HikCentral FocSign V2.3.0

User Manual

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
Danger	Indicates a hazardous situation which, if not avoided, will or could result in death or serious injury.
Caution	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
Note	Provides additional information to emphasize or supplement important points of the main text.

Legal Information

About this Document

- This Document 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 Document is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of the Document at the Hikvision website (***https://www.hikvision.com***). Unless otherwise agreed, Hangzhou Hikvision Digital Technology Co., Ltd. or its affiliates (hereinafter referred to as "Hikvision") makes no warranties, express or implied.
- Please use the Document with the guidance and assistance of professionals trained in supporting the Product.

About this Product

This product can only enjoy the after-sales service support in the country or region where the purchase is made.

Acknowledgment of Intellectual Property Rights

- Hikvision owns the copyrights and/or patents related to the technology embodied in the Products described in this Document, which may include licenses obtained from third parties.
- Any part of the Document, including text, pictures, graphics, etc., belongs to Hikvision. No part of this Document may be excerpted, copied, translated, or modified in whole or in part by any means without written permission.
- HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.
- Other trademarks and logos mentioned are the properties of their respective owners.

LEGAL DISCLAIMER

- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION 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, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE

PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.

- YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.
- YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.
- IN THE EVENT OF ANY CONFLICTS BETWEEN THIS DOCUMENT AND THE APPLICABLE LAW, THE LATTER PREVAILS.

Contents

Chapter 1 Overview

1.1 Introduction

HikCentral FocSign is a lightweight platform with multiple functions, featuring diverse content types, predefined program templates, abundant material types, flexible layout design, etc. You can add the devices (including digital signage terminals and interactive flat panels), create contents, and then release them to the devices after reviewing contents and creating schedules for contents. The platform is widely applied to the industry of entertainment, finance, traffic, etc.

1.2 Recommended Running Environment

The following is recommended system requirement for running the Web Client.

CPU

Intel® Core™ i5-8500 and later

Memory

8 GB and later

Web Browser

Firefox® 114 and later, Google Chrome® 114 and later, Safari® 16.6 and later, Microsoft® Edge 114 and later.

Chapter 2 Login

You can access and configure the platform via web browser directly, without installing any client software on your computer.

Note

- The Web Client transmits data via the HTTPS, using our self-developed HTTPS certificate, which is not issued by the Certificate Authority. So that a risk prompt will show when you opening the Web Client. To avoid the prompt, you can apply for a certificate from the Certificate Authority.
- The login session of the Web Client will expire and a prompt with countdown will appear after the configured time period in which there is no action.

2.1 First Time Login

If this is the first time for you to login, you can choose to login as admin or normal user according to your user role.

2.1.1 Login for First Time for Admin User

By default, the system predefined the administrator user named admin. When you login via the Web Client for the first time, you are required to create a password for the admin user before you can properly configure and operate the system.

Steps

1. In the address bar of the web browser, enter the address of the PC running FocSign server service and press **Enter** key.

   Example

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

   Note

   - You should set the transfer protocol before accessing the FocSign server. For details, refer to ***Set Transport Protocol*** .
   - You should set the FocSign server's IP address before accessing the FocSign server via WAN. For details, refer to ***Set WAN Access*** .

2. Enter a password and confirm the password for the admin user in the pop-up Create Password window, and click **Next**.

Note

The password strength can be checked by the system and should meet the system requirements. The default minimum password strength should be **Medium**. For setting minimum password strength, refer to ***Set Basic Security Parameters*** .

Caution

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

3. Select a method for password reset verification.
   - **Email**: Click **Verification Code → Next** and set the email address for receiving the password reset verification code.
   - **Security Question**: Click **Security Question → Next** , select three different security questions from the drop-down lists, and enter your answers accordingly.

Note

If you forget the password of your account, you can reset the password by verifying your email address or answering the security questions. Refer to ***Forgot Password*** for details.

4. Click **Finish**.

   The home page of the Web Client will show if the admin password is created successfully.

2.1.2 First Time Login for Normal User

When you log in to the system as normal user via Web Client for the first time, you should change the initial password and set a new password for login.

Steps

1. In the address bar of the web browser, input the address of the PC running FocSign server service and press the **Enter** key.

   Example

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

Note

You should configure the FocSign server's IP address in WAN Access of System Configuration before accessing the FocSign server via WAN. For details, refer to ***Set WAN Access*** .

2. Enter the user name and password.

Note

Contact the administrator for the user name and initial password.

3. Click **Log In** and the **Change Password** window opens.
4. Set a new password and confirm the password.

Note

The password strength can be checked by the system and should meet the system requirements. If password strength is lower than the required minimum strength, you will be asked to change your 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.

5. Click **OK** to change the password.

Result

Web Client home page displays after you successfully logging in.

2.2 Change Password for Reset User

When the normal user's password is reset by admin user, he/she should change the initial password and set a new password when logging into HikCentral FocSign via the Web Client.

Steps

1. In the address bar of the web browser, enter the address of the PC running FocSign server service and press **Enter** key.

   Example

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

Note

You should configure the FocSign server's IP address in WAN Access of System Configuration before accessing the FocSign server via WAN. For details, refer to ***Set WAN Access*** .

2. Enter the user name and initial password set by the administrator.
3. Click **Log In** and a **Change Password** window opens.
4. Set a new password and confirm the password.

Note

The password strength can be checked by the system and should meet the system requirements. If password strength is lower than the required minimum strength, you will be asked to change your 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.
  The password should:
  - Not contain admin, 123 or your username
  - Have no more than 3 consecutive numbers, like 1234 or 4321
  - Have no more than 3 repeating letters or numbers, like 1111 or aaaa
  - Not match commonly used risky passwords
- Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

5. Click **OK**.

Result

Web Client home page displays after you successfully changing the password.

2.3 Forgot Password

If you forget the password of your account, you can reset the password.

Before You Start

- Make sure the normal user has been configured with an available email address.
- Make sure the email server is tested successfully.

Steps

1. On the login page, click **Forgot Password**.
2. Enter your user name and click **Next**.

3. Enter the required information on the Reset Password window.
   - If you are the admin user whose account is configured with security questions, you can answer the pre-configured questions, click **Next**, and set and confirm your new password.

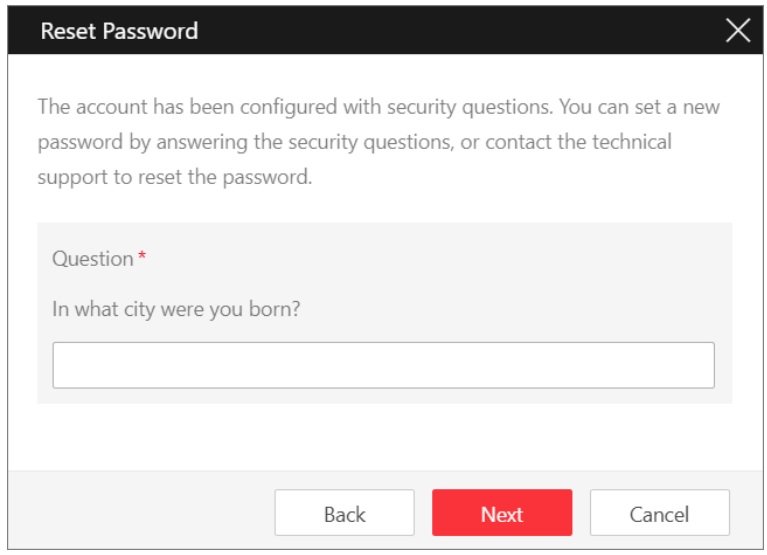

Figure 2-1 Reset Password for admin User via Security Questions

   - If you are the admin user or a normal user whose account is configured with an email address, you can click **Get Code** and a verification code will be sent to your email address. Enter the verification code you received, set a new password, and confirm the password within 10 minutes.

Note

If no email address is set for your normal user account, you need to contact the admin user to reset your password.

   - If you are an admin whose account is configured with an email address, you can select **Activation Code** and click **Next**, and then reset the password by the code you get.

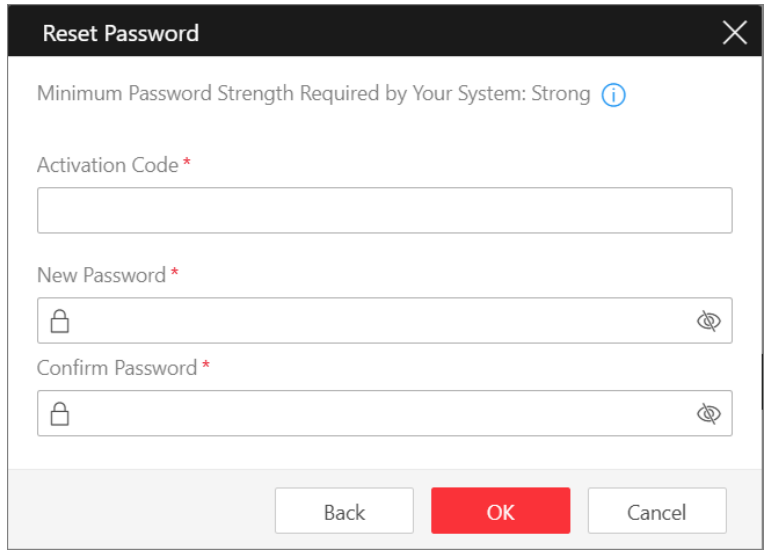

Figure 2-3 Reset Password via Activation Code

- If you are a domain user, you need to contact the admin user to reset your password.

Note

The password strength can be checked by the system and should meet the system requirements. If the password strength is lower than the required minimum strength, you will be asked to change your password. For setting the minimum password strength, refer to ***Set Basic Security Parameters*** .

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.
  The password should:
  - Not contain admin, 123 or your username
  - Have no more than 3 consecutive numbers, like 1234 or 4321
  - Have no more than 3 repeating letters or numbers, like 1111 or aaaa
  - Not match commonly used risky passwords
- Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

4. Click **OK**.

Chapter 3 Home Page Overview

The following is the introduction of the Home page.

On the top navigation bar, perform the following operations if needed.

- : View the downloading tasks.
- : View the wizards of the Digital Signage module, as well as the user manual of the Web Client.
- : Maintenance and management information of the software, such as license expiry date and license details. Refer to ***Maintenance and Management*** for details.

Centralized Device Control

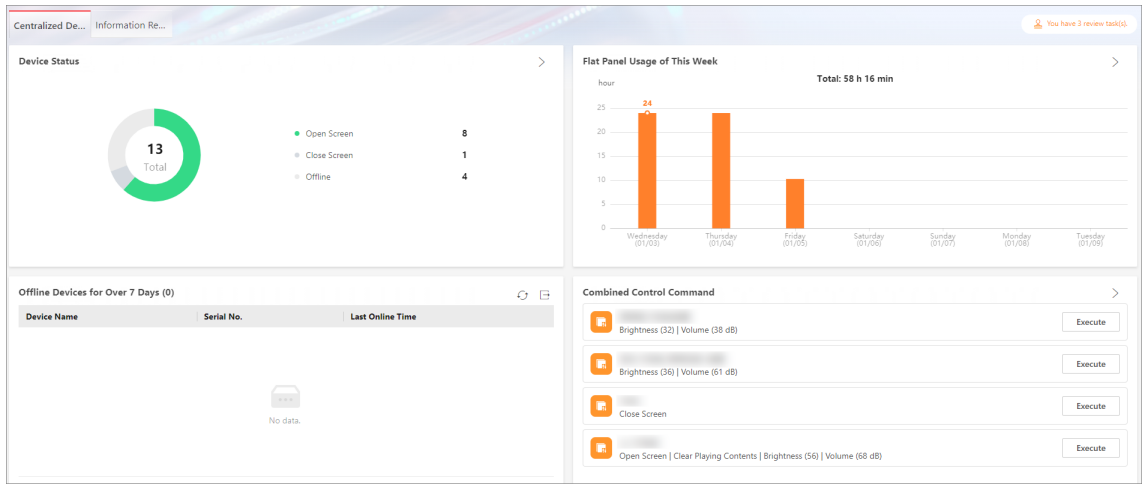

Figure 3-1 Centralized Device Control

The central device control mode supports viewing device status, flat panel usage of the this week, offline devices for over 7 days, and combined control command. You can also click › to go to the Device Control page or Flat Panel Usage Statistics page for details. In the Offline Devices for Over 7 Days area, you can refresh the list or export the information about the devices.

Information Release

In the Wizard area, click an application to perform the corresponding task.
Below the Wizard, Quick Release, Release by Template, and Material Library are displayed.

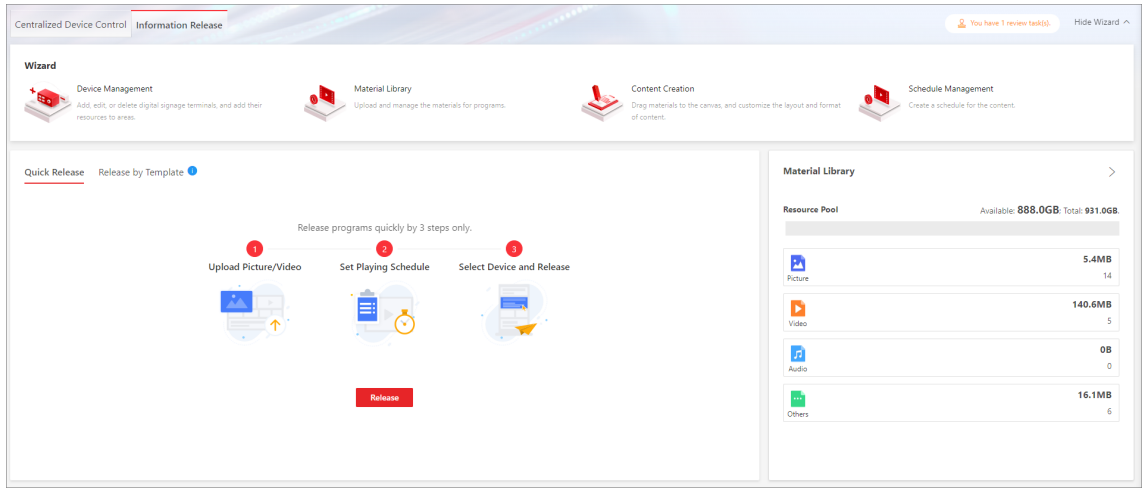

Figure 3-2 Information Release

Chapter 4 License Management

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

Two types of License are available for HikCentral FocSign:

- **Base:** You need to purchase at least one basic License to activate the HikCentral FocSign.
- **Expansion:** If you want to increase the capability of your system, you can purchase an expanded License to get additional features.

Note

- Only the admin user can perform the activation, update, and deactivation operation.
- If you encounter any problems during activation, update, and deactivation, please send the server logs to our technical support engineers.

4.1 Activate License - Online

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

Steps

1. Log in to HikCentral FocSign via the Web Client.
2. On the Home page, click **Activate** to open the Activate License panel.
3. Click **Online Activation** to activate the License in online mode.
4. Enter the activation code received when you purchased your License.

   Note

   - If you have purchased more than one Licenses, you can click + and enter other activation codes.
   - The activation code should contain 16 characters or 32 characters (except dashes).
5. Check **I accept the terms of the agreement** to open the License Agreement pane and click **OK**.
6. Click **Activate**.

   The details of the activated license will be displayed. The email settings pane will appear after you activated the License.
7. Enter an email address for the admin user.

   Note

   This email is used to receive the License activation code when the admin user forgets the password for logging in to the platform and the activation code at the same time.

8. Set the email server parameters. See details in ***Configure Email Account*** .
9. Click **OK** to save the email settings.

4.2 Activate License - Offline

If the FocSign server to be activated cannot connect to the Internet, you can activate the License in offline mode.

Steps

1. Log in to HikCentral FocSign via the Web Client.
2. On the Home page, click **Activate** to open the Activate License panel.
3. Click **Offline Activation** to activate the License in offline mode.

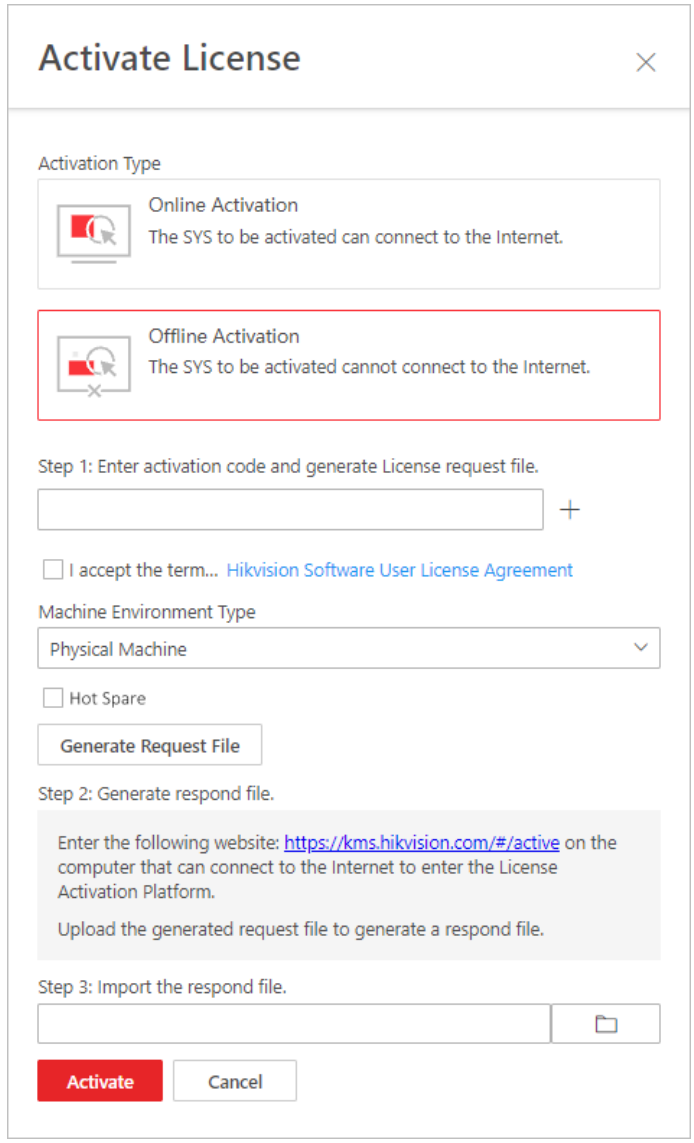

Figure 4-1 Activate License in Offline Mode

4. Enter the activation code received when you purchased your License.

Note

- If you have purchased more than one Licenses, you can click + and enter other activation codes.
- The activation code should contain 16 characters or 32 characters (except dashes).

5. Check **I accept the terms of the agreement** to open the License Agreement panel and click **OK**.
6. Click **Generate Request File**.

   A request file named "ActivationRequestFile.bin" will be downloaded. Save the request file to the proper directory or the removable storage medium (e.g., USB flash disk).
7. Copy the request file to the computer that can connect to the Internet.

8. On the computer which can connect to the Internet, enter the following website: ***https://kms.hikvision.com/#/active*** .
9. Click and then select the downloaded request file.

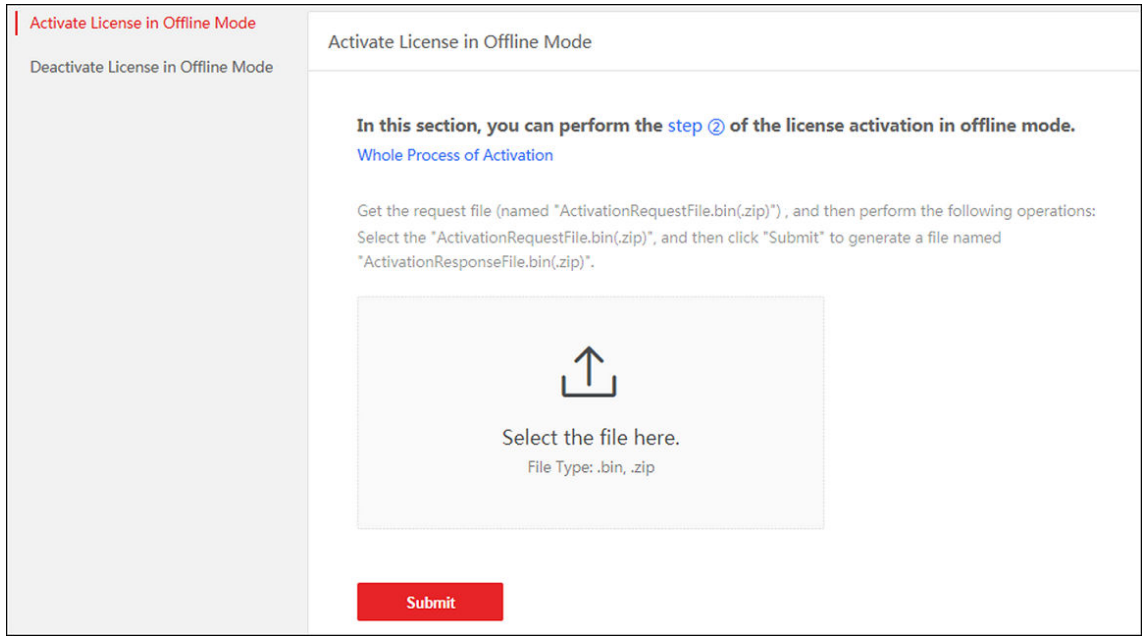

Figure 4-2 Select Request File

10. Click **Submit**.

    A respond file named "ActivationResponseFile.bin" will be downloaded. Save the respond file to the proper directory or the removable storage medium (e.g., USB flash disk).
11. Copy the respond file to the proper directory of the computer that accesses HikCentral FocSign via the Web Client.
12. In the Offline Activation panel, click and select the downloaded respond file.
13. Click **Activate**.

    The email settings pane will appear after you activated the License.
14. Enter an email address for the admin user.

    Note

    This email is used to receive the License activation code when the admin user forgets the password for logging in to the platform and the activation code at the same time.
15. Set the email server parameters. See details in ***Configure Email Account*** .
16. Click **OK** to save the email settings.

4.3 Update License - Online

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

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

Steps
1. Log in to HikCentral FocSign via the Web Client.
2. On the top, move the cursor to **Maintenance and Management** to show the drop-down menu.
3. Click **Update License** in the drop-down menu to open the Update License pane.
4. Click **Online Update** to update the License in online mode.
5. Enter the activation code received when you purchase your License.

Note
- If you have purchased more than one Licenses, you can click + and enter other activation codes.
- The activation code should contain 32 characters (except dashes).

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

4.4 Update License - Offline

As your project grows, you may need to increase the connectable number of devices for your HikCentral FocSign. If the FocSign server to be updated cannot connect to the Internet, you can update the system in offline mode.

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

Steps
1. Log in to HikCentral FocSign via the Web Client.
2. On the top, move the cursor to **Maintenance and Management** to show the drop-down menu.
3. Click **Update License** in the drop-down menu to open the Update License pane.
4. Click **Offline Update** to update the License in the offline mode.

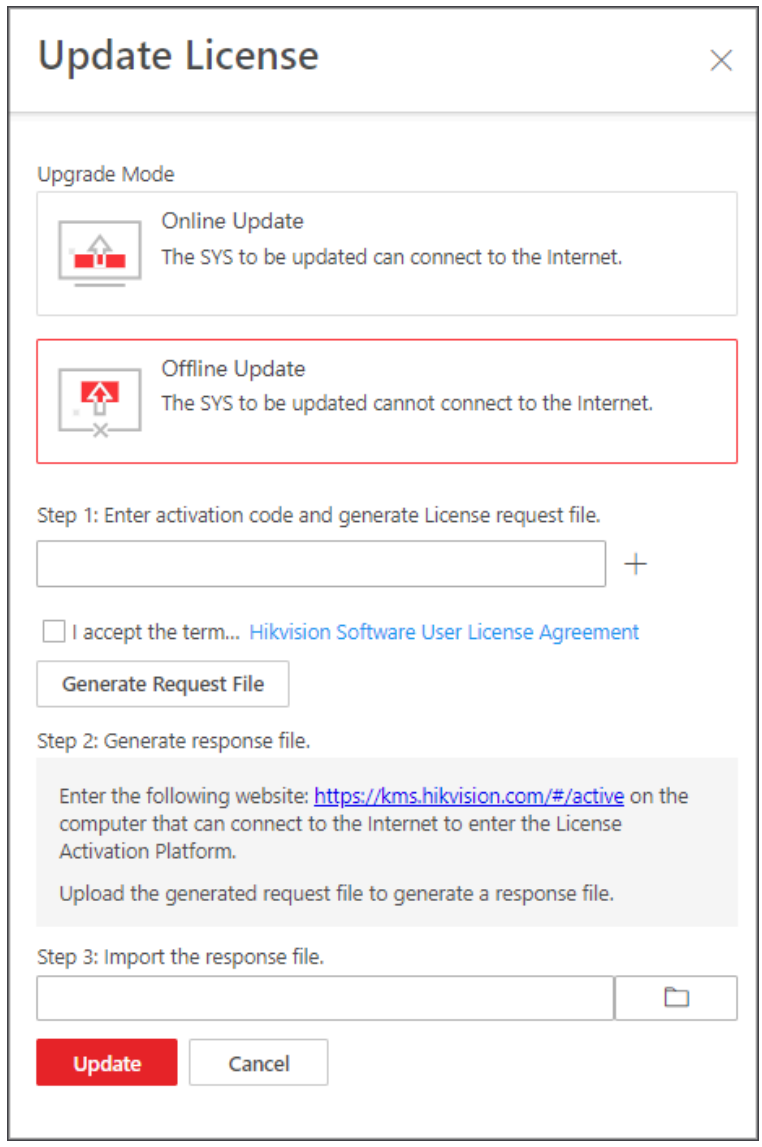

Figure 4-3 Update License in Offline Mode

5. Enter the activation code of your additional License.

Note

- If you have purchased more than one License, you can click + and enter other activation codes.
- The activation code should contain 16 characters or 32 characters (except dashes).

6. Check **I accept the terms of the agreement** to open the License Agreement panel and click **OK**.
7. Click **Generate Request File**.

   A request file named "ActivationRequestFile.bin" will be downloaded. Save the request file to the proper directory or the removable storage medium (e.g., USB flash disk).
8. Copy the request file to the computer that can connect to the Internet.

9. On the computer which can connect to the Internet, enter the following website: ***https://kms.hikvision.com/#/active*** .
10. Click and then select the downloaded request file.

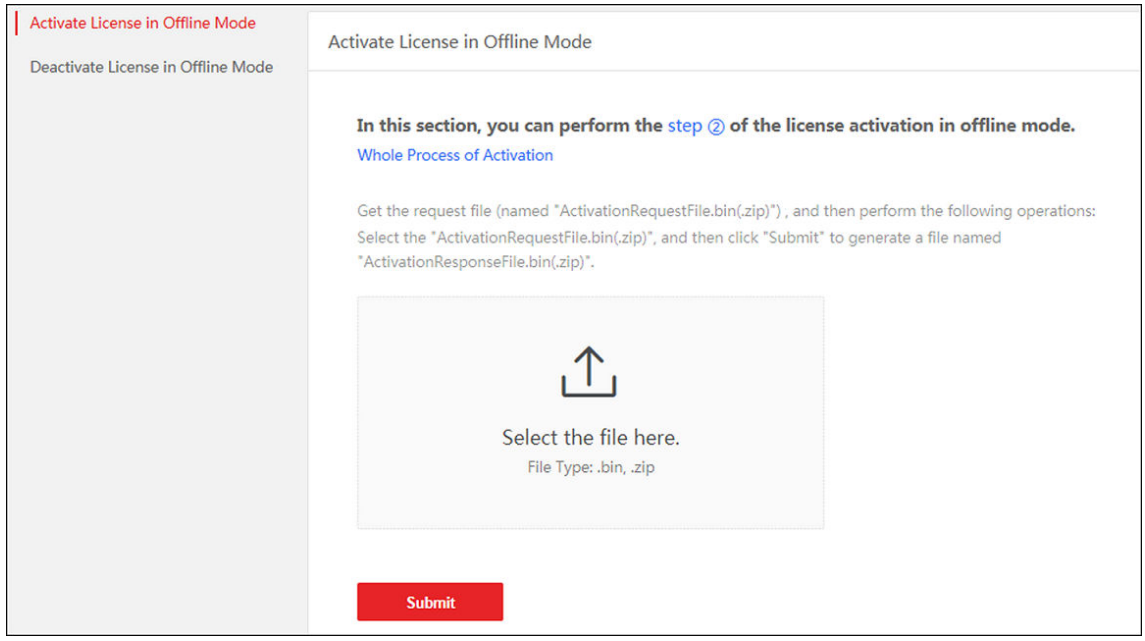

Figure 4-4 Select Request File

11. Click **Submit**.

    A respond file named "ActivationResponseFile.bin" will be downloaded. Save the respond file to the proper directory or the removable storage medium (e.g., USB flash disk).
12. Copy the respond file to the proper directory of the computer that accesses HikCentral FocSign via the Web Client.
13. In the offline update panel, click and select the downloaded respond file.
14. Click **Update**.

4.5 Deactivate License - Online

If you want to run the FocSign server on another PC or server, you should deactivate the FocSign server first and then activate it again. If the computer or server on which the FocSign serverrunning can properly connect to the Internet, you can deactivate the License in online mode.

Steps

1. Log in to HikCentral FocSign via the Web Client.
2. On the top, move the cursor to **Maintenance and Management** to show the drop-down menu.
3. Click **Deactivate License** in the drop-down menu to open the Deactivate License panel.
4. Click **Online Deactivation** to deactivate the License in online mode.
5. Check the activation code(s) to be deactivated.

6. Click **Deactivate**.

4.6 Deactivate License - Offline

If you want to run the FocSign server on another computer or server, you should deactivate the FocSign server first and then activate the FocSign server again. If the FocSign server to be deactivated cannot connect to the Internet, you can deactivate the License in offline mode.

Steps

1. Log in to the HikCentral FocSign via Web Client.
2. On the top, move the cursor to **Maintenance and Management** to show the drop-down menu.
3. Click **Deactivate License** in the drop-down menu to open the Deactivate License pane.
4. Click **Offline Deactivation** to deactivate the License in offline mode.

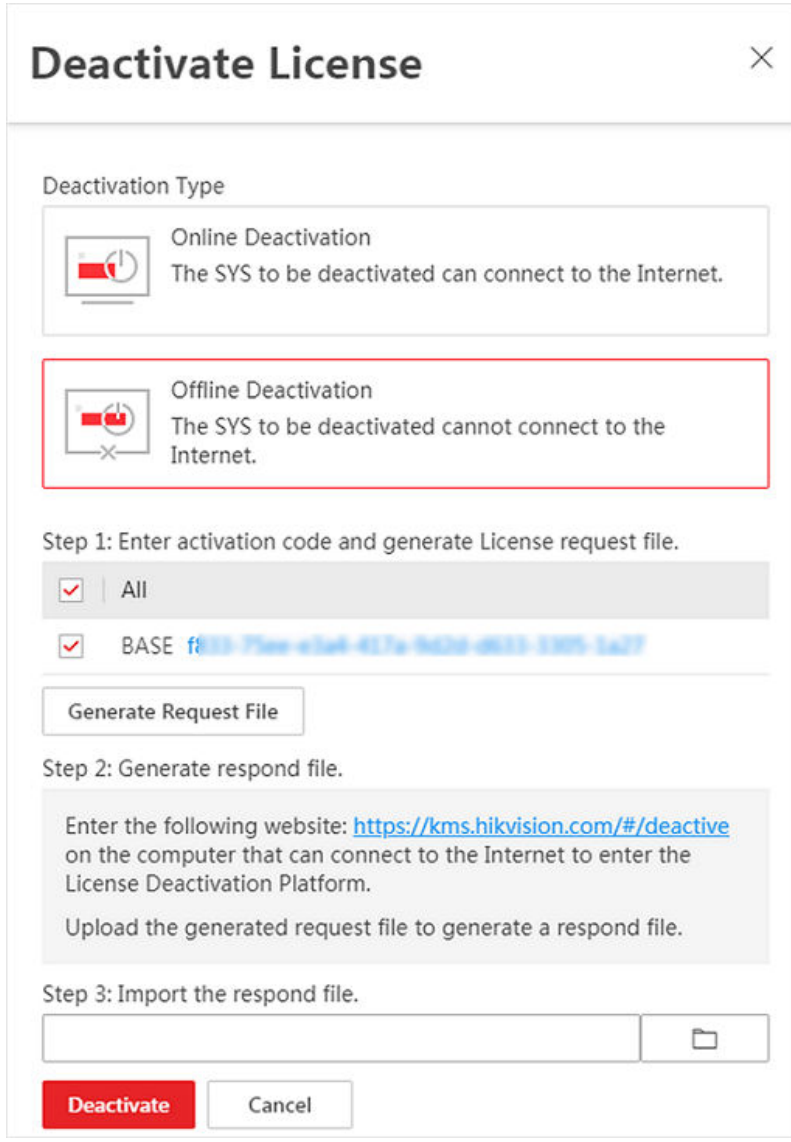

Figure 4-5 Deactivate License in Offline Mode

5. Check the activation code(s) to be deactivated.
6. Click **Generate Request File**.

Note

After the request file is generated, the selected activation code(s) will be unavailable.

A request file named "ActivationRequestFile.bin" will be downloaded. Save the request file to the proper directory or the removable storage medium (e.g., USB flash disk).

7. Copy the request file to the computer that can connect to the Internet.
8. On the computer which can connect to the Internet, enter the following website: ***https://kms.hikvision.com/#/deactive*** .

9. Click and then select the downloaded request file.

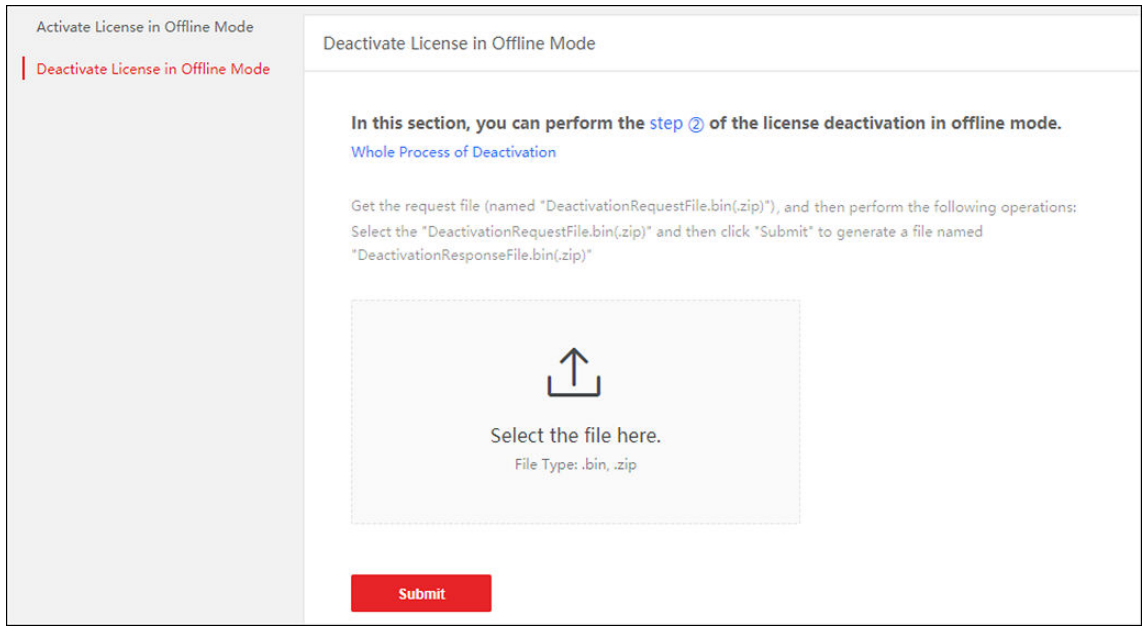

Figure 4-6 Select Request File

10. Click **Submit**.

    A respond file named "DectivationResponseFile.bin" will be downloaded. Save the respond file to the proper directory or the removable storage medium (e.g., USB flash disk).
11. Copy the respond file to the proper directory of the computer that accesses HikCentral FocSign via the Web Client.
12. In the Offline Deactivation pane, click and select the downloaded respond file.
13. Click **Deactivate**.

4.7 View License Details

You can check the authorization details of the License you purchased and view the number of manageable devices and functions of your platform. If the License is not activated, you can also view the trial period.

Steps

1. On the top, click **Maintenance and Management → License Details** to open the License Details pane.

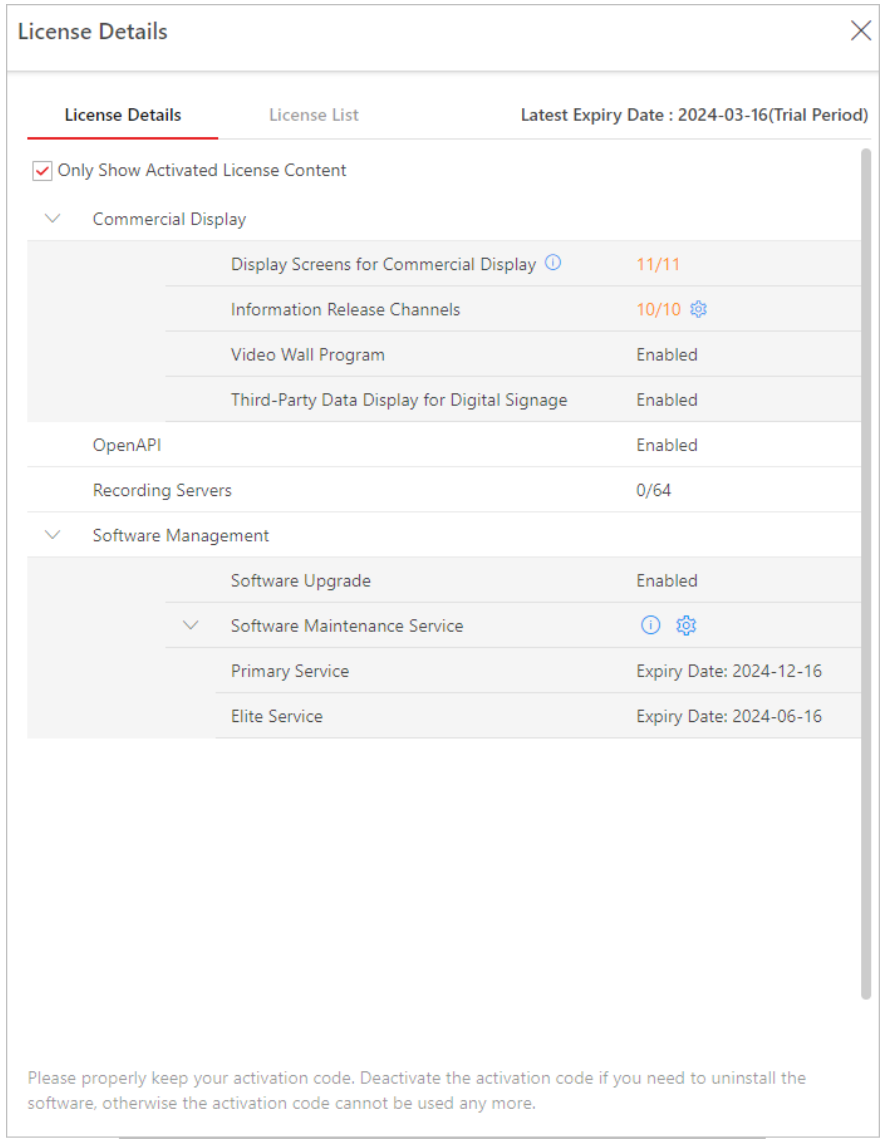

Figure 4-7 License Details Page

2. Click beside the **Information Release Channels** license to set display screens as devices for information release.
3. **Optional:** Click **License List** to check all the activated License(s) of your platform and click an activation code to view the related authorization details.

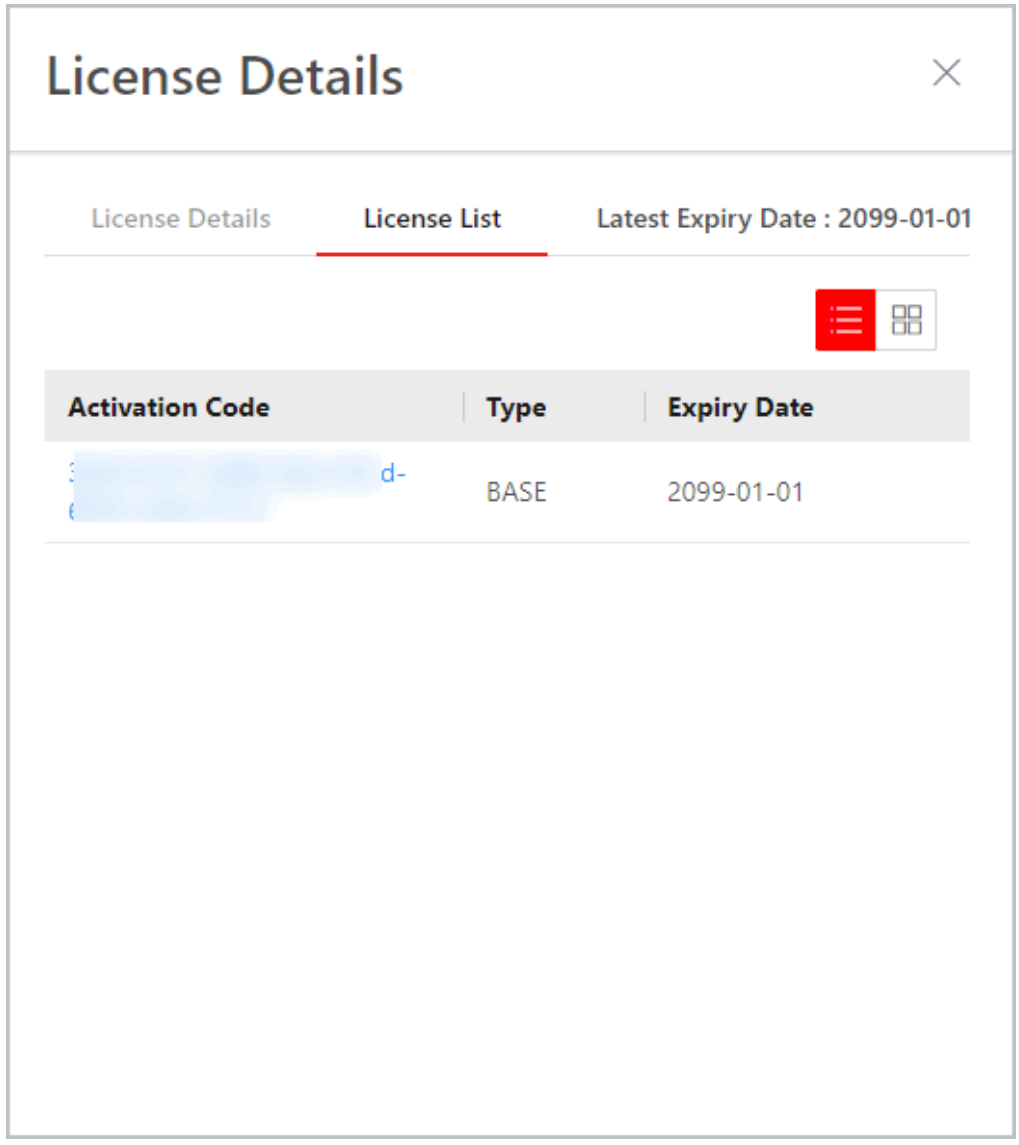

Figure 4-8 License List Page

4.8 Set SSP Expiration Prompt

SSP (Software Service Program) refers to the platform's maintenance service, which has an expire date and needs to be upgraded before expiration. You can set SSP expiration prompt on the platform. After that, when the SSP is going to expire, you can receive an email reminding the expiration every day during the configured period.

Steps

1. On the top, click **Maintenance and Management → License Details** .
2. Click beside **Software Maintenance Service** to enter the SSP Expiration Prompt Settings pane.

3. Set the **Overdue Reminder** switch to ON.
4. Set the days when you will receive the prompt email before expiration.

Note

- You should enter an integer between 1 to 365.
- By default, the platform will send a prompt email 30 days before expiration.

5. Click **Add User** to add user(s) who can receive upgrade prompt.

Note

- You should configure the users' email addresses before adding them as recipients. The added users can receive upgrade prompt via the bound email addresses.
- Up to 64 recipients can be added.
- You can click × to delete the added user(s).

6. Click **Add Email** to add email address(es).

Note

You can add email of both the platform user(s) and other user(s). The platform will send expiration prompt to the added email address(es).

7. Click **Save**.

Chapter 5 Centralized Device Control Management

HikCentral FocSign supports adding digital signage terminals, interactive flat panels, LED controllers, video wall controllers, and recording servers. You can add devices and servers to the platform and manage them according to your actual needs. Device control and interactive flat panel applications are supported after adding devices.

Note

You can go to → **Centralized Device Control** → **Device / Application** to enter this module. If you have add the target menu to the top navigation, click the menu on the top directly, and this entry will be introduced in the following.

5.1 Manage Digital Signage Terminals

Before releasing information, digital signage terminals should be added to the system first. After adding devices, you can edit and delete the devices. Further operations are also supported, including remote configuration, changing devices' password, configuring time zone, etc.

5.1.1 Add Digital Signage Terminal

You can add digital signage terminals to the platform by multiple methods: adding online terminals, adding by IP address, adding by auto registration on device, adding by IP segment, importing devices in a batch, and adding by authentication code. After adding terminals to the platform, you can configure, manage, and control the terminals.

On the left, select **Device and Server** → **Digital Signage Terminal** .

Adding Operations

Adding Mode and Scenario	Description
Add Terminal by Auto Registration on Device: you have configured the platform's IP address for the	1. Click **Add** → **Add by Auto Registration** or click **Auto Registration**. 2. Enter the platform address and authentication code on the device for registration. 3. Select device(s) from the list and click **Batch Add to Device List**. 4. Enter authentication code of the device, select time zone, and select an area. 5. Click **OK**.

Adding Mode and Scenario	Description
device by a web browser.	
Enable General Authentication Code: adding the terminal which supports OTAP/ ISUP.	The authentication code is used for the terminal to register on the platform by OTAP/ISUP. 1. Click **Auto Registration → Add by Configuring General Authentication Code on Platform** . 2. Switch on **General Authentication Code**. 3. Enter the authentication code. 4. (Optional) In the Add Resource to Area list, select an area to add the device to. 5. Click **OK**.
Add Online Terminals: the online terminals to be added are on the same LAN as the server.	Before you start, make sure: You have downloaded and installed the Web Control. 1. In the online device list, select one or multiple devices to be added, and then click **Add to Device List** to enter the Add Device page. 2. Set the basic information. 3. (Optional) Set the time zone of the device. 4. (Optional) In the Add Resource to Area list, select an area to add the device to. 5. Finish adding the device. - Click **Add** to add the current device and back to the device list page. - Click **Add and Continue** to add the current device and continue to add other devices.
Add Terminal by IP Address: you know the IP address of the terminal to be added.	1. Click **Add → Add Manually** to enter the Add Device page. 2. Select the Access Protocol as **Hikvision Private Protocol** or **Hikvision OTAP Protocol**. 3. If **Hikvision OTAP Protocol** is selected, select **IP Address/Domain** in the Adding Mode list. 4. Set the basic information. 5. (Optional) Set the time zone of the device. 6. In the Add Resource to Area list, select an area to add the device to. 7. Finish adding the device. - Click **Add** to add the current device and back to the device list page. - Click **Add and Continue** to add the current device and continue to add other devices.

Adding Mode and Scenario	Description
Add Terminals by IP Segment: multiple devices to be added have the same port number, user name, password, and have different IP addresses within a range.	1. Click **Add → Add Manually** to enter the Add Device page. 2. Select the Access Protocol as **Hikvision OTAP Protocol**. 3. (Optional) Select **IP Segment** in the Adding Mode list. 4. Enter the required information. 5. (Optional) Set the time zone of the device. 6. (Optional) In the Add Resource to Area list, select an area to add the device to. 7. Finish adding the device. - Click **Add** to add the current device and back to the device list page. - Click **Add and Continue** to add the current device and continue to add other devices.
Batch Import Terminals: multiple devices to be added.	1. Click **Add → Add Manually** to enter the Add Device page. 2. Select the Access Protocol as **Hikvision Private Protocol** or **Hikvision OTAP Protocol**. 3. Select **Batch Import** in the Adding Mode list. 4. Click **Download Template** and save the predefined template (excel file) on your PC. 5. Open the exported template file and enter the required information of the devices to be added in the corresponding column. 6. Click and select the edited file. 7. (Optional) Set the time zone of the device. 8. (Optional) In the Add Resource to Area list, select an area to add the device to. 9. Finish adding the device. - Click **Add** to add the current device and back to the device list page. - Click **Add and Continue** to add the current device and continue to add other devices.

After Adding Digital Signage Terminals: Operations on Device List Page

After you add digital signage terminals, you can perform further operations on the device list.

Operation	Description
Change Password	Select one or more devices, and click **Change Password** to change the password for the selected devices.

Operation	Description
	Note If multiple devices have the same password, you can change the password for them simultaneously.
Set Time Zone	Select one or more devices, and click **Time Zone** to configure the time zones of the selected devices. You can select **Get Device's Time Zone** or **Manually Set Time Zone** according to your requirements.
Search Device(s)	Enter a keyword in the search box on the upper right corner of the page to quickly search the target device(s).

5.1.2 Configure Device Parameters Remotely

After adding terminal (called device in the following pages) to the system, you can configure the parameters of the device remotely, including configuring built-in camera's parameters, linking external camera, configuring displaying settings and other parameters.

Configure Built-In Camera Parameters

Built-in camera is the camera built in the terminal. After adding a terminal to the platform, you should configure parameters for the built-in camera, such as device name, function, and face similarity.

Before You Start
Make sure at least one terminal is added to the platform, and make sure the terminal is online.

Steps
1. On the left navigation pane, click **Device and Server → Digital Signage Terminal** .
2. Click ⚙ on the Operation column to enter the device remote configuration page of terminal.
3. In the **Linked Device** area, click **Built-In Camera** to enter the camera parameters settings page.
4. Set the parameters.

Device Name

The device name of the built-in camera.

Live View

The live view of the camera will be displayed in the live view window of the normal programs.

Similarity

Set the face similarity. When the captured face picture's similarity reaches the value, it will be regarded as comparison succeeded.

Recognition Distance

It is used to control the recognition distance between the person and camera.

Wearing Mask

Select **Yes** or **No** from the drop-down list.

Yes: The camera will recognize persons wearing masks.

No: The camera will not recognize persons wearing masks.

Mask Detection

Check **Mask Detection**, then when the camera detects people without masks, the corresponding prompt will be displayed on the terminal.

Face Detection Frame

Check **Face Detection Frame**, then when the camera detects a face, a frame will be displayed on the terminal.

Quick Capture

Check **Quick Capture**, then the camera can recognize and capture a face more frequently even if the face is far away.

5. Click **Save** to save the above settings.

Link External Device to Terminal

After adding terminals to the platform, you can link external devices such as cameras to the terminals for attendance, live view, or temperature screening.

Before You Start

- Make sure the external device has been installed properly.
- Make sure at least one online terminal is added to the platform.

Steps

1. On the left navigation pane, click **Device and Server → Digital Signage Terminal** .
2. Click ⚙ in the Operation column of the online device to enter the remote configuration page of the terminal.
3. In the **Linked Device** area, click **Add** to enter the Add Device page.

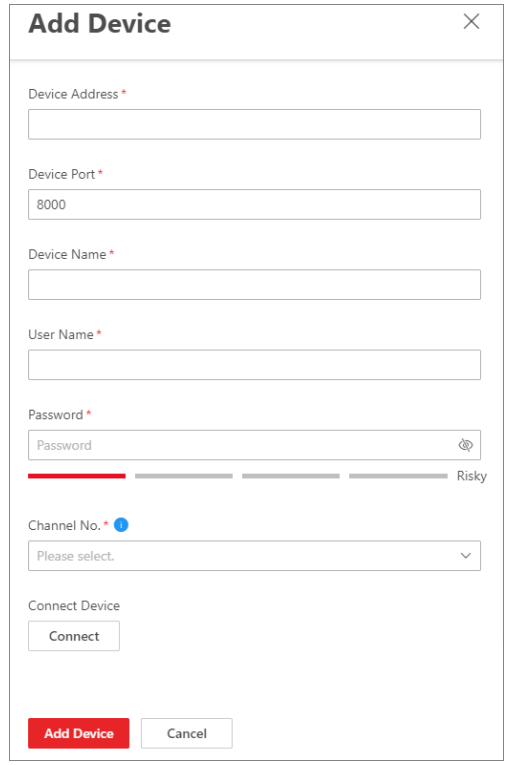

Figure 5-1 Add Device

4. Set the following parameters.

Device Address

The IP address of the device.

Device Port

The port No., of the device. By default, it is 8000.

Device Name

The name of the device, which can be used to describe the function, location, etc., of the device.

User Name

The user name of logging into the device.

Password

The password of the device.

5. Select the channel number of the device to be added to the terminal from the drop-down list.
6. **Optional:** Click **Connect** to connect to the device.

Note

- After connecting to the device, you can configure the function for the selected channel. For details, refer to ***Configure Built-In Camera Parameters*** .

7. Click **Add Device**.

Configure More Parameters

On the remote configuration page of terminal, you can configure other parameters except for built-in camera and external camera, such as basic information, time settings, device operations, timed configuration and maintenance.

Note

On the upper-right corner of the configuration page, you can click **Copy To** to copy the configuration of the current device to other devices.

Basic Information

Device Address

Display the IP address of the terminal by default.

Subnet Mask

Display the subnet mask of the terminal by default.

Gateway

Display the gateway of the terminal by default.

Time Settings

Click to customize the time settings.
You can also select **Sync with Server Time** to synchronize time from the server.

Device Operation, Timed Settings and Maintenance

The display settings of the terminal, refer to ***Configure Device Display Settings*** for details.

5.1.3 Configure Device Display Settings

After adding the digital signage terminal (called device in the following pages) to the platform, you can configure the display parameters of the device remotely, including the brightness, boot logo, etc.

Before You Start

Make sure you have added the device(s) to the platform, and the device(s) are online. Refer to ***Add Digital Signage Terminal*** for details.

Steps

1. On the left navigation pane, click **Device and Server → Digital Signage Terminal** .
2. Click on the Operation column to enter the device remote configuration page of terminal.
3. In the **Text on Screen** area, set the text related parameters.

Brightness Settings

Drag the brightness bar to adjust the brightness of the screen, or manually enter the brightness value. The brightness value is 0 to100. The bigger the value, the lighter the screen.

Boot Logo

After enabled, the logo will be displayed when the terminal starts up. The logo is set on the terminal locally.

Screen Direction

0

The screen direction is 0° by default.

90/180/270

The screen direction will rotate 90°/180°/270° clockwise.

Enter the Password to Unlock Screen

After the screen is locked, the password is required to unlock the screen. The password is set on the device locally.

4. In the **Timed Startup/Shutdown** area, set the timed related parameters.

Timed Startup / Shutdown

General Schedule

After enabled, you should select the schedule as **Daily Schedule** or **Weekly Schedule**, and then the terminal will start up or shut down according to the schedule.

Drag the mouse on the time bar to draw the start up time duration (blue bar) of one day. The terminal will be shut down on the other time period.

Holiday Schedule

a. Click **Add Holiday** to select holidy template(s). In the lower-lower left corner, you can click **add** to create a holiday template.
b. Drag the mouse on the time bar of the holiday to draw the start up time duration (blue bar) of one day. The device will be shut down on the other time period.

Note

- Supports drawing up to 8 time periods of one day.
- You can click the time period (blue bar), enter the start time and end time of the time period.
- You can click **Erase** to clear the wrong time period you draw on the time bar.

Volume Schedule

You can select the schedule as **Daily Schedule** or **Weekly Schedule**, and then the device's volume will turned on/off according to the schedule.

Drag the mouse on the time bar to draw the start up time duration (blue bar) of one day. The terminal will be shut down on the other time period.

Note

- Supports drawing up to 8 time periods of one day.
- You can click the time period (blue bar), enter the start time and end time of the time period.
- You can click **Erase** to clear the wrong time period(s) you draw on the time bar.

5. **Optional:** In the **Maintenance** area, set related parameters such as **Lock USB** and **Lock WLAN**.

SADP

After enabled, the terminal(s) can be detected by the platform via SADP protocol, and be displayed on the online device list.

Note

- You can enable SADP protocol for either single or multiple terminal(s).
- This function should be supported by the device.

Restore to Factory Settings

Click **Restore** and enter the device password to restore the displaying parameters to the default parameters.

6. Click **Save** to save the configuration.

5.2 Manage Interactive Flat Panel

On the left, select **Device and Server → Interactive Flat Panel** .

5.2.1 Add Interactive Flat Panels

You can add interactive flat panels by auto registration on device and general authentication code.

Adding Mode and Scenario	Description
Add by Auto Registration on Device	1. Click **Auto Registration → Add by Auto Registration on Device** . 2. Follow the instructions on the interface to add the interactive flat panel.
Add by Configuring General Authentication Code on Platform: the device is configured with authentication code.	1. Click **Auto Registration → Add by Configuring General Authentication Code on Platform** . 2. Switch on **General Authentication Code**. 3. Enter the authentication code. 4. Select resources in **Add Resource to Area** to import the resources of the added devices to an area.

Adding Mode and Scenario	Description
	5. Click **OK**. 6. Register the interactive flat panel online: Enter the IP address of the platform, device name, registration port No. (7660 by default), and the authentication code on the Integrated Control App on the device. Then the device will be added to the platform automatically.

5.2.2 After Adding Interactive Flat Panels: Operations on Device List Page

After adding interactive flat panels to the platform, you can configure, manage and control them as needed.

Operations	Descriptions
Remote Configurations	Click ⚙ in the Operation column to set the remote configurations of the corresponding device. **Note** For detailed operation steps about remote configuration, see the user manual of the device.
Set Time Zone	Select one or more device(s), click **Time Zone** to set/edit the time zone of the selected device(s).
Search Device	Enter keyword(s) in the search box in the top right corner, and click 🔍 (or press the Enter key) to search for the target device(s).

5.3 Add LED Controller

You can add LED controllers to the platform by multiple methods: adding online LED controllers, adding by IP address, adding by IP segment, and importing devices in a batch. After adding LED controllers to the platform, you can configure, manage, and control them.

On the left, select **Device and Server → LED Controller** , and select one of the following methods to add LED controllers.

User Intention and Adding Method	Steps
Add Online LED Controllers: the online devices to be added are on the same LAN as the server.	Before you start, make sure: You have downloaded and installed the Web Control. 1. In the online device list, select **Local Network** or **Server Network**. 2. Select one or multiple devices to be added, and then click **Add to Device List** to enter the Add Device page. 3. Set the basic information. 4. (Optional) Check **Get Device's Time Zone** or check **Manually Set Time Zone** to select the time zone of the device. 5. In the Add Resource to Area list, select an area to add the device to.
Add by IP Address: you know the IP address of the device to be added.	1. Click **Add** to enter the Add Device page. 2. Select **IP Address** as the adding mode. 3. Set the basic information. 4. (Optional) Check **Get Device's Time Zone** or check **Manually Set Time Zone** to select the time zone of the device. 5. In the Add Resource to Area list, select an area to add the device to.
Add by IP Segment: multiple devices to be added have the same port number, user name, password, and have different IP addresses within a range.	1. Click **Add** to enter the Add Device page. 2. Select **IP Segment** as the adding mode. 3. Set the basic information. 4. (Optional) Check **Get Device's Time Zone** or check **Manually Set Time Zone** to select the time zone of the device. 5. In the Add Resource to Area list, select an area to add the device to.
Batch Import: there are multiple devices to be added.	1. Click **Add** to enter the Add Device page. 2. Select **Batch Import** in the Adding Mode list. 3. Click **Download Template** and save the predefined template (excel file) on your PC. 4. Open the exported template file and enter the required information of the devices to be added in the corresponding column. 5. Click and select the edited file. 6. In the Add Resource to Area list, select an area to add the device to.

Finish adding the device.

- Click **Add** to add the current device and back to the device list page.
- Click **Add and Continue** to add the current device and continue to add other devices.

After adding LED controllers, you can perform the following operations.

Operation	Description
View Device Error	If the device error exist, hover the cursor over to view the error's cause, and click **Configure** to edit the device settings.
Remote Configuration	In the Operation column, click to enter the remote configuration page of device and configure more parameters.
Search Device	Enter keyword(s) in the search box in the top right corner, and click (or press the Enter key) to search for the target device(s).

5.4 Manage Video Wall Controllers

The video wall controller connects multiple inputs and outputs to enable a single display made up of multiple screens tiled together. It is usually applied to the over-4K ultra-size LED screen display for shopping malls, highways, football pitch, etc. with easy and smooth operating experience. On the platform, you can manage video wall controllers and configure display wall(s) for each video wall controller, control display walls, etc.

5.4.1 Add Video Wall Controller

You can add video wall controllers to show videos on LED displays.

1. On the left, select **Device and Server → Video Wall Controller** .
2. Under the **Video Wall Controller**, click **Add**.
3. Set the adding mode.

Adding Mode	Scenario
Online Device	Devices are within the network where the Web Client or FocSign server server is located. **Note** - For Google Chrome, install the SADP service according to the instructions. For Firefox, install the SADP service and import the certificate according to the instructions. - Server Network: The detected online devices in the same local subnet with the FocSign server server will be listed. Local Network: The detected online devices in the same local subnet with the Web Client will be listed.
IP Address	Add devices one by one when you know the IP address.

Adding Mode	Scenario
IP Segment	Add multiple decoding devices with the same port number, user name and password, but different IP addresses within a range.
Port Segment	Add multiple decoding devices with the same IP address, user name and password, but different port numbers within a range.

4. Click **Add**.

5.4.2 Add Display Wall

After a video wall controller is added, you can add display wall(s), and link video wall controller outputs with display wall windows.

Note

The number of total spliced windows (of all display walls) should not exceed the number of total outputs (of all video wall controllers).

Add Display Wall

On the left, select **Device and Server → Video Wall Controller** . Click **Add** under Screen Splicing.

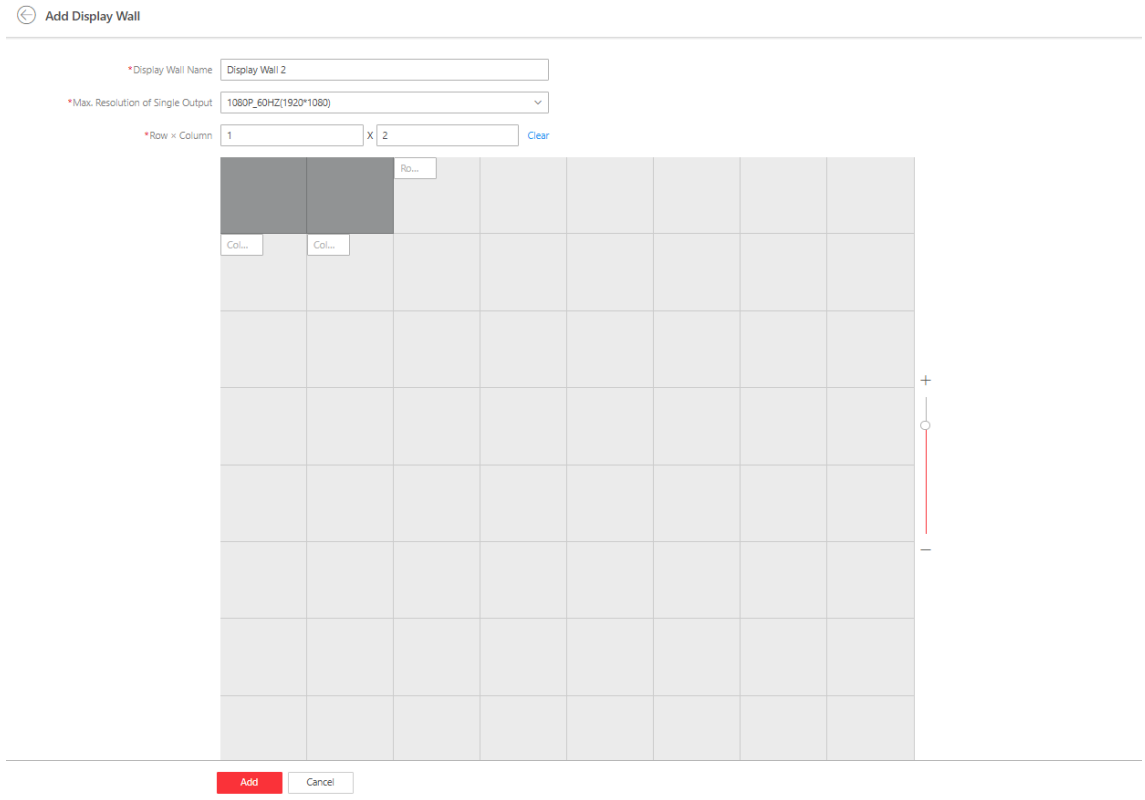

Figure 5-2 Add Display Wall

Enter the display wall name, select a max. output resolution, and specify the rows and columns.
Click **Add**.
After display walls are added, you can perform further operations.

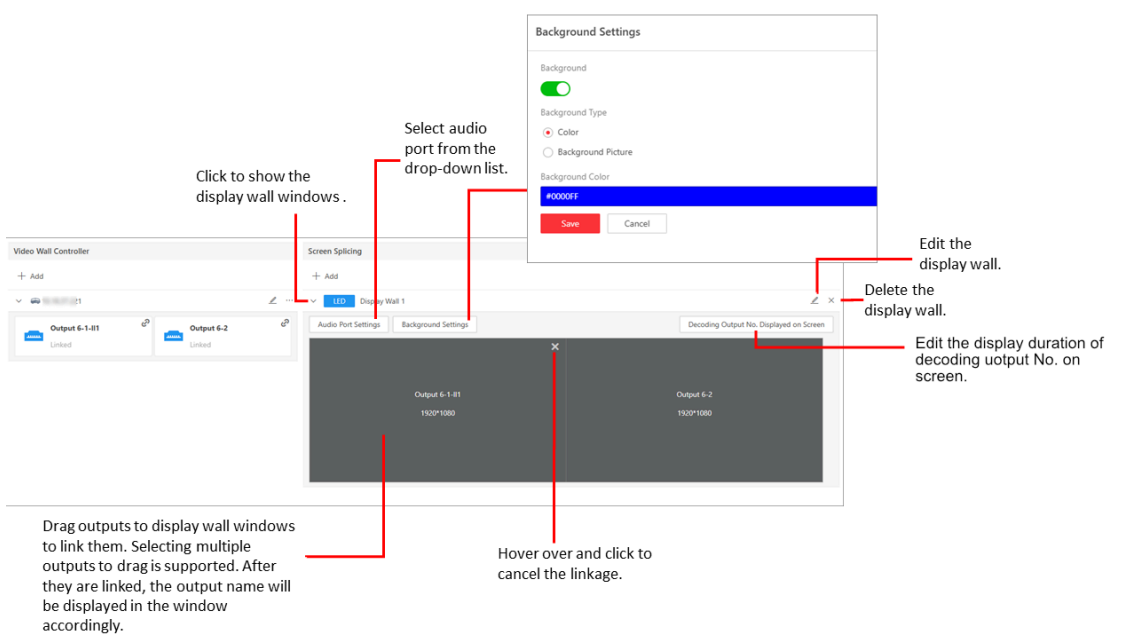

Figure 5-3 Further Operations

5.4.3 Display Control

On the Web Client, you need to add video wall controllers and create virtual display walls. Then you need to link the video wall controllers' outputs to the windows of the virtual display wall. After the configuration, the camera's videos will be displayed on the display wall to get a complete and clear overview of these videos. In this module, you can configure the display parameters of a display wall by view.

Note

Make sure you have added a display wall. Refer to ***Add Display Wall*** for details.

1. On the top, select → **Display Control** .
2. Select a display wall. The linked outputs of the display wall will be displayed on the left. You can manage them by group.

View Configuration

A view is a window division with resource channels (e.g., cameras) linked to each window. View mode enables you to save the window division and the correspondence between cameras and windows as the default so that you can quickly access these channels later. For example, you can link camera 1, camera 2, and camera 3 located in your office to the certain display windows and

save them as a view called ***office***. Then, you can access the view ***office*** and these cameras will display in the linked window quickly.

1. Add a custom view group.
   a. Click **Add View Group**, and select **Public View** or **Private View** to add the view group.

   Note

   The view groups and views that belong to the private view group are hidden from the other users.

   b. Set a name for the view group, and click **Save**.
2. Select a view group, and click **Add View**.
3. Select **Layout** on the top of the display wall windows to select a window division mode.
4. Drag a single resource to a window.
5. Perform the following operations as needed.
   - Click **Start Auto-Switch** to start the auto-switch of the views in the selected view group. You can click **Stop Auto-Switch** or **Stop** on the top of the display wall to stop auto-switch.
   - Click on a view to set the auto-switch interval.
   - Click **Text** to set the text to be displayed on the display wall.
6. Click **Save View**. You can modify the view's group and name, and configure the scheduled play and the storage location of the view.

5.5 Add pStor

You can add a pStor server as a recording server to the HikCentral FocSign for storing the videos and pictures.

Before You Start

- Make sure the pStor servers 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 FocSign via network.

Steps

1. On the top, select **Device**.
2. Select **Device and Server → Recording Server** on the left.
3. Click **Add** to enter the Add Recording Server page.

   Note

   If the NTP server is not configured, a prompt message will appear on the top of the page. You can click **Configure** to set the time synchronization.
4. Select **pStor**.
5. Enter the network parameters.

   Address

The pStor server's IP address in LAN that can communicate with FocSign server.

ANR Function

You can check this field to enable the ANR function. This function is enabled default. If the network is disconnected between the pStor and the encoding device, data can be stored on the pStor automatically.

Control Port

The control port No. of the pStor server. If it is not changed, use the default value.

Network Port

The network port No. of the pStor server. If it is not changed, use the default value.

Signaling Gateway Port

The signaling gateway port No. of the pStor server. If it is not changed, use the default value.

6. **Optional:** Check **ANR Function** or not.

Note

This function is enabled default. If the network is disconnected between the pStor and the encoding device, data can be stored on the pStor automatically.

7. Enter the user's access secret key and secret key of the pStor server for downloading pictures.

Note

You can download these two keys on the pStor server's Web Client page.

8. Enter the name, user name, and password of the pStor server.

Caution

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

9. Finish adding the server.
   - Click **Add** to add the server and back to the server list page.
   - Click **Add and Continue** to save the settings and continue to add other servers.
10. **Optional:** Perform the following operations after adding the server.

Edit Server	Click **Name** field of the server and you can edit the information of the server and view its storage information.
Delete Server	Select the server(s) from the list, and click **Delete** to remove the selected server(s).

Configure Server	Click ⚙ in the Operation column to enter the login page of the pStor server. You can log in and configure the pStor server.
Search for Server	Enter keyword(s) in the search box in the top right corner to search for the target server(s).

5.6 General Device Operations

You can perform operations including creating password for inactive device(s), editing online device's network information, upgrading device firmware, and resetting device password.

5.6.1 Create Password for Inactive Device(s)

The devices with simple default password may be accessed by the unauthorized user easily. For the security purpose, the default password is not provided for some devices. You are required to create the password to activate them before adding them to the platform. Besides activating the device one by one, you can also batch activate multiple devices which have the same password simultaneously.

Before You Start

- Make sure the devices you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the HikCentral FocSign via network.
- This function should be supported by the device. Make sure the devices you want to activate support this function.

Steps

1. On the left, click **Device and Server** to select a device type.
2. In the Online Device area, view the device status and select one or multiple inactive devices.
3. Click **Activate** to open the device activation window.
4. Create a password in the password field, and confirm the password.

Caution

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

5. Click **Save** to create the password for the device.

Note

If you have not set security questions, the window of setting security questions will pop up, and you should select the method of resetting password and set the security questions as needed.

An **Operation completed.** message is displayed when the password is set successfully.

6. Click in the Operation column to change the device's IP address, subnet mask, gateway, and so on if needed.

Note

For details, refer to ***Edit Online Device's Network Information*** .

5.6.2 Edit Online Device's Network Information

The online devices, which have IP addresses in the same local subnet with FocSign server or Web Client, can be detected by HikCentral FocSign. For the detected online devices, you can edit their network information as desired via HikCentral FocSign remotely and conveniently. For example, you can change the device IP address due to the changes of the network.

Before You Start

For some devices, you should activate it before editing its network information. Refer to ***Create Password for Inactive Device(s)*** for details.

Perform this task when you need to edit the network information for the detected online devices.

Steps

1. On the left, click **Device and Server** to select a device type.
2. In the Online Device area, select a network type.

   Server Network

   The detected online devices in the same local subnet with the FocSign server will be listed.

   Local Network

   The detected online devices in the same local subnet with the Web Client will be listed.
3. View the device status, and click in the Operation column of an active device.
4. Edit the device parameters, such as IP address, device port, subnet mask, and gateway.

Note

The parameters may vary for different device types.

5. Click .
6. Enter the device's password.
7. Click **Save**.

5.6.3 Upgrade Device Firmware

You can upgrade the firmwares of the devices added to the system according to device type and upgrade mode for accessing latest device functions. The following upgrade methods are supported: upgrading via current Web Client, upgrade via Hik-Connect, and upgrade the old device version.

Upgrade Device Firmware via Current Web Client

You can upgrade device firmware via the current Web Client.

Before You Start
Prepare the firmware package and store the package in the local disk of the PC running the Web Client.

Steps
1. On the left, select **Firmware Upgrade** to enter the firmware upgrade page.
2. Select the **Via Current Web Client** tab.
3. In the **Simultaneous Upgrade** field, set the maximum number of devices for simultaneous upgrade.

   Example

   If you set the value to 5, up to 5 devices can be selected for batch upgrade.
4. Click to select the firmware upgrade package.
5. Click **Next**.

   The devices to be upgraded are displayed in the list.
6. Select the devices to be upgraded.
7. Select an upgrade schedule to upgrade the selected device(s).
   - Select **Upgrade Now** from the **Upgrade Schedule** drop-down list to start upgrade.
   - Select **Custom** from the **Upgrade Schedule** drop-down list and then customize a time period to upgrade the selected device(s).
8. Click **OK** to save the firmware upgrade settings.

   The upgrade task list will be opened.

What to do next
Click **Upgrade Tasks** on the upper-right corner of the page to view the upgrade tasks and status.

Upgrade Device Firmware via Hik-Connect

You can upgrade firmwares of devices added to the platform. The supported device types include encoding devices, access control devices, security control devices, and so on.

Steps
1. Select **Firmware Upgrade** on the left.

2. Select the Via Hik-Connect tab.
3. In the **Device Access Protocol** field, select the relevant protocol.
4. In the **Upgrade By** field, select the upgrade method.

Note

You can hover the cursor to and view explanations of upgrade methods.

5. Set the maximum number of devices for simultaneous upgrade.

Example

For example, if you set the value to 5, up to 5 devices can be selected for batch upgrade.

6. Click **Next**.

The upgradable devices will be displayed.

7. Select the devices to be upgraded.
8. Select the upgrade schedule.
   - Select **Upgrade Now** to upgrade devices now.
   - Select **Custom** to customize a time period to upgrade devices.

Device firmware starts upgrading.

9. Click **OK** to save the firmware upgrade settings.

The upgrade task list will be open.

10. **Optional:** In the top right corner of firmware upgrade page, click **Upgrade Tasks** to view the task details and control the task status.

Upgrade Old Device Firmware

For the terminal whose firmware version is old, the platform can automatically detect this terminal need to be upgraded, and you can manually upgrade the terminal's firmware.

Click **Device and Server → Digital Signage Terminal / Interactive Flat Panel** on the left navigation pane.

The icon beside the terminal name indicates this terminal's firmware is old and firmware upgrade is required. Click to enter the Upgrade Device page.

Select the terminal(s) to be upgraded, click **Local File** to select the firmware package, and then click **Upgrade** to start upgrading.

5.6.4 Reset Device Password

If you forget the password you use to access the online device, you can request for a key file from your technical support and reset the device's password through the platform.

Before You Start

- Make sure the devices you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the HikCentral FocSign via network.
- The devices should be activated. Refer to ***Create Password for Inactive Device(s)*** for details about activating devices.

Perform this task when you need to reset the device's password.

Steps

1. On the left, click **Device and Server** to select a device type.
2. In the Online Device area, view the device status (shown on Security column) and click icon in the Operation column of an active device.

   The Reset Password window pops up.

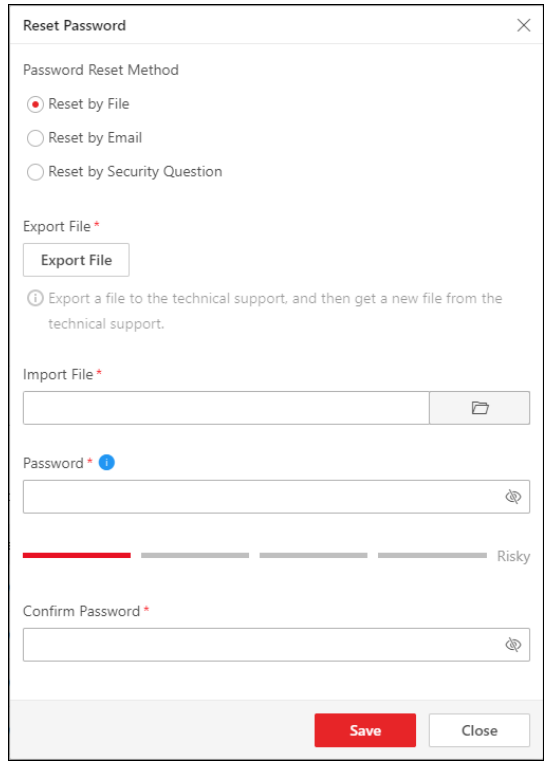

Figure 5-4 Reset Password

3. Select a password reset method:

Reset by File Click **Export File** to save the device file on your PC. Send the file to the technical support.

Note

For the following operations about resetting the password, contact the technical support.

Reset by Email	Export the QR code and sent it to the email displayed. You will receive the verification code in 5 minutes. Enter the code, new password, and confirm password.
Reset by Security Question	Enter the answer to the security question, new password, and confirm password.

Note

If you have not set security questions, the window of setting security questions will pop up, and you should set the security questions as needed.

Caution

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

4. Click **Save** to save the change.

5.7 Area Management

HikCentral FocSign 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, in a house, there mounted 16 doors, 64 alarm inputs, and 16 alarm outputs. You can organize these resources into one area (named My House) for convenient management. You can do some other operations of the devices after managing the resources by areas.

On the top, select **Device**, and click **Area** on the left.

5.7.1 Add an Area

You can add an area to manage the devices.

Steps

1. **Optional:** Select the parent area in the area list panel to add a sub area.
2. Click + on the area list panel to open the Add Area panel.

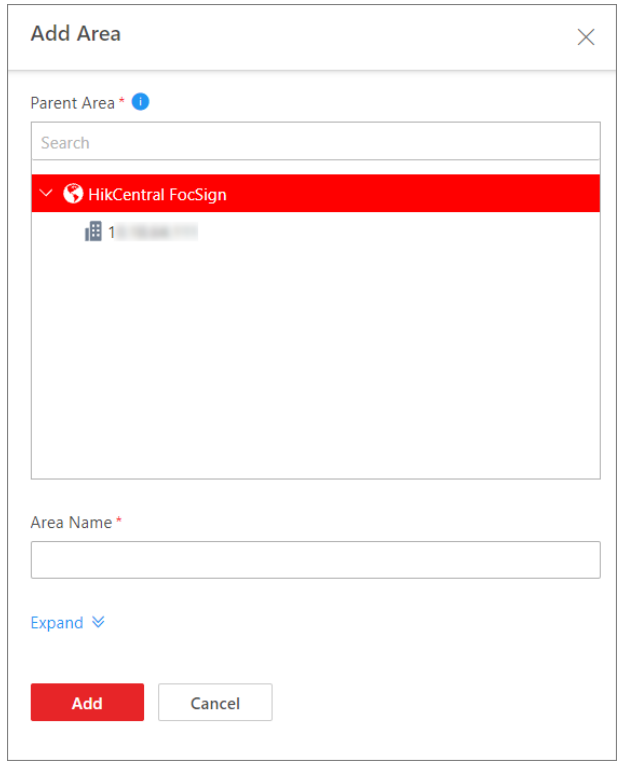

Figure 5-5 Add Area

3. Select the parent area to add a sub area.
4. Create a name for the area.
5. Click **Add**.

5.7.2 Add Commercial Display Resource to Area

You can add commercial display resources (digital signage terminals, interactive flat panels, and LED controllers) to areas for convenient management.

Before You Start

The devices need to be added to the HikCentral FocSign for area management.

Steps

Note

One device can only be added to one area.

1. Select an area from the area list on the left side.
2. Click **Add**.
3. Select **Digital Signage Terminal/Interactive Late Panel/LED Controller** as the device type.
4. Select device(s) to be added.

5. Click **Add**.
6. **Optional:** After adding the devices, perform the following operations.

Delete	Select the device(s), and then click **Delete** to delete the selected device(s) from this area.
Move to other Area	Select the device(s), and then click **Move to Other Area** to move the selected device(s) to the target area.
Edit Name	Click the name of a device to edit its name.
Search for Devices	In the top right corner, enter keywords, and click to search for devices.

5.8 Device Control

The platform supports controlling selected devices (including digital signage terminals, interactive flat panels, LED controllers, and display walls) by clicking buttons of general functions, and creating a combined control command to control devices.

5.8.1 Control a Device

You can control the devices after adding them to the platform.

Note

Make sure you have added devices to the platform.

On the Device page, select **Device Control → Device Control** on the left.

General Operations When Devices are Selected

Check devices of different types, and then click buttons on the top.

Open/Close Screen

Turn on/off the device sleep mode. If it is turned off, the screen will be woke up from the sleep mode.

Restart

Restart selected devices.

Play/Stop

Play/stop the programs on the terminal(s).

Stop Cut-In

Stop cutting in programs.

Clear Playing Contents

Clear all the contents to be played on the screen(s), including programs, cut-in programs, etc.

Volume

Set the output volume of the selected device(s).

Time Startup/Shutdown

The device(s) will start up / shut down according to the schedule. For details, refer to ***Configure Device Display Settings*** .

Combined Control

When you need to control multiple devices in a batch, you can create a combined control command for the devices and then control them in a batch. See ***Create a Combined Control Command for Multiple Devices*** .

Restore Default Settings

Only available for digital signage terminals.

Enable/Disable Sync Playing

Enable/disable sync playing the same released contents on different digital signage terminals.

Note

Make sure you have enabled the time synchronization of NTP server.

Remote Debugging

Enable the Android debug bridge for the device(s), and enter the debugging contents.

Export Log

Export the logs of the device(s) in ZIP format.

Remote Control

Hover the cursor on a device, and click **Remote Desktop** to connect the device and operate on the device remotely.

Note

This should be supported by the device.

Note

The operations should be supported by the selected device type(s).

Other Operations

Switch Display Mode

Click / to display the added devices in thumbnail/list mode.

Filter by Device Type

In the drop-down list of the **Device Type**, select **Digital Signage Terminal** / **Interactive Flat Panel** / **Display Wall**.

Filter by Device Status

Select **Open Screen** / **Close Screen** / **Offline** to filter devices by status.

Refresh Device List

Click **Refresh** to refresh the device list.

Search for a Device

In the text bar on the right, enter a device name to search for it.

5.8.2 Create a Combined Control Command for Multiple Devices

When you need to send multiple control commands to devices at a time, you can create a combined control command for the devices. The platform supports controlling digital signage terminals, interactive flat panels, and display walls.

Before You Start

Make sure you have added devices to the platform.

Steps

1. On the Device page, select **Device Control → Combined Control Command** on the left.
2. Click **Add** to enter the Create Combined Control Command page.
3. Enter a name for the command group.
4. Select a device type.
5. In the Select Control Command area, click the buttons under each tab to add it to the Command Details on the right.
6. Click **Save** to save the command, or click **Execute** to execute the command.

   The added command will be displayed in the command list.
7. **Optional:** Perform the following operations if needed.

Execute a Command	Click **Execute** to execute a command in the list.
Delete Command(s)	Click **Delete** behind a command to delete it, or check **All Commands**, and then click **Delete** on the top to delete all commands in the list.
Search for Command(s)	On the upper-right, enter the name of the combined control demand to search for it.

5.9 Application

You can give algorithm capabilities to devices by configuring device application packages. After you finish configuring, you can add and apply the applications to interactive flat panels and manage the applications.

5.9.1 Add Applications

You can add device applications to the platform, and then apply them to interactive flat panels.

Before You Start

Make sure the interactive flat panels you are going to use are added to the platform. For details, see ***Manage Interactive Flat Panel*** .

Steps

1. On the top, select **Application**.
2. Click **All Applications → Add** .
3. Click to upload application package(s) from the local PC, and add function descriptions if there are any.
4. Click **Next**, and then select available device(s) to apply the application.
5. Click **Save**.
6. **Optional:** Perform the following operations after applying applications to device(s).

Control Application Installation	On the upper right, click **Application Installation Control** to select the installation control mode. After the mode settings, you can view which applications are allowed / not allowed to be applied to the selected device(s) on the **All Applications** pane. **All Applications Allowed** All applications are allowed to be applied to devices. **Only Selected Applications Allowed** Only selected applications are allowed to be applied to the selected devices. **Only Selected Applications Not Allowed** Only selected applications are not allowed to be applied to the selected devices.
Apply Application to Device	Select added application(s) and click **Apply to Device** to apply the selected application(s) to the device(s). There will be a pop-up window showing the process of the application, and you can click **Cancel** to cancel the applying process. If the device loses power during the applying process, the platform will continue to apply the application after powering on the device again.
View Application Usage Statistics	On the upper right, click **View Application Usage Statistics** to view statistics of application usage. You can export the statistics data to the local PC. See for details.
View Application Records	Click **Application Record** to open the Application Record page, you can specify conditions, and click **Search** to view the records about adding device applications in specific time period. **Note** The icon indicates that adding device application(s) failed.

Operations for a Device

After applying applications to the device, you can go to **All Devices** to view the applied applications of a device. You can select a device on the left and perform the following operations:

- Click **Add** to upload and apply application(s) to the selected device.
- Select application(s) and click **Uninstall** to uninstall the selected application(s) on the device.

5.9.2 Manage Applications on Devices

You can manage device applications after adding the them.

Note

Make sure the devices you are going to use are added to the platform. For details about adding interactive flat panels, see ***Manage Interactive Flat Panel*** .

On the top, select **Application → All Devices** .

You can perform the following operations.

Add Device Application to Specific Device	Select an interactive flat panel in the list, and click **Add** to add an application to the device. **Note** Only one application can be added at a time.
Uninstall Application	Select an interactive flat panel in the list, select applications on the right, and click **Uninstall** on the top to uninstall applications.
Refresh Device Application List	Click **Refresh** to refresh the application list.
View Application Records	Click **Application Record** to open the Application Record page, you can specify conditions, and click **Search** to view the records about adding device applications in specific time periods. **Note** The icon ⓘ indicates that applying device application(s) failed.

Chapter 6 Digital Signage Management

Digital signage management includes managing contents, schedules, release, materials, etc. It is widely applied to the industries of entertainment, finance, and traffic for information release. You can select a proper method to create contents according to actual needs and set schedules to release the contents to the specific devices. The contents should be reviewed before they are released and played on the devices according to the configured schedule. Also, the platform supports viewing the playing statistics including content playing statistics and material playing statistics.

6.1 Flow Chart of Digital Signage Management

You can follow the flow chart below for using the digital signage module for the first time.

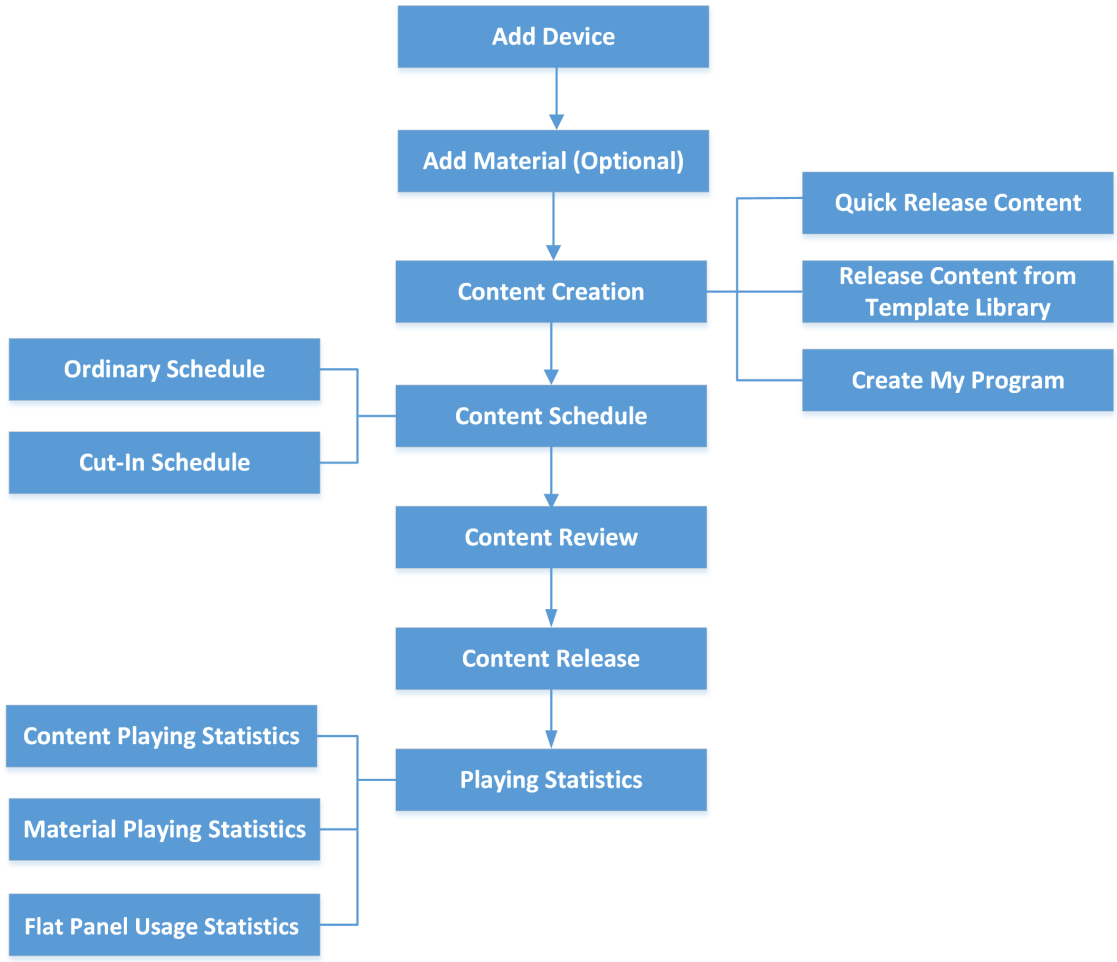

Figure 6-1 Flow Chart of Digital Signage Management

- **Add Device**: You should add devices to the platform. For details, refer to ***Add Digital Signage Terminal*** and ***Manage Interactive Flat Panel*** .
- **Add Material**: Material is used for creating programs. You can upload materials to the platform. For details, refer to ***Material*** .
- **Content Creation**: You can create contents via three methods including quick releasing contents, creating contents from the template library, and creating my programs according to actual needs. For details, refer to ***Content*** .
- **Content Schedule**: You should define a playing schedule for the added programs, which will then be played according to the scheduled time or method on the terminals. For details, refer to ***Create a Cut-In Schedule*** and ***Create an Ordinary Schedule*** .
- **Content Review**: The added contents should be reviewed before they are used. For details, refer to ***Review*** .
- **Content Release**: You can view release records of all the tasks and the details of their release status. For details, refer to ***View Release Records*** .

6.2 Content

The platform supports creating contents and releasing them to the selected devices. Then the contents can be played on the devices to function as prompts, notices, etc. According to actual needs, you can select from three entries/methods to create contents, namely, quick releasing contents, creating contents from template library, and creating my programs. When creating contents via the latter two entries/methods, you can customize the layout of the program, add materials to the program, preview the program, etc.

Note

You can go to → **Digital Signage** → **Content** to enter this module. If you have added the target menu to the top navigation, click the menu on the top directly, and this entry will be introduced in the following.

6.2.1 Quickly Release Content

You can quickly release contents by selecting device type(s), selecting material(s) from local PC or material library, setting the content playing schedule, setting the release mode, and selecting device(s) to release the contents.

Before You Start

Make sure you have added device(s) to the platform. For details, refer to ***Add Digital Signage Terminal*** , ***Manage Interactive Flat Panel*** , and ***Add LED Controller*** .

Steps

1. Click **Quick Release** on the left to enter the Quick Release page.

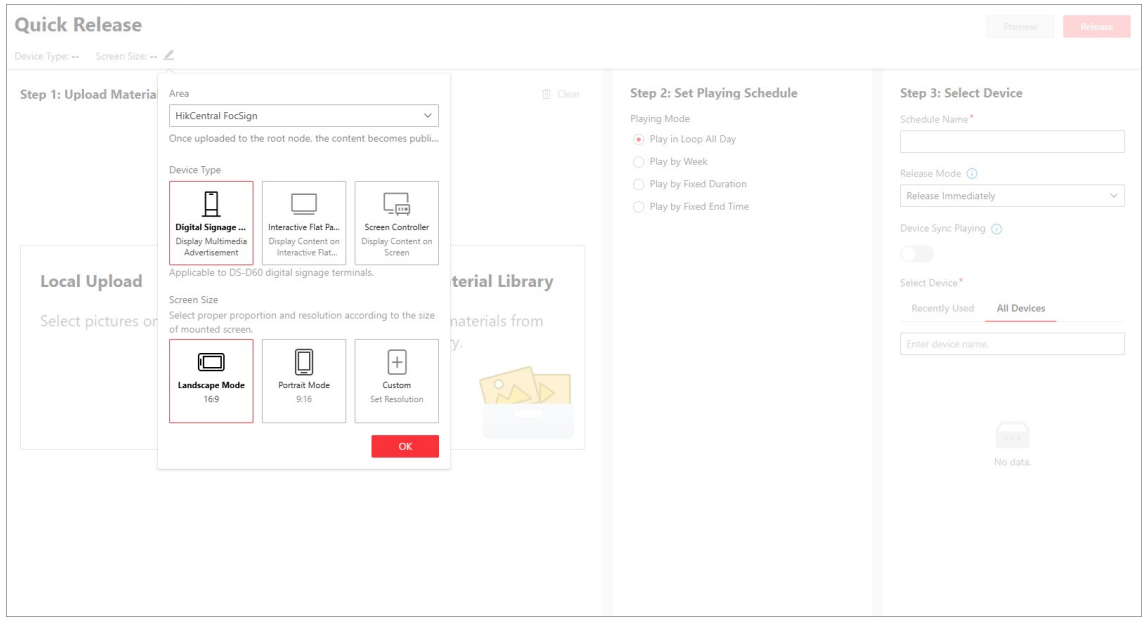

Figure 6-2 Quick Release Page

2. Select the area, device type, screen size, and click **OK**.
   - Click **Digital Signage Terminal** to select the screen size, and you can click **Custom** to enter the resolution manually.
   - Click **Interactive Flat Panel**.
   - Click **Screen Controller**, enter the resolution manually. If you select standard screen, you can click **Get Device Screen Size** to get the screen size of the added device.
3. Upload the material(s).
   - Click **Local Upload**, and select picture(s) and/or video(s) form local PC.
   - Click **Select from Material Library**, select an area from the drop-down list, and select material(s) from the Material Library.

Note

- For the selected material, move the mouse cursor to it and you can click **Edit** to edit the material size, or click **Delete** to delete the material. You can also click **Clear** to delete all the selected materials.
- On the editing material page, you can check **Show Original Aspect Ratio** to view the material in its actual proportion (only picture material supports). After resizing the material, you can click **Reset** to revert the material size to its original size.

4. Set the playing schedule.
   1) For multiple uploaded materials, drag them to adjust the playing order, and set the switching effect as **Gradient** or **None**.
   2) Set the playing duration for picture materials.
   3) Set the playing schedule as **Play In Loop All Day**, **Play by Week**, **Play by Fixed Duration**, or **Play by Fixed End Time**.

5. Select the device(s) to release the content.
   1) Enter the schedule name.
   2) **Optional:** Select the release mode as **Release Later**, or select **Release Immediately** and set the release time.
   3) **Optional:** Switch on **Device Sync Playing** (for digital signage terminals only).
   4) Select device(s) from recently used devices or all devices.
6. **Optional:** Click **Preview** to preview the content.

Note

- During previewing, you can click or to pause or start playing; click or to adjust the playing speed as 1x, 2x, or 4x; and click to preview the content in full screen.
- For the content with multiple materials, it will be played automatically according to the playing order you have set. Also, you can manually click or to preview the previous or the next material.

7. Click **Release** to start releasing the content.

   After the content is released, you will enter the Release page and view the quick release task in the list.

6.2.2 Manage Template Library

The platform provides multiple templates which can be used in different application scenarios such as chain retail and financial bank. You can preview the template, add it to My Template, and select a template according to actual needs and then start creating the content.

On the top, select **Content**.

Click **Template Library** on the left.

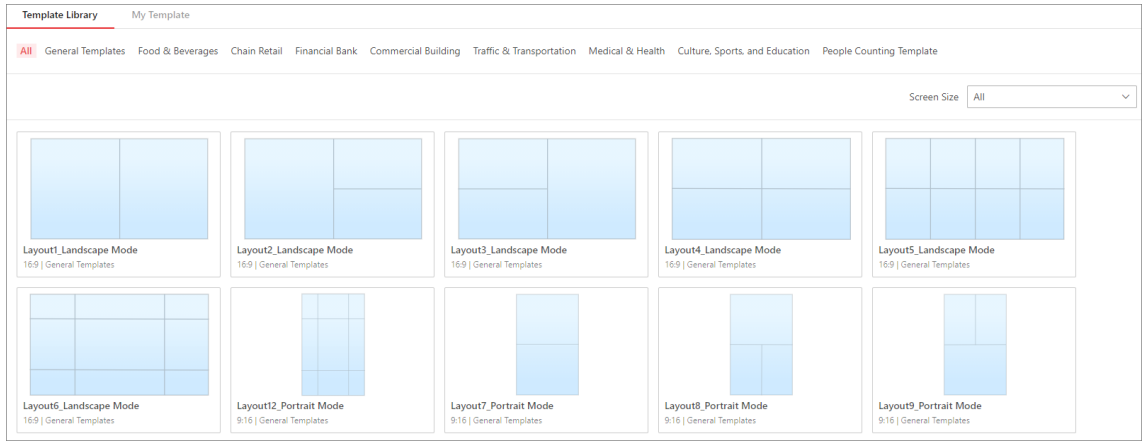

Figure 6-3 Template Library

You can perform the following operations.

- Filter templates by the template types or the screen sizes.
- Hover over a template and click **Preview** to preview the template.
- Hover over a template, and click **Add to My Template** to add it to My Template. On the My Template page, you can also filter and preview the templates, and remove them from My Template.
- Hover over the target template, and click **Create** or click **Preview → Create Program** to enter the creating content page.

6.2.3 Create My Program

The platform supports creating single-sided programs and display wall programs. Therefore, you can create programs according to the screen type (single-sided screen or display wall) of your devices. When creating the program, you can select the needed materials and design the layout to meet your requirements. After creating the programs, you can perform more operations such as previewing, copying, releasing, editing, and filtering programs.

Before You Start

Make sure you have added device(s) to the platform. For details, refer to ***Add Digital Signage Terminal*** , ***Manage Interactive Flat Panel*** , and ***Add LED Controller*** .

Steps

1. On the left, click **My Program**.
2. Click **Add**.
3. Configure program parameters including name, area, device type, screen type, screen size, and description.
   - If you select the root area, the content will be visible to all users.
   - The video format and max. resolution of ultrawide screen programs are as follows.

Table 6-1 Ultrawide Screen Program

Video Format	Max. Resolution
MP4	16384
MKV	32768
ASF	32768
MPG	4095
3GP	2048*1152
MOV	16384
WMV	32768
FLV	32768

Note

MPG (MPEG-1) does not support resolutions above 4095*4095.

4. Click **OK** to enter the creating program page.

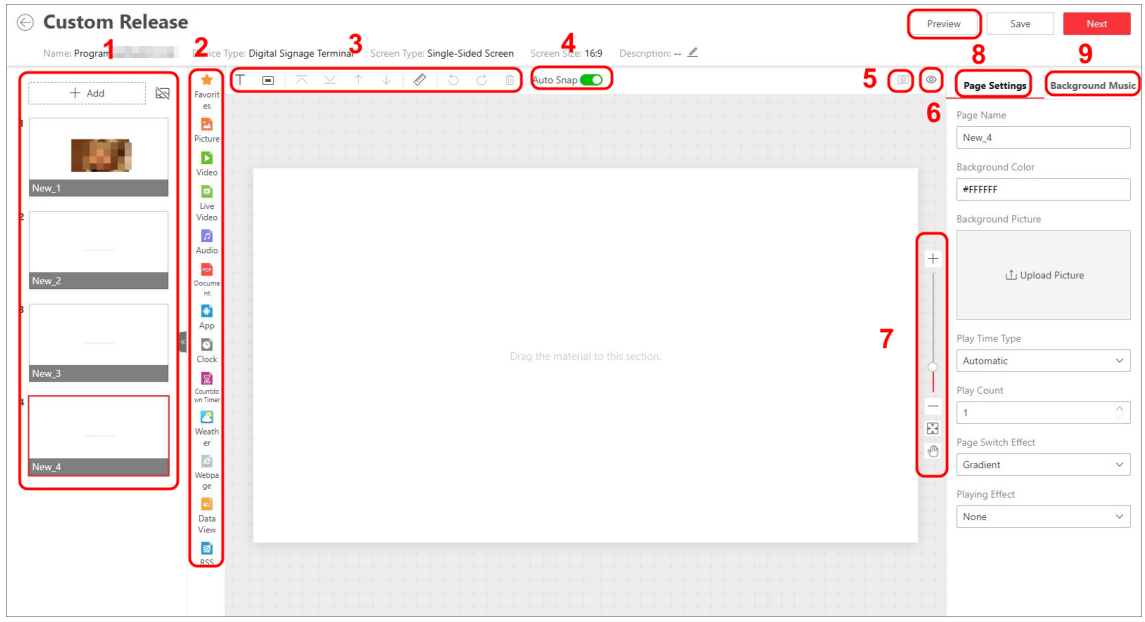

Figure 6-4 My Program

Table 6-2 Page Description

Number	Description
1	• You can choose to show thumbnail (by default) or hide thumbnail. Click to show thumbnail and click to hide it. • You can drag the page to change the page order.
2	There are multiple types of material windows. For details about operations of different material types, refer to ***Table 6-3***. **Note** • Up to 16 windows can be added for one page. • An audio window cannot be added with a video window or live video window at the same time. • You can add material(s) to Favorites in Material.
3	Here are meanings of tools. • : Add a text window in the template. • : Add a button window in the template (only available for touchscreen terminals).

Number	Description
	• / / / : Make the window layer move up / move down / stick on top / stick at bottom. • : Display rulers in the right side and top side. • / : Undo or redo the operation. • : Clear all the materials.
4	Enable **Auto Snap**, and the two windows will be connected when they are near enough.
5	Click **Window Layer** to view the number of current window layers and what each layer is.
6	• You can click **Preview Current Page** to preview the content of the current page. • During previewing, you can click or to pause or start playing. You can click or to adjust the playing speed as 1x, 2x, or 4x. Also, you can click to preview the current page in full-screen.
7	: Zoom in the canvas. : Zoom out the canvas. : Convert the canvas to its original size. : Drag the canvas.
8	Edit page settings, including page name, background, play time type, playing effect, etc. For example, if you set the balloon playing effect, you can preview it by clicking**Preview** in the upper-right corner.
9	Click **Upload** to upload the background music from the local PC or Material. After uploading, you can enable the background music, which will be played on the current page. You can delete the background music if needed.

5. **Optional:** On the left side, perform operations such as adding, copying, deleting program pages.

Add Click **Add** to add new page(s). Up to 32 pages can be added.

Copy Put the cursor on the page, and click **Copy** to copy the current page.

Delete Put the cursor on the page, and click **Delete** to delete the current page.

Note

You cannot delete the page when there is only one page.

Change Template Put the cursor on the page, click **Change Template**, and select a new template from Template Library or My Library.

Adjust Sequence Click a page and drag it to the desired location to adjust the sequence of program pages.

6. Select a material type and select the corresponding material(s) from the left list and drag it to the corresponding window in the template to add the selected material.

Table 6-3 Material Types and Corresponding Operations

Material Type	Operation
Picture/Video/Audio/ Text	• Click **Picture/Video**, move the mouse cursor to the upper-right corner of the material, and click to set its validity period. The material will be played within the validity period. • **Picture/Text**: On the right Window pane, set **Rotation Degree**, **Round Corner**, and **Micro Animation**. • **Picture/Video**: On the right Window pane, expand **Advanced Settings**, and check **Show Original Aspect Ratio** to display these materials in their original sizes. • **Text**: On the right Window pane, select the font provided by the platform or click **Upload** to custom the font. After uploading fonts, you can click **Font Library** to preview, delete, and search for fonts. You can set the word spacing (not supported by third-party data source), line spacing, background color and transparency, scrolling direction and speed, etc.
Live Video	On the right Window pane, expand **Advanced Settings**, and check **Close Audio**, then the program will be played without audio. Besides, only one Device Channel 1 can be added to one program page.
Document	Supports uploading documents in PDF, DOCX, etc. format.
App	Supports uploading APK files.
Clock / Countdown Timer	To show the corresponding time / countdown in real time.
Weather	On the right Window pane, set parameters such as **Weather Location** and **Refresh Interval** to specify the weather display effect. **Note** Make sure you have configured the weather web manufacturer. See ***Set Weather Web Manufacturer*** .
Webpage	On the right Window pane, set the display format according to actual needs.

Material Type	Operation
Data View	Click **Data View**, and select table, chart, dynamic picture, and dynamic text. For details about adding data view materials, refer to ***Upload Materials*** . For dynamic pictures, and dynamic texts, supports setting **Rotation Degree**, **Round Corner**, and **Micro Animation**.
RSS	On the right Window pane, enter the **RSS Feed URL** to subscribe to news or other information you interested in and specify other display parameters.
Signal Source	Select the signal source for LED controller such as HDMI1 and HDMI2.

Note

- When selecting materials, you can search for materials and refresh material list. Also, you can click **Local Upload** to add other materials from local PC to the platform.
- You can add the same or different types of materials to one window. When adding the same type of materials to one window, you can click **Create Window** to create a new window or click **Add More Material** to add more material to the current window.
- You can press select multiple materials of the same type and drag them to a window.

7. Set window properties, including micro animation, window position, window type, switching method, etc.

Note

You can set different parameters for different types of material windows.

Micro Animation

Supports the micro animation effect. You can preview the effect by clicking **Preview** in the upper-right corner.

Set Uniformly

Check **Set Uniformly** and set the following operations.

Switching Effect

Select the switching effect from the drop-down list for the current window. There are 11 types of switching effect.

Play Time (sec)

Set the playing duration for the current window.

Note

- The play time of a window can not exceed the playing time of a page, or the exceeding part of the program will not be played.
- For adding a web page, you can set its play time as **Unlimited**.
- You can undo operations of adding/deleting window, resizing window, and repositioning window.
- You can select a window and press Backspace or Delete to delete it.

Window Position

Set the window position by entering the width, height, and coordinate of the window.

Window Type

Normal

The normal window is displayed by default when the program is played. You can set a window jump link or page jump link for such a window.

Pop-up Window

The pop-up window is hidden by default. Only after setting a redirect link for a normal window and clicking the link, the hidden window will be popped up.

Switching Method

For Android touchscreen terminals, you can open the specified content by linking to a window or page.

Do Not Skip

There is no linked window or page to the current window which is played on the terminal.

Jump to Next Window

You should set the jump link. When the Window A is played on the terminal, you can click the link to jump to its linked window.

Jump to Next Page

You should set the jump link. When the Window A is played on the terminal, you can click the link to jump to its linked page.

8. **Optional:** On the current editing program page, perform the following operations.

Edit Program	Click to edit program parameters in the pop-up window.
Preview Program	Click **Preview** to preview the program. During previewing, you can click or to pause or start playing; click or to adjust the playing speed as 1x, 2x, or 4x; and click to preview the program in full screen.

For the program with multiple pages, it will be played automatically according to the page play time you have set. Also, you can manually click  or  to preview the previous or the next page of the program.

Create Schedule Click **Next** to enter the Ordinary Schedule page and create a schedule for the program.

Note

For details, refer to ***Create an Ordinary Schedule*** .

9. Click **Save** to save the current program.
10. **Optional:** On the My Program page, perform the following operations.

View Program in List or Thumbnail Mode Click / to view the added programs in the thumbnail mode or in the list mode.

In the list mode, you can view program name, size, duration, etc.

Preview Program Move the mouse cursor to a program, and click **Preview** to preview the program.

During previewing, you can click or to pause or start playing; click or to adjust the playing speed as 1x, 2x, or 4x; and click to preview the program in full screen.

For the program with multiple pages, it will be played automatically according to the page play time you have set. Also, you can manually click  or  to preview the previous or the next page of the program.

Copy Program Move the mouse cursor to a program, and click **Copy** to enter editing program page. Click **Save** on the upper right corner to copy the current program, and a new program with the same content is created.

Note

When copying a program (e.g., Program A) for the first time, the name of the new program (Program A_1) will be generated automatically. If you need to copy this program (Program A) for a second or more times, you should manually edit its name, or the program cannot be created successfully.

Create Schedule Move the mouse cursor to a program, and click **Release** to enter the Ordinary Schedule page and create a schedule for the program. For details, refer to ***Create an Ordinary Schedule*** .

Share / Cancel Select one or more programs, click **Share** or **Cancel Sharing** to set the sharing property of programs as **Public** or **Private**.

Sharing Program	**Public** All users in the current organization (i.e., the organization where the user who creates the schedule belongs to) and the higher-level organizations can see and use the schedule. **Private** All users in the current organization (i.e., the organization where the user who creates the schedule belongs to) can see and use the schedule.
Filter / Search for Program	In the upper right corner, click to filter programs by the screen size, or enter keywords in the search box to search for the program(s). You can check **All Exceptions** to view all exception program. Click to filter programs **With Expired Materials** and **Empty Programs**. When hovering over an abnormal program: For programs containing expired materials: Supports replacing or one-click deletion of expired materials. For empty programs: Supports deletion or re-editing of the program. When hovering over an abnormal program • Supports replacing or deleting expired materials. • Supports deleting or re-editing the empty program.
Refresh Program List	Click **Refresh** to refresh the program list. The programs will be listed according to the time they are added.
Delete Program	Check one/more programs, or click **Select All** to select all programs, and click **Delete** to delete the selected programs.

6.3 Schedule

You can create a schedule and define a playing schedule to play the added programs on the devices according to the scheduled time or method. The platform supports two types of schedules: ordinary schedule and cut-in schedule. When creating schedules, you can select the needed programs and device(s) to release the programs. For the added schedules, you can perform more operations such as editing, releasing, searching, exporting, and filtering.

Note

You can go to → **Digital Signage** → **Schedule** to enter this module. If you have added the target menu to the top navigation, click the menu on the top directly, and this entry will be introduced in the following.

6.3.1 Create an Ordinary Schedule

You can create an ordinary schedule to play the added programs on the devices according to the scheduled time or method. The platform supports loop schedule, default schedule, or you can customize your schedule and play the programs by day or by week. For the added schedules, you can perform more operations such as editing, releasing, searching, exporting, etc.

Before You Start

- Make sure you have added program(s) to the platform. For details, refer to ***Create My Program*** .
- Make sure you have added device(s) to the platform. For details, refer to ***Add Digital Signage Terminal*** , ***Manage Interactive Flat Panel*** , and ***Add LED Controller*** .

Steps

1. Click **Ordinary Schedule** on the left.
2. Click **Add** to enter the Ordinary Schedule page.

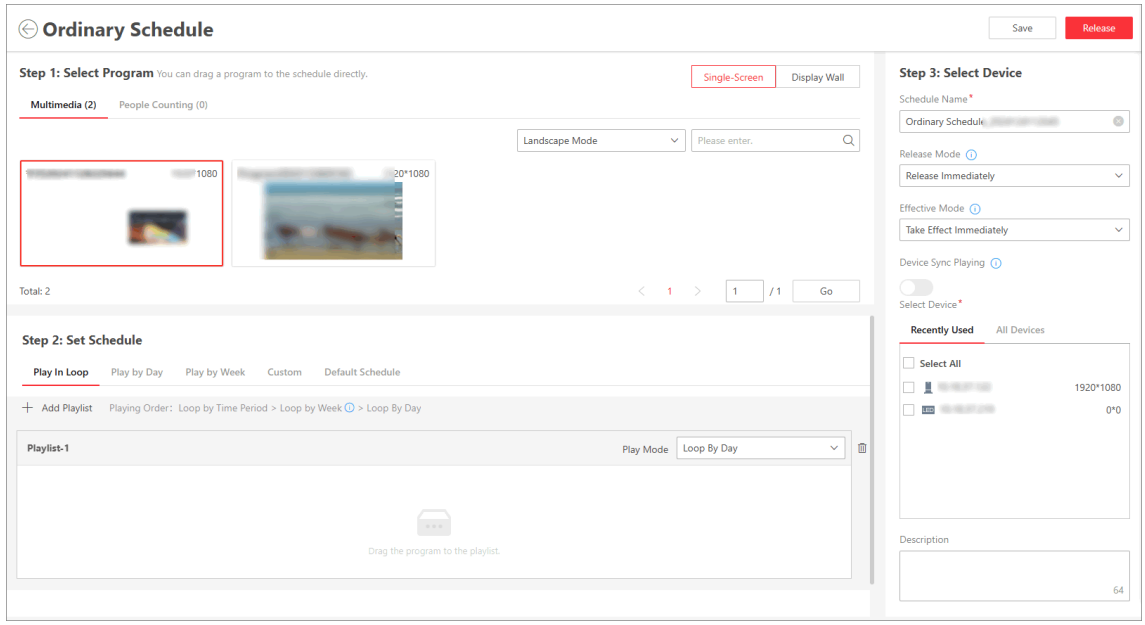

Figure 6-5 Ordinary Schedule

3. **Optional:** Filter the programs.
   - Select the program type as **Single-Screen** or **Display Wall**.
   - Select the screen size as **All**, **Landscape Mode**, **Portrait Mode**, or **Custom**.
   - Enter keywords in the search box to search for the program(s).
4. Select a program and set the schedule for it.

Play In Loop

a. Select a program in the program list and drag the program to the playlist.

Note

You can click **Add Playlist** to add more playlists as needed. Up to 8 playlists can be added, and up to 16 programs can be added to a single playlist.

b. Set the play mode.

Loop By Day

Play the program orderly and repeatedly by day. You can select the date to play.

Play By Week

Play the program orderly and repeatedly by week. You can set the playing day and time period.

Loop By Time Period

Play the program orderly and repeatedly by the selected time period.

Play by Day

Play the program according to a daily schedule.

a. Select a program from the program list and drag to the desired location on the timeline.

Note

You can add multiple programs to one day. When hovering the cursor on the program's playing time, you can view the thumbnail of the program.

b. Adjust the playing time of program(s).
c. Click on the right side of the timeline to delete all the selected programs.

Play by Week

Play the program according to a weekly schedule.

a. Select a program from the program list and drag to the desired location on the timeline.

Note

You can add multiple programs to one day. When hovering the cursor on the program's playing time, you can view the thumbnail of the program.

b. Adjust the playing time of program(s).
c. Click to copy the program to other day(s) in the week.
d. Click **Delete All** to delete all the selected programs.

Custom

Play the program according to a custom schedule.

a. Set the custom time.

Note

The time range should be within 90 days.

b. Select a program in the program list, and drag the program to the desired location on the timeline.

Note

You can add multiple programs to one day.

c. Adjust the playing time of program(s).
d. Click **Delete All** to delete all the selected programs.

Default Schedule Play the default content automatically when no contents are scheduled on the device.

Select a program in the program list, and drag the program to the playlist.

5. Select the device(s) to release the content.
   1) Enter the schedule name.
   2) **Optional:** Select the release mode as **Release Later** or **Release Immediately**.

Note

When selecting **Release Later**, you should set the release time, and the program schedule will be released at the configured time period.

   3) **Optional:** Select the effective mode as **Take Effect On Schedule** or **Take Effect Immediately**.

Note

When selecting **Take Effect On Schedule**, you should set the effective time. Only after the program takes effect, it can be played on the device.

   4) **Optional:** Switch on **Device Sync Playing**, select digital signage terminals and/or LED controllers.

Note

Make sure you have enabled the time synchronization of NTP server.

   5) Select device(s) from recently used devices or all devices.
   6) **Optional:** Enter the description.
6. Save or release the ordinary schedule.
   - In the upper-right corner, click **Save** to save the above settings and release the schedule later.
   - In the upper-right corner, click **Release** to start releasing the schedule to the selected device(s). After the schedule is released, you will enter the Release page and view the schedule releasing task in the list.

Note

- During releasing, you can click **Cancel Releasing** to cancel releasing.
- You can view the release progress and the result on the right side of the page.

7. **Optional:** Perform the following operations if you save the schedule in the previous step.

Edit Schedule Click the schedule name to enter Ordinary Schedule page and you can edit the schedule information.

Share / Cancel Sharing Schedule Select one or more schedules, click **Share** or **Cancel Sharing** to set the sharing property of schedules as **Public** or **Private**.

Release Schedule	a. Click in the Operation column to open the Schedule Releasing window. b. Set the parameters including schedule name, release mode (optional), and effective mode (optional). c. Select the device(s) from the recently used devices or all devices. d. Click **Save and Release** to save the settings and release the schedule to the selected device(s).
Export Schedule	Click in the Operation column, and select the saving path to export the selected schedule to the local PC.
Refresh Schedule List	Click **Refresh** to refresh the schedule list. The schedules will be listed according to the time they are added.
Delete Schedule	Check one or more schedules, and click **Delete** to delete the selected schedules.
Filter Schedules	In the upper right corner, select one or more play modes, or enter keywords in the search box to filter the schedules which meet the conditions. You can check **Empty Schedule** to filter empty schedules. You can delete or re-edit them.

6.3.2 Create a Cut-In Schedule

You can create a cut-in schedule to cut in the specific programs or text messages on the specific devices according to the scheduled time. The cut-in programs or text messages will precede other contents. After creating schedules, you can perform more operations such as editing, releasing, searching, etc.

Before You Start

- Make sure you have added program(s) to the platform. For details, refer to ***Create My Program*** .
- Make sure you have added device(s) to the platform. For details, refer to ***Add Digital Signage Terminal*** and ***Manage Interactive Flat Panel*** .

Steps

1. Click **Cut-In Schedule** on the left.
2. Click **Add** to enter the Cut-In Schedule page.

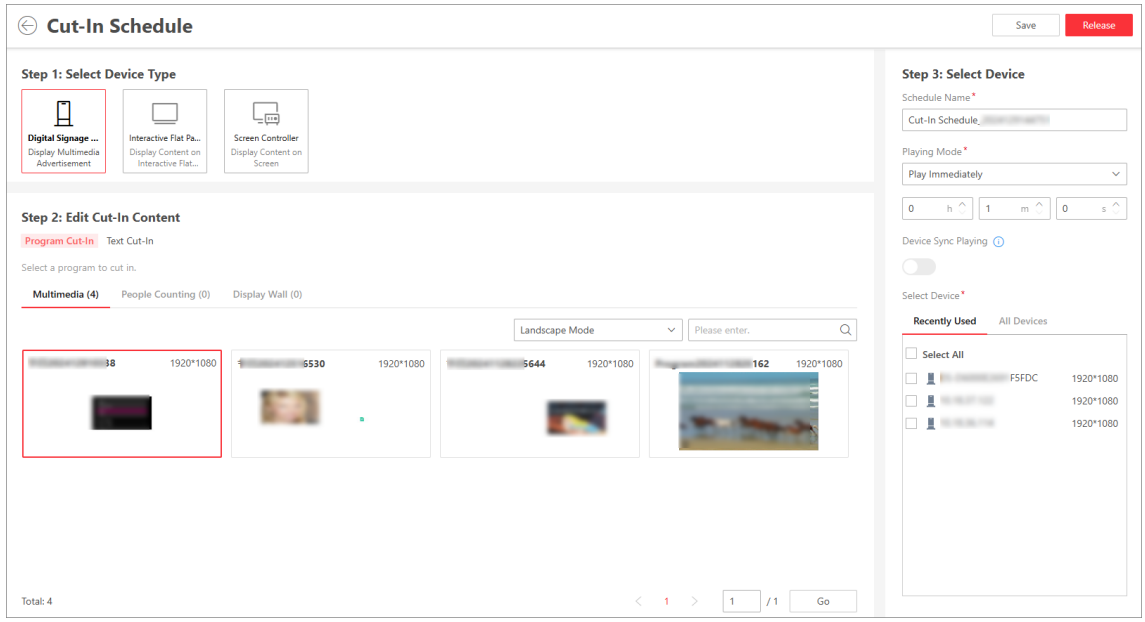

Figure 6-6 Cut-In Schedule Page

3. Select **Digital Signage**, **Interactive Flat Panel**, or **Screen Controller** as the device type.
4. Select the cut-in content.
   - Cut in a program: Click **Program Cut-In**, and select a program.
   - Cut in the text message:
     a. Click **Text Cut-In**, and select the screen size as **Landscape Mode** or **Portrait Mode**.

     Note

     For the interactive flat panel, you can check **Notification Sound**. A notification sound will be played when the text is now released.

     b. In the Edit Text Message area, set the content and the corresponding play time.

     Note

     The play time for different text messages can be overlapped. You can click in the Operation column to view the playing effect of the current text message on the left side of the page.

     c. Set the configuration mode, front size and color, background, etc., for the text message.
5. Select the device(s) to release the content.
   1) Enter the schedule name.
   2) For **Program Cut-In**, set playing duration.
   3) **Optional:** Switch on **Device Sync Playing** (for digital signage terminals only).
   4) Select device(s) from recently used devices or all devices.
6. Save or release the cut-in schedule.
   - In the upper-right corner, click **Save** to save the above settings and release the schedule later.

- In the upper-right corner, click **Release** to start releasing the schedule to the selected device(s). After the schedule is released, you will enter the Release page and view the schedule releasing task in the list.

Note

- During releasing, you can click **Cancel Releasing** to cancel releasing.
- You can view the release progress and the result on the right side of the page.

7. **Optional:** Perform the following operations if you save the schedule in the previous step.

Edit Schedule	Click the schedule name to enter Cut-In Schedule page and you can edit the schedule information.
Share / Cancel Sharing Schedule	Select one or more schedules, click **Share** or **Cancel Sharing** to set the sharing property of schedules as **Public** or **Private**.
Release Schedule	a. Click in the Operation column to open the Schedule Releasing window. b. Set the schedule name. c. Select the device(s) from the recently used devices or all devices. d. Click **Save and Release** to save the settings and release the schedule to the selected device(s).
Refresh Schedule List	Click **Refresh** to refresh the schedule list. The schedules will be listed according to the time they are added.
Delete Schedule	Check one or more schedules, and click **Delete** to delete the selected schedules.
Filter Schedules	In the upper right corner, select the playing type, or enter keywords in the search box to filter the schedules which meet the conditions. You can check **Empty Schedule** to filter empty schedules. You can delete or re-edit them.

6.3.3 View Release Records

You can view release records of all the tasks and the details of their release status.

Select **Release** on the left. You can view release details of all the tasks on the platform, including task name and type, release time, effective time, and release status (Released or Failed), etc. Also, you can perform more of the following operations.

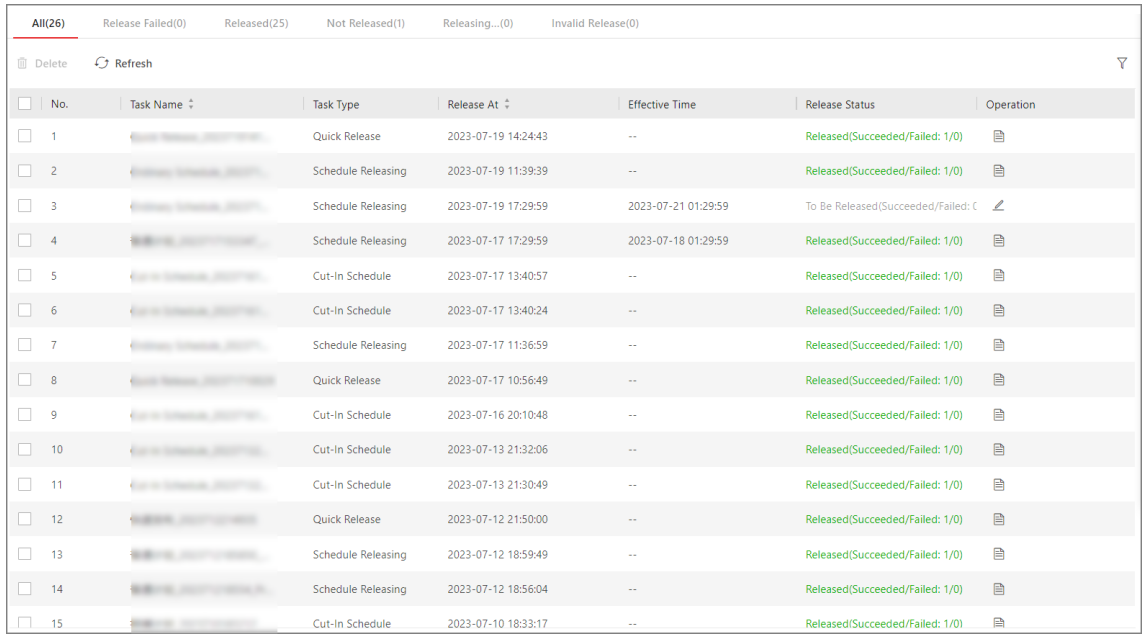

Figure 6-7 View Release Records

- **View Release Details**: Click in the Operation column to view release details such as device name and release progress.

Note

For a task that is releasing, you can click **Cancel Release** to cancel releasing the task. For a task that failed to be released or was canceled releasing, you can click **Release again** to release the task again.

- **Delete Task**: Check one or multiple tasks, and click **Delete** to delete the selected tasks.
- **Release Again**: For a task that failed to be released, you can click to release the task again.
- For tasks failed to be released due to network or electricity disconnection, they can continue to be released within the effective period (48 hours) if connected to the network or electricity again.
- **Filter Tasks**: On the top of the page, click **Release Failed**, **Released**, **Not Released**, **In Release**, or **Invalid Release** to filter tasks via release status; In the upper right corner, click , and filter tasks by conditions such as task name and type.

6.4 Review

The added contents should be reviewed before they are used. After being reviewed, the contents can be released automatically.

Note

- The contents created by the user who has the review permission can be released directly, otherwise the contents should be reviewed by the user who has the review permission.
- Review records containing empty programs/schedules cannot be approved.

On the top, select **Review**.

Perform the following operations as needed.

Description	Operation
Review Content One by One	1. On the **All** and **To Be Reviewed** pages, click in the **Operation** column. 2. On the pop-up Content Review page, review the content. 3. Select the result as **Pass** or **Deny**. 4. Enter the comment. **Note** When the result is **Deny**, the comment is required. You can enter up to 128 characters. 5. Click **Preview** to preview the program. **Note** During previewing, you can adjust the playing speed, view in full screen, and switch program pages. 6. Click **OK**.
Batch Review Contents	• On the **All** and **To Be Reviewed** pages, check multiple contents to be reviewed, click **Pass**, and enter the comment (optional) to batch pass the selected contents. • On the **All** and **To Be Reviewed** pages, check multiple contents to be reviewed, click **Deny**, and enter the comment (required) to batch deny the selected contents. **Note** When entering the comment, you can enter up to 128 characters.
Delete Content	On the **Denied** and **Passed** pages, check one or more contents, click **Delete** to delete them.

Description	Operation
Refresh Content	On the **All**, **To Be Reviewed**, **Denied** and **Passed** pages, click **Refresh** to refresh the content list.
Search for Content	On the **All**, **To Be Reviewed**, **Denied** and **Passed** pages, enter keywords in the search box in the upper right corner to search for the target contents.

6.5 Material

Material is used for creating programs. The platform supports various types of materials to meet different program requirements. You can upload local materials (such as picture and video) and other materials (such as webpage and picture URL) to the platform. After uploading the materials, you can mange materials including editing, searching, replacing, etc.

Note

Go to → **Digital Signage** → **Material** to enter this module. If you have added the target menu to the top navigation, click the menu on the top directly, and this entry will be introduced in the following.

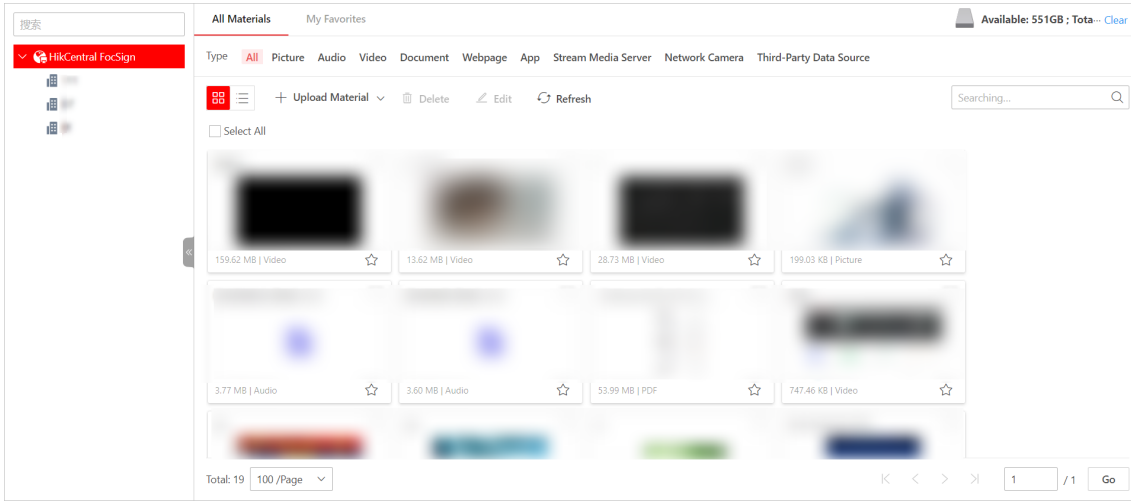

Figure 6-8 Material

6.5.1 Upload Materials

You can upload materials which can be used for creating programs. The materials supported to be uploaded include picture, video, audio, document, APP, webpage, network picture, stream media

server, network camera, etc. For the uploaded materials, you can perform more operations, including adding to favorites, editing, downloading, deleting, etc.

Steps

1. On the left, select the area.
2. Click **All → Upload Material** to select the uploading mode. Or select a material type to perform operations.

Table 6-4 Operations about Supported Material Types and Formats

Material Type	Format	Operation
Picture	BMP, JPG, PNG, GIF, JPEG	• Click **All / Picture → Upload Material → Create URL Picture Material** , enter the name, URL of the picture, and select areas. • Click **All / Picture → Upload Material → Local Upload (Picture / Audio / Video / Document / Web Page / App) / Local Upload** to upload the selected local materials. Meanwhile, the uploading progress and the failure details will be displayed (when uploading fails).
Video	ASF, AVI, MPG, 3GP, MOV, MKV, WMV, FLV, MP4	• Click **Video / Audio / Document / App → Local Upload** to upload the selected local materials. Meanwhile, the uploading progress and the failure details will be displayed (when uploading fails). • Click **All → Local Upload (Picture / Audio / Video / Document / Web Page / App)** , and follow the above steps.
Audio	MP3, WAV, WMA	
Document	PDF, DOC, DOCX, PPT, PPTX, XLS, XLSX	
App	APK	
Webpage	HTML, HTM	• Click **Webpage → Upload Material → Local Upload** to upload the selected local materials. Meanwhile, the uploading progress and the failure details will be displayed (when uploading fails). • Click **Webpage → Upload Material → Create Webpage Material** , enter the name, URL of the webpage, and select areas. • Click **All → Upload Material → Local Upload (Picture / Audio / Video / Document / Web Page / App) / Create Webpage Material** and follow the above steps.

Material Type	Format	Operation
Streaming Media Service	/	• Click **Streaming Media Service → Create Material** to receive streams from the streaming media server. • Click **All → Create Material of Streaming Media Service** and follow the above steps. If you disable **Built-In Steaming Media Service**, you should enter the URL of the streaming media server. If you enable **Built-In Steaming Media Service**, you should enter the IP address, port No., channel No., user name, and password of the network camera.
Network Camera	/	• Click **Network Camera → Create Material** to get video streams from network camera. • Click **All → Create Network Camera Material** and follow the above steps. You should enter the required information of network camera such as IP address, port No., and channel No.
Third-Party Data Source	/	• Click **Third-Party Data Source → Create Material** . • Click **All → Create Material of Third-Party Data Source** and follow the above steps. There are two types of data source: Auto-Push Data Source and Third-Party Database. If you select **Auto-Push Data Source**, you should enter data source ID and select the data type; If you select **Third-Party Database**, you should set the basic information of the third-party database, including data source ID, database type, encoding format of data interchange, database name, IP address, etc.

Note

- A single material should be smaller than 4 GB. The names of any two materials cannot be the same.
- Up to 1,000 materials can be uploaded to the platform at a time. Up to 10,000 materials can be stored in the platform.
- For those materials that fail to be uploaded, click to upload again or click to replace the material. For those materials with the failure reason "duplicated material", you can replace the material or click **Close** to cancel uploading.
- If you set **Sharing Property** to **Public**, all users in the current organization (i.e., the organization where the user who creates the material belongs to) and the higher-level organizations can see and use the material. If you set **Sharing Property** to **Private**, all users in

the current organization (i.e., the organization where the user who creates the material belongs to) can see and use the material.

3. **Optional:** After uploading the materials, perform the following operations.

Add to Favorites or Not	Click ☆ to add the material to **My Favorites**. Click again to remove it from **My Favorites**.
Edit Material	Check one/more materials, or check **Select All** to select all materials, and click **Edit** to edit the selected materials, such as editing the name and the property.
Delete Material	Check one/more materials, or check **Select All** to select all materials, and click **Delete** to delete the selected materials. **Note** If you delete materials used by programs, they will be removed from the programs.
Download Material	Click to download single material to the local PC.
View Large Picture	Click to view large picture of the material.
Refresh Materials	Click **Refresh** to refresh the material list.
Switch Display Mode of Materials	Click / to view the added materials in the thumbnail mode or in the list mode.
Search for Material	Enter keywords in the search box, and click to search for materials. You can also click tabs (**All**, **Picture**, **Audio**, etc.) on the top of the materials to filter materials.

6.5.2 Manage Materials in My Favorites

You can manage materials in **My Favorites**, such as editing materials, filtering materials, and deleting materials.

On the top, click **My Favorites**.

Table 6-5 Mange Materials

Description	Operation
Switch Display Mode of Materials	Click / to view the added materials in the thumbnail mode or in the list mode.
Add to Favorites or Not	Click or to add the material to **My Favorites** or remove it from **My Favorites**.

Description	Operation
Edit Material	Select material(s) to be deleted, and click **Edit** to edit the selected materials, such as name and sharing property.
Refresh Material	Click **Refresh** to refresh the material list.
Download Material	Click to download the material to local PC. **Note** Only materials uploaded from local PC can be downloaded.
View Large Picture	Click to view the large picture of the material.
Search for Material	Enter keywords in the search box, and click to search for materials. You can also click tabs (**All**, **Picture**, **Audio**, etc.) on the top of the materials to filter materials.
Delete Material	Select material(s) to be deleted, and click **Delete** to delete the selected materials. **Note** If you delete materials used by programs, they will be removed from the programs.

6.6 Statistics and Reports

You can select devices and set conditions to search for the content playing statistics, material playing statistics, application usage statistics, and flat panel usage statistics. Also, you can export the search results to the local PC.

Go to → **Digital Signage** → **Statistics and Reports** to enter this module. If you have added the entry to the top navigation, click it on the top directly.

Content Playing Statistics

Select **Content Playing Statistics** on the left.
Select a device, and the interface will display the programs and their specific playing durations for that device.

- You can filter data by daily, weekly, monthly, yearly, or custom time periods.
- Enter a program name to filter your search results (fuzzy search supported).
- Click to sort by playing duration.

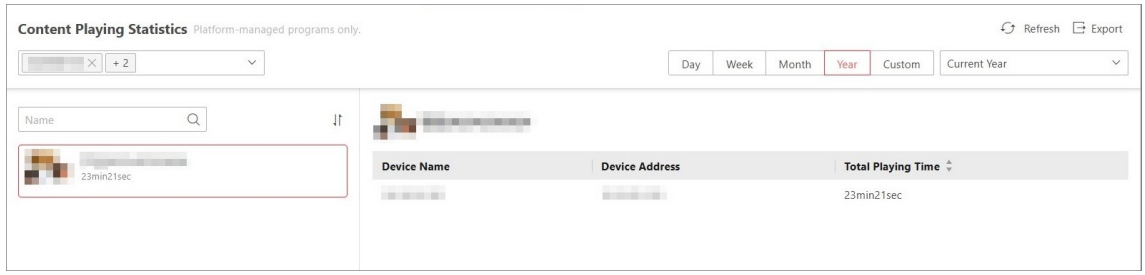

Figure 6-9 Content Playing Statistics

Material Playing Statistics

Select **Material Playing Statistics** on the left.
Select a device, and the interface will display the materials and their specific playing durations and playing count for that device.

- You can filter data by daily, weekly, monthly, yearly, or custom time periods.
- Enter a material name to filter your search results (fuzzy search supported).
- Click ⇅ to sort by playing duration.

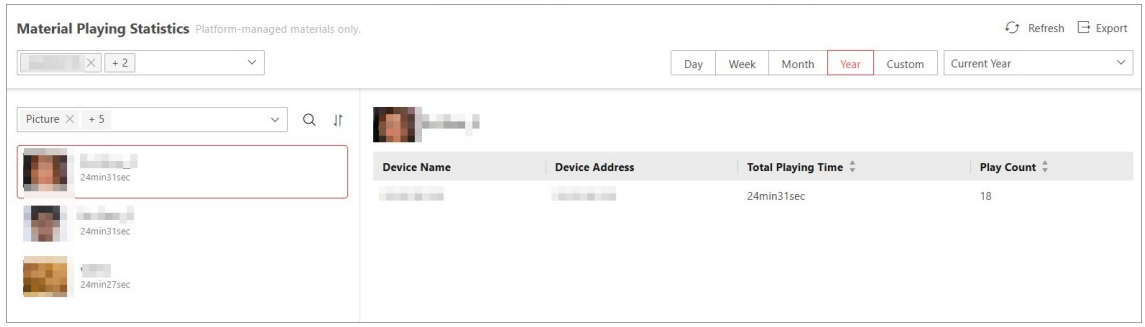

Figure 6-10 Material Playing Statistics

Application Usage Statistics

Select **Application Usage Statistics** on the left.
Select a device or devices, and the interface will display the application list and their specific usage durations.

- You can filter data by daily, weekly, monthly, yearly, or custom time periods.
- Enter an application name to filter your search results (fuzzy search supported).
- Click ⇅ to sort by usage duration.

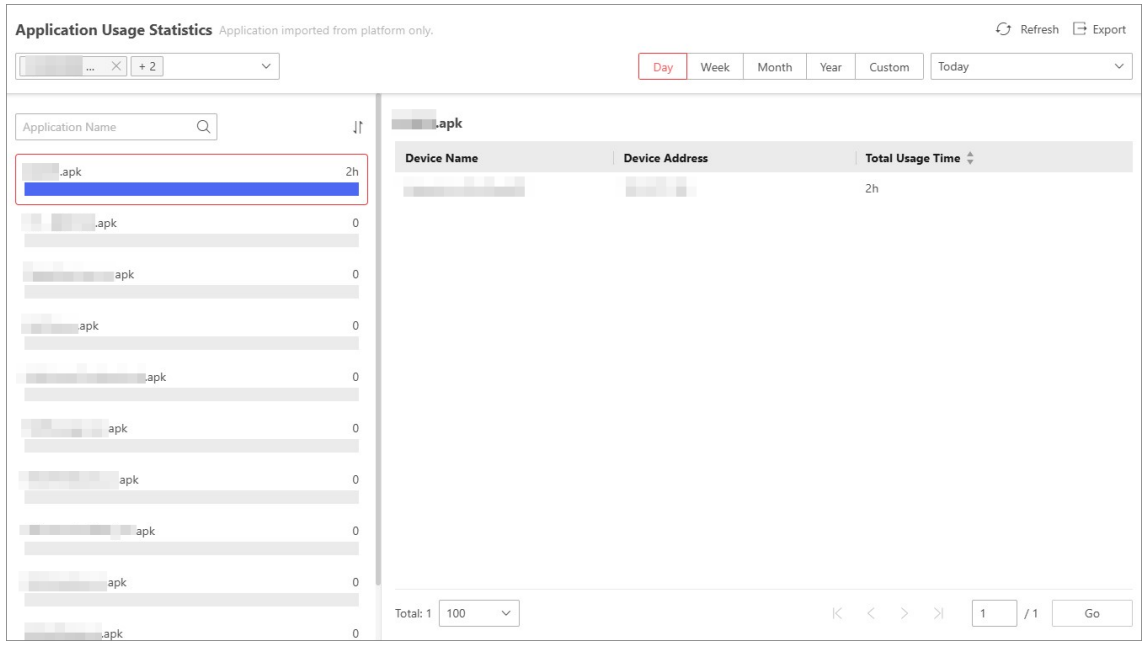

Figure 6-11 Application Usage Statistics

Flat Panel Usage Statistics

Select **Flat Panel Usage Statistics**.

Select a device or devices, you will view the bar chart of usage time of each time period. You can filter data by daily, weekly, monthly, yearly, or custom time periods.

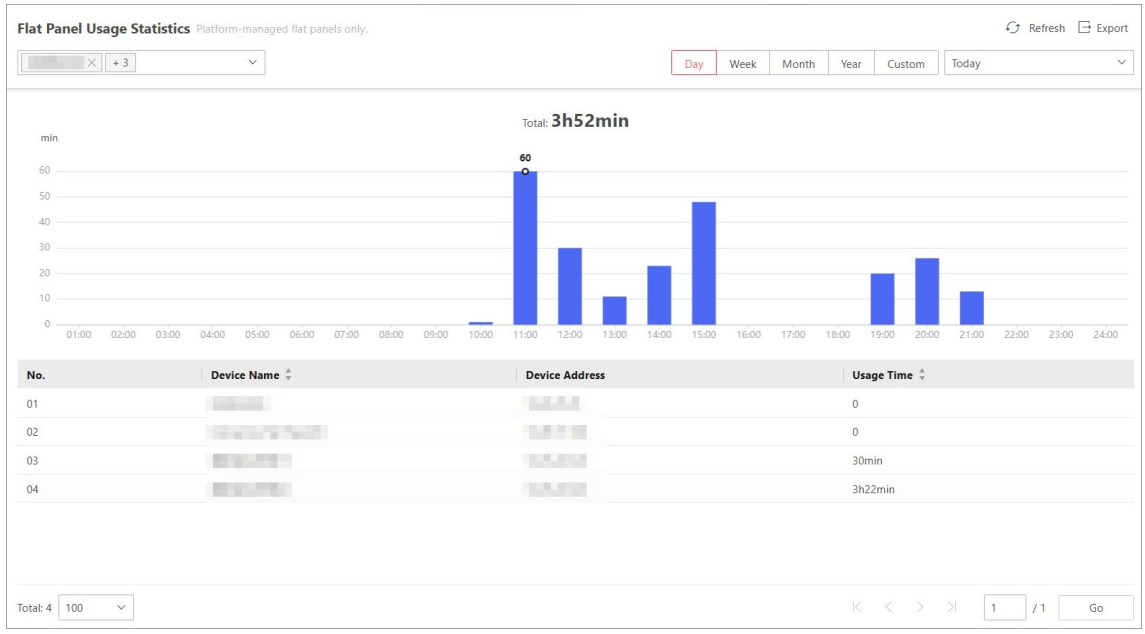

Figure 6-12 Flat Panel Usage Statistics

Export Reports

After viewing the statistics, you can click **Export** in the upper right corner and select a file type to export the searched statistics to the local PC.

Take **Flat Panel Usage Statistics** as an example. The exported Excel file is as follows.

1	Flat Panel Usage Statistics			
2	Basic Information			
3	Counting Time:2025/05/04-2025/05/10			
4	Export Time:2025/05/10 14:16:55			
5	Operator:admin			
6				
7	Usage Statistics			
8	Date	Device Usage Time(hh:mm:ss)		
9	Wed(5/7)	15:23:08		
10	Thu(5/8)	34:05:54		
11	Total:	49:29:02		
12				
13	Device Usage Details			
14	No.	Device Name	Device Address	Usage Time(hh:mm:ss)
15	1	[redacted]	[redacted]	00:00:00
16	2	[redacted]	[redacted]	14:55:00
17	3	[redacted]	[redacted]	17:00:59
18	4	[redacted]	[redacted]	17:33:03
19				
20				
21				

Flat Panel Usage Statistics

Figure 6-13 Flat Panel Usage Statistics

Chapter 7 Maintenance

You can configure network timeout parameters and health check frequency, and view resource status and server logs to find the abnormal status of resources for maintaining them in time.

Note

You can go to → **Centralized Device Control** → **Maintenance** to enter this module. If you have added the target menu to the top navigation, click the menu on the top directly, and this entry will be introduced in the following.

7.1 Basic Configuration

You can configure the default response timeout of the interactions among the Web Client, FocSign server, and devices, and specify the health check frequency.

7.1.1 Configure Scheduled Log Report

After configuring a scheduled report, the platform will record the device online/offline status by statistical cycle and automatically send the device log report as scheduled to specified recipients by email. The report can also be uploaded to SFTP and saved to the local storage.

On the top, select **Maintenance**.

Select **Basic Configuration** → **Scheduled Report** on the left.

Click  .

Time Settings

Statistical Cycle

Set the frequency of generating the report.

By Day

The platform will send a report at the sending time every day, which contains logs recorded during the day (24 hours) prior to the sending date.

For example, if you set the sending time as 20:00 and select all the dates (from Sunday to Saturday) in **Sending Date**, the platform will send a report at 20:00 every day. The report contains the logs recorded between 00:00 and 24:00 of the previous day.

By Week/Month

The platform will send a report at the sending time every week or every month, which contains logs recorded during the **Report Time** you have set.

For example, for weekly report, if you set the sending time as 6:00 on Monday in **Sending Date**, the platform will send a report at 6:00 in the morning on every Monday. The report contains logs recorded between last Monday and Sunday if you set the **Report Time** as **Last 7 Days**.

Report Time

Set the time period during which the logs will be recorded.

Advanced Settings

Send via Email

Select an email template to define the recipient information and content. You can click **Add** to add a new email template. For details, refer to ***Set Scheduled Report Email Template*** .

Upload to SFTP

Click **Configure** to set SFTP information. The saving path will take effect globally.

Save to Local Storage

Click **Configure** to set the local storage path. The saving path will take effect globally.

Click **Save**.

7.1.2 Configure Network Timeout

Network timeout is a certain amount of time which is used to define whether the interaction among the Web Client, FocSign server, and devices is successful or not. To be specific, if one party fails to response after the configured timeout, the interaction among them is regarded as a failure.

Steps

1. On the top, select **Maintenance**.
2. Select **Basic Configuration → Network Timeout** on the left.
3. Select the network timeout.
4. Click **Save**.

Table 7-1 Minimum Response Timeout in Different Interactions

Interaction Relation	Minimum Response Timeout
Between Web Client and FocSign server	60 s
Between FocSign server and Device	5 s
Between Web Client and Device	60 s

7.1.3 Configure Auto-Check Frequency

The FocSign server will check the health status of devices, resources, and servers managed on the platform. You can set the frequency which controls how often the platform gets the latest status of the devices, servers, and resources.

Steps

1. On the left of Maintenance module, select **Basic Configuration → Auto-Check Frequency** .
2. Switch on **Digital Signage Terminal / Interactive Flat Panel** to set how often the platform pings these devices to determine whether they are online.

   Note

   You should adjust the check frequency according to the number of devices. The greater the number of devices, the lower the frequency of health checks. When the frequency is too high, you will be prompted and recommended setting a lower frequency.
3. Click **Save**.

7.2 View Screen Status

You can view system topology and screen status.

On the top, select **Maintenance**.

Select **Screen Status** on the left.

View System Topology

You can have an overview of the system topology, click the device to view device information and status, view device alarm, etc.

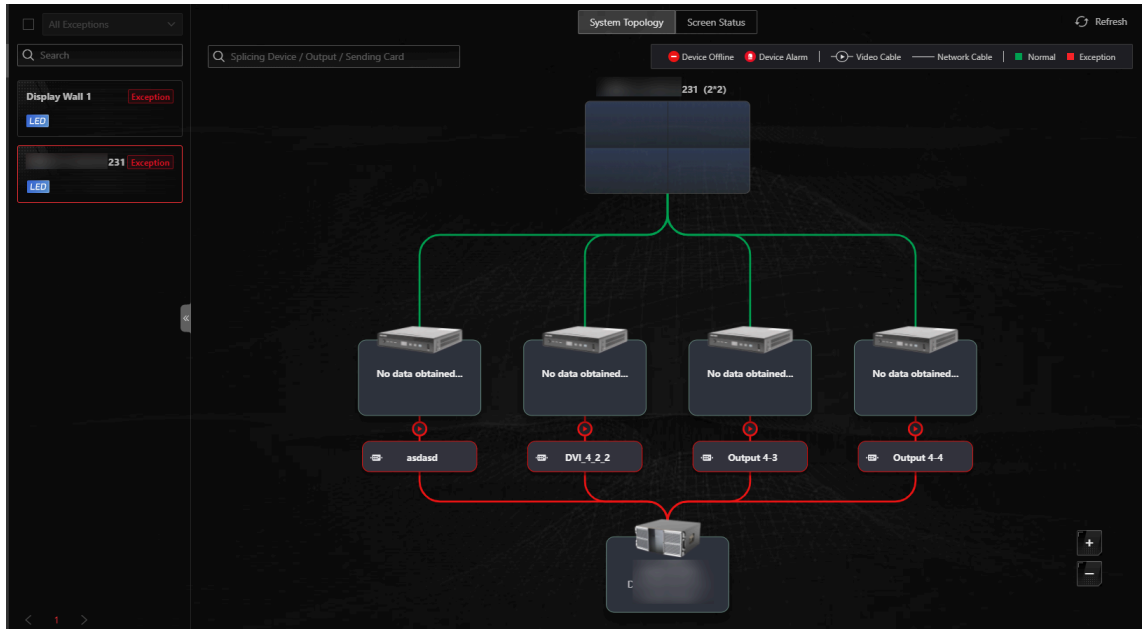

Figure 7-1 System Topology

View Screen Status

You can view information such as display wall status, screen status, and output information, refresh screen status, filter display walls by exception type, etc.

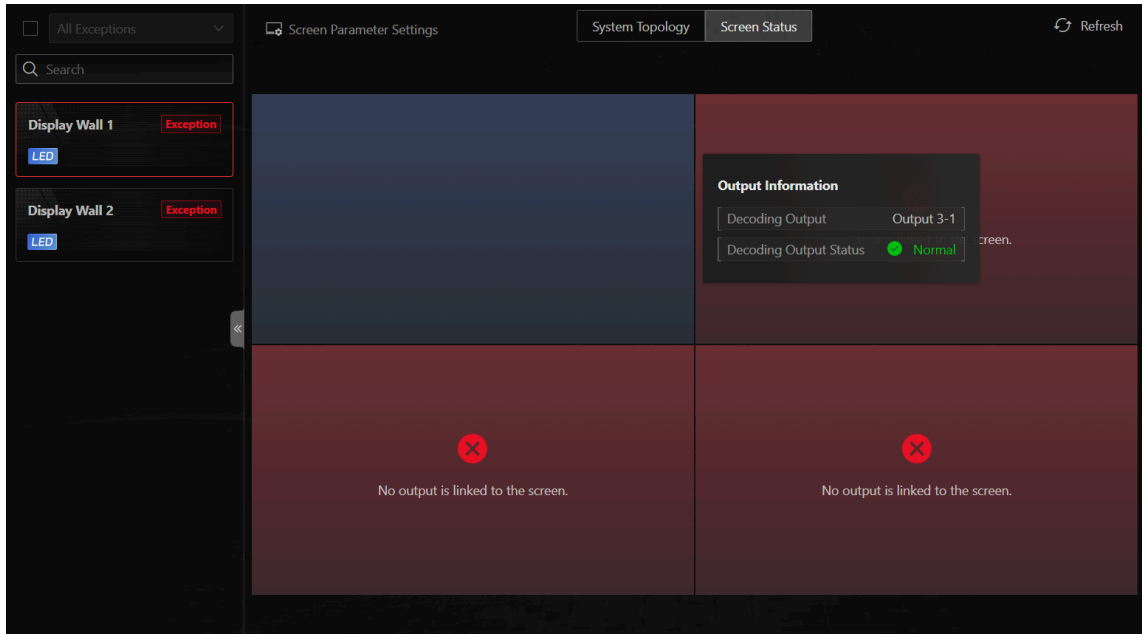

Figure 7-2 Screen Status

Screen Parameters Settings

You can go to the remote configuration page of the device to configure screen parameters. For detailed operation steps, see the user manual of the device.

7.3 View Resource Status

You can view the status and information of digital signage terminals, interactive flat panels, video wall controllers, and LED controllers.

On the top, select **Maintenance**.

Select **Resource Status → Digital Signage Terminal / Interactive Flat Panel / LED Controller / Video Wall Controller** on the left.

You can perform the following operations.

- Click the device name to view the device status and basic information. For a device with exception, click **Exception** in the Device Status column or click **Exception Details** on the Device Status pane to view information such as the issue type and possible cause.
- Click in the Operation column to go to the device configuration page to configure the device parameters. For details, see ***Configure Device Parameters Remotely*** .
- Check beside All Exceptions field, and select the exception type to filter the device information by exceptions.
- Click in the Operation column to refresh the device status, or click **Refresh** in the upper-right to refresh all device status.

Note

The platform supports checking the health of devices, resources, and servers automatically. For details, see ***Configure Auto-Check Frequency*** .

- Click to view the status of LED controllers, such as environment temperature and humidity.
- Enter keywords in the Search field to search for resources.
- Click **Switch to Local Device NTP Time Sync** to switch the time sync mode of the device with abnormal time sync status to Local Device NTP Time Sync.
- Click **Export** to export the resource status in Excel or CSV format.
- Click to set column width.
- Click to custom column items.

7.4 Search for Server Logs

You can search for server logs, which contain error logs, warning logs and information logs. Server logs contain historical user and server activities. You can search for the logs and then check the details.

Steps

1. In the top left corner, select → **All Modules → Maintenance → Server Logs** .
2. In the **Event** area, select one or multiple log types and sub types.

Note

Error logs record failures or errors. Information logs refer to other general logs which record successful or unknown operation results.

3. In the **Source** area, set the source of the logs that you want to search for.
4. **Optional:** In the **Resource Name** area, enter the name of a resource to search the logs of the resource.
5. Set the time range for search.

Note

You can select **Custom** to set a precise start time and end time.

6. Click **Search**.

   All matched logs are listed with details on the right.
7. **Optional:** Check all or specific logs, click **Export**, and then select a file format (i.e., Excel or CSV) to download the searched logs as a single file to your local PC.

Chapter 8 System Configuration

This module allows you to set different types (e.g., normal settings, network settings, storage settings, and so on) of parameters for the platform, such as defining a customized name for the site, setting NTP (Network Time Protocol) for synchronizing the time between the platform and the NTP server, and setting an IP address to allow the platform to access the WAN (Wide Area Network).

On the top, select **System** to enter this module.

8.1 Normal Settings

The normal settings menu provides entries of setting the user preference, holidays, printers, and card templates.

On the left navigation bar of the System page, select **Normal** to display the normal settings menu.

8.1.1 Set User Preference

For different countries, regions, cultures, and enterprise backgrounds, the user preference might be different. You can set the user preference according to the actual scene, such as the site name, the first day of a week, and the calendar type.

Select **User Preference** on the left navigation bar to enter the following page.

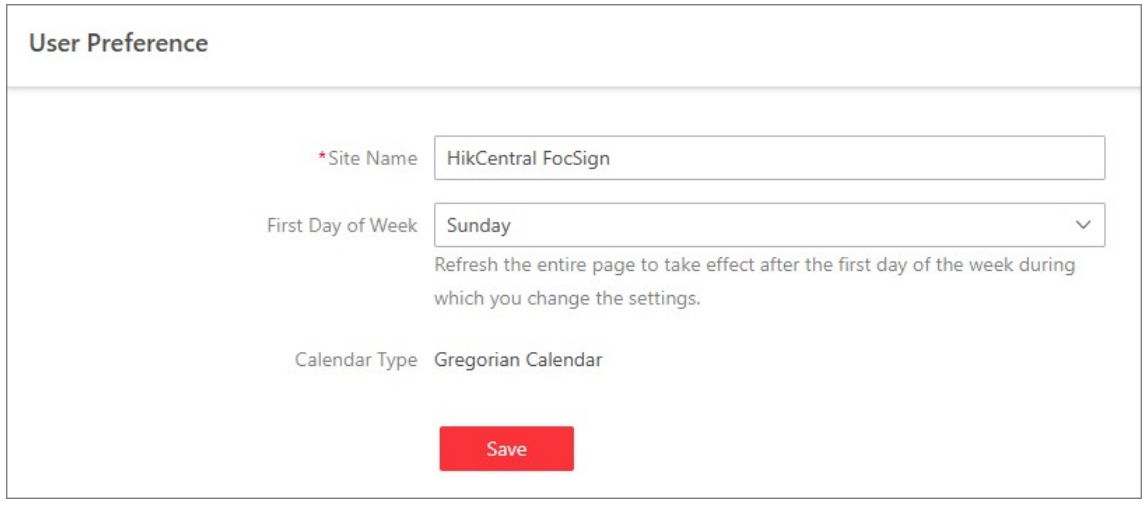

Figure 8-1 User Preference

Set the following parameters:

Site Name

Set the name of current site.

First Day of Week

Set the first day of a week as Sunday, Monday, Tuesday, etc., according to the custom of the actual scene.

Note

This parameter is used in the intelligent analysis report generation, etc.

8.1.2 Set Holiday

You can add the holiday to define the special days that can adopt a different schedule or access schedule. You can set a regular holiday and an irregular holiday according to the actual scene.

Select **Holiday Settings** on the left navigation bar to enter the Holiday Settings page.

Add Regular Holiday

The regular holiday is suitable for the holiday that has a fixed date. For example, Christmas is on December 25th of each year.

1. Click **Add** to open the adding holiday dialog.
2. Enter the holiday name and select **Regular Holiday** as the holiday type.
3. Set the parameters according to the following instructions:

   Start Time

   The start date of the holiday.

   Number of Days

   The lasting days of the holiday.

   Repeat Annually

   If checked, the platform will generate the date of the holiday according to the date of SYS (System Server).
4. Click **Add**.

Add Irregular Holiday

The irregular holiday is suitable for the holiday that is calculated by the weekdays, and the specified date might be different in a different year. For example, Mother's Day is on the second Sunday of each May.

1. Click **Add** to open the adding holiday dialog.
2. Enter the holiday name and select **Irregular Holiday** as the holiday type.
3. Set the parameters according to the following instructions:

   Start Time

   The start date of the holiday.

   For example, select **May**, **Second**, and **Sunday** for Mother's Day.

Number of Days

The lasting days of the holiday.

Repeat Annually

If checked, the system will generate the date of the holiday according to the date of SYS.

Note

If you check **Repeat Annually**, the specified date of this holiday will be generated automatically according to the current year of SYS.
For example, Mother's Day in 2019 and 2020 is on May 12th, 2019, and on May 10th, 2020. The system will automatically set these two days as holidays for Mother's Day if you have checked **Repeat Annually**.

4. Click **Add**.

8.2 Digital Signage Settings

8.2.1 Set Weather Web Manufacturer

You can enable weather service and set the weather manufacturer for the programs including weather information. After enabled, you can add a weather window in the program and display the weather information provided by the manufacturer.

Select **Weather Web Manufacturer** on the left navigation bar, and enable **Weather Web Manufacturer**.

Select the manufacturer name, and then enter the authorization code.

Note

The user should buy the weather service from the weather manufacturer and get the authorization code.

8.2.2 Set Material Storage Location

The materials uploaded can be saved to the local storage or pStor server.

Steps

1. Select **Digital Signage Settings → Material Storage Location** on the left.
2. Set the storage location as **Local Storage** or **pStor**, and select a resource pool.

Note

To select **pStor** as the storage location, make sure you have added pStor servers to the platform.

3. Click **Save** to save the above settings.

8.3 Management of Platform Accounts and Security

You can manage roles and users, assign roles with varying permissions to different users, configure security parameters and questions, and configure permission schedules to enhance system security.

On the top, select **System → Account and Security** .

8.3.1 Add Role

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

Steps

Note

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

Administrator

Role that has all permissions of the platform.

Operator

Role that has all permissions for accessing resources and operating the Applications.

1. On the top, select **System**.
2. Select **Account and Security → Roles** on the left.
3. Click **Add** to enter Add Role page.
4. Set the basic information of the role, including role name, effective period, role status, permission schedule template, description, etc.

   Copy From

   Copy all settings from an existing role.

   Permission Schedule Template

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

   Note

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

Area Display Rule

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

Resource Access

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

Note

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

User Permission

The role's permission for different operations on the platform.

6. Click **Add** to add the role and return to the role management page, or click **Add and Continue** to save the settings and continue to add another role.

8.3.2 Add Normal User

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

Steps

1. Select **Users** on the left.
2. Click **Add** on the top.
3. Set basic information for the user.

User Name

Only letters (a-z, A-Z), digits (0-9), and "-" are allowed.

Password

Create an initial password for the user. The user will be asked to change the password when logging in for first time. See ***First Time Login for Normal User*** for details.

Caution

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

Expiry Date

The date when the user account becomes invalid.

Email

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

Note

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

User Status

Active is selected by default. If you select **Inactive**, the user account will be inactivated until you activate it.

4. Configure parameters related to login protection.

Restrict Concurrent Logins

To restrict the number of simultaneous logins for user accounts, switch on **Restrict Concurrent Logins** and set the maximum number of concurrent logins.

5. Configure permission settings for the user.

Assign Role

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

Note

If you want to add new roles, click **Add**. See ***Add Role*** for details. Click a role on the list and then **View Role Details** to view the Basic Information and Permission Settings of the role.

6. Do one of the following to complete adding the user.
   - Click **Add** to add the user and return to the user management page.
   - Click **Add and Continue** to save the settings and continue to add another user.
7. **Optional:** Perform further operations on the added normal users.

Edit User	Click user name to view and edit user settings.
Reset Password	Click user name and click **Reset** to set a new password for the user. Enter a new password and click **Reset**. **Note** The admin user can reset the passwords of all the other users (except domain user). Other users with Security permission (in Configuration and Control Permission) can reset the passwords of the users without Security permission. When the normal user's password is reset by admin user, he/she should change the initial password and set a new password when logging into HikCentral FocSign via the Web Client.
Delete User	Select a users and click **Delete** to delete the selected user.
Force Logout	Select an online user and click **Force Logout** to log out the online user.

Inactivate/ Activate User	• The admin user or user with administrator permission can inactivate or activate a user. • Select an active users and click **Inactivate/Activate** to inactivate/activate the user.
Refresh User	Click **Refresh All** to get the latest status of all users.
Filter User	Click ▽ to set conditions and filter the users.
Unlock Users	For users whose account is locked due to too many failed attempts for login, Administrators can unlock their accounts for login. On the top of user list, click **Unlock for Login**, check users, and click **Unlock**.

8.3.3 Set Basic Security Parameters

System security is crucial for your system and property. You can lock IP address to prevent malicious attacks, and set other security settings to increase the system security.

Steps

1. Select **Account and Security → Basic Parameters** on the left.

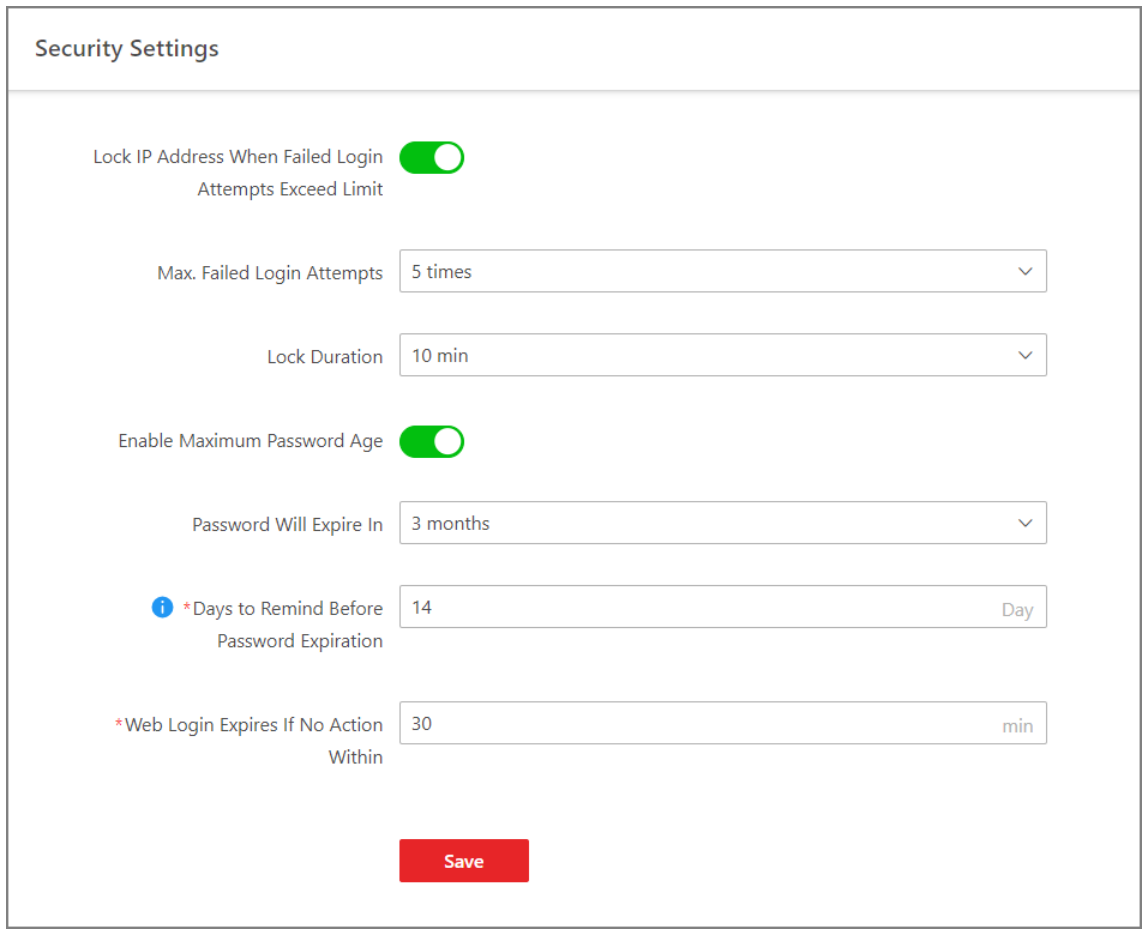

Figure 8-2 Security Settings Page

2. Limit the number of failed login attempts.

1) Select the maximum allowable login attempts for accessing HikCentral FocSign.

Note

Failed login attempts include failed password attempt and failed verification code attempt.

2) Set the lock duration for this IP address. During the lock duration, the login attempt via this IP address is not allowed.

The number of login attempts is limited.

3. Set the maximum password validity period.

1) Switch on **Enable Maximum Password Validity Period** to force user to change the password when the password expires.

2) Set the maximum number of days that the password is valid.

Note

After the maximum number of days, you should change the password. You can select the predefined time length or customize the time length.

3) Set days to remind you at each time you login or in the small hours of each day by sending an email notification before password expiration.

4. Set minutes after which the Web login will expire if there is no actions during the set minutes.
5. Click **Save** to save the above settings.

8.3.4 Configure Security Questions

Security questions can be used to verify user identity when users want to reset the password. After setting the security questions, users needs to first answer the security questions correctly before they can reset the password, so as to ensure account security.

Select **Security Question** on the left.

Set three security questions. Select a question from the drop-down list and set an answer to it.

Note

The answer should contain 1 to 128 characters, and cannot contain these special characters: / \ : * ? " < > |

Click **Save** to save the settings.

8.3.5 Configure Permission Schedule

Permission schedule defines the time when a role's permissions are valid. During unauthorized time periods, the user assigned with the role will be forced to log out and cannot log in. The platform provides 3 default permission schedule templates: All-day Template, Workday Template, and Weekend Template. You can add new templates according to actual needs.

Steps

1. On the top, select **System → Account and Security → Permission Schedule Template** .
2. Click + on the top left.
3. Set basic information.

   Copy From

   Copy the settings from another existing template.
4. In the **Weekly Schedule** area, click **Authorize** to select or draw in the box to define the authorized time periods.

   Note

   You can set up to 6 separate time periods for each day.
5. Click **Add** to add the permission schedule template.

8.4 Network Settings

The network settings menu provides entries of setting NTP for time synchronization, selecting device access protocol, setting an IP address to allow the platform to access the WAN, and so on.

On the left navigation bar of the System page, select **Network** to display the network settings menu.

8.4.1 Set NTP for Time Synchronization

You can set NTP parameters for synchronizing the time between resources managed on the platform and the NTP server.

Steps

1. Select **NTP** on the left navigation bar.
2. Select the **Time Sync Mode**.

   Note

   For time synchronization via network and the local server, just set the synchronization interval and click **Save**. For time synchronization via the NTP server, follow steps below.
3. Set the NTP server address and port No.

   Note

   If the local NTP server has been configured, click **Detect Local NTP** to fill in the NTP server address and port No. automatically.
4. Enter the interval of the automatic time synchronization.
5. **Optional:** Click **Test** to test the communication between resources and the NTP server.
6. **Optional:** Switch on **Configure WAN Mapping** and enter the IP address and port No. for WAN mapping.

   Note

   If the NTP service is locally deployed, you can configure WAN mapping to synchronize the time for devices on the WAN. Otherwise, enabling mapping is not required.
7. Click **Save**.

8.4.2 Set Active Directory

If you have an AD (Active Directory) domain controller which contains the information (e.g., user data, computer information), you can configure the settings to get the related information. In this way, you can add the users that belong to an organization unit (OU) (e.g., a department of your company) to the platform conveniently.

Steps

1. Select **Active Directory** on the left navigation bar.
2. Configure the corresponding parameters for connecting the platform to the AD domain controller.

Host Name

The IP address of DNS server. You can get it in Network Connection Details.

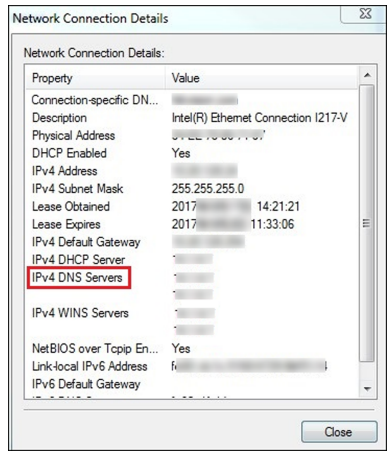

Figure 8-3 How to Get Host Name

Port No.

The port No. of the AD domain controller. By default, it is 389.

Enable SSL (Optional)

Enable SSL if it is required by the AD domain controller.

User Name / Password

The user name and password of the AD domain controller. The user should be the domain administrator.

Base DN (Distinguished Name)

Enter the filter condition in the text field if you are familiar with the format. Or you can click **Fetch DN** to get the filter condition entered automatically.

Note

- Only users found within an OU in the domain can be imported.
- If you enter the Base DN manually, you need to define the root node as desired. If you click **Fetch DN**, then the entire structure stored in the AD domain controller will be obtained.

3. Set the time to automatically synchronize the users in the AD domain to the platform.
4. Click **Save**.

After the configuration, the organization unit and domain user information will be displayed when you click **Import Domain User** on the **Account and Security → Users** page.

8.4.3 Set WAN Access

In some complicated network environments, you need to set a static IP address or a domain name and ports for HikCentral FocSign to access WAN (Wide Area Network).

Steps

1. Select **WAN Access** on the left navigation bar.
2. Click **Export**, and select ports to download a template.

	A	B	C
1	Do not edit the content in the first two columns.		
2	Port Name	LAN Port	WAN Port
3	Client Communication Port (HTTP)	80	
4	Client Communication Port (HTTPS)	443	
5	Client Communication Port (Cluster Port Segment)	18001-18021	
6	Generic Event Receiving Port (TCP)	15300	
7	Generic Event Receiving Port (UDP)	15300	
8	Generic Event Receiving Port (HTTP)	15310	
9	Generic Event Receiving Port (HTTPS)	15443	
10	ISUP Alarm Receiving Port (TCP)	7332	
11	ISUP Alarm Receiving Port (UDP)	7334	
12	ISUP Registration Port (TCP)	7660	
13	Port for Downloading Files from ISUP Devices (TCP)	8555	
14	OTAP Device Registered Port	7666	
15	IP Speaker Registration Port	8877	
16	IP Speaker Communication Port	10015	
17	SDK Alarm Listening Port	8686	
18	Sever Local Picture Storage Port (HTTP)	6011	
19	Server Local Picture Storage Port (HTTPS)	6111	
20	Sever Local File Storage Port (HTTP)	6203	
21	Server Local File Storage Port (HTTPS)	6204	
22	Remote Site Registration Port	14200	
23	Broadcast Signaling Port	7662	
24	Cluster Intercom Command Port	7668	
25	ISUP Streaming Port (TCP)	16000	
26	ISUP Port for Two-Way Audio (TCP)	16001	
27	ISUP Port for Broadcasting (TCP)	16003	
28	Cluster Intercom Streaming Port of ISUP Device	16005	
29	RTSP Streaming Port (TCP)	554	
30	Web Client Streaming Port (TCP)	559	
31	Streaming Media Signaling Port (TCP)	7661	
32	RTMP Streaming Port	1935	
33	HLS Streaming Port	83	

Figure 8-4 Exported Template

3. Send the template to your maintenance staff to enter the WAN port numbers, and get the completed file.
4. Click **Import** to import the completed file.
5. Enable **Access WAN** to enable the WAN access function.
6. Check the imported ports, and click **Save**.

8.4.4 Set IP Address for Receiving Device Information

You can select the NIC of the current FocSign server (System Server) so that the platform can receive the alarm information of the device connected via ONVIF protocol.

Before You Start
Make sure the server's ports ranging from 8087 to 8097 are available.

Steps
1. Select **Address for Receiving Device Info** on the left navigation bar.
2. Select **Get from NIC** or **Enter Manually**.

   Get from NIC

   Select the currently used NIC name of FocSign server in the drop-down list. The NIC information including description, MAC address, and IP address will be displayed.

   Enter Manually

   If you have configured hot spare for the FocSign server, you should manually enter the IP address.
3. Click **Save**.

8.5 Storage Settings

The storage settings menu provides entries of setting storage for pictures and files on FocSign server and specifying retention periods for different types of records.

On the left navigation bar of the System page, select **Storage** to display the storage settings menu.

8.5.1 Set Storage on System Server

The imported pictures (such as the static e-map pictures and the face pictures in the person list) can be stored on FocSign server. You can configure the storage locations and the corresponding quotas for them.

Steps

Note

This configuration is available only when the Web Client is running on FocSign server.

1. Select **Storage on SYS Server** on the left navigation bar.

   The disks of FocSign server are displayed with current free space and total capacity.
2. Switch on **Enable Local Storage**.
3. Configure the related parameters for storing pictures.

   1) Select the disk to store the imported pictures.

Note

The disk should have at least 1.25 GB of free space for picture storage.

2) **Optional:** Switch on **Set Quota for Pictures** and set the storage quota for the pictures.

4. Click **Add** to add a resource pool for storing files.
   1) Enter the name of the resource pool.
   2) Select a disk to store the files.

Note

The disk should have at least 9 GB of free space for file storage.

   3) **Optional:** Switch on **Restrict Quota for Pictures** and set the storage quota for the files.
   4) Check **Overwrite When Storage Space is Insufficient**, and the newly imported files will overwrite the existing files when the disk space is insufficient.
   5) Click **Add**.
   6) **Optional:** Click **Delete** or in the Operation column to delete a resource pool.
   7) **Optional:** Click a resource pool name to edit related settings.
5. Click **Save**.

8.5.2 Set Storage for Records

The data retention period specifies how long you can keep the events, logs, and some records on FocSign server.

Steps

1. Select **Records Storage** on the left navigation bar.
2. Select one language from the drop-down list to set the language of the sorting rule.
3. Set the data retention period from the drop-down list for the required data types.
4. Click **Save**.

8.6 Email Settings

You can add email templates for the scheduled report and configure the parameters of the sender's email account.

8.6.1 Set Scheduled Report Email Template

You can add email templates for the scheduled report. Go to **Email → Scheduled Report Email Template → Add** .

Recipients

You can add users in the platform or add emails. Up to 64 recipients can be added.

Subject

The email subject includes dynamic variables **Report Name** and **Time Period**. Clicking the two buttons will automatically populate the relevant information into the email subject and content.

Email Content

Select email content, including report type, report name, etc. Entering more email contents is required.

The template added here can be selected in **Maintenance → Basic Configuration → Scheduled Report → Advanced Settings → Send via Email** . For details, see ***Configure Scheduled Log Report*** .

8.6.2 Configure Email Account

You should configure the parameters of the sender's email account before the system can send the message to the designated email account(s) as the email linkage.

Steps

1. Select **Email → Email Settings** on the left navigation bar.
2. Configure the parameters according to actual needs.

Server Authentication

If your mail server requires authentication, check this checkbox to use authentication to log in to this server.

Cryptographic Protocol

Select the cryptographic protocol of the email to protect the email content if required by the SMTP server.

Sender Email Address

Enter the email address of the sender to send the message.

Sender Name

Enter the sender name to send the message.

SMTP Server Address

The SMTP server's IP address or host name (e.g., smtp.263xmail.com).

SMTP Server Port

The default TCP/IP port used for SMTP is 25.

User Name (Optional)

User name for authentication to log in to the server. This parameter is valid and optional when server authentication is enabled.

Password (Optional)

Password for authentication to log in to the server. This parameter is valid and optional when server authentication is enabled.

Note

For users of Google email, you should log in to your Google account, enable the 2-step verification function, generate the APP password, and enter here.

3. Click **Email Test** to test whether the email settings work or not.

   The corresponding attention message box will pop up.
4. Click **Save**.

8.7 Security Settings

The security settings menu provides entries of setting the transfer protocol for FocSign server, exporting service component certificate, enabling export of profile pictures, enabling watermark in video or picture, and setting the database password.

On the left navigation bar of the System page, select **Security** to display the security settings menu.

8.7.1 Set Transport Protocol

You can set FocSign server's transport protocol to define the access mode for FocSign server via clients as HTTP or HTTPS. The HTTPS protocol provides higher data security.

Steps

1. Select **Transport Protocol** on the left navigation bar.
2. In the **Transport Protocol Between Platform and Browser** field, select **HTTP** or **HTTPS** as the transport protocol between clients and FocSign server.

   Note

   For HTTPS, only the TLS 1.2 and later versions are supported. The browser must support and has enabled the TLS 1.2 or later version. You are recommended to use the browser supporting TLS 1.3.
3. **Optional:** If **HTTPS** is selected, perform the following steps to set the certificate.
   1) Select **Platform Provided Certificate**, or select **New Certificate** and click to select a new certificate file from your local PC.
   2) **Optional:** Click **Add** → → **Confirm** to add a upper-level certificate as needed.

      Note

      You can select the added certificate(s) and click **Delete** to delete them, or click in the Operation column of a certificate to download the certificate.
4. Click **Save**.
   - The FocSign server will restart automatically after the transport protocol is changed.
   - All logged-in users will be forced to log out during the restarting, which takes about one minute and after that, the users can log in again.

8.7.2 Export Service Component Certificate

For data security, before adding the Streaming Server or Cloud Storage Server to the platform, you should generate the service component certificate stored in FocSign server and input the certificate information to the Streaming Server you want to add, or export the service component certificate stored in FocSign server and import the certificate to the Cloud Storage Server, so that the certificates of the Streaming Server, Cloud Storage Server and FocSign server are the same.

Steps

1. Select **Service Component Certificate** on the left navigation bar.
2. Click **Generate Again** beside **Certificate between Services in System** to generate the security certificate for Streaming Server verification.
3. Click **Export** to export the service component certificate in XML format and save it to the local PC.

8.7.3 Set Database Password

You can set the database password of the platform on the Web Client running on FocSign server.

Note

Setting database password is only available when you access the Web Client on FocSign server locally.

Select **Database Password** on the left navigation bar.

Enter the password and then click **Verify** to generate the verification code and enter the verification code.

8.8 Configure Open API

The system provides open platform to integrate the third-party system. By the Open APIs (application programming interface) provided on the open platform, the third-party system can obtain some functions (such live view, playback, alarm, etc.) of HikCentral FocSign, to develop more customized features.

Before You Start

Setting open platform is only available when you access the Web Client on the SYS server locally.

Steps

1. On the top, select **System**.
2. On the left navigation pane, click **Third-Party Integration → Open API** to enter the configuration page.
3. Switch on **Open API**.

4. Set the IP address of the open platform, management port of the open platform, and the partner user.

Note

- The open platform should be deployed in the same network with the SYS server.
- The third-party system integrates the HikCentral FocSign by the partner user(s) you select, which defines the permission(s) of resources and operations in HikCentral FocSign.

5. Click **Test** to test the service availability of the open platform.
6. Click **Save** to save the settings.

8.9 Advanced Settings

The advanced settings menu provides entries of setting system hot spare, generating or debugging logs, downloading the event tracking information, and resetting the network information for devices.

On the left navigation bar of the System page, select **Advanced** to display the advanced settings menu.

8.9.1 Set Diagnosis & Maintenance Parameters

When faults occur in HikCentral FocSign, you can get the system information using the authentication code generated by HikCentral FocSign to help diagnose the system faults.

Steps

1. On the top, select **System**.
2. On the left navigation pane, click **Advanced → Diagnosis & Maintenance** to enter the configuration page.
3. Switch on **Remote Fault Diagnosis** to generate an authentication code for remote diagnosis.

Note

The authentication code will be refreshed every time you switch on **Remote Fault Diagnosis**.

The authentication code will be canceled automatically after 60 minutes.

4. Launch Postman, create a new request, set the HTTP method to POST, and enter the request URL (format: *http://<host>[:port]/ISAPI/Bumblebee/Platform/V1/TranckTaskInfo?&MT=GET*).
5. Then in the Body area, enter the request message in JSON format (set the **trackModuleName** to the module name and set the **AccessKey** to the authentication code generated on HikCentral FocSign), and click **Send**.
6. The response message is returned in the Body area of Response and it shows the system running information. You can perform fault diagnosis remotely according to the information.

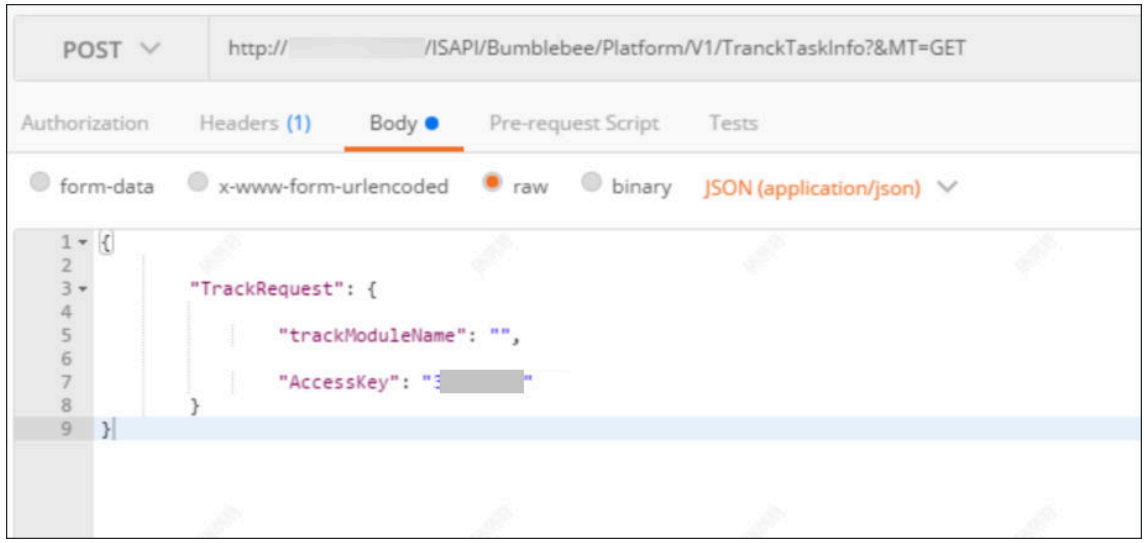

Figure 8-5 Get System Running Information Using Postman

8.9.2 Reset Device Network Information

When the system network domain changes (such as server migration), you must reset the network information for the added device to adapt to the new network environment. Otherwise, some functions of the device will be affected.

Steps

1. Select **Reset Network Information** on the left navigation bar.
2. Click **Reset** to one-touch reset the device network information.

Chapter 9 Maintenance and Management

You can view license expiry date, view license details, update license, export configuration data, etc.

In the top-right corner, click **Maintenance and Management**, and perform one of the following operations as needed.

View License Details

Click **License Details** to view the license list you purchased and license details, such as authorization details.

Update License

Two update types including online update and offline update are provided. According to the network status, select the update type, and complete updating license following the interface information. For details about updating the license, refer to ***Update License - Online*** and ***Update License - Offline*** .

Deactivate License

Two deactivation type including online deactivation and offline deactivation are provided. According to the network status, select the deactivation type, and complete deactivating license following the interface information. For details about deactivating the license, refer to ***Deactivate License - Online*** and ***Deactivate License - Offline*** .

Back Up Data

Select **Back Up and Restore System Data → Back Up** . Select the data type you want to back up, frequency, time, and maximum number of backups, and click **Save** or **Save and Back Up Now** to back up data in the configured time or immediately.

Restore Data

Select **Back Up and Restore System Data → Restore** . Select the backup file and click **Restore** to restore the data.

Export Configuration Data

Click **Export Configuration Data**, select data type, and click **Export** to export the select data.

Upgrade to HikCentral Professional

If you need application scenarios such as parking lot management and access control management, and need to extend the platform's functions, you can install HikCentral Professional (V2.2.1 or above) directly on the basis of the current platform, without unloading any original modules.

About

Click **About**, you can view the version, system ID, open-source license agreement, and license agreement of the client.


See Far, Go Further