Smart Onboard Temperature Screening Terminal

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 LATER PREVAILS.

Regulatory Information

FCC Information

Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

FCC compliance: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

FCC Conditions

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

EU Conformity Statement

This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the EMC Directive 2014/30/EU, the LVD Directive 2014/35/EU, the RoHS Directive 2011/65/EU.

2012/19/EU (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: ***www.recyclethis.info***

2006/66/EC (battery directive): This product contains a battery that cannot be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. The battery is marked with this symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling, return the battery to your supplier or to a designated collection point. For more information see: ***www.recyclethis.info***

Industry Canada ICES-003 Compliance

This device meets the CAN ICES-3 (A)/NMB-3(A) standards requirements.

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 Product Introduction

The smart onboard temperature screening terminal (hereinafter referred to as "device" or "terminal") supports human body temperature screening, face recognition, and mask detection. It is embedded with close-distance lens with scanning function, convenient for the passengers to scan the payment code or the traveling allowable code.

The device is dedicated for the mobile scene, applicable to buses, coaches, etc.

1.2 Key Feature

- Thermal imaging lens to realize temperature screening.
- Detector with high sensitivity.
- Temperature screening with high accuracy.
- Face recognition.
- QR code scanning.

Chapter 2 Activation and Login

Note

The web operations in this chapter are only applicable to the face detection camera.

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 local menu, SADP software, web browser, and client software.

Note

Refer to the user manual of client software for the activation via client software.

2.1.1 Default Information

Device default IP address and user name are as follows.

- Default IP address: 192.168.48.19
- Default user name: admin.

2.1.2 Activate via SADP

SADP is a tool to detect, activate, and modify the IP address of the devices 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.

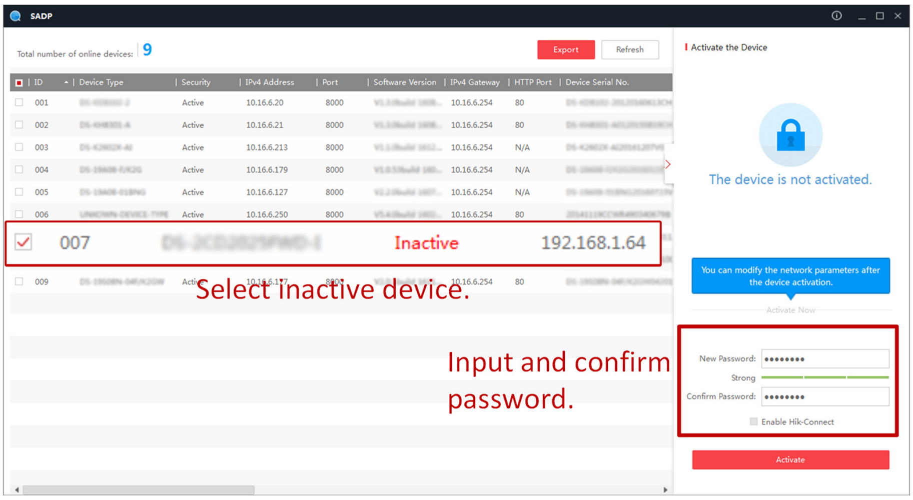
Steps

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	[redacted]	Active	10.16.6.20	8000	[redacted]	10.16.6.254	80	[redacted]
□ 002	[redacted]	Active	10.16.6.21	8000	[redacted]	10.16.6.254	80	[redacted]
□ 003	[redacted]	Active	10.16.6.213	8000	[redacted]	10.16.6.254	N/A	[redacted]
□ 004	[redacted]	Active	10.16.6.179	8000	[redacted]	10.16.6.254	N/A	[redacted]
□ 005	[redacted]	Active	10.16.6.127	8000	[redacted]	10.16.6.254	N/A	[redacted]
□ 006	[redacted]	Active	10.16.6.250	8000	[redacted]	10.16.6.254	80	[redacted]
☑ 007	[redacted]	Inactive	192.168.1.64					
□ 009	[redacted]	Active	10.16.6.177	8000	[redacted]	10.16.6.254	80	[redacted]

Select inactive device.

Activate the Device

The device is not activated.

You can modify the network parameters after the device activation.

Activate Now

New Password: ••••••••

Strong

Confirm Password: ••••••••

□ Enable Hik-Connect

Input and confirm password.

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**.
   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 connect to the same LAN.

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 Network Configuration

3.1 Connect to Network

Note

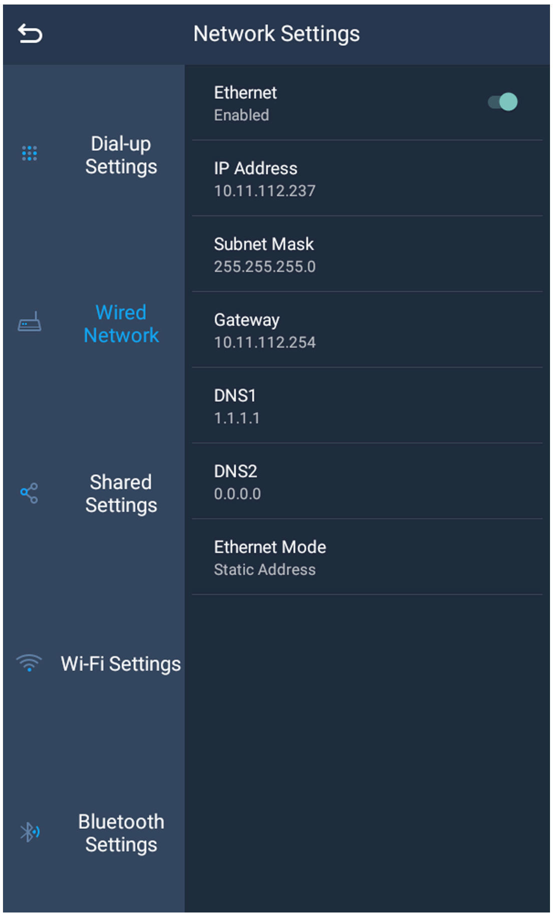
The bluetooth function is reserved.

3.1.1 Set Terminal IP Address

Set the IP address of the terminal before adding the face detection camera.

Steps

1. Tap **Network Settings → Wired Network** .



Ethernet
Enabled

IP Address
10.11.112.237

Subnet Mask
255.255.255.0

Gateway
10.11.112.254

DNS1
1.1.1.1

DNS2
0.0.0.0

Ethernet Mode
Static Address

Figure 3-1 Set Terminal IP Address

2. Enable **Ethernet**.
3. Set IP address.

Set IP address manually

a. Click **IP Address**.
b. Edit the IP address, gateway, and subnet mask according to the IP address network segment of the face detection camera.
c. Click **CONNECT**.

DHCP

If the device has been connected to the network which can get the IP address automatically via the network cable, you can select **Ethernet Mode** as **Dynamic Acquisition** to get the IP address automatically.

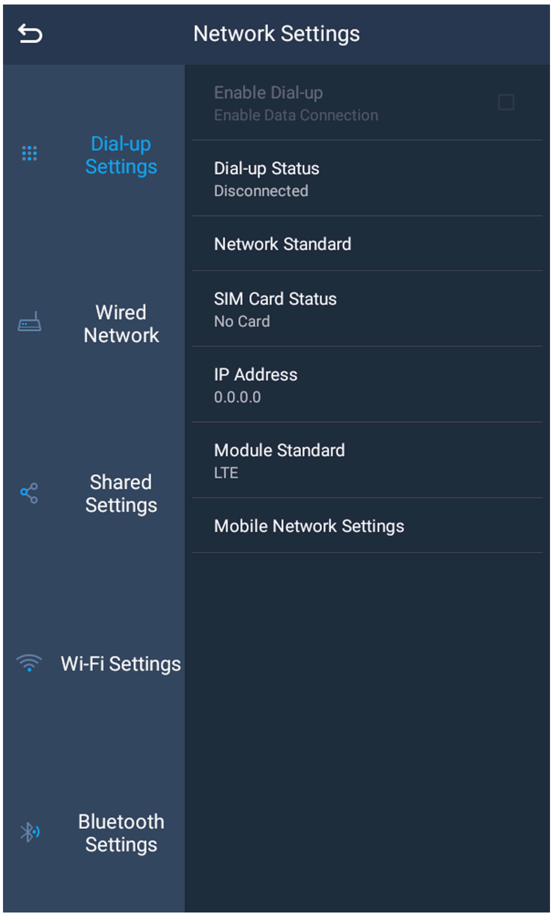
3.1.2 Dial

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

Before You Start
Install SIM card.

Steps

1. Tap **Network Settings → Dial-up Settings** .



Enable Dial-up □
Enable Data Connection

Dial-up Status
Disconnected

Network Standard

SIM Card Status
No Card

IP Address
0.0.0.0

Module Standard
LTE

Mobile Network Settings

Figure 3-2 Set Dial-up Parameters

2. Check **Enable Dial-up**.

3. Select **Network Standard** according to the actual needs.
4. Set the dial-up parameters.
   - When you connect the device to the normal network, you do not need to set the dial-up parameters.
   - When you connect the device to the private network, set the APN information, such as the user name, APN, etc.

Note

- Consult the operator about the dial-up parameters of the private network.
- When you have enabled 3G/4G and Wi-Fi simultaneously, the device will use Wi-Fi in priority.

5. **Optional:** Tap **Dial-up Status** to view the dial-up status.

3.1.3 Connect to Wi-Fi

Set Wi-Fi parameters to transmit data via wireless network.

Steps

1. Tap **Network Settings → Wi-Fi Settings** .

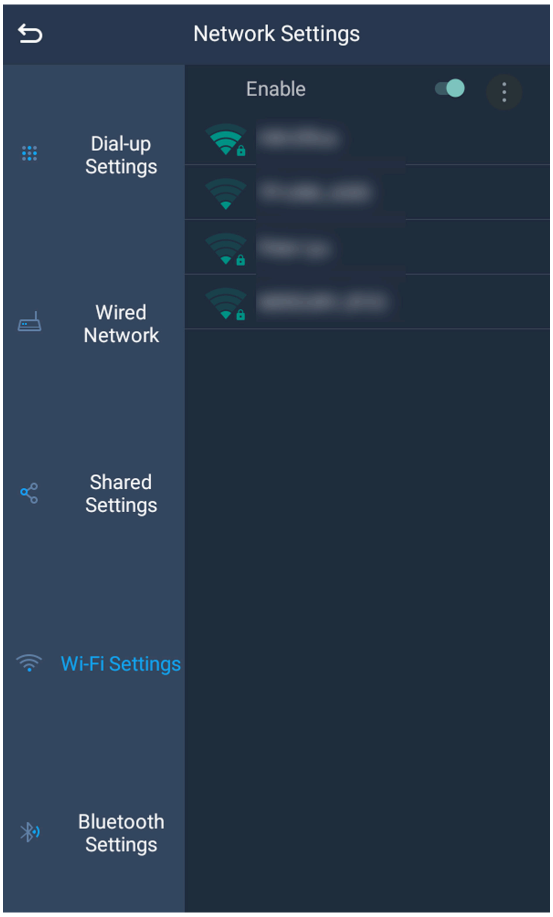


Figure 3-3 Connect to Wi-Fi

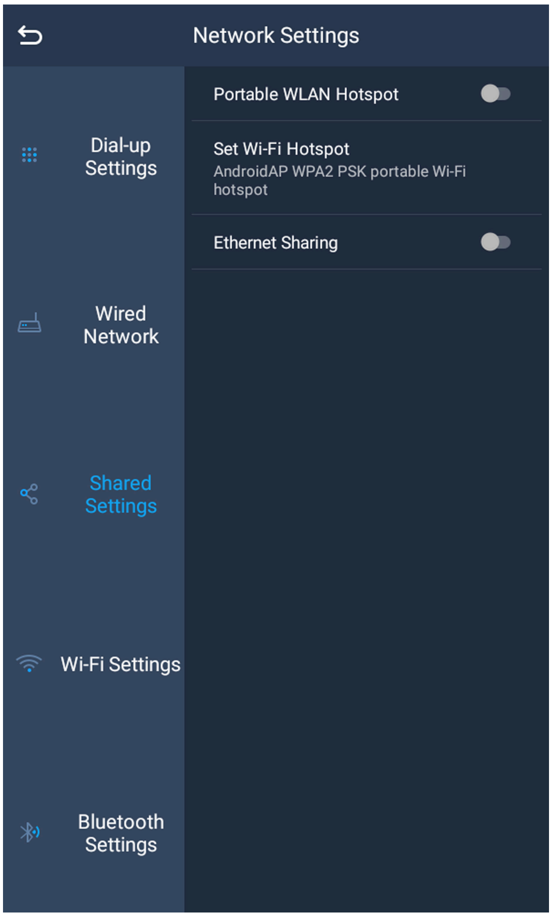
2. Enable Wi-Fi.
3. Select a Wi-Fi to connect.
4. Enter the password, and tap **CONNECT**.

3.2 Set Network Sharing

Set network sharing to share the device network to other terminals.

Steps

1. Tap **Network Settings → Shared Settings** .



Portable WLAN Hotspot ○

Set Wi-Fi Hotspot
AndroidAP WPA2 PSK portable Wi-Fi hotspot

Ethernet Sharing ○

Figure 3-4 Set Network Sharing

2. Select the sharing mode.

Share network via Wi-Fi
Enable **Portable WLAN Hotspot**. Set the SSID and password. Then the peripheral device can share the device network via Wi-Fi.

Share network via wired network
Enable **Ethernet Sharing**. Then the peripheral device can share the device network by connecting to the device network interface via the network cable.

Result

When the device connects to the network via dialing, the connected peripheral device can get access to the network either. In this condition, the device serves as a router.

Chapter 4 System Configuration

Note

- Refer to the user manual of the Android system for **Settings**, **Explorer**, and **Browser**.
- **Configuration** and **WIDGETS** are reserved functions.

4.1 Manage Files

Tap **Explorer** to manage files.

4.2 Enable Factory Test

You can enable factory test to check all the hardware functions of the device to troubleshoot.

Steps

1. Tap **Factory Test**.
2. Tap to run the factory test.
3. Exit from the page after all the tests finish.

Chapter 5 Operation via Client

5.1 Add Face Detection Camera via Client

Add the face detection camera to the client to start temperature screening and face detection.

Before You Start

The IP address of the terminal has been set.

Steps

1. Tap **4500b** on the main menu.
2. Tap ☰ → **Devices** .
3. Select the existed device.
4. Enter **Address**, **User Name**, and **Password** of the face detection camera.

   Note

   If the IP address of the face detection camera has been changed, enter the edited IP address.

5. Tap **Start Live View**.

Result

If live view succeeded, the camera is added, and you can start temperature screening and face detection. If live view failed, check the entered IP address and password.

5.2 Live View

After the face detection camera is added, tap ☰ → **Live View** to start temperature screening and face detection.

5.3 Set Parameters

Tap ☰ → **Configuration** to set the device parameters and view the client information.

Voice Broadcast

Enable the function, and the device will broadcast voice prompt during the temperature screening.

Code Scanning Supplement Light

Enable the function, and the supplement light will light on automatically when it inducts the QR code to make it convenient to scan the QR code.

Select Mode

Thermography Mode

Only the temperature screening function is enabled.

Customer Traffic Mode

Only the face recognition function is enabled.

All

Both the temperature screening and face recognition functions are enabled.

ACC

Set the delayed shutdown time. After the settings take effect, the device will shut down after the set time after the automobile is off.

Scheduled Startup

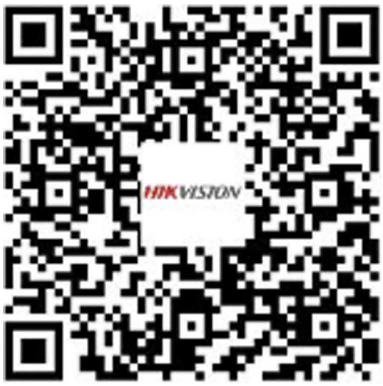
The device will start up automatically at the set time. If the device has been started up before the set time, the startup status will continue.

About

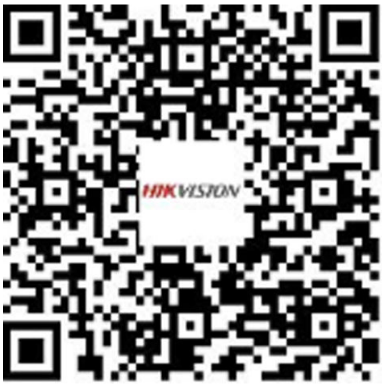
View the information such as the client version.

Appendix A. Communication Matrix and Device Command

Scan the QR code below to get the communication matrix of the device.



Scan the QR code below to get the device command.



See Far, Go Further