HikCentral Quick Start Guide

Contents

Chapter 1 Guide Content

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

To ensure the properness of usage and stability of the HikCentral system, 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, clients, and software, 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 Installation

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

Two installation packages are available for building your system.

Basic Installation Package:

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

Control Client Installation Package:

Contains the Control Client module only.

Here we introduce the procedure for installing the basic installation package. For Control Client installation package, you can install them by following the installation instructions.

Note

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

We introduce the typical installation method here, where HikCentral VSM Service and Control Client will be installed on the same PC or server. For installing service modules and clients on different servers or PCs, please refer to the *User Manual of HikCentral Web Client.*

3.1 System Requirements

3.1.1 System Requirements for Servers

Server without Remote Site Management (RSM) Module

- **Operating System:** Microsoft® Windows 7 (64-bit), Windows 8 (64-bit), Windows 8.1 (64-bit), Windows 10 (64-bit), Windows Server 2008 R2 (64-bit), Windows Server 2012 (64-bit), Windows Server 2016 (64-bit)
- **CPU:** Intel® Xeon® E3-1220 V5 @ 3.00 GHz
- **Memory:** 16 GB
- **HDD:** Enterprise-class SATA disk with 601 GB storage capacity
- **Network Controller:** RJ45 Gigabit self-adaptive Ethernet interfaces

Server with Remote Site Management (RSM) Module

- **Operating System:** Microsoft® Windows 7 (64-bit), Windows 8 (64-bit), Windows 8.1 (64-bit), Windows 10 (64-bit), Windows Server 2008 R2 (64-bit), Windows Server 2012 (64-bit), Windows Server 2016 (64-bit)
- **CPU:** Intel® Xeon® E5-2620 V4 @ 2.10 GHz
- **Memory:** 16 GB

- **HDD:** Enterprise-class SATA disk with 601 GB storage capacity
- **Network Controller:** RJ45 Gigabit self-adaptive Ethernet interfaces

3.1.2 System Requirements for Control Client

- **Operating System:** Microsoft® Windows 7 (32/64-bit), Windows 8 (32/64-bit), Windows 8.1 (32/64-bit), Windows 10 (64-bit), Windows Server 2008 R2 (64-bit), Windows Server 2012 (64-bit), Windows Server 2016 (64-bit)
- **CPU:** Intel® Core™ i5-4590 @ 3.3 GHz and above
- **Memory:** 8 GB and above
- **Video Card:** NVIDIA® Geforce GTX 970 and above

3.2 Install Service Module in Typical Mode

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

Perform this task when you want to install service module in typical mode.

Steps

1. Double-click (HikCentral) 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 if you select to install VSM 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 VSM 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 VSM 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.

Chapter 4 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.

4.1 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 32 and above (32-bit), Google Chrome 35 and above (32-bit)

Note

You should run the web browser as administrator.

4.2 Log into the Web Client for the First Time

By default, the system predefined the administrator user named admin. When you log in 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.

Perform this task when you access the system for the first time.

Steps

1. In the address bar of the web browser, input the address of the PC running VSM (Video Surveillance Management Service) and press **Enter** key.

   Example

   If the IP address of PC running VSM is 172.6.21.96, and you should enter http://172.6.21.96 in the address bar.

Note

You should configure the VSM's IP address in WAN Access of System Configuration before accessing the VSM via WAN.

2. When you login via current Internet Explorer browser for the first time, you should install the plug-in before you can access the functions.
   1) Click **OK** in the pop-up dialog to install the plug-in.
   2) Save the plug-in file to your PC and close the web browser.
   3) Find the plug-in that stores on your PC and install the plug-in according to the prompt.
   4) Re-open the web browser and log in to the system (step 1).
3. Input the password and confirm password for the admin user in the pop-up Create Password window.

Note

The password strength can be checked by the system and should meet the system requirements. The default minimum password strength should be **Medium**.

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.

4. 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 5 Manage License

After you install HikCentral, you have a temporary License for a specified number of cameras and limited functions. To ensure the proper use of HikCentral, you can activate the VSM to access more functions and manage more devices. If you do not want to activate the VSM now, you can skip this chapter and perform this operation later.

Two types of License are available for HikCentral:

- **Base:** You need to purchase at least one basic License to activate HikCentral.
- **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 Web Client*.

5.1 Activate License - Online

Input the activation code received when you purchase your License for activation.

If the VSM to be activated can properly connect to the Internet, you can perform the following steps to activate the License.

Steps

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

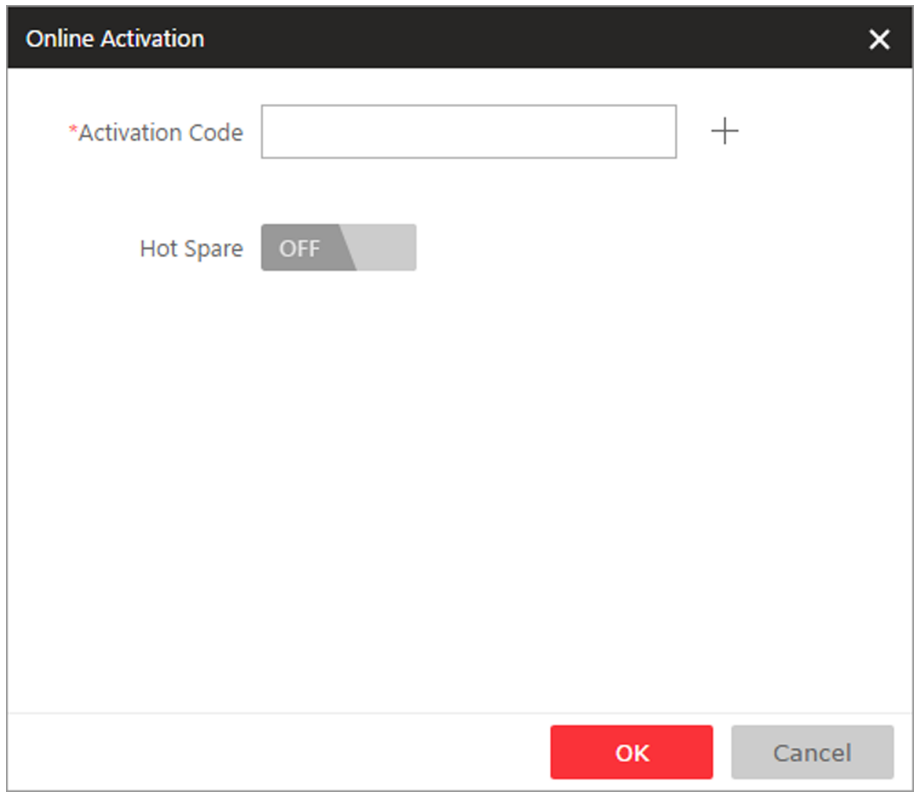

Figure 5-1 License Configuration Window

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

Note

- At least one basic License is required for activating the system.
- If you have purchased more than one License, you can click + and input 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, select the **I accept the terms of the agreement** checkbox and click **OK** to continue.
   - If you do not accept the agreement, click **Cancel** to cancel the activation.

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

5.2 Activate License - Offline

If the VSM to be activated cannot connect to the Internet, you can perform the following steps to activate the License.

Perform this task when you need to activate license offline.

Note

You must enter HIKVISION's website (http://overseas.hikvision.com/) and go to **VMS → VMS Support → License Management** , click **NEW USER** and register an account.

Steps

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

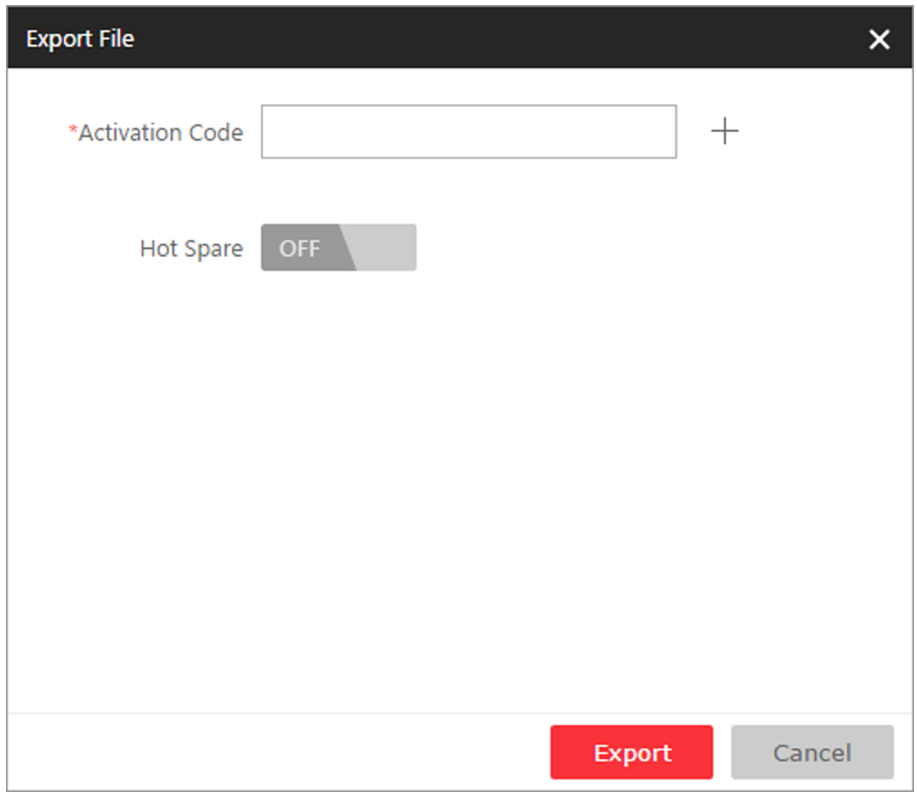

Figure 5-2 License Configuration Window

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

   Note

   If you have purchased more than one License, you can click + and input 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 Hikvision's technical support engineers.

5. Click **Export** and save the request file to the proper directory or the removable storage medium (e.g., USB flash disk).
6. Copy the request file to the PC that can connect to the Internet.

Note

If the PC accessing HikCentral via the Web Client can connect to the Internet, you can skip this step.

7. Enter HIKVISION's website (http://overseas.hikvision.com/) and go to **VMS → VMS Support → License Management** page,
8. Login to your account.
9. Select **How to Activate Your Account** and click **Browse** at the bottom of the page to select the license request file exported in step 5.
10. In the pop-up dialog, click **Download** to download the generated activation file and set the name and saving path.
11. Save the activation file to the proper directory of the PC that accesses HikCentral via the Web Client.
12. In the License configuration window, click **Import the activation file** to import the activation file and the License Agreement dialog opens.
13. Read the License Agreement.
    - If you accept the terms of the license agreement, select the **I accept the terms of the agreement** checkbox and click **OK** to continue.
    - If you do not accept the agreement, click **Cancel** to cancel the activation.

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

Chapter 6 Manage Resource

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, ect., 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 Web Client*.

6.1 Add Device by IP Address or Domain Name

When you know the IP address or domain name of the device to add, you can add the devices to your system by specifying the IP address (or domain name), user name, password, and other related parameters.

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 via network.

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

Steps

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

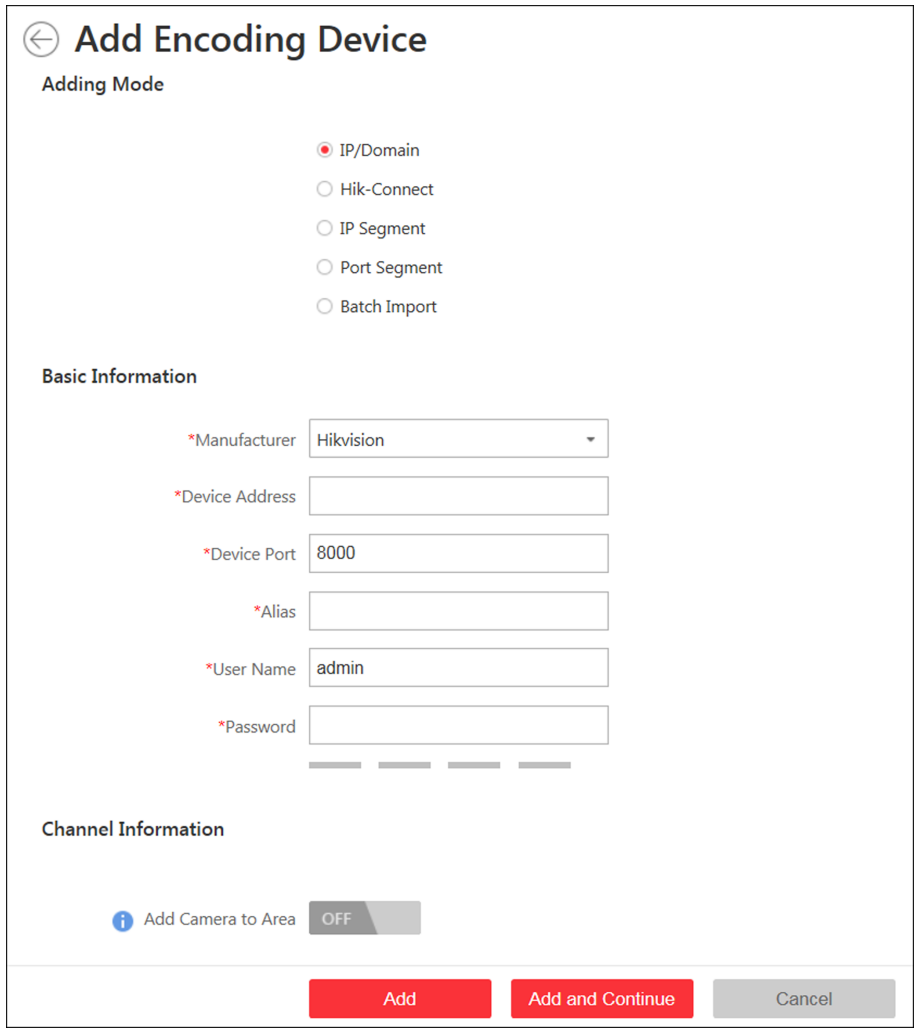

Figure 6-1 Add Encoding Device Page

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

Note

By default, the device port No. is 8000.

Caution

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

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

5. **Optional:** Set the **Add Camera to Area** switch to ON to import the cameras of the added devices to an area.

   Note

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

6. **Optional:** If you choose to add cameras to area, check the **Synchronize Camera Name** checkbox to get the camera name from the device.
7. **Optional:** If you choose to add cameras to area, enable the **Video Storage** function and select the storage location for recording. Here we only introduce storing the videos in the added encoding device.

   Encoding Device

   The video files will be stored in the device according to the configured recording schedule.
8. Set the quick recording schedule for added cameras.
   - Check the **Get Device's Recording Settings** checkbox to get the recording schedule from the device and the recording task of the cameras of the device will automatically perform according to schedule.
   - Uncheck the **Get Device's Recording Settings** and set the required information such as recording schedule template, stream type, pre-record, etc.
9. Finish adding the device.
   - Click **Add** to add the encoding device and back to the decoding device list page.
   - Click **Add and Continue** to save the settings and continue to add other encoding devices.

6.2 Manage Area

You should organize the added cameras, doors, alarm inputs, alarm outputs, Under Vehicle Surveillance Systems (UVSSs) into areas for the convenient management. You can get the live view, play back the video files, and do some other operations of the devices after managing the devices by areas.

6.2.1 Add Area

You can add area to manage the devices.

Perform this task when you need to add an area.

Steps

1. Click **Logical View** on the Home page to enter the Area Management page.
2. 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 6-2 Adding Area Icon

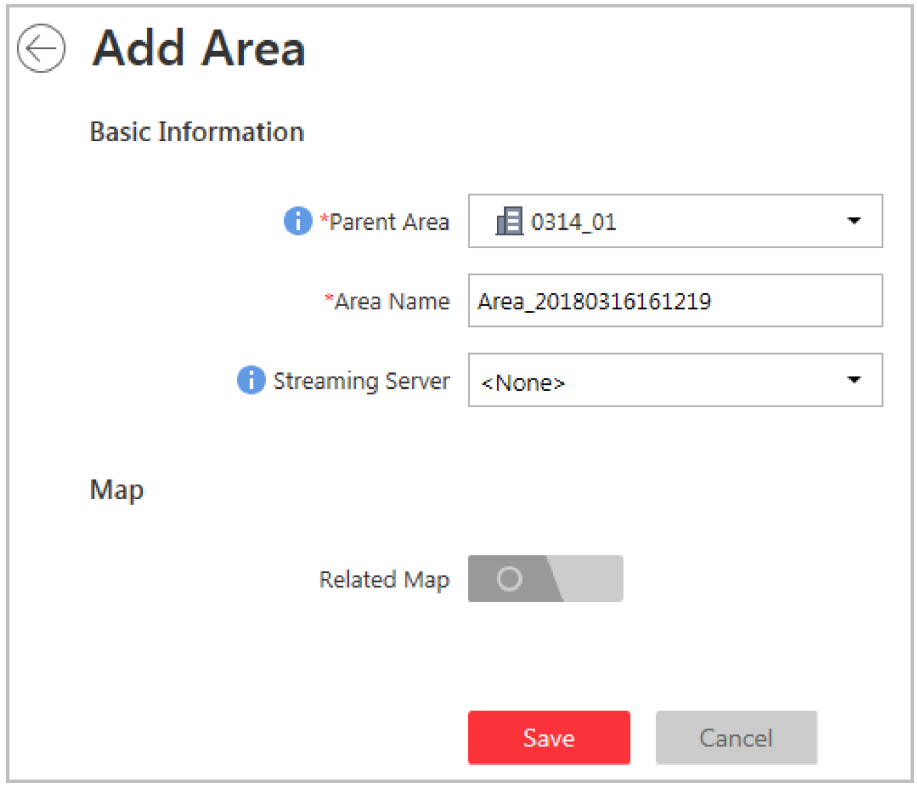

Figure 6-3 Add Area

4. Create a name for the area.
5. Click **Save**.

6.2.2 Add Camera to Area

You can add elements including cameras, alarm inputs, alarm outputs, doors, and under vehicle surveillance systems into areas for management. Here we take adding the cameras to the area as an example.

Perform this task when you need to add cameras to areas.

Steps

Note

Cameras can only belong to one area. You cannot add one 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 cameras to add.
6. **Optional:** Check **Synchronize Camera Name** to get the camera name from the device.

   Note

   You can only synchronize the camera name of online HIKVISION camera.

7. **Optional:** Check **Get Device's Recording Settings** to obtain the recording schedule configured on the local device and the recording task will automatically perform according to schedule.

   Note

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

8. Click **Add**.

Chapter 7 Configure Recording for Cameras

For the cameras, HikCentral provides three storage methods (storing on encoding devices, Hybrid Storage Area Network, or Cloud Storage Server) for storing the video files of the cameras according to the configured recording schedule.

Perform this task when you need to record videos for the cameras.

Steps

Note

- In this document, we only cover the method of storing video files of cameras on the encoding devices. For the configuration of storing the video files on other location, refer to the *User Manual of HikCentral Web Client*.
- If the recording schedule was imported from the device upon adding it to HikCentral, this section should be skipped.

1. Enter the recording setting page.
   1) Click **Logical View → Cameras** to enter the area management page.
   2) Select an area to show its cameras.
   3) Select a camera and click the **Name** field to enter the Edit Camera page.

   In the Recording Setting area, you can modify the configured schedule or enable the function to add a new one.

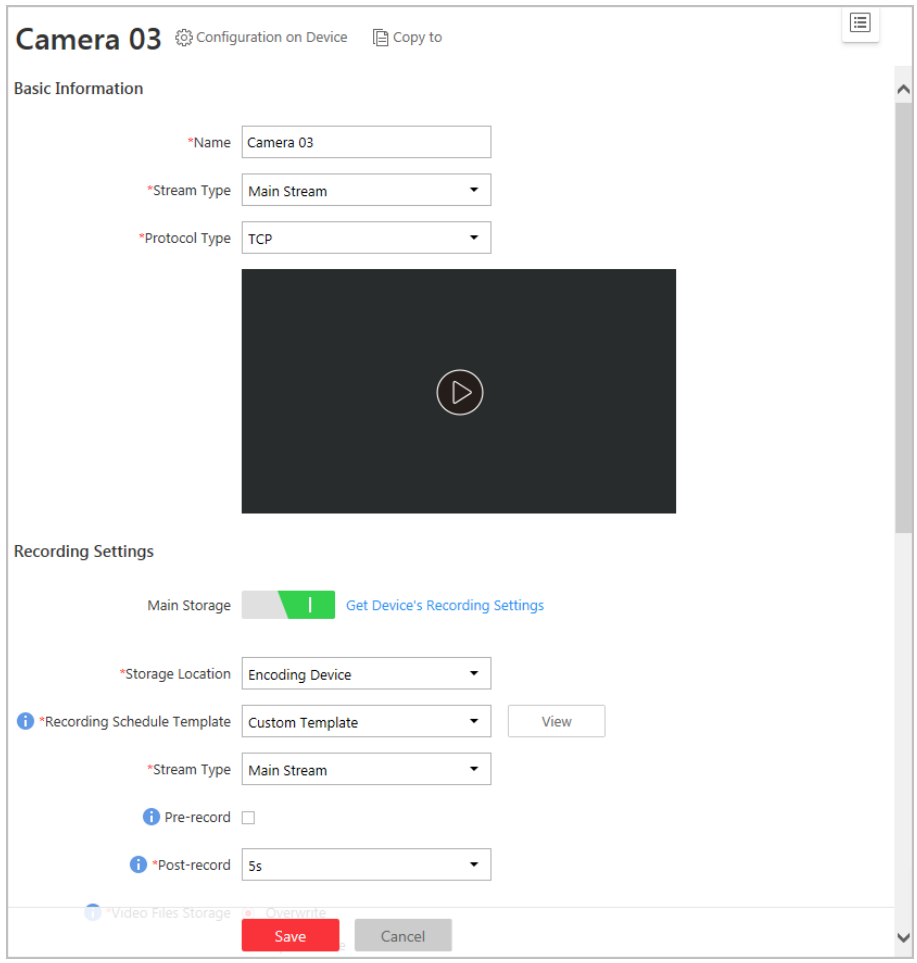

Figure 7-1 Edit Camera Page

2. Set the switch of **Main Storage** to ON and set the main storage location.
3. Select the storage location for storing the recorded video file on the encoding device.
4. Set the template which defines when to record the camera's video.
   - Select the template as all-day time-based template or all-day event-based template.

     All-Day Time-Based Template

     Record the video for all-day continuously.

     All-Day Event-Based Template

     Record the video when alarm occurs.
   - Click **Add New** to set a customized template.
5. Select the stream type for recording the video.
6. Set the pre-record and post-record for recording the video.

   Pre-Record

   Record video from periods preceding detected events.

Note

- The value of the pre-record period is not editable.
- This field is available for the camera that is configured with event-based recording.

Post-Record

Record video from periods following detected events.

7. In the Video Files Storage field, select the storage mode for the recorded videos.
Overwrite

Overwrite the oldest videos when disk or allocated quota is full.

Expired Time

Automatically delete the oldest videos after the specified retention period. This method allows you to define the longest time period to keep the videos as desired and the actual retention period for the videos depends on the allocated quota.

8. Click **Save** to complete adding the recording settings.

Chapter 8 Live View and Playback

After adding the encoding devices to the system, grouping the cameras into areas, and setting recording schedule for the cameras, you can perform live view and playback via the Control Client to view the live video and recorded video files of the added cameras.

8.1 Log into the Control Client for the First Time

When normal user (except admin user) logs in to the system for the first time, he/she should change the initial password and set a new password for login.

Before You Start

When you log in the system for the first time, you are required to create the password for the system pre-defined the administrator user (named admin) on Web Client before you can properly configure and operate the system.

Perform the following steps when you access the system via Control Client for the first time as normal user (except admin).

Steps

1. Double-click on the desktop to run the Control Client.

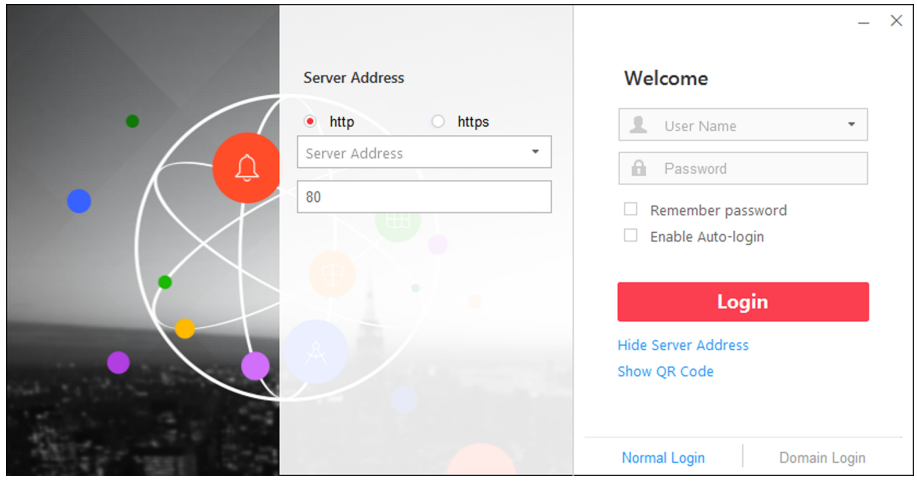

Figure 8-1 Login Page

2. Select **Normal Login** tab on the bottom.
3. Input the server parameters.

Note

You can click **Hide Server Address** or **Show Server Address** to hide or show the panel.

Transfer Protocol

Select the transfer protocol. You can select **HTTP** or **HTTPS** as configured on the Web Client.

Server Address

Input the address (IP address or domain name) of the VSM that you want to connect to.

Port

Input the port No. of the VSM. By default, it's 80 for HTTP and 443 for HTTPS.

4. Input the user name and password of the VSM server.

Note

Contact the administrator for the user name and initial password.

5. Click **Login**.
6. Click **Close** in the pop-up dialog to continue.
7. Set the new password and confirm the password.

Caution

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

8. Click **Login** to change the password.

   You enter the Control Client home page after you change the password.

8.2 Start Live View

Live view shows you the live video getting from cameras.

Before You Start

Make sure camera already added in Web Client. The correspondence of a camera to area is also configured in Web Client.

Steps

1. Click **Monitoring** to enter the Monitoring module.

   The live view or playback page will display according to previous operation on this page.
2. **Optional:** Click **Go to Live View** at the bottom to enter the live view page, if the playback page displays.
3. Click to enter Camera/ Area mode.
4. Start live view.

For one camera	Drag the selected camera to the display window. Or double-click the camera name to start the live view in a free display window. You also can select a display window and double-click the camera name to start live view in this window.
For all cameras of the same area	Double-click the area name after selecting the display window to start live view. Or you can click-and-drag the area to the display window, and click **Play in Batch** to start the live view.

You can click-and-drag the video of the camera in live view to another display window if needed.

Note

The display windows adapt to the number of cameras in the area.

8.3 Normal Playback

After configuring the recording settings for the camera via the Web Client, the video files can be searched and played back remotely.

Note

Here we only introduce the playback of continuous video files. For other operations, please refer to the *User Manual of HikCentral Control Client*.

8.3.1 Search Video File

You can search video files for normal playback.

Perform this when you need to search a specific video files.

Steps

1. Enter the Monitoring module.

   The live view or playback page will display according to previous operation on this page.
2. **Optional:** Click **Go to Playback** at the bottom to enter the playback page, if the live view page displays.

   Note

   The playback window supports up to 16 channels. If exceeding the limit in live video display window, select the channels within 16 before switching to playback.

   The playback window will play today's recording of the selected channel in live view window.
3. **Optional:** Drag the camera or area to the display window, or double-click the camera or area to play the recording of the specified camera(s) in selected window.
4. Click on the toolbar to set the date and time to search video files by time.

Note

In the calendar, the date with video files will be marked with a triangle.

After selecting the date and time, the matched video files will start playing in the display window.

8.3.2 Play Video File

After searching the video files for the normal playback, you can play the video via timeline or thumbnails.

Perform this task when you need to play the video files.

Steps

1. Click **Monitoring** to enter the Monitoring module.

   The live view or playback page displays.

2. **Optional:** Click **Go to Playback** at the bottom to enter the playback page, if the live view page displays.

   The playback window will play today's recording of the selected channel in live view window.

3. Select a date with videos to start playing video and show the timeline after searching the video files.

   Note

   The timeline indicates the time duration for the video files, and the video files of different types are color coded.

4. Play video in specified time period by timeline or thumbnails.
   - Drag the timeline forward or backward to position the desired video segment.
   - Move the cursor over the timeline to take a quick view of video thumbnails (if supported by the device) and click the appearing thumbnail to play the specific video segment.

Chapter 9 Configure Event and Alarm

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

Note

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 Web Client*.

9.1 Add Motion Detection Event for Camera

The camera exception types vary according to the connected device. In the following example, we will introduce the motion detection settings. Motion detection events are triggered when the camera detects motion within its defined area. For the settings of other camera exception types (e.g., video loss, video tampering), refer to the User Manual of the connected devices.

Perform this task when you need to configure a motion detection event for the camera added in the system.

Steps

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

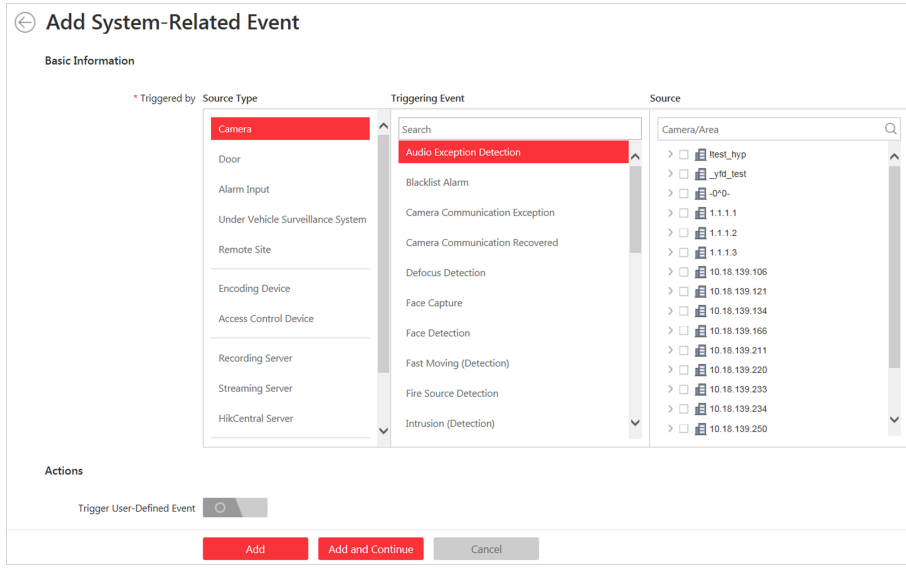

Figure 9-1 Add a System-Related Event

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

Source Type

The resource type of the event source. Select **Camera** as the source type.

Triggering Event

The event detected on the event source and it will trigger the system-related event in the system. Select **Motion Detection** as the triggering event.

Note

The triggering event varies with the selected source type.

Source

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

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

   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 Motion Detection Alarm for Camera

After configuring the event, you can configure the alarm (here we still take the motion detection alarm as an example) for trigger actions for notification. For exmaple, HikCentral can send notification email to designated recipient when motion is detected.

Perform this task when you need to configure a motion detection alarm for the added cameras.

Steps

1. Click **Event & Alarm → Alarm → Add** to enter the adding alarm page.

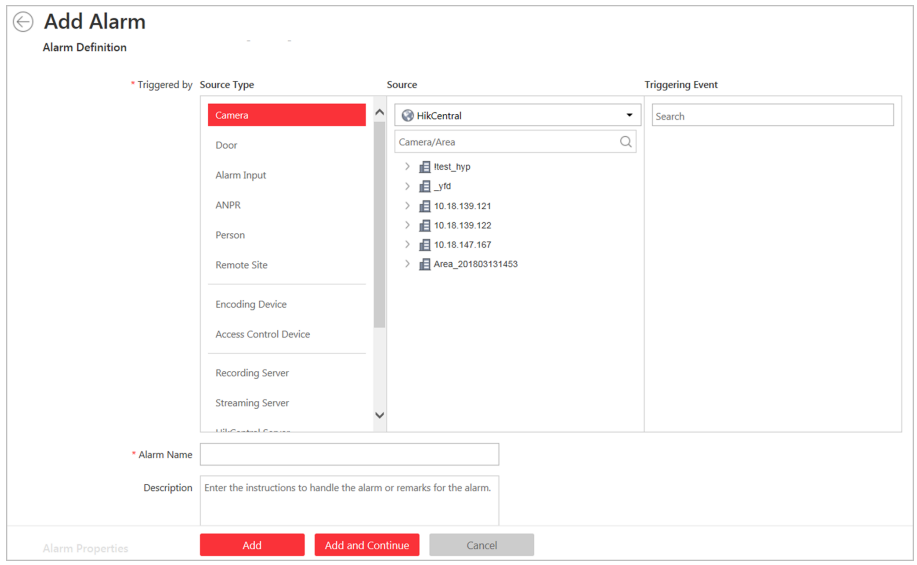

Figure 9-2 Add Alarm for Camera

2. Set the source type as **Camera** in the **Triggered by** field.
3. Select the specific camera and triggering event as the source for triggering the alarm.

Note

If the event is not properly configured on the device, **Disabled On Device** appears under the event type. You can click and set the parameters for the event in the pop-up interface. For detailed settings about the event configuration, please refer to the user manual of the device.

4. Configure the alarm definition including alarm name and description.
5. 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. Select an arming schedule template for the alarm to define when the alarm can be triggered.

Alarm Priority

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

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 via Control Client or Mobile Client.

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 the recorded video files when alarm occurs in the Alarm Center of Control Client. You can select the storage location for storing the video files.

Lock Video Files for

Set the days for protecting the video file from being overwritten.

Trigger Pop-up Window

Pop up the alarm window on Control Client to display the alarm details and all the alarm related cameras' live videos and playback when alarm occurs.

6. Set the alarm linkage actions.

Trigger Audible Warning

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

Link Alarm Output

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

Trigger PTZ

Call the preset, patrol or pattern of the selected camera(s) when alarm is triggered.

Create Tag

Add tag to the alarm triggered video if you have selected cameras in **Related Cameras** field, and the tagged video can be searched and checked via Control Client.

Send Email

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

7. 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.

   After adding the alarm, it displays on the alarm list, and you can view the alarm name and alarm status.

9.3 Search Camera Event/Alarm Logs

You can search the event and alarm log files of the added resource for checking.

Perform this task when you need to search event or alarm logs.

Steps

1. Log into the Control Client.
2. Enter the Alarm & Event Search module and click the **Alarm Search** or **Event Search** tab.
3. Select the types of event source as **Camera**.
4. Set search conditions for different event source types.
5. Set the time range for search.
6. Click **Search**.

   The matched event or alarm logs display on the list.

Chapter 10 Manage Role and User

The Security page allows you to add and delete users, 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 link with many different roles.

10.1 Add Role

You can assign the permissions to the roles as required, and the user can link to the role to obtain different permissions.

Perform this task when you add role.

Steps

1. On the Web Client, 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.

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

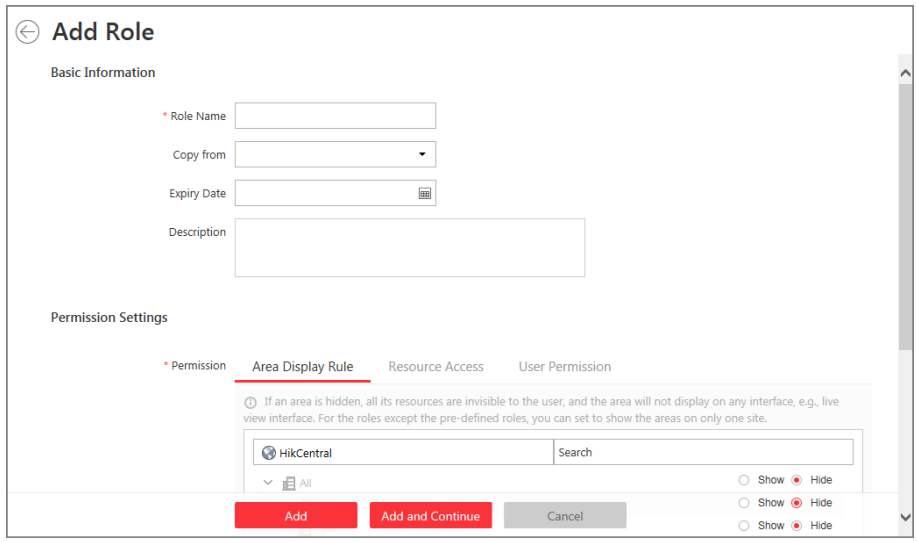

Figure 10-1 Add Role Page

3. Set the role name, expiry date, and description as desired.

Expiry Date

The date that this role becomes invalid.

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.

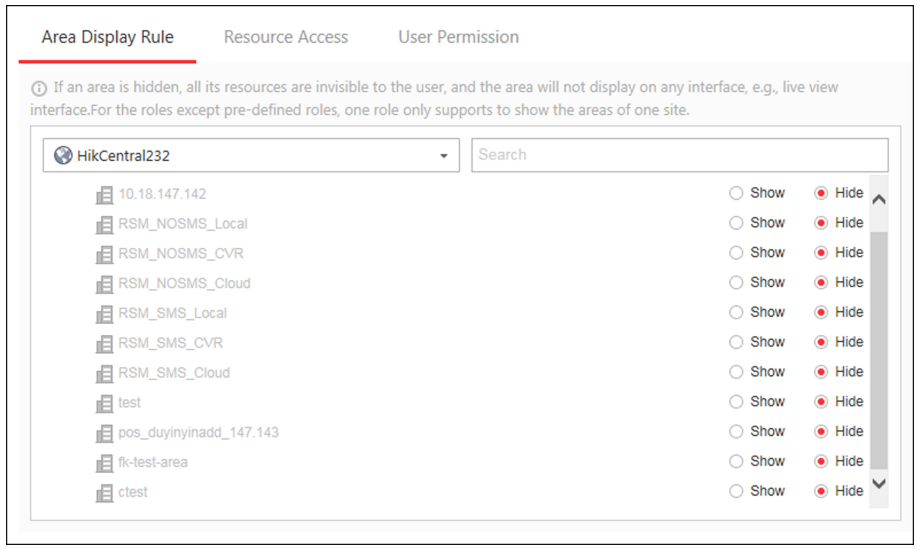

Figure 10-2 Area Display Role

Resource Permission

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

Note

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

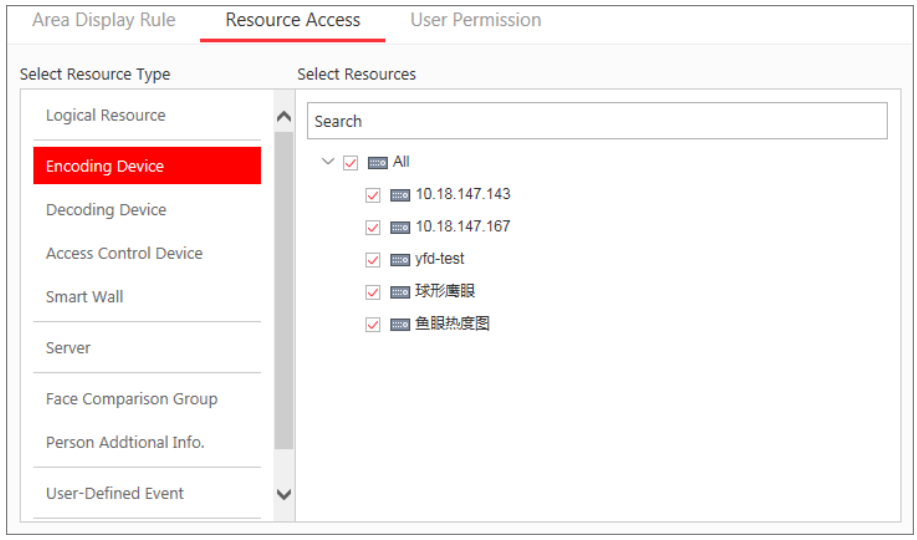

Figure 10-3 Resource Permission

User Permission

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

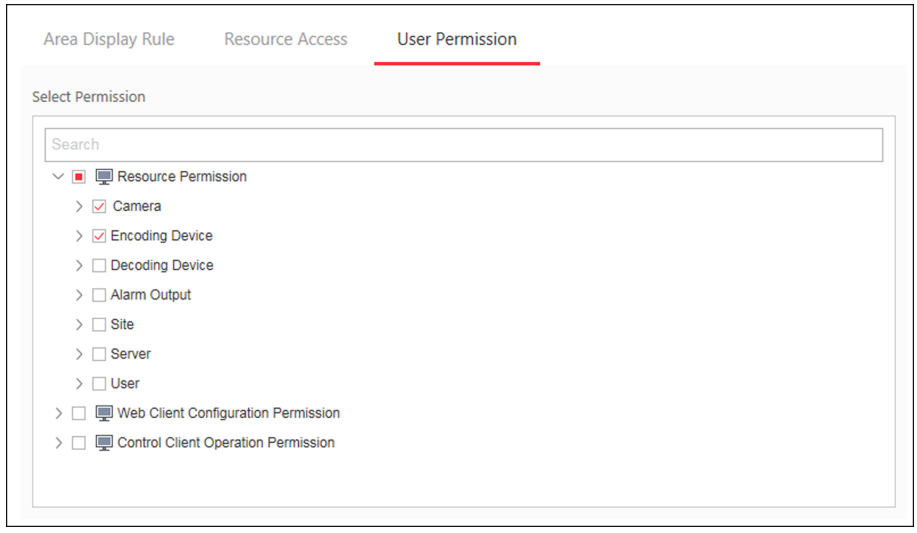

Figure 10-4 User Permission

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

10.2 Add Normal User

You can add normal users for accessing the system and assign role to the normal user.

Perform this task when you need to add normal user.

Steps

1. On the Web Client, click **Security → Users** to enter the User Management page.
2. Click **Add** to enter the Add User page.

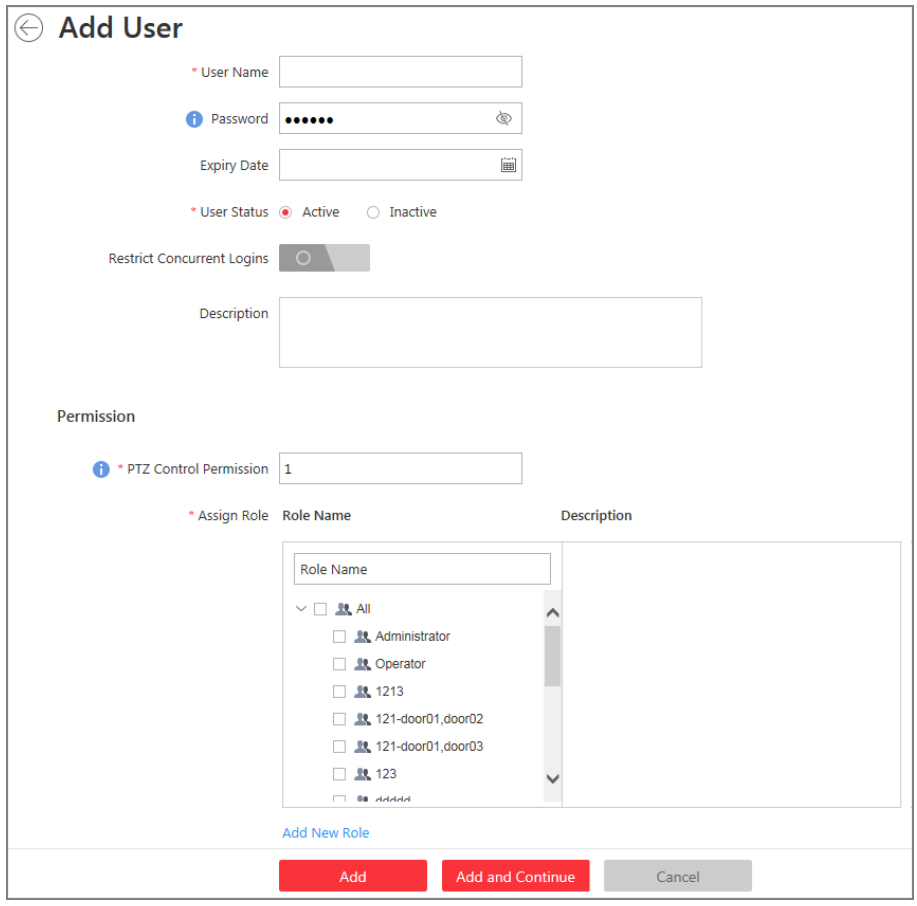

Figure 10-5 Add User Page

3. Set the required parameters.

User Name

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

Password

The system provides a default password (Abc123). You can use it or customize a stronger password. However, you must change the initial password for first time login in.

Expiry Date

The date when this user account becomes invalid.

Restrict Concurrent Logins

If necessory, set **Restrict Concurrent Logins** switch to ON and input the maximum number of logins.

User Status

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

Example

When user1 and user2 control the PTZ unit at the same time, the user who has the higher PTZ control permission level will take the control of the PTZ movement.

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

Note

- If no role has been added, two default roles are selectable: administrator and operator.
  Administrator
  The role that has all permissions of the system.

  Operator
  The role that has all permissions of the system Control Client.
- If you want to add customized roles, you can click **Add New Role** to quickly enter the Add Role page.

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