

## Versionshinweise für IP-Geräte

Die Vervielfältigung, Verbreitung, Verwendung oder Weitergabe dieses Dokuments an Dritte ohne ausdrückliche Genehmigung ist untersagt; Zuwiderhandlungen verpflichten den Verursacher zum Schadenersatz. Alle Rechte vorbehalten, einschließlich, aber nicht beschränkt auf Patente, Gebrauchsmuster und Designrechte.

Der Hersteller übernimmt keine Haftung für materielle oder finanzielle Schäden, die durch geringfügige Mängel am Produkt oder in der Dokumentation – z. B. Druck- oder Rechtschreibfehler – entstehen, es sei denn, diese Mängel sind auf Vorsatz oder grobe Fahrlässigkeit seitens des Herstellers zurückzuführen.

Technische Daten können ohne vorherige Ankündigung geändert werden. Irrtümer und Auslassungen vorbehalten.

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

## Über dieses Dokument

Dieses Dokument beschreibt das standardisierte Verfahren für Firmware-Updates auf IP-Geräten. Ziel ist es, einen sicheren und konsistenten Update-Prozess zu gewährleisten und Ausfallzeiten und Betriebsunterbrechungen zu minimieren.

Es enthält Informationen zu neuen Funktionen und Fehlerbehebungen in der neuen Firmware. Darüber hinaus werden die grundlegenden Schritte zur Durchführung des Firmware-Updates und die erforderlichen Überprüfungen nach der Installation erläutert.

## Anweisungen zur Installation der Firmware

Die Installation der Firmware umfasst mehrere Schritte und sollte sorgfältig vorbereitet werden, um Fehlfunktionen oder Schäden am Gerät zu vermeiden. Zunächst ist es wichtig, das genaue Modell und die entsprechende Hardwareversion zu ermitteln, da die Firmware immer modellspezifisch ist. Laden Sie dann die entsprechende, von Grundig zugelassene Firmware herunter. Lesen Sie vor der Aktualisierung die entsprechenden Hinweise und Versionsinformationen, da diese wichtige Informationen zu Änderungen oder besonderen Anforderungen enthalten. Außerdem müssen Sie sicherstellen, dass das Gerät während des gesamten Vorgangs zuverlässig mit Strom versorgt wird und über ein Netzkabel mit dem Netzwerk verbunden ist. Wenn möglich, ist es außerdem ratsam, die aktuelle Konfiguration des Geräts zu sichern.

Schalten Sie das Gerät nach der Vorbereitung ein und verbinden Sie es mit dem Netzwerk. Anschließend können Sie über einen Webbrowser unter der von Ihnen ermittelten IP-Adresse auf die Weboberfläche des Geräts zugreifen. Melden Sie sich dort mit den Administrator-Zugangsdaten an. Die Funktion zum Firmware-Update finden Sie im Menübereich System → Wartung. Wählen Sie mit dieser Option die zuvor heruntergeladene Firmware-Datei aus und starten Sie das Update. Während des Update-Vorgangs darf das Gerät nicht ausgeschaltet oder vom Netzwerk getrennt und der Browser nicht geschlossen werden, da dies zu einer Unterbrechung des Updates führen kann. Der Vorgang kann einige Minuten dauern.

Sobald das Update abgeschlossen ist, startet das Gerät in der Regel automatisch neu. Sobald es wieder zugänglich ist, rufen Sie erneut die Webschnittstelle auf, um die installierte Firmware-Version zu überprüfen. Anschließend sollten Sie überprüfen, ob alle Grundfunktionen wie Livebild, Netzwerkverbindung und gegebenenfalls Aufzeichnung ordnungsgemäß funktionieren. Wenn Sie zuvor eine Konfiguration gespeichert haben, können Sie diese nun wiederherstellen. Abschließend empfiehlt es sich, sicherheitsrelevante Einstellungen wie Passwörter, Datum, Uhrzeit und Zeitzone zu überprüfen und neue oder geänderte Firmware-Funktionen zu testen.

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

**Veröffentlichungsdatum:** 11. Juni 2025

Es wird empfohlen, nur von früheren Versionen zu aktualisieren. Eine Deinstallation der Vorgängerversion ist nicht erforderlich.

### **Unterstützte Produkte:**

Kategorie	Modell
Panorama	GU-CI-AP8616Q

### **Verbesserungen/Änderungen:**

1. Ein ONVIF-Bericht ist erforderlich, ONVIF-Testbericht/Funktionsliste/Guide\_Interface
2. Unterstützung der Suche über mehrere Monate hinweg; wenn die Startzeit die Endzeit überschreitet und zurückkehrt, schlägt die Suche fehl.
3. Die aktuelle Version der Audiokodierung verfügt nur über die Standard-PCMA-Kodierung. Die Version V21.45.8.2.4.2.1-241026 enthält sowohl PCMA- als auch PCMU-Kodierung für den Kunden.
4. API/Login/DeviceInfo/Get-Anfrage, Felder „RecFileType“: „MP4“ und „RecFileType“: „GU“ sind doppelt vorhanden.
5. Wenn IPC uses/API/PReview/StreamURL/Get verwendet, um RTSP-URL-Beispiele abzurufen, und der Port manuell auf 555 geändert wird, lautet der abgerufene Beispielport weiterhin 554.
6. Die ExaqVision CMS-Plattform kann nach dem Öffnen der Metadaten „Allgemein“ keine Motion-Aufzeichnungen empfangen.
7. Die Übersetzung muss aktualisiert werden.

Die Meldung, die angezeigt wird, wenn man sich wiederholt beim WEB anmeldet und rausgeworfen wird, lautet:

- Englische Lokalisierung: Ein neues Verbindungstoken wurde verwendet und die aktuelle Sitzung wurde abgebrochen.
- Deutsche Lokalisierung: Es wurde ein neues Verbindungstoken verwendet, und die aktuelle Sitzung wurde abgebrochen.

8. Wenn Sie den HTTP-Port manuell auf 82 ändern und das Gerät nicht neu starten, kann es den Stream nicht abrufen.

- C:\ffmpeg\bin\ffplay.exe-rtsp\_transporthttp-i " rtsp://admin:OutdoorCAM1@172.26.7.39:82/rtsp/streaming? channel=01&subtype=0"

- 9: SFTP unterstützt, Unterstützung für Verzeichnisnamen zum Erstellen von Unterverzeichnissen hinzufügen, Test-Schaltfläche hinzufügen

10: Das Zeitstempelformat für die Ereignisprüfung muss in „2025-02-07T15:19:47Z+00:00“ geändert werden

11: Unterstützung von RTCP

12: HTTP-API zum Zurücksetzen des Passworts, /API/RecoverPassword-Anfragetext zum Entfernen des Felds „email\_flag“

13. ONIVF-Sonde so modifizieren, dass die Geräteparameter im folgenden Format (519) abgerufen werden können

14. Abschirmung IR-/Weißlicht leuchtet auf und löst beim Bildwechsel einen Manipulationsalarm aus

15. Unterstützen Sie diese API (/API/Layback/LaybackRtspURL/Get), um RTSPURL-Beispiele abzufragen.

16. Video-Manipulation ausgelöst, fehlende Aufzeichnung in der WEB-Protokollabfrage

17: Cloud-Plugins sollten HTTP-Ports unterstützen

18: P2P verbindet sich nur mit europäischen Servern

19. Plugin-Version -1.22.24, siehe Anhang

20: Die Anpassung der Direct Cloud-Funktionalität erfordert die Unterstützung für das Aufheben der Bindung von Plugins und die Anzeige von Geräteinformationen auf der Direct Cloud-Informationssseite. Auf die Plugin-Geräteinformationen kann über <http://127.0.0.1:6790/status> zugegriffen werden – siehe Anhang als Referenz.

21. Unter „Gerätename“ und „Gerätetyp“ wird das Kundenmodell angezeigt, und das Motherboard-Modell muss mit mindestens 15 Ziffern eingebrannt sein.

22. Nach dem Ausfüllen der Adresse auf der Cloud-Seite zeigte die Plugin-Verbindung das Token nicht an und es fehlten dynamische Geräteinformationen.

23. Nach Eingabe der neuen Adresse hat sich die Adresse der Cloud nicht geändert.

24. ETR im NVR aktivieren, IPC löschen. IPC kann keine Stream-Parameter konfigurieren.

25. Ändern des RTP-Zeitstempels für die Videowiedergabe mit IPC-Sendefehlern.

26. Nach dem Ändern der ONVIF-Anforderung GetNodes und  $\alpha$ configurationOption geben auch Geräte ohne PanTilt eine Unterstützungsantwort zurück.

27. SFTP unterstützt, Unterstützung für Verzeichnisnamen zum Erstellen von Unterverzeichnissen hinzufügen und Test-Schaltfläche hinzufügen. Die aktuelle Version öffnet keine Eingabefelder für Unterverzeichnisse, und IE unterstützt keine Sonderzeichen-Ausfüll- und Test-Schaltflächen.

28: Die Standardeinstellung für die Auflösung des zweiten Streams ist 1024x288.

29: Die Standardbelichtungszeit ist auf 1/25 eingestellt.

30. Die neue Logik für das Pushen von Metadaten muss auf intelligente Alarminformationen umgestellt werden, die über RTP übertragen werden.

## **Haftungsbeschränkung / Haftungsausschluss**

Die Abetechs GmbH (Grundig-Security) unternimmt alle zumutbaren Anstrengungen, um die Integrität und Richtigkeit der Inhalte dieses Dokuments zu überprüfen, übernimmt jedoch keine formelle Garantie. Die Verwendung dieses Dokuments und die daraus resultierenden Ergebnisse liegen vollständig in der Verantwortung des Benutzers. Die Abetechs GmbH (Grundig Security) behält sich das Recht vor, den Inhalt dieses Dokuments ohne vorherige Ankündigung zu ändern. Design und Spezifikationen können ohne vorherige Ankündigung geändert werden.

Das hier beschriebene Produkt mit seiner Hardware, Software und Dokumentation wird „wie besehen“ ohne jegliche ausdrückliche oder stillschweigende Gewährleistung bereitgestellt, einschließlich, aber nicht beschränkt auf die Marktgängigkeit, zufriedenstellende Qualität, Eignung für einen bestimmten Zweck und Nichtverletzung von Rechten Dritter.

In keinem Fall haften unser Unternehmen und seine Mitarbeiter oder Vertreter Ihnen gegenüber für besondere, Folge-, zufällige oder indirekte Schäden, einschließlich unter anderem Schäden aufgrund von entgangenen Gewinnen, Betriebsunterbrechungen oder Verlust von Daten oder Dokumentationen im Zusammenhang mit der Verwendung dieses Produkts, selbst wenn unser Unternehmen auf die Möglichkeit solcher Schäden hingewiesen wurde.

Bei Produkten mit Internetzugang erfolgt die Nutzung des Produkts vollständig auf Ihr eigenes Risiko. Unser Unternehmen übernimmt keine Verantwortung für Fehlfunktionen, Datenschutzverletzungen oder andere Schäden, die durch Cyberangriffe, Hackerangriffe, Virenprüfungen oder andere Sicherheitsrisiken im Internet entstehen; unser Unternehmen leistet jedoch bei Bedarf zeitnahen technischen Support. Die Überwachungsgesetze variieren je nach Gerichtsbarkeit. Vergewissern Sie sich vor der Verwendung dieses Produkts, dass Ihre Nutzung den geltenden Gesetzen entspricht. Unser Unternehmen haftet nicht, wenn dieses Produkt für illegale Zwecke verwendet wird.

Im Falle von Widersprüchen zwischen dieser Anleitung und dem geltenden Recht hat Letzteres Vorrang.

### **Markenzeichen**

Alle hierin genannten Marken sind eingetragen. Der Name dieses Produkts und andere in diesem Handbuch erwähnte Marken sind eingetragene Marken der jeweiligen Unternehmen.

Das Urheberrecht an diesem Dokument ist vorbehalten. Dieses Dokument darf ohne ausdrückliche Genehmigung weder ganz noch teilweise reproduziert, verbreitet oder verändert werden.

### **Informationen zur Open-Source-Softwarelizenz**

Die mit Grundig-Produkten gelieferten Softwarekomponenten können urheberrechtlich geschützte Software enthalten, die unter verschiedenen Open-Source-Softwarelizenzen lizenziert ist.

Ausführliche Informationen zu den enthaltenen Open-Source-Softwarepaketen, den verwendeten Paketversionen, Lizenzinformationen und vollständigen Lizenzbedingungen finden Sie auf den Produktdetailseiten unserer Website. Die vollständigen Open-Source-Softwarelizenzinformationen sind auch in den Firmware-Dateien der betroffenen Produkte enthalten.

Sie können den vollständigen entsprechenden Open-Source-Teil eines bestimmten Produkts für einen Zeitraum von drei Jahren nach unserer letzten Lieferung dieses Produkts von uns erhalten, indem Sie eine E-Mail an [info@grundig-security.com](mailto:info@grundig-security.com) senden.

