
Supercircuits

Network Video Recorders

Quick Installation Guide

NVRE0401-0

NVRE0801-0

NVRE1602-0



1 Default IP, Username and Password

IP address: 192.168.1.30

Username: admin

Password: 123456

NOTE!

For security, we strongly recommend that you set a strong password of at least nine characters with numbers, letters and special characters.

2 Indicators

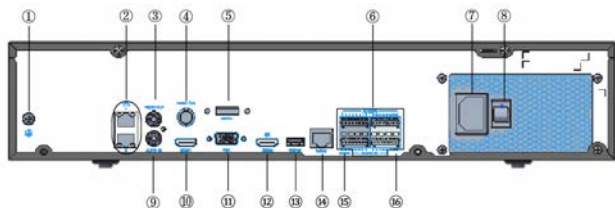
LED	Status	Description
PWR (Power)	Steady on	Connected to power.
RUN (Operation)	Steady on	Normal
	Blinking	Starting up
IR	Steady on	Activated for remote control
	Blinking	Authenticating device code
ALM (Alarm)	Steady on	Device alarm occurred
NET (Network)	Steady on	Connected to network
GUARD (Arming)	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

LED	Status	Description
	Steady red	Abnormal
	Blinking red	Rebuilding array

3 Interfaces

The following drawings show the interfaces of two typical recorders.

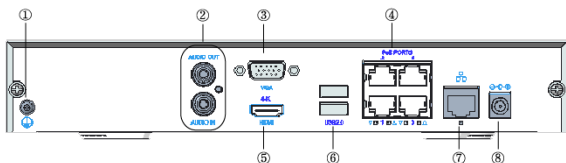
Figure 3-1 Model 1



Interface	Description	Interface	Description
①	Ground terminal	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

Interface	Description	Interface	Description
⑮	RS485	⑯	12Vdc output

Figure 3-2 Model 2



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

4 Disk Installation

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

4.1 Preparation

- Acquire a #1 or #2 Philips screwdriver
- Acquire antistatic gloves or a wrist strap.
- Disconnect power and all interface cables before installation.

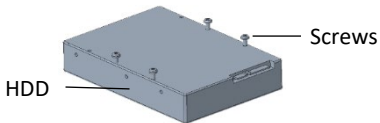
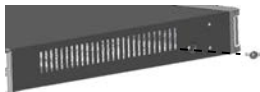
4.2 1 or 2 HDD Installation

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

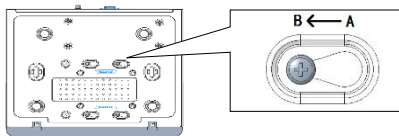
Figure 4-1 Rear Panel



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 tighten the screws to secure the hard disk.



4. Connect the power cables and data cables.
5. Reinstall the cover. Tighten all screws.

4.3 4 or 8 HDD Installation

4.3.1 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.



4.3.2 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

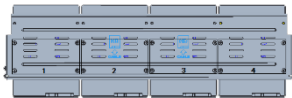
1. Loosen the screws of the mounting plate on the side panels.



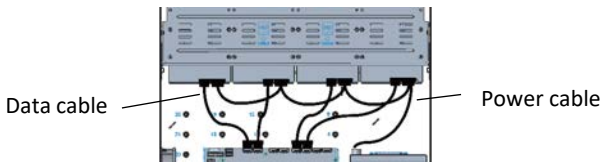
2. Turn the upper mounting plate in the shown direction, then remove the plate. Repeat the steps to remove the lower mounting plate (for 8-HDD devices only).



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



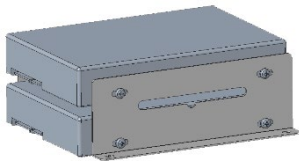
4. Put the mounting plate back in place. Connect the power cables and data cables as shown in the figure. Repeat the steps to connect all the disks.



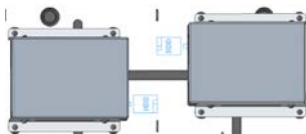
5. Put the cover back in place, and secure it and the mounting plates with screws.

4.3.3 Device with disk bracket

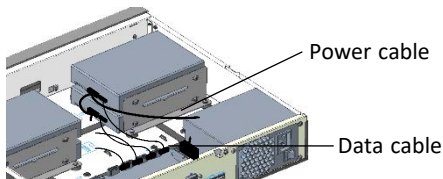
1. Fasten the disks to the brackets.



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



3. Connect the power cables and data cables.



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 and turn on the power switch (if applicable).

5.2 Shutdown

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



CAUTION!

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

6 Local Operations

6.1 Add IP Devices

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


6.1.1 Quick Add

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

Select IP Addr.	Status	Qty	Device Model	Protocol	Port	Vendor	Serial No.	
<input type="checkbox"/> 1	206.3.0.11	Added	1	HNC24-A-0	ONVIF	80	Supercir	210235C
<input type="checkbox"/> 2	206.3.0.12	Added	1	HNC512-A-0	ONVIF	80	Supercir	210235C
<input type="checkbox"/> 3	206.3.0.13	Added	1	HNC42-LZA-0	ONVIF	80	Supercir	210235C
<input type="checkbox"/> 4	206.3.0.28	Added	1	HNC42-LZA-0	ONVIF	80	Supercir	210235C
<input type="checkbox"/> 5	206.3.0.29	Added	1	HNC512-A-0	ONVIF	80	Supercir	210235C



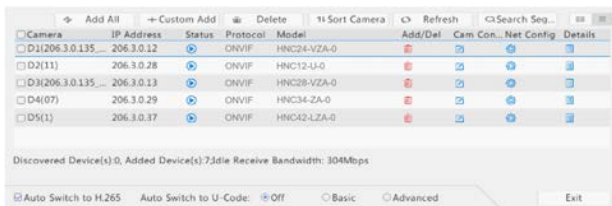
NOTE!

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.

6.1.2 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.



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.

6.2 Playback

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




NOTE!

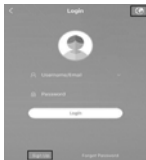
- A 7*24 (Continuous) recording schedule is enabled by default. To set a recording schedule manually, right click and select Menu > Storage > Recording and then set recording type and time based on your needs.
- If you choose Event type recording, you need to enable the corresponding alarm function and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

7 Guard Viewer mobile app


Please download **Guard Viewer** mobile app on the App Store (iOS) or on Google Play (Android) first.

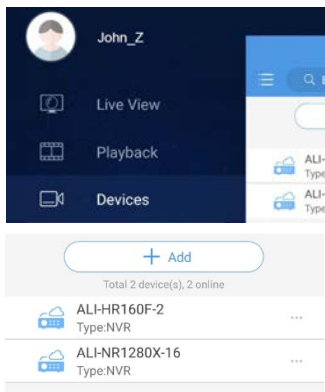
7.1 Sign Up an Account

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






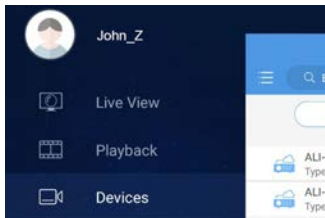
7.2 Add Devices

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.




7.3 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).



7.4 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.

8 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 required at first login. Close your browser during the installation.

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

Copyright Statement

All 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

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

Privacy Protection Reminder

The Provider 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. 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. The Provider 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 Provider 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 the Provider 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 non-infringement.

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

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

- **Change default password and create a 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 with digits, letters and special characters.
- **Keep firmware up to date:** Upgrade the firmware in your devices whenever new firmware becomes available. New firmware versions usually include the latest functions and better security. Visit The Provider's official website or contact your local dealer for the latest firmware.
- **Change password regularly:** Change the passwords of your devices on a regular basis and keep the password(s) secure. Make sure only authorized users 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 usernames and passwords 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. For improved security, 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, SNMPv3 is recommended.
- **Multicast:** Multicast is intended to transmit video to multiple devices. If you do not use this function, 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 from other service networks helps prevent unauthorized access to devices in your security system from other 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 and use the device in an environment that complies with the temperature and humidity shown in the specifications. The

environment should also be free of 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 all kinds.
- Make sure the power supply provides a stable voltage that meets the power requirements of the device. Make sure the power supply output power exceeds the total maximum power of all the devices connected to it.
- Verify that the device is properly installed before connecting it to a power source.
- Do not remove the seal from the device body without consulting the Provider. 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

- Installation and use of the device must be in strict accordance with local electrical codes.
- Use a UL certified power supply that meets LPS requirements if an adapter is used.
- Use a 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 ground connection.

- Ground your device properly in accordance with local codes.

Battery Use Caution

When a battery is used, avoid:

- High or low extreme temperatures during use, storage and transportation;
- Extremely low air pressure, or low air pressure at high altitudes;
- Use the battery properly. Improper use of a battery may cause fires, explosions or leakage of flammable or caustic liquids or gas.
- Replace a battery with only the correct type.
- Never dispose of a battery in a fire, a hot oven, or by crushing or cutting of a battery.

Personal safety warnings:

- **Chemical Burn Hazard.** This product contains a coin cell battery. Do not ingest the battery. If the coin cell battery is swallowed, it can cause severe internal burns in just 2 hours and can lead to death.
- Keep new and used batteries away from children.
- If the battery compartment does not close securely, stop using the product and keep it away from children.
- If you think batteries might have been swallowed or placed inside any part of the body, seek immediate medical attention.
- Dispose of used battery in accordance with 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.

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.