

**Conference TV terminal**

**Quick Start Guide**

V1.0.0

Foreword

General

This document describes the installation and connection of the video conference endpoint.

Symbols

The following symbols may appear in this document and their meanings are as follows:

| Symbol | Description |
| --- | --- |
|  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, lower performance, or unpredictable result. |
|  Prevent Static | Indicates a static-sensitive device. |
|  Electric Shock | Indicate a potential high voltage hazard. |
| Laser Radiation | Indicate intense laser radiation. |
|  Tips | Provide methods to help you solve a problem or save your time. |
|  Notes | Provide additional information as the emphasis and supplement to the text. |

Revision History

| Version | Revision Content | Release Date |
| --- | --- | --- |
| V1.0.0 | V4.0 First Release | December 2023 |

Important Safeguards and Warnings

The following section describes how to use this product correctly and how to prevent dangers and property loss when using it. Before using this product, read this Guide carefully and comply with it strictly. Keep this Guide properly after reading.

Requirements

● There is high voltage in the device, non-professionals should not open the back cover to prevent the risk of electric shock.

● Do not place or install the device in a place exposed to sunlight or near the heat source.

● Keep the device away from dampness, dust or soot.

● Please install the device in a well-ventilated place and do not block the ventilation openings of the device.

● Place the device stably on a platform with sufficient strength to prevent the device from falling and causing damage.

● Do not drip or splash liquid onto the device. Make sure that the device does not bear any objects filled with liquid to prevent liquid from flowing into the device.

● Use the device only within the rated input and output range.

● Do not dismantle the device arbitrarily.

● Please transport, use and store the device within the permitted humidity and temperature range.

● Cut off the power before cleaning the device. Do not use the liquid cleaner or spray cleaner during the cleaning process.

● When cleaning the display surface, use a clean, soft cloth or a special lens wipe. Do not wipe with a damp cloth, otherwise, it may cause damage to the display.

Power Source

● Make sure to use the battery as required, otherwise it may cause the battery to catch fire, explode or burn!

● When replacing batteries, only use batteries of the same type!

● Make sure to use the standard power adapter of the device, otherwise the user shall be responsible for personal injury or equipment damage.

● The product must use the cord sets (power cords) recommended for this region and use them within its rated specifications!

● Make sure all cables are connected correctly before turning on the power. Do not overload the power socket or pull the power cord, otherwise, it may cause dangers such as fire and electric shock.

● Please connect the products of the class I structure to the grid power output socket with the protective grounding connection.

● The appliance coupler is a disconnect device, please keep it at an angle that is convenient for operation during normal use.

Table of Contents

[Foreword II](#_Toc154677695)

[Important Safeguards and Warnings III](#_Toc154677696)

[1 Product Overview 2](#_Toc154677697)

[1.1 Product Description 2](#_Toc154677698)

[1.2 Product Features 2](#_Toc154677699)

[2 Product Structure 3](#_Toc154677700)

[2.1 Front Panel 3](#_Toc154677701)

[2.2 Rear Panel 3](#_Toc154677702)

[2.3 Networking graph 4](#_Toc154677703)

[2.4 Remote controller 5](#_Toc154677704)

[3 Product List 6](#_Toc154677705)

[3.1 Product List 6](#_Toc154677706)

[3.2 Installation 7](#_Toc154677707)

[3.2.1 Desktop Mounting 7](#_Toc154677708)

[3.2.2 Wall Mounting 7](#_Toc154677709)

[3.2.3 Ceiling Mounting 8](#_Toc154677710)

[Legal Notices 10](#_Toc154677711)

[Cyber Security Advice 12](#_Toc154677712)

# Product Overview

## Product Description

This product is a next-generation 4K Ultra HD modular conference terminal with rich audio and video interfaces and multi-angle transmission capabilities. It supports the connection of 4K Ultra HD cameras and provides multiple streams of 4K ultra-clear video and OPUS wideband audio. It is an ideal choice for large-scale video conference integration projects, delivering an ultimate face-to-face communication experience to users.

## Product Features

* Integrated design with built-in 4K camera and codec.
* Supports 4K 30fps video capture with 12x optical zoom and an 80° horizontal field of view.
* Supports 4K 30fps dual-stream conferences.
* Supports OPUS audio encoding with a sampling frequency of 48kHz.
* Supports connection of omnidirectional microphones.
* Supports infrared remote control, mouse, keyboard, and other peripheral devices for control.
* Supports multiple installation methods, including wall-mount, ceiling-mount, and hanging.

# Product Structure

## Front Panel

Front Panel



## Rear Panel

Rear Panel



## Networking graph

Networking graph



## Remote controller

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Remote controller | Buttons

| No. | Icon | Meaning |
| --- | --- | --- |
| 1 |  | Status indicator. |
| 2 |  | The output volume adjustment button. |
|  | Mic on/off switch. |
|  | Camera focus adjustment button. |
|  | Menu direction selection button, camera direction adjustment button. |
|  | Up, down, left, right buttons. |
|  | OK button. |
|  | Remote camera button. |
|  | Camera selection button. |
|  | After the device is correctly connected to a laptop, the demo stream can be sent by pressing this button once. |
| 3 |  | Button for switching local image layout. |
|  | "Return" button. When this button is pressed, the menu returns to the previous interface or operation. |
|  | Menu button. When this button is pressed, the expanded functions interface or the main menu appears. |
|  | Backspace button/Deletion button. |
|  | Dialing button. When this button is pressed, the menu goes to the dialing interface or the number is dialed. |
|  | The button for hanging up the meeting, powering on/off the device. |

 |

# Product List

## Product List

Before installation, check the items in the package according to table3-1

Product List

| Item | Name | Quantity | Description |
| --- | --- | --- | --- |
| 1 | Terminal Host | 1 unit | The main device of the terminal. |
| 2 | Host Bracket Component | 1 piece | Used for mounting the terminal. |
| 3 | Remote Control | 1 unit | Used for remote control of the terminal. |
| 4 | Power Adapter | 1 unit | Used to connect the device to power. |
| 5 | Power Cord  | 1 piece |
| 6 | Standard External Cable - HDMI Cable, High-End 19-Core Male to Male - Black - 2000mm | 1 piece | Audio-video cable. |
| 7 | Standard External Cable - CAT5E UTP Network Cable (Multi-core Copper, Black) - 5m | 1 piece | Used to connect the device to the network. |
| 8 | Standard External Cable - Serial Cable (DB9F to Mini USB Male) - Black - 2000mm | 1 piece | Debugging cable. |
| 9 | M3×8 Cross-Slot Pan Head Machine Tooth Combination Screw | 4 pieces | Used for wall-mounting the terminal device. |
| 10 | Screw Package | 1 pack |
| 11 | Product Documentation QR Code | 1 sheet | Guides users for quick device connection and use of the video terminal device. |
| 12 | Qualification Certificate & Warranty Card & Hazardous Substance Content List | 1 copy | Product ualification certificate, warranty card, and hazardous substance content list. |

## Installation

The endpoint has three ways of installation: Desktop Mounting, Wall Mounting and Ceiling Mounting.

### 3.2.1 Desktop Mounting

When the thickness of the monitor is less than or equal to 170mm, you can choose to mount the video terminal product on the monitor. The specific installation steps are shown in Figure 3-1.

Desktop Mounting



### 3.2.2 Wall Mounting

When the thickness of the monitor is more than 170mm or it needs to be mounted on the wall, the wall mounting method can be selected. The specific installation steps are shown in Figure 3-2.

 Wall Mounting



### 3.2.3 Ceiling Mounting

Notes

Ceiling brackets are sold separately.

When the endpoint cannot be mounted on the monitor or on the wall, you can choose the method of ceiling mounting. The specific installation steps are shown in Figure 3-3.

Ceiling Mounting



Legal Notices

Trademark Statement

● VGA is a trademark of IBM Corporation.

● The Windows logo and Windows are trademarks or registered trademarks of Microsoft Corporation.

● Other trademarks or company names that may be mentioned in this document are the property of their respective owners.

Responsibility Statement

● To the extent permitted by applicable law, under no circumstances shall the company make any compensation for any special, incidental, indirect, consequential damages arising from the relevant content and products described in this document, nor shall it be liable for any compensation for loss of profits, data, goodwill, loss of documentation or anticipated savings.

● The products described in this document are provided "as is", and unless required by applicable law, the company makes no warranties, express or implied, with respect to all contents in this document, including but not limited to merchantability, satisfactory quality, fitness for a particular purpose, Guarantees such as non-infringement of third-party rights.

Privacy Protection Reminder

After you install our product, we may collect personal information such as the face, fingerprint, license plate, email, phone, GPS, etc. In the process of using the product, you need to comply with the privacy protection laws and regulations of the region or country where you are located to protect the legitimate rights and interests of others. For example, you may need to provide clear and visible signs, inform relevant rights holders of the existence of video surveillance areas, and provide corresponding contact information.

About the Document

● This document is used for multiple models of products. Please refer to the actual product for the appearance and function of the product.

● Any damage caused by not following the instructions in this document is the responsibility of the user.

● The contents of this document will be updated in real-time according to the laws and regulations of the relevant regions. For details, please refer to the paper, electronic CD, QR code, or official website of the product. If the contents of the paper and electronic files are inconsistent, the electronic files shall prevail.

● The company reserves the right to revise any information in this document at any time, and the revised content will be added to the new version of this document without prior notice.

● This document may contain technical inaccuracies, inconsistencies with product functions and operations, or typographical errors, subject to the company's final interpretation.

● If the obtained PDF document cannot be opened, please use the latest version or the most mainstream reading tool.

Cyber Security Advice

**Necessary measures to ensure basic network security of equipment:**

**1. Use complex passwords**

Please refer to the following suggestions for password setting:

● Not less than 8 characters in length.

● Contains at least two-character types, including uppercase and lowercase letters, numbers, and symbols.

● Does not contain account names or reverse order of account names.

● Do not use consecutive characters like 123, abc, etc.

● Don't use same characters including 111, aaa, etc.

**2. Update firmware and client software in time**

● According to the standard operating practices of the technology industry, the firmware of the device needs to be updated to the latest version in time to ensure that the device has the latest functions and security. When the device is connected to the public network, it is recommended to enable the online upgrade automatic detection function, so as to obtain the firmware update information released by the manufacturer in time.

● It is recommended that you download and use the latest version of the client software.

**Recommended actions to enhance device network security:**

**1. Physical Protection**

It is recommended that you physically protect devices (especially storage devices), such as placing devices in dedicated computer rooms and cabinets and managing access rights and keys to prevent unauthorized personnel from destroying hardware and external devices such as U disks, serial ports, and other physical contact behaviors.

**2. Change your password regularly**

It is recommended that you change your password regularly to reduce the risk of being guessed or cracked.

**3. Set and update password reset information in time**

The device supports the password reset function. To reduce the risk of this function being exploited by attackers, please set up password reset-related information in time, including reserved mobile phone number/email address and security questions. If the information changes, please modify it in time. When setting up secret questions, it is recommended not to use easy-to-guess answers.

**4. Enable account lockout**

The account lock function is enabled by default at the factory. It is recommended that you keep it enabled to protect account security. After the attacker fails multiple password attempts, the corresponding account and source IP will be locked.

**5. Change the default port for HTTP and other services**

It is recommended that you change the default port of HTTP and other services to any port between 1024 and 65535 to reduce the risk of attackers guessing the service port.

**6. Enable HTTPS**

It is recommended that you enable HTTPS to access web services through a secure channel.

**7. Enable whitelisting**

It is recommended that you enable the whitelist function. After enabling, only the IPs in the whitelist are allowed to access the device. Therefore, please be sure to add your computer IP address and the IP address of the supporting device to the whitelist.

**8. MAC address binding**

It is recommended that you bind the IP and MAC addresses of the gateway device on the device side to reduce the risk of ARP spoofing.

**9. Reasonable allocation of accounts and permissions**

According to business and management needs, reasonably add users, and reasonably assign minimum permission sets to them.

**10. Turn off non-essential services and use safe mode**

● If it is not required, it is recommended that you disable SNMP, SMTP, UPnP and other functions to reduce the risk to the device.

● If necessary, it is strongly recommended that you use safe mode, including but not limited to:

◇ SNMP: Select SNMP v3 and set a complex encryption password and authentication password.

◇ SMTP: Select TLS to access the email server.

◇ FTP: Select SFTP and set a complex password.

◇ AP hotspot: Select WPA2-PSK encryption mode and set a complex password.

**11. Audio and video encrypted transmission**

If your audio and video data contain important or sensitive content, it is recommended to enable encrypted transmission to reduce the risk of audio and video data being stolen during transmission.

**12. Use PoE to connect devices**

If the device supports the PoE function, it is recommended to use PoE to connect the device to isolate the camera from other networks.

**13. Security Audit**

● Check online users: It is recommended that you check online users from time to time to identify whether there are illegal users logging in.

● View device log: By viewing the log, you can learn the IP information of the device trying to log in, as well as the key operation information of the logged-in user.

**14. Weblogs**

Due to the limited storage capacity of the device, the log storage capacity is limited. If you need to store logs for a long time, it is recommended that you enable the network log function to ensure that key logs are synchronized to the network log server to facilitate problem tracing.

**15. Construction of a secure network environment**

To better ensure device security and reduce network security risks, it is recommended that you:

● Disable the router port mapping function to prevent the external network from directly accessing the services of the router's internal network devices.

● According to the actual network needs, partition the network: If there is no communication requirement between the two subnets, it is recommended to use VLAN, gatekeeper, etc. to divide the network to achieve the effect of network isolation.

● Establish an 802.1x access authentication system to reduce the risk of illegal terminals accessing the private network.

● Enable the firewall or blacklist function of the device to reduce the risk of possible attacks on the device.