



HikCentral Quick Start Guide

Contents

Chapter 1 Guide Content	1
Chapter 2 Administrator Rights	2
Chapter 3 Installation	3
3.1 System Requirements	3
3.1.1 System Requirements for VSM Service	3
3.1.2 System Requirements for Control Client	4
3.2 Install Service Module in Typical Mode	4
Chapter 4 Log into the Web Client	6
4.1 Recommended Running Environment	6
4.2 Login for First Time for admin User	6
Chapter 5 Manage License	8
5.1 Activate License - Online	8
5.2 Update License - Online	10
Chapter 6 Manage Resource	11
6.1 Add Device by IP Address or Domain Name	11
6.2 Manage Area	14
6.2.1 Add Area	14
6.2.2 Add Camera to Area	15
Chapter 7 Configure Recording for Cameras	17
Chapter 8 Configure Event and Alarm	21
8.1 Add System-Monitored Event for Camera	21
8.2 Add Alarm for Camera on Current Site	24
Chapter 9 Manage Role and User	28
9.1 Add Role	28
9.2 Add Normal User	31
Chapter 10 Live View and Playback	33

10.1 First Time Login	33
10.2 Start Live View	34
10.3 Normal Playback	35
10.3.1 Search Video File	35
10.3.2 Play Video File	36
Chapter 11 Search Event/Alarm Logs	38

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, 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.



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.

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 VSM Service

VSM Service 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. When running the VSM service, there should be at least 1 GB free space.
- **Network Controller:** RJ45 Gigabit self-adaptive Ethernet interfaces.

VSM Service 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. When running the VSM service, there should be at least 1 GB free space.
- **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.
- **HDD:** When running the Control Client, there should be at least 1 GB free space.

3.2 Install Service Module in Typical Mode

During installation 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 VSM server fails, the spare VSM 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 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.



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 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.

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

Steps

1. In the address bar of the web browser, enter 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` or `https://172.6.21.96` in the address bar.

2. Enter the password and confirm password for the admin user in the pop-up Create Password window.



Caution

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

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

3. Click OK.

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

Result

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

Chapter 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

Enter 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.

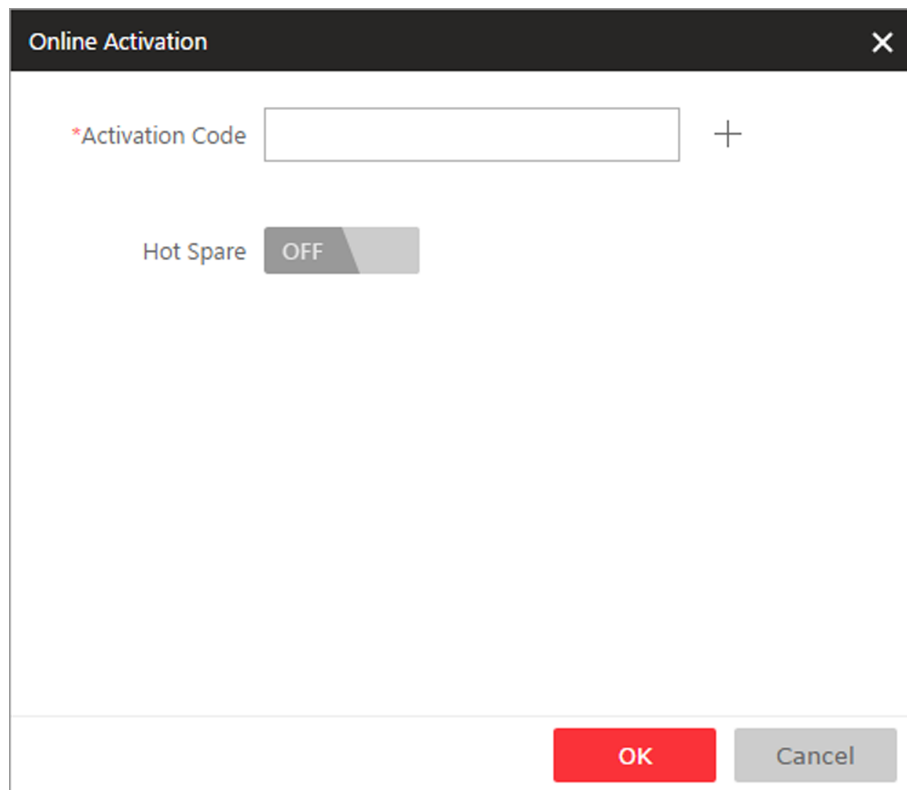


Figure 5-1 License Configuration Window

3. Enter 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 enter 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 Update License - Online

As your project grows, you may need to increase the connectable number of resources (e.g., cameras) for your HikCentral. If the VSM 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

Perform this task when you need to update your License in online mode.

Steps

1. Log in to HikCentral via the Web Client.
2. Click **Update License** at the License area to open the update panel.
3. Enter the activation code received when you purchase your License.



Note

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

4. Click **Update** and the License Agreement dialog opens.
5. Read the License Agreement.
 - If you accept the terms of the license agreement, check **I accept the terms of the agreement** and click **OK** to continue.
 - If you do not accept the agreement, click **Cancel** to cancel the update.

Result

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

Chapter 6 Manage Resource

HikCentral supports multiple resource types, such as encoding device, access control device, Remote Site, decoding device and Smart Wall. After adding them to the system, you can manage them, configure required settings and perform further operations. For example, you can add encoding devices for live view, playback, recording settings, event configuration, etc., add access control devices for access control, time and attendance management, etc., add Remote Site for central management of multiple systems, add Recording Server for storing the videos, add Streaming Server for getting the video data stream from the server, and add Smart Wall for displaying decoded video on smart wall.

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

Add Encoding Device

Adding Mode

☒ IP/Domain
☐ Hik-Connect
☐ IP Segment
☐ Port Segment
☐ Batch Import

Basic Information

* Access Protocol: Hikvision Protocol

* Device Address:

* Device Port: 8000

i Verify Stream Encryption Key: ☐

* Alias:

* User Name: admin

* Password:

Risky

Channel Information

i Add Channel to area: ☒

* Channel:

Figure 6-1 Add Encoding Device Page

3. Select **IP/Domain** as the adding mode.
4. Set the required information, including access protocol, device address, device port, stream encryption key, alias, user name, and password.

Access Protocol

Select **Hikvision Protocol** to add the Hikvision devices and select **ONVIF Protocol** to add the third-party devices.

Device Address

The IP address or domain name of the device.

Device Port

The devices to add should have the same port No. By default, the device port No. is 8000.

Verify Stream Encryption Key

You can set the **Verify Stream Encryption Key** switch to ON, and enter stream encryption key in **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 VSM server for security purpose.

Note

This function should be supported by the devices. Refer to the user manual of the device for getting key.

Alias

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

Caution

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

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

5. **Optional:** Set the **Add Channel to Area** switch 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 the live view, playback, event settings, etc., for the cameras.
-

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

Encoding Device

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

Hybrid Storage Area Network

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

Cloud Storage Server

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

pStor

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

Note

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

7. 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. Refer to **Configure Recording for Cameras** for details.
8. 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.

6.2 Manage Area

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

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

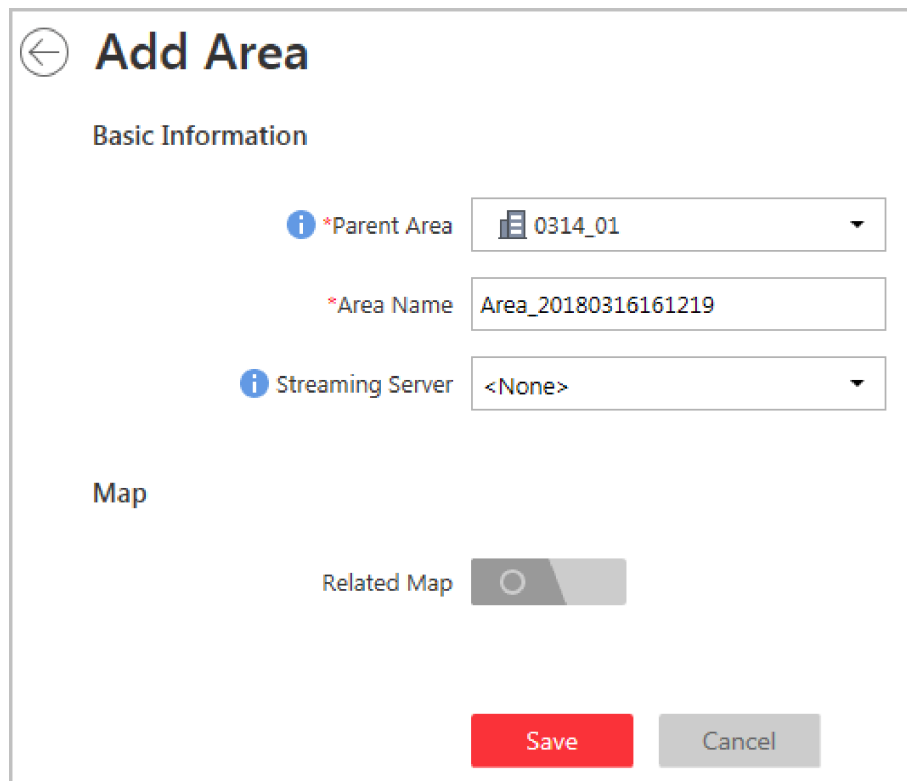


Figure 6-3 Add Area

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

6.2.2 Add Camera to Area

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

Perform this task when you need to add current site's cameras to areas.

Steps



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

1. Click **Logical View** on the Home page to enter the Area Management page.
2. Select an area for adding cameras to.
3. Select the **Cameras** tab.
4. Click **Add** to enter the Add Camera page.
5. Select the device type as **Encoding Device** or **Security Control Device**.

Note

Some security control devices, such as the panic alarm stations, also contain the cameras.

6. Select the cameras to add.
 7. **Optional:** Check **Get Device's Recording Settings** to obtain the recording schedule configured on the local device and the device can start recording according to the schedule.
-

Note

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

8. Click **Add**.
9. **Optional:** After adding the cameras, you can do one or more of the followings

Get Camera Name	Select the cameras and click Get Camera Name to get the cameras' names from the device in a batch.
------------------------	---

Note

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

Move to Other Area	Select the cameras and click Move to Other Area . Then select the target area to move the selected cameras to and click Move .
---------------------------	--

Display Cameras of Child Areas	Check Include Sub-area to display the cameras of child areas.
---------------------------------------	--

Chapter 7 Configure Recording for Cameras

For the cameras on the current site, HikCentral provides four storage methods (storing on encoding devices, Hybrid Storage Area Network, Cloud Storage Server, or pStor) for storing the video files of the cameras according to the configured recording schedule. You can get device's recording settings when adding camera to an area.

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

Steps

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.

← **Camera 01** ⚙️ Configuration on Device 📄 Copy to

Basic Information

*Name

*Protocol Type

Recording Settings

Main Storage ☒ [Get Device's Recording Settings](#)

*Storage Location

i *Recording Schedule Template

*Stream Type

i Pre-record ☐

i *Post-record

Video Expiration

i Enable ANR

Figure 7-1 Edit Camera

2. Set the **Main Storage** switch to ON.
3. Select the storage location for storing the recorded video file.

Note

If you select **Hybrid Storage Area Network**, **Cloud Storage Server** or **pStor**, specify a server and (optional) select a Streaming Server to get the video stream of the camera via it.

4. Select the storage type and configure the required parameters.
 - Select **Real-Time Storage** as the storage type to store the recorded video files in the specified storage location at the real time.

Note

If you choose **Encoding Device** as the storage location, you needn't select the storage type, but configure the following parameters as real-time storage settings by default.

Recording Schedule Template

Set the template which defines when to record the camera's video.

All-Day Time-Based Template

Record the video for all-day continuously.

All-Day Event-Based Template

Record the video when alarm occurs.

Note

The event-based recording schedule can not be configured for the **Cloud Storage Server**, and the command-based recording schedule can not be configured for the **Cloud Storage Server** and **pStor**.

Stream Type

Select the stream type as main stream, sub-stream or dual-stream.

Note

For storing on Hybrid Storage Area Network, Cloud Storage Server or pStor, dual-stream is not supported.

Pre-Record

Record video from periods preceding detected events. For example, when someone opens a door, you can see what happens right before the door opened.

This field displays when the storage location is set as Encoding Device or pStor, and it is available for the camera that is configured with event-based recording.

Post-Record

Record video from periods following detected events.

This field displays when the storage location is set as Encoding Device or Hybrid Storage Area Network. It is available for the camera that is configured with event-based recording.

Video Expiration

If you select **Encoding Device** as the storage location , set Video Expiration switch to ON and enter expiration day(s).

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.

Enable ANR

If you select the **Encoding Device** or **Hybrid Storage Area Network** as the storage location, check **Enable ANR** to turn the automatic network replenishment on to temporarily store the video in the camera when network fails and transport the video to storage device when network recovers.

- Select **Scheduled Uploading** as the storage type to upload the recorded video files from the encoding device or pStor to the specified storage location according to scheduled period



Note

- Make sure you have configured recording schedule stored in the device local storage or pStor for auxiliary storage first. Otherwise, the schedule uploading is not configurable.
 - The recordings can be uploaded only from the encoding device to Hybrid Storage Area Network, Cloud Storage Server or pStor, or from pStor to another pStor.
-

Upload between

Specify the time period to upload the recorded video files to the specified storage location during the period.

Recording for Uploading

Select the recorded video file type to backup.

5. Click **Save**.

Chapter 8 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 the Mobile Client, and you can check the details via the Control Client and the Mobile Client.

System-monitored event is the signal that resource (e.g., camera, device, server) sends when something occurs. System can trigger linkage actions (such as recording, capturing, sending email, etc.) to record the received event for checking.

Alarm is used to notify security personnel of the particular situation which helps handle the situation promptly. An alarm can trigger a series of linkage actions (e.g., popping up window) for notification and alarm handling.



Note

You can set linkage actions for both events and alarms. An event's linkage actions are used to record the event details (such as recording and capturing) and trigger basic actions (such as linking access point to lock or unlock, triggering alarm output, sending email, etc.). An alarm's linkage actions are used to record the alarm details and provide the recipients multiple ways to view alarm information for alarm acknowledgment and handling, such as popping up alarm window, displaying on smart wall, audible warning, etc.

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

8.1 Add System-Monitored Event for Camera

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

Perform this task when you need to add a system-monitored event triggered by the cameras in the system.

Steps

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

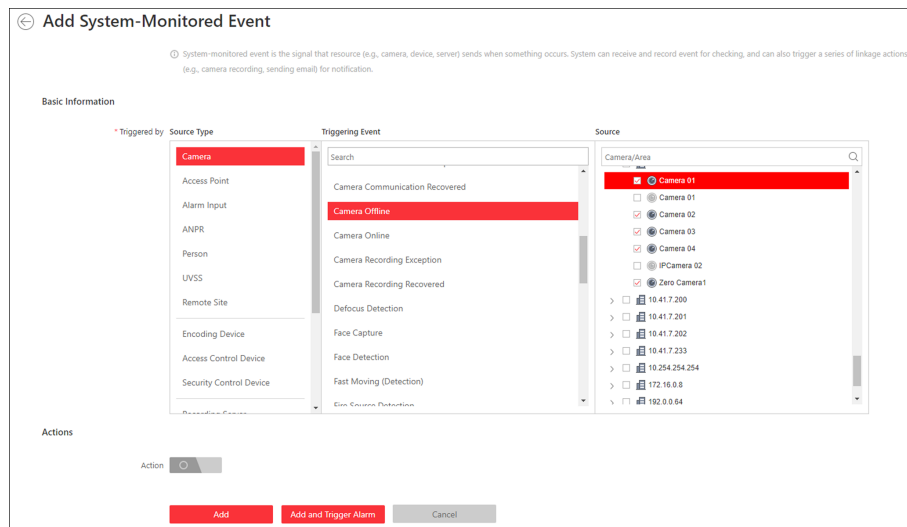


Figure 8-1 Add a System-Monitored Event

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

Source Type

Select the source type as **Camera**.

Triggering Event

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

Source

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

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

Arming Schedule Template

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

Trigger Recording

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

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

View Pre-Event Video: If the camera has recorded video files before the event, you can view the video recorded from periods preceding the event. Specify the number of seconds which you want to view the recorded video for before the event starts. For example, when someone opens a door, you can view the recorded video to see what happens right before the door opened.

Post-record: Record video from periods following detected 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.

Create Tag

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

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

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

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

Add the description to the tagged video as needed.

Capture Picture

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

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

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

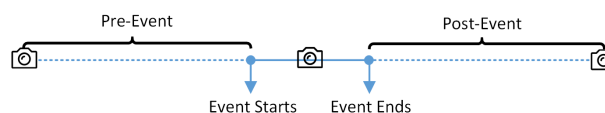


Figure 8-2 Capture Pictures

Note

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

Link Access Point

Select the access point(s) as the linkage target(s). You can set the access point action so that the access point will be unlocked, locked, remained unlocked, or remained locked when the event occurs.

Link Alarm Output

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

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

Trigger PTZ

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

Send Email

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

Trigger User-Defined Event

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

4. Finish adding the event.

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

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

8.2 Add Alarm for Camera on Current Site

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

Perform this task when you need to add a new alarm for cameras on current site.

Steps

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

Figure 8-3 Add Alarm for Camera on Current Site

2. Set the source type as **Camera** in the **Triggered by** field.
3. Select a triggering event as the source for triggering the alarm.
4. In the site drop-down list, select the current site.
5. Select a specific camera for triggering the alarm.
6. **Optional:** Enter the instructions for handling the alarm or enter remarks for the alarm.
7. Set the required information.

Arming Schedule

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

- **Schedule Template:** Select an arming schedule template for the alarm to define when the alarm can be triggered.
- **Event Based:** Specify a user-defined event or an alarm input as the start or end event of the arming schedule. When the user defined event or alarm input is triggered, the arming schedule will start or end.

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 the Control Client or Mobile Client.

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

Related Camera

Select the related camera to record the alarm video when the alarm is triggered. You can view the live video and play back the recorded video files when alarm occurs 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:** If the camera has recorded video files before the alarm, 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.



Note

Make sure the related camera(s) have been configured with recording schedule.

Related Map

Select a map to show the alarm information and you should add the camera to the map as a hot spot. You can check the map in the Alarm Center and Alarm & Event Search of the Control Client.

Trigger Pop-up Window

Display the alarm window on the Control Client to show the alarm details and all the alarm related cameras' live videos and playback when alarm occurs.

Display on Smart Wall

Display the alarm video of the alarm's related camera or display the specified public view on the smart wall. You can select the added smart wall and select which window to display the alarm.

- **Alarm's Related Cameras:** Display the video of the alarm's related cameras on the smart wall. You can select to display the video on which smart wall and which window. Select the stream type for the alarm video displayed on smart wall.
- **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.
- **Stop Displaying Alarm:** Define when the system will stop displaying the alarm on the smart wall. The system can stop displaying alarm within specified seconds, or replace the original alarm when other alarm with higher alarm priority is triggered.

Restrict Alarm Handling Time

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

Trigger Audible Warning

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

Trigger User-Defined Event

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

9. Finish adding the alarm.

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

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

Chapter 9 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.

9.1 Add Role

You can assign the permissions to the roles as required, and the users can be assigned with different roles to obtain different permissions.

Perform this task when you add role.

Steps

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



Note

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

Administrator

The role that has all the permission of the system.

Operator

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

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

← Add Role

Basic Information

* Role Name

Copy from

Expiry Date

Description

Permission Settings

* Permission Area Display Rule Resource Access User Permission

① If an area is hidden, all its resources are invisible to the user, and the area will not display on any interface, e.g., live view interface. For the roles except the pre-defined roles, you can set to show the areas on only one site.

HikCentral

Search

⌵ All ☐ Show ☒ Hide

☐ Show ☒ Hide

☐ Show ☒ Hide

Add Add and Continue Cancel

Figure 9-1 Add Role

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.
 - Select the default or pre-defined role from the **Copy from** drop-down list to copy the permission settings of selected role.
 - 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 with the role cannot view and access the area and its resources on any interface.

Area Display Rule Resource Access User Permission

① If an area is hidden, all its resources are invisible to the user, and the area will not display on any interface, e.g., live view interface. For the roles except pre-defined roles, one role only supports to show the areas of one site.

HikCentral232

Search

10.18.147.142	☐ Show ☒ Hide
RSM_NOSMS_Local	☐ Show ☒ Hide
RSM_NOSMS_CVR	☐ Show ☒ Hide
RSM_NOSMS_Cloud	☐ Show ☒ Hide
RSM_SMS_Local	☐ Show ☒ Hide
RSM_SMS_CVR	☐ Show ☒ Hide
RSM_SMS_Cloud	☐ Show ☒ Hide
test	☐ Show ☒ Hide
pos_duyinyinadd_147.143	☐ Show ☒ Hide
flk-test-area	☐ Show ☒ Hide
ctest	☐ Show ☒ Hide

Figure 9-2 Area Display Rule

Resource Access Permission

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



Note

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

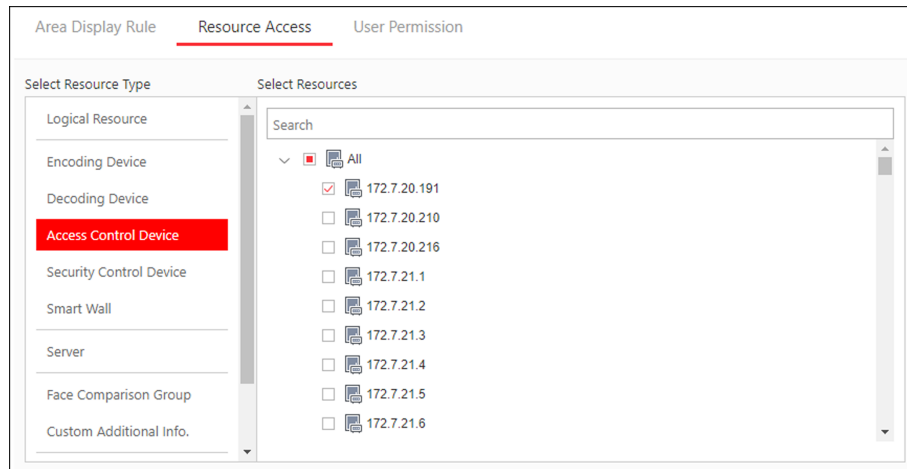


Figure 9-3 Resource Access Permission

User Permission

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

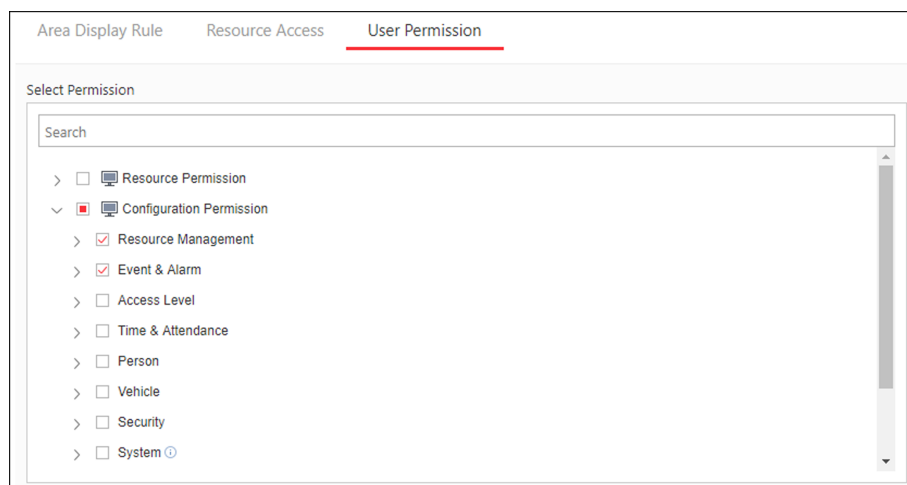


Figure 9-4 User Permission

5. Complete adding the role.

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

9.2 Add Normal User

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

Perform this task when you need to add normal user.

Steps

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

Add User

* User Name

i Password

Expiry Date

i Email

* User Status ☒ Active ☐ Inactive

Restrict Concurrent Logins ☐

Description

Permission

i * PTZ Control Permission

* Assign Role

Role Name	Description
☐ All	
☐ Administrator	
☐ Operator	
☐ 1213	
☐ 121-door01,door02	
☐ 121-door01,door03	
☐ 123	
☐ Admin	

[Add New Role](#)

Add **Add and Continue** **Cancel**

Figure 9-5 Add User

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.

Expiry Date

The date when this user account becomes invalid.

Email

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

Restrict Concurrent Logins

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

User Status

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

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



Note

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

Example

When user1 and 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.

6. Complete adding the user.
 - Click **Add** to add the user.
 - Click **Add and Continue** to save the settings and continue to add users.

Chapter 10 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.

10.1 First Time Login

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

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

Steps

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

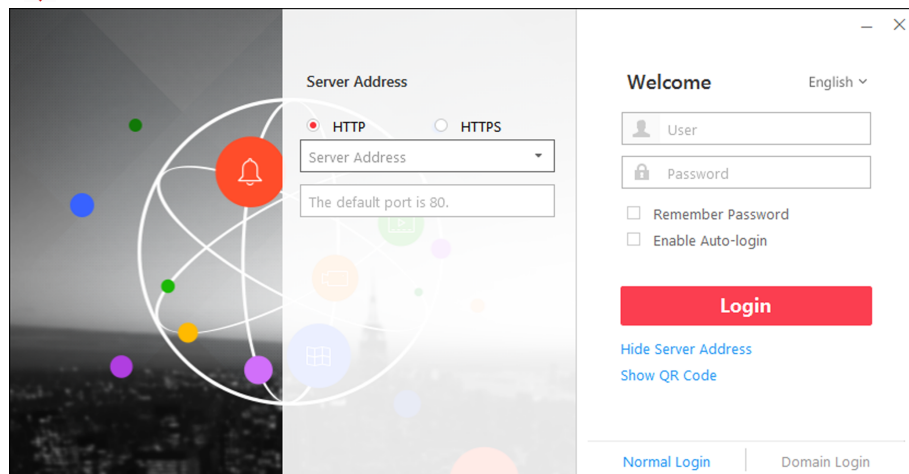


Figure 10-1 Login Page

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

Note

You can click **Hide Server Address** or **Show Server Address** to hide or show the server network information.

Transfer Protocol

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

Server Address

Enter the address (IP address or domain name) of the server that running the VSM service you want to connect to.

Port

Enter the port number of the server that running the VSM service. By default, it's 80 for HTTP and 443 for HTTPS.

4. Enter the user name and password of the HikCentral.



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 a 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.

10.2 Start Live View

Live view shows you the live video getting from cameras.

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  (Logical Resource) tab.

The areas which the current user has permission to access are displayed in the list and the logical resources which the user has permission to access are displayed in the corresponding areas.

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 in the same area

Double-click the area name after selecting the display window to start live view. Or you can drag the area to the display window, and click **Play in Batch** to start the live view.



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

10.3 Normal Playback

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



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

10.3.1 Search Video File

You can search video files by camera, by area, or by time for normal playback. And you can also filter the searched video files by video type or by storage location.

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.



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.

Today's recorded video files of the selected camera will be played.

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.

5. **Optional:** Click  on the toolbar to select video type and storage location for playback.



Note

To set the storage location for recording, refer to *User Manual of HikCentral Web Client*.

10.3.2 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.



Note

The playback window supports up to 16 cameras.

The playback window will play today's recorded video files of the channels in live view.

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



Note

The video files of different types are color coded.



Figure 10-2 Play Video Files

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 11 Search 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. Enter the Control Client's Alarm & Event Search module and click the **Alarm Search** or **Event Search** tab.
2. Select the types of event source.
3. Set search conditions for different event source types.
4. Set the time range for search.
 - Select a predefined time period for search.
 - Select **Custom Time Interval** and specify the start time and end time for search.
5. Click **Search**.

The matched event or alarm logs display on the list.

6. **Optional:** Perform the following operation(s) after searching alarms or events.

View Alarm Details	Click the Name field of the searched event or alarm to view the details and the linked picture, video, and map.
View Event Details	Click the Name field of the searched event to view the details and linked video.
Save Logs to PC	Click  to download the log to your PC.
Export Alarms or Events	Click Export and select the format to save the found events or alarms to your PC.



See Far, Go Further