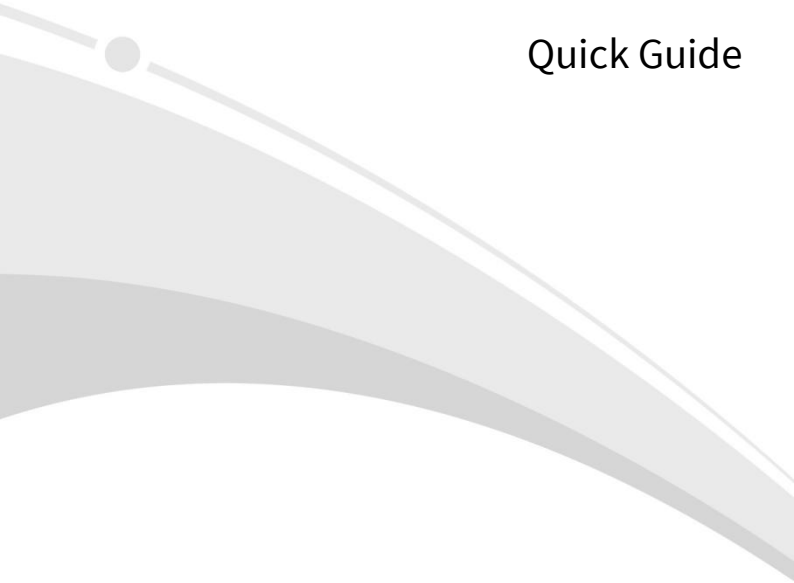




Network Video Recorders

Quick Guide

1 Packing List

Contact your local dealer if the package is damaged or incomplete. The package contents may vary with device model.

No.	Name	Qty	Unit
1	Network Video Recorder	1	PCS
2*	Power adapter	1	PCS
3	Screws	1	Set
4*	Mouse	1	PCS
5*	HDD data cable ⁽¹⁾	1 or 2	PCS
6*	HDD power cable ⁽²⁾	1 or 2	PCS
7	Product documents	1	Set

Remarks:

* means optional and supplied with certain models only.

(1) Each HDD is supplied with one data cable.

(2) Each HDD is supplied with one power cable.

2 Default IP, Username and Password

IP address: **192.168.1.30**

Username: **admin**

Password: **123456**

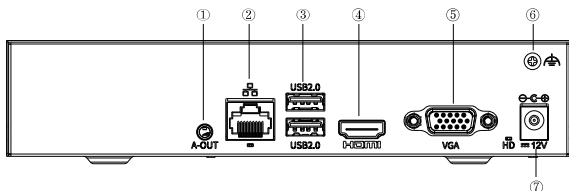
NOTE!

For security, it's strongly recommended to change the default password into a strong password that includes more than 8 characters comprising uppercase letter, lowercase letter, digit and special character.

3 Ports and Interfaces

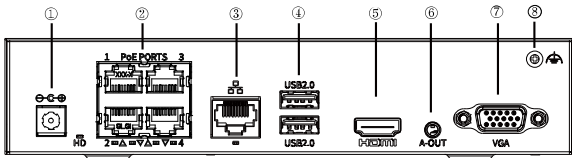
The interface may vary with device model. The figures below show the interface of two device models.

Figure 3-1 Non-PoE Device



Interface	Description	Interface	Description
①	Audio output	②	Network
③	USB	④	HDMI output
⑤	VGA output	⑥	Grounding
⑦	12V power	-	-

Figure 3-2 PoE Device



Interface	Description	Interface	Description
①	Power connector	②	PoE ports
③	Network	④	USB
⑤	HDMI output	⑥	Audio output
⑦	VGA output	⑧	Grounding

4 Disk Installation

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

4.1 Preparation

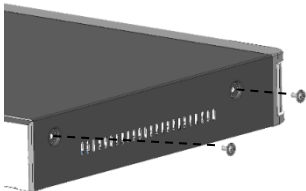
- Prepare a 1# or 2# Philips screwdriver, a pair of antistatic gloves or a wrist strap.
- Disconnect power before installation.

4.2 HDD Installation

The disk installation may vary with device model. The following introduces HDD installation of two device models.

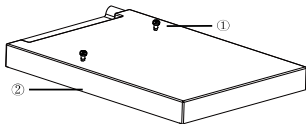
4.2.1 Wired HDD

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

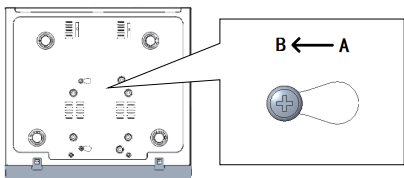


2. Insert the screws into the disk and tighten the screws halfway. In the figure below,

① is screw, ② is HDD.



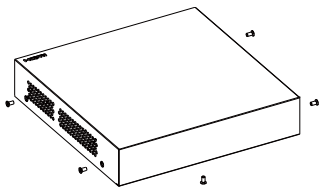
3. Slide the screws in step 2 into the chassis from A to B, and tighten them. Then fasten another two screws to fasten the hard disk.



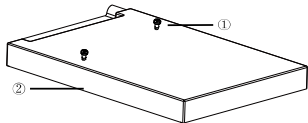
4. Connect the power cables and data cables.
5. Put the cover back in place and tighten the screws.

4.2.2 Pluggable HDD

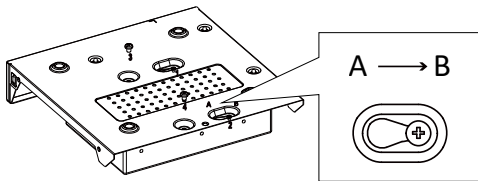
1. Loosen the four screws on the side panels and one screw at the bottom, and remove the upper cover.



2. Insert the screws into the disk and tighten the screws halfway. In the figure below, ① is screw, ② is HDD.



3. Slide the screws in step 2 into the chassis from A to B, and tighten them. Then fasten another two screws to fasten the hard disk.



4. Put the cover back in place and tighten the screws.

5 Startup and Shutdown

Make sure the cables are connected correctly and the device is grounded properly. Use a power supply that meets requirements.

5.1 Startup

Connect the device to power to start up the device.

5.2 Shutdown

Go to the live view page, right click and then select **Shutdown** in the shortcut menu.



CAUTION!

Do not disconnect power when the NVR is operating or shutting down.

6 Local Operations

6.1 Add IP Camera

Before add or manage IP cameras, make sure the IP camera is connected to the network.

1. Right click in the live view page, and then click **Camera > Camera > Camera**.
 2. Click **Add Manually**, enter the IP address and other required information.
 3. Check the status of camera .
- If the status icon is highlighted, it means the camera gets online successfully.

- If the status icon is grayed out, place your mouse cursor on the icon to view the cause of error. Click the edit button to modify device information.



NOTE!

- You can also click  to add a device.
- To search for devices in a specified network segment, click **Search Segment**.

6.2 Recording and Playback

6.2.1 Recording

A 7*24 recording schedule is enabled by default. To set a recording schedule manually, right click and select **Menu > Storage > Recording Schedule** and then set recording type and time based on your needs.

6.2.2 Playback

In live view page, right-click a preview window and select **Playback** to play the recording of the current day.



NOTE!

If you choose **Event** type recording, you need to enable the corresponding alarm function and configure alarm-triggered recording/snapshot first.

7 Web Login

Before you begin, check that your PC is connected to your NVR through network.

1. Open the browser on your PC, enter the IP address in the address bar, then press **Enter**.



NOTE!

- Install the plugin as prompted at first login.
- Close all browsers during the installation.

2. In the login page, enter the correct username and password, then click **Login**.

Disclaimer and Safety Warnings

Copyright Statement

No part of this manual may be copied, reproduced, translated or distributed in any form or by any means without prior consent in writing from our company (referred to as us hereafter).

The product described in this manual may contain proprietary software owned by our company and its possible licensors. Unless permitted, no one is allowed to copy, distribute, modify, abstract, decompile, disassemble, decrypt, reverse engineer, rent, transfer, or sublicense the software in any form or by any means.

Trademark Acknowledgements



The terms HDMI, HDMI High-Definition Multimedia Interface, HDMI Trade dress and the HDMI Logos are trademarks or registered trademarks of HDMI Licensing Administrator, Inc.

All other trademarks, products, services and companies in this manual or the product described in this manual are the property of their respective owners.

Export Compliance Statement

Our company complies with applicable export control laws and regulations worldwide, including that of the People's Republic of China and the United States, and abides by relevant regulations relating to the export, re-export and transfer of hardware, software and technology. Regarding the product described in this manual, our company asks you to fully understand and strictly abide by the applicable export laws and regulations worldwide.

EU Authorised Representative

UNV Technology EUROPE B.V. Treubstraat 1, 2288 EG, Rijswijk, Netherlands.

If you have any feedback, please contact us at service@uniview.com.

Privacy Protection Reminder

Our company complies with appropriate privacy protection laws and is committed to protecting user privacy. You may want to read our full privacy policy at our website and get to know the ways we process your personal information. Please be aware, using the product described in this manual may involve the collection of personal information such as face, fingerprint, license plate number, email, phone number, GPS. Please abide by your local laws and regulations while using the product.

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 GUI and functions of the software.

- Despite our best efforts, technical or typographical errors may exist in this manual. Our company 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.
- Our company 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.

Disclaimer of Liability

- To the extent allowed by applicable law, in no event will our company 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. We strongly recommend that users take all necessary measures to enhance the protection of network, device, data and personal information. Our company 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 our company and its employees, licensors, subsidiary, affiliates be liable for results 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 our company 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 our 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 our 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 discretely:** 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.

Safety Warnings

The device must be installed, serviced and maintained by a trained professional with necessary safety knowledge and skills. Before you start using the device, please read through this guide carefully and make sure all applicable requirements are met to avoid danger and loss of property.

Storage, Transportation, and Use

- Store or use the device in a proper environment that meets environmental requirements, including and not limited to, temperature, humidity, dust, corrosive gases, electromagnetic radiation, etc.
- Make sure the device is securely installed or placed on a flat surface to prevent falling.
- Unless otherwise specified, do not stack devices.
- Ensure good ventilation in the operating environment. Do not cover the vents on the device. Allow adequate space for ventilation.
- Protect the device from liquid of any kind.
- Make sure the power supply provides a stable voltage that meets the power requirements of the device. Make sure the power supply's output power exceeds the total maximum power of all the connected devices.

- Verify that the device is properly installed before connecting it to power.
- Do not remove the seal from the device body without consulting our company first. Do not attempt to service the product yourself. Contact a trained professional for maintenance.
- Always disconnect the device from power before attempting to move the device.
- Take proper waterproof measures in accordance with requirements before using the device outdoors.

Power Requirements

- Install and use the device in strict accordance with your local electrical safety regulations.
- Use a UL certified power supply that meets LPS requirements if an adapter is used.
- Use the recommended cordset (power cord) in accordance with the specified ratings.
- Only use the power adapter supplied with your device.
- Use a power adapter that matches your device in specifications and complies with LPS requirements.
- Use a mains socket outlet with a protective earthing (grounding) connection.
- Ground your device properly if the device is intended to be grounded.

Battery Use Caution

- When battery is used, avoid:
 - Extremely high or low temperature and air pressure during use, storage and transportation;
 - Battery replacement.
 - Use the battery properly. Improper use of the battery such as the following may cause risks of fire, explosion or leakage of flammable liquid or gas.
 - Replace battery with an incorrect type;
 - Dispose of a battery into fire or a hot oven, or mechanically crushing or cutting of a battery;
- Dispose of the used battery according to your local regulations or the battery manufacturer's instructions.

Avertissement de l'utilisation de la batterie

- Lorsque utiliser la batterie, évitez:
 - Température et pression d'air extrêmement élevées ou basses pendant l'utilisation, le stockage et le transport.
 - Remplacement de la batterie.
- Utilisez la batterie correctement. Mauvaise utilisation de la batterie comme celles mentionnées ici, peut entraîner des risques d'incendie, d'explosion ou de fuite liquide de gaz inflammables.
 - Remplacer la batterie par un type incorrect;
 - Disposer d'une batterie dans le feu ou un four chaud, écraser mécaniquement ou couper la batterie;
- Disposer la batterie utilisée conformément à vos règlements locaux ou aux instructions du fabricant de la batterie.

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



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.

Battery Regulation- (EU) 2023/1542



Battery in the product complies with the European Battery Regulation (EU) 2023/1542. For proper recycling, return the battery to your supplier or to a designated collection point.