Fall Detection Radar

User Manual

Legal Information

About this Manual

The Manual 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 Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of this Manual at the Hikvision website (***https://www.hikvision.com/***).
Please use this Manual with the guidance and assistance of professionals trained in supporting the Product.

Trademarks

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.

Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS MANUAL 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 MANUAL AND THE APPLICABLE LAW, THE LATTER PREVAILS.

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.
ℹ**Note**	Provides additional information to emphasize or supplement important points of the main text.

Contents

Chapter 1 Introduction 1

1.1 Product Introduction 1

1.2 Key Feature 1

Chapter 2 Activation and Login 2

2.1 Activation 2

2.1.1 Default Information 2

2.1.2 Activate via SADP 2

2.1.3 Activate via Web Browser 3

2.2 Login 4

Chapter 3 Radar Detection 5

3.1 Set Radar Mode 5

3.2 Set Detection Parameters 6

Chapter 4 Storage 7

4.1 Set SDK Listening 7

4.2 Set ISAPI Listening 7

Chapter 5 Network Configuration 8

5.1 Set IP Address 8

5.2 Set Wi-Fi 10

5.3 Set Wi-Fi AP 10

5.4 Connect to Platform 11

5.4.1 Connect to OTAP 11

5.4.2 Connect to Hik-Connect 12

5.5 Set DDNS 13

5.6 Set SNMP 14

5.7 Set IEEE 802.1X 15

5.8 Set Port 16

Chapter 6 Exception Alarm 17

Chapter 7 Safety Management 18

7.1 Manage User 18

7.2 Enable User Lock 18

7.3 Install Authorized Certificate 19

7.4 Create and Install Self-signed Certificate 19

7.5 Set SSH 19

7.6 Set IP Address Filtering 20

7.7 Set Timeout Logout 20

7.8 Set Password Validity Period 21

Chapter 8 Maintenance 22

8.1 View Device Information 22

8.2 Log 22

8.2.1 Enable System Log Service 22

8.2.2 Enable Log According to Module 22

8.3 Upgrade 23

8.4 Reboot 23

8.5 Restore Parameters 23

8.6 Set Serial Port 24

8.7 Synchronize Time 25

8.8 Set DST 25

8.9 Export Parameters 26

8.10 Import Configuration File 26

8.11 Export Debug File 27

8.12 Export Diagnosis Information 27

Chapter 1 Introduction

1.1 Product Introduction

Fall detection radar (hereinafter referred to as "device") adopts FMCW, MIMO, beamforming, KNN, and other technologies. It can obtain target information, including person location, speed, posture, etc., and can provide non-contact fall detection.

1.2 Key Feature

- Supports to follow the target and output the real-time location information.
- Real-time and non-contact fall detection. No privacy disclosure.
- Supports to connect to OTAP.
- Supports data transmission via Wi-Fi.
- Small size and easy installation.
- It can be used to the indoor safety and health monitoring for the elderly people in hospitals, nursing homes, and other scenarios.

Chapter 2 Activation and Login

2.1 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.

2.1.1 Default Information

The device default information is shown as below.

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

2.1.2 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.

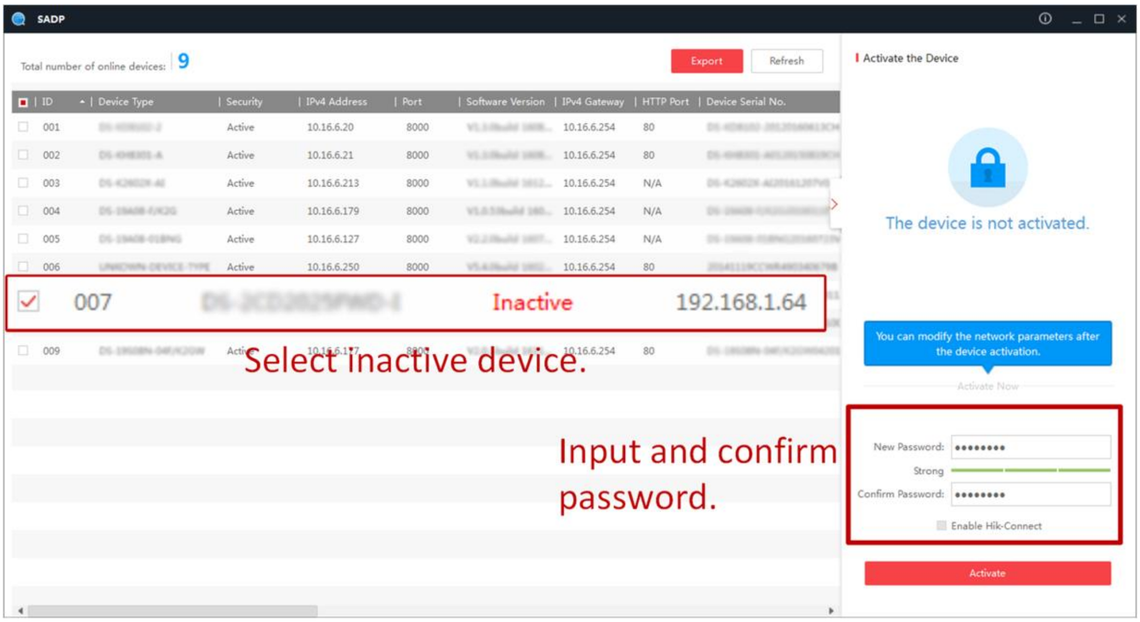
Steps

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.



SADP

Total number of online devices: 9

ID	Device Type	Security	IPv4 Address	Port	Software Version	IPv4 Gateway	HTTP Port	Device Serial No.
□ 001	[illegible]	Active	10.16.6.20	8000	[illegible]	10.16.6.254	80	[illegible]
□ 002	[illegible]	Active	10.16.6.21	8000	[illegible]	10.16.6.254	80	[illegible]
□ 003	[illegible]	Active	10.16.6.213	8000	[illegible]	10.16.6.254	N/A	[illegible]
□ 004	[illegible]	Active	10.16.6.179	8000	[illegible]	10.16.6.254	N/A	[illegible]
□ 005	[illegible]	Active	10.16.6.127	8000	[illegible]	10.16.6.254	N/A	[illegible]
□ 006	[illegible]	Active	10.16.6.250	8000	[illegible]	10.16.6.254	80	[illegible]
☑ 007	[illegible]	Inactive	192.168.1.64					
□ 009	[illegible]	Active	10.16.6.177	8000	[illegible]	10.16.6.254	80	[illegible]

Select inactive device.

Input and confirm password.

Activate the Device

The device is not activated.

You can modify the network parameters after the device activation.

New Password: ••••••••

Strong

Confirm Password: ••••••••

□ Enable Hik-Connect

Figure 2-1 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.

2.1.3 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.

2.2 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.

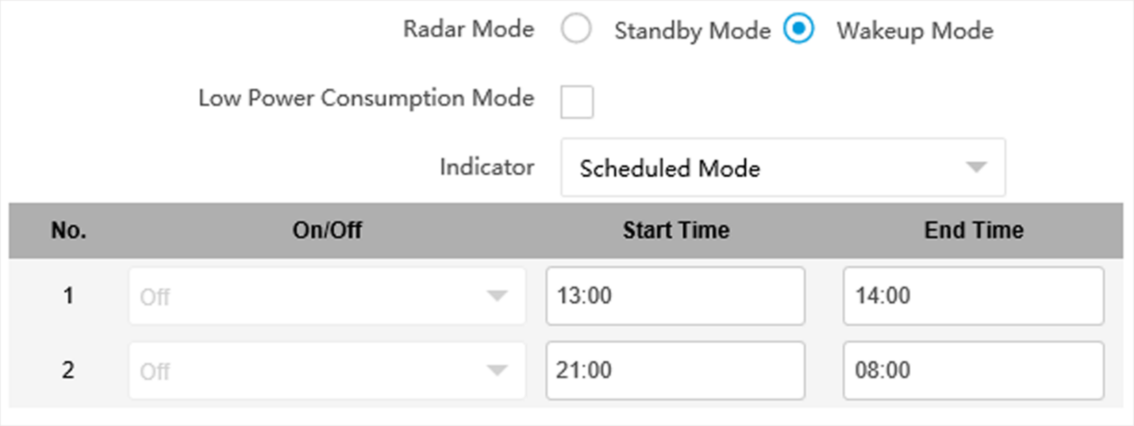
Chapter 3 Radar Detection

3.1 Set Radar Mode

Set radar mode according to the actual needs.

Steps

1. Go to **Configuration** → **System** → **System Settings** → **Radar**.



Radar Mode ○ Standby Mode ● Wakeup Mode

Low Power Consumption Mode □

Indicator: Scheduled Mode

No.	On/Off	Start Time	End Time
1	Off	13:00	14:00
2	Off	21:00	08:00

Figure 3-1 Set Radar Mode

2. Select **Radar Mode** according to the actual needs.

   Standby Mode

   The radar is not detecting.

   Wakeup Mode

   The radar is detecting.

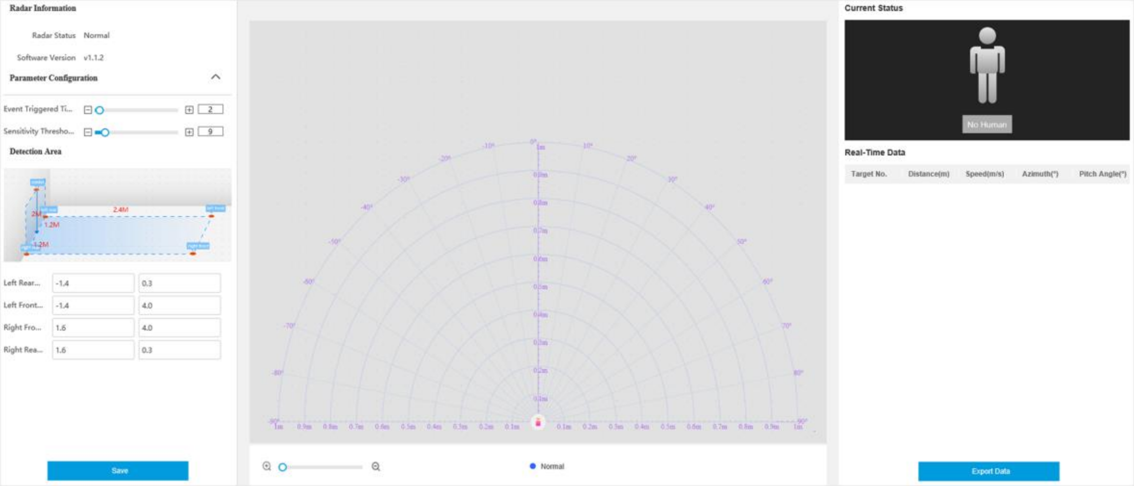
3. Optional: Check **Low Power Consumption Mode** and set **Interval** according to the actual needs. If no human body is detected after the set **Interval**, the radar will automatically switch to **Standby Mode** and detect according to the set **Interval**.
4. Set the indicator mode.
   - **Scheduled Mode**: The indicator will be turned on/off according to the set **Start Time** and **End Time**.
   - **Manual Switch**: Turn on/off the indicator manually.
5. Click **Save**.

3.2 Set Detection Parameters

Set radar detection parameters according to the actual needs and installation environment.

Steps

1. Click **Falling Monitoring**.



Radar Information

Radar Status Normal

Software Version v1.1.2

Parameter Configuration

Event Triggered Ti... 2

Sensitivity Thresho... 9

Detection Area

Left Rear...	-1.4	0.3
Left Front...	-1.4	4.0
Right Fro...	1.6	4.0
Right Rea...	1.6	0.3

Current Status

No Human

Real-Time Data

Target No.	Distance(m)	Speed(m/s)	Azimuth(°)	Pitch Angle(°)

Figure 3-2 Set Detection Parameters

2. View the radar information.

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.

Software Version

The software version of the radar.

3. Set the radar detection parameters.

Event Triggered Time

If the target falls and stands up within the set **Event Triggered Time**, the system will not output fall alarm.

Sensitivity Threshold of Human Body Detection

The higher the value is, the less sensitive the detection will be. The default value is recommended.

4. Set **Detection Area**.
5. Optional: You can also do the following operations.

⊕ ○ ⊖ Adjust the view scale.

Export Data Click **Export Data**, select the saving path, and click **OK** to export the location information.

Chapter 4 Storage

4.1 Set SDK Listening

The SDK listening can be used to receive the uploaded information of the device arming alarm.

Before You Start

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

Steps

1. Go to **Configuration** → **Network** → **Data Connection** → **SDK Listening**.
2. Check **Enable SDK Listening**.
3. Set **IP Address/Domain** and **Port** if you need to upload the alarm information.
4. Click **Save**.

4.2 Set ISAPI Listening

ISAPI listening and SDK listening are mutually exclusive protocols.

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. Check **Enable ISAPI Listening**.
3. Set **ANPR IP/Domain**, **ANPR Port**, and **Host URL**.
4. Click **Save**.

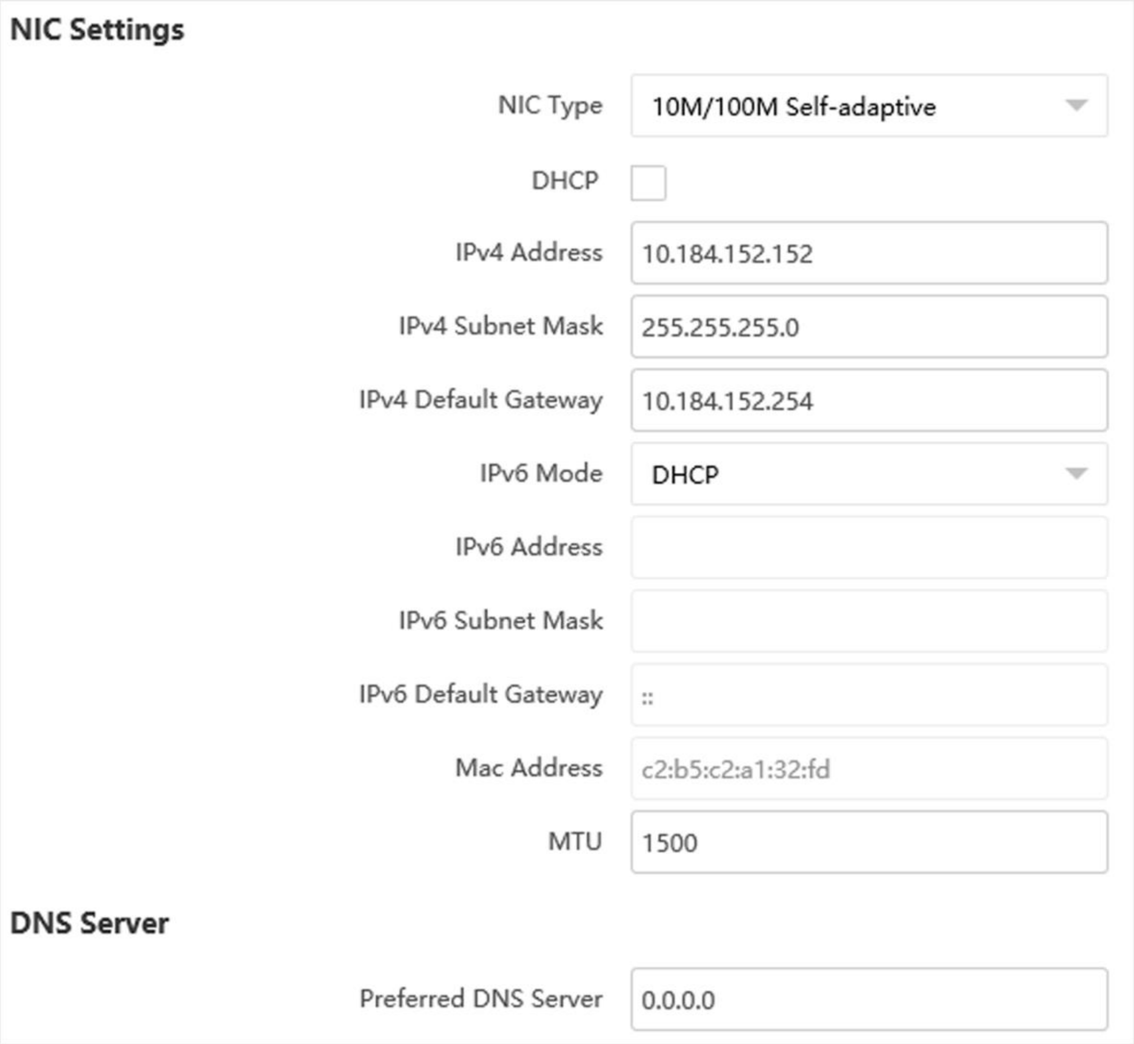
Chapter 5 Network Configuration

5.1 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**.



NIC Settings

NIC Type: 10M/100M Self-adaptive

DHCP: □

IPv4 Address: 10.184.152.152

IPv4 Subnet Mask: 255.255.255.0

IPv4 Default Gateway: 10.184.152.254

IPv6 Mode: DHCP

IPv6 Address:

IPv6 Subnet Mask:

IPv6 Default Gateway: ::

Mac Address: c2:b5:c2:a1:32:fd

MTU: 1500

DNS Server

Preferred DNS Server: 0.0.0.0

Figure 5-1 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**.

5.2 Set Wi-Fi

Set Wi-Fi parameters if you want to connect the device to the network via Wi-Fi.

Steps

1. Go to **Configuration** → **Network** → **Network Parameters** → **Wi-Fi**.
2. Select **Wi-Fi Mode** as **Wi-Fi**.
3. Click **Search** and select Wi-Fi to connect in the Wi-Fi list.
4. Select **Security Mode** and **Encryption Type** according to the actual needs.
5. Enter **Key**.
6. Click **Save**.
7. Optional: If you want to edit the IP address connected to the Wi-Fi to make it convenient to access to the device via the IP address of WLAN, set the IP address of WLAN.
   1) Select **IP Address Type** as **Static IP**.
   2) Enter **IP Address**, **Subnet Mask**, **Route Address**, etc.
   3) Click **Set**.
8. Optional: Click **Refresh** to view the Wi-Fi connection status.

5.3 Set Wi-Fi AP

The device can be set as a hotspot to share network to other devices.

Steps

1. Go to **Configuration** → **Network** → **Network Parameters** → **Wi-Fi**.
2. Select **Wi-Fi Mode** as **Wi-Fi Hotspot**.
3. Enable **AP Broadcast** or **WLAN Hotspot**.

   AP Broadcast

   Once enabled, other devices are able to detect the SSID of the device.

   WLAN Hotspot

   Enable it to share the device's internet connection. Other devices can access to internet via joining the hotspot.
4. Set Wi-Fi hotspot parameters.
   1) Enter **SSID** (hotspot name).
   2) Select **Security Mode** and **Encryption Type**.
   3) Set **Key**.
5. Check **DHCP**, and enter an IP address from the address pool that allows automatic obtaining.

Note

IP address and TCP/IP address have to be in different network segments.

6. Optional: Set DNS server address if you need to visit the device with domain name.
7. Click **Save**.

5.4 Connect to Platform

5.4.1 Connect to OTAP

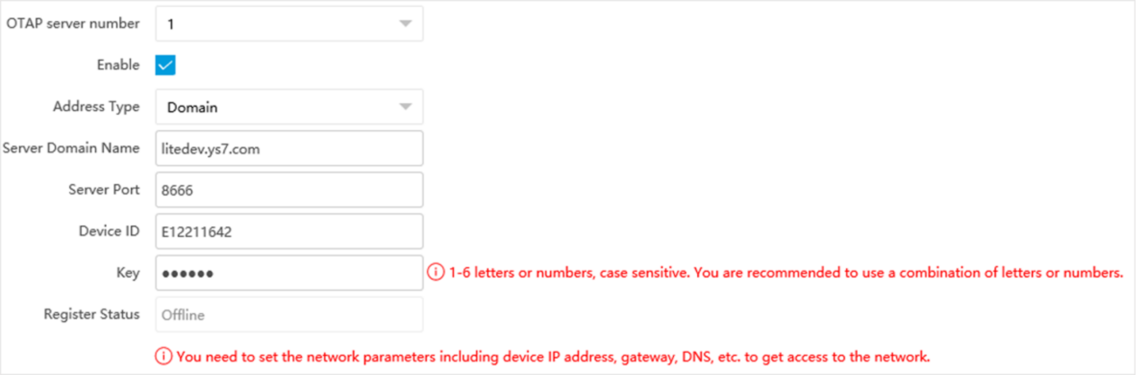
The device can be accessed to the maintenance platform via OTAP protocol, in order to search and acquire device information.

Before You Start

Ensure the device can communicate with the platform normally.

Steps

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



OTAP server number	1
Enable	☑
Address Type	Domain
Server Domain Name	litedev.ys7.com
Server Port	8666
Device ID	E12211642
Key	•••••• ⓘ 1-6 letters or numbers, case sensitive. You are recommended to use a combination of letters or numbers.
Register Status	Offline

ⓘ You need to set the network parameters including device IP address, gateway, DNS, etc. to get access to the network.

Figure 5-2 Connect to OTAP

3. Select **Address Type**.
4. Enter the server IP address/domain, port, and device ID.

Note

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

5. Enter **Key**.

Note

Enter the same **Key** on the platform.

6. Click **Save**.

What to do next

When the registration status is online, you can add or manage the device via the platform software. Refer to its corresponding manual for details.

5.4.2 Connect to Hik-Connect

The device can be remotely accessed via Hik-Connect.

Enable Hik-Connect Service on Radar

Hik-Connect service should be enabled on your radar before using the service. You can enable the service through Web browser.

Before You Start

- Connect the device to the Internet.
- Set the IP address, subnet mask, gateway, and DNS server of the LAN.

Steps

1. Go to **Configuration** → **Network** → **Data Connection** → **Hik-Connect Platform**.
2. Check **Enable**.
3. Select **Protocol Version**.
4. Optional: Check **Custom** to enter the deployed server IP address.
5. Click **Save**.

Note

Check the network connection if the **Register Status** is **Offline**.

What to do next

Use the Hik-Connect mobile client to add the device.

Set Up Hik-Connect

Steps

1. Get and install Hik-Connect application by the following ways.
   - Visit ***https://appstore.hikvision.com*** to download the application according to your mobile phone system.
   - Visit the official site of our company. Then go to **Support** → **Tools** → **Hikvision App Store**.
   - Scan the QR code below to download the application.

Figure 5-3 Hik-Connect

Note

If errors like "Unknown app" occur during the installation, solve the problem in two ways.

- Visit ***https://appstore.hikvision.com/static/help/index.html*** to refer to the troubleshooting.
- Visit ***https://appstore.hikvision.com/***, and click **Installation Help** at the upper right corner of the interface to refer to the troubleshooting.

2. Start the application and register for a Hik-Connect user account.
3. Log in after registration.

Add Radar to Hik-Connect

Before You Start

Ensure your radar and mobile device are on the same LAN.

Steps

1. Log in to the Hik-Connect app.
2. On the home page, tap **Add Device** to select an adding method.
   – **Scan QR Code**: Scan the QR/bar code on the radar body.
   – **Manual Adding**: Enter the serial number on the tag of the radar, and tap 💾.
3. Follow the prompts to set the network connection and add the radar to your Hik-Connect account.

Note

- In the **Verify Device** page, the password required is the one you set when activating the radar.
- For detailed information, refer to the user manual of the Hik-Connect app.

5.5 Set DDNS

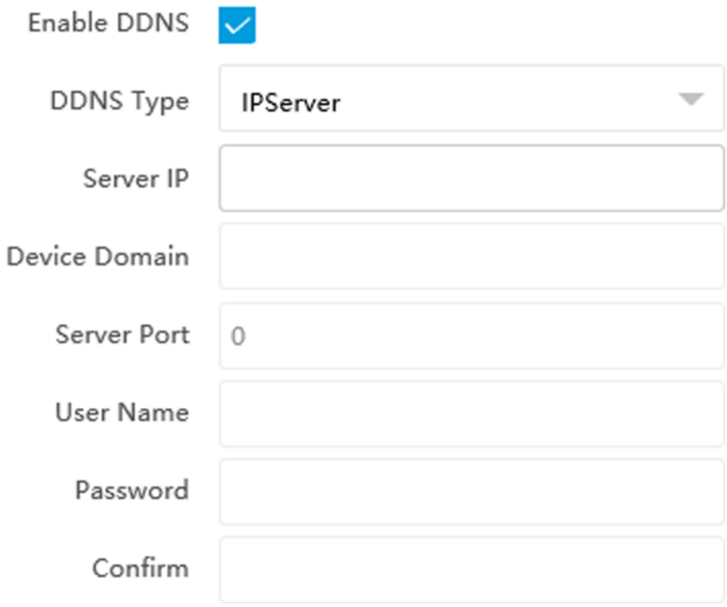
You can use the Dynamic DNS (DDNS) for network access. The dynamic IP address of the device can be mapped to a domain name resolution server to realize the network access via domain name.

Before You Start

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

Steps

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



Enable DDNS	☑
DDNS Type	IPServer
Server IP	
Device Domain	
Server Port	0
User Name	
Password	
Confirm	

Figure 5-4 Set DDNS

3. Enter the server address, domain, and other information.
4. Click **Save**.
5. Optional: Enter the domain name in the browser address bar to access the device.

5.6 Set SNMP

You can set the SNMP network management protocol to get the alarm event and exception messages in network transmission.

Before You Start

Download the SNMP software and manage to receive the device information via SNMP port.

Steps

1. Go to **Configuration** → **Network** → **Network Parameters** → **SNMP**.
2. Check **Enable SNMPv1/Enable SNMP v2c/Enable SNMPv3**.

Note

- The SNMP version you select should be the same as that of the SNMP software.
- Use different versions according to the security levels required. SNMP v1 is not secure and SNMP v2 requires password for access. SNMP v3 provides encryption and if you use the third version, HTTPS protocol must be enabled.

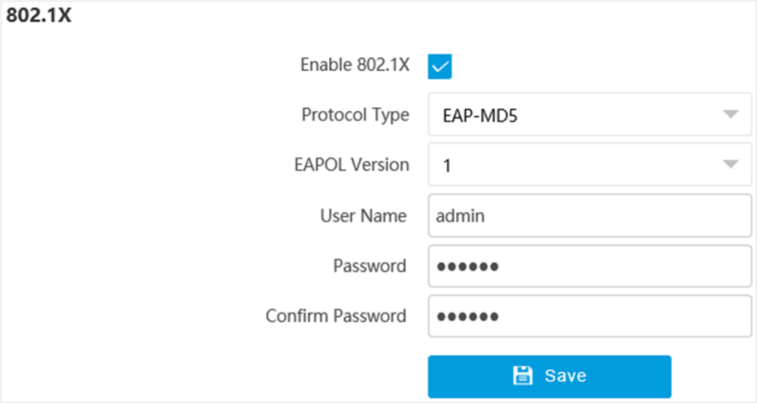
3. Set the SNMP parameters.
4. Click **Save**.

5.7 Set IEEE 802.1X

IEEE 802.1X is a port-based network access control. It enhances the security level of the LAN/WLAN. When devices connect to the network with IEEE 802.1X standard, the authentication is needed.

Steps

1. Go to **Configuration** → **Network** → **Network Parameters** → **802.1X**.
2. Check **Enable 802.1X**.



802.1X

Enable 802.1X ☑

Protocol Type: EAP-MD5

EAPOL Version: 1

User Name: admin

Password: ●●●●●●

Confirm Password: ●●●●●●

Figure 5-5 Set IEEE 802.1X

3. Select **Protocol Type** and **EAPOL Version**.

Protocol Type

The authentication server must be configured. Register a user name and password for 802.1X in the server in advance. Enter the user name and password for authentication.

EAPOL Version

The EAPOL version must be identical with that of the router or the switch.

4. Enter **User Name** and **Password** registered in the server.
5. Confirm the password.
6. Click **Save**.

5.8 Set Port

The device port can be modified when the device cannot access the network due to port conflicts.

Steps

1. Go to **Configuration** → **Network** → **Network Parameters** → **Port**.
2. You can view and edit the 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.

   HTTPS Port

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

   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.
3. Click **Save**.

Note

- After editing the port, access to the device via the new port.
- Reboot the device to bring the new settings into effect.

Chapter 6 Exception Alarm

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

Steps

1. Go to **Configuration** → **Event** → **Alarm Linkage** → **Exception**.
2. Select the exception type(s) according to the actual needs.
3. Click **Save**.

Chapter 7 Safety Management

7.1 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**.
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) Click **OK**.
4. Optional: You can do the following operations.

Edit the user information	Click ✏ to edit the user information.
Delete the user	Click 🗑 to delete the user.

7.2 Enable User Lock

To raise the data security, you are recommended to lock the current IP address.

Steps

1. Go to **Configuration** → **System** → **Security** → **Security Service** → **Software**.
2. Check **Enable User Lock**.
3. Click **Save**.

Result

When the times you entered incorrect passwords have reached the limit, the current IP address will be locked automatically.

7.3 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**.

7.4 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.

7.5 Set SSH

To raise network security, 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. Disable **SSH Service**.
3. Click **Save**.

7.6 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**.

7.7 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.

7.8 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**.

Chapter 8 Maintenance

8.1 View Device Information

Basic Information and Algorithms Library Version

Go to **Configuration** → **System** → **System Settings** → **Basic Information** to view the basic information 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.

8.2 Log

8.2.1 Enable System Log Service

The security audit logs refer to the security operation logs. You can search and analyze the security log files of the device so as to find out the illegal intrusion and troubleshoot the security events. Security audit logs can be saved on device internal storage. The log will be saved every half hour after device booting. Due to limited storage space, you are recommended to save the logs on a log server.

Steps

1. Go to **Configuration** → **System** → **Security** → **Security Service** → **Log Audit Service**.
2. Enable system log service.
3. Enter **IP Address** and **Port** of the log server.
4. Click **Save**.

Result

The device will upload the security audit logs to the log server regularly.

8.2.2 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**.

8.3 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.

8.4 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.

8.5 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**.

8.6 Set Serial Port

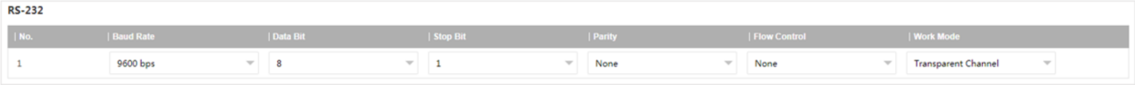
Set RS-232 parameters if you need to debug the device via RS-232 serial port.

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

No.	Baud Rate	Data Bit	Stop Bit	Parity	Flow Control	Work Mode
1	9600 bps	8	1	None	None	Transparent Channel

Figure 8-1 Set 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**.

8.7 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.

   ONVIF

   Select it to synchronize time via the third-party device.

   No

   Select it to disable time synchronization.

   All

   Select it, and you can select any mode above.
4. Click **Save**.

8.8 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**.

8.9 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**.

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

Result

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

8.11 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**.

8.12 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**.

See Far, Go Further