



Radar-Assisted Speed LED Display

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.
- If the product you choose is a video product, please scan the following QR code to obtain the "Initiatives on the Use of Video Products", and read it carefully.



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.

© Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

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.

Contents

Chapter 1 Activation and Login	1
1.1 Activation.....	1
1.1.1 Default Information	1
1.1.2 Activate via HiTools Delivery	1
1.1.3 Activate via Web Browser.....	3
1.2 Login.....	3
Chapter 2 Network Configuration	5
2.1 Set IP Address	5
2.2 Connect to Mobile Network	7
2.3 Set Port	8
2.4 Set Wi-Fi Hotspot.....	10
2.5 Data Connection	11
2.5.1 Set Email	11
2.5.2 Set ISAPI Listening	12
2.5.3 Connect to ISUP Platform	13
Chapter 3 Display Configuration	15
Chapter 4 Email Event	19
Chapter 5 Extended Interface	20
Chapter 6 Radar Detection	21
6.1 Set Detection Parameters	21
6.2 Search Detected Vehicles.....	23
Chapter 7 Traffic Flow Statistics.....	24
Chapter 8 Safety Management	25
8.1 Manage User.....	25
8.2 Set SSH	26
8.3 Prohibit PING	26
8.4 Set Timeout Logout	26
8.5 Set Password Validity Period	26
8.6 Set IP Address Filtering	27

8.7 Set HTTPS	27
8.7.1 Create and Install Self-signed Certificate	27
8.7.2 Install Authorized Certificate	28
Chapter 9 Maintenance	29
9.1 View Device Information	29
9.2 Synchronize Time	29
9.3 Set DST	30
9.4 Set RS-232	30
9.5 Reboot.....	31
9.6 Restore Parameters.....	31
9.7 Export Parameters.....	31
9.8 Export Debug File	32
9.9 Export Diagnosis Information	32
9.10 Upgrade	32
9.11 Import Configuration File.....	33
Port Information	34

Chapter 1 Activation and Login

1.1 Activation

For the first-time access, you need to activate the device by setting an admin password. No operation is allowed before activation. The device supports multiple activation methods, such as activation via HiTools Delivery and web browser.

1.1.1 Default Information

The device default information is shown as below.

- Default IP address: 192.168.1.64
- Default user name: admin

1.1.2 Activate via HiTools Delivery

HiTools Delivery aims to streamline and enhance the activation, networking, and batch configuration for various devices. You can use the software to detect, activate, and modify the IP addresses of multiple devices over the LAN.

Before You Start

- Set the device and the computer that runs the software to the same network segment.
- Access the official website (<https://www.hikvision.com/en>) and enter **Support** → **Download** → **Software** → **HiTools** → **HiTools Delivery** to download HiTools Delivery and install it according to the prompts.

Steps

1. Run the software.
2. Click **Home Page** → **Search** → **Current Subnet**. Click **Refresh**, and the list will display all the online devices in the same network segment.
3. Select the inactive device(s) in the list. Set a new password according to the popup requirements and confirm the password.
4. Click **Activation**. The device activation status will change to **Activated** after successful activation.

Radar-Assisted Speed LED Display User Manual

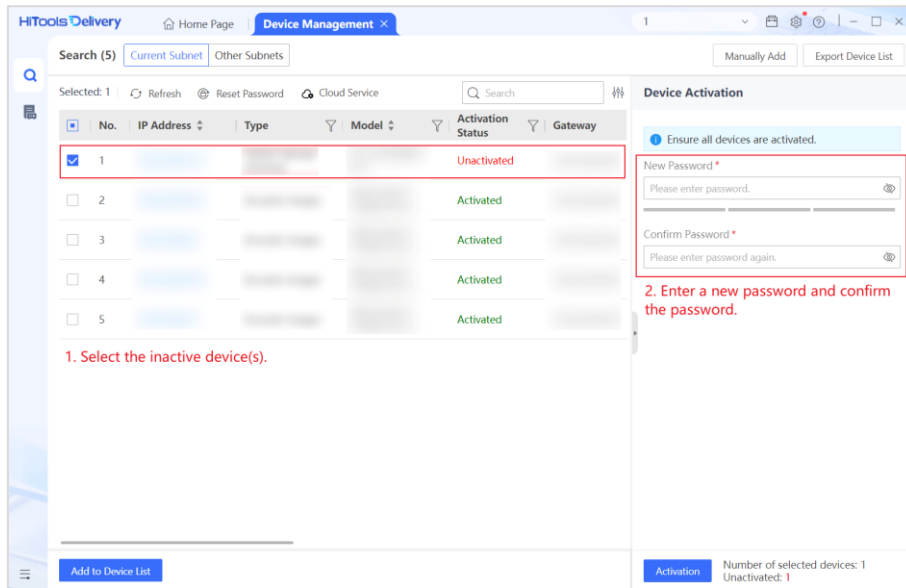


Figure 1-1 Activation

5. Optional: Change the IP address of the device.
 - 1) On **Current Subnet** interface, select multiple devices that need to change the IP addresses.
 - 2) On the right **Network Parameter** window, set the start IP address, port No., IPv4 subnet mask, IPv4 gateway, etc., and the selected devices will be automatically assigned to increasing IP addresses. Or check **Enable DHCP** to assign dynamic IP addresses.
 - 3) Enter the admin password and click **OK**.

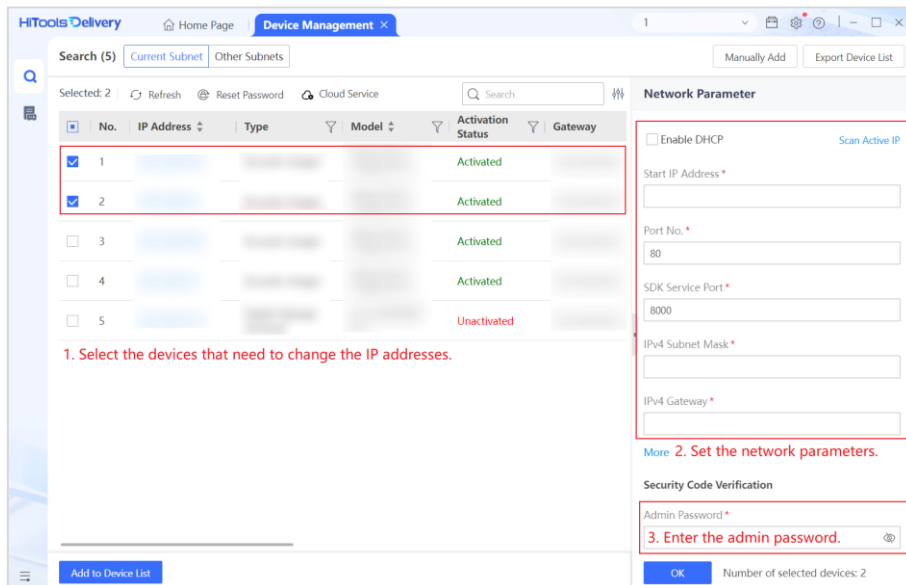


Figure 1-2 Modify Network Parameters

Note

- Set the device IP address to the same network segment with that of your computer.
- You can click **Scan Active IP** to detect and view the available IP addresses. Refer to the help of

HiTools Delivery for details.

- You can also click **Home Page** → **Maintenance** → **Change IP** to change the IP addresses in batch by exporting and importing the template. Refer to the help of HiTools Delivery for details.
-

1.1.3 Activate via Web Browser

Use web browser to activate the device. For the device with the DHCP enabled by default, use SADP software or client software to activate the device.

Before You Start

Ensure the device and the computer are in the LAN with the same network segment.

Steps

1. Change the IP address of your computer to the same network segment as the device.
 2. Open the web browser, and enter the default IP address of the device to enter the activation interface.
 3. Create and confirm the admin password.
-



Caution

STRONG PASSWORD RECOMMENDED-We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

4. Click **OK** to complete activation.
5. Go to the network settings interface to modify IP address of the device.

1.2 Login

You can log in to the device via web browser for further operations such as live view and local configuration.

Before You Start

Connect the device to the network directly, or via a switch or a router.

Steps

1. Open the web browser, and enter the IP address of the device to enter the login interface.
 2. Enter **User Name** and **Password**.
 3. Click **Login**.
 4. Download and install appropriate plug-in for your web browser. Follow the installation prompts to install the plug-in.
-

5. Reopen the web browser after the installation of the plug-in and repeat steps 1 to 3 to login.
6. Optional: Click **Logout** on the upper right corner of the interface to log out of the device.

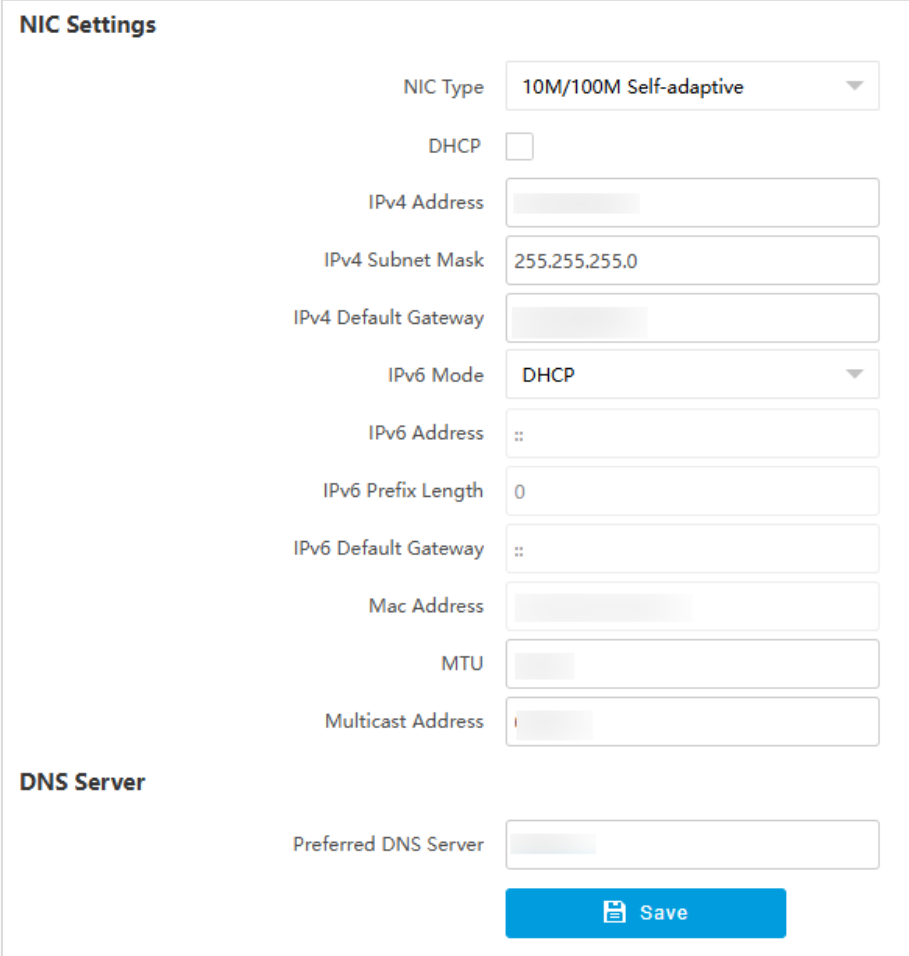
Chapter 2 Network Configuration

2.1 Set IP Address

IP address must be properly configured before you operate the device over network. IPv4 and IPv6 are both supported. Both versions can be configured simultaneously without conflicting to each other.

Steps

1. Go to **Configuration** → **Network** → **Network Parameters** → **Network Interface**.



The image shows a web-based configuration form titled "NIC Settings". It contains several input fields and a "Save" button. The fields are organized into two sections: "NIC Settings" and "DNS Server".

Field	Value
NIC Type	10M/100M Self-adaptive
DHCP	☐
IPv4 Address	
IPv4 Subnet Mask	255.255.255.0
IPv4 Default Gateway	
IPv6 Mode	DHCP
IPv6 Address	::
IPv6 Prefix Length	0
IPv6 Default Gateway	::
Mac Address	
MTU	
Multicast Address	
Preferred DNS Server	

Save

Figure 2-1 Set IP Address

2. Set network parameters.

NIC Type

Select a NIC (Network Interface Card) type according to your network condition.

IPv4

Two modes are available.

DHCP

The device automatically gets the IP parameters from the network if you check **DHCP**. The device IP address is changed after enabling the function. You can use SADP to get the device IP address.



The network that the device is connected to should support DHCP (Dynamic Host Configuration Protocol).

Manual

You can set the device IP parameters manually. Enter **IPv4 Address**, **IPv4 Subnet Mask**, and **IPv4 Default Gateway**.

IPv6

Three IPv6 modes are available.

Route Advertisement

The IPv6 address is generated by combining the route advertisement and the device Mac address.



Route advertisement mode requires the support from the router that the device is connected to.

DHCP

The IPv6 address is assigned by the server, router, or gateway.

Manual

Enter **IPv6 Address**, **IPv6 Subnet Mask**, and **IPv6 Default Gateway**. Consult the network administrator for required information.

MTU

It stands for maximum transmission unit. It is the size of the largest protocol data unit that can be communicated in a single network layer transaction.

The valid value range of MTU is 1280 to 1500.

Multicast Address

Multicast is group communication where data transmission is addressed to a group of destination devices simultaneously. After setting the IP address of the multicast host, you can send the source data efficiently to multiple receivers.

DNS

It stands for domain name server. It is required if you need to visit the device with domain name. And it is also required for some applications (e.g., sending email). Set **Preferred DNS Address** properly if needed.

3. Click **Save**.

2.2 Connect to Mobile Network

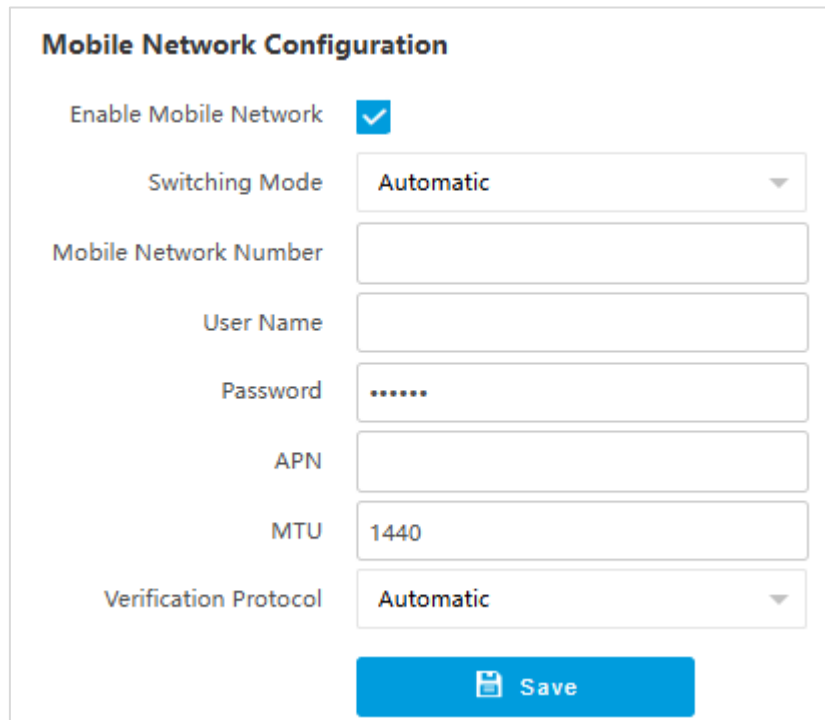
Set the mobile network parameters if you want to connect the device to the network via the SIM card.

Before You Start

Install the SIM card.

Steps

1. Go to **Configuration** → **Network** → **Network Parameters** → **Mobile Network**.
2. Check **Enable Mobile Network**.



The screenshot shows the 'Mobile Network Configuration' window. It contains the following fields and controls:

- Enable Mobile Network:** A checkbox that is checked with a blue checkmark.
- Switching Mode:** A dropdown menu currently set to 'Automatic'.
- Mobile Network Number:** An empty text input field.
- User Name:** An empty text input field.
- Password:** A text input field with six dots representing masked characters.
- APN:** An empty text input field.
- MTU:** A text input field containing the value '1440'.
- Verification Protocol:** A dropdown menu currently set to 'Automatic'.
- Save Button:** A blue button with a floppy disk icon and the text 'Save'.

Figure 2-2 Connect to Mobile Network

3. Select **Switching Mode**. If you select it as **Automatic**, the device will switch the mobile network module automatically according to the network conditions.
4. Set the mobile network parameters including **Mobile Network Number**, **User Name**, **Password**, and **APN**.

Note

- Consult the operator about the mobile network parameters.
 - When you have enabled mobile network and Wi-Fi simultaneously, the device will use Wi-Fi in priority.
-

5. Select **Verification Protocol**.

Automatic

The verification protocol will be switched automatically according to the network conditions.

CHAP

CHAP (Challenge-Handshake Authentication Protocol) is a challenge and response authentication method that Point-to-Point Protocol (PPP) servers use to verify the identity of a remote user. CHAP authentication begins after the remote user initiates a PPP link. CHAP enables remote users to identify themselves to an authenticating system, without exposing their password. With CHAP, authenticating systems use a shared secret - the password - to create a cryptographic hash using the MD5 message digest algorithm. In contrast to the two-way handshake and plain text password of PAP, CHAP is a three-way handshake process and more secure.

PAP

PAP (Password Authentication Protocol) is a simple authentication protocol used by Point-to-Point Protocol (PPP) to validate users. PAP is specified in RFC 1334 and is supported by almost all network operating systems and network access servers. PAP is a two-way handshake: a client requests authentication, and a server responds. Passwords are delivered in plain text. The system then verifies that the credentials match what is stored for that user and responds with an ack or nack as appropriate. Since the password is sent across the network as regular text, PAP is not the most secure method.

6. Click **Save**.

7. Optional: Click **Refresh** to view the mobile network status.

2.3 Set Port

The device port can be modified when the device cannot access the network due to port conflicts. Go to **Configuration** → **Network** → **Network Parameters** → **Port** for port settings.

The screenshot shows a configuration window titled 'Set Port' with five sections, each for a different port type. Each section has an 'Enable' checkbox (all are checked) and a text input field for the port number.

Port Type	Enable	Port Number
HTTP Port	☒	80
HTTPS Port	☒	443
SDK Port	☒	8000
SADP Port	☒	
SDK over TLS Port	☒	8443

A blue 'Save' button is located at the bottom right of the configuration area.

Figure 2-3 Set Port

HTTP Port

It refers to the port through which the browser accesses the device. For example, when the **HTTP Port** is modified to 81, you need to enter ***http://192.168.1.64:81*** in the browser for login. It is disabled by default.

HTTPS Port

It refers to the port through which the browser accesses the device, but certificate verification is needed. It is enabled by default.

SDK Port

It refers to the port through which the client adds the device.

SADP Port

It refers to the port through which the SADP software searches the device.

SDK over TLS Port

It refers to the port that adopts TLS protocol over the SDK service, to provide safer data transmission.



Note

- After editing the port, access to the device via the new port.

- Reboot the device to bring the new settings into effect.
 - The supported ports vary with different models. The actual device prevails.
-

2.4 Set Wi-Fi Hotspot

Set Wi-Fi hotspot to use the device as a hotspot to share network to another terminal device.

Steps

1. Go to **Configuration** → **Network** → **Network Parameters** → **Wifi**.
2. Enable **Wi-Fi**.
3. Select **Wi-Fi Mode** as **Wi-Fi Hotspot**.

The image shows a 'Wi-Fi' configuration window. At the top, 'Wi-Fi' is checked and labeled 'Enable'. Below it, 'Wi-Fi Mode' has 'Wi-Fi Hotspot' selected with a radio button. The 'Wi-Fi Configuration' section includes: 'AP Broadcast' checked; 'WLAN Hotspot' unchecked; 'SSID' as an empty text field; 'Security Mode' set to 'WPA2-personal'; 'Encryption Type' set to 'AES'; 'Key' selected with a radio button and a masked password field; 'IP Address', 'Subnet Mask', 'Start IP Address', 'End IP Address', 'Preferred DNS Server', 'Alternate DNS Server', and 'Gateway' as empty text fields; and 'DHCP' checked and labeled 'Enable'. A blue 'Save' button is at the bottom right.

Figure 2-4 Set Wi-Fi Hotspot

4. Enable **AP Broadcast** or **WLAN Hotspot** as needed.

5. Set the hotspot information.
 - 1) Enter **SSID** (hotspot name).
 - 2) Select **Security Mode** and **Encryption Type**.
 - 3) Enter **Key**, **IP Address**, and **Subnet Mask**.
 6. Optional: Enable **DHCP** and enter the start/end IP address.
-



Note

The IP address should be different from the one that set in the network parameters.

7. Click **Save**.

2.5 Data Connection

2.5.1 Set Email

When the email is enabled and set, the device will send an email notification to all designated receivers if an alarm event is detected.

Before You Start

Set the DNS server before using the email function. Go to **Configuration** → **Network** → **Network Parameters** → **Network Interface** for DNS settings.

Steps

1. Go to **Configuration** → **Network** → **Data Connection** → **Email**.
2. Check **Enable Email**.

Email

Enable Email ☒

Sender

Sender's Address

SMTP Server

SMTP Port

Email Encryption TLS

Authentication ☒

User Name

Password

Confirm Password

Enable xOAuth2 Authentication ☐

Receiver

No.	Receiver	Receiver's Address	Test
1			Test
2			Test
3			Test

Figure 2-5 Set Email

3. Set email parameters.

- 1) Enter the sender's email information, including **Sender**, **Sender's Address**, **SMTP Server**, and **SMTP Port**.
- 2) Select **Email Encryption**.

TLS

Emails are sent after being encrypted by TLS.

None

Emails are sent without encryption.

- 3) Optional: If you want to upload no-plate data, check **Upload No-Plate Data**.
 - 4) Optional: If your email server requires authentication, check **Authentication** and enter your user name and password to log in to the server.
 - 5) Optional: The device supports Google email xOAuth 2.0 authentication. You can check **Enable xOAuth2 Authentication** to enable the function, and set **Client ID**, **Client Key**, and **Proxy** as needed.
 - 6) Enter the receiver's information, including the receiver's name and address.
 - 7) Optional: Click **Test** to see if the function is well configured.
4. Click **Save**.

2.5.2 Set ISAPI Listening

The device supports receiving and uploading the target speed information detected by the radar

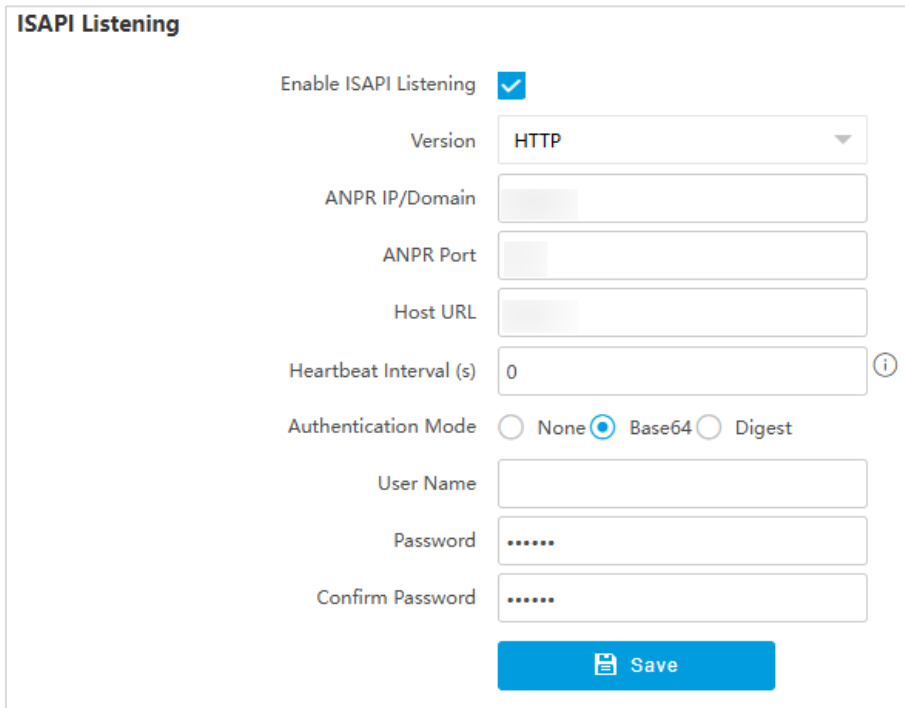
via ISAPI protocol after the ISAPI parameters are set.

Before You Start

The listening service has been enabled for the ISAPI host, and the network communication with the device is normal.

Steps

1. Go to **Configuration** → **Network** → **Data Connection** → **ISAPI Listening**.
2. Enable ISAPI listening.



The screenshot shows the 'ISAPI Listening' configuration window. It includes a checkbox for 'Enable ISAPI Listening' which is checked. Below it is a 'Version' dropdown menu set to 'HTTP'. There are input fields for 'ANPR IP/Domain', 'ANPR Port', and 'Host URL'. A 'Heartbeat Interval (s)' field is set to '0' with an information icon. The 'Authentication Mode' section has three radio buttons: 'None', 'Base64' (which is selected), and 'Digest'. At the bottom, there are input fields for 'User Name', 'Password', and 'Confirm Password', followed by a blue 'Save' button.

Figure 2-6 Set ISAPI Listening

3. Select **Version**.
4. Set **ANPR IP/Domain**, **ANPR Port**, and **Host URL**.
5. Set the parameters.

Heartbeat Interval

If you set it as 0, the heartbeat is disabled.

Authentication Mode

Only the authorized users can access the device. If you select **None**, the device will not verify the authentication condition of the access users. It is recommended to select an authentication mode to guarantee the device information security.

6. Click **Save**.

2.5.3 Connect to ISUP Platform

When the device detects solar energy device connection when initializing, it can get the solar

energy battery and temperature information, and judge the current battery status (normal or low battery) according to the solar low battery threshold applied by the platform. ISUP is a platform access protocol, via which the device can upload the battery, temperature, and low battery status information of the solar energy device to the platform.

Before You Start

- Create the device ID on ISUP platform.
- Ensure the device can communicate with the platform normally.

Steps

1. Go to **Configuration** → **Network** → **Data Connection** → **ISUP**.
2. Enable ISUP.

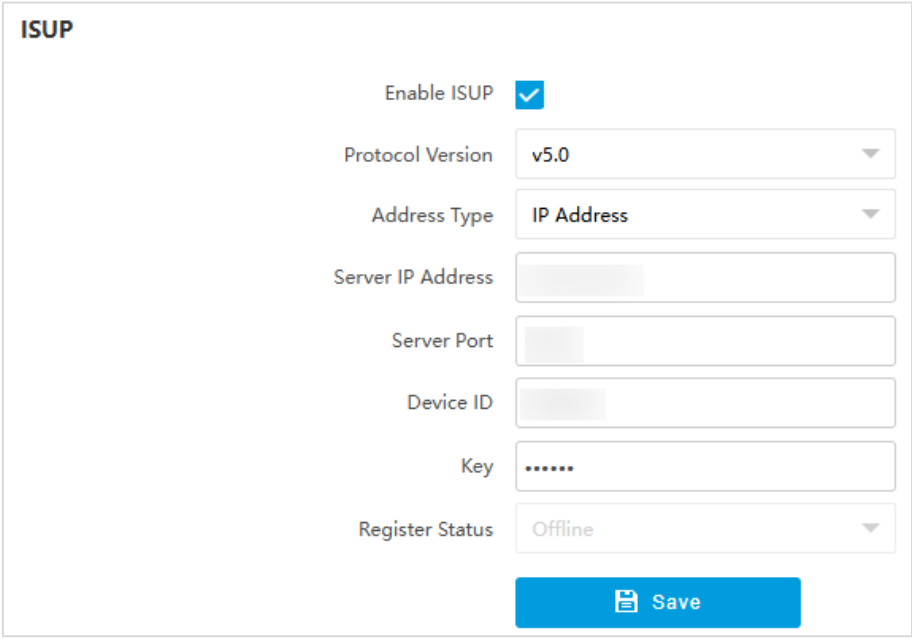


Figure 2-7 Connect to ISUP Platform

3. Select **Protocol Version**.
4. Select **Address Type** and enter IP address or domain name of the platform.
5. Enter **Server Port**, **Device ID**, and **Key**.

Note

The device ID should be the same with the added one on the platform.

6. Click **Save**.

What to do next

When the registration status is online, you can view the battery, temperature, and low battery status information of the solar energy device on the platform.

Chapter 3 Display Configuration

The device is equipped with two screens. The upper screen can display the speed information and emoji. The lower screen can display the custom prompt information. You can set the display parameters.

Steps

1. Go to **Configuration** → **Display**.

The screenshot shows a configuration interface with the following elements:

- Speed Unit:** A dropdown menu set to "km/h".
- Overspeed Threshold:** A text input field containing "150".
- Screen Speed Threshold:** A text input field containing "5".
- Target Distance Lowerbound(m):** A text input field containing "0".
- Target Distance Upperbound(m):** A text input field containing "100".
- No speeding:** A section header.
- Display color:** A dropdown menu set to "Green".
- Speeding:** A section header.
- Display color:** A dropdown menu set to "Red".
- Screen Brightness:** A slider control with a blue bar and a white knob, with a numeric input field set to "5".
- Screen Selection:** Two buttons, "Emoji screen" (highlighted in blue) and "LED screen".
- Emoji display time(s):** A text input field containing "2".
- Speed display time(s):** A text input field containing "3".
- Save:** A blue button with a floppy disk icon and the text "Save".

Figure 3-1 Display Configuration (Without Solar Energy Device Connection)

Speed Unit: km/h

Overspeed Threshold: 150

Screen Speed Threshold: 5

Target Distance Lowerbound(m): 0

Target Distance Upperbound(m): 100

No speeding

Display color: Green

Speeding

Display color: Red

Brightness Control Mode: Schedule Mode

Daytime Brightness: 10

Night Brightness: 8

Night Start Time: 18:00

Night End Time: 06:00

Emoji screen | LED screen

Emoji display time(s): 2

Speed display time(s): 3

Save

Figure 3-2 Display Configuration (With Solar Energy Device Connection)

2. Set the parameters below.

Speed Unit

Select the unit of the speed displayed on the screen. mph refers to miles per hour.

Overspeed Threshold

Set the speed value beyond which the vehicle is regarded as speeding.

Screen Speed Threshold

Only when the vehicle speed is higher than the set threshold, will the speed be displayed on the screen.

Target Distance Lowerbound/Upperbound

Set the target distance range within which the target will be detected. When there are multiple targets appearing in the range, the speed of the forefront target will be displayed.

Display Color

Set the speed value display color for normal speed and speeding. For example, if you set green for the normal speed and red for speeding, when the vehicle's speed is within the allowed limit, the speed value is displayed in green with a smiley face emoji. Conversely, when the vehicle's speed exceeds the upper speed limit, the speed value is displayed in red with a sad face emoji.

Screen Brightness

If no solar energy device is connected, set the emoji screen brightness manually.

Brightness Control Mode

If the solar energy device is connected, you can select the brightness control mode. The default control mode is solar mode.

Solar Mode

When the display has been connected with Hikvision solar charging kit, the screen brightness will be adjusted automatically according to the gotten battery percentage of the connected solar energy device. The relationship between the solar energy device battery and the screen brightness is shown as below.

Solar Energy Device Battery	Screen Brightness
≥ 80%	10
[60% - 80%)	8
[40% - 60%)	6
[20% - 40%)	4
> 20%	2

Schedule Mode

You can set **Daytime Brightness**, **Night Brightness**, **Night Start Time**, and **Night End Time**.

During the set night start time and end time, the system will adjust the screen brightness as the value set for the night brightness. Outside the set night start time and end time, the system will adjust the screen brightness as the value set for the daytime brightness.

- Click **Emoji screen** to set the information display time and brightness for the upper screen.

Emoji/Speed display time

Set the display duration for the emoji/speed value. During the display time, the speed value will refresh every second, and the displayed emoji depends on the speed of the last second. If the speed of the last second is within the allowed limit, the screen will display a smiley face emoji. If the speed of the last second exceeds the upper speed limit, the screen will display a sad face emoji.

- Click **LED screen** to set the display content for the normal speed and speeding on the lower screen.



The display content length should no more than eight bytes.

5. Click **Save**.

Chapter 4 Email Event

When the set event occurs, the device can be set to send an email with alarm information to the user.

Before You Start

The email has been enabled and related email parameters have been configured. Refer to **2.5.1 Set Email** for details.

Steps

1. Go to **Configuration** → **Event** → **Alarm Linkage** → **Email Event**.
2. Check **Enable** to trigger an email for login alarm.
3. Click **Save**.

Chapter 5 Extended Interface

You can set the cycle and format for sending the statistics data to the set email address.

Before You Start

Set the email parameters. Refer to [2.5.1 Set Email](#) for details.

Steps

1. Go to **Configuration** → **Expand**.
2. Set the parameters below.

Cycle for Sending Email

Set the cycle (daily, weekly, monthly, or yearly) for sending email. The statistics data during the cycle will be sent to the email at the end of the cycle.

Format for Sending Email

Set the content (time or speed) to be sent. The corresponding statistics data during the cycle will be sent to the email at the end of the cycle.

Solar Low Battery Email Alert Threshold

If a solar energy device is connected, set the low battery threshold of the solar energy device, lower than which the solar low battery alert will be sent to the email.

3. Click **Save**.

Chapter 6 Radar Detection

The device adopts high-frequency band and millimeter-wave radar. The radar can detect the vehicle speed which will be displayed on the screen.

6.1 Set Detection Parameters

Set radar speed detection parameters.

Steps

1. Click **Radar**.
2. View the radar information.

Software Version

The software version of the radar.

Radar Status

The current radar status. The radar can be normally used in normal status. If the radar is in upgrading status, do not reboot the device. Refresh the interface every one minute, and the status can be restored to normal.

3. Expand **Advanced Settings** menu, and enable **Debug Mode** to set the parameters.

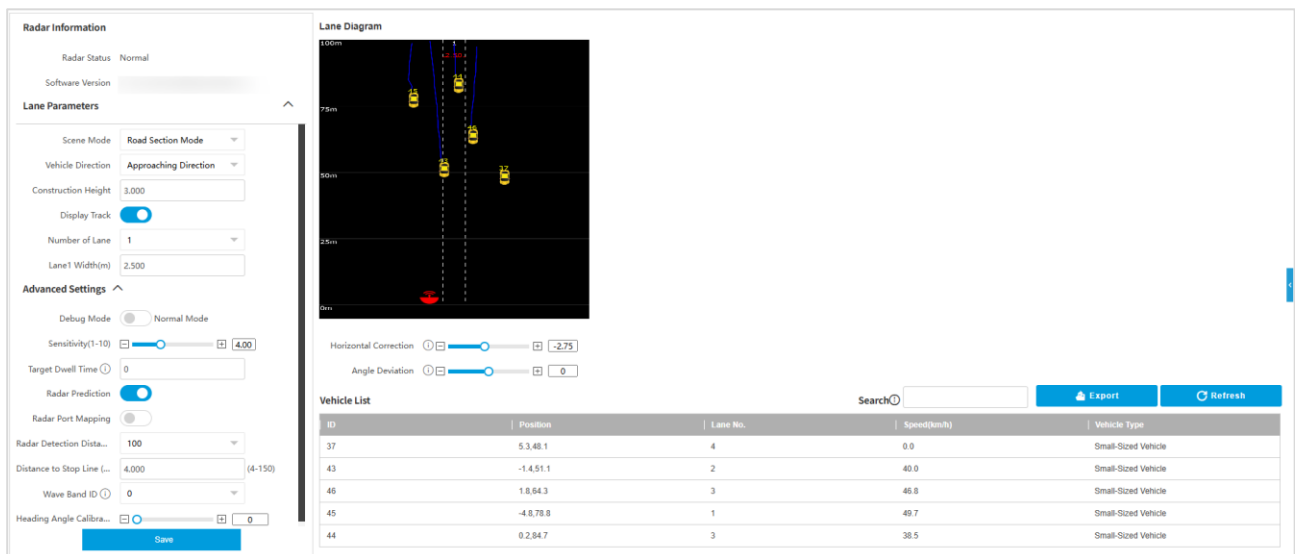


Figure 6-1 Set Radar Parameters

- 1) Set lane parameters.

Scene Mode

Select the scene mode according to the actual scene.

Vehicle Direction

Select the direction from which the vehicle speed will be detected.

Construction Height

Set the construction height of the radar according to construction at the actual scene.

Display Track

Enable the function, and the target track will be displayed on the interface according to the detected coordinates.

Number of Lane

Select the number of lanes on which the vehicle speed will be detected according to the actual scene. Up to three lanes can be detected.

Lane X Width

Enter the lane width according to the actual condition.

2) Set horizontal correction and angle deviation parameters.

Angle Deviation

It is the angle deviation between the radar detected lane and the actual lane. Rotate the angle of the detected lane in the diagram to overlap it with the actual lane to correct the difference.

Horizontal Deviation

It is the horizontal position deviation between the radar detected lane and the actual lane. You can set it in two ways.

- Method 1: Move the detected lane in the diagram leftwards or rightwards to overlap it with the actual lane to correct the difference.
- Method 2: Enter the horizontal distance (m) from the radar installation position to the middle line of the actual lane to correct the difference.

3) Expand **Advanced Settings** menu, and set the corresponding parameters.

Sensitivity

The lower the sensitivity is, the more sensitive the detection will be. For the detection which is too sensitive (e.g., some fixed facilities, such as the bus station on the lane, are detected as vehicles), you can adjust the sensitivity higher.

Target Dwell Time

The dwell time of the vehicle. Set it as 0 when measuring the queue length.

Radar Prediction

Enable the function, and the radar will predict the target track which can be displayed on the interface according to the detected coordinates.

Radar Port Mapping

Enable the function and **SSH Service**, the debugging command with radar configuration information will be sent to the device.

Radar Detection Distance

It is the range of the radar track. The default value is 200 m. You can select the value to adjust the radar track range.

Distance to Stop Line

It is the distance from the point on the ground just below the installed radar to the stop line at the intersection. The targets detected in this range will be filtered.

Wave Band ID

0 to 4 stand for five frequencies. Set different wave bands for different radars in the same scene to prevent the radars in the same wave band from influencing each other.

Heading Angle Calibration

Adjust the course angle of the radar for target detection.

4) Click **Save**.

4. Disable **Debug Mode** to return to the normal mode to detect the vehicle speed.

You can view the captured vehicle information such as the license plate number and speed in the vehicle list.

6.2 Search Detected Vehicles

You can search the radar detected vehicles and export the information.

Steps

1. Click **Radar**.
2. View the vehicle information in the vehicle list.
3. Enter the vehicle No. in the text field, and press **Enter** to search the vehicle information.
4. Optional: Export the vehicle information.
 - Search the vehicle first, and click **Export** to export the searched vehicle information to the computer.
 - Click **Export** directly to export the information of all the detected vehicles to the computer.

Chapter 7 Traffic Flow Statistics

You can search and export the daily, weekly, monthly, or yearly traffic flow statistics report for large-sized vehicles and small-sized vehicles.

Steps

1. Click **Traffic Flow Statistics**.
2. Set the search conditions.

Report Type

Daily, weekly, monthly, or yearly reports are supported.

Select Time

Select the time according to the selected report type.

Counting Type

Time and speed reports are supported. For time report, the X coordinate unit is time, and the Y coordinate unit is the number of vehicles. For speed report, select **Speed Segmentation**.

The X coordinate unit is speed, and the displayed X coordinate interval depends on the selected speed segmentation. The Y coordinate unit is the number of vehicles.

3. Click **Search**, and the traffic flow statistics conforming to the set condition will be displayed on the right.

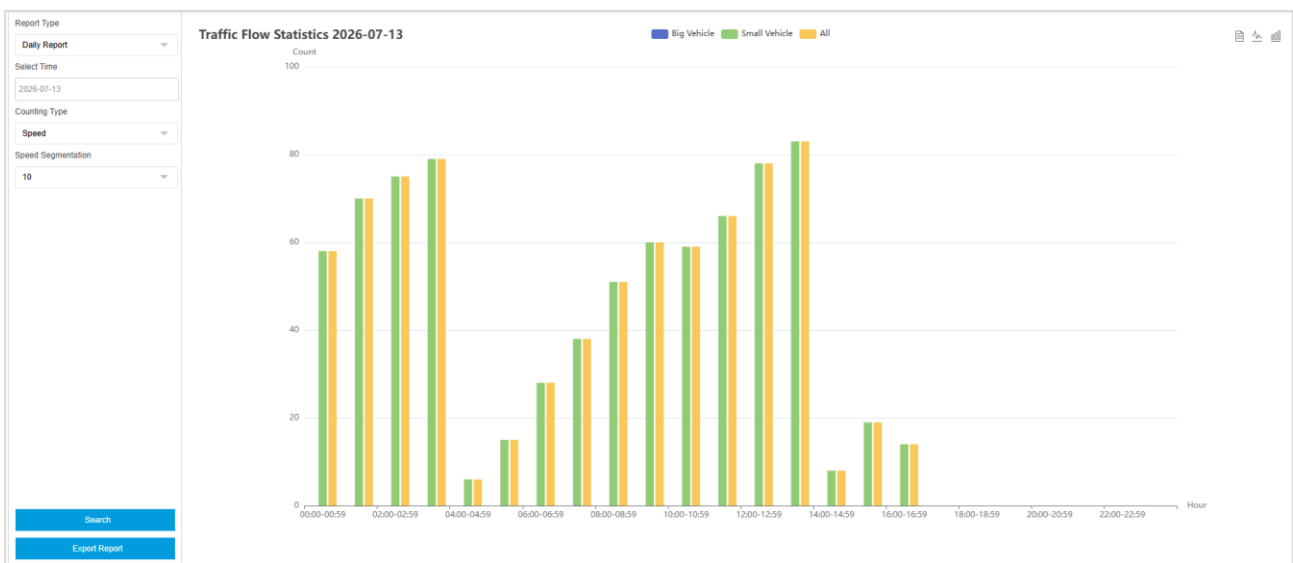


Figure 7-1 Traffic Flow Statistics

4. Optional: You can click  or  on the upper right corner of the interface to switch the statistics displayed as a line chart or bar chart. Or click  to view the statistics in a list, and click **close** to exit from the list.
5. Click **Export Report** to export the traffic flow statistics report to the computer as a file in the format of .xlsx.

Chapter 8 Safety Management

8.1 Manage User

The administrator can add, modify, or delete other accounts, and grant different permissions to different user levels.

Steps

1. Go to **Configuration** → **System** → **User Management** → **User List**.
2. Select **Password Level**.
The password level of the added user should conform to the selected level.
3. Add a user.
 - 1) Click **Add**.
 - 2) Enter **User Name** and select **Type**.
 - 3) Enter **Admin Password**, **New Password**, and confirm the password.



Caution

To increase security of using the device on the network, please change the password of your account regularly. Changing the password every 3 months is recommended. If the device is used in high-risk environment, it is recommended that the password should be changed every month or week.

- 4) Assign remote permission to users based on needs.

User

Users can be assigned permission of viewing live video and changing their own passwords, but no permission for other operations.

Operator

Operators can be assigned all permission except for operations on the administrator and creating accounts.

- 5) Click **OK**.
4. Optional: You can do the following operations.
 - Change the password and permission** Click  to change the password and permission.

Delete the user Click  to delete the user.

8.2 Set SSH

To raise network security, you are recommended to disable SSH service. The configuration is only used to debug the device for the professionals.

Steps

1. Go to **Configuration** → **System** → **Security** → **Security Service** → **Software**.
2. Enable or disable **SSH Service**, and set **SSH Port** if you enable the function.
3. Click **Save**.

8.3 Prohibit PING

You can prohibit the external devices to operate network connection volume test to the current device.

Steps

1. Go to **Configuration** → **System** → **Security** → **Security Service** → **Software**.
2. Enable **Prohibit PING**.
3. Click **Save**.

8.4 Set Timeout Logout

You can improve network access security by setting timeout logout.

Steps

1. Go to **Configuration** → **System** → **Security** → **Security Service** → **Timeout Logout**.
2. Enable timeout logout for static page.
3. Set **Max. Timeout**.
4. Click **Save**.

Result

When the page static time exceeds the set time, the device will automatically log out.

8.5 Set Password Validity Period

You can improve network access security by setting password validity period.

Steps

1. Go to **Configuration** → **System** → **Security** → **Security Service** → **Password Validity Period**.
2. Select **Validity Type**.
 - Select **Permanent**. The password will be permanently valid.
 - Select **Daily** and set **Password Expiry Time**. It will prompt you that the password is expired according to the set password expiry time, and you need to set the new password.

3. Click **Save**.

8.6 Set IP Address Filtering

You can set the IP addresses allowable and not allowable to access the device.

Steps

1. Go to **Configuration** → **System** → **Security** → **Security Settings**.
2. Check **Enable IP Address Filtering**.
3. Set **Filtering Mode**.

Blocklist Mode

The added IP addresses are not allowed to access the device.

Allowlist Mode

The added IP addresses are allowed to access the device.

4. Click **Add**, enter the IP address, and click **OK**.



Note

The IP address only refers to the IPv4 address.

5. Optional: Edit, delete, or clear the added IP addresses.
6. Click **Save**.

8.7 Set HTTPS

8.7.1 Create and Install Self-signed Certificate

HTTPS is a network protocol that enables encrypted transmission and identity authentication, which improves the security of remote access.

Steps

1. Go to **Configuration** → **Network** → **Network Parameters** → **HTTPS**.
2. Select **Create Self-signed Certificate**.
3. Click **Create**.
4. Follow the prompt to enter **Country/Region**, **Domain/IP**, **Validity**, and other parameters.
5. Click **OK**.

Result

The device will install the self-signed certificate by default.

8.7.2 Install Authorized Certificate

If the demand for external access security is high, you can create and install authorized certificate via HTTPS protocol to ensure the data transmission security.

Steps

1. Go to **Configuration** → **Network** → **Network Parameters** → **HTTPS**.
2. Select **Create certificate request first and continue the installation**.
3. Click **Create**.
4. Follow the prompt to enter **Country/Region**, **Domain/IP**, **Validity**, and other parameters.
5. Click **Download** to download the certificate request and submit it to the trusted authority for signature.
6. Import certificate to the device.
 - Select **Signed certificate is available, start the installation directly**. Click **Browse** and **Install** to import the certificate to the device.
 - Select **Create the certificate request first and continue the installation**. Click **Browse** and **Install** to import the certificate to the device.
7. Click **Save**.

Chapter 9 Maintenance

9.1 View Device Information

Basic Information

Go to **Configuration** → **System** → **System Settings** → **Basic Information** to view the basic information and algorithms library version of the device.

You can edit **Device Name** and **Device No.** The device No. is used to control the device. It is recommended to reserve the default value.

Device Status

Go to **Configuration** → **System** → **System Settings** → **Device Status** to view the device status.

9.2 Synchronize Time

Synchronize the device time when it is inconsistent with the actual time.

Steps

1. Go to **Configuration** → **System** → **System Settings** → **Time Settings**.
2. Select **Time Zone**.
3. Select **Sync Mode**.

NTP Synchronization

Select it to synchronize the device time with that of the NTP server. Set **Server IP**, **NTP Port**, and **Interval**. Click **NTP Test** to test if the connection between the device and the server is normal.

Manual Synchronization

Select it to synchronize the device time with that of the computer. Set time manually, or check **Sync. with computer time**.

SDK

If the remote host has been set for the device, select it to synchronize time via the remote host.

No

Select it to disable time synchronization.

All

Select it, and you can select any mode above.



The time synchronization modes vary with different models. The actual device prevails.

4. Click **Save**.

9.3 Set DST

If the region where the device is located adopts Daylight Saving Time (DST), you can set this function.

Steps

1. Go to **Configuration** → **System** → **System Settings** → **DST**.
2. Check **Enable DST**.
3. Set **Start Time**, **End Time**, and **DST Bias**.
4. Click **Save**.

9.4 Set RS-232

Set RS-232 parameters if you need to debug the device via RS-232 serial port.

Before You Start

The debugging device has been connected via the RS-232 serial port.

Steps

1. Go to **Configuration** → **System** → **System Settings** → **Serial Port** → **RS-232**.
2. Set **Baud Rate**, **Data Bit**, **Stop Bit**, etc.



The parameters should be same with those of the connected device.

3. Select **Work Mode**.

Console

Select it when you need to debug the device via RS-232 serial port.

Transparent Channel

Select it, and the network command can be transmitted to RS-232 control command via the RS-232 serial port.

Narrow Bandwidth Transmission

Reserved.

4. Click **Save**.

9.5 Reboot

When the device needs to be rebooted, reboot it via the software instead of cutting off the power directly.

Steps

1. Go to **Configuration** → **System** → **Maintenance** → **Upgrade & Maintenance** → **Device Maintenance**.
2. Click **Reboot**.
3. Click **OK** to reboot the device.



You can also click **Reboot** on the upper right corner of the page to reboot the device.

9.6 Restore Parameters

When the device is abnormal caused by the incorrect set parameters, you can restore the parameters.

Steps

1. Go to **Configuration** → **System** → **Maintenance** → **Upgrade & Maintenance** → **Device Maintenance**.
2. Select the restoration mode.
 - Click **Restore** and click **OK**. Then the parameters except the IP parameters, user parameters, and the saved parameters will be restored to the default settings.
 - Click **Restore Factory Settings** and click **OK** to restore all the parameters to the factory settings.
3. Click **OK**.

9.7 Export Parameters

You can export the parameters of one device, and import them to another device to set the two devices with the same parameters.

Steps

1. Go to **Configuration** → **System** → **Maintenance** → **Upgrade & Maintenance** → **Data Export**.
2. Click **Export** after **Configuring Parameters**.
3. Set an encryption password, confirm the password, and click **OK**.



The password is used for importing the configuration file of the current device to other devices.

4. Select the saving path, and enter the file name.
5. Click **Save**.

9.8 Export Debug File

The technicians can export the debug file to troubleshoot and maintain the device.

Steps

1. Go to **Configuration** → **System** → **Maintenance** → **Upgrade & Maintenance** → **Data Export**.
2. Click **Export** after **Debug File**.
3. Select the saving path, and enter the file name.
4. Click **Save**.

9.9 Export Diagnosis Information

The technicians can export the diagnosis information to troubleshoot and maintain the device.

Steps

1. Go to **Configuration** → **System** → **Maintenance** → **Upgrade & Maintenance** → **Data Export**.
2. Click **Export** after **Diagnosis Information**.
3. Select the saving path, and enter the file name.
4. Click **Save**.

9.10 Upgrade

Upgrade the system when you need to update the device version.

Before You Start

Prepare the upgrade file. If the upgrade file is a compressed package, it needs to be decompressed into the .dav format.

Steps

1. Go to **Configuration** → **System** → **Maintenance** → **Upgrade & Maintenance** → **Upgrade**.
2. Click **Browse** to select the upgrade file.
3. Click **Upgrade**.
4. Click **OK** in the popup window.



The upgrade process will take 1 to 10 minutes. Do not cut off the power supply.

Result

The device will reboot automatically after upgrade.

9.11 Import Configuration File

Import the configuration file of another device to the current device to set the same parameters.

Before You Start

Save the configuration file to the computer.

Steps



Importing configuration file is only available to the devices of the same model and same version.

1. Go to **Configuration** → **System** → **Maintenance** → **Upgrade & Maintenance** → **Advanced Settings** → **Data Import**.
 2. Select **Importing Method**.
-



If you select **Import Part**, check the parameters to be imported.

3. Click **Browse** to select the configuration file.
 4. Click **Import**.
 5. Enter the password which is set when the configuration file is exported, and click **OK**.
-



If you have entered the incorrect password for 5 times continuously, the system will be locked for 30 minutes.

6. Click **OK** on the popup window.

Result

The parameters will be imported, and the device will reboot.

Port Information

For Radar-Assisted Speed LED Display, the device will open the following network ports to provide corresponding services. The service names, ports, and functions are as follows:

- SADP Discovery: UDP 37020 (multicast 239.255.255.250), LAN device search and activation.
- HTTPS Management: TCP 443, for browser access, parameter configuration and data query.
- SDK OVER TLS: TCP 8443, for device connection, activation, upgrade, restart, and parameter restoration.
- Ethernet Interface: RJ45 Port for Physical Connection, the device can be directly connected to the network via an Ethernet port, enabling initial setup, firmware upgrades, and parameter configuration over the network.



See Far, Go Further