Keyboard Video Mouse

User Manual

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.
- HDMI The terms HDMI and HDMI High-Definition Multimedia Interface, and the HDMI Logo are trademarks or registered trademarks of HDMI Licensing Administrator, Inc. in the United States and other countries.

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.

Preface

Applicable Models

This manual is applicable to the DS-C80K keyboard video mouse.

Default Parameters

Type	Default Parameter
Device	• Login user name: admin • IP address: 192.0.0.64
SSH connection	

Caution

To improve system security, it is highly recommended to change password regularly. In order to protect your privacy and corporate data and avoid network security issues, it is recommended to set strong password that meets security requirements.

Symbol Conventions

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

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

Safety Instructions

Caution

In the use of the product, you must be in strict compliance with the electrical safety regulations of the nation and region.

Note

- Provide a surge suppressor at the inlet opening of the device under special conditions such as the mountain top, iron tower, and forest.
- + identifies the positive terminals of the device which is used with, or generates direct current, and - identifies the negative terminals of the device which is used with, or generates direct current.
- The serial port of the device is used for debugging only.
- The interface varies with the models. Please refer to the product datasheet for details.

TABLE OF CONTENTS

Chapter 1 Introduction

1.1 Overview

The keyboard video mouse (hereinafter referred to as the KVM or device) is based on IP architecture and adopts the distributed technology without center server, which consists of multiple input nodes and output nodes. The KVM supports seamlessly data changing of different seats, elastic expansion of the device scale, information sharing and problem solving among seats, and interconnection between the local and remote seats. With a visual operation interface, the KVM supports online monitoring and management of maintenance data and device running condition. It is applicable to the monitoring or command centers in public security, transportation, and electricity industry.

1.2 First-Time Configuration Process

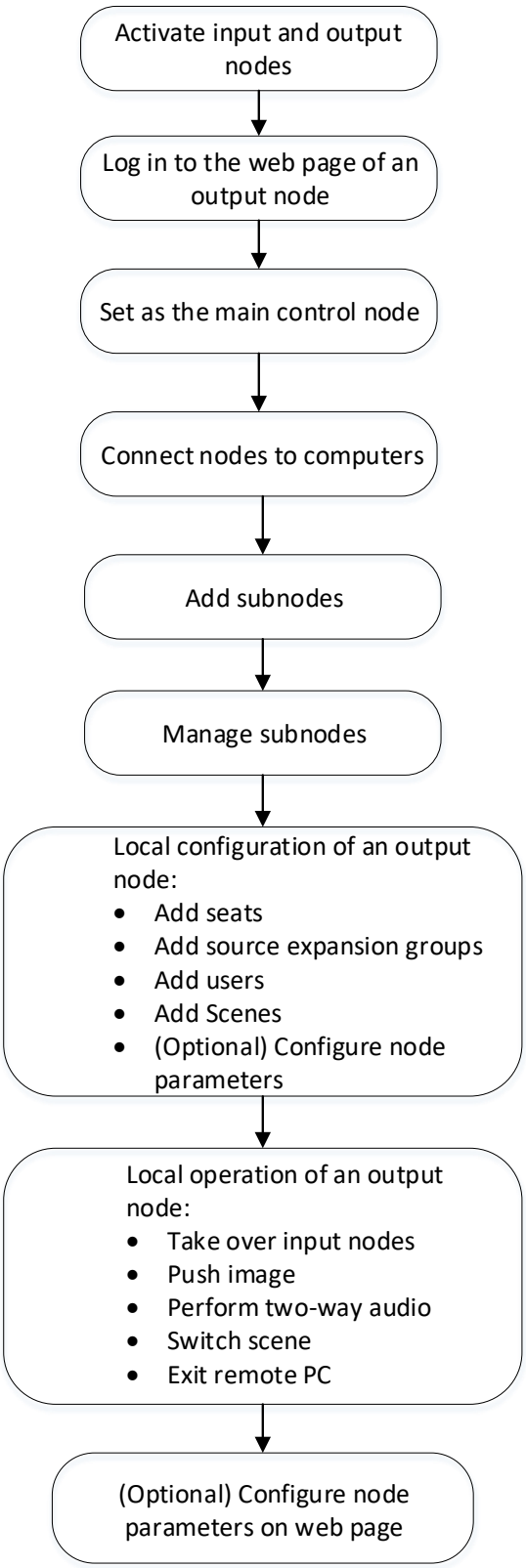

Figure 1-1 First-Time Configuration Process

1.3 Node Function Comparison

The input nodes, output nodes, and the main control node support configuration, and maintenance and security. On the **Configuration** and **Maintenance and Security** pages, the supported functions vary by the node type.

Table 1-1 Configuration Page

Function			Main Control Node	Output Node	Input Node
System	System Settings	Basic Information	√	√	√
		Time Settings			√
	User Management			√	√
Network	Network Configuration	TCP/IP		√	√
	Network Service	HTTPS		√	√
Node Configuration	Node Status				
	Node Management				
Device Settings				√	
Signal Source Settings	Image Settings	Source Clipping			√
	Encoding Settings				√
Other Settings	Streaming Mode				
	Local Source Mode				

Table 1-2 Maintenance and Security Page

Web Page		Main Control Node	Output Node	Input Node
System Maintenance	Restart		√	
	Upgrade		√	
	Backup and Reset			
	Log			
	Device Debugging	√	√	√
Security Management	IP Address Filter			
	HTTPS Certificate		√	
	SADP			
	Syslog			

Note

The main control node supports more functions than an input node or output node. This manual uses the main control node as an example.

Chapter 2 Node Batch Activation

You should activate the nodes before using the nodes for the first time. When activating the nodes, obey the following requirements to set the password:

- Password should contain 8 to 16 characters and at least 2 of the following types: digits, lowercase letters, uppercase letters, and special characters.
- Password cannot contain user name, 123, admin, 4 or more continuously ascending or descending digits, or 4 or more consecutive repeated characters.
- To improve system security, it is highly recommended to change the password regularly.

2.1 Use SADP Client

Step 1 Connect all nodes and the computer to the same LAN.

Step 2 Visit https://www.hikvision.com/en/support/tools/hitools/clea8b3e4ea7da90a9/ to download the SADP client from the Hikvision website and install the SADP client on the computer.

Step 3 Open the SADP client.

Step 4 Select the nodes that are not activated, enter the activation password and confirm it, and click **Activate**.

If no nodes can be found, you can restart the SADP client.

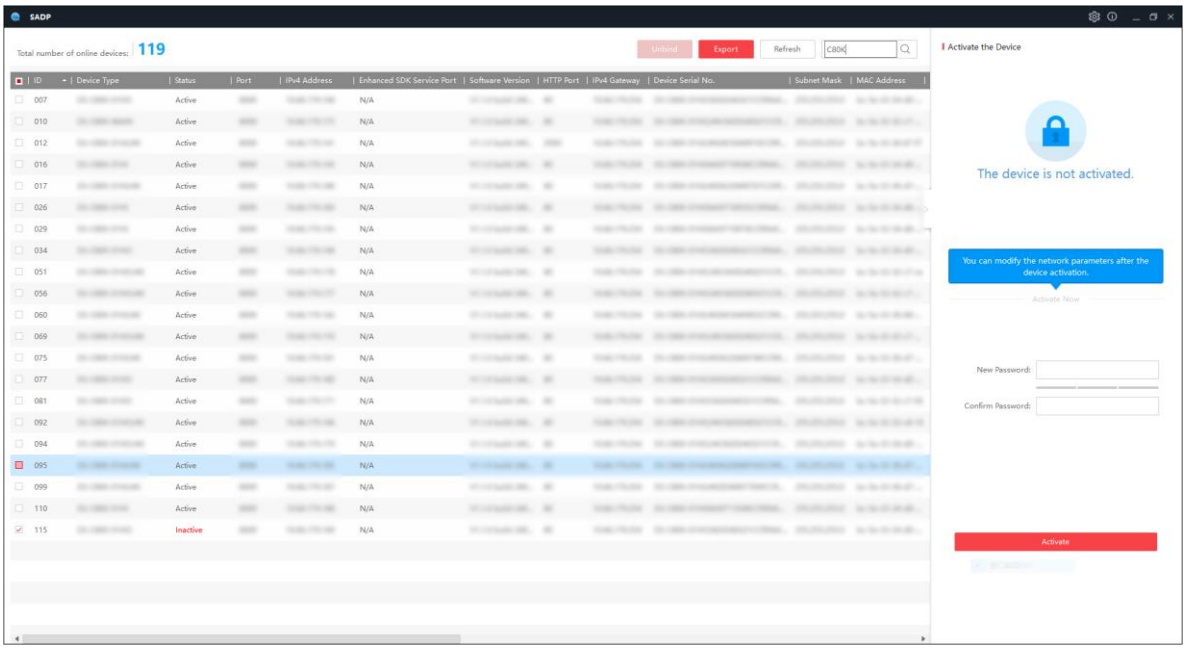

Figure 2-1 Batch Activate Nodes

Note

To activate a single node, you can log in to the web page of the node and activate it.

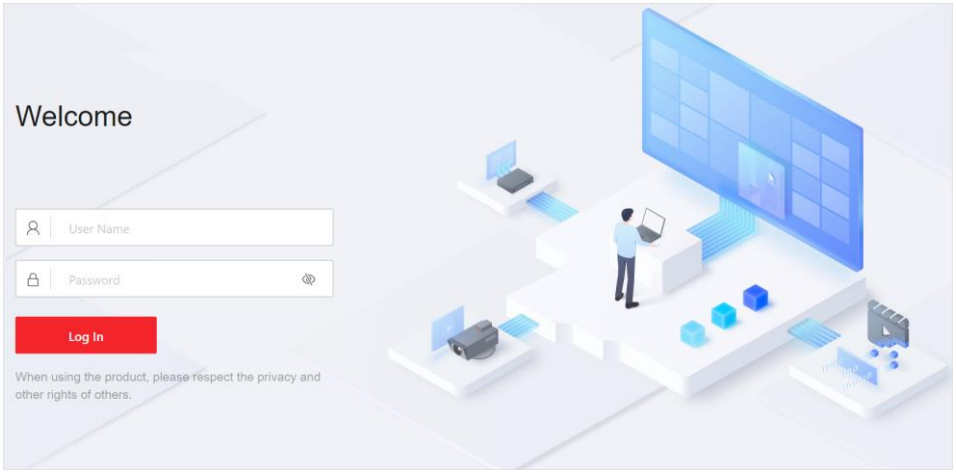

Figure 2-2 Activate a Single Node

Step 5 Select the activated nodes to batch edit their IP addresses.

Enter the start IP, port No., subnet mask, gateway, HTTP port No. and the administrator password, and then click **Modify**.

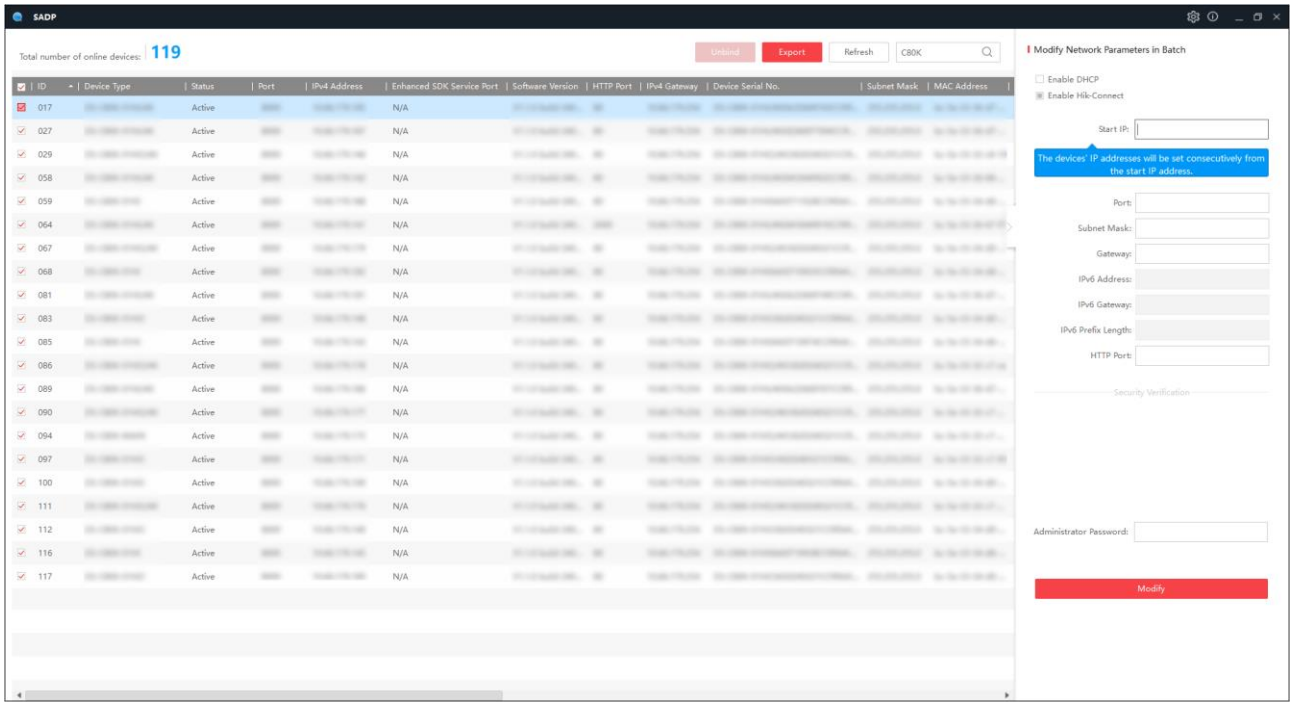

Figure 2-3 Batch Edit IP Addresses

2.2 Use HiTools Delivery

Step 1 Connect all nodes and the computer to the same LAN.

Step 2 Visit https://www.hikvision.com/en/support/tools/hitools/cl7f0143d2c781a3e3/ to download the HiTools Delivery client from the Hikvision website and install the HiTools Delivery client on the computer.

Step 3 Open the HiTools Delivery client.

Step 4 Select the nodes that are not activated, enter the activation password and confirm it, and click **Activation**.

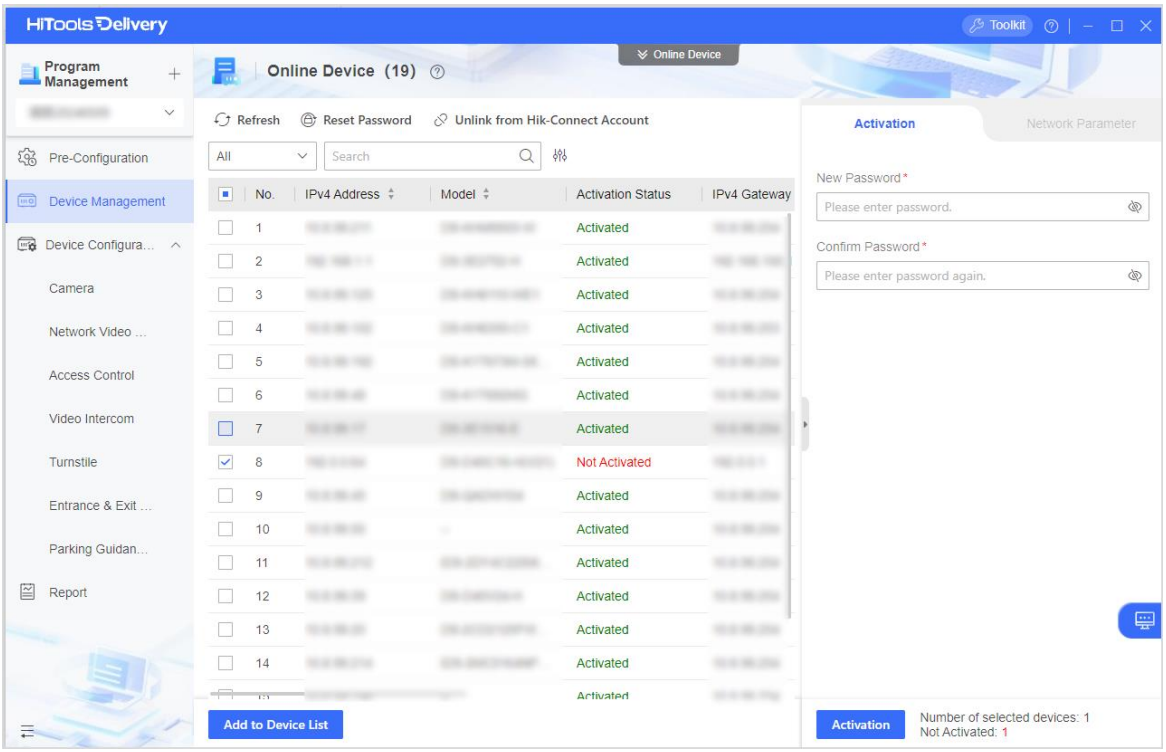

Figure 2-4 Batch Activate Nodes

Note

To activate a single node, you can log in to the web page of the node and activate it.

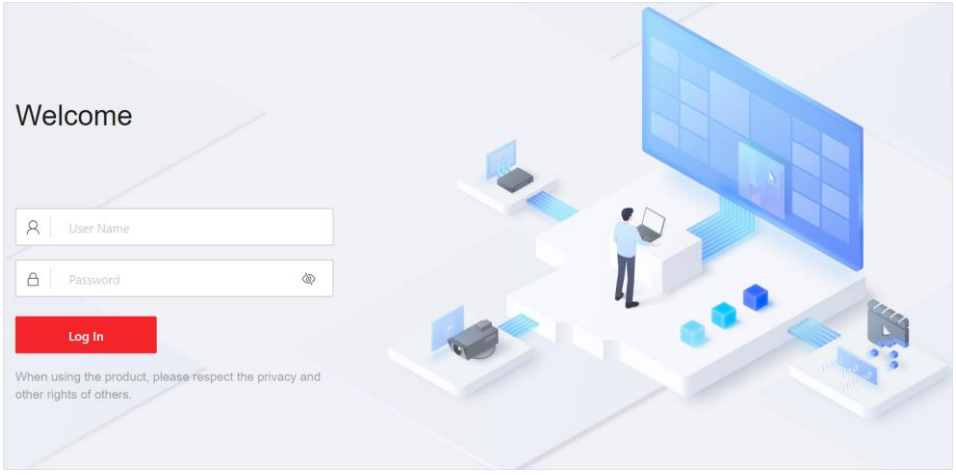

Figure 2-5 Activate a Single Node

Step 5 Select the activated nodes to batch edit their IP addresses.

Enter the start IP address, HTTP port No., SDK service port No., subnet mask, IPv4 gateway, and the admin password, and then click **OK**.

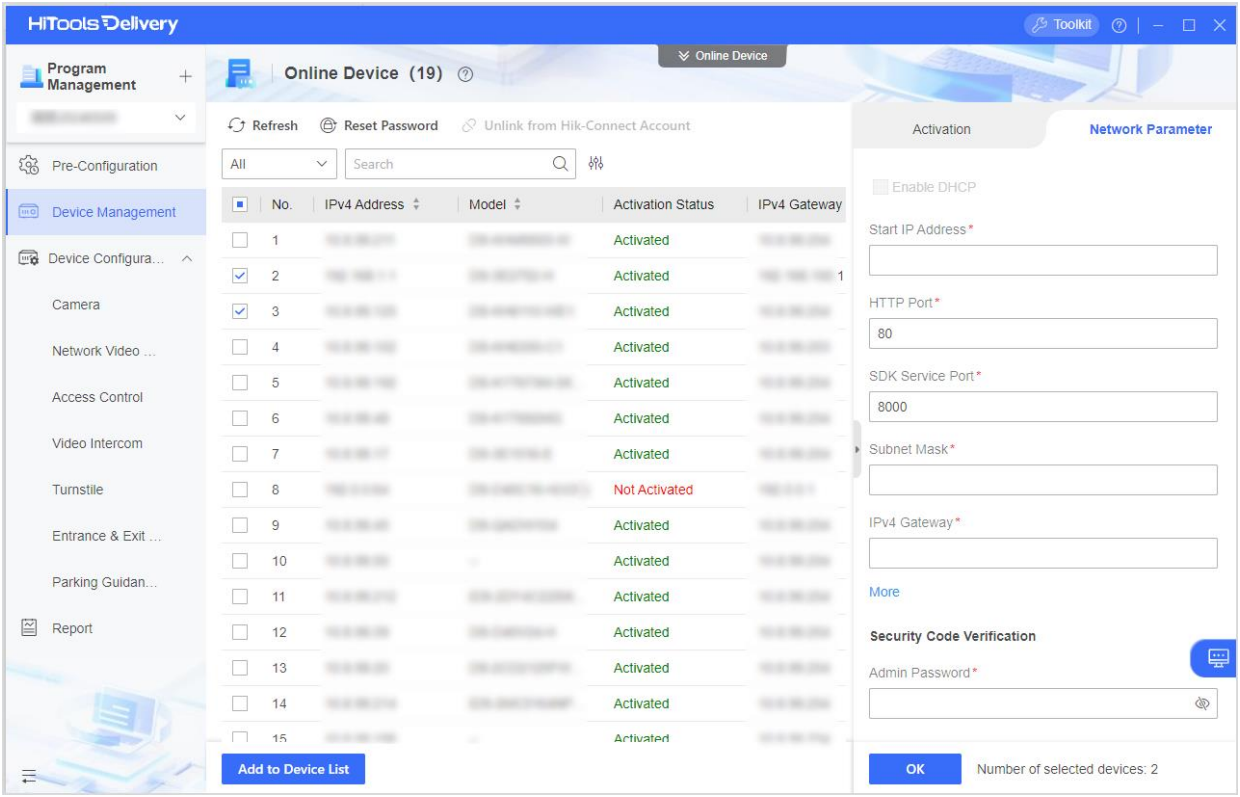

Figure 2-6 Batch Edit IP Addresses

Chapter 3 Main Control Node Configuration

3.1 Configure an Output Node as the Main Control Node

Step 1 Enter the IP address of an output node in the web browser of the computer.

Step 2 Enter the user name and the set activation password.

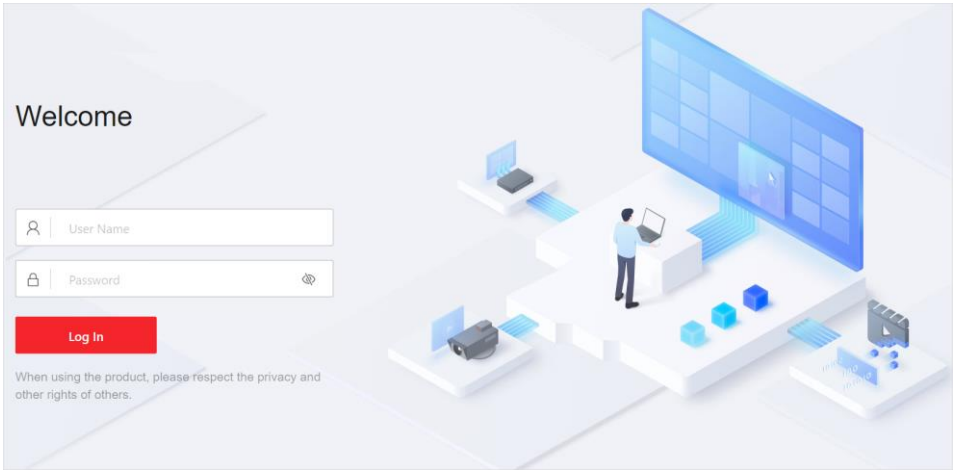

Figure 3-1 Login Page

Step 3 Click **Log In**.

Step 4 Go to **Configuration** → **Device Settings**, enable **Set as Main Control** and set the output resolution.

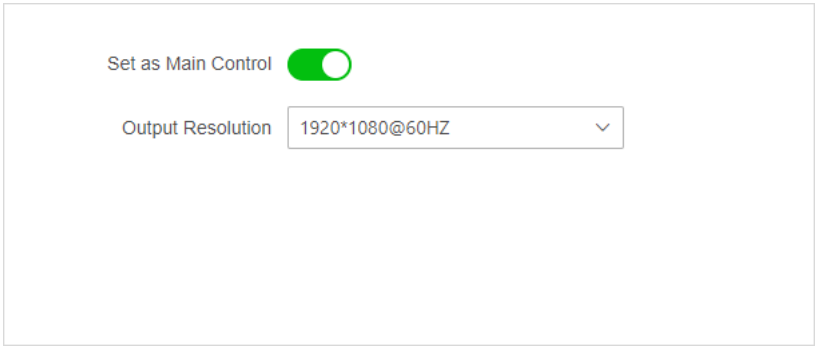

Figure 3-2 Set as Main Control

Note

The configured output resolution is valid only for the current node.

3.2 Connect Nodes to Computers

3.2.1 Connect Nodes to a Computer with One Display Port

Step 1 Connect an input node to a computer that provides one display port:

- Use a USB to USB cable to connect the HID port of an input node to the USB port of a computer.
- Use an HDMI cable to connect the input node to the computer.

Step 2 Configure at least one output node and connect at least an output node to a display:

- Connect a keyboard and a mouse to the MOUSE/KEYBOARD ports of an output node.
- Use an HDMI cable to connect the output node to a display.

3.2.2 Connect Nodes to a Computer with Multiple Display Ports

Step 1 Determine the number of input nodes and output nodes.

- Configure the same number of input nodes according to the number of display ports of a computer.
- Configure at least the same number of output nodes as the number of input nodes.

Note

- If the number of output nodes in a seat is less than the number of input nodes in a source expansion group, only the images of the same number of input nodes as the output nodes can be displayed after an output node or a seat takes over the input nodes. The order of the input nodes in the source expansion group from left to right is the order of images that can be displayed.
- To display the images of all input nodes on the limited displays when the number of output nodes in a seat is less than the number of input nodes in a source expansion group, you can configure multiple input nodes in one scene. For more information, see 4.4 Add Scenes.

Step 2 Connect a keyboard and a mouse to the MOUSE/KEYBOARD ports of each output node, and use an HDMI cable to connect a display to each output node.

Step 3 Use an HDMI cable to connect a computer to each input node, and at least use a USB to USB cable to connect the HID port of the leftmost input node in the source expansion group to the USB port of a computer.

Note

After any output node takes over the input nodes, you can log in to an output node and remotely control the computers connected with the input nodes.

3.3 Add Subnodes

The node parameters configured in the web page and the local configuration page will be synchronized.

3.3.1 Add Subnodes via Web Page

Step 1 Go to **Configuration** → **Node Configuration** → **Node Management**.

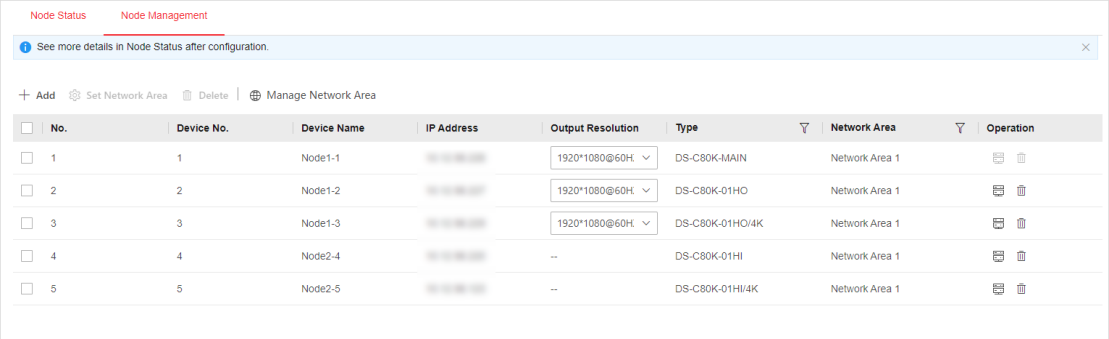

Figure 3-3 Figure 2-8 Node Management

Step 2 Click **Add**.

Step 3 Select IP/domain name or IP segment to add output and input nodes.

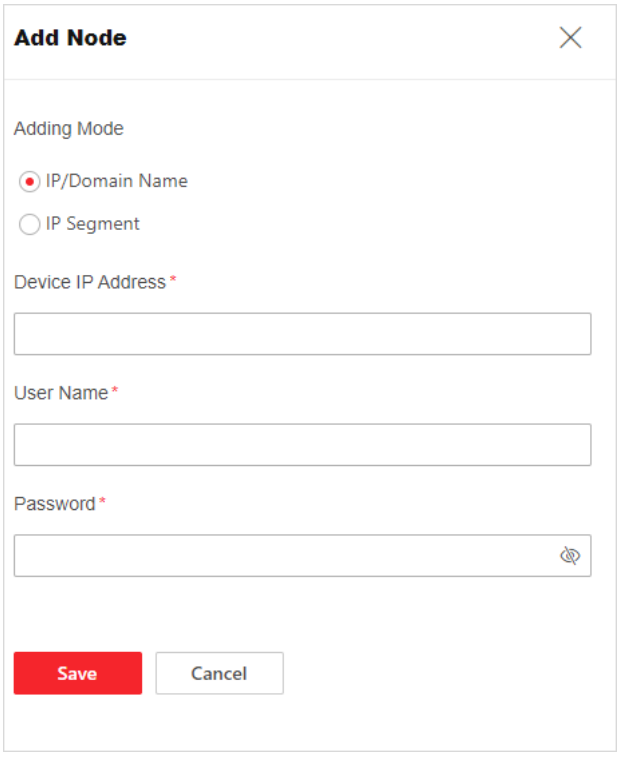

Figure 3-4 Figure 2-9 Add Nodes

Step 4 Click **Save**.

3.3.2 Add Subnodes via Local Configuration Page

Log in to Local Configuration Page of the Main Control Node

Step 1 On the local configuration page of the main control node, enter the user name and password set during activation.

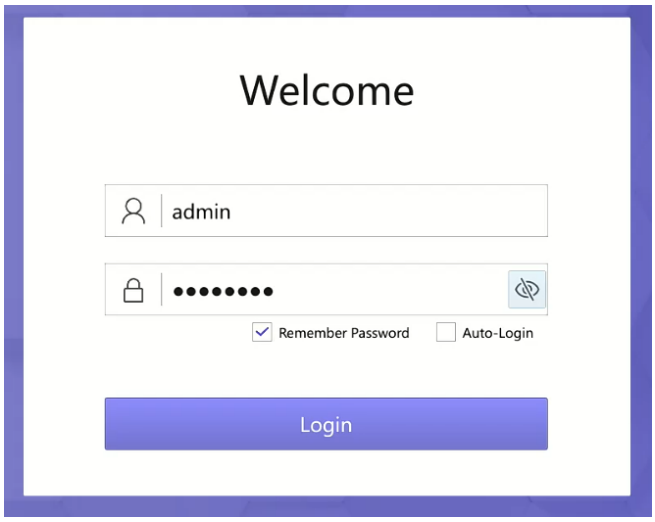

Figure 3-5 Local Login Page

Step 2 Click **Login** to enter the main local configuration page.

- Click  to collapse the toolbar.
- Click  to take over the input nodes.
- Click  to push the images of the taken-over input nodes to other output nodes or push the control of the taken-over input nodes to other output nodes.
- Click  to configure scenes and change scenes.
- Click  to configure nodes, users, source expansion groups, scenes, and seats.
- Click  for logout.
- Move  to adjust the toolbar position.
- Click  to exit remote PC.

Figure 3-6 Main Page with Expanded Toolbar

Figure 3-7 Main Page with Collapsed Toolbar

Add Subnodes

Up to 25 input or output node groups can be created. Up to 20 nodes are allowed in each input or output node group.

Step 1 On the main page, click → **Node Management**.

Step 2 Select a node type and add a node group:

- Click **Input Node** and click **Add**. Enter the node group name and click **Save**.

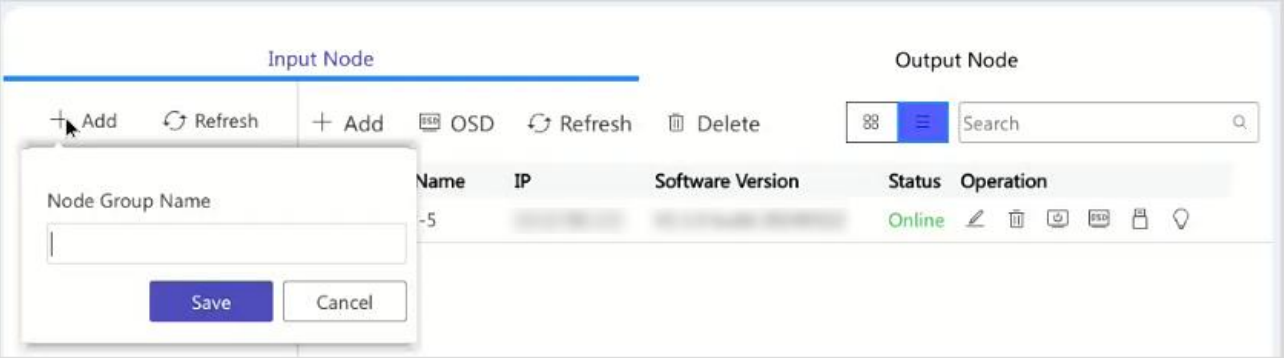

Figure 3-8 Create Input Node Group

- Click **Output Node** and click **Add**. Enter the node group name and click **Save**.

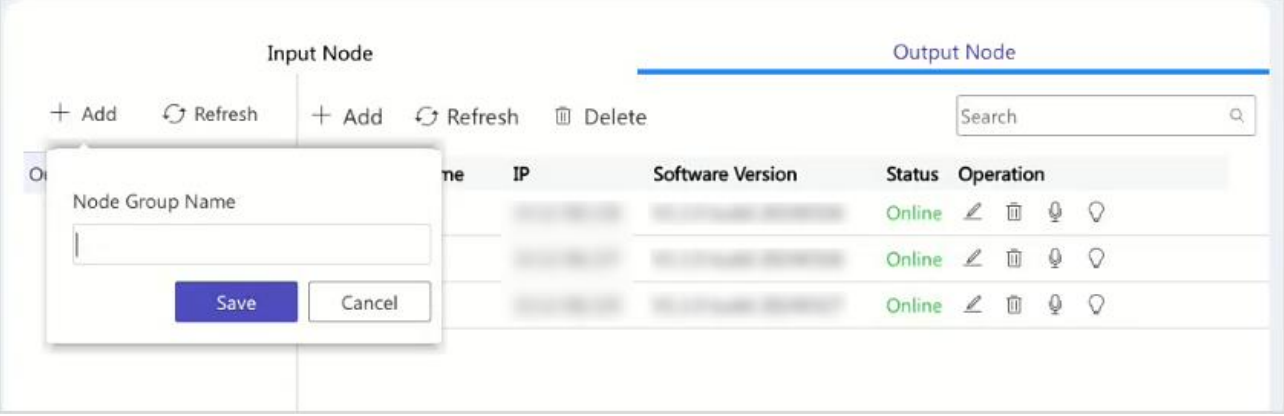

Figure 3-9 Create Output Node Group

Step 3 The adding methods are the same for an input node and output node. The following uses an input node as an example.

1) Click Input Node.
2) Click a node group or select a node group when you add a node manually.
3) Click **Add**.

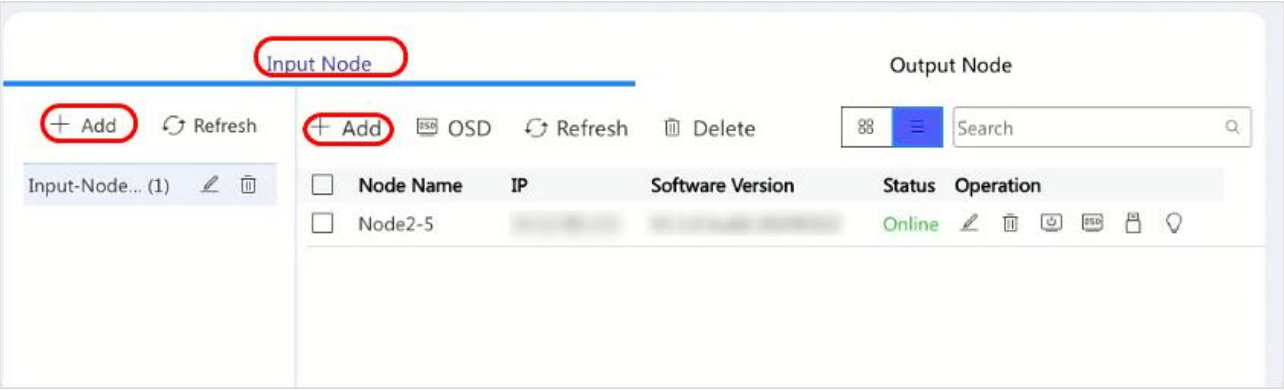

Figure 3-10 Add an Input Node

4) Select an adding mode.

– Select **Manual**, enter the node name and IP address, select a node group (optional), enter the password, and click **Save**. You can click **Save_Add More** to save the current node settings and add more nodes.

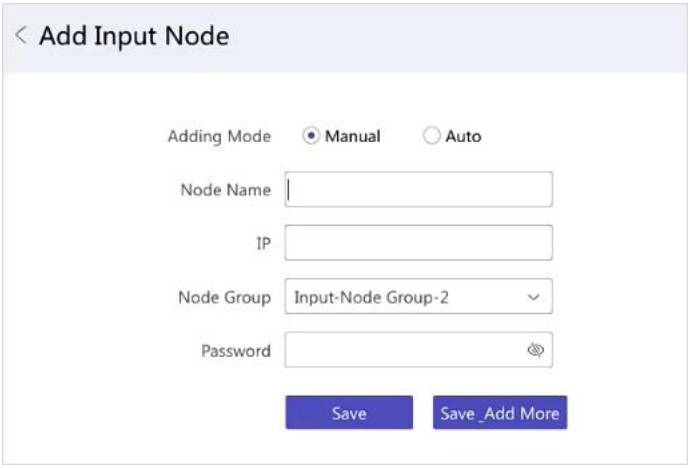

Figure 3-11 Manually Add an Input Node

– Select **Auto**. The nodes in the same LAN will be found automatically. Select the activated nodes, enter the password, and click **Save**. By default, those nodes will join the first available node group.

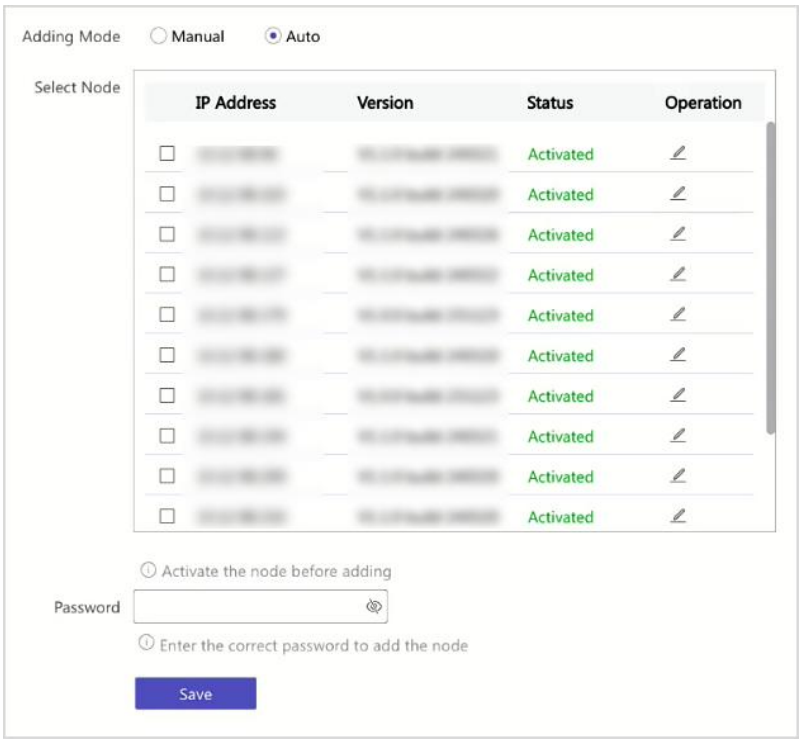

Figure 3-12 Automatically Add Input Nodes

3.4 Manage Subnodes

3.4.1 Manage Subnodes via Web Page

Step 1 Go to **Configuration** → **Node Configuration** → **Node Status**, select a node to view its status, restart it or lighten its indicator.

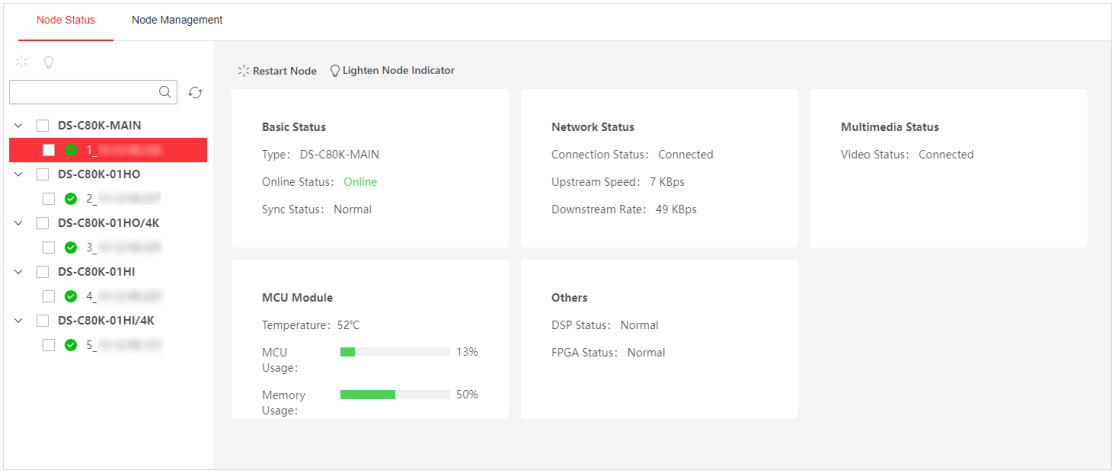

Figure 3-13 View Node Status

Step 2 Click **Node Management** to edit the output resolutions of the main control node and output nodes.

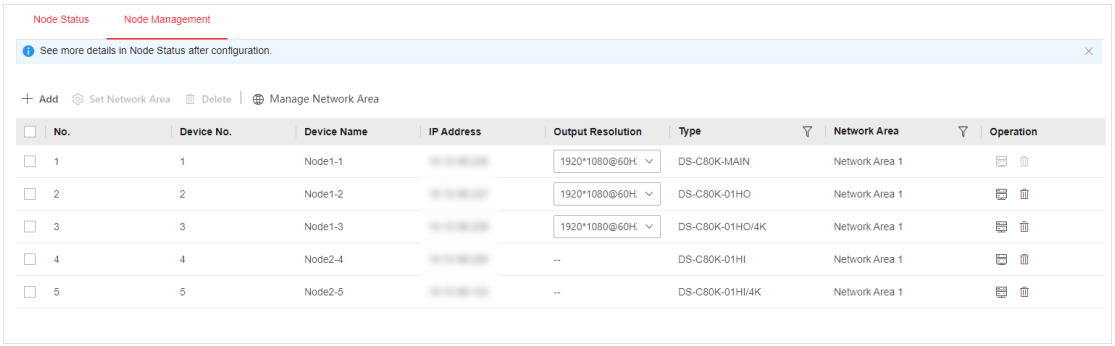

Figure 3-14 Edit Output Resolution

Step 3 Set the network area for nodes: Click **Manage Network Area** to add, edit, or delete network areas. Select the nodes, and click **Set Network Area** to set the network area of the node.

If the nodes are in the same network area, the delay will be low, but more bandwidth will be occupied.

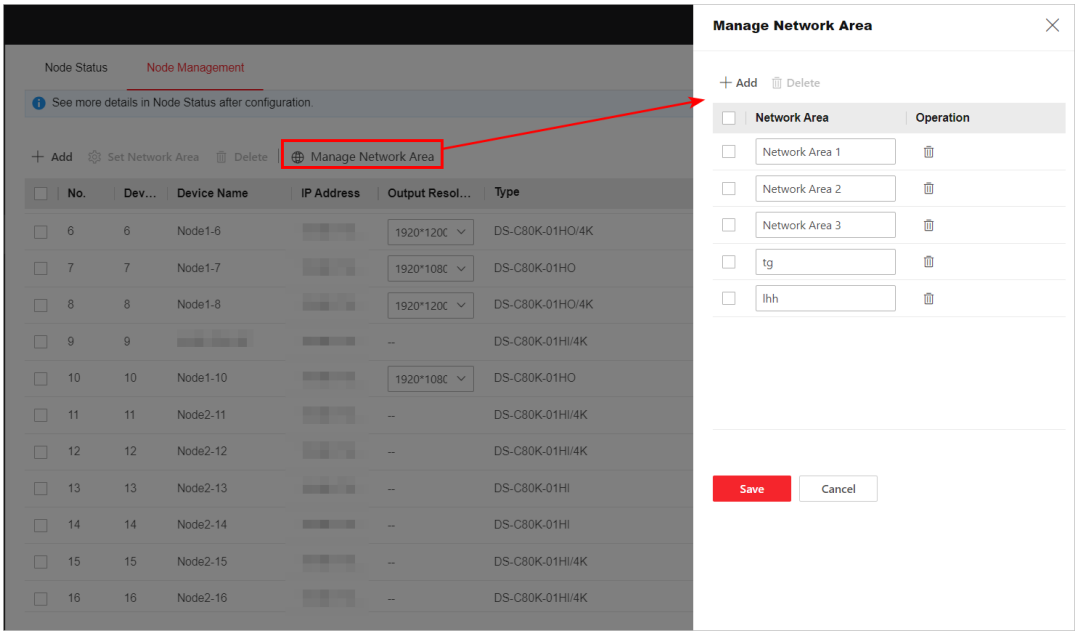

Figure 3-15 Manage Network Area

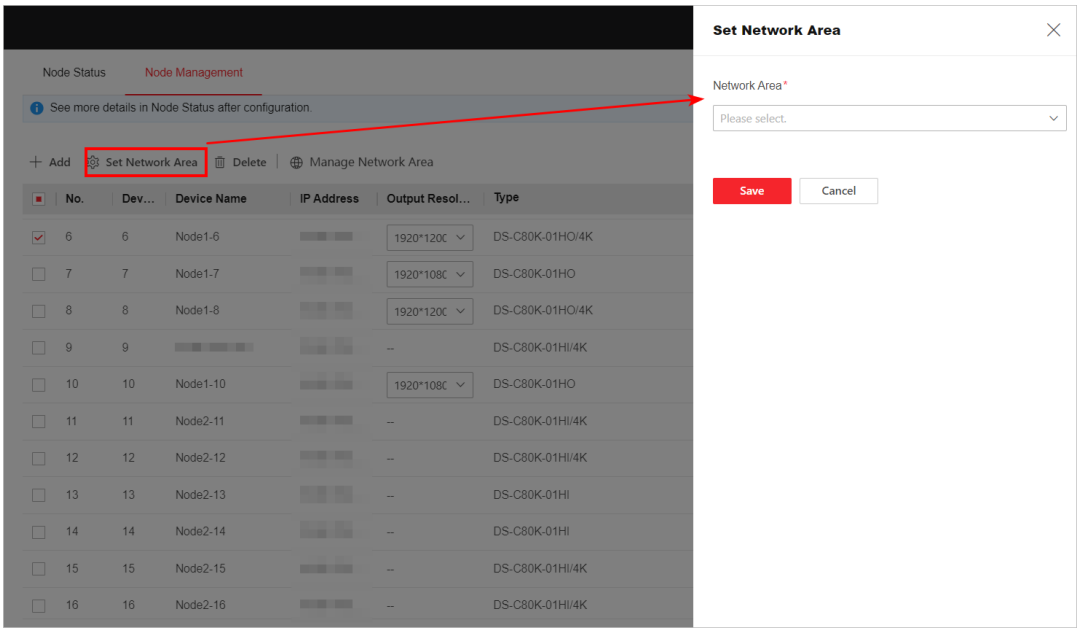

Figure 3-16 Set Network Area

Step 4 (Optional) You can configure the following operations as required:

- Delete a node: select a node and click **Delete**, or click of a node.
- Click to edit the main control node.

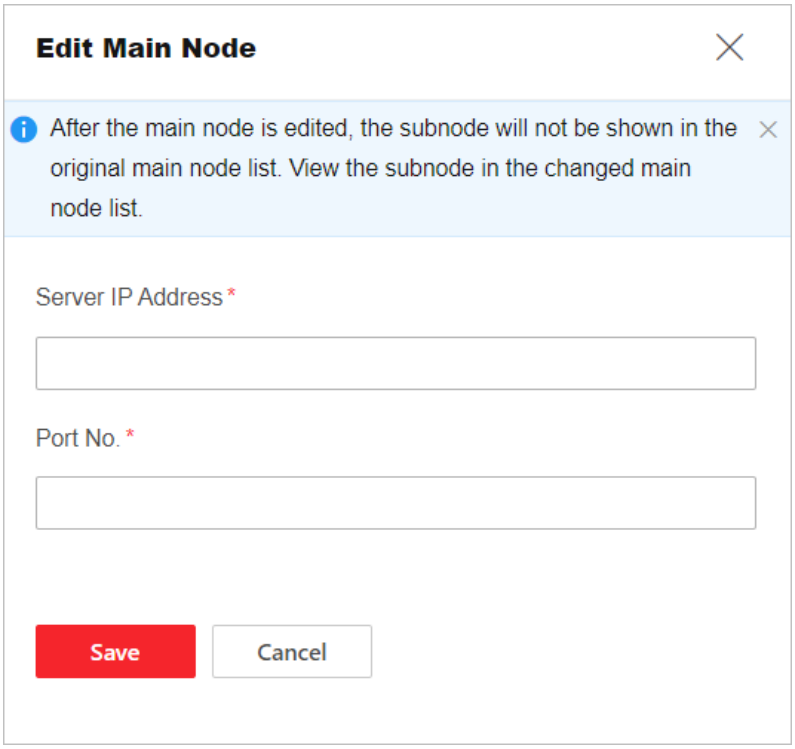

Figure 3-17 Edit Main Control Node

3.4.2 Manage Subnodes via Local Configuration Page

On the main page, click → **Node Management** to manage the nodes.

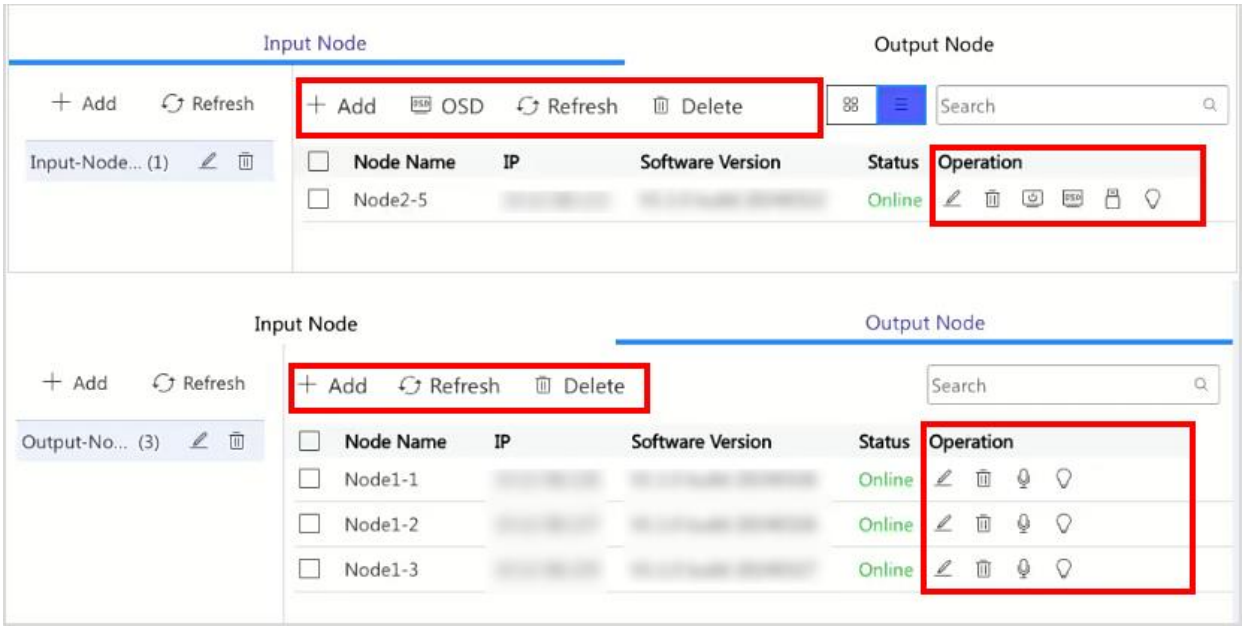

Figure 3-18 Node Management on Local Configuration Page

- Click of a node to edit the node name, network parameters, and node group.
- Click of a node, or select nodes and click **Delete**.

- Click of a node to make its front panel indicator flash. Thus, you can locate the node easily.
- Click **Refresh** to refresh the node information.
- Click of an input node to control the on/off status of the computer connected to the input node.
- Click of an input node, or select a node and then click **OSD** to enable/disable OSD. The default OSD is the node name. By default, the node name is the OSD. If you need to edit the OSD, you need to edit the node name.
- Bind a USB device:
  - To allow the import and export of the output node data: Use a USB to USB cable to connect the REMOTE port of an input node with the USB port of a computer, insert the USB flash drive into the REMOTE port of an output node, and then click . Click again to unbind the USB flash drive.
  - To provide the camera capability for a computer that does not have a camera: Use a USB to USB cable to connect the REMOTE port of an input node with the USB port of a computer, connect the USB camera to the REMOTE port of an output node, and then click . Click again to unbind the USB camera.
- Adjust the layout of input nodes:
  - Click to display input nodes by icons.

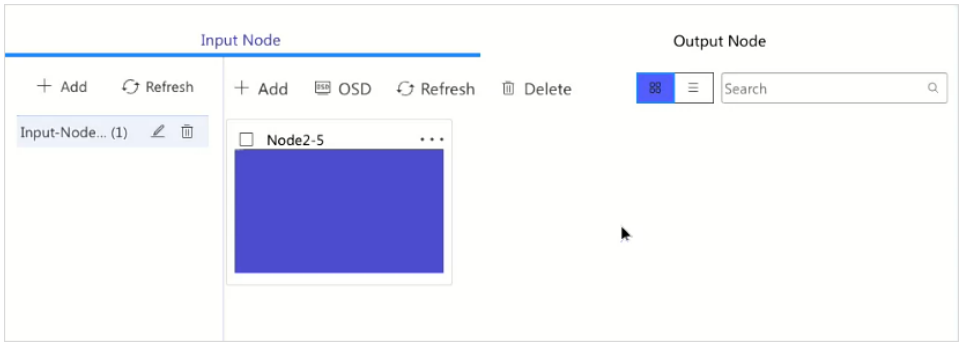

Figure 3-19 Icon Layout

  - Click to display input nodes by list.

Chapter 4 Output Node Local Configuration

4.1 Add Seats

Only the output nodes support local configuration. You can configure multiple output nodes as one seat to allow using one mouse and keyboard to control multiple input nodes.

Step 1 Log in to the local configuration page of an output node, click → **Seat Settings**, and then click **Add**.

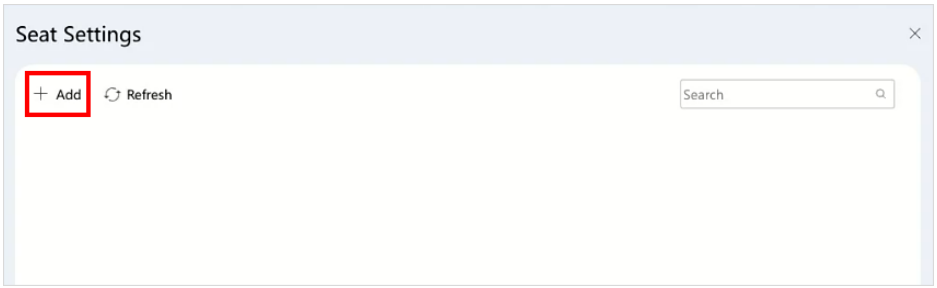

Figure 4-1 Seat Settings Page

Step 2 Enter the seat name and set the seat scale according to the number of output nodes.

Step 3 Drag the output nodes to the seat area to bind the output nodes to the seat.

Step 4 Click **Save**.

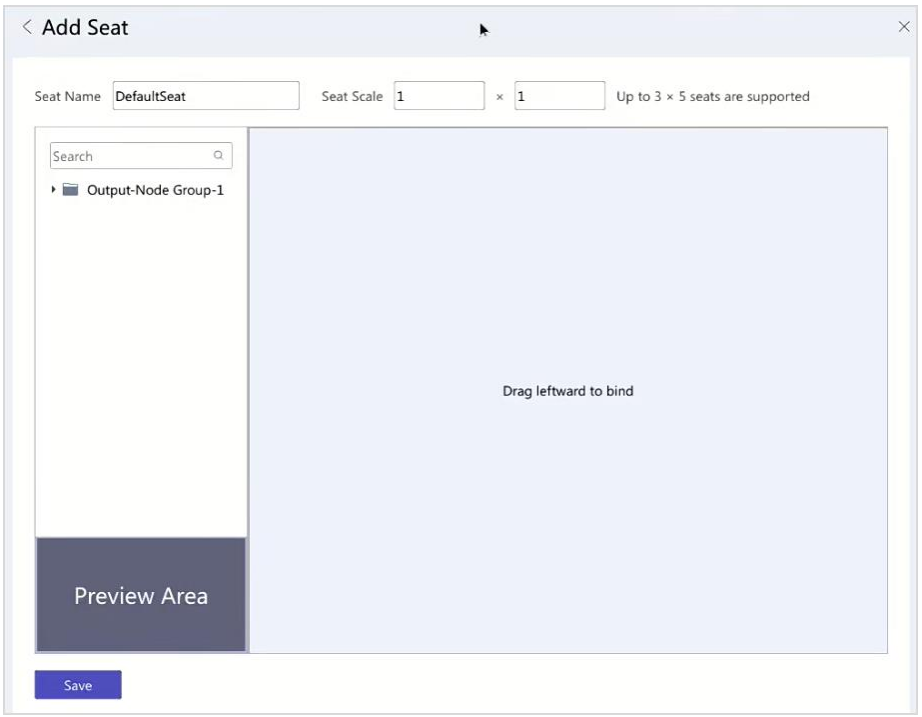

Figure 4-2 Add Seat

4.2 Add Source Expansion Groups

Step 1 On the computers connected to the input nodes, disable the mouse pointer acceleration function and set the pointer moving speed to the intermediate speed.

Step 2 Click → **Source Expansion**.

Step 3 Click **Add**.

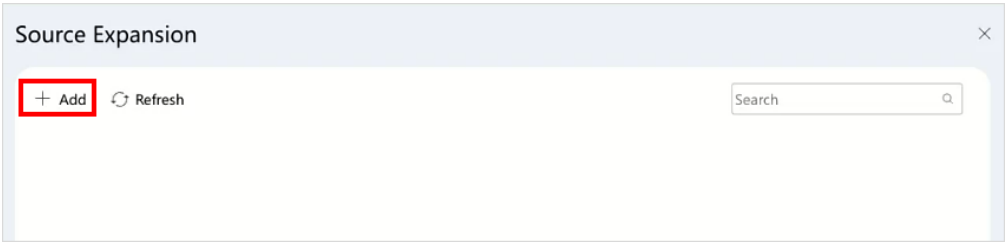

Figure 4-3 Source Expansion Settings Page

Step 4 Enter the expansion group name and set the expansion group parameters:

1) Set the expansion group scale. Up to 1 × 4 scale is allowed. Arrange the input nodes according to the actual desktop order.
2) Select a zoom rate. If the computers use Windows 10 and above version, the configured zoom rate of the expansion group and the zoom rates of the computers must be consistent.
3) Drag the input nodes to the source expansion group area to bind the input nodes to the source expansion group.

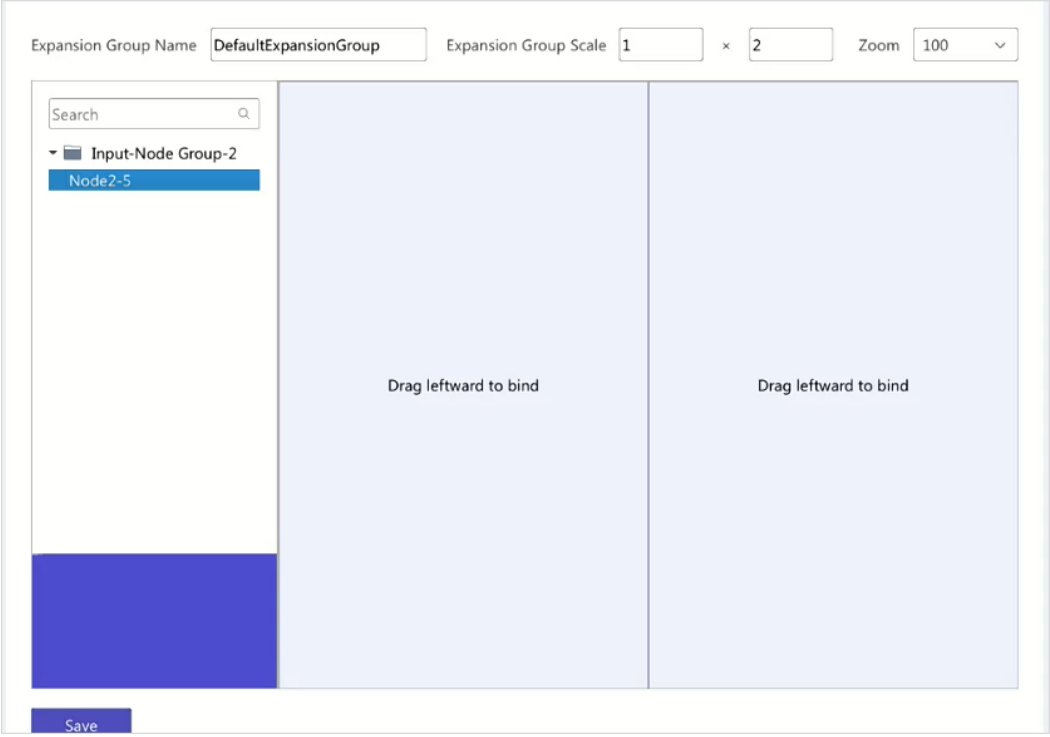

Figure 4-4 Add Source Expansion Group

Step 5 Click **Save**.

4.3 Add Users

Step 1 Click → **User Management**, and then click **Add**.

When you use the super admin account to log in to the local configuration page, you can change the password of the super admin account, the user name and password of the admin account, and the user name and password the operator.

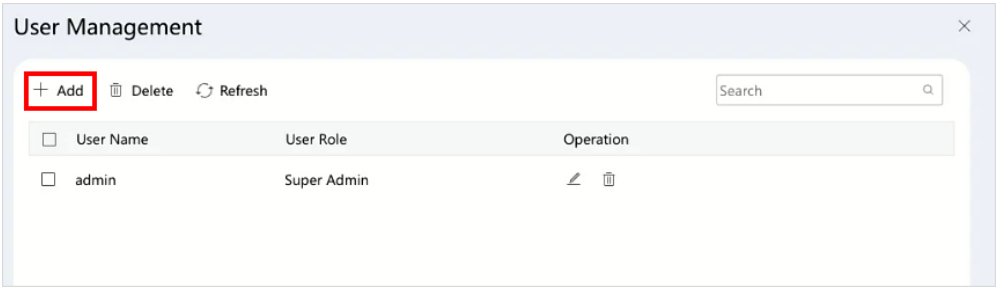

Figure 4-5 User Management Page

Step 2 Click **Add** to enter user information.

1) Select a user role.
   - If you select **Admin**, you can change the password of the current admin account and the passwords of all operators. You cannot change the password of other admin accounts.
   - If you select **Operator**, you can change the password of the current operator account. You cannot change the password of other operator accounts.
2) Enter the user name, new password and confirm password.
   - Both the user name and password support illegal character check. Up to 32 characters are allowed for the user name and up to 16 characters are allowed for the password.
   - To improve system security, it is highly recommended to change password regularly. In order to protect your privacy and corporate data and avoid network security issues, it is recommended to set a strong password that meets security requirements.
   - Password should contain at least 8 characters, including 2 or more character types (digits, lowercase letters, uppercase letters, and special characters).
   - Password cannot contain user name, 123, admin (case-insensitive), 4 or more continuously ascending or descending digits, or 4 or more consecutive repeated characters.
3) Set the permission control:
   - Select **Signal Source** to set the user permission for input nodes or source expansion groups.
   - Select **Seat** to set the user permission for output nodes or seats.

4) Enter the login password for the currently logged in user.

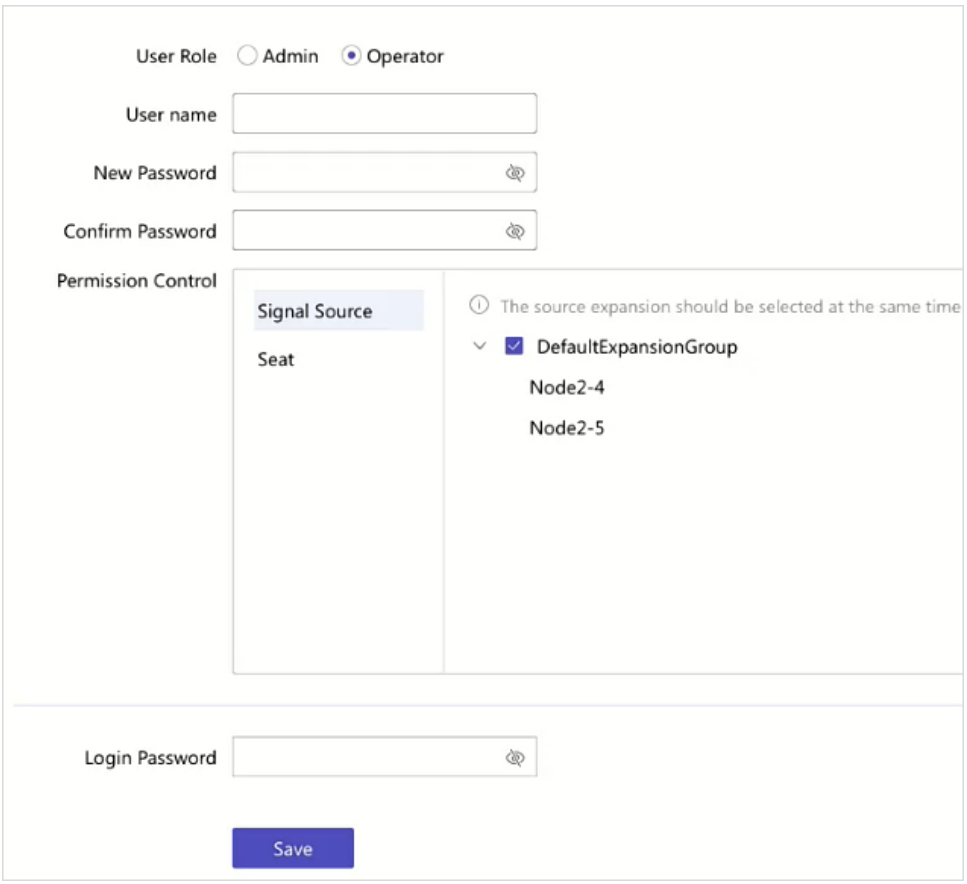

Figure 4-6 Add an Operator

Step 3 Click **Save**.

After adding a new user, you can use the new user name and password to log in the web page of any input or output node and the local configuration page of any output node.

4.4 Add Scenes

Configure the layout of input node images and save the layout as a scene. After an output node takes over the input nodes, the layout of input node images can be used quickly. The scene settings page varies by the user type. One user can add up to 8 scenes.

Step 1 Click → **Scene Settings**, and then click **Add**.

Figure 4-7 Scene Settings Page

Step 2 Enter the scene name.

Step 3 Enter the division number. You can select 1, 4, 6, or 8 as the division number or customize the scene scale. The maximum scene scale can be 2 × 4.

Step 4 Drag the input nodes to the scene area to bind the input nodes to the scene.

Step 5 Click **Save**.

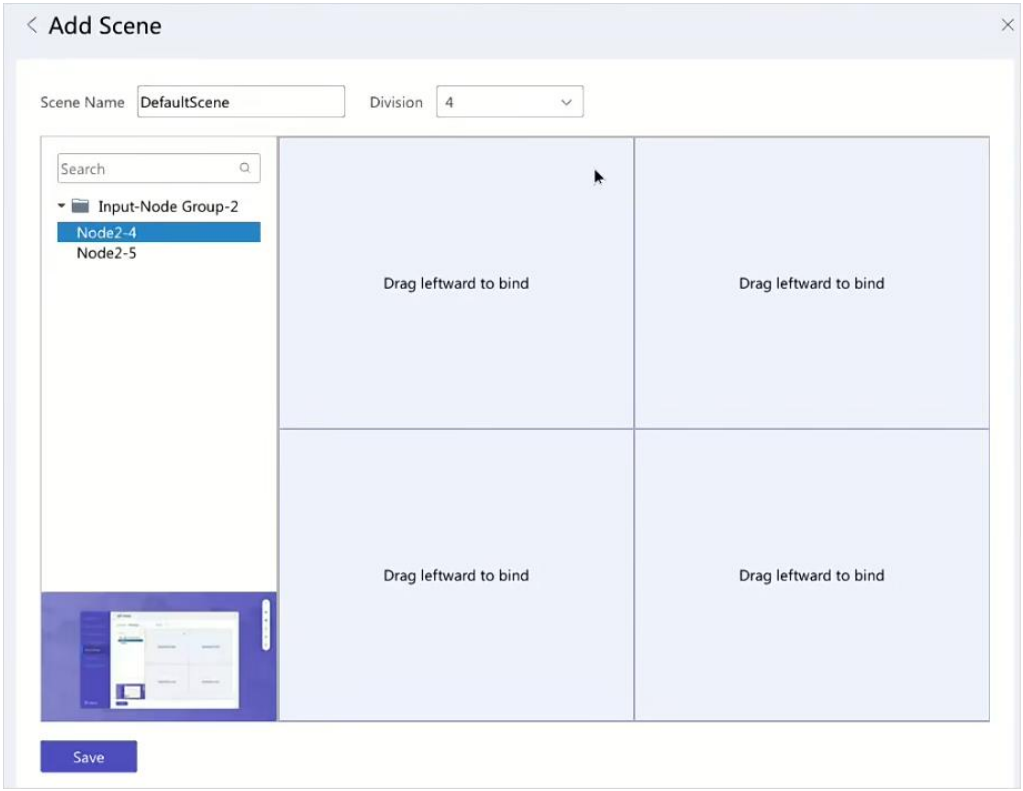

Figure 4-8 Add Scene

4.5 Configure Node Parameters

4.5.1 Manage Users

- Edit user information: Click  of a user, enter the login password of the current user, and then edit the user information.
- Delete user:
  - Click  of a user, and then enter the login password of the current user to delete the user.
  - Select the users to delete, click **Delete**, and then enter the login password of the current user to delete the selected users.
- Refresh user information: Click **Refresh**.

4.5.2 Configure Basic Parameters and Shortcut Keys

Step 1 Go to  → **Personalization**.

Step 2 Configure the basic parameters and shortcut keys:

- Set the resolution of the current login output node. The higher the resolution, the clearer the image.
- Set the seat lock time.
- Enable **Show Toolbar By Default**. If you disable the default toolbar displaying, you can use the shortcut key to display the toolbar on the main page.
- Customize the shortcut keys.

Step 3 Click **Save**. The node will restart automatically.

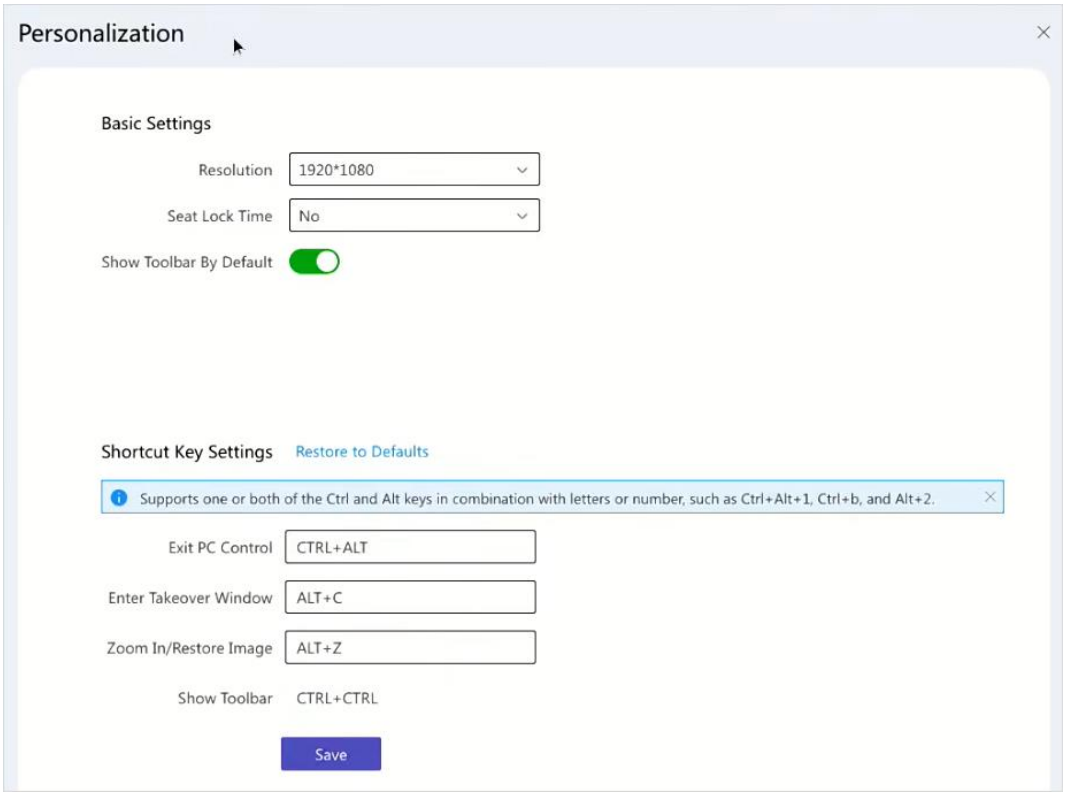

Figure 4-9 Personalization Settings Page

4.5.3 View Node Status

Go to → **Visual Maintenance** to view the health status and exception events of input and output nodes.

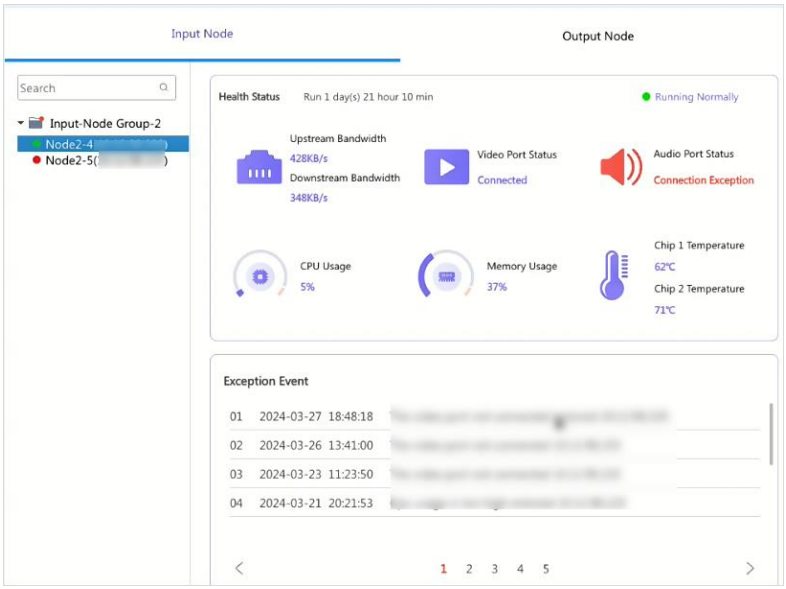

Figure 4-10 View Node Status

Chapter 5 Output Node Local Operation

5.1 Take Over Input Nodes

After an output node takes over input nodes, the output node can control the computers that are connected with the input nodes.

Click  on the main page or use the shortcut key to enter the takeover settings page. For more information about shortcut key, see 4.5.2 Configure Basic Parameters and Shortcut Keys.

- Select an input node group and then select a single input node to be taken over.

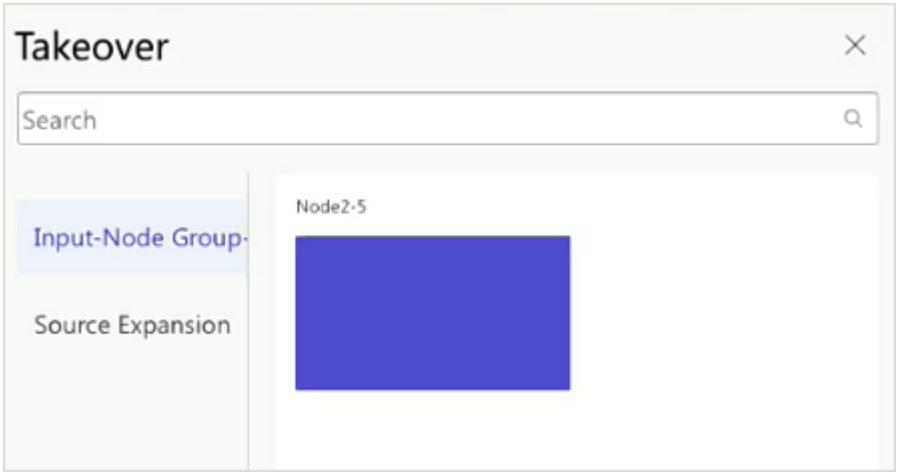

Figure 5-1 Take Over a Single Input Node

- Select a source expansion group and then select one or multiple input nodes to be taken over.

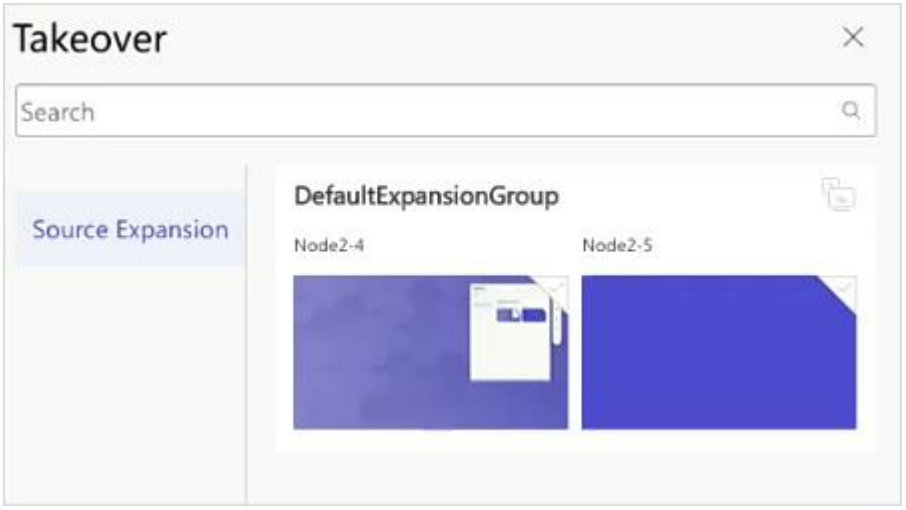

Figure 5-2 Take Over Multiple Input Nodes

5.2 Push Image

If an output node that sends the image pushing request manages only one input image, you can push the input image to another output node. If an output node that sends the image pushing request manages multiple input images, you can push only the first valid input image to another output node.

Step 1 On the main page, click  .

Step 2 Select an output node to be pushed and select a pushing method:

- Click  to push the control permission and image of the input node controlled by the selected output node to another output node. The output node that receives and accepts the image pushing request can remotely control the computer connected with the input node.
- Click  to push the image of the input node controlled by the selected output node to another output node. The output node that receives and accepts the image pushing request can view the image of the computer connected with the input node.

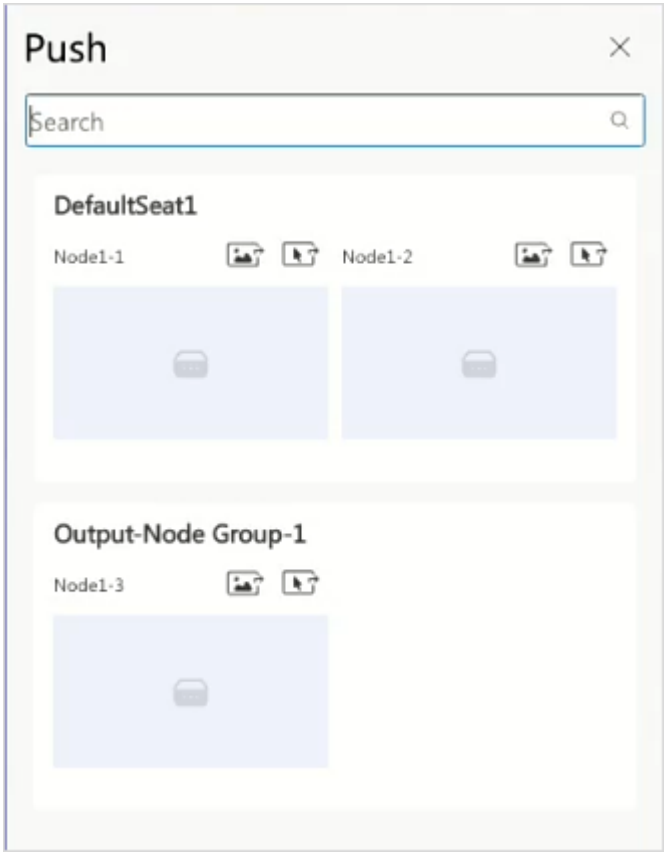

Figure 5-3 Image Push Settings Page

Step 3 The output node that receives the image pushing request accepts the request.

Step 4 (Optional) The output node that sends the image pushing request can cancel pushing as required.

5.3 Initiate Two-Way Audio

5.3.1 Initiate Two-Way Audio Between Output Nodes

Step 1 Make sure the two output nodes are in the same network segment.

Step 2 For each output node, connect an active microphone to the LINE IN port of the output node, and connect an audio output equipment such as an audio speaker to the LINE OUT port of the output node.

Step 3 On the main page, click → **Node Management.**

Step 4 Click **Output Node.**

Step 5 Select an output node and click to initiate the two-way audio request between the logged-in output node and the selected output node.

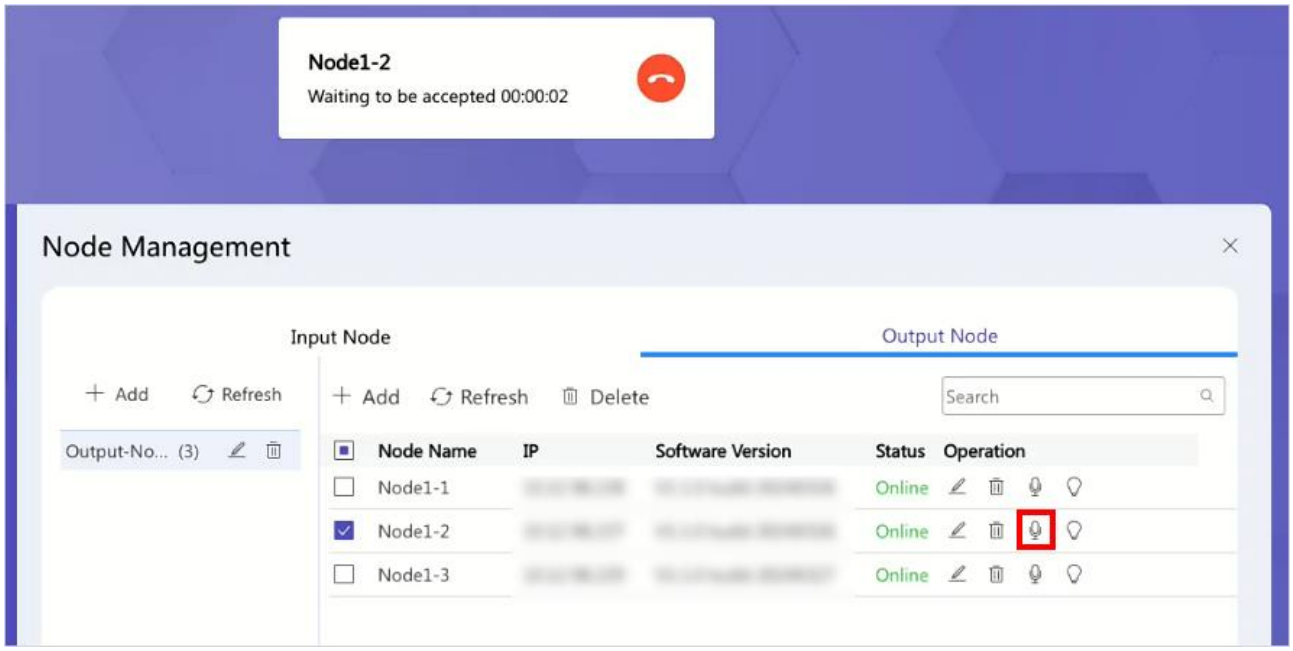

Figure 5-4 Initiate Two-Way Audio

Step 6 The other output node accepts the request.

5.3.2 Initiate Two-Way Audio Between Input and Output Nodes

To perform two-way audio between an input node and an output node:

- Connect an active microphone to the LINE IN port of the output node, and connect an audio output equipment such as an audio speaker to the LINE OUT port of the output node.

- Connect the LINE IN port of the input node to the audio output port of the computer, and connect the LINE OUT port of the input node to the audio input port of the computer.

5.4 Switch Scene

On the main page, click  and then click  to switch scene.

Figure 5-5 Switch Scene

5.5 Exit Remote PC

To exit remote PC:

- Click  .
- Use the shortcut key to exit remote PC. For more information about shortcut key, see 4.5.2 Configure Basic Parameters and Shortcut Keys.
- When you can view the image of a computer on the display, click an area except the toolbar.

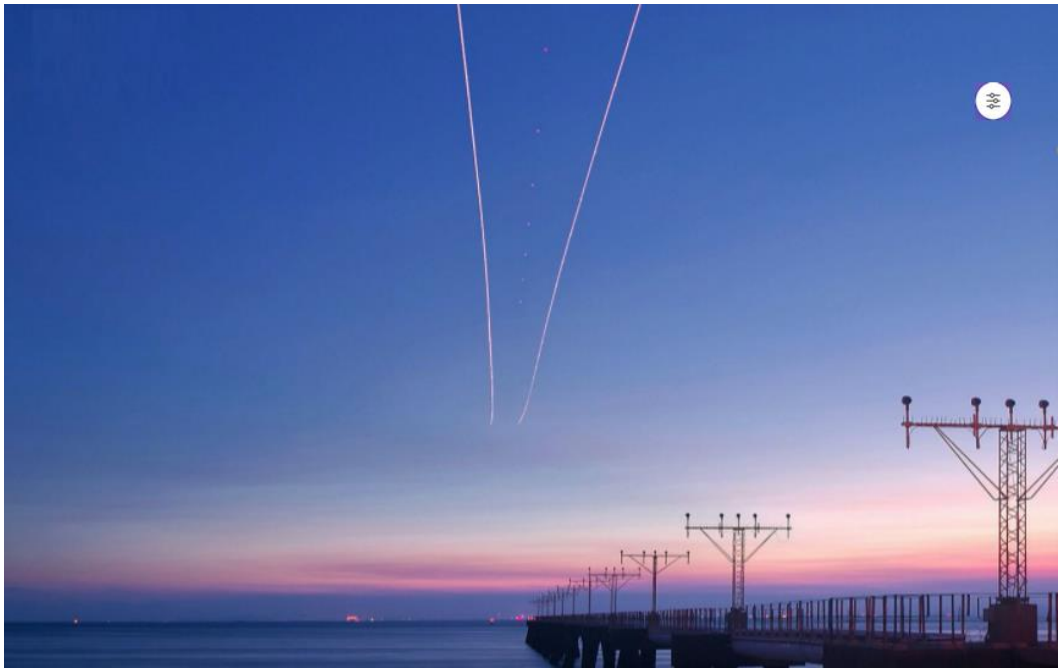

Figure 5-6 Computer Image on the Display

Chapter 6 Web Configuration of Main Control Node

6.1 Configure System Parameters

Go to **Configuration** → **System** to configure the following parameters:

- Go to **System Settings** → **Basic Information** to view the device information and edit the device name as required. You can click **Upgrade** to go to the upgrade page.

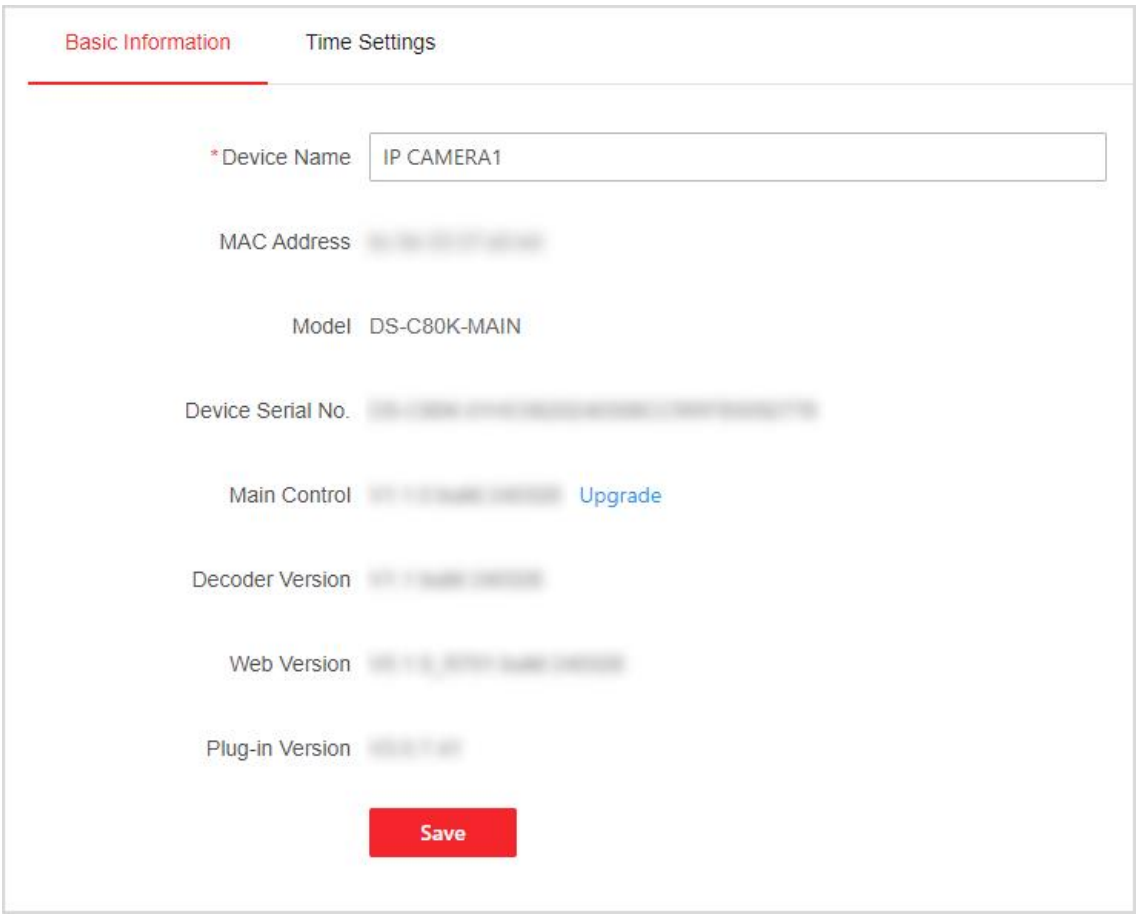

Figure 6-1 View Basic Information

- Go to **System Settings** → **Time Settings**, if you select **NTP Sync**, the device time synchronizes with the time of the NTP server at the specified interval.
  - Set the address and port number of the NTP server.
  - Set the synchronization interval.

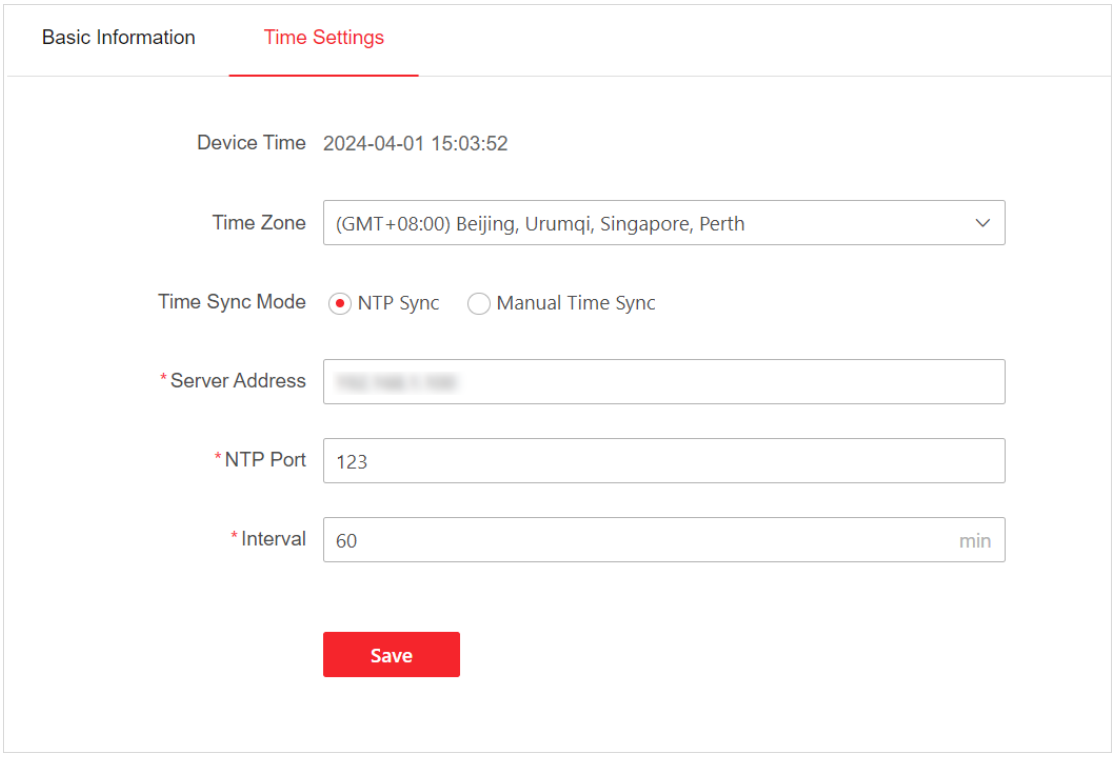

Figure 6-2 Select NTP Sync

- On the **Time Settings** page, if you select **Manual Time Sync**, you can click **Sync with Computer** to make the device time same as the computer time.

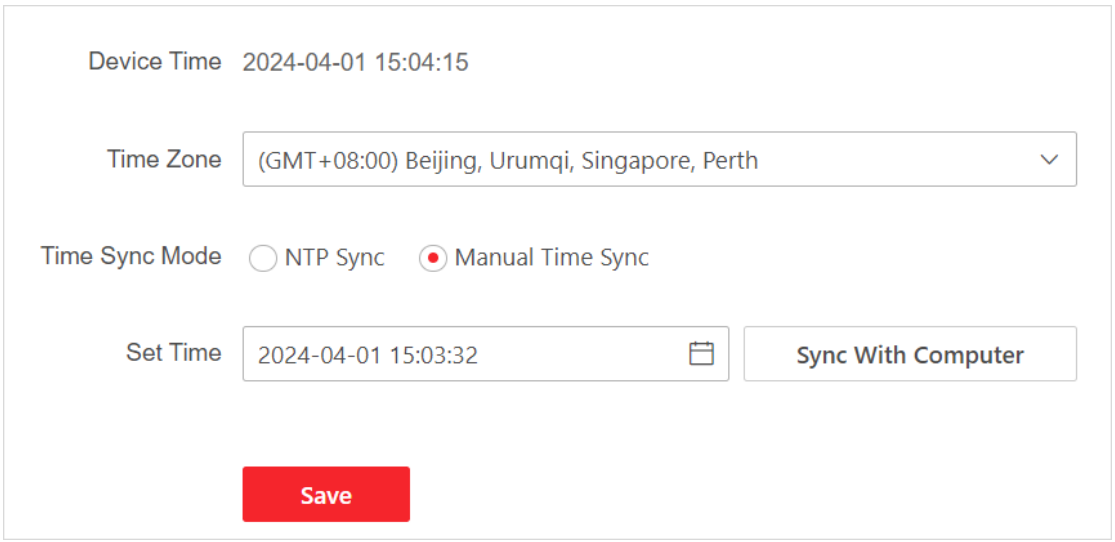

Figure 6-3 Select Manual Time Sync

- Go to **Configuration** → **System** → **User Management**, and click to edit the password of the admin user.

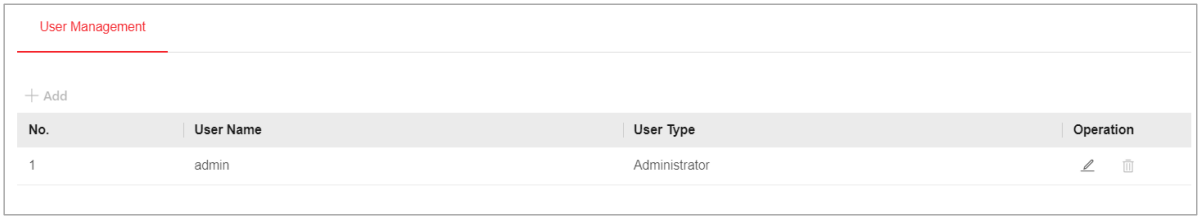

Figure 6-4 Manage Users

6.2 Configure Network Parameters

Go to **Configuration** → **Network** to configure TCP/IP and HTTP(S) parameters.

6.2.1 Configure TCP/IP

Step 1 Go to **Network Configuration** → **TCP/IP**.

Step 2 Set IPv4 address, IPv4 subnet mask and IPv4 default gateway.

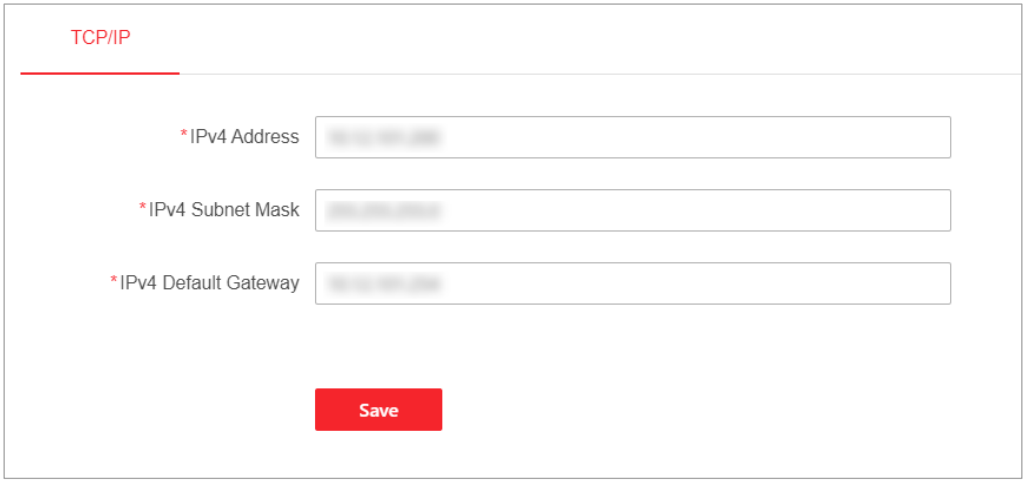

Figure 6-5 Configure Network Parameters

Note

Disable the STP protocol of the switch that is connected with the main control node to avoid function exception.

Step 3 Click **Save**.

6.2.2 Configure HTTP(S)

Step 1 Go to **Network Service** → **HTTP(S)**.

Step 2 Set the HTTP port number.

The port number can be either 80 or any value from 2000 to 65535. After editing the HTTP port, you need to enter HTTP://Device IP Address: Port in the browser to access the device.

Step 3 Enable HTTPS.

- HTTPS security is higher, and HTTPS private certificate is supported. See for details in 6.5 Maintain the Security of Main Control Node. Enabling HTTPS will increase the loading time of the interface and consume more hardware resources.
- After you change the HTTPS configuration of the input node, the input node will restart automatically.

Step 4 Set the HTTPS port.

The default port number is 443. After editing the HTTPS port No., you need to enter HTTPS://Device IP Address: Port in the browser to access the device.

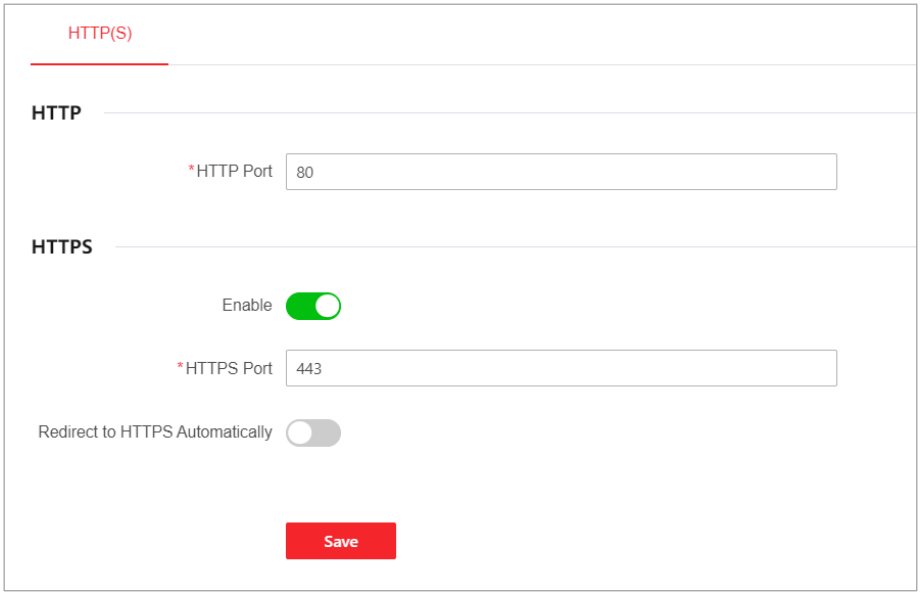

Figure 6-6 Configure HTTP(S) Parameters

Step 5 (Optional) Enable redirect to HTTPS automatically. Thus, the device access via HTTPS is used by default.

Step 6 Click **Save**.

6.3 Configure Signal Source Parameters

6.3.1 Customize Resolution

If the resolution of a signal source does not match the resolution of the display, you can customize the resolution of the signal source.

Step 1 Go to **Configuration** → **Signal Source Settings** → **Image Settings**.

Step 2 Select a signal source.

Step 3 Enable custom resolution and set the refresh rate and resolution.

- The width should be a multiple of 4 and the height should be a multiple of 2.

- For a UHD signal source, the resolution should be between 1920 × 1080 and 4092 × 2160, and the refresh rate can be 30 or 60.
- For a normal signal source, the resolution should be between 1280 × 720 and 1920 × 1200, and the refresh rate can be 30 or 60.

Step 4 (Optional) Click **Copy To** to copy the current signal source configuration to other signal sources.

Step 5 Click **Save**.

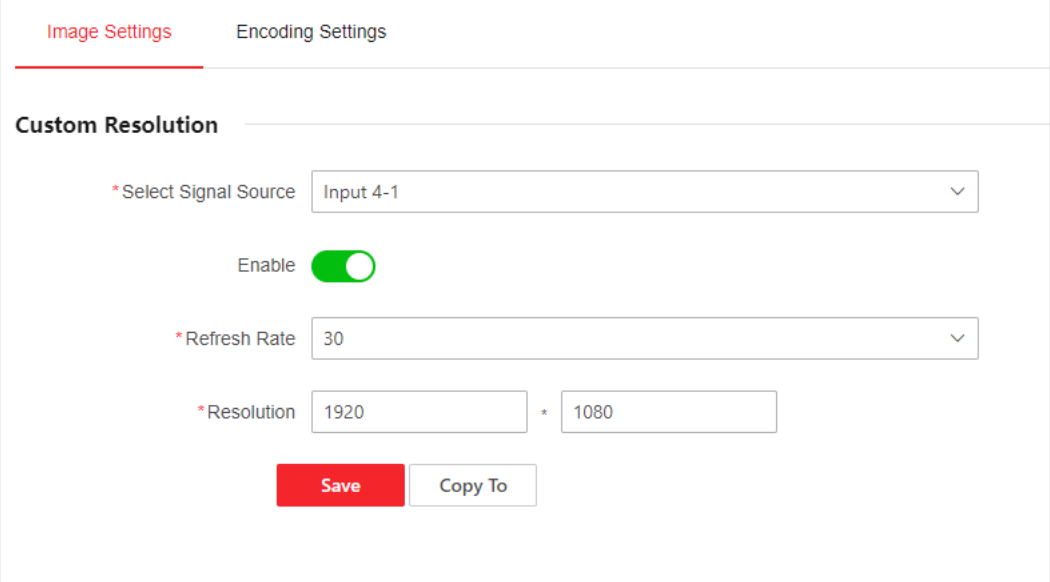

Figure 6-7 Customize Resolution

6.3.2 Set Encoding Parameters

Step 1 Go to **Configuration** → **Signal Source Settings** → **Encoding Settings**.

Step 2 Select a signal source.

Step 3 Set the video encoding parameters.

- Select a stream type.
- Set the bit rate type and maximum bit rate.
  - If you select **Constant Bit Rate**, the device uses the average bit rate for transmission and uses fast compression speed. The video mosaic might occur.
  - If you select **Variable Bit Rate**, the device automatically adjusts the bit rate for transmission as long as the bit rate is within the limit and uses slow compression speed to ensure the image definition in complex scenarios.
- If you select **Variable Bit Rate**, you should select a video quality. The higher video quality, the higher the bandwidth requirements.
- Set an I-frame interval: the number of frames between the two key frames. The larger the I-frame interval, the smaller the stream fluctuation, and the lower the image quality.

- Select a resolution. The higher resolution, the higher the bandwidth requirements.
- Select a frame rate: the number of frames per second. The higher frame rate, the higher the bandwidth requirements.
- Select a video encoding type, H.264 or H.265.
- Select a video type.
- Set shallow/deep compression rate: Set the compression rate according to the actual need. Keep the default value.
  - Shallow compression: Low video compression, high resolution, and high bandwidth requirements.
  - Deep compression: High video compression, average resolution, and low bandwidth requirements.

Step 4 Select an audio encoding type, G722.1, G711ulaw, G711alaw or AAC.

Step 5 Click **Save**.

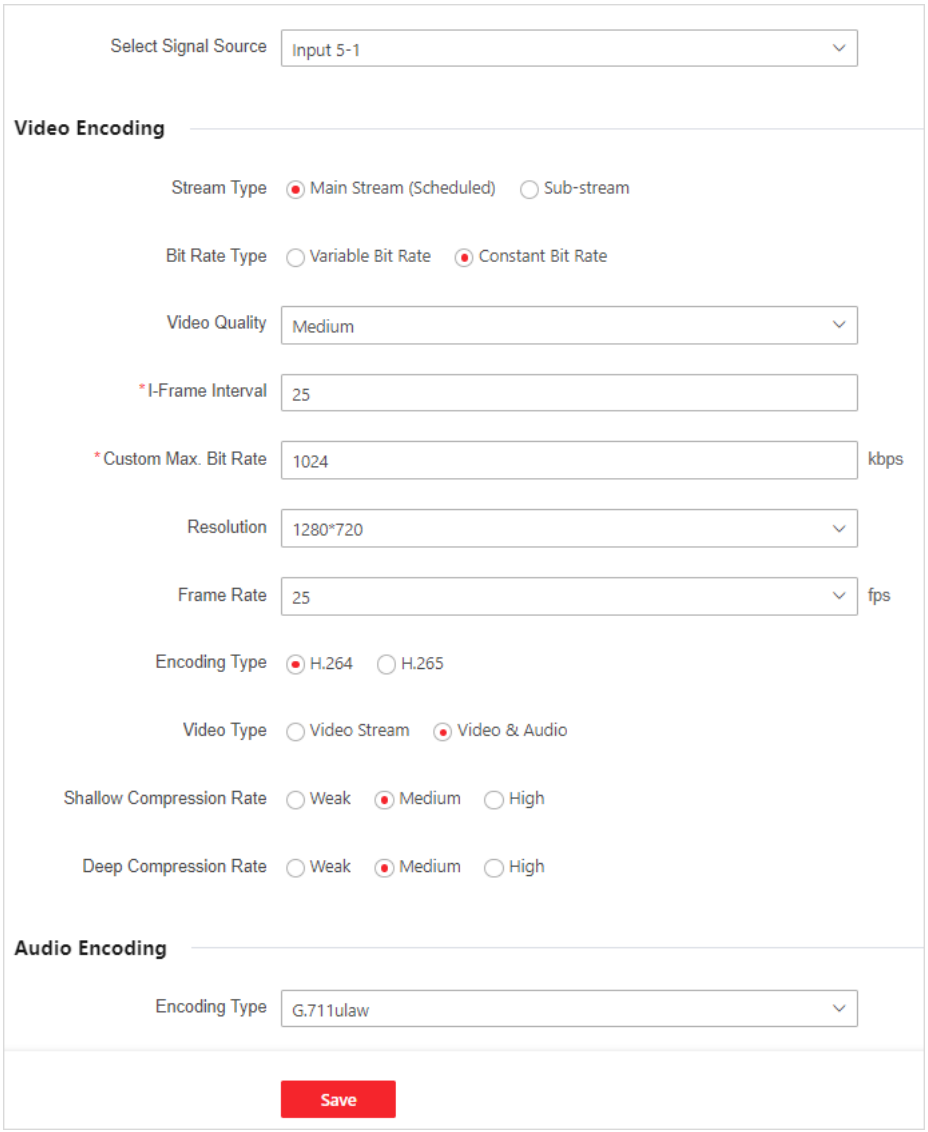

Figure 6-8 Set Signal Source Encoding Parameters

6.3.3 Set Other Parameters

Go to **Configuration** → **Other Settings** to set the following parameters:

- Click **Streaming Mode**, and then select **Unicast** or **Broadcast**. After setting unicast or broadcast, the device will restart.

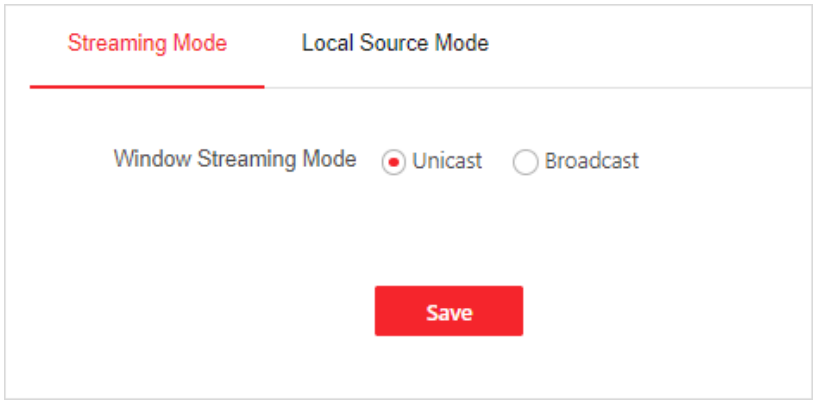

Figure 6-9 Select Streaming Mode

- Click **Local Source Mode** to set the compression mode. In high-quality mode, the video image has high definition, but it will occupy more bandwidth.

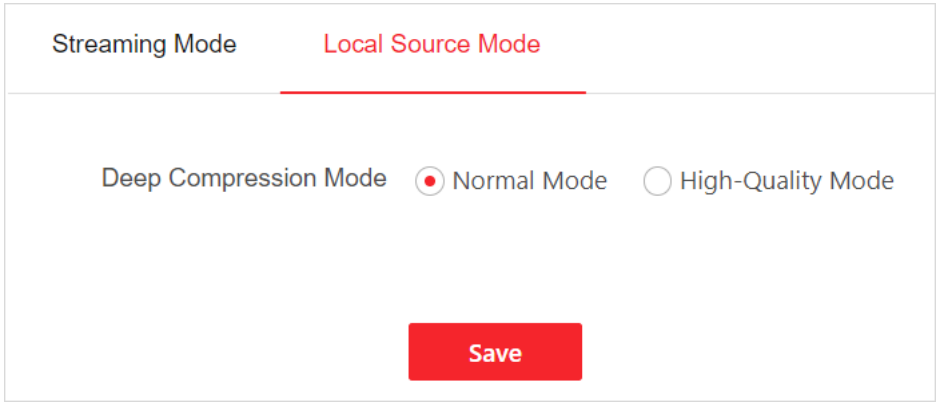

Figure 6-10 Set Local Source Mode

6.4 Maintain the System

Go to **Maintenance and Security** → **System Maintenance** to configure the following parameters:

- Click **Restart** to restart the device.
- Click to select an upgrade file, and click **Upgrade**.

  You need to get the upgrade file in advance and save it locally.

  Upgrading the main control node will upgrade the nodes controlled by the main control node simultaneously. To upgrade a single input node or output node, log in to the node and upgrade it. To upgrade multiple input nodes or output nodes, you can use the HiTools Delivery client to upgrade those nodes.

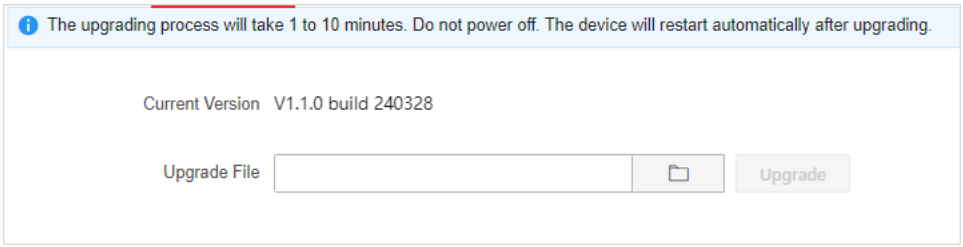

Figure 6-11 Upgrade the Main Control Node

- Export the parameters of the main control node. To export the parameters of a single input node, log in to the node and export its parameters.

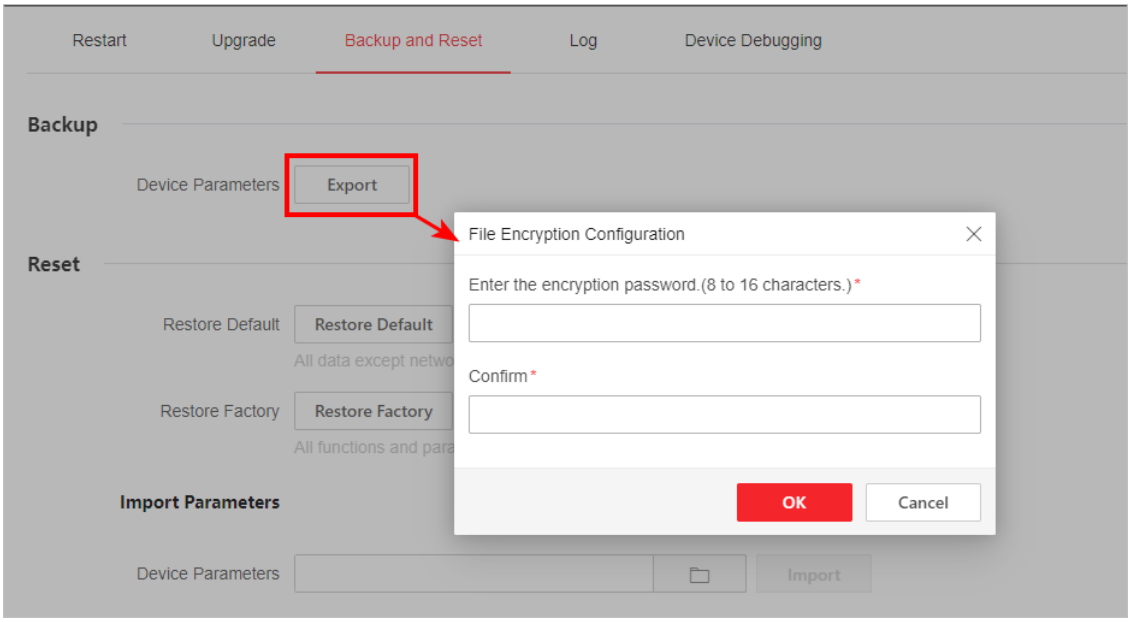

Figure 6-12 Export Parameters of Main Control Node

- Reset the main control node. To reset a single input node, log in to the node and reset it.
  - Click **Restore Default** to restore the parameters except for user information and network parameters to the default settings. Please use this function with caution.
  - Click **Restore Factory** to restore all functions and parameters of the main control node to the factory settings. Please use this function with caution.
  - Click to select a parameter file saved locally, and click **Import** to import device parameters.

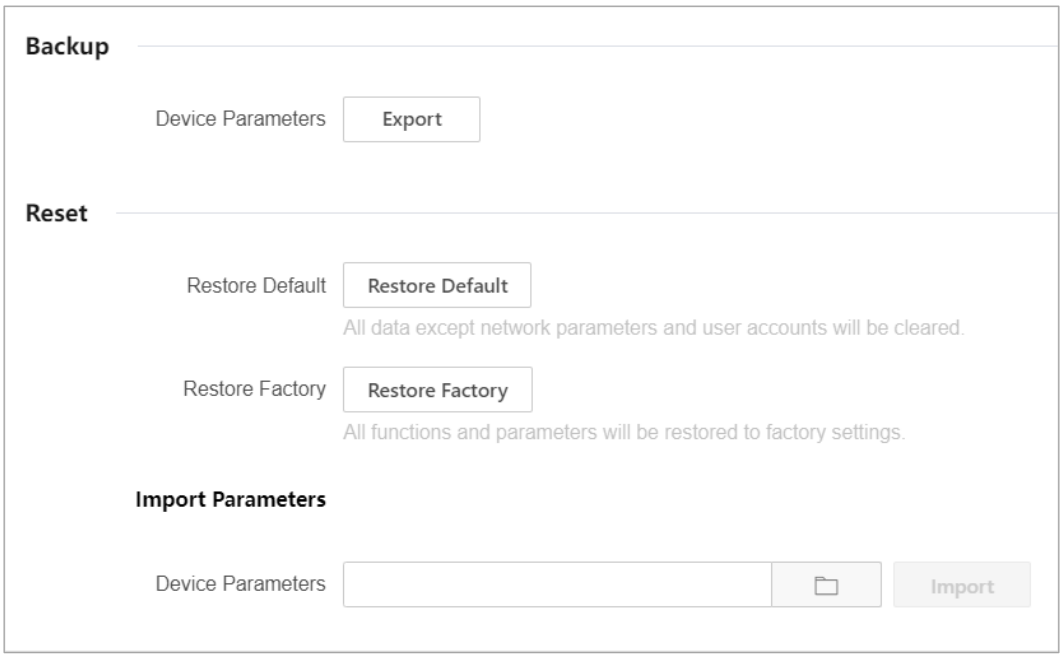

Figure 6-13 Reset Main Control Node

- Search logs: Click **Log** to set the search condition and click **Search**. You can view the searched logs of the main control node and controlled nodes in the list below. To view the logs of a single input node, log in to the node and view its logs.

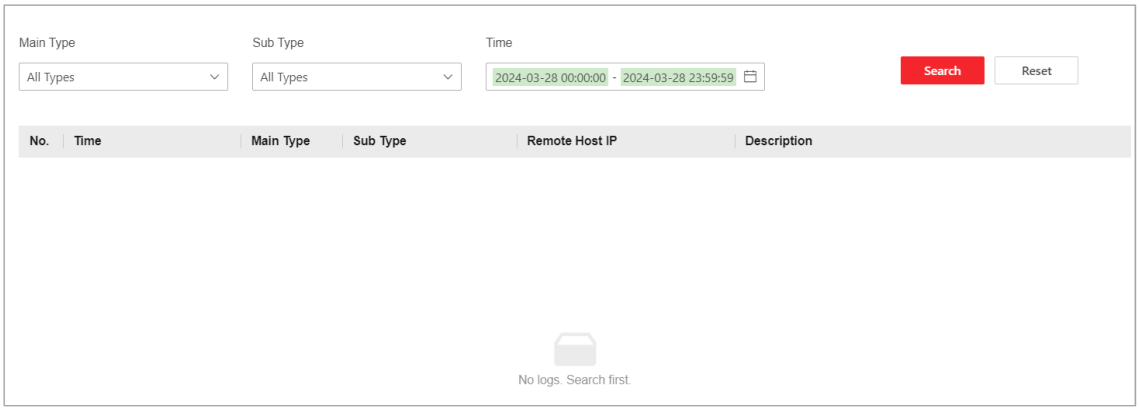

Figure 6-14 Search Logs

Debug Main Control Node

Click **Device Debugging** to configure the following parameters:

- Enable SSH (Secure Shell) as required. With SSH enabled, you can use a computer installed with the SSH client to access the device.
- Format the FAT32 USB flash drive before inserting it into the node, and then export logs to the USB flash drive:
  - To export the logs of the main control node, insert a USB flash drive into the main control node, and click **Start Exporting**.

- To export the logs of an output node, insert a USB flash drive into the output node, and click **Start Exporting**.
- To export the logs of an input node, insert a USB flash drive into the input node, and click **Start Exporting**.

- Select a sub-system, click **Start Capturing** and then you can download the obtained packet capture file of the main control node. To download the packet capture file of a single input node or output node, log in to the node to download the obtained packet capture file of the node.

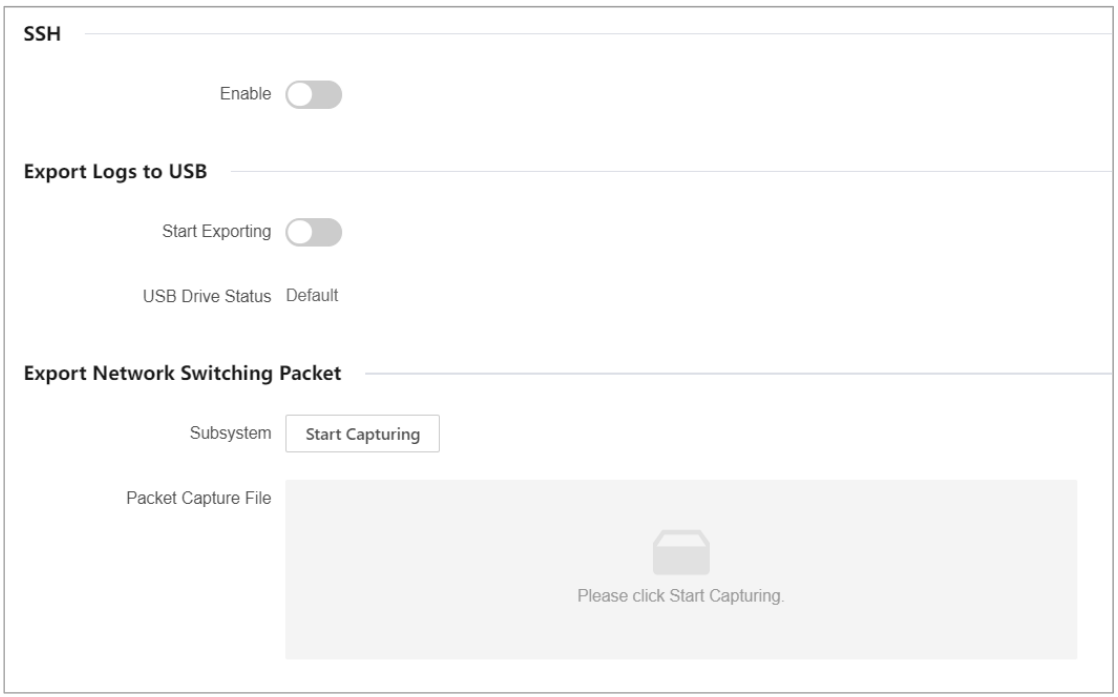

Figure 6-15 Debug the Device

6.5 Maintain the Security of Main Control Node

Go to **Maintenance and Security** → **Security Management** to configure the following parameters:

- Configure the IP addresses that are allowed to or forbidden to access the device.

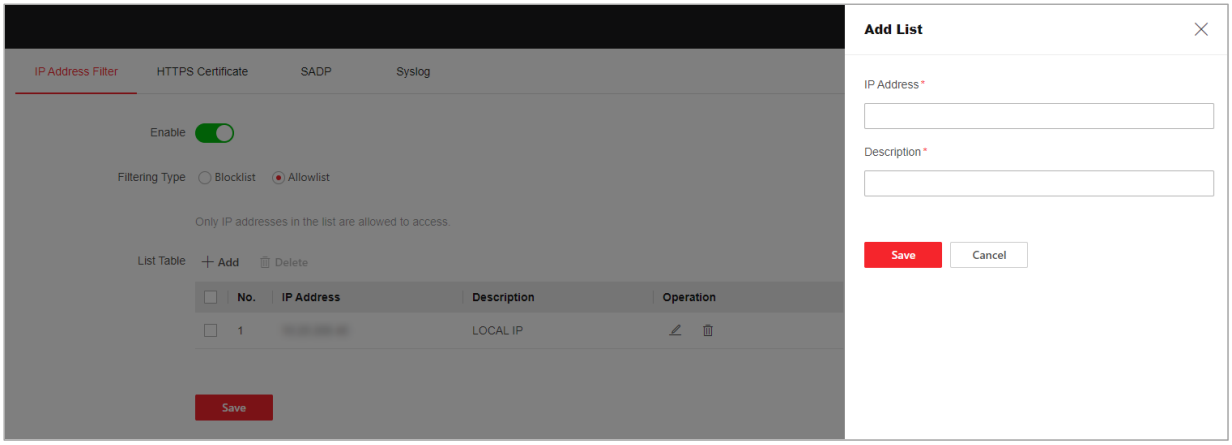

Figure 6-16 Configure IP Address Filter

- Click **HTTPS Certificate**, and then import the locally saved HTTPS certificate and secret key.

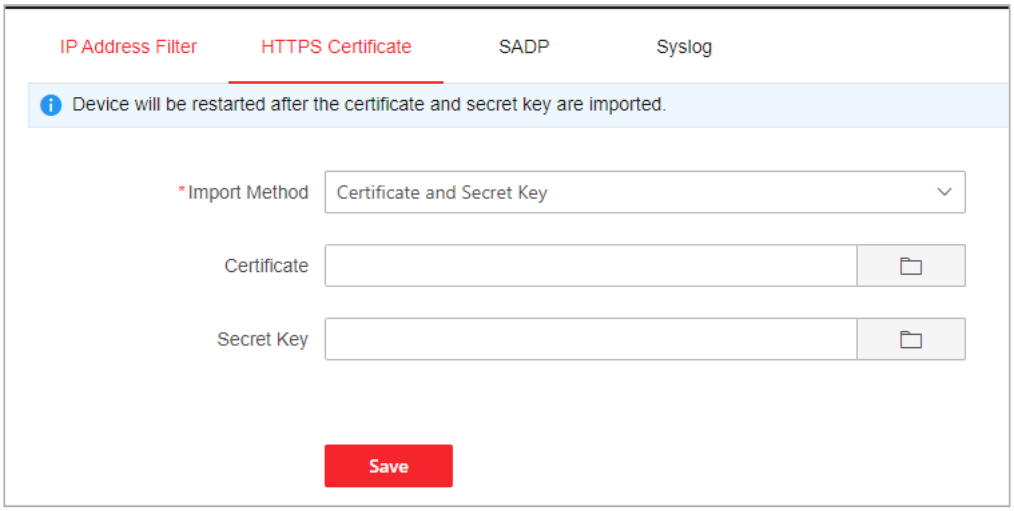

Figure 6-17 Import HTTPS Certificate and Secret Key

- Enable SADP as required. With SADP enabled, you can use the SADP client to search for the node when it is in the same network segment with the computer.
- Enable Syslog as required. With Syslog enabled, the node logs can be uploaded to the Syslog server.

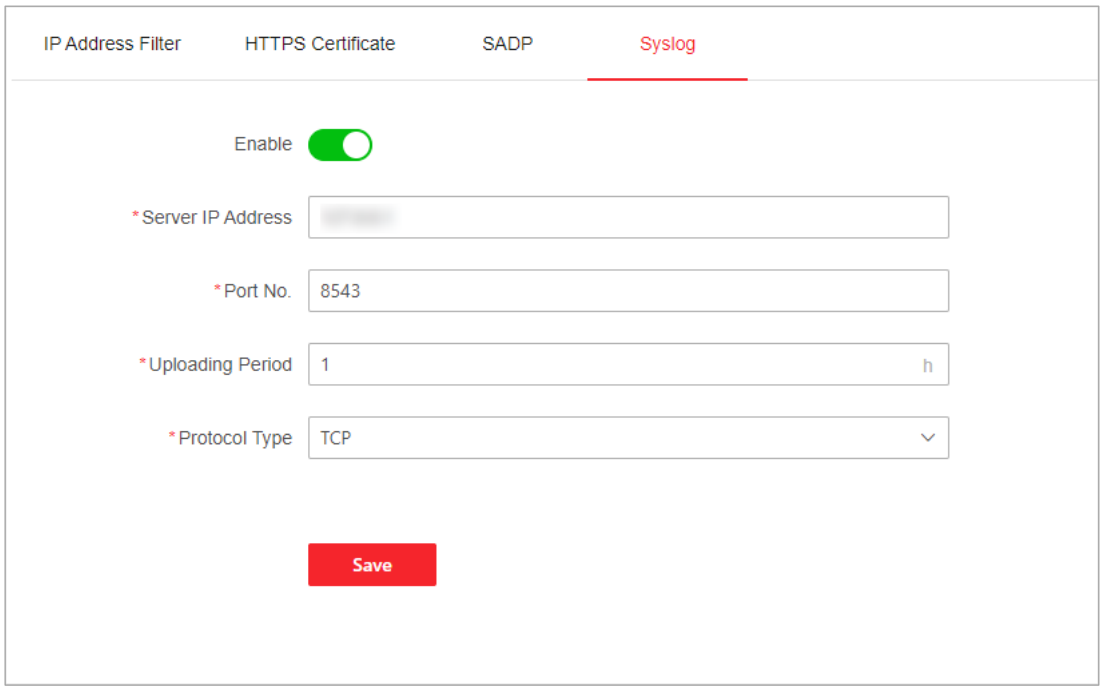

Figure 6-18 Enable Syslog

UD38487B