



ENS UNV-5 Series Network Video Recorders User Guide

[Home](#) » [ENS](#) » ENS UNV-5 Series Network Video Recorders User Guide 

ENS UNV-5 Series Network Video Recorders User Guide



Contents

- [1 Default IP, Username and Password](#)
- [2 LEDs](#)
- [3 Interfaces](#)
- [4 Connection](#)
- [5 Install Hard Disks](#)
- [6 Replace a Disk](#)
- [7 \(Optional\)Install a Power Module](#)
- [8 \(Optional\)Install a Decoding Card](#)
- [9 \(Optional\) Mount on a Cabinet](#)
- [10 Startup and Shutdown](#)
 - [10.1 Startup](#)
 - [10.2 Shutdown](#)
- [11 Live View](#)
- [12 Playback](#)
- [13 Access Using a Web Browser](#)
- [14 Disclaimer and Safety Warnings](#)
- [15 Regulatory Compliance](#)
 - [15.1 FCC Statements](#)
- [16 Documents / Resources](#)
 - [16.1 References](#)
- [17 Related Posts](#)

Default IP, Username and Password

- **IP address:** 192.168.1.30
- **Username:** admin
- **Password:** 123456

Note!

For security, you are strongly recommended to set a strong password of at least nine characters including all three elements: digits, letters and special characters.

LEDs

LED	Description
RUN (Operation)	<ul style="list-style-type: none">• Steady on: Normal.• Blinks: Starting up.
ALM (Alarm)	Steady on: Device alarm occurred.
NET (Network)	Steady on: Connected to network.
SLOT (Slot card)	Steady on: Card is installed.
HD (Hard disk)	<ul style="list-style-type: none">• Steady green: Normal.• Blinks green: Reading or writing data.• Steady yellow: Abnormal.• Blinks yellow: Rebuilding array.
LINK (Connection)	Located next to miniSAS interfaces on the rear panel. <ul style="list-style-type: none">• Steady on: Connected to disk enclosure.• Blinks: Communicating with disk enclosure.

Interfaces

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

Figure 3-1 Model 1

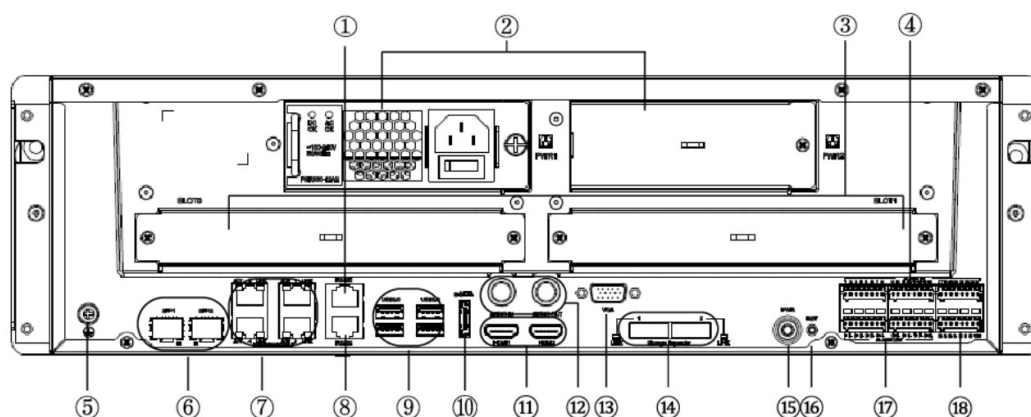
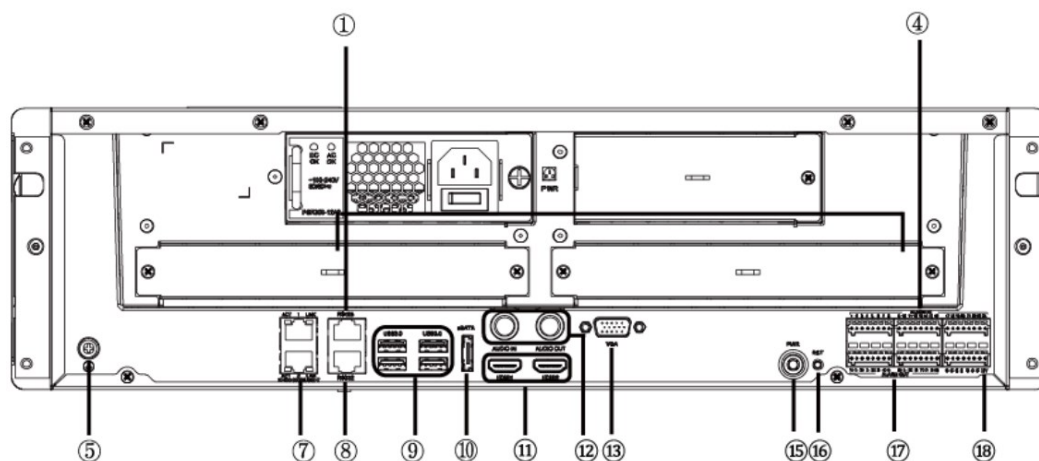


Figure 3-2 Model 2



Interface	Description	Interface	Description
①	RS485	②	100V~240V AC input Note: One power supply is provided as standard for some models, you may prepare a second power supply as needed.
③	Decoding card	④	Alarm input
⑤	Grounding	⑥	Optical interface
⑦	Ethernet interface	⑧	RS232 Note: The RS232 interface is used for debug and maintenance.
⑨	USB	⑩	eSATA
	HDMI output		Audio input/output
	VGA output		miniSAS
	Power button		RST Note: Press and hold RST (reset) for at least five seconds and then the device will restart.
	Alarm output		12V DC output

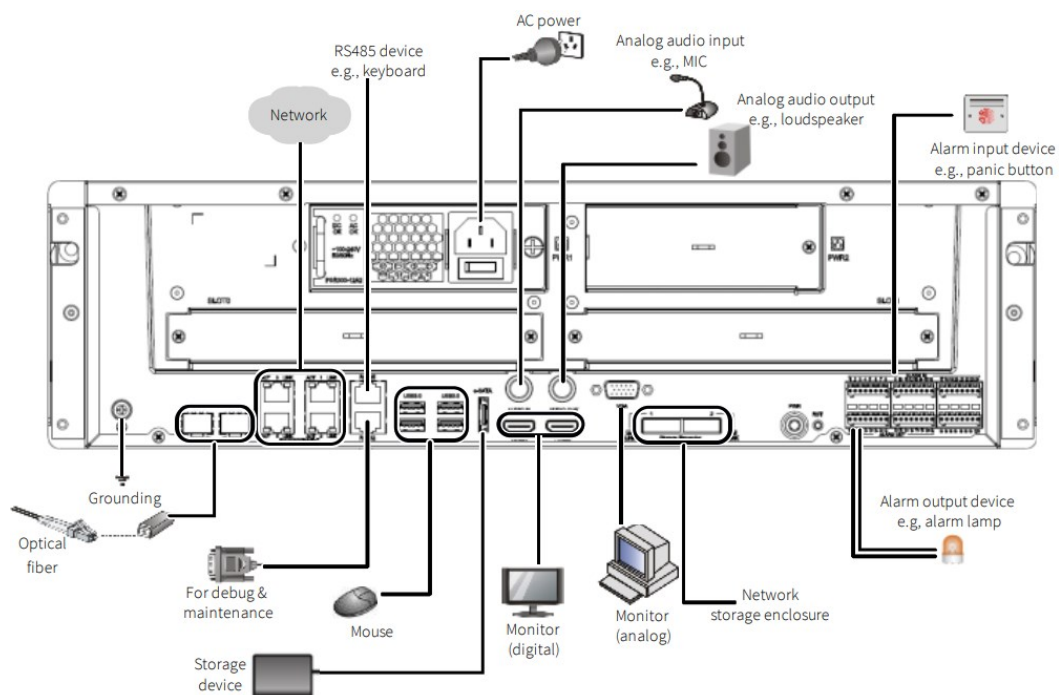


NOTE!

Do not connect or disconnect disk enclosure with power applied.

Connection

The connection may vary with device model. The following part takes model 1 as an example.



Install Hard Disks

Prepare a 1# or 2# Phillips screwdriver, a pair of antistatic gloves or an antistatic wrist strap. Disconnect power before installation. Photos are only for illustration.

1. Fix the mounting brackets to the disk with screws (L for left and R for right).



2. Loosen the screws and then open the front panel.



3. Align the disk with the slot and then insert the disk gently.



4. Push the disk until it clicks. Repeat the steps to install all the disks.



5. Install the front panel.

Replace a Disk

Wear antistatic gloves or an antistatic wrist strap. Open the front panel and then follow the steps.

1. Gently pull the handles to detach the disk. Pull out the disk when it stops operations (takes at least 30s).



2. Remove the fixing screws and then replace the disk. See [Install Hard Disks](#) for detailed steps.



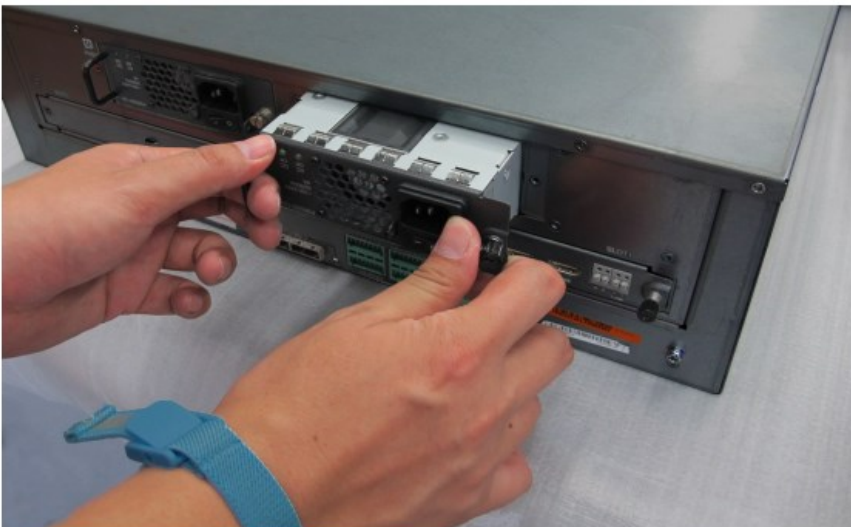
(Optional) Install a Power Module

Install a backup power module (see datasheet for specifications). Disconnect power before you start. Wear antistatic gloves or an antistatic wrist strap.

1. Loosen the screw and remove the blank faceplate.



2. Insert the power module and then fasten the screw.



(Optional) Install a Decoding Card

Install a decoding card (see datasheet for specifications). Disconnect power before you install or extract a decoding card. Wear antistatic gloves or an antistatic wrist strap.

1. Loosen the screws and then remove the blank faceplate.



2. Insert the decoding card and then fasten the screws.



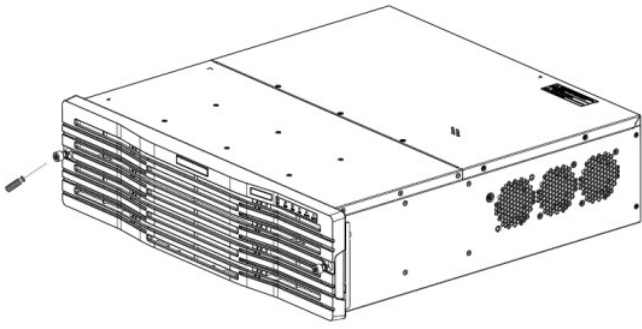
(Optional) Mount on a Cabinet

The cabinet must have slide rails or a tray to hold the device.
Photos are only for illustration.

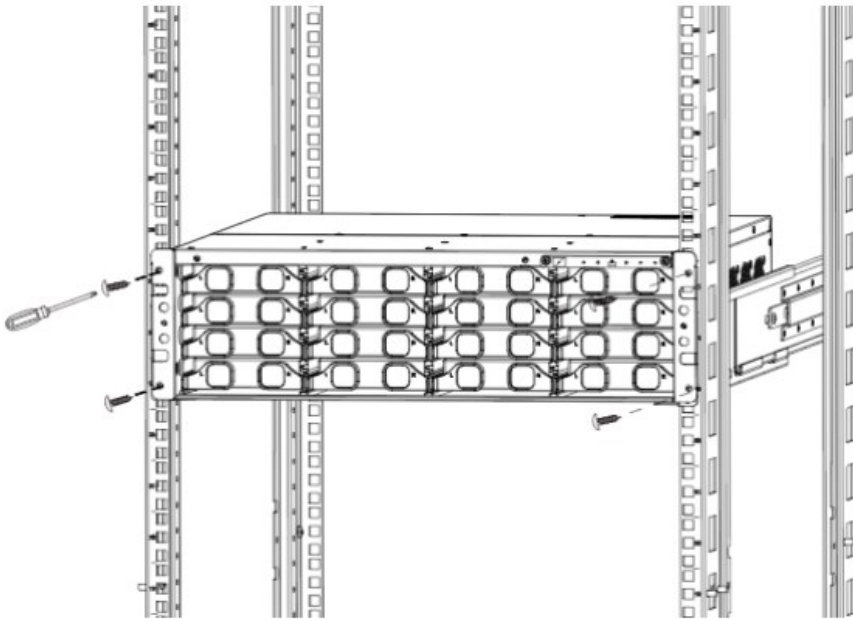
CAUTION!

Do not stack the device up or place anything heavy on it. Otherwise heat dissipation will be affected.

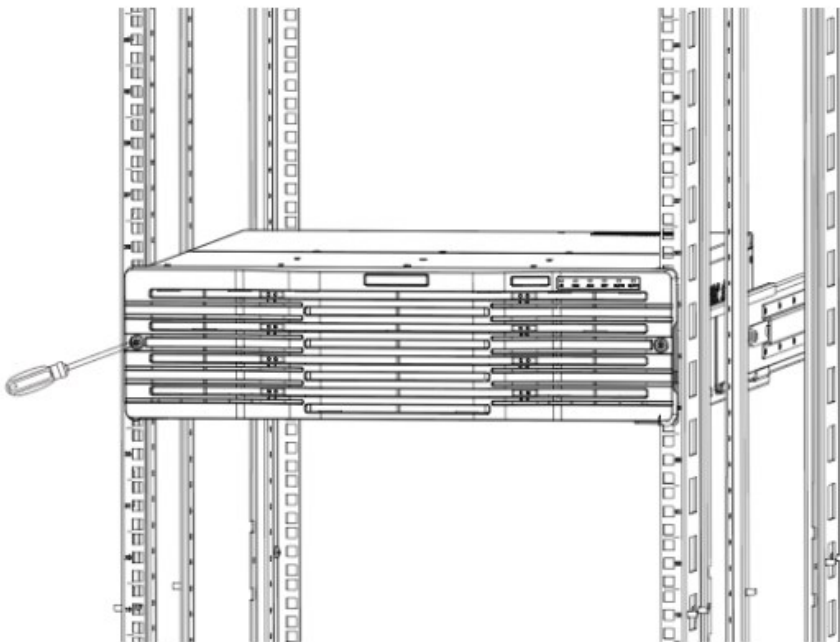
1. Loosen the screws and then open the front panel.



2. Install supports (such as bracket slides or trays) on the cabinet.
3. Place the device on the support, and push it in slowly until it is blocked by the hole strip on the front of the cabinet.
4. Secure the front bracket to the rack with screws.



5. Replace the front panel.



Startup and Shutdown

Make sure the cables are connected correctly and operating environment is normal. Use a power supply that

meets requirements.


Startup

Connect power and then turn on the power on/off switch. Follow the wizard to complete setup.

Shutdown

Use the Shutdown menu. DO NOT shut down by disconnecting power or turning off the power on/off switch. A sudden power failure may cause device damage and loss of data.

Live View

Click **Menu > Camera > Camera**. The discovered cameras are listed. Click  to add a camera. To search a network segment, click **Search**. If a camera is added but there is no live video, check network connection and make sure the correct camera username and password are set in the system. Modify the username and password if necessary.

Playback

Right-click a preview window and then choose **Playback** to view video recorded on the current day. A 24×7 recording schedule is enabled at delivery and can be edited under **Menu > Storage > Recording**.

Access Using a Web Browser

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

1. Enter the device's IP address in the address bar and then press **Enter**. Install a plugin if prompted. Close all Web browsers when the installation starts.
2. Open the Web browser and log in with the correct username and password.

Disclaimer and Safety Warnings

Copyright Statement

©2015-2022 Zhejiang Uniview Technologies Co., Ltd. All rights reserved.

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 Zhejiang Uniview Technologies Co., Ltd (referred to as Uniview or us hereafter).

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

 **univ** uniarch

HDMITM
HIGH DEFINITION MULTIMEDIA INTERFACE

Trademark Acknowledgements are trademarks or registered trademarks of Uniview. The terms HDMI and HDMI High-Definition Multimedia Interface, and the HDMI Logo are trademarks or registered trademarks of HDMI Licensing LLC in the United States and other countries.

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

Uniview 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, Uniview asks you to fully understand and strictly abide by the applicable export laws and regulations worldwide.

EU Authorised Representative

UNV Technology EUROPE B.V. Room 2945, 3rd Floor, Randstad 21-05 G, 1314 BD, Almere, Netherlands.

Privacy Protection Reminder

Uniview 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. Uniview 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.
- Uniview 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 Uniview 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. Uniview strongly recommends that users take all necessary measures to enhance the protection of network, device, data and personal information. Uniview 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 Uniview 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 Uniview 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 Uniview'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 Uniview'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 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.

Learn More

You may also obtain security information under Security Response Center at Uniview's official website.

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 Uniview 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 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.

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. Visit

http://en.uniview.com/Support/Download_Center/Product_Installation/Declaration/ for SDoC.

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 Directive-2013/56/EC



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.

Documents / Resources

 The image shows the cover of a 'Network Video Recorders Quick Guide'. It features a stylized graphic of a curved line with a dot at the end, and the text 'Network Video Recorders Quick Guide' at the top. A small '10.00' is visible at the bottom left.	<p>ENS UNV-5 Series Network Video Recorders [pdf] User Guide</p> <p>UNV-5 Series Network Video Recorders, UNV-5, Series Network Video Recorders, Network Video Recorders, Video Recorders, Recorders</p>
--	--

References

- [U Suppliers Declaration of Conformity - Uniview - Leader of AIoT Solution](#)