



Radio Modem WiFi 6 HG G-76354-A (5G)

Changelog Firmware Versions 3.14i -> 3.14t

English, Revision 02

Date: 26.04.2024

Dev. by: TC

Author(s): RAD



© 2024 Götting KG, errors and modifications reserved.

The Götting KG in D-31275 Lehrte has a certified quality management system according to ISO 9001.



Contents

1	Firmware Changelog	4
1.1	Firmware 3.14i -> 3.14k (16.05.2023)	4
1.2	Firmware 3.14k -> 3.14m (14.06.2023)	4
1.3	Firmware 3.14m -> 3.14n (14.07.2023)	4
1.4	Firmware 3.14n -> 3.14o (25.08.2023)	5
1.5	Firmware 3.14o -> 3.14p (18.10.2023)	6
1.6	Firmware 3.14p -> 3.14r (10.01.2024)	6
1.7	Firmware 3.14r --> 3.14s (19.03.2024)	6
1.8	Firmware 3.14s --> 3.14t (10.04.2024)	7
2	Copyright and Terms of Liability	8
2.1	Copyright	8
2.2	Exclusion of Liability	8
2.3	Trade Marks and Company Names	8

1

Firmware Changelog

Below you find a list of the firmware versions released to date with the changes made in each case.

1.1 Firmware 3.14i → 3.14k (16.05.2023)

Functional changes:

1. The relay is now controllable via REST API and using statement sequences.
2. Authentication of individual API/URLs: This makes it possible to secure access to specific API functions with a separate user/password without having to use the user/password for device configuration.
3. 5G/LTE: Firmware update support for RM520N-GL

Bugfix:

1. Segfault error in the MQTT function fixed (TLS-Write).
2. Segfault error in the timer module fixed (Blacklist + ConfigChange)

1.2 Firmware 3.14k → 3.14m (14.06.2023)

Security updates:

- ♦ Change of Linux kernel version from 6.1.23 → 6.1.33

Functional changes:

1. wpa_supplicant updated to 2.11-dev (Git Rev. 95C3f0d1)
2. Improvement in relay control via REST API: Erroneous sequences and relay commands are now rejected with HTTP Error 400.
3. Output a warning in the debug log if all matching SSIDs are evaluated with 0 during the score calculation. This indicates that one of the crypto settings does not fit.
4. Warning in debug log after startup if certificates (client and CA certificates) are loaded that are about to expire or have already expired.

1.3 Firmware 3.14m → 3.14n (14.07.2023)

Security updates:

- ♦ Change Linux kernel version from 6.1.33 → 6.1.36

Functional changes:

1. Web server security:
 - Preferences for the TLS session handshake algorithms can now be set.
 - New option Send HSTS header

2. EAP: EAP-TTLS can now also be performed without certificates. (similar to EAP-PEAP)
3. Wireless: wpa_supplicant now with 802.11v support.
4. Wireless: now shows in the AP list whether an access point supports 802.11v.
5. Serial: The serial interface can now also communicate via TLS. Certificates for authentication can also be installed for this purpose
6. Bridge/NAT: now with warnings for conflicts of local services of the device with NAT rules defined by setup.
7. MQTT Bridge: Now also with local web socket port (default 8080)

Bugfix:

1. Serial: Approx. 1.5KB of memory were not released on each TCP reconnect.
2. WLAN dump: If a filter was set in LAN client cloning to record only its own traffic, then the correct MAC was not taken to define the filter.

1.4 Firmware 3.14n → 3.14o (25.08.2023)

Security updates:

Change Linux kernel version from 6.1.36 → 6.1.44

Functional changes:

1. SYN flood detection increased to 40 SYN burst. On average 5 SYN / second is still ok.
2. SNMP: Addition of status values from the info of /proc/net/dev
3. Improvement for IPv6 bridging
4. SCEP: If the CA Identity parameter for the URL contains illegal characters the value is URL-Encoded
5. Display of additional warnings in MConfig (from Vers.: 2_0_3_9) in the column "Status":
 - For certificates that are about to expire or have already expired.
 - For incorrectly configured ping test.
6. After a "reset to defaults" of the config via the web interface or also when uploading a configuration, the view automatically changes to the configuration web page after 2 seconds.

Bugfix:

1. the AuxIn is now processed correctly
2. The USB voltage is now switched on earlier, so that an inserted USB memory can be detected early. Thus the Config-Stick detection works now also reliably.
3. Correction when uploading a configuration via the web interface: The passwords are now processed correctly

1.5 Firmware 3.14o → 3.14p (18.10.2023)

Security updates:

1. Change Linux kernel version from 6.1.44 → 6.1.51
2. Buildroot: Move to OpenSSL 3 (OpenSSL 3.0.11 19 Sep 2023).

Functional changes:

1. input status: the status is displayed on the web page (Home) and can be queried via the API.
2. API/Status/Wireless.Connection Information for LANCloning adapted.
3. new element "Encryption" in "/API/Status/Wireless/Accesspoints/xx".

1.6 Firmware 3.14p → 3.14r (10.01.2024)

Security updates:

1. Update of the Linux kernel version from 6.1.51 → 6.1.70
2. OpenSSL update to version: 3.1.4

Functional changes:

1. SCEP: Challenge variant now also possible with V_ASN1_UTF8STRING.
2. SCEP: RFC 5652: Cryptographic Message Syntax (CMS) implemented
3. WLAN-Dump: new option for selecting what is to be recorded:
 - moni0 → (Wireless Header)
 - wlan0 → (Ethernet Header)
4. DNS forwarding: now with active handling instead of simple forwarding.
5. The Network Test website now also supports IPv6
6. Pseudo Level2 Bridge Mode: the client IP is now also "learned" from received ARP packets.
7. Reverse lookup of the host name via WLAN IP is now possible
8. MQTT Client + Serial can communicate via IPv6.
9. VPN: IPSec extended and WireGuard® added

1.7 Firmware 3.14r → 3.14s (19.03.2024)

Security updates:

1. Update of the Linux kernel version from 6.1.70 → 6.1.81
2. OpenSSL update to version: 3.2.1 (30 Jan 2024)

Functional changes:

1. implemented EST as an additional method for certificate distribution and updating
2. ping test: Adjustable parameter "Short Interval", which defines the shortened ping interval after an AP change.
3. update for the WPA supplicant

4. MQTT client: Server Name Indicator (SNI) added for TLS connections.

Bugfix:

1. deleting all dump and log files could cause the firmware to crash

1.8 Firmware 3.14s --> 3.14t (10.04.2024)

Functional changes:

1. Display of Captive Portal if the DHCP client was supplied with option 114 by the DHCP server.
2. LTE/5G: Service domain can be set (CS&PS, CS, PS)

Bugfix:

1. Roaming/Score: Bugfix for TPC rating for APs transmitting on 5GHz channels \geq 128. Under certain circumstances it could happen that APs with low SNR value were rated higher than APs with a higher SNR.
2. Login form with background blocking (CDC) - After more than 5 seconds, it was no longer possible to log in with read-only users.

2

Copyright and Terms of Liability

2.1 Copyright

This manual is protected by copyright. All rights reserved. Violations are subject to penal legislation of the Copyright.

2.2 Exclusion of Liability

Any information given is to be understood as system description only, but is not to be taken as guaranteed features. Any values are reference values. The product characteristics are only valid if the systems are used according to the description.

This instruction manual has been drawn up to the best of our knowledge. Installation, setup and operation of the device will be on the customer's own risk. Liability for consequential defects is excluded. We reserve the right for changes encouraging technical improvements. We also reserve the right to change the contents of this manual without having to give notice to any third party.

2.3 Trade Marks and Company Names

Unless stated otherwise, the herein mentioned logos and product names are legally protected trade marks of Götting KG. All third party product or company names may be trade marks or registered trade marks of the corresponding companies.

Innovation through Guidance

Götting KG

Celler Str. 5 | D-31275 Lehrte

Tel. +49 (0) 5136 / 8096 -0

Fax +49(0) 5136 / 8096 -80

info@goetting-agv.com | www.goetting-agv.com



www.goetting-agv.com