



Quick Start Guide

GD-RN-BP8616P

GD-RN-BP8632N

GD-RN-CT8832N

GD-RN-CT8864N

GD-RN-AT819128N

EN

Quick Guide

About this guide

The guide includes instructions for using and managing the product. Pictures, charts, images and all other information hereinafter are for description and explanation only. The information contained in the guide is subject to change, without notice, due to firmware updates or other reasons.

Please find the latest version at **WWW.GRUNDIG-SECURITY.COM**

Limitation of Liability / Legal Disclaimer

Abetechs GmbH (Grundig Security) undertakes all reasonable efforts to verify the integrity and correctness of the contents in this document, but no formal guarantee shall be provided. Use of this document and the subsequent results shall be entirely on the user's own responsibility. Abetechs GmbH (Grundig Security) reserves the right to change the contents of this document without prior notice. Design and specifications are subject to change without prior notice.

The product described herein, with its hardware, software and documentation is provided "as is", without any warranty, expressed or implies, including without limitation, merchantability, satisfactory quality, fitness for a particular purpose, and non-infringement of a third party.

In no event will our company and its employees or agents be liable to you for any special, consequential, incidental, or indirect damages, including among others, damages for loss of business profits, business interruption, or loss of data or documentation, in connection with the use of this product, even if our company has been advised of the possibility of such damages.

Regarding to products with internet access, the use of the product shall be wholly at your own risks. Our company shall not take any responsibilities for abnormal operation, privacy leakage or other damages resulting from cyber-attack, hacker attack, virus inspection, or other internet security risks; however our company will provide timely technical support if required. Surveillance laws vary by jurisdiction before using this product in order to ensure that your use conforms to the applicable law. Our company shall not be liable in the event that this product is used with illegitimate purposes.

In the event of any conflicts between this manual and the applicable law, the later prevails.

Trademark

Each of trademarks herein is registered. The name of this product and other trademarks mentioned in this manual are the registered trademark of their respective company.

Copyright of this document is reserved. This document shall not be reproduced, distributed or changed, partially or wholly, without formal authorization.

OPEN SOURCE SOFTWARE LICENSE INFORMATION

The software components provided with Grundig products may contain copyrighted software that is licensed under various open-source software licenses. For detailed information about the contained open-source software packages, the used package versions, license information and complete license terms, please refer to the product detail pages on our website. The complete open-source software license information is also included in firmware files

of affected products. Please also check your manuals for additional information.

You may obtain the complete corresponding open-source part of a specific product from us for a period of three years after our last shipment of this product by sending an email to: info@grundig-security.com

Safety and Installation Instruction

Introduction

Please read these instructions carefully and keep them for future reference. You must heed all the warnings and cautions as well as follow all the safety and installation instructions.

The appearance of the products, functions and firmware or software upgrade may differ from this manual.

GRUNDIG reserves the right to perform needed changes without prior notice.

Safety Instructions

Make sure that you only use the power adapter that is specified in the specifications sheet of the product. If you use any other adapter or connect the power supply incorrectly, this may cause explosion, fire, electric shocks or damage the product. Do not connect several devices to one power adapter as this may cause an adapter overload and can lead to over-heating and fire. Make sure that the plug of the power adapter is firmly connected to the power socket.

Do not place containers with liquids on the product. Do not place conducting items like tools, screws, coins or other metal items on the product. These may fall from the product or can cause fire or electric shocks or other physical injuries.

Do not push or insert any sharp items or any objects into the device as this may cause damage to the product, fire, electric shocks and/or physical injuries.

Do not block any ventilation openings, if there are any. Ensure that the product is well ventilated to prevent any over-heating. Do not subject the device to physical shock or drop the product.

If the product uses batteries, please use a battery type that is recommended by the manufacturer. Improper use or replacement of the battery may result in the hazard of explosion.

Do not use any accessories that are not recommended by GRUNDIG. Do not modify the product in any way.

If the product starts to smell or smoke comes out of the device, immediately stop using the product and disconnect it from the power supply to prevent fire or electric shocks. Then contact your dealer or the nearest service center.

If the product does not work correctly, contact your dealer or nearest service center. Never open, disassemble or alter the product yourself. GRUNDIG cannot accept any liability or responsibility for problems caused by attempted and unauthorized repair and maintenance.

Installation Instructions

It is necessary to fix the device firmly if the product is installed on a wall or ceiling. Do not install the product on surfaces or in places that are vibrating. Do not install the product near radiation sources.

Do not install the product near heat sources, like radiators or other equipment that produces some heat. If the product is not classified by any IP class, do not install the product in very cold or hot temperatures (please refer to the working temperature specified in the specification sheet of the product), dusty, dirty or damp environment.

If the product is classified by any IP class, never touch the product cover directly with your fingers, because the acidic sweat of the fingers may damage the surface coating of the product cover. To clean the inside and outside of the product cover, use a soft and dry cloth. In any case, do not use alkaline detergents. The correct configuration of all passwords and other security settings is the sole responsibility of the installer and/or end-user (this applies especially to IP Cameras and Recorders).

Special Installation Instructions for Recorders (NVRs and DVRs)

Make sure that the last actual firmware is installed on the IP Device. You may get the actual firmware from tech-support@grundig-security.com.

Make sure that the product is secured after installation and locate the recorder in safe places where children are not able to reach it.

Make sure the device is properly secured to a rack or shelf. Major shocks or jolts to the unit as a result of dropping it may cause damage to the sensitive electronics within the unit.

Make sure the device is installed in a room that is well-ventilated and dust-free.

Power down the unit before connecting and disconnecting accessories and peripherals.

Only use an HDD for this device that is recommended by GRUNDIG.

The USB flash drive can only be connected to the USB-port of the device.

Use the device in conjunction with an UPS if possible.

To clean the product, gently wipe the outside with a clean dry cloth.

Table of content

| | |
|---|----|
| 1 Rear Panel Interfaces Description | 9 |
| 2 Installation and Connections | 10 |
| 2.1 NVR Installation | 10 |
| 2.2 HDD Installation | 10 |
| 2.2.1 Bracket Installation | 10 |
| 2.2.2 Front Panel Installation | 11 |
| 2.2.3 HDD Case Installation | 12 |
| 3 Menu Operation | 13 |
| 3.1 Startup | 13 |
| 3.2 Activate Device | 13 |
| 3.3 Set Unlock Pattern | 15 |
| 3.4 User Login | 16 |

| | |
|--|----|
| 3.5 User Logout, Shutdown and Reboot | 16 |
| 3.6 Network Settings | 17 |
| 3.6.1 Configure TCP/IP Settings | 17 |
| 3.6.2 Configure SCMS | 18 |
| 3.7 Add IP Cameras | 19 |
| 3.8 Live View | 20 |
| 3.9 Recording Settings | 20 |
| 3.10 Playback | 20 |
| 4 Accessing by Web Browser | 22 |

1 Rear Panel Interfaces Description

Rear view of the recorder GD-RN-BP8616P. The rear panel interfaces vary with different models.

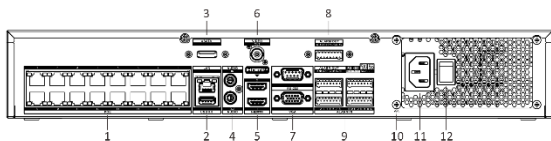


Figure 1-1 Connections on the rear panel

Refer to Table 1-1 for the common interface description of rear panels.

Table 1-1 Common Interfaces Description of Rear Panels

| No. | Description | No. | Description |
|-----|--------------------------|-----|---------------------------|
| 1 | PoE Network-Interfaces | 7 | VGA & RS232 interfaces |
| 2 | USB 3.0 & LAN interfaces | 8 | Alarm out |
| 3 | eSATA interface | 9 | Alarm IN/OUT, RS485 |
| 4 | Audio input/output | 10 | GND |
| 5 | HDMI 1&2 interfaces | 11 | 100 – 240 VAC power input |
| 6 | CVBS out | 12 | Power switch |

2 Installation and Connections

2.1 NVR Installation

During installation of the NVR:

- Use the supplied brackets for rack mounting.
- Ensure ample room for audio and video cables.
- When routing cables, ensure the bend radius of the cables are no less than five times of its diameter.
- Allow at least 2 cm (≈ 0.75 inch) of space among racks mounted devices.
- Ensure the NVR is grounded.
- Environmental temperature should be within the range of working temperature.
- Environmental humidity should be within the range of 10% to 90%.

2.2 HDD Installation

For NVR that has not been pre-installed HDD, it requires to install HDD for storage.

Before you start

- Ensure power is disconnected.
- Prepare a factory recommended HDD, and cross screwdriver.

2.2.1 Bracket Installation

Bracket installation is applicable when it requires to remove the device cover, and install HDD on the internal bracket.

Steps

- Step 1 Unfasten screws on the back, and push the cover backwards to remove the cover. Refer to Figure 2-1.
- Step 2 Fix the HDD on the bracket with screws. Refer to Figure 2-2.

Note

Please uninstall the upper layer bracket first before installing HDD on the lower layer bracket.

- Step 3 Connect the data cable and power cable. Refer to Figure 2-3.

Note

You can repeat the steps above to install other HDDs.

- Step 4 Reinstall the device cover and fasten screws.

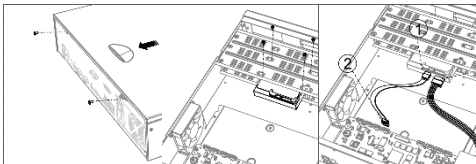


Figure 2-1 Remove
Cover

Figure 2-2 Fix HDD

Figure 2-3 Connect
Cable

2.2.2 Front Panel Installation

Front panel plug-pull installation is applicable when you need to open the device front panel with key and install the HDD.

- Step 1 Fix mounting ears to HDD with screws, Fig. 2-4.
- Step 2 Unlock the front panel with the attached key, and press the buttons on both sides of the front panel to open it, Fig. 2-5.
- Step 3 Insert the HDD until it is fixed firmly, Fig 2-6.
- You can repeat the steps above to install other HDDs.
- Step 4 Optional: Repeat the steps above to install other HDDs.
- Step 5 Close the front panel and lock it with key.

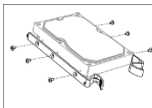


Figure 2-4 Fix
mounting ears to
HDD

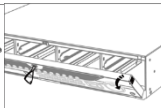


Figure 2-5 Open
frontpanel

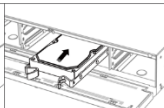


Figure 2-6 Insert
HDD

2.2.3 HDD Case Installation

HDD case installation refers to the method that you install the HDD in the case, and then plug the HDD case into the slot.

Steps

1. Unlock the front panel with panel key.
2. Pull the front panel out of the device and make it a little above the left handle.

Note

The angle between front panel and the device must be within 10°.

3. Press the blue button to pop up the handle and hold the handle and pull the HDD case out of the slot.
4. Fix the hard disk in the HDD case.
 - 1) Place an HDD in the case. The SATA interface must face the case bottom.
 - 2) Adjust the HDD position. Ensure the hard disk rear aligns with HDD bottom.
 - 3) Use a screwdriver to fasten the four screws into the screw holes in both sides.
5. Push the HDD case back into the slot.

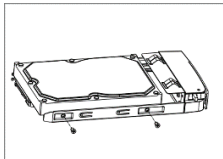


Figure 2-7 Fix HDD

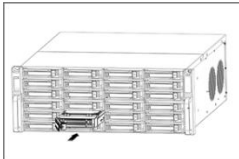


Figure 2-8 Push HDD case into slot

6. Press the handle until you hear a click. Thus to fix the HDD case.
Repeat above steps to install the rest hard disk boxes.

7. Close the front panel, and lock it with the panel key.

3 Menu Operation

3.1 Startup

Proper startup is crucial to expand the life of NVR. It is **HIGHLY** recommended to use an uninterruptible Power Supply (UPS) with the device.

Step 1 Plug power supply into an electrical outlet.

Step 2 Press the power button (certain models may have power button on the front or rear panel). The device begins to start.

3.2 Activate Device

No operation is allowed before activation. For the first-time access, it requires to set an admin password for device activation. You can also activate the device via web browser, IP-Finder tool or client software.

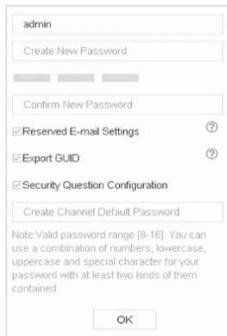
Step 1 Enter the same password in **Create New Password** and **Confirm New Password**.

STRONG PASSWORD RECOMMENDED—We highly recommend you create a strong password of your own choosing (Using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters.) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

Step 2 Optionally, check **Reserved E-mail Settings**, **Export GUID**, or **Security Question Configuration** for password resetting in the future.

Step 3 Enter the password in **Create Channel Default Password** to activate the network camera(s) connected to the device.

Step 4 Click **OK** to save the password and activate the device.



The screenshot shows a configuration window titled "Set Admin Password". It contains the following elements:

- A text field with "admin" entered.
- A "Create New Password" button.
- A password strength indicator consisting of three bars.
- A "Confirm New Password" text field.
- Three checked checkboxes: "Reserved E-mail Settings", "Export GUID", and "Security Question Configuration". Each checkbox has a question mark icon to its right.
- A "Create Channel Default Password" button.
- A note: "Note: Valid password range [8-16]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained."
- An "OK" button at the bottom.

Figure 3-1 Set Admin Password

next steps:

- When you have enabled **Reserved E-mail Settings**, continue to set the reserved email for the future password resetting.
- When you have enabled **Export GUID**, continue to export the GUID file to the USB flash drive for the future password resetting.
- When you have enabled **Security Question Configuration**, continue to set the security questions for the future password resetting.

3.3 Set Unlock Pattern

Admin user can use the unlock pattern to login. You can configure the unlock pattern after the device is activated.

Steps

Step 1 Use mouse to draw a pattern among the 9 dots on the screen. Release the mouse when the pattern is done.

Note

- The pattern shall have 4 dots at least.
- Each dot can be connected for once only.

Step 2 Draw the same pattern again to confirm it. When the two patterns match, the pattern is configured successfully.

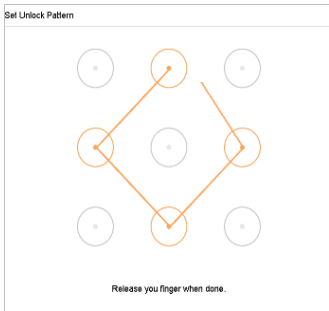


Figure 3-2 Draw the Unlock Pattern

3.4 User Login

You have to log in to the device before operating the menu and other functions.

Step 1 Select **User Name**.

Step 2 Enter password for the selected user.

Step 3 Click **OK** to log in.

Note

For the admin, if you have entered the wrong password for 7 times, the account will be locked for 60 seconds. For the operator, if you have entered the wrong password for 5 times, the account will be locked for 60 seconds.

3.5 User Logout, Shutdown and Reboot

You can log out of the system, shut down, or reboot the device.

Step 1 Click  on the menu bar.

Step 2 Click **Logout**, **Shutdown**, or **Reboot** as your desire.

3.6 Network Settings

3.6.1 Configure TCP/IP Settings

TCP/IP settings must be properly configured before you can operate the device over a network.

Steps

1. Go to System → Network → TCP/IP

The screenshot displays the 'TCP/IP' configuration page for the 'Lan1' interface. At the top, there are tabs for 'TCP/IP', 'DDNS', 'PPPoE', 'Port', and 'NAT'. Below the tabs, the 'Lan1' interface is selected. The configuration fields are as follows:

| Parameter | Value | Status |
|-------------------------------|-------------------------|--------|
| NIC Type | Auto | |
| <input type="checkbox"/> DHCP | | |
| IPv4 Address | 10.22.1.100 | ✓ |
| IPv4 Subnet Mask | 255.255.255.0 | ✓ |
| IPv4 Default Gateway | 10.22.1.1 | ✓ |
| IPv6 Address | fe80::a6da:22ff:fea0:ae | |
| Subnet Prefix Length | ffff:ffff:ffff:: | |
| IPv6 Default Gateway | | |
| Mac Address | a4:da:22:a0:00:ae | |
| MTU | 1500 | ✓ |

Figure 3-3 TCP/IP setting

2. Configure network parameters as needed.

Note

- Check Enable DHCP to obtain IP settings automatically if a DHCP server is available on the network.
- Valid MTU value range is from 500 to 1500.

3. Click **Apply**.

3.6.2 Configure SCMS

SCMS provides mobile phone application and platform service to access and manage your connected devices, which enables you to get a convenient remote access to the surveillance system.

Step 1 Go to **System > Network > Advanced > Platform Access**.

Step 2 Check **Enable** to activate the function. Then the service terms will pop up.

- 1) Enter a verification code in **Verification Code**.
- 2) Scan the QR code to read the service terms and privacy statement.
- 3) Check **the SCMS service will require internet access**.
Please read Service Terms and Privacy Statement before enabling the service if you agree the service terms and privacy statement.
- 4) Click **OK** to save the settings.

Note

- SCMS is disabled by default.
- The verification code is empty by default. It must contain 6 to 12 letters or numbers, and it is case sensitive.

Step 3 (Optional) Check **Custom** to enter the server address as your desire.

Step 4 (Optional) Check **Enable Stream Encryption**, verification code is required for remote access and live view.

Step 5 Click **Apply**.

next steps:

After configuration, you can access and manage your devices through SCMS app or website.

3.7 Add IP Cameras

Before you can get live video or record the video files, you should add network cameras to the device.

Before you start

Ensure the network connection is valid and correct, and the IP camera to add has already been activated. Please refer to the *User Manual* for activating the inactive IP camera.

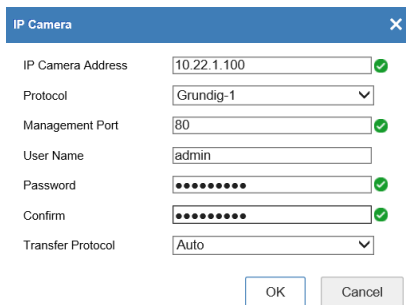
Steps

Step 1 Go to **Configuration > System > Camera Management**.

Step 2 Click **Add**.

Step 3 Enter IP address, protocol, management port, and other information of the IP camera.

Step 4 Click **OK**.



| | | |
|-------------------|-------------|---|
| IP Camera Address | 10.22.1.100 | ✓ |
| Protocol | Grundig-1 | ▼ |
| Management Port | 80 | ✓ |
| User Name | admin | |
| Password | •••••••• | ✓ |
| Confirm | •••••••• | ✓ |
| Transfer Protocol | Auto | ▼ |

OK Cancel

Figure 3-4 Add IP Camera

3.8 Live View

Enter the live view mode



- You can select a window and double click a camera from the list to play the video from the camera in the selected window.
- Use the toolbar at the playing window bottom to achieve functions of capture, instant playback, audio on/off, digital zoom, live view strategy, show information and start/stop recording.

3.9 Recording Settings

Before you start

Make sure that the disk has already been installed.

Steps

1. Go to **Storage > Schedule > Record**.
2. Select a camera.
3. Check **Enable Schedule**.
4. Select a recording type. The record type can be continuous, motion detection, alarm, motion or alarm, motion and alarm, event, etc.
5. Select a day and drag the cursor on the time bar to set the record schedule.
6. Click **Apply**.

3.10 Playback

The recorded video files and pictures on HDD can be played back. Refer to the user manual for details of each playback mode.

Steps

1. Go to Playback.



Figure 3-5 Playback

2. Select camera(s) in the list.
3. Double click a date on the calendar.
4. Use the toolbar at the bottom to control the playing progress

4 Accessing by Web Browser

You can get access to the device via web browser. The following web browsers are supported: Internet Explorer 11, Apple Safari V12, Mozilla Firefox V52, Edge V89, and Google Chrome V57. The supported resolutions include 1024*768 and above.

Note

The use of the product with Internet access might be under network security risks. For avoidance of any network attacks and information leakage, please strengthen your own protection. If the product does not work properly, please contact with your dealer or the nearest service center.

Steps

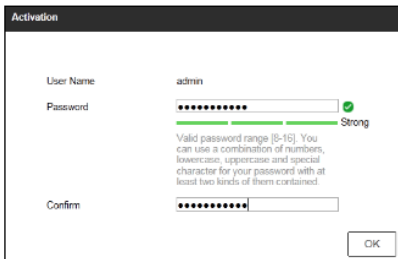
Step 1 Open web browser, enter the IP address of the device and then press **Enter**.

Step 2 Log in to the device.

- If the device has not been activated, activate the device first by setting the password for the admin user account.

STRONG PASSWORD RECOMMENDED—We highly recommend you create a strong password of your own choosing (Using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters.) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

- If the device is already activated, enter the user name and password to log in.



The image shows a software activation window titled "Activation". It contains three input fields: "User Name" with the text "admin", "Password" with masked characters and a green checkmark, and "Confirm" with masked characters. Below the password field is a green progress bar and the word "Strong". A text block explains the password requirements: "Valid password range [8-16]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained." An "OK" button is located at the bottom right.

| | |
|-----------|------------|
| User Name | admin |
| Password | •••••••••• |
| Confirm | •••••••••• |

Valid password range [8-16]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained.

Strong

OK

Figure 4-1 Activate the Device

Follow the installation prompts to install the plug-in before viewing the live video and managing the device.

Note

- You may have to close the web browser to finish the installation of the plug-in.
- After login, you can perform the operation and configuration of the device, including the live view, playback, log search, configuration, etc.

QG-GD-RN-BP8616P-2023-10-02-V5-EN ©ABETECHS GMBH, DÜSSELDORF, GERMANY

grundig-security.com

GRUNDIG