Quick Start Guide

GD-RT-AP8004P
GD-RT-AP8008P
GD-RT-AP8016P
GD-RT-AP8016N
GD-RT-AT8016N

EN

grundig-security.com

GRUNDIG

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.

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 www.grundig-security.com. The complete open-source software license

information is also included in firmware files of affected products. Please also check your product's CD-ROM and 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 techsupport@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

The rear panel interfaces vary with different models. Refer to Table 1-1 for the common interface description of rear panels.

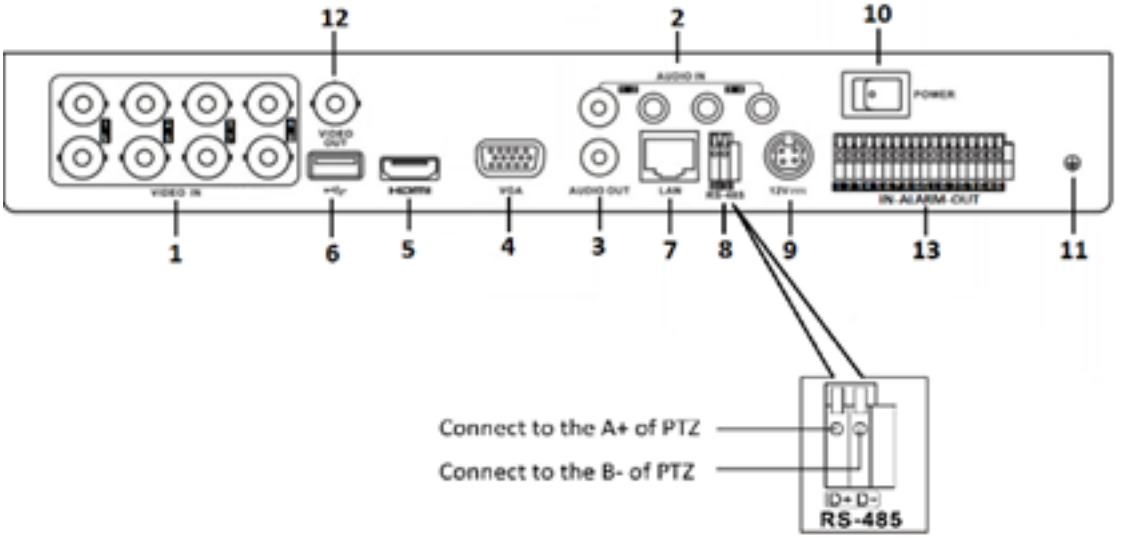

Figure 1-1 Rear panel

Table 1-1 Common Interfaces Description of Rear Panels

Item	Description	Item	Description
1	Video Inputs	8	RS485 Interface
2	Audio Inputs	9	48 VDC Power Input
3	Audio Output	10	Power Switch
4	VGA Output	11	Ground
5	HDMI Output	12	BNC Output
6	e-SATA	13	Alarm IN/OUT
7	LAN Interface		

2 Installation and Connections

2.1 DVR Installation

During installation of the DVR:

- Use 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 DVR is grounded.
- Environmental temperature should be within the range of -10 °C to 55 °C (14 °F to 131 °F).
- Environmental humidity should be within the range of 10% to 90%.

2.2 HDD Installation

For DVR 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.

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.

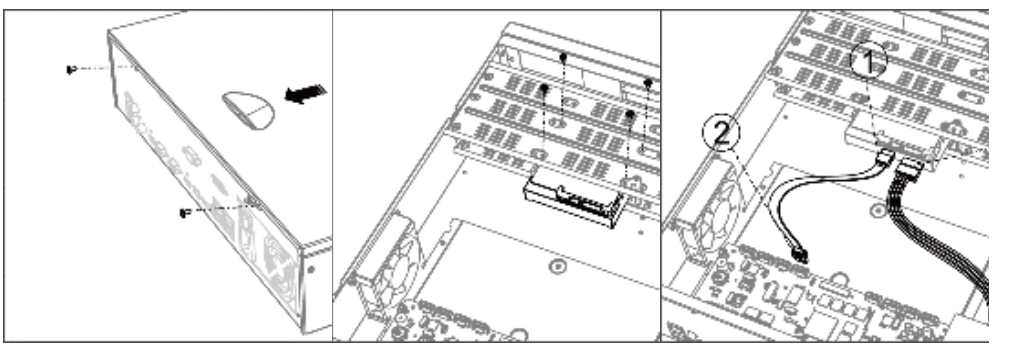

Figure 2-1 Remove Cover Figure 2-2 Fix HDD Figure 2-3 Connect Cable

2.2.2 Fix-on-Bottom Installation

Fix-on-bottom installation is applicable when it requires to install the HDD at the internal bottom.

Step 1 Unfasten screws on each panel to remove the device cover. Refer to Figure 2-4.

Step 2 Connect the data cable and power cable. Refer to Figure 2-5.

Step 3 Match HDD screw threads with the reserved holes on the device bottom, and fix HDD with screws. Refer to Figure 2-6.

Note

You can repeat the steps above to install other HDDs.

Step 4 Reinstall the device cover and fasten screws.

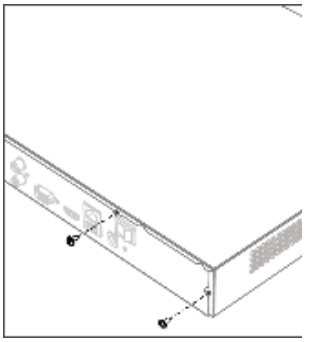

Figure 2-4 Remove Cover

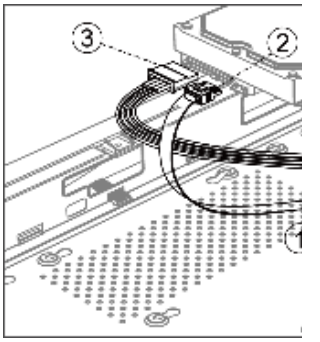

Figure 2-5 Connect Cable

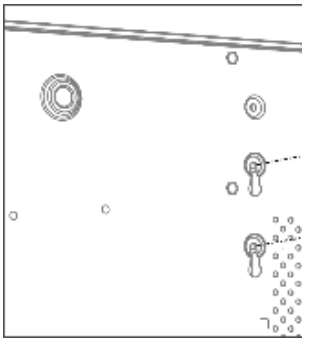

Figure 2-6 Fix HDD

2.3 RS-485 and Camera Connection

Use RS- 485 interface to connect a PTZ-camera with DVR.

Before you start

Ensure both camera and DVR are grounded.

Step 1 Pull out the pluggable block at the RS-485 terminal block.

Step 2 Press and hold the orange part of the pluggable block, insert signal cables into slots.

Step 3 Release the orange part. Ensure signal cables are in tight.

Step 4 Connect A+ on PTZ to D+ on terminal block and B- on PTZ to D- on terminal block.

Step 5 Plug pluggable block back into terminal block.

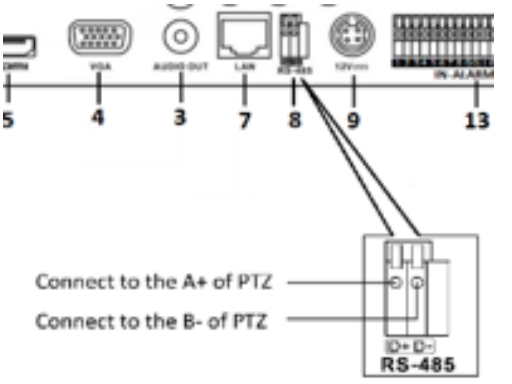

Figure 2-7 PTZ Connection

3 Menu Operation

3.1 Startup

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

Plug power supply into an electrical outlet. 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.

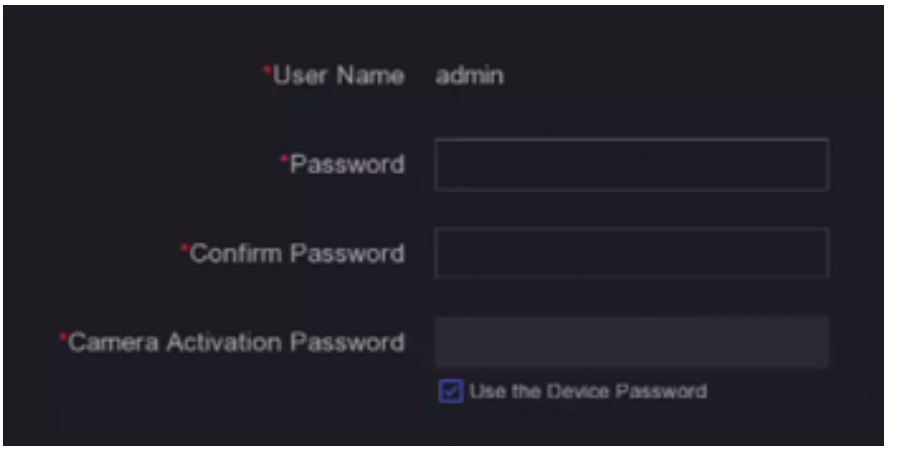

Figure 3-1 Set Admin Password

When you have enabled **Reserved E-mail Settings**, continue to set the reserved email for the future password resetting.

3.3 Set Unlock Pattern

For the Admin user, you can configure the unlock pattern for device login.

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.

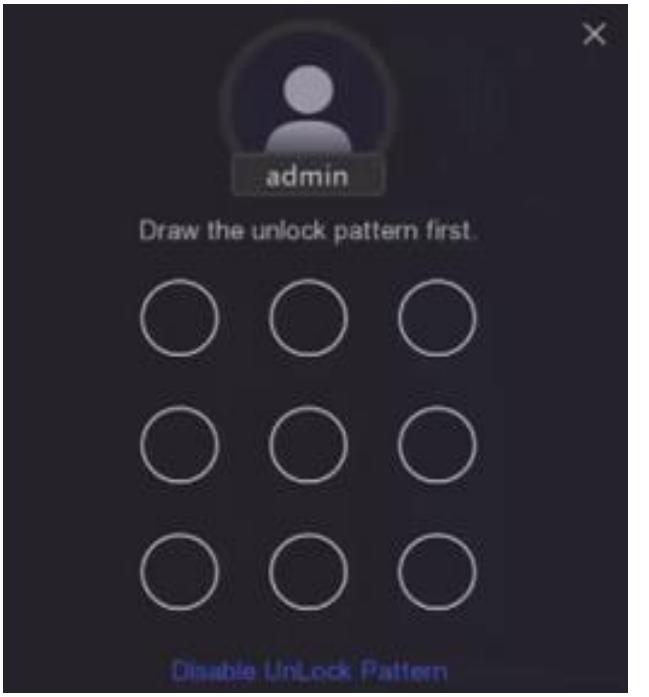

Figure 3-2 Draw the Unlock Pattern

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 Configure Signal Input

For certain models, you can configure the analog and IP signal input types and enable 5 MP long distance transmission.

Step 1 Go to **Camera** > **Camera** > **Analog**.

Step 2 Set the analog signal input channels and types, and the connectable maximum IP camera number. Disabling analog channel(s) would increase the connectable IP camera number.

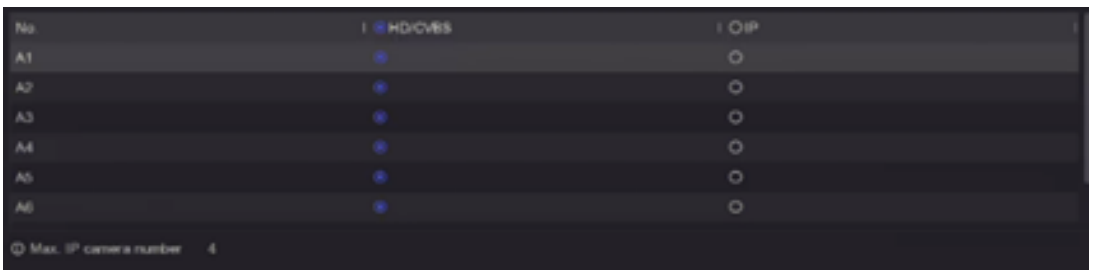

Figure 3-3 Signal Input Status

3.7 Add Network 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 network camera has already been activated.

Step 1 Go to **Configuration** > **Camera** > **IP Camera**.

Step 2 Click  .

Step 3 Set the IP camera parameters, including IP address, protocol, management port, etc. You can enable **Use Camera Activation Password** to use the device password to add the IP camera.

Step 4 (Optional) Click **Add More** to add other IP cameras.

Step 5 Click **OK**.

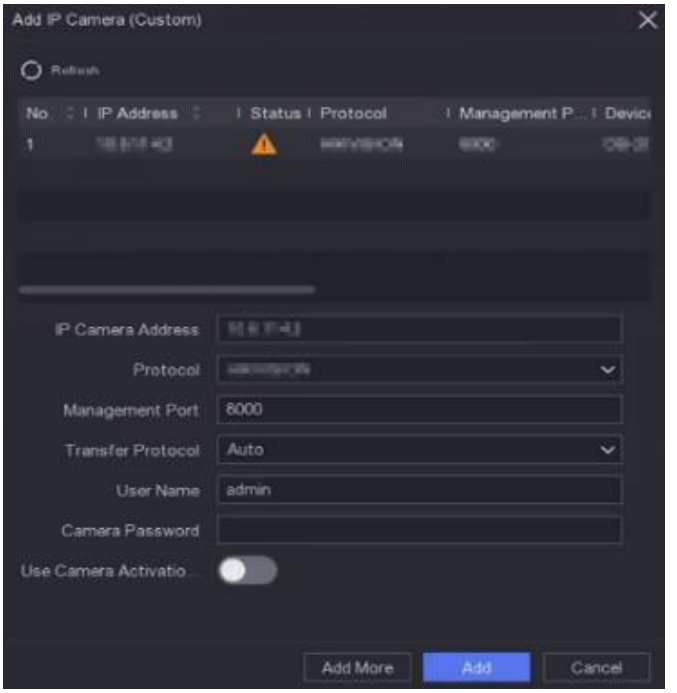

Figure 3-4 Signal Input Status

3.8 Connect PoC Cameras

The Grundig models GD-RT-AP8004P, GD-RT-AP8008P and GD-RT-AP8016P support PoC (Power over Coaxitron) cameras connection. The DVR will detect the connected PoC cameras automatically, manage the power consumption via the coaxial communication, and provide power to the cameras via coaxitron.

Before you start

- Ensure your device supports PoC (Power over Coaxitron) cameras connection.
- Ensure your device has free analog channel resource. The analog channel resource is configurable in **Configuration** > **Camera** > **Analog**.
- Connect the PoC camera to the DVR.

Note

Only specified PoC camera is supported. Please turn off the PoC function if the camera does not support PoC, or the camera is not produced by the same manufacture. Otherwise, it may result in permanent damage to the camera or DVR.

Step 1: Go to **Configuration > Camera > Analog > PoC Setting**.

Step 2: Turn on the PoC for the channel(s) as your desire.

Step 3: Check the status of connected PoC camera.

If the power consumption of the DVR is lower than that of AF camera, when AF or AT camera is connected, there is no video and **Insufficient Power for PoC** would be overlaid on the live view image.

If the power consumption of the DVR is higher than that of the AF camera and lower than that of the AT camera, when AF camera is connected, it would be powered on normally; when AT camera is connected, it would be powered on and then powered off, thereafter, the DVR displays **Insufficient Power for PoC** on the live view image.

If the power consumption of the DVR is higher than that of the AT camera, when AF or AT camera is connected, it would be powered on normally.

Step 4: Check the connected AF or AT camera number and the connectable camera number.

Note

The maximum connectable AT/AF camera number varies according to different models.

3.9 Network Settings

3.9.1 Configure General Settings

You shall properly configure the network settings before you operate DVR over network.

Step 1 Go to **System** > **Network** > **General**.

Step 2 Set the network general parameters.

Step 3 Click **Apply** to save the settings.

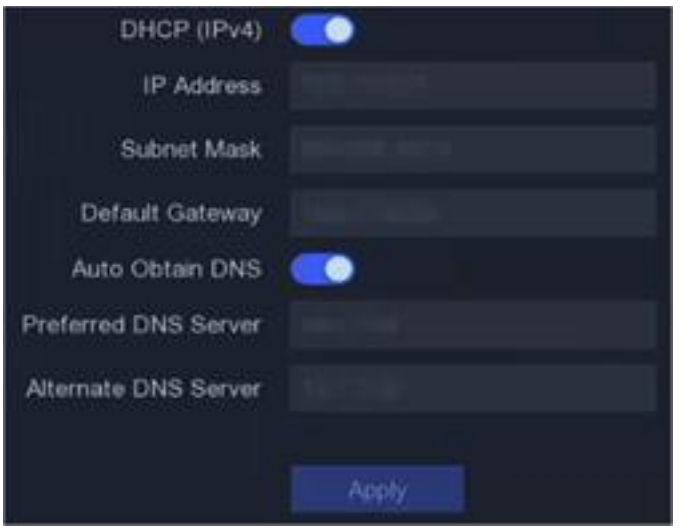

Figure 3-5 Network Settings

3.9.2 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.

3.10 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.

3.11 Recording Settings

Before you start

Make sure that the disk has already been installed. If not, please install a disk and initialize it. You may refer to the user manual for detailed information.

In the live view mode, select a connected camera window and click  at the toolbar to start recording.

3.12 Playback

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

Step 1 Go to **Playback**.

Step 2 Choose any channel(s) from the channel list.

Step 3 Double click a date on the calendar.

Step 4 (Optional) Use the toolbar in 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 6.0, 7.0, 8.0, 9.0 & 10.0, Apple Safari, Mozilla Firefox, and Google Chrome. 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.

Step 5 Open web browser, enter the IP address of the device and then press **Enter**.

Step 6 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.

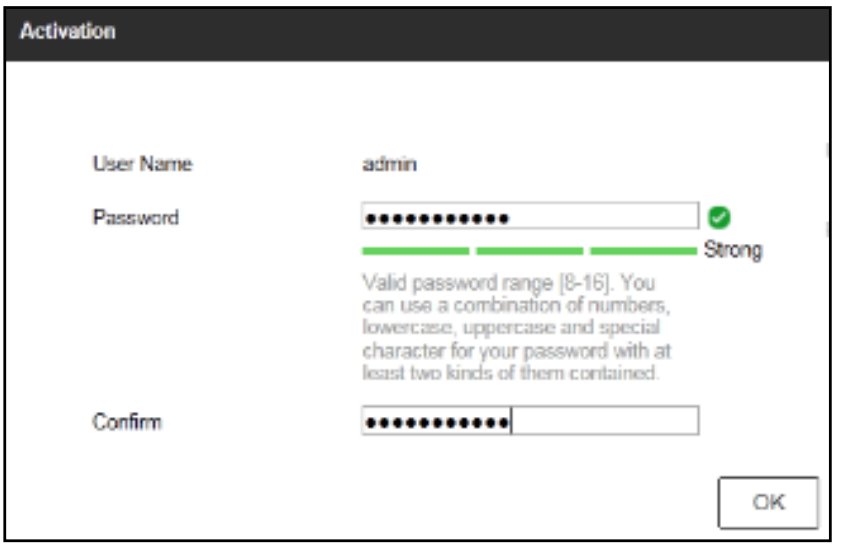

Figure 3-6 Activate the Device

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.

grundig-security.com

GRUNDIG