



ENS Security NVR304 Network Video Recorders User Guide

May 3,
2025

Contents [[hide](#)]

- 1 Network Video Recorders
 - 1.1 Quick Guide
 - 1.2 1 Indicators
 - 1.3 2 Interfaces
 - 1.4 3 Disk Installation
 - 1.4.1 3.1 Preparation
 - 1.4.2 3.2 1 or 2 HDD Installation
 - 1.4.3 3.3 4 or 8 HDD Installation
 - 1.4.3.1 3.3.1 Remove Upper Cover
 - 1.4.3.2 3.3.2 Install Disks
 - 1.4.4 3.4 8 or 16 HDD Installation
 - 1.5 4 Startup and Shutdown
 - 1.5.1 4.1 Startup
 - 1.5.2 4.2 Shutdown
 - 1.6 5 Local Operations
 - 1.6.1 5.1 Add IP Devices
 - 1.6.1.1 5.1.1 Quick Add
 - 1.6.1.2 5.1.2 Custom Add
 - 1.6.2 5.2 Playback
 - 1.7 6 EZView
 - 1.7.1 6.1 Sign Up an Account
 - 1.7.2 6.2 Add Devices
 - 1.7.3 6.3 Live View/Playback
 - 1.7.4 6.4 Share Devices
 - 1.8 7 Web Login
 - 1.9 Disclaimer and Safety Warnings
- 2 Documents / Resources
 - 2.1 References
- 3 Related Posts

Network Video Recorders

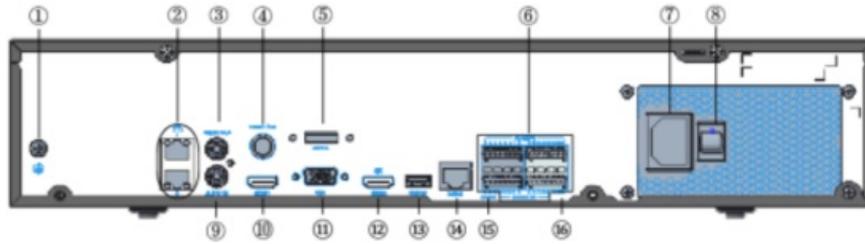
1 Indicators

LED	Status	Description
PWR(Power)	Steady on	Connected to power.
RUN(Operation)	Steady on	Normal.
	Blinking	Starting up.
IR	Steady on	Activated for remote control.
	Blinking	Authenticating device code.
ALM(Alarm)	Steady on	Device alarm occurred.
NET(Network)	Steady on	Connected to network.
GUARD(Arming)	Steady on	Arming is enabled.
CLOUD	Steady on	Connected to cloud.
HD(Hard disk)	Steady on	No disk; or disk is abnormal.
	Blinking	Reading or writing data.
HDn(Hard disk)	Steady green	Normal.
	Blinking green	Reading or writing data.
	Steady red	Abnormal.
	Blinking red	Rebuilding array.

2 Interfaces

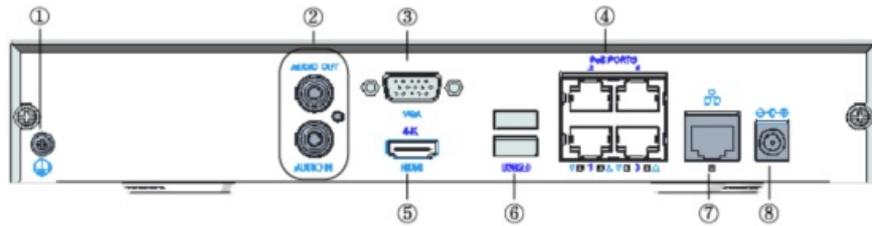
The following part shows the interfaces of two typical models.

Figure 2-1 Model 1



Interface	Description
1	Grounding
2	Network
3	Audio out
4	CVBS output
5	eSATA interface
6	Alarm input/output
7	AC power
8	Power on/off
9	Audio in
10	HDMI 1 output
11	VGA output
12	HDMI 2 output
13	USB
14	RS232
15	RS485
16	12V DC output

Figure 2-2 Model 2



Interface	Description
1	Grounding
2	Audio in/out
3	VGA output
4	PoE ports
5	HDMI output
6	USB
7	Network
8	DC power

3 Disk Installation

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

3.1 Preparation

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

 **CAUTION!**

For NVR supports the face library function, the function may be unavailable if there are no disks in slot 1 and slot 2.

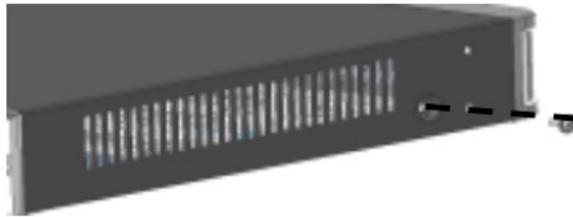
3.2 1 or 2 HDD Installation

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

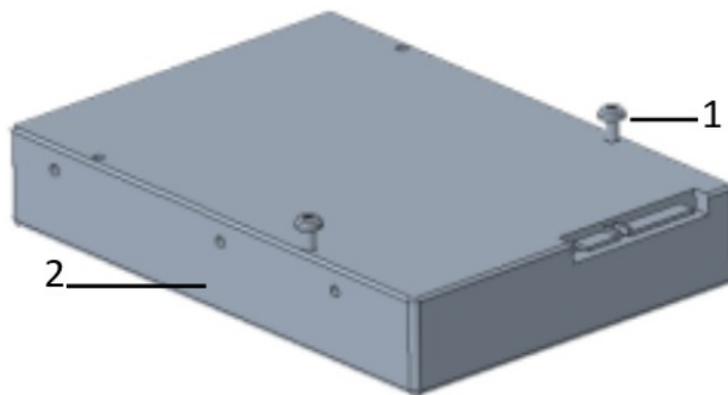
Figure 3-1 Rear Panel



Figure 3-2 Side Panel



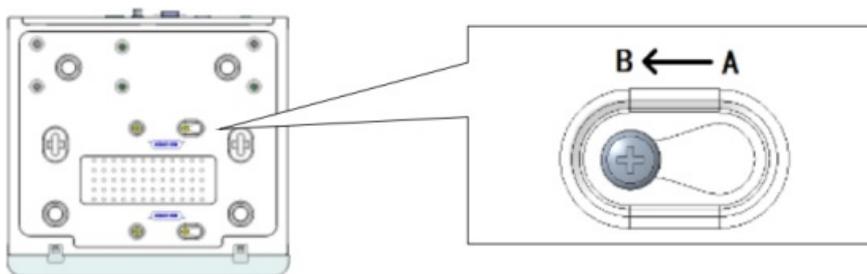
2. Insert the screws into the disk and tighten the screws halfway.



1. Screws

2. HDD

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



4. Connect the power cables and data cables.

5. Put the cover back in place and tighten the four screws.

3.3 4 or 8 HDD Installation

3.3.1 Remove Upper Cover

1. Loosen the screws on the upper cover.



2. Slide the upper cover backward, then lift it up to remove the cover.

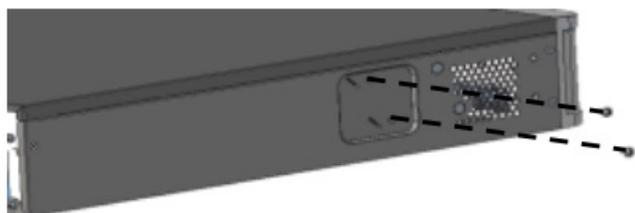


3.3.2 Install Disks

The installation steps for devices with mounting plate and disk bracket are different. Choose the installation method according to your device model.

- Device with mounting plate

1. Loosen the screws of the mounting plate on the side panels.



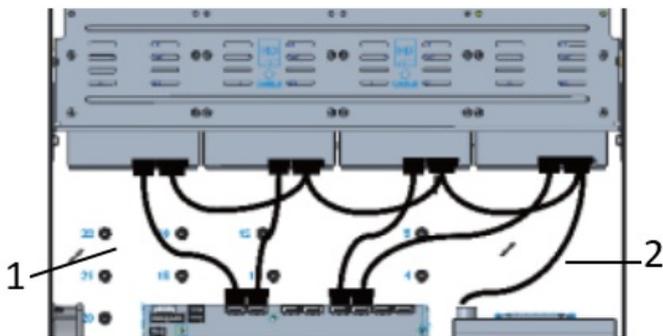
2. Turn the upper mounting plate in the shown direction, then remove the plate. Repeat the steps to remove the lower mounting plate (for 8-HDD devices only).



3. Secure the disks on the mounting plate. Fix the screws according to the figure below. Avoid damaging the disk in the process.



4. Put the mounting plate back in place. Connect the power cables and data cables as shown in the figure. Repeat the steps to connect all the disks.

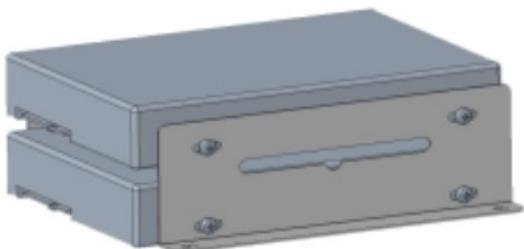


1. Data cable
2. Power cable

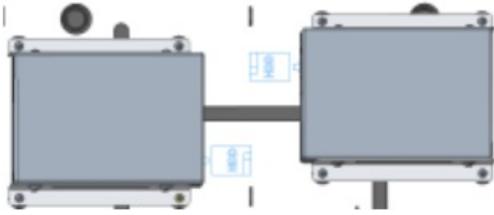
5. Put the cover back in place, and secure it and the mounting plates with screws.

- Device with disk bracket

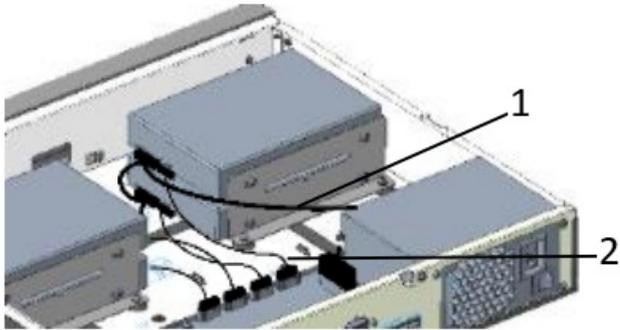
1. Fasten the disks to the brackets.



2. Fasten the brackets installed with hard disks to the device.



3. Connect the power cables and data cables.



1. Power cable
2. Data cable

3.4 8 or 16 HDD Installation

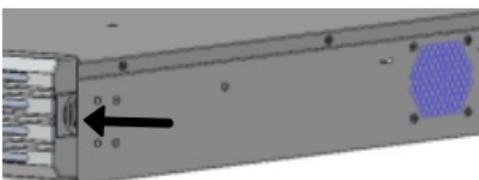
1. Fix the mounting brackets to the disk with screws. With the disk interface side down, install the R (for right) and L (for left) bracket according to the figure below.



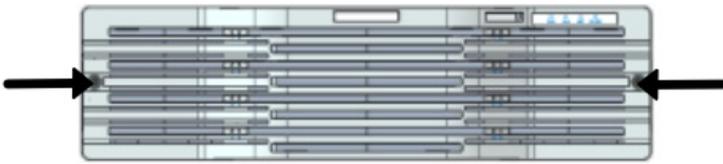
Down

2. Remove the front panel.

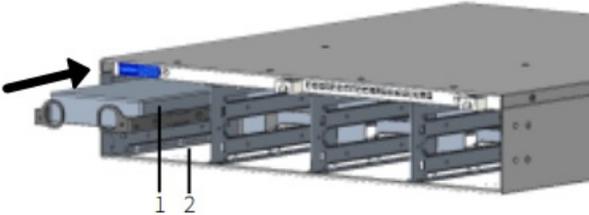
- For front panel with buttons, press the buttons on both sides of the front panel.



- For front panel with screws, loosen the screws on the front panel.



3. Align the disk with the slot and slide the disk inward gently until it clicks. Repeat the steps to install all the disks.



1. Slot 1

2. Slot 2

4. Install the front panel.

4 Startup and Shutdown

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

4.1 Startup

Connect the device to power to start the device. If the device has a power switch on the rear panel, you need to turn on the power switch to start the device.

When the device is off and still connected to power, press the power button on the front panel for 1-2s to turn on the device.

If the device has no power button on the front panel, or if the device does not start up after you press the power button for 1-2s, you need to reconnect the power to turn on the device.



NOTE!

For some devices, the power button on the front panel is only used to turn off the device.

4.2 Shutdown

Click  > **Shutdown** on the screen toolbar in live view page.



CAUTION!

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

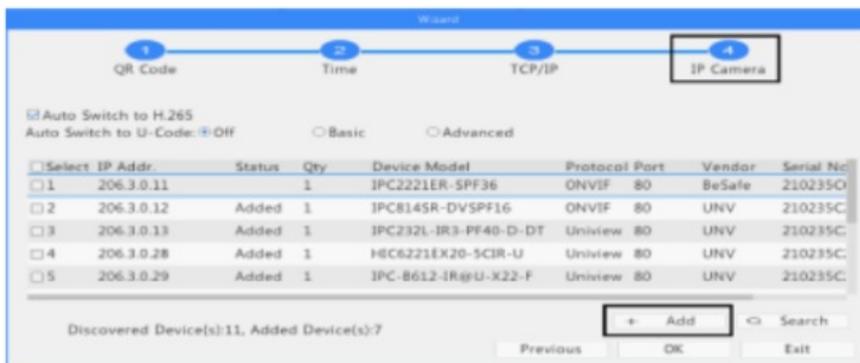
5 Local Operations

5.1 Add IP Devices

Before you begin, make sure the devices are connected to your NVR via network.

5.1.1 Quick Add

Follow the wizard to the fourth step. Select the devices to add in the discovered device list, and then click **Add**.



NOTE!

After the device is added, if wrong username or password message shows in the preview window, click  in the window toolbar and enter the correct username and password.

5.1.2 Custom Add

1. Right click in the preview page, click **Menu** > **Camera** > **Camera**.
2. Click **Custom Add**, enter the IP address and other required information.

Camera	IP Address	Status	Protocol	Model	Add/Del	Cam Con...	Net Config	Details
D1(206.3.0.135_...)	206.3.0.12		ONVIF	IPC8145R-DV5PF16				
D2(11)	206.3.0.28		Uniview	HIC6271EX20-SCR-U				
D3(206.3.0.135_...)	206.3.0.13		Uniview	IPC232L-IR3-PF40-D-DT				
D4(07)	206.3.0.29		Uniview	IPC-8612-IR@U-X22-F				
D5(1)	206.3.0.37		Uniview	IPC2445-IR9-PF36-DT				

Discovered Device(s):0, Added Device(s):7,Idle Receive Bandwidth: 304Mbps

Auto Switch to H.265
 Auto Switch to U-Code: OFF
 Basic
 Advanced

3. Check the status of camera. means the camera gets online successfully. If the status icon is grayed out, place your mouse cursor over 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.
- Click **Search Segment** to search for devices in a specified network segment.

5.2 Playback

In the preview page, select the desired window, then right click and select **Playback** to play the recording of the current day.

NOTE!

- A 7*24 recording schedule is enabled by default. To set a recording schedule manually, right click and select **Menu > Storage > Recording** and then set recording type and time based on your needs.
- If you choose **Event** type recording, you need to enable the corresponding alarm function and configure alarm-triggered recording/snapshot first.

6 EZView

Please download EZView on the App Store (iOS) or on Google Play (Android) first.

6.1 Sign Up an Account

1. Tap in the upper right corner and choose **International** service area.
2. Tap **Sign Up** and follow the steps to complete sign up.

6.2 Add Devices

After logging in to your account, tap  > **Devices** > **Add**, then select a way to add devices. It's recommended to choose **Scan** and scan the QR code on the device body.

6.3 Live View/Playback

Tap  > **Live View/Playback**. Tap  in a window, then select a device to start live view or playback. You can also tap  in the upper-right corner and select device(s).

6.4 Share Devices

Tap  > **Devices**, select the desired device and tap **Share**, then complete the sharing settings. You may also share the device by generating a QR code.

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(192.168.1.30) in the address bar, then press **Enter**.



NOTE!

Install the plugin as required at first login. Close your browser during the installation.

2. In the login page, enter the correct username(admin) and password(123456), then click **Login**.

Disclaimer and Safety Warnings

Copyright Statement

©2021-2024 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 or by any means.

Trademark Acknowledgements

 are trademarks or registered trademarks of Uniview. 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

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

- 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.
- 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.
- 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).

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.
- **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.
- **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.
- **Physical protection:** Keep the device in a locked room or cabinet to prevent unauthorized physical access.
- **SNMP:** Disable SNMP if you do not use it. If you do use it, then SNMPv3 is recommended.

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 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.

Documents / Resources

	<p>ENS Security NVR304 Network Video Recorders [pdf] User Guide NVR302-16B-P16-IQ, NVR301-16B-LP8-IQ, NVR301-08B-LP8-IQ, NVR502-16B-IQ, NVR301-04B-LP4-IQ, NVR304-16B-P16-IQ, NVR304 Network Video Recorders, Network Video Recorders, Video Recorders, Recorders</p>
--	---

References

- [User Manual](#)

Related Posts



[MAGLLAN Security System User Guide](#)

MAGLLAN Security System User Guide - Download
[optimized] MAGLLAN Security System User Guide - Download



[Aruba 8.6 Network User Guide](#)

Aruba 8.6 Network User Guide

[Aruba 8.7 Network User Guide](#)



Aruba 8.7 Network User Guide



[verizon LTE Network Extender User Guide](#)

verizon LTE Network Extender User Guide - Download
[optimized] verizon LTE Network Extender User Guide -
Download

ENS SECURITY

ENS SECURITY, Network Video Recorders, NVR301-04B-LP4-IQ, NVR301-08B-LP8-IQ, NVR301-16B-LP8-IQ, NVR302-16B-P16-IQ, NVR304 Network Video Recorders, NVR304-16B-P16-IQ, NVR502-16B-IQ, Recorders, Video Recorders

—Previous Post

[ENS Security HNC3I189T1-ZASPV 4MP Bullet Network Camera User Guide](#)

Leave a comment

Your email address will not be published. Required fields are marked *

Comment *

Name

Email

Website

Save my name, email, and website in this browser for the next time I comment.

Post Comment

[Manuals+](#), [Privacy Policy](#) | [@manuals.plus](#) | [YouTube](#)

This website is an independent publication and is neither affiliated with nor endorsed by any of the trademark owners. The "Bluetooth®" word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. The "Wi-Fi®" word mark and logos are registered trademarks owned by the Wi-Fi Alliance. Any use of these marks on this website does not imply any affiliation with or endorsement.