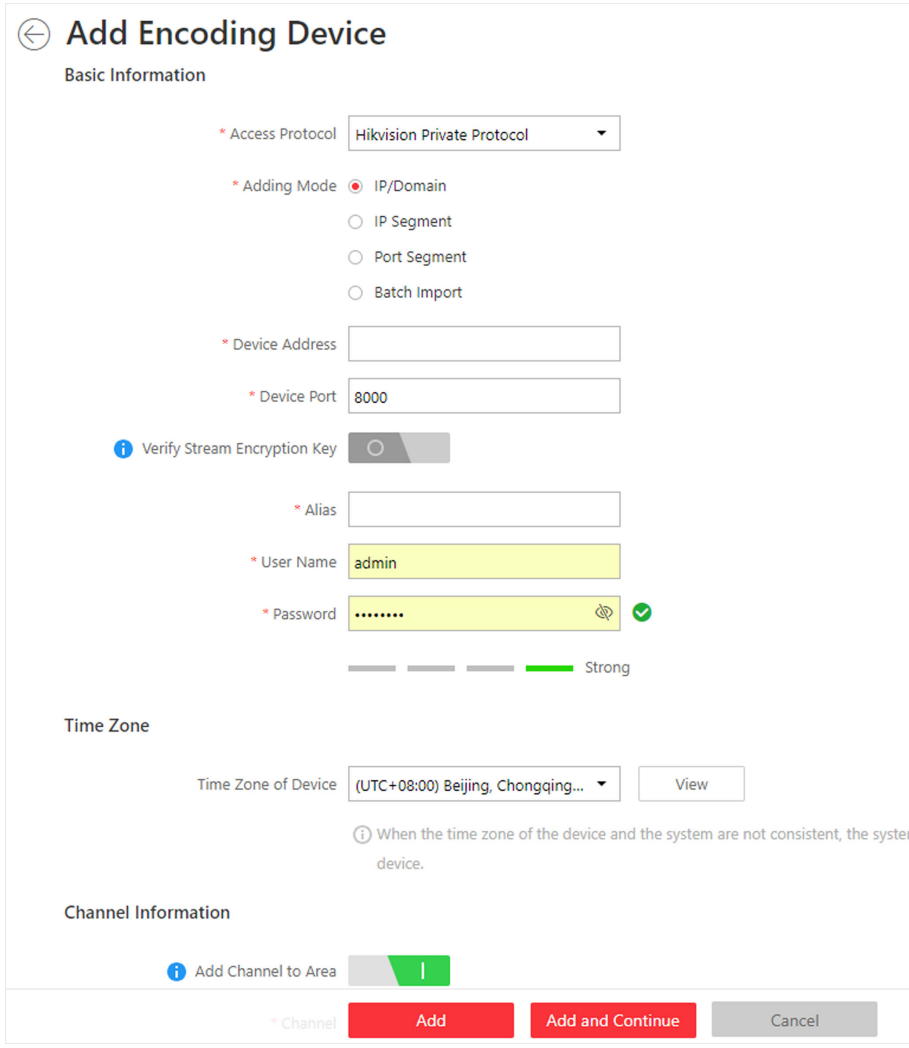

Figure 8-1 Add Encoding Device Page

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.

Alias

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

Caution

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

6. **Optional:** Select a time zone for the device in drop-down list of **Time Zone of Device** when the time zones of the device and the SYS server are not consistent.
7. **Optional:** Switch **Add Channel to Area** to on to import the channels of the added devices to an area.

Note

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

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

Note

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

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

Encoding Device

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

Hybrid Storage Area Network

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

Cloud Storage Server

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

pStor

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

Note

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

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

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

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

6. **Optional:** Select a time zone for the device in drop-down list of **Time Zone of Device** when the time zones of the device and the SYS server are not consistent.
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

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.

How to add an Application Data Server?

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.

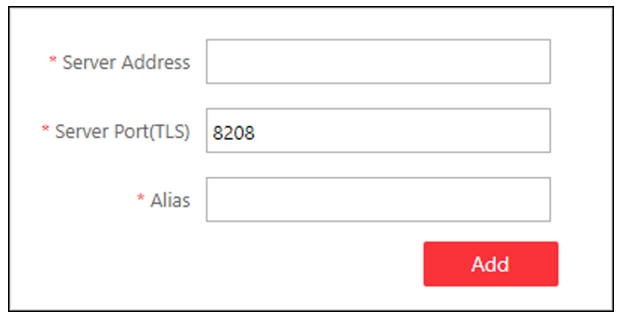

Figure 8-2 Add Application Data Server

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.

8.4 Manage Area

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

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.

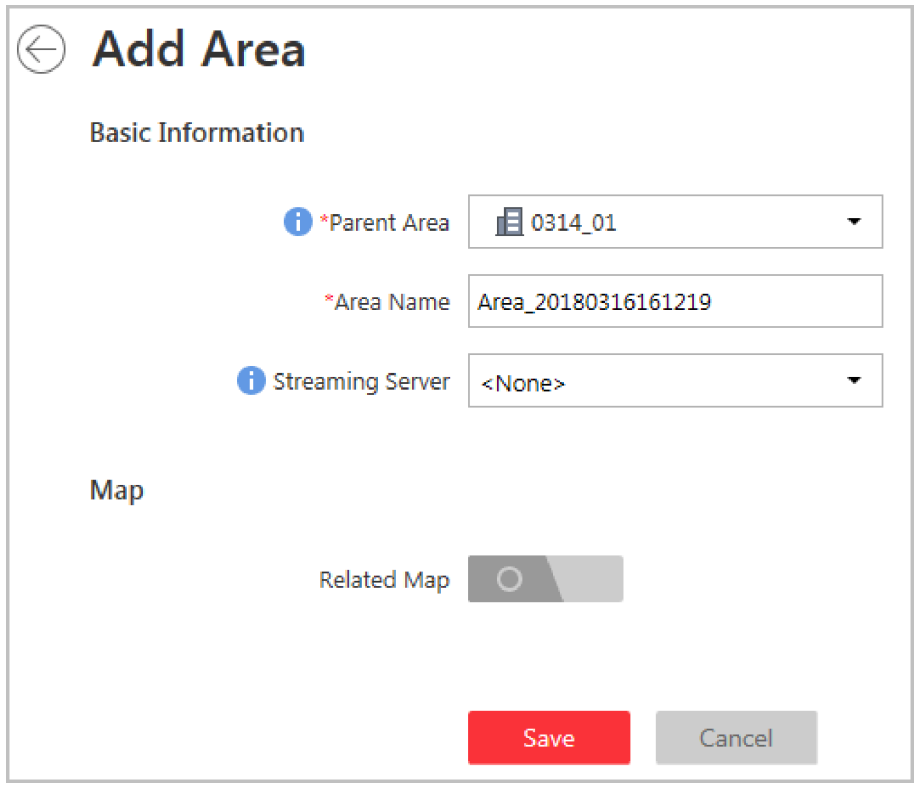

Figure 8-4 Add Area for Current Site

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.

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.
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.

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).

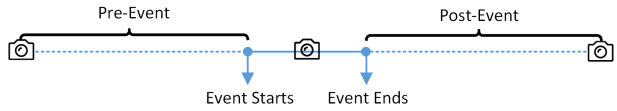

Figure 9-1 Capture Pictures

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 point(s) to be locked or unlocked when the event occurs. For example, you can set to trigger all the access points closed when the system detects suspicious person entering.

- **All Access Points:** When the event occurs, all the access points in the system will be unlocked, locked, remain unlocked, or remain locked.
- **Specified Access Point:** Click **Add** to select the access point(s) as the linkage target(s). You can set the access point action so that the access point will be unlocked, locked, remained unlocked, or remained locked when the event occurs.

Link Alarm Output

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

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.

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. Select a specific camera for triggering the alarm.
5. **Optional:** Enter the instructions for handling the alarm or enter remarks for the alarm.
6. 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.

   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.

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.

7. **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.

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.

Trigger User-Defined Event

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

8. 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 Access Control

After adding the persons to the person list, you can assign the access permission to persons to define when they can get access to which door(s). To define the access permission, you should create an access level to group the doors and an access group to group the persons. After assigning the access level to the access group, the persons in the access group will be authorized to access the doors in the access level with their credentials during the authorized time period.

10.1 Add Access Group

Access group is a group of persons who have the same access permission. The persons in the access group can access the same doors (the doors in the linked access level) during the same authorized time period. You need to assign the access level(s) to the access group so that these persons in the access group can access the door(s) in the access level.

Steps

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

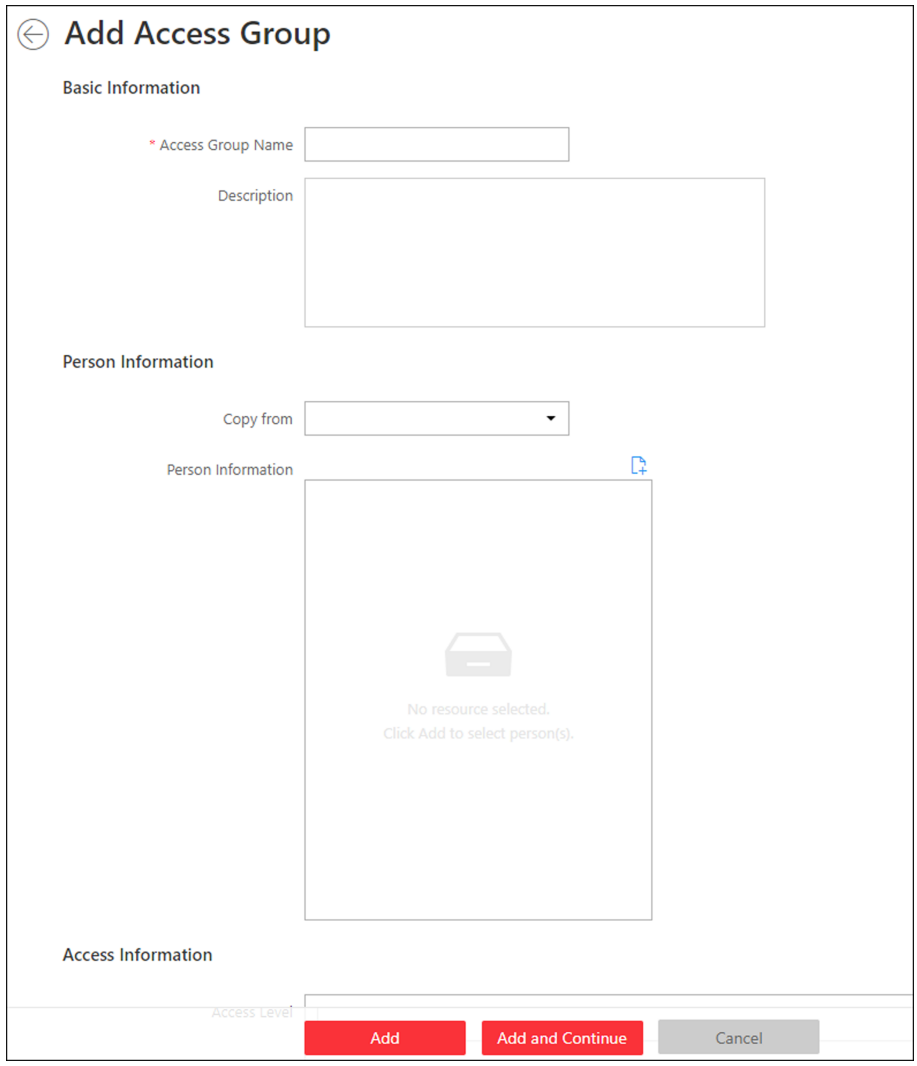

Figure 10-1 Add Access Group

2. Set the basic information.

Access Group Name

Create a name for the access group.

3. Optional: Set the person(s) to add to the access group.

1) Click .

All the persons added to the system display. You can view the person name, picture, person ID, and remark information.

2) Filter the persons by setting the filtering conditions.

Person List

Filter persons in the person list by person name or additional information.

Enter the keyword or search scope and press **Enter** or click to search.

Imported Domain Group

The imported domain groups will display. Enter the keyword of group name to search the group.

Click the group to add all the persons in the group.

3) **Optional:** You can also select the existing access group or attendance group from the **Copy from** drop-down list to copy person information from other group.

4. **Optional:** Select the access level(s) to link the access group to the access level(s) so that the person(s) you selected in step 3 can access the doors linked to the access level(s) during the authorized time period.
5. Finish adding the access group.
   - Click **Add** to add the access group and return to the access group management page.
   - Click **Add and Continue** to add the access group and continue to add other access groups.

10.2 Manage Access Level

In access control, access level is a group of door(s). After assigning the access level to certain access group(s), it defines the access permission that which person(s) can get access to which door(s) during the authorized time period.

10.2.1 Add Access Level

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

Steps

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

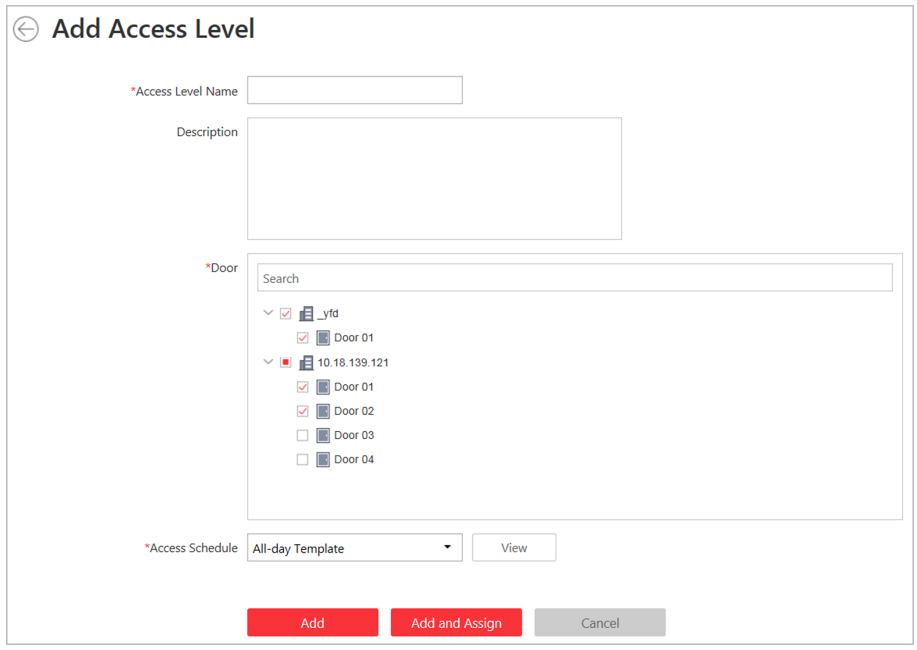

Figure 10-2 Add Access Level

3. Create a name for the access level.
4. **Optional:** Enter the description for the access level.
5. Select the door(s) to add the access point(s) to the access level.
6. Select the access schedule to define in which time period, the persons are authorized to access the doors (selected in step 5).
7. Finish adding the access level.
   - Click **Add** to add the access level and return to the access level management page.
   - Click **Add and Assign** to assign the access level to some access group(s) so that the person(s) in the access group(s) will have access permission to access door(s) selected in step 5.

10.2.2 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) you want to assign the access level to.
4. **Optional:** Click **Add New** to add a new access group.
5. Click **Save**.

Chapter 11 Manage Role and User

The system allows you to add users and assign user's permissions for accessing and managing the system. Before adding users to the system, you should create roles to define the user's access rights to system resources and then assign the role to the user for granting the permissions to the user. A user can have many different roles.

11.1 Add Role

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.
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.

   Area Display Rule

   Show or hide the specific area(s) for the role. If the area is hidden, the user with the role cannot view and access the area and its resources on any interface.

   Resource Access Permission

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

User Permission

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

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

11.2 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.
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 reset your password regularly, especially in the high security system, resetting 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.

Restrict Concurrent Logins

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

User Status

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

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

Note

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

Example

When user1 and 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