



Uniview XVR301-16G3 Digital Video Recorders User Guide

[Home](#) » [uniview](#) » Uniview XVR301-16G3 Digital Video Recorders User Guide 

Uniview XVR301-16G3 Digital Video Recorders



Contents

- 1 Default IP, Username and Password
- 2 LEDs
- 3 Ports and Interfaces
- 4 Disk Installation
 - 4.1 Preparation
- 5 Connect Devices
- 6 Startup
- 7 Add Cameras
 - 7.1 Analog Camera
 - 7.2 IP Camera
- 8 Change Camera Type
- 9 Recording and Playback
 - 9.1 Recording
 - 9.2 Playback
- 10 Access Using a Web Browser
- 11 Access from Mobile App
- 12 Shutdown
- 13 Disclaimer and Safety Warnings
- 14 Safety Warnings
- 15 Regulatory Compliance
- 16 Documents / Resources
 - 16.1 References
- 17 Related Posts

Default IP, Username and Password

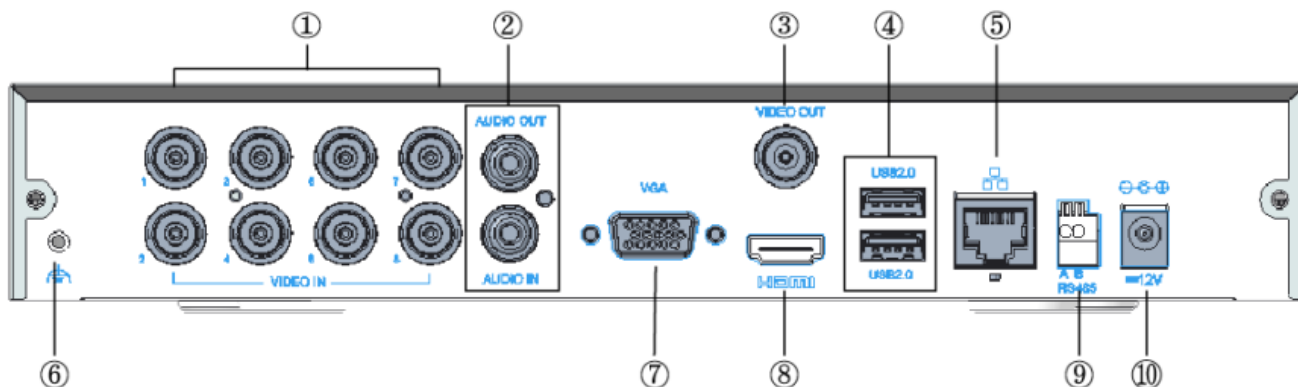
- Default IP address: 192.168.1.30
- Default admin username: admin
- Default admin password: 123456 (only for first login and should be changed to a strong one with at least 8 characters including upper and lower case letters, digits and symbols to enhance account security.)

LEDs

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

Ports and Interfaces

Take One Model for Example.



Interface	Description	Interface	Description
①	Video input	②	Audio input / output
③	Video output	④	USB

Interface	Description	Interface	Description
⑤	Network	⑥	Grounding
⑦	VGA output	⑧	HDMI output
⑨	RS485	⑩	12V DC output

Disk Installation

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

Preparation

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

HDD Installation

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

Figure 4-1 Rear Panel

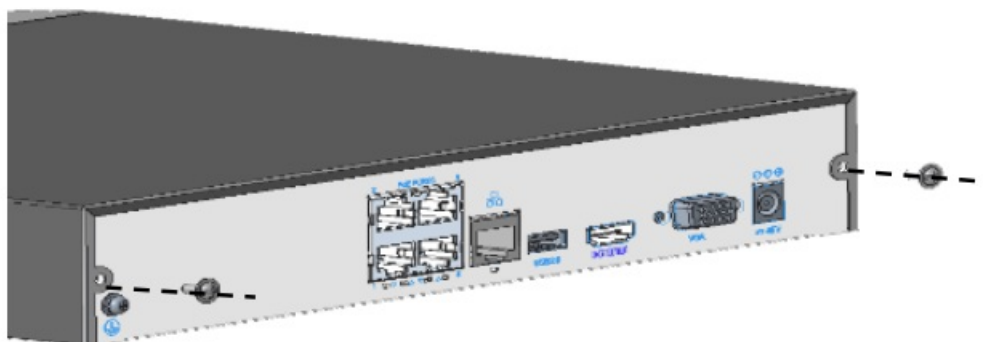
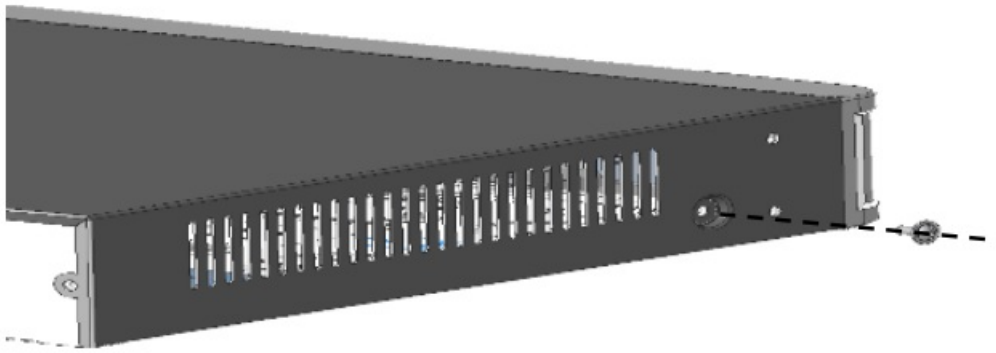
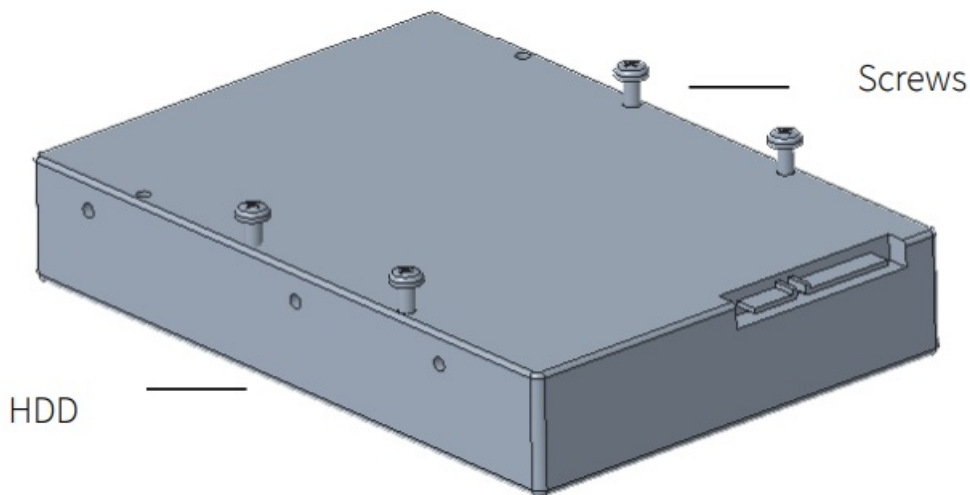


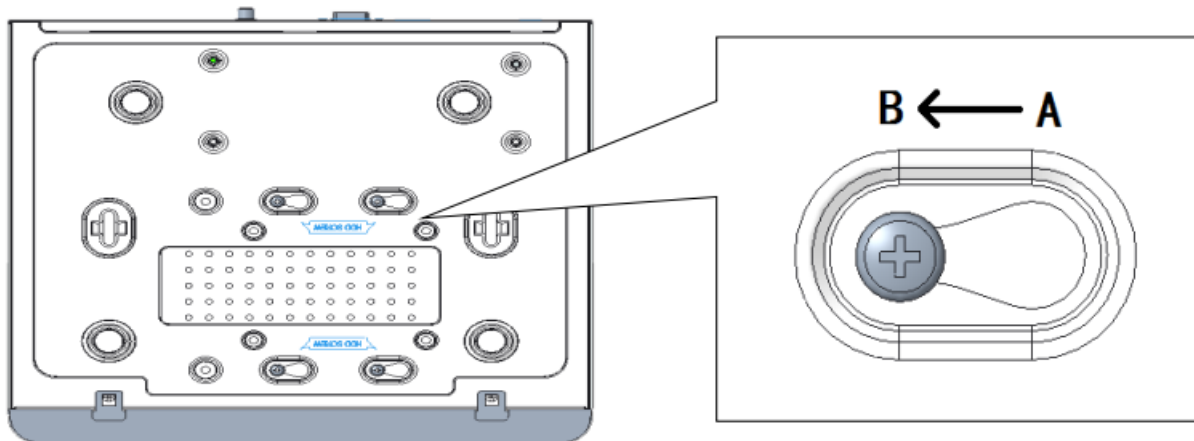
Figure 4-2 Side Panel



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 power cables and data 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 camera only) 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. Connect power.

Startup

Verify installation and cable connection are correct. Connect power to start the device.

Add Cameras

Analog Camera

Please prepare a coaxial cable (sold separately). Connect BNC connectors to the camera and the device.



NOTE!

Please refer to PTZ descriptions for presets if the analog camera is connected to the PTZ via RS485.

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, please check network and make sure the username/password are correct. Click the edit button to modify if necessary.

Change Camera Type

By default the device can connect 2 IP cameras. To connect more IP cameras, click **Menu > Camera > Camera > Camera** Type and change camera type to digital. An analog camera cannot be connected when the camera type is set to digital.

Recording and Playback

Recording

- For analog camera: 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.

- For IP camera: A 24/7 recording schedule is enable by default for all IP cameras.

You may edit recording time and type at **Menu > Storage > Recording**

Playback

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

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 the plugin as prompted. Close all Web browsers when the installation starts.
2. Open the Web browser and log in with the correct username and password.

Access from Mobile App

Install the app on your mobile phone and sign up for a cloud account. For details please contact your dealer. Connect your device to a router with Internet connection, and connect your mobile phone to the router's Wi-Fi network. Scan the QR code on the device with the mobile app to add the device

Shutdown

Click **Menu > Shutdown**.



CAUTION!

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

Disclaimer and Safety Warnings

Copyright Statement

©2021-2023 Zhejiang Unified 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 Unified Technologies Co., Ltd (referred to as Unified or us hereafter).

The product described in this manual may contain proprietary software owned by Unified and its possible licensors. Unless permitted by Unified 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.

Trademark Acknowledgements



are trademarks or registered trademarks of Unified.



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

Unified 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, Unified 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

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

Documents / Resources

	Uniview XVR301-16G3 Digital Video Recorders [pdf] User Guide XVR301-16G3 Digital Video Recorders, XVR301-16G3, Digital Video Recorders, Video Record ers, Recorders
---	--

References

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