

## Release Notes for IP-Devices

The reproduction, distribution, use, or disclosure of this document to third parties without express permission is prohibited; violations will render the perpetrator liable for damages. All rights are reserved, including but not limited to patents, utility models, and design rights.

The manufacturer assumes no liability for material or financial losses resulting from minor defects in the product or documentation—e.g., printing or spelling errors—unless these defects are due to intent or gross negligence on the part of the manufacturer.

Specifications are subject to change without notice. Errors and omissions excepted.

Abetechs GmbH (Grundig-Security), [www.grundig-security.com](http://www.grundig-security.com)

## About this document

This document describes the standardized procedure for firmware updates on IP devices. Its goal is to ensure a secure and consistent update process and to minimize operational disruptions and downtime.

It contains information about new features and bug fixes in the new firmware. Furthermore, it explains the basic steps for performing the firmware update and the necessary checks after installation.

## Instructions for installing firmware

Firmware installation involves several steps and should be carefully prepared to avoid malfunctions or damage to the device. First, it is important to determine the exact model and the corresponding hardware version, as firmware is always model-specific. Then, download the appropriate firmware approved by Grundig. Before updating, read the relevant notes and version information, as these contain important information about changes or special requirements. You must also ensure that the device has a reliable power supply throughout the entire process and is connected to the network via a network cable. If possible, it is also advisable to back up the current configuration of the device.

After preparation, switch on the device and connect it to the network. You can then access the device's web interface using a web browser via the IP-address you have determined. Log in there with the administrator access data. The firmware update function can be found in the System → Maintenance menu area. Use this option to select the firmware file you downloaded earlier and start the update. During the update process, the device must not be switched off or disconnected from the network, and the browser should not be closed, as this may cause the update to be interrupted. The process may take several minutes.

Once the update is complete, the device will usually restart automatically. As soon as it is accessible again, access the web interface once more to check the installed firmware version. You should then check that all basic functions such as live image, network connection, and, if applicable, recording are working properly. If you saved a configuration previously, you can now restore it. Finally, it is recommended to check security-related settings such as passwords, date, time, and time zone, and to test new or changed firmware functions.

**FW-Version:** V8.2.4.1\_250611

**Release Date:** 2025, June 11th

It is recommended to upgrade from earlier versions only. Deinstallation of the previous version is not required.

### Supported Products:

Category	Model
Panoramic	GU-CI-AP8616Q

### Improvements/Changes:

- 1: An ONVIF report is required, ONVIF Testreport/Feature list/Guide\_Interface
2. Support cross month search, if the start time exceeds the end time and returns, it will fail.
3. The current version of the audio encoding only has the default PCMA encoding. The V21.45.8.2.4.2.1-241026 version includes both PCMA and PCMU encoding for the customer.
4. API/Login/DeviceInfo/Get request, "RecFileType": "MP4", "RecFileType": "GU" fields are duplicated;
5. When IPC uses/API/PReview/StreamURL/Get to obtain RTSP URL examples, manually changing the port to 555, the obtained example port is still 554
6. The ExaqVision CMS platform cannot receive Motion recordings after opening metadata General;
7. Translation needs to be updated,

The prompt when repeatedly logging into the WEB is kicked out is:

- English localization: New connection token has been used, and the current session has been canceled.
  - Russian localization: И с п о л ь з о в а н н ы й т о к е н с о е д и н е н и я , т е к у щ а я с е с с и я а н н у л и р о в а н а .
  - German localization: Es wurde ein neues Verbindungstoken verwendet, und die aktuelle Sitzung wurde abgebrochen..
8. When manually changing the HTTP port to 82, if not restarted, the device will fail to pull the stream.
    - C:\ffmpeg\bin\ffmpeg.exe-rtsp\_transporthttp-i " rtsp://admin:OutdoorCAM1@172.26.7.39:82/rtsp/streaming? channel=01&subtype=0"
  - 9: Support SFTP, add Dir name support for creating subdirectories, add Test button
  - 10: The timestamp format for event check needs to be modified to "2025-02-07T15:19:47Z+00:00"

- 11: Support RTCP
- 12: HTTP API reset password,/API/RecoverPassword request body to remove the "email\_flag" field
13. Modify ONVIF probe to obtain device parameters in the following format (519)
14. Shielding IR/white light lights up, triggering Tampering alarm when switching images
15. Support this API (/API/Layback/LaybackRtspURL/Get) to query RTSPURL examples;
16. Video Tampering Triggered, Missing Record in WEB Log Query (DVCM-535)
- 17: Cloud plugins should support HTTP ports
- 18: P2P only connects to European servers
19. Plugin version -1.22.24, see attachment
- 20: Customizing Direct Cloud functionality requires support for unbinding plugins and displaying device information on the Direct Cloud Information page. Plugin device information can be accessed through <http://127.0.0.1:6790/status> Obtain - see attachment for reference
21. Device name and Device type display the customer model, and the motherboard model must be burned with at least 15 digits
22. After filling in the address on the Cloud page, the plugin connection did not display the token and lacked dynamic device information
23. After entering the new address, the address of the cloud did not change.
24. Modify NVR to enable ETR and delete IPC, IPC cannot configure stream parameters;
25. Modify the RTP timestamp for video playback with IPC sending errors
26. After modifying the ONVIF request GetNodes and  $\infty$  configurationOption, devices without PanTilt will also return a support response
27. Support SFTP, add Dir name support for creating subdirectories, and add Test button. The current version does not open sub directory input boxes, and IE does not support special character filling and testing buttons.
- 28: The default setting for the resolution of the second stream is 1024x288
- 29: The default exposure time is set to 1/25
30. The new logic for metadata push needs to be changed to intelligent alarm information carried out through RTP

## **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 implied, 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.

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](mailto:info@grundig-security.com).