# Edge Storage Terminal

## Quick Start Guide

V1.0.1

# Foreword

## General

This manual introduces the installation, functions and operations of the 12-ch edge storage terminal (hereinafter referred to as "the Device"). Read carefully before using the Device, and keep the manual safe for future reference.

## Safety Instructions

The following signal words might appear in the manual.

| Signal Words | Meaning |
|---|---|
| DANGER | Indicates a high potential hazard which, if not avoided, will result in death or serious injury. |
| WARNING | Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury. |
| CAUTION | Indicates a potential risk which, if not avoided, could result in property damage, data loss, reductions in performance, or unpredictable results. |
| TIPS | Provides methods to help you solve a problem or save time. |
| NOTE | Provides additional information as a supplement to the text. |

## Revision History

| Version | Revision Content | Release Time |
|---|---|---|
| V1.0.1 | Updated "Important Safeguards and Warnings". | August 2022 |
| V1.0.0 | First Release. | February 2022 |

## Privacy Protection Notice

As the Device user or data controller, you might collect the personal data of others such as their face, fingerprints, and license plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

## About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between

the electronic version and the paper version.

- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the Device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

# Important Safeguards and Warnings

This section introduces content covering the proper handling of the Device, hazard prevention, and prevention of property damage. Read carefully before using the Device, and comply with the guidelines when using it.

## Transportation Requirements

- Pack the Device with packaging provided by its manufacturer or packaging of the same quality before transporting it.
- Transport the Device under allowed humidity and temperature conditions.

## Storage Requirements

Store the Device under allowed humidity and temperature conditions.

## Installation Requirements

 WARNING

- To avoid damage to the hard disk, the Device must be carefully installed in a horizontal position. The device must never be placed in an inclined or vertical position.
- Do not install the Device in locations where children are likely to be present.
- Do not connect the power adapter to the Device while the adapter is powered on.
- Strictly comply with the local electrical safety code and standards. Make sure the ambient voltage is stable and meets the power supply requirements of the device.
- Do not connect the Device to two or more kinds of power supplies, to avoid damage to the Device.
- Use the accessories suggested by the manufacturer. Installation and maintenance must be performed by qualified professionals.
- When using a laser beam device, avoid exposing the surface of the Device to laser beam radiation.

- Personnel working at heights must take all necessary measures to ensure personal safety including wearing a helmet and safety belts.
- Do not place the Device in a place exposed to sunlight or near heat sources.
- Keep the Device away from dampness, dust, and soot.
- Put the Device in a well-ventilated place, and do not block its ventilation.
- Use an adapter or cabinet power supply provided by the manufacturer.
- The power supply must conform to the requirements of ES1 in IEC 62368-1 standard and be no higher than PS2. Please note that the power supply requirements are subject to the Device label.
- The device is a class I electrical appliance. Make sure that the power supply of the Device is connected to a power socket with protective earthing.
- An emergency disconnect device must be installed during installation and wiring at a readily

accessible location for emergency power cut-off.

- Operating temperature: –30 °C to +65 °C (–22 °F to +149 °F).
- The rated current of the Device is 5 A and the rated power is 60 W (for device with a 4 T HDD).
- The power and communication port of the Device can sustain a surge of±6 KV in common mode and±4 KV in differential mode. Extra surge protection is required when the Device is connected to a circuit with higher surge levels.
- To ensure heat dissipation, the gap between the Device and the surrounding area should not be less than 50 mm on the sides and 50 mm on top of the Device.
- A safety circuit breaker is designed on the connector of the Device to cut the power of the Device. Make sure the breaker can be easily operated during installation.
- Only applicable for use in altitudes below 2,000 meters.
- Only applicable for use in non-tropical climates.

## Operation Requirements

**WARNING**

This is a class A product. In a domestic environment this may cause radio interference in which case you may be required to take adequate measures.

- Make sure that the power supply is correct before use.
- Do not unplug the power cord on the side of the Device while the adapter is powered on.
- Operate the Device within the rated range of power input and output.
- Use the Device under allowed humidity and temperature conditions.
- Do not drop or splash liquid onto the Device, and make sure that there is no object filled with liquid on the Device to prevent liquid from flowing into it.
- Do not disassemble the Device.
- We recommend you use the Device with a lightning protection device for stronger protection against lightning. For outdoor scenarios, strictly comply with the lightning protection regulations.
- Protect the line cord and wires from being walked on or squeezed particularly at plugs, power sockets, and the point where they exit from the Device.
- Do not block the ventilation near the Device.
- Do not vibrate, squeeze or immerse the Device in liquid.
- Ground the function earthing portion of the Device to improve its reliability. The device is a class I electrical appliance. Make sure that the power supply of the Device is connected to a power socket with protective earthing.
- Prevent water from flowing into the Device during on-site installation to avoid the risk of damage.
- Do not place an open flame on the Device, such as a lit candle.
- The device is applicable for DC power supplies with the negative pole grounded.
- Replace unwanted batteries with new batteries of the same type and model. To prevent explosion, replace the battery with the correct model and dispose of the old ones as instructed.
- Do not expose the battery to extremely hot environments, such as direct sunlight and fire.

## Maintenance Requirements

- Clean the Device with a soft dry cloth or a clean soft cloth dipped in neutral detergent.
- Use the accessories suggested by the manufacturer. Installation and maintenance must be performed by qualified professionals.
- Power off the Device before maintenance.
- Clean the dust off the circuit board, connectors and the cabinet to avoid the device short circuiting due to dampness.
- Make sure the Device is properly grounded to avoid being damaged by static electricity or induced voltage.
- Do not plug in or unplug RS-232, RS-485 and other ports while the power is on to avoid damage to the ports.
- Do not expose the Device to heat sources and high temperature environments. Keep the area around the Device cabinet well-ventilated.
- Regularly inspect and perform maintenance on the Device.

# Table of Contents

# 1 Appearance and Structure

## 1.1 Appearance

Figure 1-1 Device appearance

## 1.2 Front Panel

Figure 1-2 Front panel

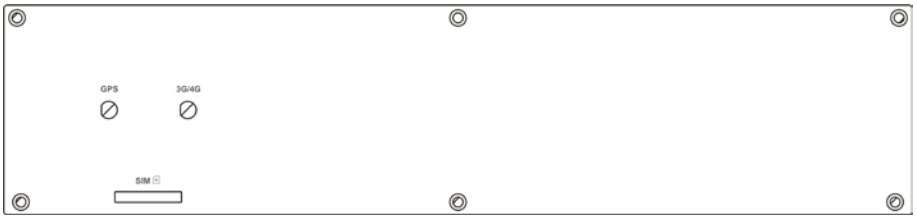



Table 1-1 Front panel ports

| Port | Description |
|---|---|
| 3G/4G | This antenna port can be used to enhance the signal when the Device is configured with the 3G/4G module. |
| GPS | This antenna port can be used when the Device is configured with the GPS module. Place the GPS antenna in an open area to enhance the signal when using it. |
| SIM | When the Device has 3G/4G module configured, you can insert the SIM card to use the 3G/4G function. |

# 1.3 Rear Panel

Figure 1-3 Rear panel

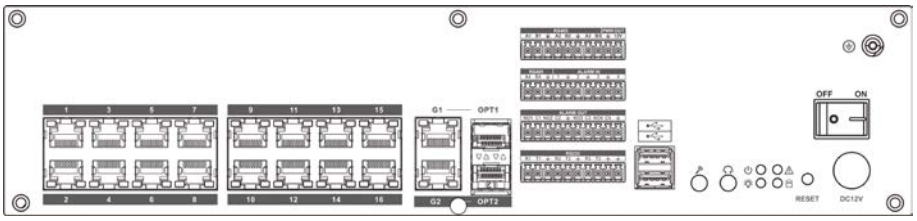



Table 1-2 Description of ports on rear panel

| Port | | Description |
|---|---|---|
| 1–16 | Network port | 16 RJ-45 self-adaptive Ethernet ports.<br>They are on the same network segment with G2. |
| G1/G2 | Dual NICs port | Two 1000 Mbps Ethernet ports.<br>They are physically separated, available for connecting to cameras and platforms on different network segments. |
| OPT1/OPT2 | Optical port | Two 1000 M SFP optical fiber ports.<br>OPT1 and G1, OPT2 and G2 are respectively on the same network segment. |
| | USB3.0 port | Connects with external USB storage devices. Reserved function. |
| | Audio input port | 1-channel audio input port. Reserved function. |
| | Audio output port | 1-channel audio output port. Reserved function. |
| | Power indicator | Displays the status of the power supply. Solid red means the Device is working normally. |
| | Operation indicator | Displays the operation status of the Device.<br>● Solid green: The Device runs normally.<br>● Flashes green: The Device is being upgraded. |
| | Alarm indicator | Display the alarm status of the Device.<br>● Solid red: The alarm is enabled.<br>● Flashes red: The alarm is triggered. |
| | HDD status indicator | Displays the status of HDD. The indicator flashes green when the HDD is exchanging data. |
| | Ground port | This port must be grounded to improve device reliability. Otherwise, the Device will lose its lightning protection function. |
| | Power button | Turns on/off the Device. |
| RESET | Reset button | Restores the Device to factory defaults.<br>Press and hold the button for more than 10 seconds when the Device is working, and the system configuration restores to factory defaults. |

| Port | | Description |
|---|---|---|
| DC 12V | 12 VDC power | Power port. |

Figure 1-4 Ports on the middle of rear panel

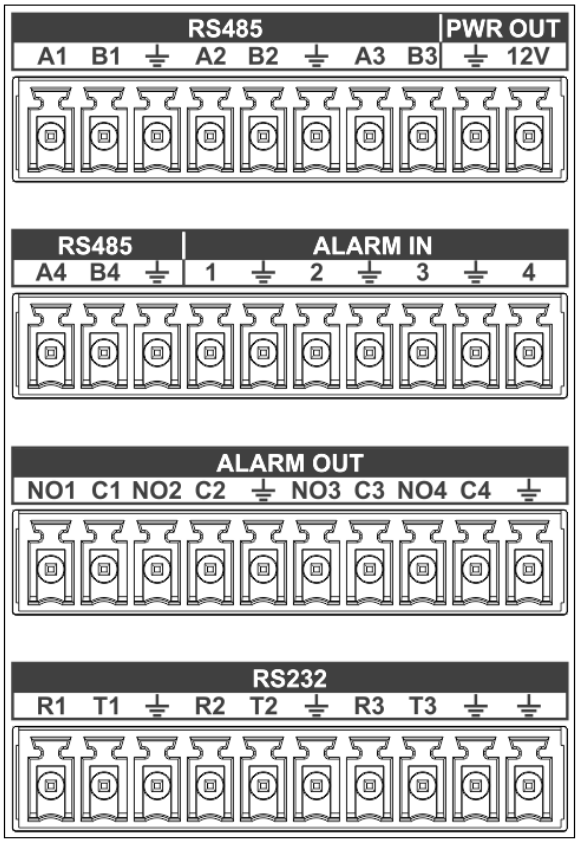



Table 1-3 Middle ports description

| Port Name | | Group | Description |
|---|---|---|---|
| PWR OUT | 12 V | — | Power output port. |
| | ⏚ | — | Ground. |
| RS485 | Four sets of RS-485 ports. | A1, B1 | • A1, A2, A3, A4: RS-485_A port.<br>• B1, B2, B3, B4: RS-485_B port. |
| | | A2, B2 | |
| | | A3, B3 | |
| | | A4, B4 | |
| ALARM IN | 4-channel alarm input port | 1 | Receives switch quantity signals from external alarm sources.<br>• 1, 2, 3, 4: alarm input ports.<br>• ⏚: alarm input ground terminal. |
| | | 2 | |
| | | 3 | |
| | | 4 | |
| | | ⏚ | |
| ALARM OUT | 4-channel alarm output port | NO1, C1 | Outputs alarm signals to external alarm devices that must have power supply.<br>• NO1, NO2, NO3, NO4: normally open alarm output ports.<br>• C1, C2, C3, C4: common alarm output ports. |
| | | NO2, C2 | |
| | | NO3, C3 | |
| | | NO4, C4 | |

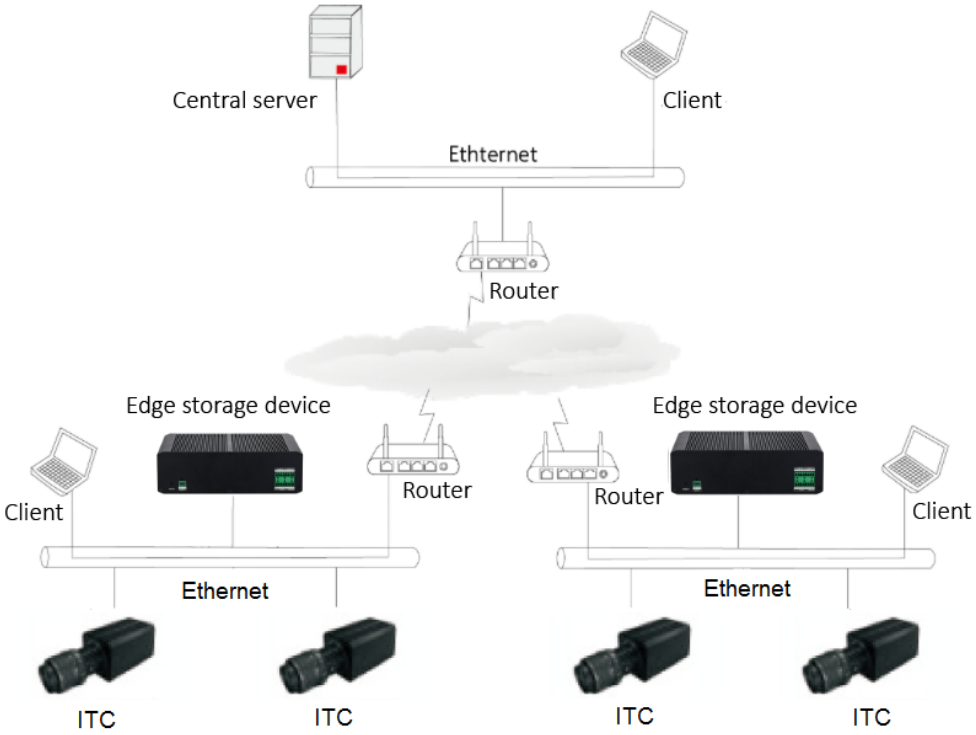
| Port Name | | Group | Description |
|---|---|---|---|
| RS232 | 3 sets of RS-232 ports | R1, T1 | • R1, R2, R3: RS-232 serial port receivers.<br>• T1, T2, T3: RS-232 serial port senders. |
| | | R2, T2 | |
| | | R3, T3 | |

# 2 System Networking

In the system networking, the central server and the monitoring point (where the camera is located) must be connected to network, but there is no need to lay network cables from the central server to the monitoring point.

The Device is designed to store high-definition encoded videos and pictures transmitted by cameras, save the information of passed vehicles, and upload them to the central server for unified management.

Figure 2-1 System networking



# 3 Quick Configuration

You can use the ConfigTool to quickly configure the Device, including initialization, system update and web client login.

- The operation pages vary depending on different versions.
- Get the ConfigTool installation package from technical support and install it on your local computer.

## 3.1 Initializing the Device

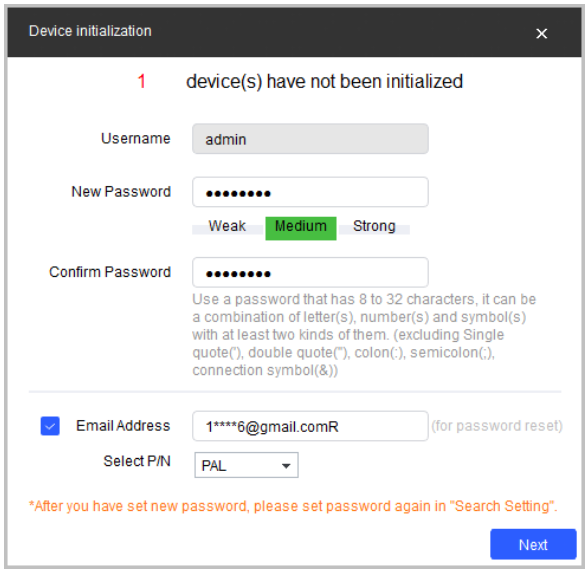
You can initialize the Device, and cameras connected to the Device in batches through the ConfigTool.

Uninitialized devices are not available for any operations and are displayed in gray on the device list.

Step 1 Start the ConfigTool, and then click **Modify IP**.
The ConfigTool automatically searches for devices on the same network segment with the computer.

Step 2 Select a device to be initialized, and then click **Initialize**.

Figure 3-1 Device initialization




Step 3 Set and confirm the password, and enter an email for future password reset.

The pages are for reference only, and might differ from the actual page.

Step 4 Click **Initialize**, and the system starts initializing the Device.
is displayed for successful initialization, and is displayed for initialization failure. Click the icon to view details.

Step 5 Click **Finish**.

## 3.2 Changing IP Address

You can acquire and change the IP address of devices accessed through wired network. This section uses changing IP address with the ConfigTool as the example.

Step 1 Get the ConfigTool from technical support and install it on your local computer.

Step 2 Start the ConfigTool.

Step 3 Click **Modify IP**.

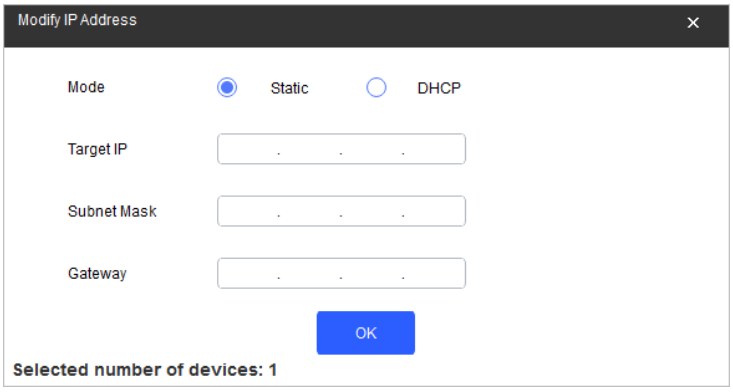
Step 4 Select the device(s) whose IP need(s) to be changed.

- Change one IP address: Click **Edit** corresponding to the device.
- Change IP addresses in batches: Select the devices, and then click **Batch Modify IP**.

Step 5 Set mode, IP, subnet mask and gateway.

Step 6 Click **OK**.

Figure 3-2 Change IP addresses in batches




## 3.3 Updating the Device

Single upgrade and batch upgrade are supported.

Step 1 Start the ConfigTool.

Step 2 Click **Device Upgrade**.

Step 3 Select the Device to be updated.

- Update one by one: Click corresponding to the Device.
- Update in batches: Select multiple devices, and then click **Batch Upgrade**.

Step 4 Select the update file.

Step 5 Update the Device.

- Update one by one: Click to start updating.
- Update in batches: Click **OK** to start updating.

During update, if the Device is disconnected, as long as the ConfigTool stays on the update page, the upgrade will continue when the Device is reconnected.

## 3.4 Logging in to Webpage

On the **Modify IP** page, click **Web** corresponding to the Device, and then you are directed to the

login page of the webpage. Enter the login username and password to log in.

# Appendix 1 Cybersecurity Recommendations

**Mandatory actions to be taken for basic device network security:**

1. **Use Strong Passwords**

   Please refer to the following suggestions to set passwords:

   - The length should not be less than 8 characters.
   - Include at least two types of characters; character types include upper and lower case letters, numbers and symbols.
   - Do not contain the account name or the account name in reverse order.
   - Do not use continuous characters, such as 123, abc, etc.
   - Do not use overlapped characters, such as 111, aaa, etc.

2. **Update Firmware and Client Software in Time**

   - According to the standard procedure in Tech-industry, we recommend to keep your device (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the device is connected to the public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
   - We suggest that you download and use the latest version of client software.

**"Nice to have" recommendations to improve your device network security:**

1. **Physical Protection**

   We suggest that you perform physical protection to device, especially storage devices. For example, place the device in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable device (such as USB flash disk, serial port), etc.

2. **Change Passwords Regularly**

   We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

3. **Set and Update Passwords Reset Information Timely**

   The device supports password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

4. **Enable Account Lock**

   The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

5. **Change Default HTTP and Other Service Ports**

   We suggest you to change default HTTP and other service ports into any set of numbers between 1024–65535, reducing the risk of outsiders being able to guess which ports you are using.

6. **Enable HTTPS**

   We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

7. **MAC Address Binding**

   We recommend you to bind the IP and MAC address of the gateway to the device, thus reducing

the risk of ARP spoofing.

8. **Assign Accounts and Privileges Reasonably**
   According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.
9. **Disable Unnecessary Services and Choose Secure Modes**
   If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.
   If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:
   - SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
   - SMTP: Choose TLS to access mailbox server.
   - FTP: Choose SFTP, and set up strong passwords.
   - AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.
10. **Audio and Video Encrypted Transmission**
    If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.
    Reminder: encrypted transmission will cause some loss in transmission efficiency.
11. **Secure Auditing**
    - Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
    - Check device log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.
12. **Network Log**
    Due to the limited storage capacity of the device, the stored log is limited. If you need to save the log for a long time, it is recommended that you enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.
13. **Construct a Safe Network Environment**
    In order to better ensure the safety of device and reduce potential cyber risks, we recommend:
    - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
    - The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
    - Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
    - Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.