HikCentral

Quick Start Guide

Quick Start Guide

About this Manual

This Manual is applicable to HikCentral.

The Manual includes instructions for using and managing the product. Pictures, charts, images and all other information hereinafter are for description and explanation only. The information contained in the Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version in the company website (http://overseas.hikvision.com/en/).

Please use this user manual under the guidance of professionals.

Trademarks Acknowledgement

HIKVISION and other Hikvision’s trademarks and logos are the properties of Hikvision in various jurisdictions. Other trademarks and logos mentioned below are the properties of their respective owners.

Legal Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, IS PROVIDED “AS IS”, WITH ALL FAULTS AND ERRORS, AND HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF THIRD PARTY. IN NO EVENT WILL HIKVISION, ITS DIRECTORS, OFFICERS, EMPLOYEES, OR AGENTS BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR

INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA OR DOCUMENTATION, IN CONNECTION WITH THE USE OF THIS PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

REGARDING TO THE PRODUCT WITH INTERNET ACCESS, THE USE OF PRODUCT SHALL BE WHOLLY AT YOUR OWN RISKS. HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER ATTACK, HACKER ATTACK, VIRUS INSPECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

SURVEILLANCE LAWS VARY BY JURISDICTION. PLEASE CHECK ALL RELEVANT LAWS IN YOUR JURISDICTION BEFORE USING THIS PRODUCT IN ORDER TO ENSURE THAT YOUR USE CONFORMS THE APPLICABLE LAW. HIKVISION SHALL NOT BE LIABLE IN THE EVENT THAT THIS PRODUCT IS USED WITH ILLEGITIMATE PURPOSES.

IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATER PREVAILS.

Contents

1. Overview

1.1 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.

1.2 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 will run these components. Otherwise, you cannot install and configure the HikCentral.
Consult your IT system administrator to confirm you have the proper access rights.

1.3 System Requirements

1.3.1 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)
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)
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

1.3.2 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).

CPU: Intel® Core™ i5-4590 @ 3.3 GHz and above

Memory: 8 GB and above

Video Card: NVIDIA® Geforce GTX 970 and above

2. Installation

Two installation packages are available for building your HikCentral system.

- Basic Installation Package (HikCentral_V1.1_XXXXXXXX): contains the must-have modules to build the system, including Video Surveillance Management Service, Streaming Service, and Control Client.
- Control Client Installation Package (HikCentral_Client_V1.1_XXXXXXXX): 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.

The basic installation package which is provided by HIKVISION contains two service modules and one client: the HikCentral Video Surveillance Management (VSM) Service, HikCentral Streaming Service, and HikCentral Control Client. The service modules must be installed on different servers or PCs separately. They cannot be on the same server.

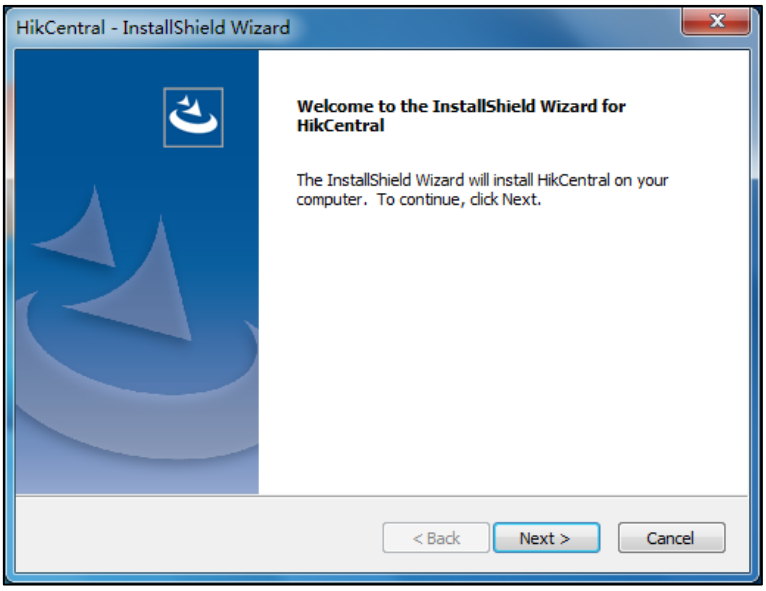
Note: The VSM Service and Streaming Service cannot be installed on the same PC.

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*.

Perform the following steps to install the system.

Steps:

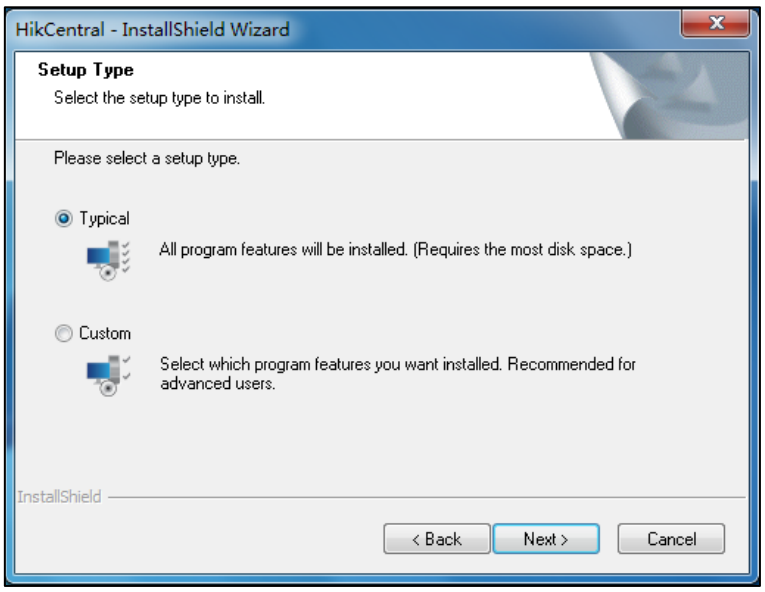
1. Double-click the program file  (HikCentral_V1.1_XXXXXXXX) to enter the Welcome panel of the InstallShield Wizard. Click **Next** to start the InstallShield Wizard.



2. Read the License Agreement. Click **Print** if you want to print the license agreement.
   If you accept the terms of the license agreement, click **I accept the terms of the license agreement** and continue.
   Otherwise click **I do not accept the terms of the license agreement** to cancel the installation.
3. On the next panel, you are prompted to select a setup type to install.
   Select **Typical** for installing all the service modules (except the Streaming Service) and client, and

click **Next** to continue.

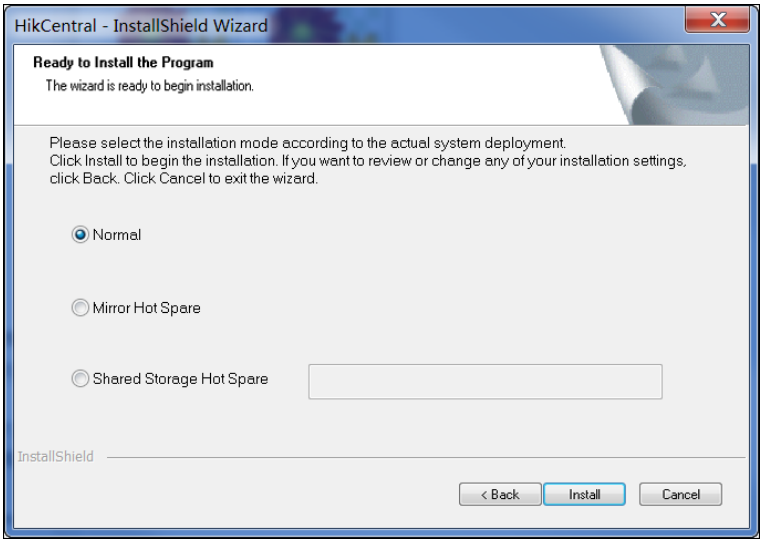
Note: The VSM and Streaming Service cannot be installed on the same PC.



4. Click **Change…** and select the desired directory to install the module(s). Click **Next** to continue.

   Note: The default directory is *C:\Program Files (x86)\ HikCentral* (for 64-bit OS).

5. (Optional) You can select to set the system as a hot spare in mirror hot spare or shared storage hot spare mode. For building the hot spare system, please contact our technical support engineer.



- **Mirror Hot Spare:** 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 VSM server fails, the spare VSM server switches into operation without interruption, thus increasing the reliability of the system.
- **Shared Storage Hot Spare:** There are two VSM servers and one HDD (installed on another server) in the hot spare system: host server, spare server, and the HDD you selected. When the host server works, the data is stored in the HDD. When the host VSM server fails, the spare VSM server switches into operation and will take over the HDD to use the same data file.
- If you do not need hot spare system, select **Normal**.

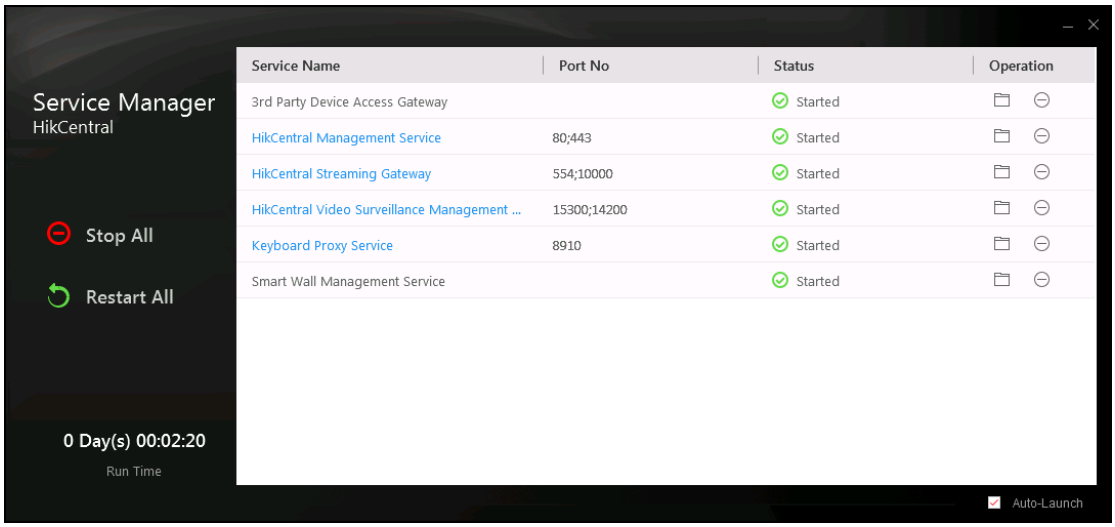
6. Click **Install** to begin the installation.
   A panel indicating progress of the installation is displayed.
7. Read the post-install information and click **Finish** to complete the installation.
   Note: You can check the **Run Web Client** checkbox to open the login interface of Web Client via web browser. The web browser will pop up and then the login page of the Web Client shows. If the settings of your web browser block the login page, please follow the prompt on the web browser to allow the proper display of the page.

After installing the service module(s), the Service Manager runs automatically.

Notes:

- If you select the hot spare system installation, the Service Manager will not be installed.
- The Service Manager should be run as administrator. If not, please exit the Service Manager and then run it as administrator.

The Service Manager screen is shown below and the displayed items vary according to the service modules you selected for installation.



You can click the service name to edit the port of the corresponding service.

You can click ⊖ to stop the service, and click 🗀 to go to the installation folder of the service module.

Note: If the port No. of the service is occupied by other service, the port No. will be shown in red. You should change the port No. to another value before the service can work properly.

You can also click **Stop All** to stop all the services and click **Restart All** to run them again.

You can check the **Auto-Launch** checkbox to enable launching the Service Manager automatically after the PC startup. If the auto-launch function is not enabled, all of the service modules you have installed will not run automatically after the server startup, and HikCentral will not be functional until the service modules are started manually.

3. Accessing HikCentral via Web Client

After installing HikCentral, you can access the system via Web Client which is the client for management of HikCentral.

Running Environment

- **CPU:** Intel Pentium IV 3.0 GHz and above
- **Memory:** 1GB and above
- **Video Card:** RADEON X700 Series
- **Web Browser:** Internet Explorer 10/11 or above (32-bit)
  Firefox 32 or above (32-bit)
  Google Chrome 35 or above (32-bit)

Notes:

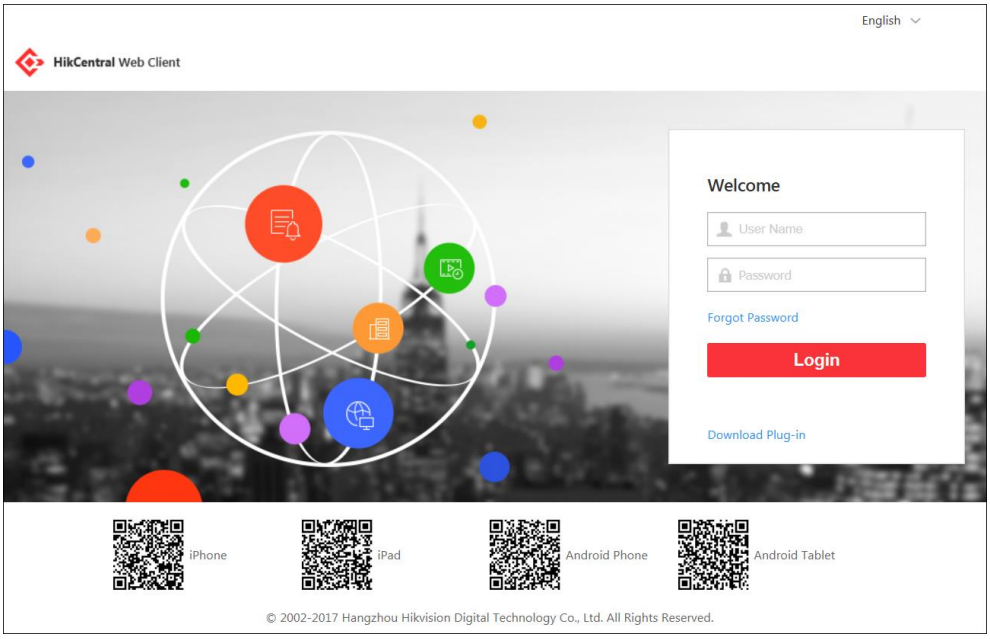
- Google Chrome and Firefox do not support live view, playback, online device detection, and device remote upgrade.
- You should run the web browser as an administrator.

Steps:

1. In the address bar of the web browser, input the IP address of the PC running VSM (Video Surveillance Management Service) and press the **Enter** key. A login window will pop up.

   Notes:

   - The address is in the format of http://VSM IP address.
     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.
   - Before the VSM can be accessed via a WAN, please configure the VSM's IP address in **WAN Access** of System Configuration. For details, refer to the *User Manual of HikCentral Web Client.*



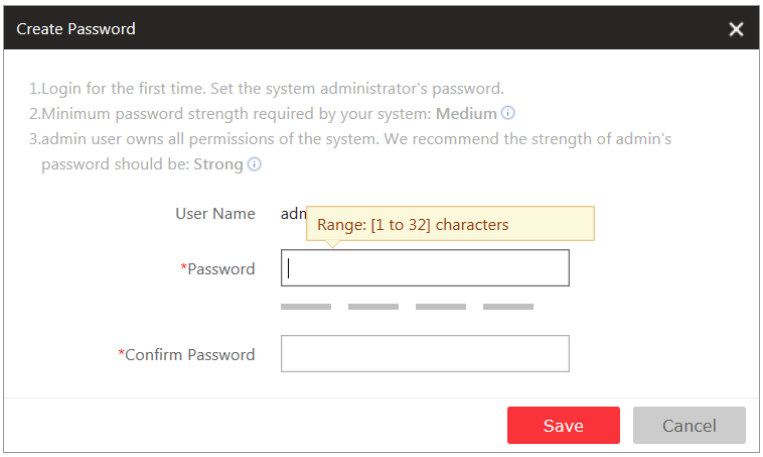
2. On the first login via the Internet Explorer browser, you need to install the plug-in before you can access the functions.
   1) Click **Download Plug-in**, save the plug-in file and then close the web browser.

2) Install the plug-in according to the prompt.

3) After the installation, re-open the web browser and log into the VSM (step 1).

3. If it is the first time accessing the Web Client, you are required to create the *admin* password for HikCentral.

   The following dialog will pop up.



   Input the password and confirm password for the *admin* user and click **Save** to create the password.

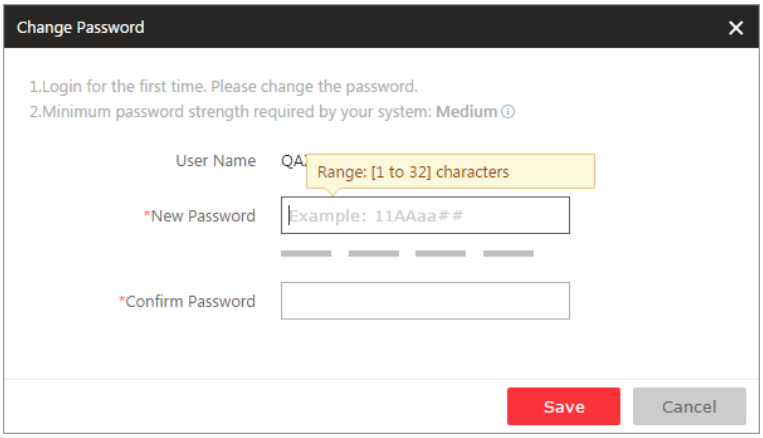
   Note: The password strength should meet the system requirements. The default minimum password strength is **Medium**.

   - *The password strength can be checked by the system. For your privacy, you must set the password to something of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product.*
   - *Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.*

4. If it is not the first time login as an *admin* user, input the user name and password of VSM and click **Login**.

   Notes:

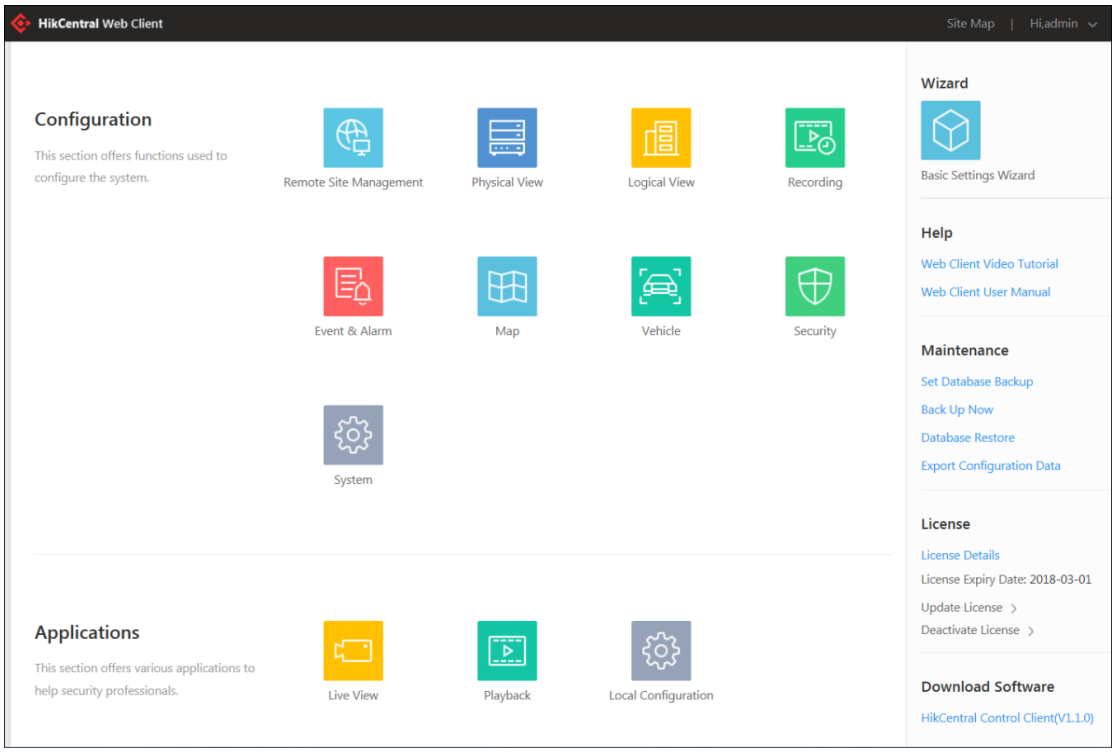
   - When other users (except *admin* user) first log in to HikCentral, he/she should input the initial password (*Abc123*), new password and confirm password, and click **Save** to create the password.



- If a failed password attempt is detected, you are required to input a verification code before you can log in.
- Any failed password attempts and verification code attempts from all sources will be accumulated. After a specified number of failed password or verification code attempts, your IP address will be locked for a defined period of time. For detailed settings of failed login attempts and locking duration, refer to the *User Manual of HikCentral Web Client*.
- The default settings for the above enforce that the account will be frozen for 30 minutes after 5 failed password attempts. The failed password attempts from the current client, other client (e.g., Control Client) and other address will all be accumulated.

After logging in, you enter the home page of HikCentral Web Client.

Note: The displayed modules on the home page vary with the License you purchased. For detailed information, please contact our technical support engineers.



The HikCentral Web Client is composed of the following function modules:

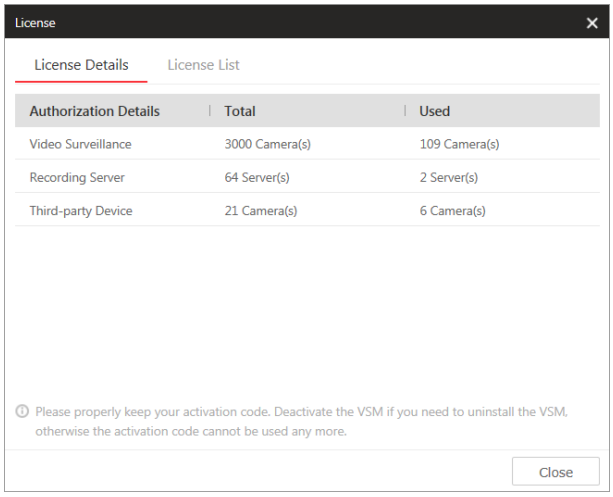
Note: For detailed introduction about the Web Client, please refer to the *User Manual of HikCentral Web Client*.

4. Activating HikCentral

After you install HikCentral, you get a temporary License for certain number of connected cameras within a certain time period. This is called the trial period. If trial period has expired and the HikCentral has not been activated, you cannot login and/or operate HikCentral anymore.
To ensure the proper use of HikCentral, you should activate it before the trial period ends.

Notes:

- If you do not want to activate HikCentral immediately, you can skip this chapter and perform this operation when you purchase your license.
- Please log in to HikCentral via Web Client, click **License Details** at the License area to check the trial period and the manageable device number of your HikCentral.
  You can click **License List** to check all the activated License of your system and click an activation code to view the related authorization details.



Two types of License are available for HikCentral, you can choose to purchase the specific License as required.

- **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., enlarge the connectable cameras), you can purchase expanded License to get additional features.

When you purchase the License, you will receive an activation code from HIKVISION. T Two activation methods are available according to your network condition: online activation and offline activation. We introduce the configuration of these two modes separately here.

Notes:

- Only the *admin* user can perform the activation 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 problem during activating, please send the hardware server's logs to our technical support engineers.
- For other License operation, refer to *User Manual of HikCentral Web Client*.

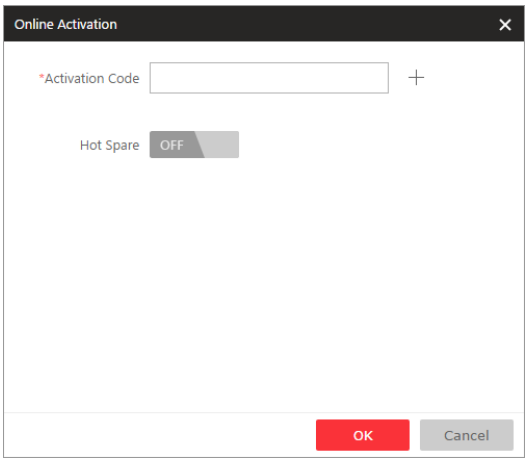
4.1 Online Activation

Purpose:

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 in to the HikCentral via Web Client.
2. After successfully logging in, you enter the home page of HikCentral Web Client. Click **Online Activation** at the License area to pop up the License configuration window.



3. Input the activation code received when you purchase your License. If you have purchased more than one License, you can click + and input other activation codes.

   Note: At least one basic License is required for activating the system.
4. (Optional) Set the **Hot Spare** switch as **ON** and input the required parameters if you want to build a hot spare system.

   Notes:

   - You must select **Mirror Hot Spare** or **Shared Storage Hot Spare** when you install the system.
   - For how to build the hots spare system, please contact our technical support engineers.
5. Click **OK** and the License Agreement dialog pops up. Read the License Agreement. If you accept the terms of the license agreement, check 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.
6. The prompt “Operation completed” will pop up when the VSM is successfully activated.

4.2 Offline Activation

Purpose:

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

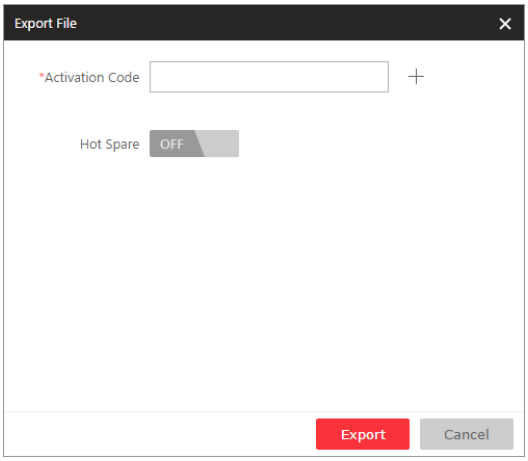
Note: You must enter HIKVISION's website (http://overseas.hikvision.com/) and go to **VMS** > **VMS Support** > **License Management**. Click **NEW USER** to register an account.

Steps:

1. Log in to HikCentral via the Web Client.

After successfully logging in, you enter the home page of HikCentral Web Client.

2. Export the license request file.
   1) Click **Export the license request file** at the License area to pop up the License configuration window.



   2) Input the activation code received when you purchase your License.
   3) (Optional) Set the **Hot Spare** switch as **ON** and input the required parameters if you want to build a hot spare system.

      Notes:

      - You must select **Mirror Hot Spare** or **Shared Storage Hot Spare** when you install the system.
      - For how to build the hots spare system, please contact our technical support engineers.

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

   Note: If the PC accessing the HikCentral via Web Client can connect to the Internet, you can skip this step.
4. Enter HIKVISION's website (http://overseas.hikvision.com/) and go to **VMS** > **VMS Support** > **License Management**.
5. Login with your account.
6. Generate the activation file.
   1) Select **How to Activate Your Account**.
   2) Click **Browse** at the bottom of the page to select the license request file exported in step 2.
   3) Click **Submit** to generate the activation file.
   4) In the pop-up dialog, click **Download** to download the generated activation file and set the name and saving path.
7. Save the activation file to the proper directory of the PC that accesses HikCentral via the Web Client.
8. In the License configuration window, click **Import the activation file** to import the response file and the License Agreement dialog pops up.

   Read the License Agreement. If you accept the terms of the license agreement, check 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.
9. The prompt “Operation completed” will pop up when the VSM is successfully activated.

5. Quick Start

Here we introduce the configuration for some basic HikCentral Web and Control Client features.

5.1 Resource Management and Live View

Purpose:

Before using live view, viewing playback, setting a recording schedule, or configuring events, you need to add devices to the system, and manage them by areas.

If the system is central system with Remote Site Management (based on the license you purchased), you can also add other HikCentral systems without Remote Site Management as remote sites to manage their resources.

Notes:

- Make sure the devices (cameras, DVR, etc.) you are going to use are correctly installed and connected to the network as specified by the manufacturer's instructions. This initial configuration is required in order for the networked devices to link up with HikConnect.
- This section only addresses the addition of remote site via an IP address, and addition of online encoding device via an IP address or domain name. For other methods, please refer to the *User Manual of HikCentral Web Client*.

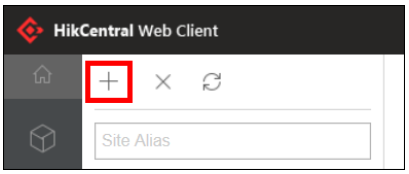
5.1.1 Adding Remote Site

Purpose:

You can add one remote site by inputting the site's IP address or domain name.

Steps:

1. Click **Remote Site Management** on home page to open the remote site management page.
2. Click + on the left to enter the adding remote site page.



3. Select **IP/Domain** as the adding mode.
4. Input the required information.
   - **Site Address:** Input the remote site IP address.
   - **Site Port:** Input the remote site port No. By default, it's 80.
   - **Alias:** Create a remote site name. You can select the **Synchronize Name** to synchronize the remote site's name automatically.
   - **User Name:** Input the remote site user name.
   - **Password:** Input the remote site password.

     Note: The password strength of the remote site can be checked by the system. For your privacy, we strongly recommend changing the password to something of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers,

and special characters) in order to increase the security of your product.

- **Description:** Input the brief information to describe the site.

5. (Optional) Enable to receive the alarm configured on the remote site.
   1) Set the **Select Alarm** switch to **ON** to display all the configured alarms on remote site.
   2) Select the checkbox(es) to select the configured alarm(s).

   Note: After receiving the alarm from remote site, the alarm will be configured as alarm in central system automatically. You can click **Default Configuration Rule** to view the imported alarms' default settings including alarm name, alarm priority, actions, etc.
6. Click **Add** to add the remote site and return to the remote site list page. You can also click **Add and Continue** to save the settings and continue to add other remote sites.

5.1.2 Adding Encoding Device

Click **Physical View** to open the device and server management page.

Creating a Password

Purpose:

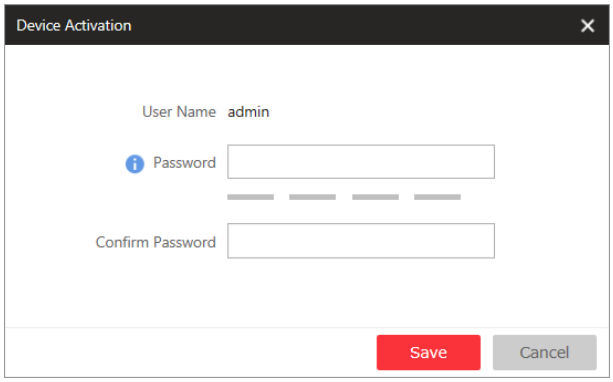
For certain devices you must first create a password to activate them before they can be added to the software and work properly.

Note: This function should be supported by the device.

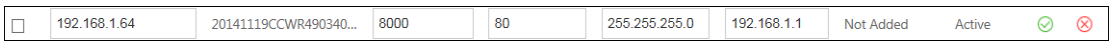
Steps:

1. Click the **Physical View** to access the device and display the server management page.
2. Click **Encoding Device** tab to enter the encoding device management interface.
3. On the Online Device panel, view the device status (shown in the **Security** column) and select the checkbox to select an inactive device.
4. Click to pop up the Device Activation interface.
5. Create a password in the password field, and confirm it.

Strong Password Recommended– *We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including 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.*



6. Click **Save** to create the device password. The “Operation completed” window will display when the password is successfully set.
7. Click in the Operation column of the device to edit the network information of it.



8. Change the device IP address to the same subnet with your computer if you need to add the device to the system.
9. Click , input the password set in step 5 and click **Save** to complete the network settings.

Adding Online Devices

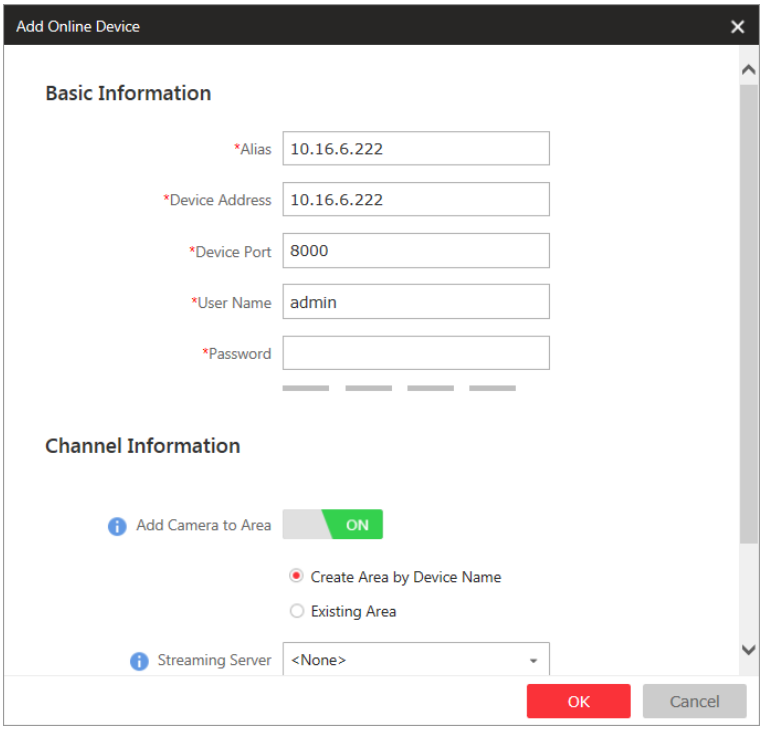
Purpose:

A list of encoding devices located in the same local subnet as the Web Client will be displayed.

Steps:

1. Click **Physical View**.
2. Click **Encoding Device** tab to enter the encoding device management interface.
3. Check the checkbox of the device(s) to be added from the Online Device panel.

   Note: You need to create the password for an inactive device before you can add it properly.
4. Click **Add to Device List** to open the camera adding dialog.
5. Input the required information.



- **Alias:** Create a device name.
- **Device Address:** The device IP address will be obtained automatically in this adding mode.
- **Device Port:** Input the device port No. The port will be obtained automatically in this adding mode.
- **User Name:** Input the device user name. The default user name is *admin*.
- **Password:** Input the device password.

  Note: The password strength of the device can be checked by the system. For your privacy, we strongly recommend changing the password to something of your own choosing (using a

minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product.

6. (Optional) Import the encoding device's cameras to area.
   1) Set the **Add Camera to Area** switch to **ON.**
   2) Select to import all the cameras of the encoding device, or select specified cameras to import.
   3) Select an area. You can create a new area by the device name (or custom) or select an existing area.

   Note: If you do not import cameras to an area, you cannot perform the live view, playback, event settings, etc., for the cameras.
7. After adding cameras to an area, select the **Synchronize Camera Name** checkbox to obtain the camera name from the device, and select **Get Device's Recording Settings** to get the recording schedule from the device. The device cameras will record automatically according to this schedule.
8. Click **OK** to confirm adding the device.

Adding Devices by IP Address or Domain Name

Steps:

1. Click **Physical View**.
2. Click **Encoding Device** and click **Add** to enter the Add Encoding Device page.
3. Select **IP/Domain** as the adding mode.
4. Input the required information.
   - **Manufacturer:** Select the device manufacturer.
   - **Device Address:** Input the device IP address.
   - **Device Port:** Input the device port number. By default, it's *8000*.
   - **Alias:** Create a device name.
   - **User Name:** Input the device user name.
   - **Password:** Input the device password.

     Note: The password strength of the camera can be checked by the system. For your privacy, we strongly recommend changing the password to something of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product.
5. Set the **Add Camera to Area** switch to **ON** in order to import the cameras of the added devices to an area. Create a new area by the device name (or custom) or select an existing area.

   Note: If you do not import cameras to area, you cannot perform the live view, playback, event settings, etc., for the cameras.
6. After adding cameras to an area, select the **Synchronize Camera Name** checkbox to obtain the camera name from the device. Select **Get Device's Recording Settings** to get the recording schedule from the device. The device cameras will record automatically according to this schedule.
7. Click **Add** to add the device and return to the device list page. You can also click **Add and Continue** to save the settings and continue to add other devices.

5.1.3 Area Management

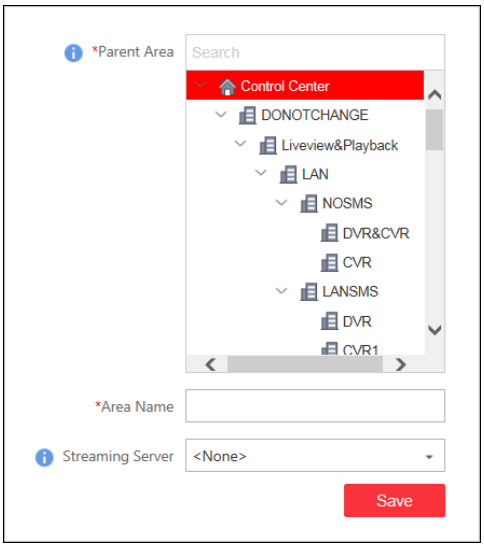
Purpose:

The added cameras, alarm inputs, and alarm outputs should be organized into areas for convenient management. You can watch the live view, play back the video files, and perform some other device operations when you manage the devices by areas.

Steps:

1. Log in to the HikCentral via Web Client, and click **Logical View** to open the area management page.
2. Click + on the area list panel to open the Add Area dialog window.

3. Select the parent area in the **Parent Area** drop-down list.



4. Input an area name.
5. Click **Save** to add the new area.
6. In the area tree panel, select an area to add elements to.
7. In the element area, select an element type tab. The element types are: camera, alarm input, and alarm output.
8. Click **Add** and a dialog box will be displayed. Add the element(s) to the area.
   1) Select the checkbox(es) to choose the elements to be added.
   2) (Optional) When adding a camera to the area, select the **Synchronize Camera Name** checkbox to obtain the camera name from the device.
      Select the **Get Device's Recording Schedule** checkbox to obtain the recording schedule configured on the local device. The cameras will record automatically according to this schedule.
   3) Click **Add** to add the elements to the area.

Notes:

- Up to 64 cameras can be added per area.
- A camera, alarm input, and alarm output, can only be added to an individual area.

5.1.4 Live View

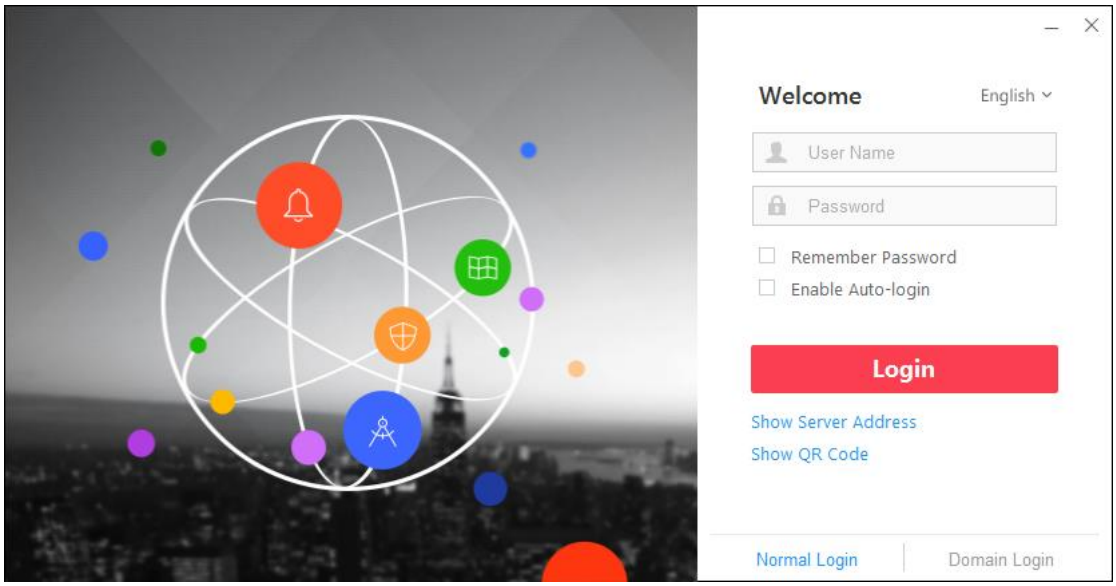
After adding the devices to your managed area, you can use the live view of the camera via the Control Client which provides multiple operating functionalities.

Login via Control Client

Two kinds of user (normal and domain) are supported for logging into HikCentral via the Control Client. We will only introduce the normal user login in this document. Please refer to *the User Manual of HikCentral Control Client* for the domain user login and refer to *User Manual of HikCentral Web Client* for the Active Directory setup.

Steps:

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



2. Select **Normal Login** tab on the bottom.
3. Click **Show Server Address** and input the parameters.
   - **Server Address:** Input the address (IP address or domain name) of the VSM that you want to connect to.
   - **Port:** Input the VSM port number. It is 80 by default.
4. Input the HikCentral user name and password.
5. Click **Login** to enter the Control Client.

   Notes:
   - If failed password attempt of current user is detected, you are required to input the verification code before you can log in. The failed password attempt from current client, other client and other address will all require the verification code.
   - The failed password attempt from current client, other client (e.g., Control Client) and other address will all be accumulated. Your IP address will be locked for a specified period of time after specific number of failed password or verification code attempts. For detailed settings of failed login attempts and locking duration, refer to the *User Manual of HikCentral Web Client.*
   - The account will be frozen for 30 minutes after 5 failed password attempts. The failed

password attempt from current client, other client (e.g., Control Client) and other address will all be accumulated.

6. The QR code for downloading the Mobile Client is also available on the login interface. Click **Show QR Code** to reveal the QR code and scan the corresponding QR code with your mobile terminal to download the Mobile Client.

Live View

Steps:

1. After login the Control Client, click  to enter the Live View interface.
2. Click  on the left to enter the area mode.
3. Optionally, click  and select window division mode for live view.
4. Click-and-drag the camera to the display window,
   or double-click the camera name after selecting the display window to start the live view.

Note: For information about live view operations, please refer to the *User Manual of HikCentral Control Client*.

5.2 Recording Schedule Settings and Playback

In order to view the camera's video files via the Control Client, schedule recordings via the Web Client.

5.2.1 Recording Schedule Settings

Purpose:

HikCentral provides three storage methods: 1) storing on the encoding devices, 2) storing on the Central Video Recorder, 3) storing on the Cloud Storage Server for storing the video files of the cameras according to the configured recording schedule. You can also store the video files of the remote site's cameras in the central system's Recording Server.

Notes:

- In this document, we only cover the method of storing video files of current site's 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.

Steps:

1. In the HikCentral Web Client, click the **Recording** to open the recording settings page.
2. Click **Add** to configure camera recording settings.
3. Select the camera(s) to configure the recording settings for.
4. Set the **Main Storage** switch to **ON** to set the main storage location.
5. Input the required information.
   - **Storage Location:** Store the video files on the Encoding Device.
   - **Recording Schedule Template**: Select the recording type as all-day time-based template, all-day event-based template, or customized template. Click **View** to view the template. For details in setting the custom recording, refer to *User Manual of HikCentral Web Client*.

All-Day Time-Based Template: Record video all-day continuously.

All-Day Event-Based Template: Record video when the event occurs.

- **Stream Type**: Select the recording stream type.
- **Pre-record**: Time to record video preceding detected events. The value of the pre-record period is not editable. This field is available for cameras that are configured with event-based recording.
- **Post-record**: Time to record video following detected events. This field is available for cameras that are configured with event-based recording.
- **Video Files Storage:** Select the storage mode for the recorded videos.

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

  Expired Time: When this option is selected, HikCentral will automatically delete the oldest videos after the specified retention period. This method allows you to define the longest time period for keeping videos. The actual retention period for the videos depends on the allocated storage.

6. Click **Add** to save the recording settings and back to the recording list page. You can also click **Add and Continue** to save the settings and continue to add other recording settings.

After configuring the recording settings for the camera, the recording schedule item will be displayed.

5.2.2 Remote Playback

Purpose:

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*.

Searching Video Files for Playback

Steps:

1. After logging into the Control Client, click  on the control panel to enter the Remote Playback page.
2. Click-and-drag the camera/area to the display window, or double-click the camera/area to begin playback.
3. You can click the calendar  on the toolbar to select the date and time to search the video files for playback.

Playing Video Files

After searching the video files for normal playback, you can control the video playback in the following ways:

- **Timeline**

  The timeline indicates the video files duration, and video files of different types are color coded. Click  or  to zoom in or out the timeline bar. You can also use the mouse wheel to zoom in or out on the timeline.

  Drag the timeline bar to go to the previous or the next time period.

- **Thumbnails**

  Hover the cursor over the timeline to view the video thumbnails. Click the thumbnail (if supported) to play back the video of the specific time.

- **Locking Files**

  Move the mouse to the playback window. Click and set the locking duration to protect the video file from being overwritten when the HDD is full or from being "manually" deleted.

5.3 Event and Alarm Configuration

Purpose:

In the HikCentral Web Client, set the linkage actions for the detected events and alarms. Status of the events and alarms can be received by the Control Client from the devices.

Click the **Event & Alarm** to enter the Event and Alarm Configuration page.

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), please refer to the *User Manual of HikCentral Web Client*.

5.3.1 Configuring Motion Detection Event

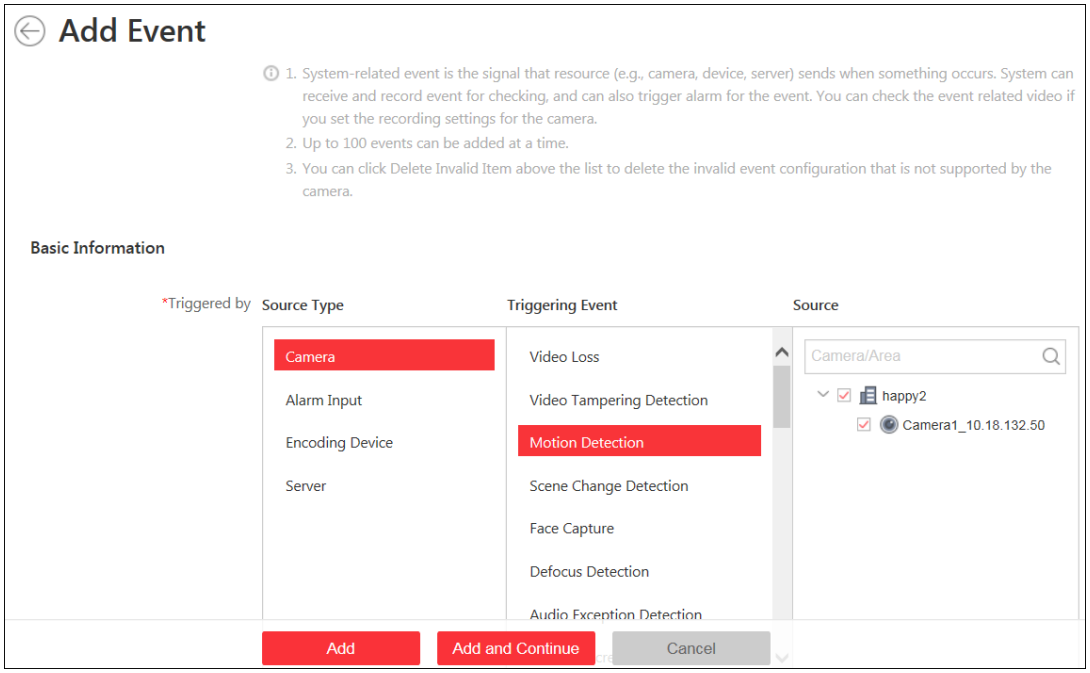
The camera exception types vary according to the connected device. In the following example, we will introduce the motion detection settings. For the settings of other camera exception types (e.g., video loss, video tampering), please refer to the *User Manual* of the connected devices.

Purpose:

Motion detection events are triggered when the camera detects motion within its defined area.

Steps:

1. Click **Event & Alarm** and click **System-Related Event** tab to enter the Event Management interface.
2. Click **Add** to enter the Add Event page.



3. Select the source type as *Camera* and select the triggering event as *Motion Detection*.

4. Select the specific camera in the Source panel.
5. Click **Add** to add the event and return to the event list page. You can also click **Add and Continue** to save the event settings and continue to add event.

5.3.2 Configuring Motion Detection Alarm

Purpose:

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.

Example: HikCentral can send notification email to designated recipient when motion is detected.

Steps:

1. Click **Event & Alarm** and click **Alarm** tab to enter the alarm settings page.
2. Click **Add** to enter the Add Alarm page.
3. Set the required parameters.
   - **Triggered by:** Click to select the source type as *Camera*, source – a specific camera, and the triggering event as *Motion Detection* for triggering the alarm.
   - **Alarm Name:** Create an alarm name.
   - **Description:** Optionally, input alarm handling instructions and remarks.
   - **Arming Schedule Template:** Create an alarm arming schedule, and define when the alarm will be triggered.
   - **Alarm Priority:** Define alarm priority, and filter alarms that will be displayed in the Control Client.
   - **Recipient:** Select the user that will receive alarm information, as well as the user that will receive alarm information when they log into HikCentral via Control Client or Mobile Client.

   Additional Settings:
   - **Related Cameras:** Select the cameras for viewing the live video and playback when the alarm occurs in the Control Client's Alarm Center.
   - **Lock Video Files for:** Set the time duration for protecting the video file from being deleted.
   - **Related Map:** Select the map to show the alarm information and you should add the camera to the map as a hot spot.
   - **Trigger Pop-up Window:** Select to pop up the alarm window on Control Client to display all the alarm related cameras' live videos and playback when alarm occurs.
   - **Actions:** Trigger linkage actions when alarm occurs.
     - **Trigger actions when:** Select to triggering of linkage actions immediately after alarm occurs, or trigger actions after the alarm is not handled within a certain time period (customizable).
     - **Trigger Audible Warning:** Set the sound file to play on the PC when an alarm is triggered.
     - **Link Alarm Output:** Select the alarm output (if available) of an external device to be activated when alarm is triggered.
     - **Trigger PTZ:** Trigger selected camera preset, patrol or pattern of the selected camera(s) when an alarm is triggered.
     - **Display on Smart Wall:** Trigger to display the alarm video of the related camera on the smart wall. You can select the added smart wall and select which window to display the

alarm.

- **Create Tag:** Add tag to the video that is triggered by the alarm when you select cameras in the **Related Cameras** field. You can search for and check the video in the Control Client.
- **Send Email:** Select an email template to join the alarm information to, according to the defined email settings.

4. Click **Add** to add the alarm and return to the Alarm page. You can also click **Add and Continue** to save the settings and continue to add other alarms.

5.3.3 Checking Event Logs

If the camera detects motion, the event logs can be checked in the Control Client.

Steps:

1. Log in to the HikCentral via the Control Client.
2. Click  on the control panel to enter the Alarm Center page, and click the **Search** tab.
3. Select the event source, triggering event type, and time range.
4. Select the **Event** radio button to select the log type.
5. Click **Search**. The matched log files will display in the list. You can check the detailed event information.
6. Click the **Alarm Name** field of the searched alarm to view the detailed information, as well as the linked picture, video, and map.
7. Click  to save the information to your PC.

5.4 User and Role Management

Purpose:

The Security module on the HikCentral Web Client allows you to add and delete users, as well as 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.

5.4.1 Role Management

Purpose:

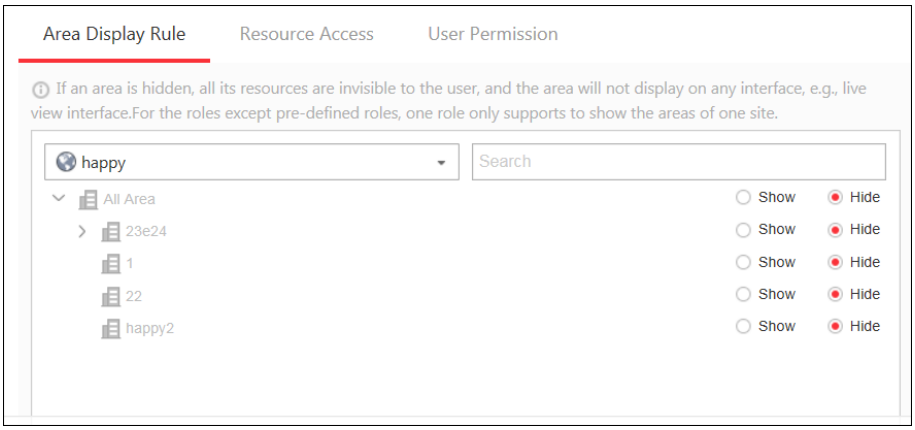
You can assign the permissions to the roles as required, and the user can link to the role to obtain different permissions.

Steps:

1. Click the **Security** tab to open the User Management page.
2. Open the User Management page and click **Roles** tab.
   Two roles are listed by default: administrators and operators.
   - **Administrator:** role with all HikCentral permissions.

- **Operator:** role with permission to access all the resources and all permissions for operating the Control Client.

3. Click **Add** to enter the Add Role page.
4. Input the role name as desired.
5. Assign the permissions to the role.
   - **Area Display Rule:** Show or hide the specific area(s) for the role. If the area is hidden, the user who is assigned the role will not be able to view and access the area and its resources on any interface.
   - **Resource Permission:** Select the resource type from the left panel and select resources from right panel to assign the selected resources' permissions to the role.
   - **User Permission:** Assign the resource permission, configuration permission on Web Client, and the control permission on Control Client to the role.



6. Click **Add** to add the role. You can also click **Add and Continue** to save the settings and continue to add roles.

5.4.2 User Management

Purpose:

Users can be added for accessing HikCentral.

The administrator role "admin" is pre-defined by default and cannot be edited or deleted.

Steps:

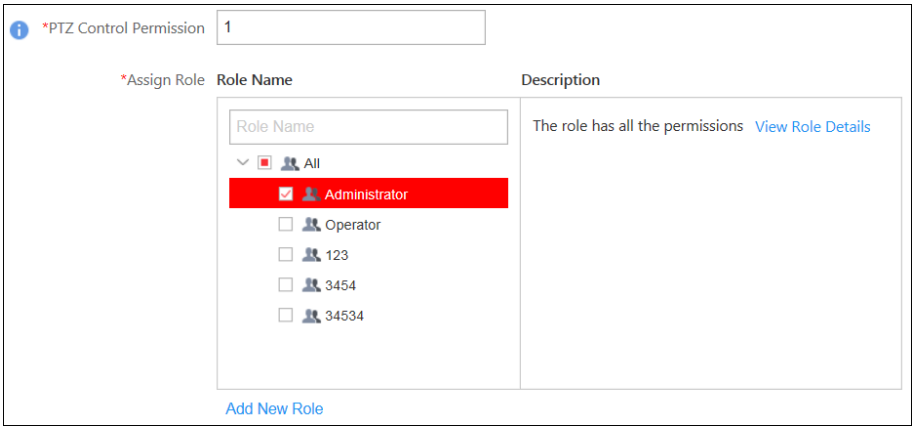
1. Open the User Management page and click the **Users** tab.
2. Click **Add** to enter the Add User page.
3. Input the user name, expiry date, user status, and description.

   Expiry Date: User account expiry date.

   User Status: Two kinds of status are available. If you select inactive, the user account will become inactive until you set the user status as active.

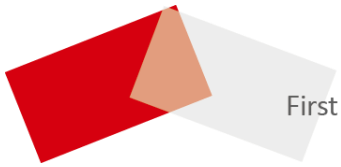
   Note: A user name cannot contain any of the following characters: / \ : * ? " < > |.
4. Set the PTZ Control Permission level.

   Set the PTZ Control permission level (1~100). The larger the value is, the higher the level of permission the user will have. For example, if two users attempt to control the PTZ unit at the same time, the user with greater PTZ permissions will control the PTZ movement.
5. Check the checkboxes of the existing roles to assign the role(s) for the created user.



6. Click **Add** to add the user.
   You can also click **Add and Continue** to save the settings and continue to add users.
   The user's initial password is *Abc123* which is used for first-time login. You will be asked to change the password when logging in with your initial password.

- *The password strength can be checked by the system. For your privacy, we strongly recommend setting the password to something of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product.*
- *Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.*



First Choice for Security Professionals

UD07025B