Quick Guide

YVR-120
YVR-121
YVR-122

2023/08/16

ACTi
Connecting Vision

Table of Contents

Preface

Thank you for purchasing our product. If you have any questions or feedback, please contact your local dealer. Without the written permission of the company, no part of this manual may be reproduced, reproduced, translated, or distributed in any form or by any means. The contents of this manual are subject to change without notice. No statement, information or advice in this brochure shall create a formal warranty of any kind, express or implied.

About This Manual

- This manual is intended for multiple product models, and the photos, illustrations, descriptions, etc, in this manual may be different from the actual appearances, functions, features, etc, of the product.
- This manual is intended for multiple software versions, and the illustrations and descriptions in this manual may be different from the actual user interface and functions of the software.
- Despite our best efforts, technical or typographical errors may exist in this manual. The manufacturer cannot be held responsible for any such errors and reserves the right to change the manual without prior notice.
- Users are fully responsible for the damages and losses that arise due to improper operation.
- The manufacturer reserves the right to change any information in this manual without any prior notice or indication. Due to such reasons as product version upgrade or regulatory requirement of relevant regions, this manual will be periodically updated.

Safety Information

Please read the instructions carefully before starting installation and operation.

- Installation and maintenance must be performed by qualified personnel.
- This equipment is a Class A product and may cause radio interference. Take action if necessary.
- Disconnect power before installing and connecting cables. Wear antistatic gloves during installation. Please use the battery recommended by the manufacturer. Improper use or replacement of battery may present a risk of explosion. Dispose of used batteries according to local regulations or the battery manufacturer's instructions. Never throw batteries into fire.
- This device is intended for indoor use only. Ensure correct operating environment, including temperature, humidity, ventilation, power supply and lightning protection. Equipment must always be properly grounded. Keep the device away from dust, excessive vibration, any liquid, and strong electromagnetic radiation. Sudden power failure may result in damage to the device or loss of data.
- Take necessary steps to ensure data security and protect it from cyber-attacks and hackers (when connected to the Internet).

Disclaimer of Liability

- To the extent allowed by applicable law, in no event will the manufacturer be liable for any special, incidental, indirect, consequential damages, nor for any loss of profits, data, and documents.
- The product described in this manual is provided on an "as is" basis. Unless required by applicable law, this manual is only for informational purpose, and all statements, information, and recommendations in this manual are presented without warranty of any kind, expressed or implied, including, but not limited to, merchantability, satisfaction with quality, fitness for a particular purpose, and noninfringement.
- Users must assume total responsibility and all risks for connecting the product to the Internet, including, but not limited to, network attack, hacking, and virus. The manufacturer strongly recommends that users take all necessary measures to enhance the protection of network, device, data and personal information. The manufacturer disclaims any liability related thereto but will readily provide necessary security related support.
- To the extent not prohibited by applicable law, in no event will the manufacturer and its employees, licensors, subsidiary, affiliates be liable for resuelts arising out of using or inability to use the product or service, including, not limited to, loss of profits and any other commercial damages or losses, loss of data, procurement of substitute goods or services; property damage, personal injury, business interruption, loss of business information, or any special, direct, indirect, incidental, consequential, pecuniary, coverage, exemplary, subsidiary losses, however caused and on any theory of liability, whether in contract, strict liability or tort (including negligence or otherwise) in any way out of the use of the product, even if the manufacturer has been advised of the possibility of such damages (other than as may be required by applicable law in cases involving personal injury, incidental or subsidiary damage).
- To the extent allowed by applicable law, in no event shall the manufacturer’s total liability to you for all damages for the product described in this manual (other than as may be required by applicable law in cases involving personal injury) exceed the amount of money that you have paid for the product.

Network Security

Please take all necessary measures to enhance network security for your device.

The following are necessary measures for the network security of your device:

- Change default password and set strong password: You are strongly recommended to change the default password after your first login and set a strong password of at least nine characters including all three elements: digits, letters and special characters.
- Keep firmware up to date: It is recommended that your device is always upgraded to the latest version for the latest functions and better security. Visit the manufacturer’s official website or contact your local dealer for the latest firmware.

The following are recommendations for enhancing network security of your device:

- Change password regularly: Change your device password on a regular basis and keep the password safe. Make sure only the authorized user can log in to the device.

- Enable HTTPS/SSL: Use SSL certificate to encrypt HTTP communications and ensure data security.
- Enable IP address filtering: Allow access only from the specified IP addresses.
- Minimum port mapping: Configure your router or firewall to open a minimum set of ports to the WAN and keep only the necessary port mappings. Never set the device as the DMZ host or configure a full cone NAT.
- Disable the automatic login and save password features: If multiple users have access to your computer, it is recommended that you disable these features to prevent unauthorized access.
- Choose username and password discreetely: Avoid using the username and password of your social media, bank, email account, etc, as the username and password of your device, in case your social media, bank and email account information is leaked.
- Restrict user permissions: If more than one user needs access to your system, make sure each user is granted only the necessary permissions.
- Disable UPnP: When UPnP is enabled, the router will automatically map internal ports, and the system will automatically forward port data, which results in the risks of data leakage. Therefore, it is recommended to disable UPnP if HTTP and TCP port mapping have been enabled manually on your router.
- SNMP: Disable SNMP if you do not use it. If you do use it, then SNMPv3 is recommended.
- Multicast: Multicast is intended to transmit video to multiple devices. If you do not use this function, it is recommended you disable multicast on your network.
- Check logs: Check your device logs regularly to detect unauthorized access or abnormal operations.
- Physical protection: Keep the device in a locked room or cabinet to prevent unauthorized physical access.
- Isolate video surveillance network: Isolating your video surveillance network with other service networks helps prevent unauthorized access to devices in your security system from other service networks.

Regulatory Compliance

FCC Statements

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, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Caution: The user is cautioned that changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

NOTE: 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.

LVD/EMC Directive

CE This product complies with the European Low Voltage Directive 2014/35/EU and EMC Directive 2014/30/EU.

WEEE Directive–2012/19/EU

The product this manual refers to is covered by the Waste Electrical & Electronic Equipment (WEEE) Directive and must be disposed of in a responsible manner.

WEEE Directive–2013/56/EU

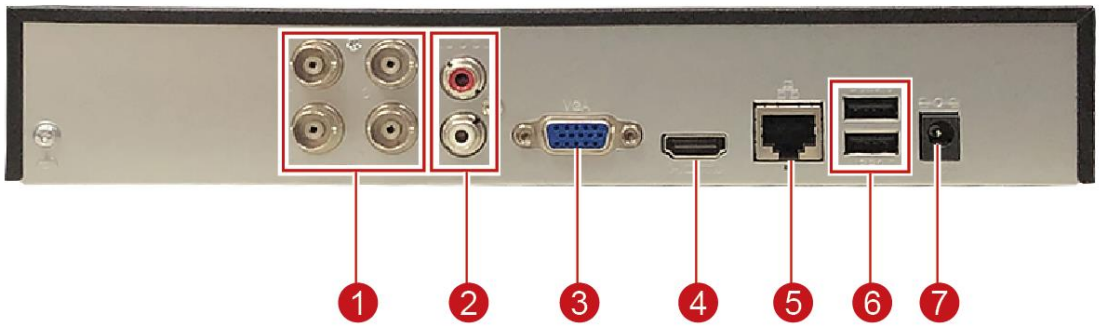
Battery in the product complies with the European Battery Directive 2013/56/EC. For proper recycling, return the battery to your supplier or to a designated collection point.

Introduction

LED Indicator

LED	Description
RUN (Operation)	• Steady on: Normal • Blinking: Starting up
NET (Network)	Steady on: Connected to the network
CLOUD	• Steady on: Connected to the cloud server
HD (Hard Disk)	• Steady on: No disk, or disk is abnormal • Blinking: Normal, reading / writing data

Physical Description



Item		Description
1	Video Input	Connects to analog cameras using coaxial cable. **NOTE:** The number of video input connectors vary depending on model.
2	Audio Input / Output	These connectors connect to audio input and output devices, such as microphones and speakers using RCA cables.
3	VGA Port	Connects to a display monitor using VGA cable.
4	HDMI Port	Connects to a display monitor using HDMI cable.
5	Ethernet Port	Connects to a network using an Ethernet cable.
6	USB Ports	Connects to USB devices, like keyboard and mouse.
7	Power Connector	Connects to a power source using the bundled power adapter.

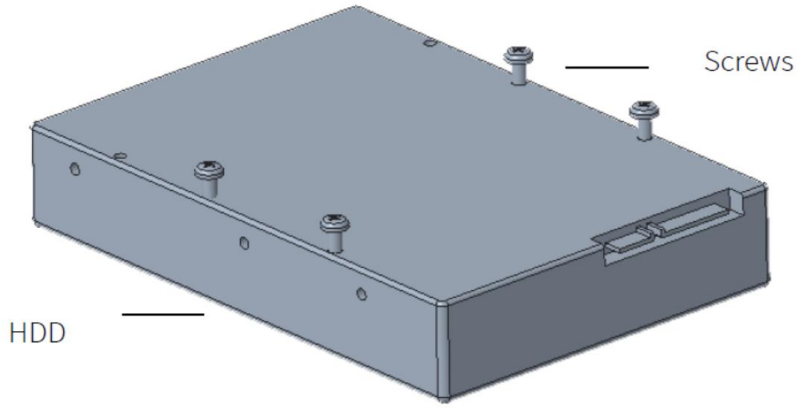
Installation and Connection

Disk Installation

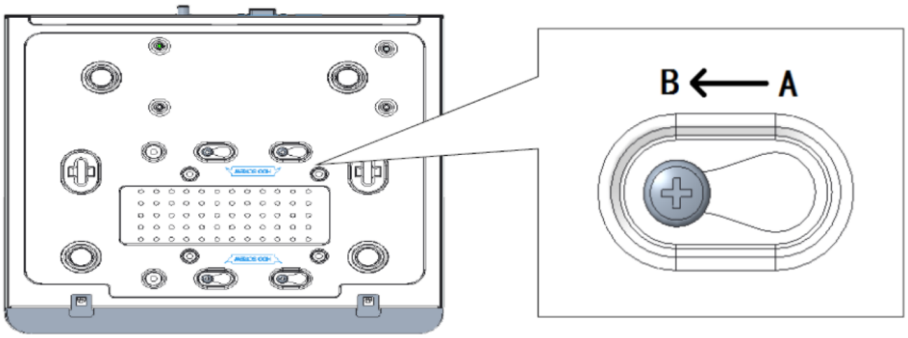
The illustrations are for reference only. The actual device may slightly vary.

1. Loosen the screws on the rear and side panels and remove the upper cover.

2. Insert the screws into the disk and tighten the screws halfway.



3. Slide the disk into place from A to B, and fix the screws to secure the hard disk.



4. Connect the data cables and the power cables.
5. Put the cover back in place and tighten the screws.

Connect Devices

1. Connect the device to a monitor with a VGA/HDMI cable (sold separately).
2. Connect a USB mouse to the device.
3. For analog cameras, connect the camera to a Video In interface with a coaxial cable. Skip this step if you are connecting an IP camera.
4. Connect the network cable.
   NOTE: Normally a network switch is used to connect the device and IP cameras with one network.
5. Verify installation and cable connections are correct. Connect the power to start the device.

Start Up

Connect the power to start the device.

Device Operation

Add Cameras

Analog Camera

Prepare coaxial cables (sold separately). Then connect the BNC connectors to the camera and the device.

IP Camera

Make sure the IP camera is connected to the network.

1. Click **Menu > Camera > Camera**.
2. Click  to add the camera.
   NOTE:
   - To search a specified network segment, click **Search Segment**.
   - Normally all discovered cameras can be added. If the status is  , it means the camera has been added successfully and is ready for live view; otherwise, check the network and make sure the username/password are correct. Click the edit button to modify if necessary.

Recording

Analog Camera

For analog cameras, you need to manually enable the recording schedule for the camera: **Menu > Storage > Recording** ◦

NOTE: When recording schedule is enabled, the device still records even when no analog camera is connected.

IP Camera

For IP cameras, a 24/7 recording schedule is enabled by default for all IP cameras. You may edit the recording time and type at **Menu > Storage > Recording**.

Playback

Right-click a preview window and then choose **Playback** to view the recorded video of the current day.

Access Using Web Browser

Access the device using a web browser (e.g., Internet Explorer) a connected computer.

1. Enter the device IP address in the address bar and then press Enter. Install the plugin as prompted. Close all web browswers when installation starts.
2. Open the web browser and log in with the default username and password (admin / 123456).

Shutdown

Click **Menu > Shutdown**.

CAUTION! Do not disconnect the power when the device is operating. A sudden power failure may cause device damage and loss of data.

7F, No. 1, Alley 20, Lane 407, Sec. 2, Ti-Ding Blvd., Neihu District, Taipei, Taiwan 114, R.O.C.
TEL : +886-2-2656-2588 FAX : +886-2-2656-2599
Email: sales@acti.com