HikCentral Professional

Quick Start Guide

Contents

Chapter 1 Guide Content

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

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

Chapter 2 Administrator Rights

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

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

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

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

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

Note

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

Chapter 3 System Requirements

3.1 System Requirements for Servers

Server without Remote Site Management (RSM) Module

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

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

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

Server with Remote Site Management (RSM) Module

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

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

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

3.2 System Requirements for Control Client

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

⬚**i 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 Installation

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

Two installation packages are available for building your system.

Basic Installation Package

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

Control Client Installation Package

Contains the Control Client module only.

[i] **Note**

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

4.1 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.

4.1.1 Install Service Module in Custom Mode

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

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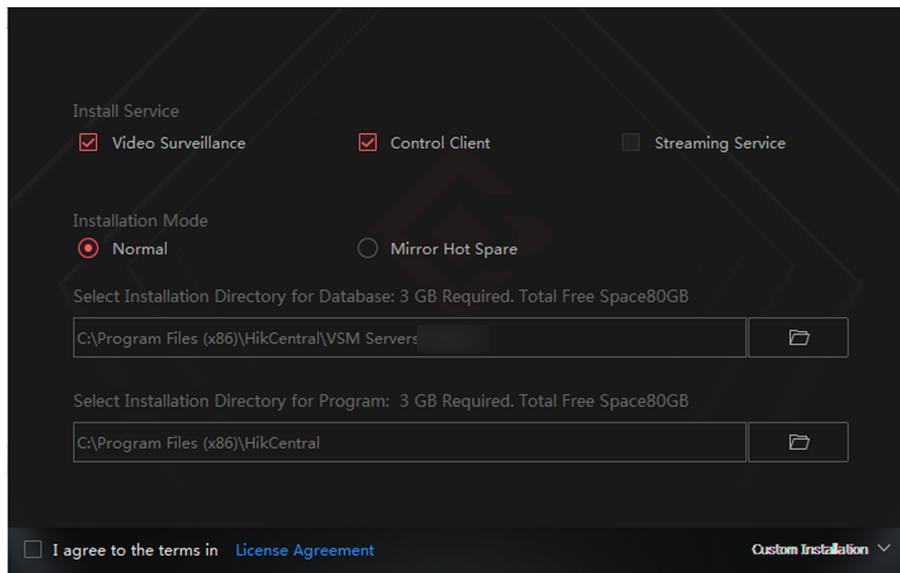
Figure 4-1 Select Modules to Install

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

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

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

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

6. **Optional:** Select a proper directory as desired to install the program module(s) and the database.
7. Click **Custom Installation** again to return to the Welcome panel.
8. Click **Install Now** to begin the installation.
   A panel indicating progress of the installation will display.
9. Click **Finish** to complete the installation.

4.1.2 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 ![icon] (HikCentral Professional) to enter the welcome panel of the InstallShield Wizard.
2. Click **I agree to the terms in License Agreement** and read the License Agreement.
3. Click **Install Now** to begin the installation.

   A panel indicating progress of the installation will display.

4. Click **Finish** to complete the installation.

4.2 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 (64-bit).

Steps

![Note icon] **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 ![icon] (HikCentral Professional_Client) to enter the welcome panel of the InstallShield Wizard.
2. **Optional:** Select a proper directory on your computer to install the Control Client.
3. Click **Install Now** to begin the installation.

   A panel indicating progress of the installation will display.

4. Click **Finish** to complete the installation.

4.3 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 ![icon] and select **Run as Administrator** to run the Service Manager.
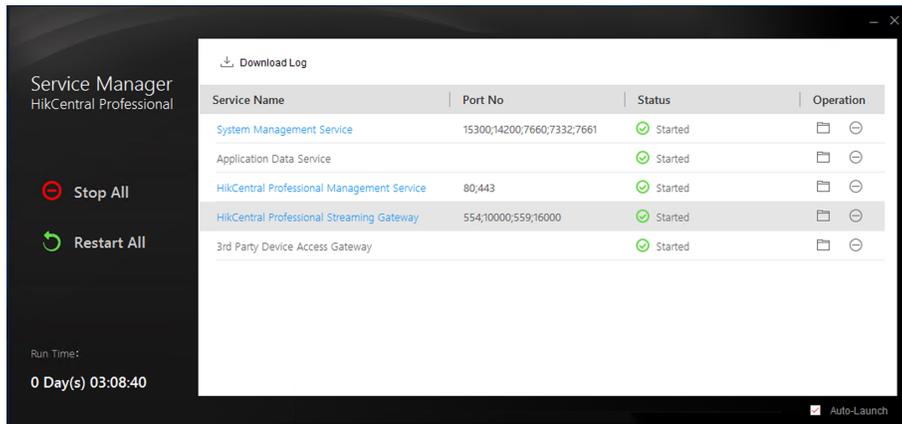
Figure 4-2 Service Manager Main Page

📖**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 5 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.

5.1 Recommended Running Environment

The following is recommended system requirement for running Web Client.

CPU

Intel Pentium IV 3.0 GHz and above

Memory

1 GB and above

Video Card

RADEON X700 Series

Web Browser

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

⌨**Note**

You should run the web browser as administrator.

5.2 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 6 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.

$\boxed{i}$**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*.

6.1 Activate License - Online

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

Steps

1. Log in to HikCentral Professional via the Web Client.
2. On the Home page, click **Activate → Online Activation** to open the Online Activation panel.
3. Enter the activation code.

   $\boxed{i}$**Note**

   - If you have purchased more than one Licenses, you can click $+$ and enter other activation codes.
   - Up to 110 Licenses are allowed in one system.

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

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

6. Click **Activate**.

6.2 Update License - Online

As your project grows, you may need to increase the connectable number of resources (e.g., cameras) for your HikCentral Professional. If the SYS to be updated can properly connect to the Internet, you can update the License in online mode.

Before You Start
Contact your dealer or our sales team to purchase a License for additional features

Steps
1. Log in to HikCentral Professional via the Web Client.
2. In the top right corner of Home page, select **Maintenance and Management → Update License → Online Update** to open the Online Update panel.
3. Enter the activation code.

Note
- If you have purchased more than one Licenses, you can click $+$ and enter other activation codes.
- Up to 110 Licenses are allowed in one system.

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

Chapter 7 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 device via an IP address or domain name. For other methods, please refer to the *User Manual of HikCentral Professional Web Client*.

7.1 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 platform by specifying the IP address (or domain name), user name, password, etc.

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

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

   $\boxed{i}$**Note**

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

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

   Device Address

   The IP address or domain name of the device.

   Device Port

   By default, the device port No. is 8000.

   Mapped Port

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

Verify Stream Encryption Key

This button is for **Hikvision Private Protocol** only. Switch **Verify Stream Encryption Key** to on, and enter the stream encryption key in the following **Stream Encryption Key on Device** field. Then when starting live view or remote playback of the device, the client will verify the key stored in SYS server for security purpose.

$\boxed{i}$**Note**

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

Device Name

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

Password

The password required to access the account.

$\triangle$**Caution**

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

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

$\boxed{i}$**Note**

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

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

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

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

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

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

    Encoding Device

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

    Hybrid Storage Area Network

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

    Cloud Storage Server

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

    pStor

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

    pStor Cluster Service

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

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

11. Set the quick recording schedule for added channels.

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

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

What to do next

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

7.2 Add an Access Control Device by IP Address

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

Before You Start

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

Steps

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

ℹ️**Note**

By default, the device port is 8000.

⚠️**Caution**

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

your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

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

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

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

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

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

7.3 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.

7.3.1 Add an Area

You can add an area to manage the added resources.

Steps

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

2. Click **Area** on the left.

3. Optional: Select the parent area in the area list panel to add a sub area.

4. Click $+$ on the area list panel to open the Add Area panel.

Figure 7-1 Add an Area

5. Select the parent area to add a sub area.

6. Create a name for the area.

7. Click **Add**.

7.3.2 Add Camera to Area

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

Steps

ℹ️**Note**

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

1. In the top left corner of Home page, select ▤ → **All Modules** → **General** → **Resource Management** .
2. Click **Area** on the left.
3. Select an area for adding cameras to.
4. Select the **Camera** tab.
5. Click + on the element page to enter the Add Camera page.
6. Select the device type.
7. Select the cameras to add.
8. **Optional:** Check **Get Device's Recording Settings** to obtain the recording schedule configured on the local device and the device can start recording according to the schedule.

   ℹ️**Note**

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

9. Click **Add**.

7.3.3 Add Door to Area

You can add doors to areas for management.

Steps

ℹ️**Note**

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

1. In the top left corner of Home page, select ▤ → **All Modules** → **General** → **Resource Management** .
2. Click **Area** on the left.
3. Select an area for adding doors to in the area list panel.
4. Select the **Door** tab.
5. Click + on the element page to enter the Add Door page.
6. Select the device type.

7. Select the door(s) to add.

8. Click **Add**.

Chapter 8 Configure Event and Alarm

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

Event

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

The rule of an event includes four elements, namely, "**event source**" (i.e., the device which detects the event), "**triggering event**" (specified event type), "**what to do**" (linkage actions after this alarm is triggered), and "**when**" (during specified time period, the linkage actions can be triggered).

$\boxed{i}$**Note**

You can set linkage actions for events. 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.).

Example

The event can be defined as intrusion (**triggering event**) which happens in the bank vault and be detected by cameras mounted in the bank vault (**event source**) on weekend (**when**), and trigger the camera to start recording (**what to do**) once happened.

Alarm

Alarm is used to notify security personnel of the particular situation which helps handle the situation promptly. Alarm can trigger a series of linkage actions (e.g., popping up window on the Control Client, showing the alarm details) for notification and alarm handling. You can check the received real-time alarm message via the Control Client and search the history alarms.

The rule of an alarm includes six elements, namely, "**alarm source**" (i.e., the device which detects the triggering event), "**triggering event**" (specified event type occurred on the alarm source and triggers the alarm), "**when**" (during specified time period, the alarm can be triggered), "**recipient**" (the user in the system who can receive this alarm), "**priority**" (the priority of this alarm), and "**what to do**" (linkage actions after this alarm is triggered). Besides these five elements, you can also set other properties for this alarm such as alarm description, etc.

$\boxed{i}$**Note**

You can set linkage actions for alarms. 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.

Example

The alarm can be defined as intrusion (**triggering event**) which happens in the bank vault and be detected by cameras mounted in the bank vault (**alarm source**) on weekend (**when**), and trigger the camera to start recording (**what to do**) once happened. this alarm is marked as High priority (**priority**), and users including admin and operators (**recipient**) can receive this alarm notification and check the alarm details.

8.1 Supported Events and Alarms

Currently, the system supports events and alarms for the following types of resources:

Video

Camera

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

Alarm Input

The event or alarm triggered by the alarm input of the video device in the system.

Access Control

Door

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

Elevator

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

Alarm Input

The event or alarm triggered by the alarm input of the access control device in the system.

Person

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

Alarm

Security Radar

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

Alarm Input

The event or alarm triggered by the alarm input of the resources in the system, such as a smoke detector and zones of a security control panel.

Maintenance

The operating exceptions of the resources (e.g. camera, door, UVSS, dock station, recording server, security audit server) added to the system, such as camera offline, server exception, and so on.

User-Defined Event

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

Combined Alarm

The combined alarm added in the system.

Digital Signage

The event or alarm triggered in the Digital Signage, such as abnormal temperature and person amount more than threshold.

8.2 Add Event and Alarm

In the top left corner of Home page, select ▤ → **All Modules** → **General** → **Event & Alarm** → **Event & Alarm** and click **Add** to add an alarm or event.

Triggering Event and Source

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

Source Type

This field refers to **"event or alarm source"** in the rule, defining the specific the type of source that can trigger this event and alarm.

Triggering Event

This field refers to **"triggering event"** in the rule. The specific event type detected on the event source will trigger an event and alarm of the selected major type.

Source

This field refers to **"event or alarm source"** in the rule, defining the specific entity (such as cameras, devices, servers, etc.) which can trigger this event and alarm.

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

Threshold

If the source type you selected is **Regional People Counting**, you need to set extra conditions to define the triggering event.

Currently, you can set **Person Amount More/Less than Threshold** and **Person Amount More/ Less than Threshold (Pre-Alarm)** for people counting group. For these two alarms, you need to set the threshold which determines whether the selected people counting groups will trigger an alarm when the detected number of people stayed less than or more than the threshold.

For example, if you set the threshold as **"≥ 100 or ≤ 10"**, when the number of people detected in the selected people counting group is more than 100 or less than 10, an alarm will be triggered to notify the security personnel.

Card No.

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

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

Frequency

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

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

Vehicle Type

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

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

Color

Click the color to select the color to indicate this event or alarm, which will be displayed in the event center. You can set the color according to the emergency of this event or alarm. For example, you can set red color for the urgent alarm and set green color for the prompt event.

Ignore Recurring Events

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

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

Note

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

Delay Alarm

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

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

When

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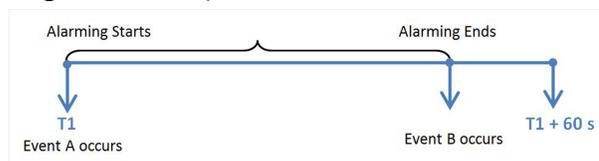
Notification Schedule

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

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

Note

For example, assume that you have set event A as start event, event B as end event, and set the value of **Auto-End Arming in** to *60 s*. Under these conditions, when event A occurs at T1, if event B occurs within 60 s , the arming schedule ends at the occurrence of event B (see the following figure Arming Schedule 1); if not, ends at 60 s after the occurrence of event A (see the following figure Arming Schedule 2).
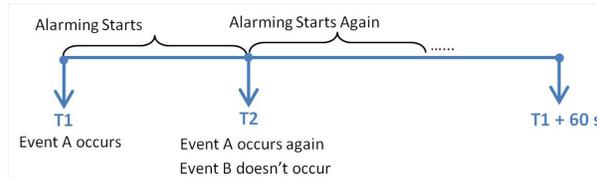

Figure 8-1 Notification Schedule 1

Figure 8-2 Notification Schedule 2

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

Figure 8-3 Notification Schedule 3

Priority

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

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

Recipient

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

Select the user to send the alarm information to and the user can receive the alarm information when he/she logs in to HikCentral Professional via the Control Client or Mobile Client.

What to Do

The fields in the Alarm Settings indicate one element in the rule: "what to do". It defines what actions the system will take to record the event and alarm details and notify security personnel.

Trigger Recording

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

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

- **Post-record:** Record video from periods following detected alarms. Specify the number of seconds which you want to record video for after the alarm stops.
- **Lock Video Files for:** Set the days for protecting the video file from being overwritten.
- **Display Video by Default:** Set the video to be displayed by default on the Control Client when receiving the triggered alarm information. You can select the recorded video or the live video to be displayed.

ⓘNote

- Make sure the related camera(s) have been configured with recording schedule.
- Up to 16 cameras can be set as related camera.

Capture Picture

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

ⓘNote

Only one camera can be set for capturing pictures.

- If the alarm source is a camera, you can set to trigger the source camera itself for capturing pictures by selecting **Source Camera**.
- To trigger other camera for capturing pictures, select **Specified Camera** and select one camera for capturing pictures.

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

Figure 8-4 Capture Pictures

ⓘNote

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

Create Tag

Select the cameras to record video when the event occurs and set the storage location for storing the video files. The system will add a tag to the event triggered video footage for convenient search. The tagged video can be searched and checked via the Control Client.

- If the event source is a camera, you can set to trigger the source camera itself for tagged recording by selecting **Source Camera**.
- To trigger other cameras for tagged recording, select **Specified Camera** and click **Add** to add other cameras.

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

Set the time range to define the tagged length of the video footage. For example, you can set to record the tagged video started from 5 seconds before the event and lasted until10 seconds after the event. The tagged video can be searched and checked via the Control Client.

Add the description to the tagged video as needed.

Restrict Alarm Handling Time

When the alarm is triggered, you need to handle the alarm on the Control Client. Enable this function to trigger user-defined event(s) or alarm output(s) if the alarm is not handled within the configured alarm handling time.

ⓘNote

Up to 16 user-defined events and alarm outputs can be set as the triggered event when handling alarm timed out.

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 alarm 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 intrusion of suspicious person is detected.

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

Link Alarm Input

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

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

Link Alarm Output

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

> **⌐Ꭵ⌐Note**
>
> Up to 64 alarm outputs can be selected as event linkage.

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

Trigger PTZ

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

> **⌐Ꭵ⌐Note**
>
> Up to 64 PTZ linkages can be selected as event linkage.

Link Third-Party Integrated Resource

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

Send Email

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

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

Attach with Entry & Exit Counting

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

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

Trigger User-Defined Event

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

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

You can also click **Add New** below to set a new user-defined event(s).

> **⌐Ꭵ⌐Note**
>
> Up to 16 user-defined events can be selected as alarm linkage.

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.

Related Map

Select a map to show the alarm information and you should add the camera to the map as a hot spot.

Trigger Audible Warning

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

⃞ⁱNote

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

Chapter 9 Manage Person

You can add person information to the system for further operations such as access control (adding the person to access group), face comparison (adding the person to face comparison group), time and attendance (adding the person to attendance group), etc. After adding the persons, you can edit and delete the person information if needed.

9.1 Add Person Group

When there are a large number of persons managed in the system, you can put the persons in different person groups. For example, you can group employees of a company to different departments.

Steps

⛶i Note

The person groups (including group quantity) being viewed by different users are different. You can go to **General → Security → Roles** to edit the role assigned to the user. Click a role, select **Permission Settings → Resource Access → Person Group** , and check the person group(s) that will be viewed by the selected role.

1. In the top left corner of Home page, select 🟥 **→ All Modules → General → Person** to enter the person page.
2. Click ＋ to enter the Add Person Group page.
3. Set person group information, including parent group, group name, etc.
4. Confirm to add the person group.
   - Click **Add** to finish adding the current person group and go back to person group page.
   - Click **Add and Add Person** to finish adding the current person group and continue to add other person groups.

9.2 Add a Person

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

Steps
1. In the top left corner of Home page, select 🟥 **→ All Modules → General → Person** .
2. Click **Add** to enter the adding person page.
3. Set basic information for the person.

   ID

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

⬚**Note**

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

Person Group

Select a person group for the person.

⬚**Note**

See **Add Person Group** for details about adding a person group.

Person Picture

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

From Device

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

⬚**Note**

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

Take a Picture

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

Upload Picture

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

⬚**Note**

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

Skin-surface Temperature

Enter the person's skin-surface temperature and select the corresponding temperature status.

> **ⓘNote**
>
> For example, if a person's skin-surface temperature is 37℃, then you can select her/his temperature status as normal.

Effective Period

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

Super User

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

Extended Access

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

> **ⓘNote**
>
> The extended access and super user functions cannot be enabled concurrently.

PIN Code

The PIN code must be used after card or fingerprint when accessing. It cannot be used independently.

> **ⓘNote**
>
> It should contain 1 to 8 digits.

4. **Optional:** Set access control and elevator control permission for the person to define which access point(s) the person can access in the authorized period.
   1) Click **Relate**.
   2) Select one or more access levels for the person.
   3) Click **Add** to add the person to the selected access level(s).

> **ⓘNote**
>
> You can click 📄 to view its access point(s) and access schedule.

5. **Optional:** View shift schedule of the person in the table.

> **ⓘNote**
>
> You can click ‹ or › to switch the time (month).

6. **Optional:** Add the person to the existing face comparison group(s) which will be used for face recognition and comparison.

⌐i⌐Note

After adding the person to the face comparison group, you should apply the face comparison group to a device to make the settings effective.

---

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

⌐i⌐Note

By default, the login password is 123456.

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

8. Set resident information to link the person with the indoor station and room number.

⌐i⌐Note

Make sure the room number is consistent with the actual location information of the indoor station.

---

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

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

Chapter 10 Manage Access Control and Elevator Control

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

On the Web Client, the administrator can add access control devices, elevator control devices, and video intercom 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.

10.1 Manage Access Level

In access control, access level is a group of doors and floors. Assigning access level to persons, person groups, or access groups can define the access permission that which persons can get access to which doors and floors during the authorized time period.

10.1.1 Add Access Level

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

Steps
1. In the top left corner of Home page, select ▤ → **All Modules** → **Access Control** → **Access Level** .
2. Click **Add** to enter the Add Access Level page.
3. Create a name for the access level.
4. **Optional:** Edit the description for the access level.
5. Select the access point(s) to add to the access level.
   1) In the **Available** list, select the access point(s) you want to add to the system and click ⟩ . You can view your selection in the **Selected** list.
   2) **Optional:** In the **Selected** list, select the access point(s) that you no longer want to add to the system, and click ⟨ to undo selection.
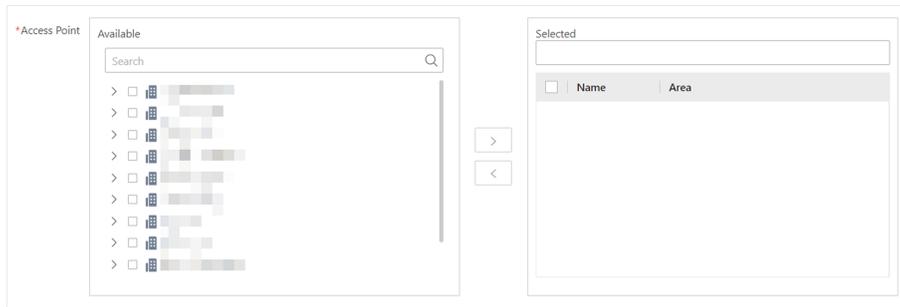
Figure 10-1 Select Access Points

6. Select an access schedule to define in which time period, persons are authorized to access the access points you select in the previous step.
7. Click **Add** to add the access level and return to the access level management page.

What to do next
You need to assign the access level to persons, so that the assignees can have the access to the access points in the access level according to the access schedule.

10.1.2 Assign Access Level to Persons

You can assign an access level to multiple persons so that the assigned persons can have the access to the access points in the access level.

Before You Start
• Make sure you have added access levels to the system. For details, refer to ***Add Access Level*** .
• Make sure you have added persons to the system. For details, refer to ***Manage Person*** .

Steps
1. In the top left corner of Home page, select ▤ → **All Modules → Access Control → Access Level** .
2. Click **Assign by Access Level** on the left.
3. Click on the access level that you want to assign to persons.
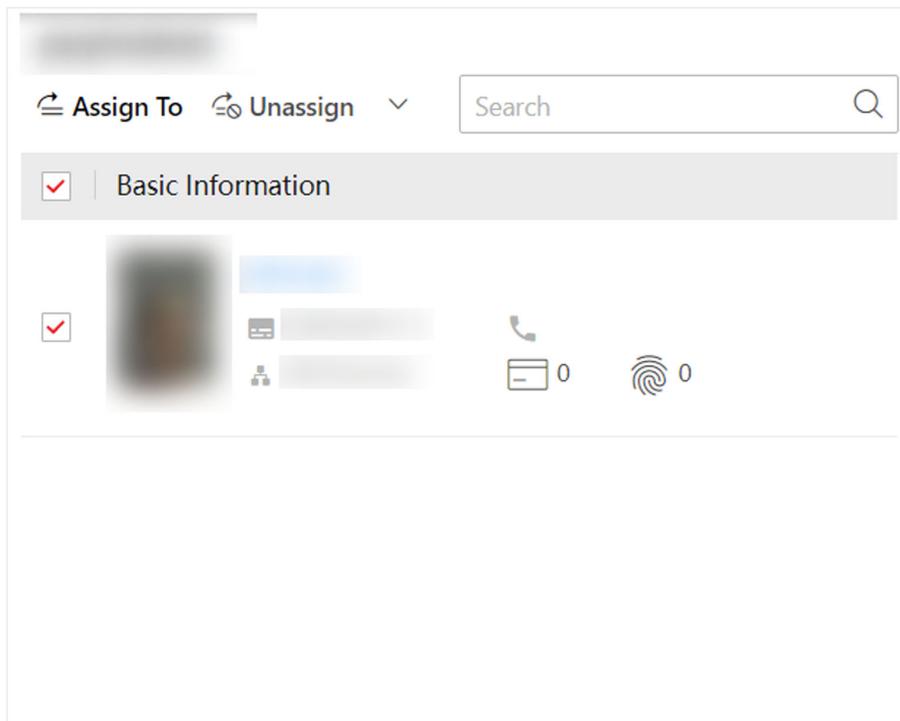
Figure 10-2 Assignee Panel

4. On the assignee panel, click **Assign To** to show person list.
5. Select the persons whom you want to assign the access level to and click **Add**.
6. Do one of the following to apply access level settings to devices.
   - In the pop-up window, click **Apply Now** to apply the settings immediately.
   - In the pop-up window, click **Apply Later**. When ready, click 🗐 to apply the settings. You can also set a schedule to apply automatically.

What to do next
Test your access control configurations and devices before putting them into use.

Chapter 11 Manage Role and User

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

11.1 Add Role

Role is a group of platform permissions. You can add roles and assign permissions to roles, so that users can be assigned with different roles to get different permissions.

Steps

$\boxed{i}$**Note**

The platform has predefined two default roles: Administrator and Operator. You can click the role name to view details. The two default roles cannot be edited or deleted.

Administrator

Role that has all permissions of the platform.

Operator

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

1. Click **Add**.

Figure 11-1 Add Role Page

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

Copy from

Copy all settings from an existing role.

Effective Period

Set the time range within which the role takes effect. The role is inactive outside the effective period.

Permission Schedule Template

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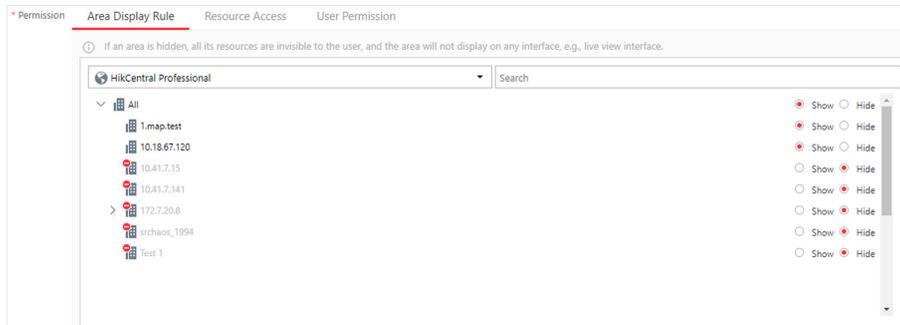

ⓘNote

- When role expires or the role's permission is invalid after editing the permission schedule, users assigned with the role will be forced to log out and not able to log in.
- The permission schedule's time zone is consistent with that of the platform.
- By default, the role will be linked with All-day Template after updating the platform.

---

3. Configure permission settings for the role.

Area Display Rule

Show or hide specific area(s) for the role. If an area is hidden, the user assigned with the role cannot see and access the area and its resources.

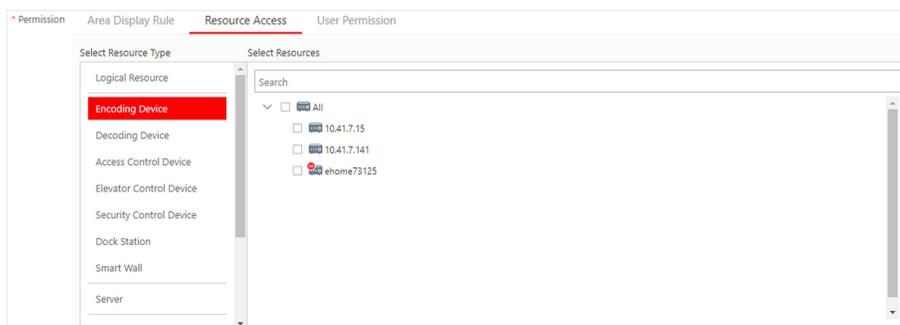**Figure 11-2 Area Display Rule**

Resource Access Permission

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

ℹ️**Note**

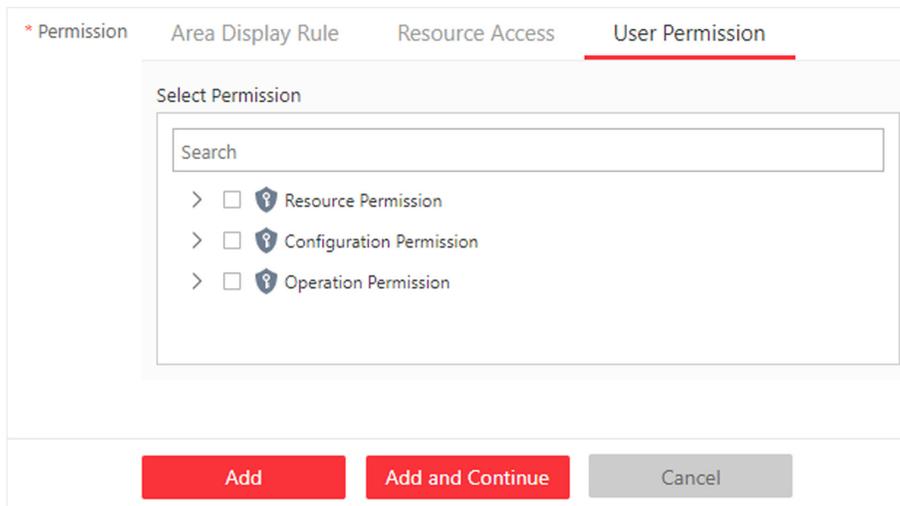If you do not check the resources, the resource permission cannot be applied to the role.

**Figure 11-3 Resource Access Permission**

User Permission

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

Figure 11-4 User Permission

ⓘNote

In **Resource Permission**, you can set time restriction for video playback permission. Once set, the role's permission of viewing and downloading video playback will be restricted within the configured time period. For example, if you set restriction for recent video to 6 minutes, the role can only view video playback of the last 6 minutes.
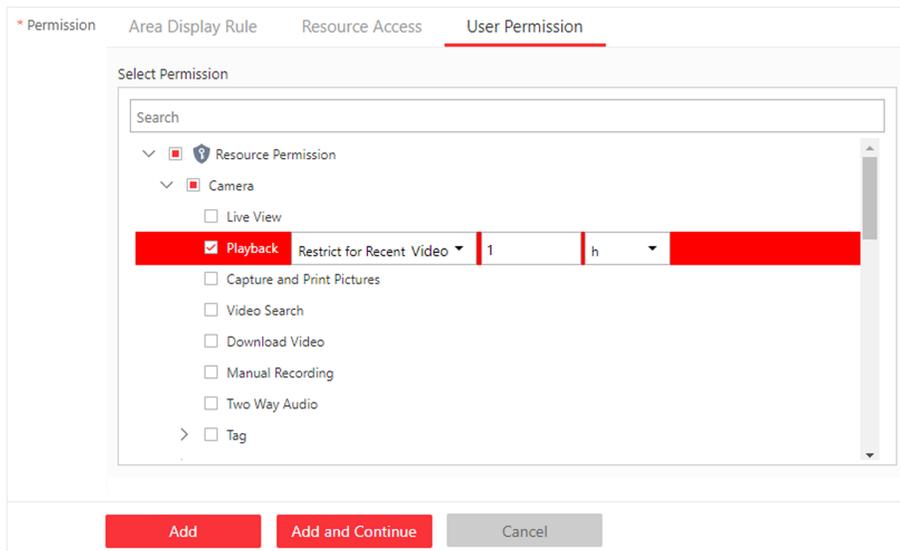
Figure 11-5 Playback Permission

4. Do one of the following to complete adding the role.
- Click **Add** to add the role and return to the role management page.
- Click **Add and Continue** to save the settings and continue to add another role.

11.2 Add Normal User

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

Steps
1. In the top left corner of Home page, select ▤ → **All Modules** → **General** → **Security** .
2. Click **Add**.
3. Set basic information for the user.

   User Name

   Can contain letters (a-z, A-Z), digits (0-9), and "-" only.

   Password

   Create an initial password for the user. The user will be asked to change the password when logging in for first time.

   ⎙**Note**

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

   Expiry Date

   The date when the user account becomes invalid.

   Email

   The system can notify user by sending an email to the email address. The user can also reset the password via email.

   ⎙**Note**

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

   User Status

   If you select **Inactive**, the user account will be inactivated until you activate it.

   Restrict Concurrent Logins

   To limit the maximum IP addresses logged in to the system using the user account, switch on **Restrict Concurrent Logins** and set the maximum number of concurrent logins.
4. Configure permission settings for the user.

   PTZ Control Permission

Set the permission level (1-100) for PTZ control. The larger the value is, the higher permission level the user has. The user with higher permission level has the priority to control the PTZ of a camera.

Automatically Receive Alarm

Switch on and users with this role will receive resource alarms no matter configured as recipients of each alarm individually or not.

Assign Role

Select the roles that you want to assign to the user.

5. Do one of the following to complete adding the user.
   - Click **Add** to add the user and return to the user management page.
   - Click **Add and Continue** to save the settings and continue to add another user.

See Far, Go Further