Supercircuits

Hybrid Digital Video Recorders

Quick Installation Guide

HVRH0401-0

HVRH0801-0

HVRH1602-0

SUPER CIRCUITS

HVRH0401-0801_1602-0-CQ
200903

1 Default IP, Username and Password

IP address: 192.168.1.30

Username: **admin**

Password: **123456**

NOTE!

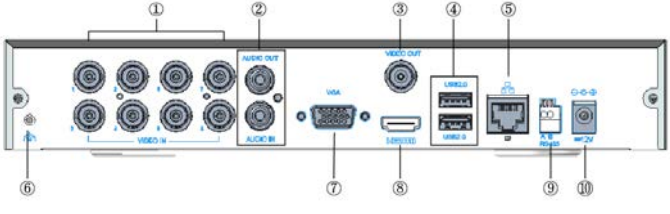
- For security, we strongly recommend that you set a strong password of at least nine characters with numbers, letters and special characters.

2 LEDs

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

3 Ports and Interfaces

Take One Model for Example.



Interface	Description	Interface	Description
①	Video input	②	Audio input / output
③	Video output	④	USB
⑤	Network	⑥	Grounding
⑦	VGA output	⑧	HDMI output
⑨	RS485	⑩	12 Vdc input

4 Disk Installation

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

4.1 Preparation

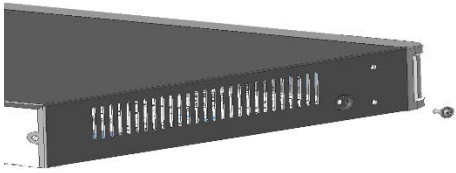
- Use a #1 or #2 Philips screwdriver.
- Use antistatic gloves or a wrist strap.
- Disconnect power and all interface cables before installation.

4.2 HDD Installation

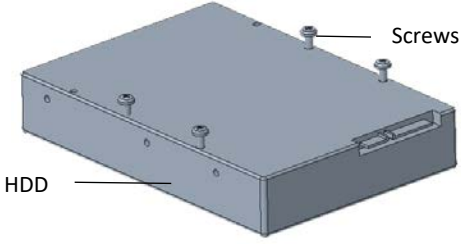
1. Loosen the cover screws on the rear panel and side panels, and then slide the cover back and up to remove it.

Figure 4-1 Rear Panel

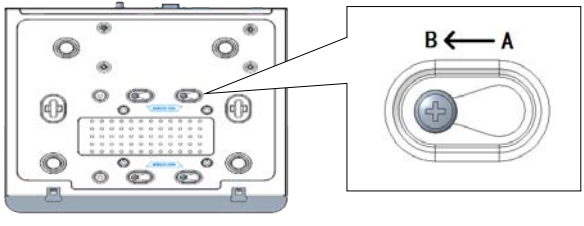
Figure 4-2 Side Panel



2. Insert the screws into the disk about 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.

5 Connect Devices

1. Connect the monitor to the recorder with a VGA or HDMI cable (cable not provided).
2. Connect a USB mouse to the recorder.
3. Connect analog cameras to a Video In interface on the back panel with a coaxial cable.
4. Connect a network cable to the recorder and a network switch.

NOTE!

Normally a network switch is used to connect the recorder to IP cameras on one network.

6 Startup

Connect the device to power and turn on the power switch (if applicable).

7 Add Cameras

7.1 Analog Camera

Connect analog cameras to the video in BNC connectors on the recorder back panel. Cables are not provided with the recorder or camera.

NOTE!

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

7.2 IP Camera

Make sure the IP camera is connected to the network.

1. Click **Menu > Camera > Camera**.
2. Click ✚ to add the camera to the recorder for monitoring.

NOTE!

- To search a specified network segment, click **Search Segment**.
- Normally all IP cameras discovered on the network can be added. If the status shows ▶, 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 camera settings if needed.

8 Change Camera Type

By default the recorder can add IP cameras for monitoring:

ALI-NR040F-1 – can add 2 IP cameras

ALI-NR080F-1 – can add 4 IP cameras

ALI-NR160F-2 – can add 8 IP cameras

You can add additional IP cameras by changing an unused analog port status to digital. Click **Menu > Camera > Camera > Camera Type** and change an unused Video In port to digital. An analog camera cannot be used on the port when the port is set to digital.

9 Recording and Playback

9.1 Recording

- For analog camera: Enable the recording schedule for the camera. Go to **Menu > Storage > Recording**.

NOTE!

When a recording schedule is enabled, the recorder will record even when no analog camera is connected.

- For IP camera, a continuous recording schedule is enable by default. To change this schedule, go to Menu > Storage > Recording.

9.2 Playback

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

10 Access Using a Web Browser

Access the deivce 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.

11 Access from Mobile App

Install the **Guard Tools Mobile** 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.

12 Shutdown

Click **Menu > Shutdown**.

CAUTION!

Do not disconnect power when the recorder is operating. A suddent power failure may damage the recorder and cause data loss.

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.