

Outdoor Speed Sign 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 SADP 1
1.1.3 Activate via Web Browser 2
1.2 Login 3
Chapter 2 Network Configuration 4
2.1 Set IP Address 4
2.2 Set Port 6
2.3 Set DDNS 7
2.4 Set Wi-Fi Hotspot 8
Chapter 3 Display Configuration 10
Chapter 4 Exception Alarm 12
Chapter 5 Safety Management 13
5.1 Manage User 13
5.2 Set SSH 14
5.3 Prohibit PING 14
5.4 Set Timeout Logout 14
5.5 Set Password Validity Period 14
5.6 Set IP Address Filtering 15
5.7 Set HTTPS 15
5.7.1 Create and Install Self-signed Certificate 15
5.7.2 Install Authorized Certificate 16
Chapter 6 Maintenance 17
6.1 View Device Information 17
6.2 Synchronize Time 17
6.3 Set DST 18
6.4 Set RS-232 18
6.5 Reboot 19

6.6 Restore Parameters 19
6.7 Export Parameters 19
6.8 Export Debug File 20
6.9 Export Diagnosis Information 20
6.10 Upgrade 20
6.11 Import Configuration File 21
6.12 Enable Log According to Module 21
Port Information 22

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 SADP software, web browser, and iVMS-4200 Client.

Note

Refer to the user manual of iVMS-4200 Client for the activation via client software.

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 SADP

SADP is a tool to detect, activate, and modify the IP address of the device over the LAN.

Before You Start

- Get the SADP software from the supplied disk or the official website (***http://www.hikvision.com/***), and install it according to the prompts.
- The device and the computer that runs the SADP tool should belong to the same network segment.

The following steps show how to activate one device and modify its IP address. For batch activation and IP address modification, refer to *User Manual of SADP* for details.

Steps

1. Run the SADP software and search the online devices.
2. Find and select your device in online device list.
3. Enter a new password (admin password) and confirm the 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 **Activate** to start activation.

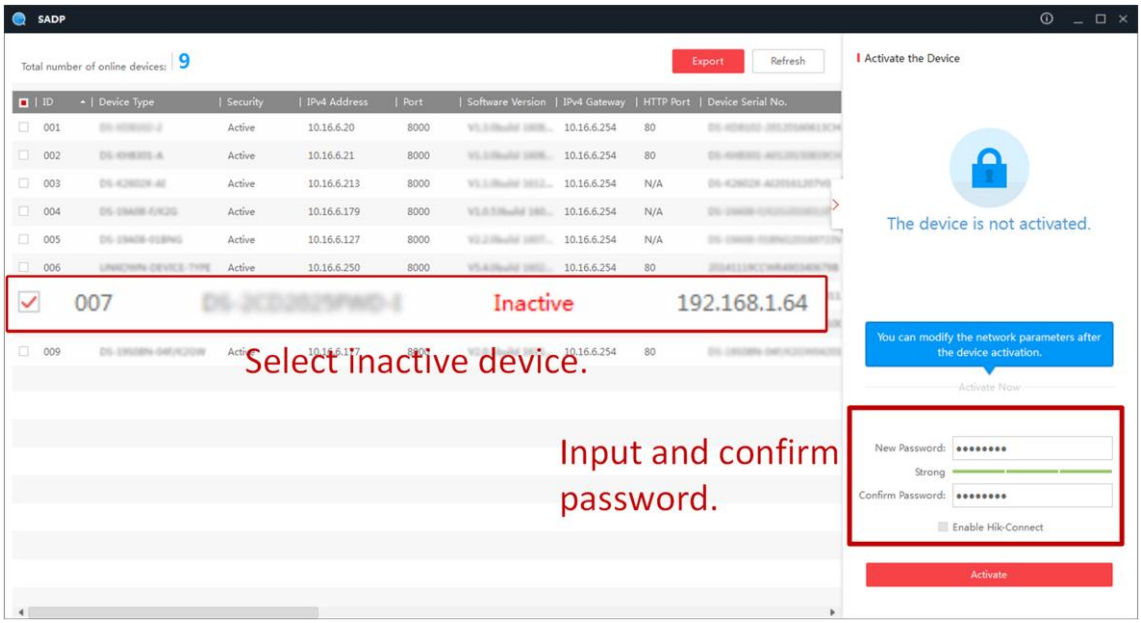


Figure 1-1 Activate via SADP

Status of the device becomes **Active** after successful activation.

5. Modify IP address of the device.
   1) Select the device.
   2) Change the device IP address to the same network segment as your computer by either modifying the IP address manually or checking **Enable DHCP** (Dynamic Host Configuration Protocol).
   3) Enter the admin password and click **Modify** to activate your IP address modification.

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**.

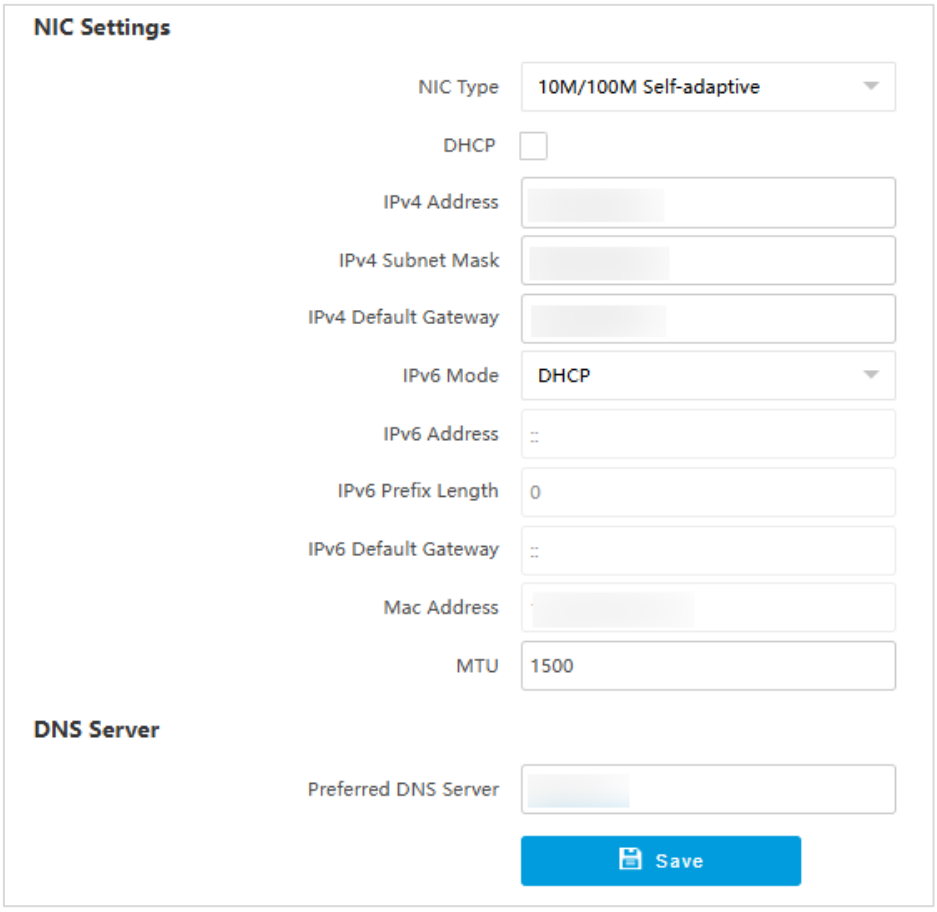


Figure 2-1 Set IP Address

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.

Note

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.

Note

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.

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 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.

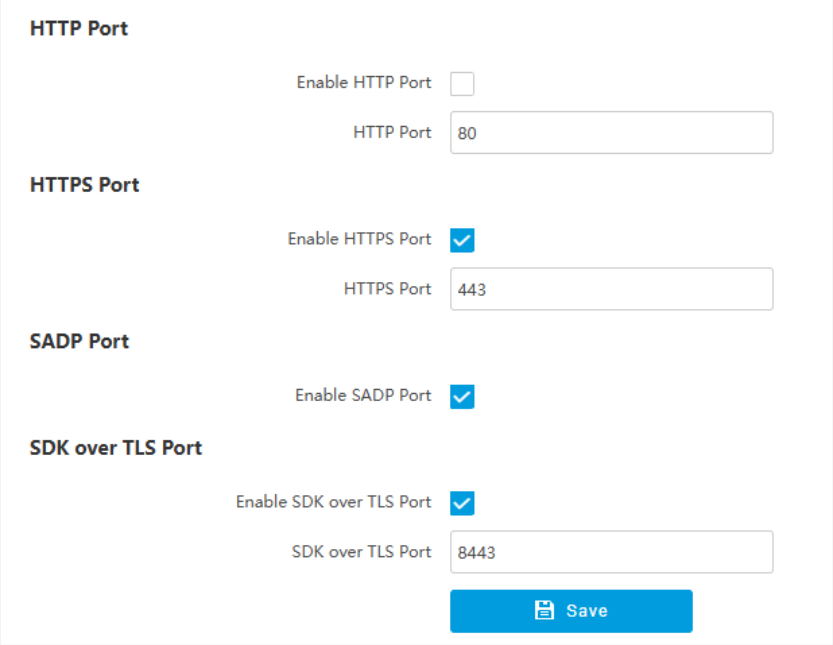


Figure 2-2 Set Port

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.

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.

2.3 Set DDNS

You can use the Dynamic DNS (DDNS) for network access. The dynamic IP address of the device can be mapped to a domain name resolution server to realize the network access via domain name.

Before You Start

- Register the domain name on the DDNS server.
- Set the LAN IP address, subnet mask, gateway, and DNS server parameters. Refer to ***Set IP Address*** for details.
- Complete port mapping. The default ports are 80, 8000, and 554.

Steps

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

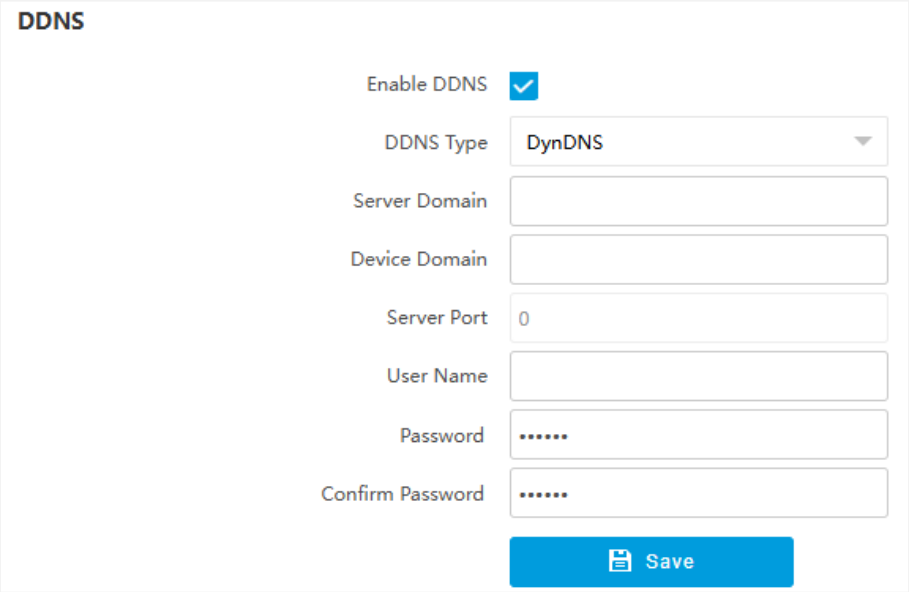


Figure 2-3 Set DDNS

2. Check **Enable DDNS**.
3. Select **DDNS Type** as **DynDNS**.
4. Enter the server domain, device domain, and other information.
5. Click **Save**.
6. Access the device.

By Browsers	Enter the domain name in the browser address bar to access the device.
By Client Software	Add domain name to the client software. Refer to the client software manual for specific adding methods.

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**.

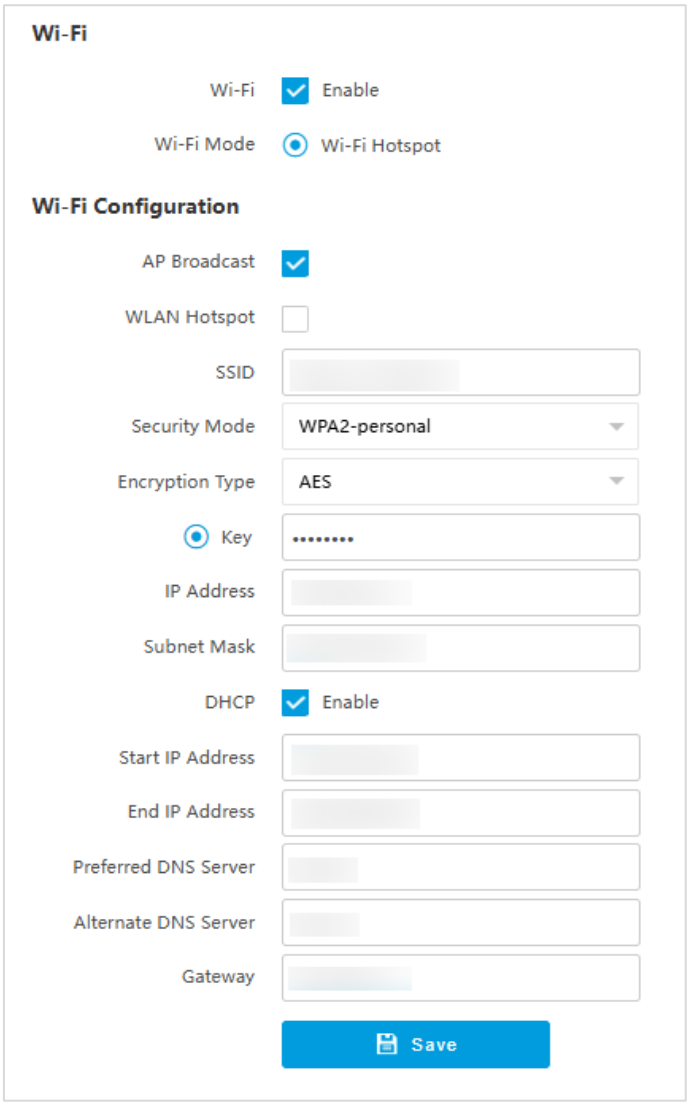


Figure 2-4 Set Wi-Fi Hotspot

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**.

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 when a vehicle is passing.

Steps

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

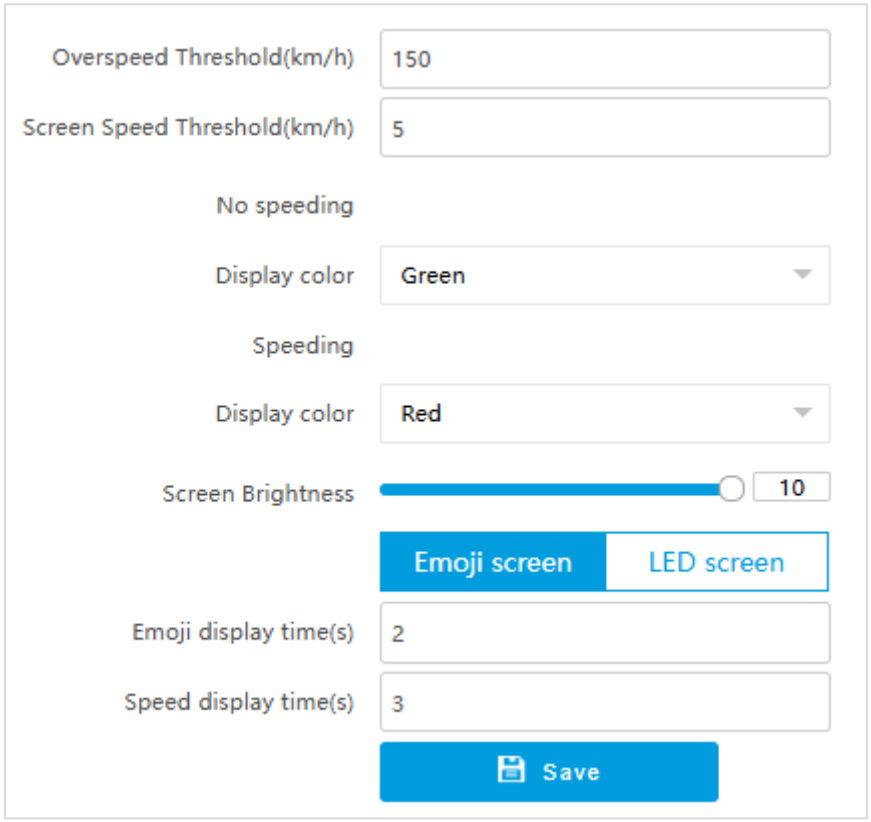


Figure 3-1 Display Configuration

2. Set the parameters below.

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.

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.

3. 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.

Screen Brightness

Set the brightness for the upper screen.

4. Click **LED screen** to set the information displayed on the lower screen.
   1) Enable **Display License Plate Number** to display the recognized license plate number of the passing vehicle.
   2) Set the display content for the normal speed and speeding on the lower screen.

Note

The display content length should be no more than eight bytes.

5. Click **Save**.

Chapter 4 Exception Alarm

Set exception alarm when the network is disconnected and the IP address is conflicted.

Steps

Note

The supported exception types vary with different models. The actual device prevails.

1. Go to **Configuration** → **Event** → **Alarm Linkage** → **Exception**.
2. Select the exception type(s) and the linkage method.
3. Click **Save**.

Chapter 5 Safety Management

5.1 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.

5.2 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**.

5.3 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**.

5.4 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.

5.5 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**.

5.6 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**.

5.7 Set HTTPS

5.7.1 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.

5.7.2 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 6 Maintenance

6.1 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.

6.2 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.

Note

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

4. Click **Save**.

6.3 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**.

6.4 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.

Note

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**.

6.5 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.

Note

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

6.6 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**.

6.7 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**.

Note

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**.

6.8 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**.

6.9 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**.

6.10 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.

Note

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

Result

The device will reboot automatically after upgrade.

6.11 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

Caution

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**.

Note

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**.

Note

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.

6.12 Enable Log According to Module

You can enable the log according to the module for debugging.

Steps

1. Go to **Configuration** → **System** → **Maintenance** → **Debug** → **Log**.
2. Check the module(s) according to your needs.
3. Click **Save**.

Port Information

For Outdoor Speed Sign 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