Firmware Change Log (new features and bug fixes) for Industrial Security Router Series IE-SR-2/6GT

List of affected Router models:

Article name	Article number
IE-SR-2GT-LAN	1345270000
IE-SR-2GT-LAN-FN	1489940000
IE-SR-2GT-LTE/4G-US	2535780000
IE-SR-2GT-LTE/4G-EU	2535930000
IE-SR-6GT-LAN	2535940000
IE-SR-6GT-LTE/4G-US	2535950000
IE-SR-6GT-LTE/4G-EU	2535960000
IE-SR-2GT-LAN-M	2535980000
IE-SR-2GT-LTE/4G-EU-M	2535970000

Important note when using the Weidmüller u-link Remote Access Service:

The u-link Remote Access Service can be used with each Weidmüller router model except the variant IE-SR-2GT-LAN-FN which does not support any VPN functions.

General Upgrade/Downgrade information:

Upgrade to version 5.0.10 or higher is only possible from version 4.5.9. For Routers with versions < 4.5.9 first update to version 4.5.9 followed by a final update to latest version.

Downgrades from version 5.0.10 or higher to version 4.0.0 or below is not possible anymore. For downgrades from version 5.0.10 or higher to version 4.x it is necessary to bring the router into compatibility mode. Refer to the manual to find out how to activate compatibility mode.

Upgrade to version 4.x is only possible from version 3.5.0 or higher. For Routers with versions < 3.5.0 first update to version 3.5.x followed by a final update to latest version.

Version 5.0.10, Build number 174445. Release date: Jan 16, 2025

Bug Fixes:

- Fixed WWAN issue on system startup where the WWAN modem was enabled for permanent connection without a SIM card inserted. This caused a memory leak, resulting in a non-functional WWAN connection even after inserting a SIM card and led to high CPU usage.
- Configurations in which the device functions as an OpenVPN server were affected by a regression error. The IP port forwarding no longer worked correctly since the version 4.5.9.
- Products with an integrated Fibocom NL668 WWAN modem experienced issues selecting the correct profile when the SIM card was shipped with a custom profile (including settings like APN, etc.). Affected systems would never go online.
- Fixed a bug affecting the behavior of external digital inputs and the packet filter. Rules that depended on the state of the digital input were not activated during startup because the input state was not evaluated initially. The rules only activated or deactivated after a change in the input state, based on the configuration. This issue was introduced in version 4.2.2.
- In individual setups with the Router, Ethernet problems were observed, which manifested themselves in infrequent 1-10 second interruptions of Ethernet switch data traffic on ports LAN1-LAN3. In the event of a fault, the Ethernet link was not affected and still displayed a good link. The problem could be solved by selected parameter changes of the internal switch chip.
- Errors in connection with the cellular modem have been fixed. If the cellular modem is activated but no SIM card is inserted, there were connection problems with u-link, although u-link is operated via Ethernet in this case. Furthermore, the automatic reset of the cell modem to automatically find a newly inserted SIM card is now stopped after three attempts and then only retried every 24 hours.
- Removed adsdpd debug log messages from Eventlog.
- The IPsec aggressive mode has not worked properly. This behavior has now been fixed.
- The WWAN LED could remain active after a reboot or if the modem was configured to go online and the firewall device was later reset to factory defaults. In such cases, the WWAN LED status did not correctly reflect the firewall's WWAN online/offline state. This bug was fixed.

Feature updates:

- The firmware update page on the device's web interface has been enhanced. Now, there are two methods to check for updates. The device will first attempt to contact the update server directly. If this fails, it will then use the user's browser as a fallback to relay the contact, verify, and update the device firmware. Previously, the device itself required an internet connection for this process.
- USB sticks formatted with the EXT4 filesystem can now be used for firmware updates and settings file uploads. Additionally, a race condition has been resolved, which previously could cause the USB stick not to be processed during bootup if it was too slow.
- New self-signed HTTPS certificates: The device will generate a self-signed device Certificate Authority (CA) from which all HTTPS web server certificates will be derived. This device CA will be created once and will remain valid even after a factory reset. The derived web server certificates will be updated whenever there are changes to the static IP or hostname, and these certificates will include this updated information.
- We are introducing a new implementation for authentication. This update employs sessions and Argon2 hashing, replacing the previous use of MD5 hashes and HTTP digest authentication. However, the previous method can still be enabled for compatibility purposes. As a result of these changes, users will see a completely new login page and a revised logout mechanism, including a session timeout set to 300 seconds of inactivity.
- Improved syslog reporting of successful and failed logins on the device web interface or APIs.
- The OpenVPN server with RADIUS authentication, which had been previously removed, has now been reintegrated.
- The range of supported IPSec PSK values has been expanded. You can now configure PSKs as Base64-encoded binary values, Hex values, or regular strings with all special characters supported by the StrongSwan backend.

New webpages:

- The packet filter has now a new status page with traffic graphs for each filter rule.
- The web interface of the product now additionally lists the OSS components and licenses currently included in the product.
- Firmware updates or settings files can be imported via the USB port of the devices. This function can now also be deactivated on a new subpage in the web interface. If the storage of Syslog messages on the USB stick is disabled as well, then the USB stick will remain completely unmounted for improved security.

Features disabled:

- The Web Interface of the device is now reachable by HTTPS only for security reasons. The firewall web interface will automatically redirect HTTP requests to HTTPS, ensuring secure web access. However, if your previous configuration used HTTP (port 80), this will now be redirected to HTTPS (port 443). All HTTP requests from the allowed interfaces will be automatically redirected to HTTPS if HTTP is allowed on the Web access page. If HTTP is disabled on the Web access page the redirect is disabled.
- The classic HTTP API is deactivated with the default settings mode for security reasons. The classic HTTP API is still available in compatibility mode. Refer to the manual to find out how to activate compatibility mode. For security reasons, it is recommended to switch to the HTTPS API.

Version 4.5.9, Build number 163580. — Release date: Feb 06, 2024

Bug Fixes:

- The following features had a concurrence issue starting with version 4.5.5: U-link route push on devices with LTE modems, remote capture service, WWAN channel scan and VPN UP blink service. Therefore, only one of the features could work well at a time. The issue is fixed with this version.
- Fixed a possible memory leak that could lead to a shortage of free RAM after an uptime of more than 200 days.
- A bug has been fixed that, under certain circumstances, could cause TCP streams directed to other IP addresses neighboring on a switch to be forwarded through the device. Therefore, setups with IP settings via DHCP and simultaneous TCP port forwards on these network interfaces are recommended to update to this version.

Version 4.5.7, Build number 160692. — Release date: Dec 07, 2023

Bug Fixes:

- The remote syslog was not working correctly after a system reboot.
- The PPPoE settings on the web interface had been invisible due to a regression bug.
- introduced with following versions IE-SR-2GT/6GT*: 4.5.4
- It was not possible to put a date later than 2023 in the settings.
- Fixed Software Update webpage
- Fix broken u-link CA certificates due to invalid settings. The error message indicating such a problem was "scep: Fatal error: server certificate not valid. Please check date & time settings! (Config-Datei)".

Feature updates:

- Fixed the VPN LED / VPN UP configuration drop down. The IPsec option was lost in the drop down due to a regression bug. This has been fixed.

Version 4.5.4, Build number 157901. Release date: Sep 25, 2023

Bug Fixes:

- U-link remote network routes will now be automatically configured for network interfaces using DHCP or Fallback IP assignment when the device is in 'Transparent Bridge' mode. Previously all network interfaces in these modes were skipped. Please note that u-link does not support changing network routes while the VPN connection is established!
- A regression bug in the web UI, specifically concerning the enabling of SNAT on interfaces with DHCP IP assignment, has been fixed.
- Fixed the logging of authentication failures on the web interface.
- Increased the maximum length of Eventlog entries as some lines were cut after 256 characters.
- A regression bug was identified in the web UI. The packet filter interface selection dropdown was not accommodating all possible combinations of input and output interfaces.
- The automatic transmission of new or modified static routes to u-link was not functioning as intended. It necessitated a manual u-link VPN restart on the device. With the current update, the u-link VPN on the device will now automatically restart when a change or addition is made to a static route along with u-link synchronization. As a result, the new route will promptly become visible to the u-link server. It's important to note that any u-link VPN connected users must still perform a restart on their VPN endpoints to access the newly added routes.
- OpenVPN client: Static routes with a gateway on the OpenVPN interface were not restored during the VPN reconnect, but only during the initial connection until it is lost. This has been fixed.

Feature updates:

- The Wireshark Remote Capture service "rpcapd" has been updated.
- The configuration variables for controlling u-link VPN are added to the Permission list

Version 4.5.3, Build number 156160. Release date: Aug 04, 2023

Bug Fixes:

- If the IP assignment of the WAN interface was changed from DHCP to static and the "Gateway via DHCP" option was activated at the same time, then the gateway field in the IP configuration was deactivated and it was not possible to make a gateway entry. This is fixed now.
- Improved the initial connection time and the time needed for reconnection after a link loss for the u-link WWH connections.
- The DNS proxy and the DHCP server must be configured separately since version 4.5.0. This separation was incomplete. The DNS proxy was running automatically in the background if the DHCP server was enabled on a certain interface. This has been fixed. Existing configurations will get updated on firmware update as follows: The DNS proxy will be enabled on all DHCP server interfaces if it was off before.
- Fixed a race condition which occurred since version 4.2.0. The firmware update and configuration file loading via USB stick might not processed on boot up in some situations.

Feature updates:

- Allow the configuration of an NTP relay which will always step its clock directly to the NTP servers time. For example, if the time on the uplink NTP server changes spontaneously with a large value even during runtime. The option is named "Allow spontaneous NTP time step" and can be found at “Date & time”. It is disabled by default.
- The devices can now use the u-link WWH connection to synchronize their date and time to the u-link server. To enable the feature, activate "World-wide heartbeat time synchronization" on the Date & Time configuration page. The time will be synced if it differs more than 60 seconds from the server. The synchronization is done inline in the WWH protocol and therefore the interval is dynamic at ~60-200 seconds.

Version 4.5.2, Build number 154725. Release date: Jun 13, 2023

Bug Fixes:

- Network groups: The string length of the newly introduced DNS based entries has been increased.
- Fixed SNMP service when configuration uses 0.0.0.0 (any IP) as allowed source IP for client.
- New packet filter rules were not applied or saved. This regression bug was introduced with version 4.5.1.

Version 4.5.1, Build number 154281. Release date: May 30, 2023

Bug Fixes:

- In the IP router (extended) mode, the error was fixed that the default gateway could only be entered after pressing Apply once.
- On the System State page, the u-link references in the Interface State table have been corrected.
- Incorrect entries in tables are now intercepted via an error message. No error message appeared in the previous versions 4.4.0 and 4.4.1.
- Fixed problems with the NTP relay and Siemens PLCs, the ntpd server process reported "Rate Limit reached" in the Eventlog and stopped working. This has been fixed.
- Improved NTP client behavior on power up. In some cases, it took days to synchronize the clock if there was a dynamic IP setting on the uplink like DHCP or WWAN. This issue has been resolved.
- In the Packet filter layer 3 section, the rules were incorrectly numbered, which has been fixed in this version.
- In versions 4.4.0 and 4.4.1 it could happen that WWAN PIN, MNC, and MCC and smartcard PIN settings with leading zeroes became invalid. This has been fixed in the current version, but there is a possibility that these codes must be entered again.

Feature updates:

- The HTTP/S and the DNS proxy access filter network interfaces have changed from physical mapping to interfaces with IP address only. Old configurations will continue to work as before, but on reconfiguration all pure Ethernet interface on bridges will get removed.
- Added the possibility to enable debug logs for the DHCP server.
- There is a new diagnostics download. It contains more internal details for Weidmüller support, is stored in plain text and does not contain any credentials or other confidential data from the configuration.
- Introduce DNS based packet filter. The already existent network groups can now be used with DNS host and domain names. In combination with integrated DNS proxy every DNS lookup will get synchronized with the packet filter IP addresses.

Version 4.4.1, Build number 151672. Release date: Apr 27, 2023

Bug Fixes:

- The Permissions web page did not allow to remove checked elements due to a regression bug introduced with version 4.4.0.
- Fixed a regression bug regarding transparent bridge mode on the device web interface introduced with version 4.4.0. It was not possible to change the IP address due to a Java Script exception.
- The Permissions for the filter wizard were not controllable due to a regression bug introduced with version 4.4.0.
- Fixed a regression bug which prevented devices with u-link VPN or SCM memory cards to load and apply a cf2 settings file generated with the firmware version 4.4.0.
- The HTTP API (get.php) did respond with wrong multiline formating on "statuslong" calls due to a regression bug introduced with version 4.4.0.

Version 4.4.0, Build number 150458. Release date: Apr 12, 2023

Bug Fixes:

- Fix DHCP server web interface page. It was not possible to disable the DHCP server using the web page once it had been enabled.
- More user-friendly configuration of the setup wizard regarding date and time selection (Web menu)
- The current date and time were displayed differently on the home page than on the date and time page.
- Fixes a race condition that was observed in the lab in connection with WWAN/LTE/4G on version 4.3.4. Under certain circumstances, a permanent reset loop of the WWAN modem occurs during the initial configuration of the WWAN parameters or during reconfiguration to a different SIM card. In this case, no WWAN connectivity is established. The event log of the device then shows the resets of the WWAN modem accordingly.

Feature updates:

- Cumulative update of integrated open source software components.
- The WAN port can now be configured to use PPPoE either with or without an additional VLAN tag.
- Log IP changes on WWAN interfaces in the Eventlog

Version 4.3.4, Build number 147503. Release date: Jan 17, 2023

Bug Fixes:

- OpenSSL update to version 1.1.1o. Fixes several CVEs;. Please see https://www.openssl.org/news/openssl-1.1.1-notes.html for details.
- Packet filters with a negated IP network group did not work correctly. This has been fixed. This bug was introduced with version 4.0.1

- The control of switched IPsec connections by using the JSON/RPC or Modbus/TCP API could run into a dead lock if the connection could not be established. This bug was introduced with version 4.0.1
- The internal WWAN connection monitor process was not stopped when the feature was disabled. A save and reboot cycle was required to really stop the feature.
- The WWAN MMC and MNC settings were only applied when they got configured for the first time but not any more after a reboot.
- Updated integrated zlib library regarding CVE-2018-25032
- Fix WAN-2 usage in dynamic routing
- The available configuration settings on the permissions web page have been cleaned up and those missing up to now have been added.
- The global permissions list on the web interface has been reviewed and cleaned up.
- The internal OpenVPN processes have not been stopped in case of reconfiguration from layer 2 to layer 3 mode. This has led to strange behaviours as the old process continued to run and the did not like to start. A save and reboot was required to fix the situation up to now.
- The OpenVPN status page did show OpenVPN connections as alive even if they had been shut down.
- OpenVPN server connections in TUN mode did not add the IP routes to the subnets behind the connected clients to their routing table.
- Web interface: fixed size of packet filter wizard popup
- Fixed several uplink state checks in the setup wizard
- Re-added the item folder "Information" to the web interface which got lost due to a regression error since versions 4.0.1
- IPsec connections with DNS host names as the remote endpoint did not retry DNS lookups. If the first attempt failed, the IPsec connection was not started. This has been changed to infinite repetitions with an interval of 5 seconds. Otherwise, the connection was not established if the DNS server could not be reached directly when booting, as is usual with WWAN connections
- A broken USB stick could lead to a dead lock of the system when inserted or when present on boot up
- Fixed display of WAN port Ethernet link state within the Config Wizard which was broken since 4.1.0 due to a regression bug.
- Changing the configuration of IPsec parameters can take up to 60 seconds due to internal timeouts in the IPsec stack while the old connection is open, and the remote terminal is already gone. This timeout has been shortened to 5 seconds, which leads to a much faster reaction of the web interface to configuration changes.
- Fix IPsec option "send certificates". This option was ignored internally since version 4.0.1 due to a regression bug.
- The internal time zone database has been updated
- The various u-link checks in the startup wizard, configuration page and status page have been synchronized.
- The Web interface Event log is now a "read only" HTML element.
- U-link Interface was missing in forwarding menu
- The On Demand mode was described in the WWAN connection mode tool tip. However, this mode cannot be selected. The EN tool tip was ok.
- The configured time zone was ignored. This bug was introduced with version 4.0.1
- Modbus/TCP API: The behavior has been changed on write access. Several registers like VPN switching require some internal processing time. Previously these actions have been forked into the background. This has led to problems in case of fast changes due to additional writes. Now the device will process these things directly and the Modbus/TCP reply will be delayed until the process is finished.
- Security Update of the integrated libcurl to version 7.83.1
- u-link internal configuration variable vpn_list_10 will now contain "switched" instead of "deactivated" as default in its last field. All running configurations will be updated on firmware update.
- Standard OpenVPN connections with a certificate chain of intermediate CA certificates did not work. OpenVPN was not able to follow the chain to the root CA and the connection could not be established.
- Layer2 packet filter rules on switched Ethernet traffic using the CUT or ALARM signals as condition stopped working on IE-SR-2/6GT* with version 4.0.1.
- The u-link VPN servers are now dynamically requested via world wide heartbeat (WWH) on each new connection allowing a better control for the new world wide u-link VPN servers.
- Update of integrated software package dnsmasq to version 2.86. (see CVE-2021-3448)
- The virtual IPsec network interface adapter was not displayed correctly in the various drop-down menus in the web interface. Especially if an uplink device ≠ WAN was used. Now the value is rewritten to match the current uplink device.
- PPPoE text in Tooltip has been removed
- IPsec Update to strongSwan 5.9.6
- Added German text on SMS service tool tips
- The network mapping (1:1 NAT) feature on IE-SR-6GT* contained an error when disabling the function. If enhanced IP router mode is used and network mapping is disabled on ports LAN-3/LAN-4, those ports will be shut down until reboot. This has been fixed
- WWAN: configuration of an empty APN is no longer allowed as it makes no functional sense.

- Improved WWAN connection recovery. In case of signal loss, the connection will get re-established faster or the following integrated WWAN modems: EM7455, EM73x4, MC7455, MC73x4 and SIM8202G
- Fixes the initial WWAN configuration of IE-SR* devices with the following integrated WWAN modems: EM7455, EM73x4, MC7455, MC73x4 and SIM8202G in combination with M2M SIM cards. In details this version fixes several issues where M2M SIM cards failed to register on 4G networks for the first time. Devices with WWAN connections that have already been set up are not affected!

Feature updates:

- IPsec: It is now possible to use wildcards to match remote identities (e.g. *@weidmueller.com, *.weidmueller.com, or C=DE, O=weidmueller, CN=*).
- Improved WWAN SIM card exchange on IE-SR* devices with the following built-in WWAN modems: EM7455, EM73x4, MC7455, MC73x4 and SIM8202G. It was necessary to save the new settings and restart the device to get a new WWAN connection with a new SIM card and a different APN. This is now no longer necessary; the setting change works on the fly and recognizes the new SIM card.

Features disabled:

- The support of PPPoE for pass through DSL modems has been removed.
- Configurations of the device acting as OpenVPN server with authentication against Radius servers is no longer supported.
- The DHCP relay feature has been removed.

Version 4.1.9, Build number 138039: Release date: May 16, 2022

Bug Fixes:

- The JSON/RPC method alarm.get() did not work as expected. This has been fixed.
- Complete rewrite of the Modbus/TCP service for controlling and monitoring the VPNs of the device.

Feature updates:

- The system can now be configured with a scheduler so that certain actions are carried out at certain times. Only the Reboot action is currently available.

Version 4.1.7, Build number 132590: Release date: February 17, 2022

Bug Fixes:

- Fixed a regression bug of version 4.1.6. If IPsec connection is configured to start by the VPN switch it starts on power up or reboot even if the switch was off.

Version 4.1.6, Build number 132129: Release date: November 18, 2021

Bug Fixes:

- For setups with WWAN fallback and IPsec, there was an error reactivating the WAN connection in the recovery case. The IPsec connection was not re-established via the WAN link. This bug has been fixed.
- If the VPN LED was configured for IPsec, it indicated a link while the connection was being established by shining permanently. This behavior has been fixed, while the VPN connection is being established, the LED is now blinking, as it does for u-link VPN or OpenVPN.
- Switching an IPsec VPN connection on and off via the digital input (VPN KEY) was not possible since version 4.0.0 due to a regression error. This bug has been fixed.

Version 4.1.2, Build number 125088: Release date: August 25, 2021

Bug Fixes:

- New OpenVPN Static Key Dropdown was always empty. This has been corrected.

Version 4.1.0, Build number 123477: Release date: July 23, 2021

Feature updates:

- JSON/RPC API was extended to upload certificates and keys and setting files (.cf2). A new object on the API named "file" will therefore appear.
- The forwarding has been enhanced with Reverse SNAT per line. This can now be activated for a forwarding entry with an IP alias and any protocol (*). For IP connections that are started from the internal network, the source IP is replaced by the specified IP alias.
- Added "slow link" checkbox to the u-link configuration page. Enable this feature if you have links with round trip times above 1000ms, i.e. satellite connections or a slow mobile network.
- Added Config Wizard.

- OpenVPN client or server connections can now be configured to use the OpenVPN TLS protection options tls-auth or tls-crypt.

Bug Fixes:

- Configuration changes which arrived trough JSON/RPC API did not appear in the Eventlog.
- Fixed 4G fallback mode when using a monitored service with a TCP port. This bug was introduced in 4.0.6. Improved fallback to work even if SNAT is not active on the monitoring interface. Monitoring with ICMP was not affected.
- It was not possible to disable the DNS proxy on the LAN1-4 interfaces in IP-router extended mode.
- Optimized API status calls for OpenVPN and u-link state to get a faster feedback. about the current state.
- Write permissions for u-link configuration and SMS service configuration can now be changed using the web interface permissions page.
- The VPN key setting for u-link did not work directly if it was activated before entering the activation code. This behavior has been corrected. The system now goes online immediately after setting the activation code and the VPN key is still on.

Downgrade Information:

- Downgrades from 4.1.x or later to 4.0.x or earlier will lose settings regarding Forwarding and OpenVPN.

Version 4.0.6, Build number 116462 Release date: March 02, 2021

Bug Fixes:

- Fixed an internal race condition of the IP forwarding feature in cases of configuration changes with parallel traffic. In seldom cases this has led to some running TCP streams not forwarded as expected.
- Fix of impact to IP forwarding with IP aliases by OpenVPN or u-link connection events due to an internal race condition with the connection tracking with parallel traffic in rare cases.
- Fix IP forwarding which was broken to a regression bug with version 4.0.2. Since this version the port field had to be not empty. This is now allowed again.
- Fix of issue referenced by CVE-2020-25684: If the DNS Proxy feature is enabled the device is vulnerable to a DNS Cache poisoning attack as described by the CVE.
- Fix of issue referenced by CVE-2021-3156: Update of integrated FOSS component 'sudo' to version 1.9.5p2. Prior to that version there was a privileged escalation bug. Update is recommended to strengthen the internal security chain.

Version 4.0.4, Build number 114187 Release date: January 04, 2021

Feature updates:

- The Syslog can now be stored on an inserted USB stick which has to be preformatted with a Linux ext4 filesystem. This feature can be enabled on the Event Log → Configuration page. The syslog files are used as ring buffer. The file size depends on the size of the stick.
- IPsec IKEv2 can now be activated. By default, active connections are now initiated using IKEv2 but IKEv1 connections are passively accepted.
- The Forwarding feature has been extended to forward UDP or TCP port ranges.
- Subnet mask value /0 is now allowed for u-link's destination SNAT configuration parameter.

Bug Fixes:

- USB Sticks with FAT file system got formatted with the Linux ext4 file system when inserted. Bug was introduced with version 4.0.1.
- USB sticks with configuration or firmware files have been processed correctly but the device was caught in a reboot loop until the stick was removed. This regression bug was introduced in version 4.0.1 and has been fixed now.
- Fixed a regression bug introduced with 4.0.1. NATing and filtering of active FTP was broken.
- 3G models did not get a DNS-Server from the mobile radio provider. This bug was introduced with version 4.0.1.

Version 4.0.1, Build number 110276 Release date: October 1, 2020

Feature updates:

- Added possibility to use hostname for 4G fallback check and added capability to check for open TCP port.
- Enabled new type of 4G modem.

- Added keepalive and hash-algorithm for OpenVPN.
- Removed clear button for Event Log.

Bug Fixes:

- Fixed bug in DNS-proxy which didn't filter requests on interface correctly.
- Username and password for proxy can now be cleared.
- Fixed bug with SNMP filter of community IPs.
- Removed passwords from downloadable config file.
- Fixed bug with layer 2 filter rules which use Network groups as source.
- Fixed setting of manual mobile provider after reboot.

Version 3.5.1, Build number 104506 Release date: June 02, 2020

Feature updates:

- Bug fix only release

Bug Fixes:

- Fixed bug with transmission interruptions when using full gigabit speed.

Version 3.5.0, Build number 102278 Release date: March 25, 2020

Feature updates:

- Added IPsec Fallback mode for 4G mobile Variants.
- Added option to let the VPN Active output blink during establishing of a VPN connection.
- Added mobile Band selection for cellular interface (2G/3G/4G) for cellular models to select all dedicated operating frequency bands instead of the previous 2G/3G/4G mode dropdown.
- Preparation of new functionality and update to major release 4.0.0

Bug Fixes:

- Fixed bug with the new server addresses for u-link WWH server. The new addresses can be checked in the Technical User Guide for u-link.
- Fixed permission settings for some pages. Added permissions for future functionality, which is not released yet.
- Removed the non-functional network scan button for 3G mobile variants which was intended for 4G devices only.
- Fixed bug in packet filter using hardware groups.
- The software can now handle SIM cards with ICCID length of 18.
- Syntax check of contact email now allows subdomains.
- Allow email addresses with subdomains for 'contact_email'
- Fixed displayed subnet mask of packet filter rules.
- Fixed CIDR notation of subnet mask in packet filter wizard
- Fixed WAN Port disabling on CUT signal under certain circumstances if feature is enabled.
- Fixed setting of preferred network mode after reboot on 3G devices. On previous firmware versions this setting did not outlast a reboot.
- Fixed loss of static routes after network interface setting modifications under certain circumstances while the system is running. Static routes were always correctly applied after reboots.
- Fixed static routes handling after cellular connection.
- Fixed configuration of hostname. Changes were applied after reboot and are now applied immediately.
- Fixed handling of default gateway in cellular fallback mode if the WWAN connection fails. On previous firmware versions the default route got lost if the WWAN connection could not be established when switch from wired to WWAN uplink.

Version 3.2.3, Build number 87950 Release date: December 03, 2018

Feature updates:

- Added IPsec Fallback mode for 3G mobile Variants
- Added new server addresses for u-link WWH server

Bug Fixes:

- When updating the firmware with version 3.2.3 build 86546 a configured and activated u-link instance automatically was disabled. As result the u-link instance had to be re-activated manually after update by setting again checkbox “Enable u-link instance” in menu “VPN → u-link” of the web interface.
- Improved check method to recognize and identify an inserted SIM based on the received SIM ICCID.

- Fallback function from WAN to 4G did not work correctly if WAN port was configured with static IP address.
- Fixed scanning of available mobile networks

Version 3.2.2, Build number 86546 Release date: September 14, 2018

Feature updates:

- Added mechanism to upload 4G mobile modem firmware useable for a specific provider (e.g. for US models different modem firmware versions have been to be used dependent on the provider like Verizon or AT&T).
- Extended 4G status view about installed mobile modem firmware.
- Implementation of additional parameters for mobile settings: roaming, allowed & preferred networks, network modes, forcing a connection to a specific carrier via Mobile Country Code (MCC) & Mobile Network Code(MNC).
- Implementation of function “Network Scan” for evaluation of available mobile networks.
- Implementation of additional status symbol for mobile network signal quality.

Bug Fixes:

- Improved stability of 4G modem configuration.
- Fixed bug with timeout in SNMP mobile disconnect.
- Update “openssl” to version 1.0.2p (fix of security vulnerability CVE-2018-0732 & CVE-2018-0737).

Version 3.2.2, Build number 83558 Release date: July 16, 2018

Bug Fixes:

- Improved interoperability of mobile network connections (Problem when setting APN).
- Handle SIM cards with variable ICCID length.

Version 3.2.2, Build number 82950 Release date: June 28, 2018

Feature updates:

- Improved stability of mobile connections with low signal strength.
- Improved performance of menu Diagnostics → 4G. New mobile connection parameters added.
- New SMS Service features for control and information (SMS traps) implemented (Note: Only available for variants with an integrated 4G modem).
- Additional SNMP parameters for requesting LTE/4G status data implemented.

Bug Fixes:

- Update openssl to version 1.0.2o to fix security vulnerability CVE-2018-0739.
- Internal debug messages removed from Eventlog.
- Update of expired Demo Certificates included in the firmware.
- Restriction of Ethernet ARP announcements and ARP response packets on network interfaces with the matching IP address and subnet.

Version 3.2.1, Build number 79368 Release date: January 18, 2018

Bug Fix:

- In Menu “Packet Filter” of Web interface neither existing firewall rule sets could be edited nor new ones could be added due to a Java script error. Trying to add a new firewall rule set was resulting in displaying an empty window (no contents were displayed). This problem was introduced in previous version V3.2.0, Build 78720.

Version 3.0.0, Build number 78720 Release date: December 19, 2017

Feature updates:

- Improved SSL parameters for internal web server (SHA1 and 3DES disallowed, SHA256 or AES 128/256 required).
- Allow configuration of interfaces on which DNS relay service is running (by default DNS relay service is enabled on each network interface.
- Improved SSL parameters for internal web server (SHA1 and 3DES disallowed, SHA256 or AES 128/256 required).

Bug Fixes:

- Improvement of system stability by optimizing memory controller parameters.

- Fix of denial of service vulnerability and Pre-authentication remote crash/information disclosure for clients when using “http_proxy_passthrough” in OpenVPN (CVE-2017-7520).
- Fix of dnsmasq function (CVE-2017-13704).
- Fix of OpenSSL vulnerability by update to version 1.0.2l (CVE-2017-3736 and CVE-2017-3735).
- Fix of unreliable detection when inserting a cellular SIM card.
- Fix of memory leak which could lead to problems regarding a cellular-based (mobile) u-link VPN connection.

Version 3.1.2, Build number 77018 Release date: July 14, 2017

Feature update:

- Adaption of behaviour when restoring a backup configuration via USB stick (using backup file of type <name>.cf2).
  New procedure:
  1. Copy cf2-backup file to USB stick (FAT or FAT32) into directory named settings.
  2. Plug USB stick into the Router and power-up / reboot the device (Router automatically will load the cf2-file).
  3. Wait around 1 minute until the Router is ready again (PWR LED is lit constantly), having loaded the parameters of the configuration file.
  4. Un-plug USB stick from Router.

  How to check the result of the import procedure via USB stick:
  1. Plug USB stick into a PC and check directory settings which now should have a new sub directory with name same as the device serial number (e.g. AX1367406). This directory contains a log file named settings.log created by the Router at configuration upload.
  2. Open text file settings.log and check the status of the restoring process (e.g. containing message “Device configuration successfully updated”).

Note:
If you will use the same USB stick - containing a general template configuration file - for an initial setup of several Routers, then each Router will create during the restoring process its own sub directory AX.... (based on the unique serial number) below directory settings containing in the sub directory the Router specific text file settings.log.

Bug Fixes:

- u-link: DNS related problems fixed in terms of WWH-function when DNS settings have been changed.
- Counters for dropped/overrun packets of Ethernet Interfaces (LAN / WAN) now will be reset at system boot.
- Now short DNS names (<4 characters) to be used with DNS provider dyndns.org are allowed.
- Bug fix in terms of static configured link parameters of Ethernet ports (no Auto-Negotiation). No change of configured parameters after system boot (Elimination of fallback to 10Mbit/half after reboot when no link is available).
- Bug fix in terms of assignment of the default gateway via 3G. A setting could be get lost when opening IP configuration page and applying the settings.
- Several security updates.

Version 3.1.0, Build number 74521 Release date: December 05, 2016

New features:

- A saved configuration file (with extension .cf2) created from any Router model (IE-SR-2GT-LAN, IE-SR-2GT-LAN-FN or IE-SR-2GT-UMTS/3G) now can be load into any other Router model. All relevant parameters of the target Router will be imported. Not relevant parameters (eg. 3G configuration parameters when importing a backup file from a 3G-Router to a LAN/WAN-Router) will be ignored.
- Update of OpenSSL library to version 1.0.2j
- Improved calculation of CPU Load

Bug Fixes:

- Fix of behavior of the user interface when configuring the “Client monitoring” function sending an alarm via mail. This feature got disabled if the mail server address has been changed.
- When uploading a configuration file a new self signed certificate for the HTTPS server is generated. The host name used on this new self signed certificate was taken from the running configuration (false) and not from the uploaded configuration (correct). This problem was only relevant for configurations where the host name explicitly was configured. By default the host name is automatically generated from the device serial number. For such a default setting the problem did not arise.
- Regarding a configured fall back Internet connection (from WAN to 3G) always the WAN-Port related DNS server was used and not the DNS configuration of the active Internet connection (either WAN or

3G). In case of an activated fallback connection to 3G the DNS was not switched to the server obtained from the mobile network.
- Automatic synchronization of an inserted USB stick when the Router is rebooting. This avoids a possible file system corruption of the stick when loading a configuration file (cf2) from the stick.
- Improved restoring of configuration via USB stick (using backup file with extension <name>.cf2). After successful loading of the cf2-backup file from USB stick the file extension always has been renamed to *<name>.cf2.rej* even on successful loading. Now the cf2-backup file (on USB stick) will be renamed correctly to *<name>.cf2.ok*.
- The “Logoff” button in the web interface did not logout the user in some cases but simply returned to page “System state”.

Version 3.0.2, Build number 72728 Release date: May 09, 2016

New features:
- Added support for u-link Internet connection via Proxy server
- Improved diagnostic management (status messages) for u-link registration process

Bug Fixes:
- Fixed display error of OpenVPN state on page “System state”
- Improved SSL parameters of internal webserver

Version 3.0.1, Build number 72391 Release date: March 02, 2016

New features:
- Update openssl to version 1.0.2g

Bug Fixes:
- Improved stability of u-link/OpenVPN connections.
- Fixed internal timing issue which temporary could lead to 100% cpu load

Version 3.0.0, Build number 72188 Release date: January 18, 2016

New features:
- Implementation of new VPN-based functionality to use the Router with the Weidmüller u-link Remote Access Service. This feature can be configured in menu VPN → u-link.
- An IPsec connection now can be configured in aggressive mode (additional to existing main mode).
- For configuring an IPsec connection several new encryption parameters now explicitly can be set.
- The Packet Filter (Firewall settings) has now the ability to filter on the VPN UP (online) condition. Thus a filter rule matches if the VPN UP LED is on or off. The VPN UP signal can be activated via u-link, OpenVPN or IPsec.

Bug Fixes:
- IPsec connections did not always come back online after changes of time or date on a device. Additionally more detailed IPsec debug information was included on the IPsec status web page.
- The needed time for changing the operational mode (from IP Routing to Transparent Mode and vice versa) has been improved.
- Temporary UMTS/3G connection problems could lead to a complete shutdown of a permanent OpenVPN client connection.

Version 2.7.0, Build number 69965 Release date: June 01, 2015

New features:
- 1:1 Network mapping now can also be used on network interfaces if they are configured using dynamic address assignment (DHCP or OpenVPN).

Bug Fixes:
- IPsec connections did not always come back online after changes of time or date on a device. Additionally more detailed IPsec debug information was included on the IPsec status web page.
- Syslog server support on remote OpenVPN links did not work properly.

Version 2.6.3, Build number 68963 Release date: February 10, 2015

Bug Fixes:

- Optimizing function 'NTP relay server'
- Problem to manually reboot with selection of the second firmware image was fixed.

Version 2.6.3, Build number 68843 Release date: January 26, 2015

Bug Fixes:

- IP-Forwarding from WAN to LAN interface sometimes did not work properly. This failure behaviour was introduced in Version 2.6.3 / Build number 68653.
- DynDNS service could not be configured outgoing to LAN interface (No problem when configuring DynDNS for WAN interface). This failure behaviour was introduced in Version 2.6.3 / Build number 68653.

Version 2.6.3, Build number 68653 Release date: December 08, 2014

New features:

- Implementation of a fall back mechanism when the Firmware is updated. Even if the power supply fails while updating process (Phase Flashing) is running an abort never will result in a broken device.
- Implementation of a "reboot timer" in menu System→Reboot. This feature is quite useful to remotely test new configurations which might lead to a connectivity loss (e.g. based on an unintended firewall configuration). If the reboot timer is activated the device automatically will reboot after the configured time and will come back with the last saved configuration. The reboot timer can be deactivated in menu System→Reboot (Cancel Reboot)
- The Router configuration (Backup file of type *.cf2) now can be loaded also by using an USB stick. The cf2-file has to be placed on a USB Stick in the directory "settings" or "settings/<serial number>". The stick has to be inserted and the device has to be rebooted. The device will load the settings at boot time.

Bug Fixes:

- Patched OpenVPN DoS Bug CVE-2014-810. This update is recommended for all setups running the Router as OpenVPN server with untrusted clients.
- Filter wizard Java Script error was fixed on insertion of predefined rule sets. Was broken since 2.6.0

Version 2.6.0, Build number 67659 Release date: July 07, 2014

New features:

- Automatic fallback mode to a 3G connection if a remote target device no longer is accessible via the WAN port. It is now possible to actively monitor a target IP address via ICMP over the Ethernet link. In case of failures the 3G uplink will be activated.
- 3G interface now can be used for static device routes

Bug Fixes:

- OpenSSL Update to version 0.9.8za (CVS-2014-0224). Update is recommend for all OpenVPNusers with an IE-SR-2GT-xxx OpenVPN counterpart at least on one side of two devices. Otherwise the connection is vulnerable to a Man-in-the-Middle attack due to a OpenSSL bug if both sides of a VPN connection have a vulnerable version of the OpenSSL library

Version 2.5.1, Build number 67460 Release date: June 02, 2014

Bug Fixes:

- German Umlauts were broken on the Permissions page since version 2.3.2
- NTP time synchronization and NTP server relay features have undergone a big cleanup. This includes a new NTP server state page in the web interface. Update is recommended for everyone using the NTP server relay or a highly accurate time synchronization.
- 1:1 NAT now allows an overlapping of local network IP addresses and 1:1 NAT mapping address spaces. Previously the web interface blocked this configuration.

Version 2.3.3, Build number 66690 Release date: January 24, 2014

New features:

- Firmware adapted to be used also for new model IE-SR-2GT-LAN-FN, means that this firmware version can be used for all Weidmüller Router models

  - IE-SR-2GT-LAN →LAN/WAN Router. General features: Routing, Firewall, NAT, VPN IPsec and OpenVPN
  - IE-SR-2GT-LAN-FN →LAN/WAN Router. General features: Routing, Firewall, NAT, No VPN
  - IE-SR-2GT-UMTS/3G →LAN/WAN Router plus additional 3G interface. General features: Routing, Firewall, NAT, VPN IPsec and OpenVPN
- The integrated HTTPS web server now is using a unique self signed certificate generated on factory defaults.
- Performance improvements for pure layer 2 filter without connection tracking.
- 1:1 NAT did not work as uplink network mapping or on local networks with communication across attached IP routers

Bug Fixes:
- Web access restrictions to the HTTP(S) server on the 3G interface did not have an effect.
- 3G connections on private APNs without DNS servers were not marked as CONNECTED because the DNS server was missing.

Version 2.3.2, Build number 65829 Release date: September 20, 2013

Bug Fixes:
- The Forwarding table (Port- and IP-Forwarding) had a wrong sorting for more than 10 entries.
- Under special conditions the DNS server of the 3G interface was used even if the corresponding checkbox was disabled.

Version 2.3.2, Build number 65490 Release date: August 02, 2013

Bug Fixes:
- Problem to show the Forwarding table correctly in Web interface page was solved (caused by a Java script error occured by using Microsoft Internet Explorer).
- A “Dial-On-Demand“ configured 3G/UMTS connection was unintentionally initiated each time a configured NTP time server tried to do a time synchronization even if internal IP addresses are used for NTP time server (cause by an unintended DNS lookup).
- The internal connection tracking table was increased to 32768 entries providing more robustness against DoS attacks and high load.

New features:
- Forwarding table (IP and Port forwardings) now has a new column for comments
- IPsec connections now can be switched by using the VPN key input. Configured connection entries have to be set to the mode “Active (Switched)”

Version 2.3.1, Build number 64408 Release date: April 12, 2013

Bug Fixes:
- Web configuration: Removed the possibility to disable the HTTP server completely in menu ‘Web server’. Use alternatively menu ‚Web access‘ to disable HTTP access.
- Web access control on the LAN port did not work. Access was allowed in any case.
- Function ‘Client monitoring’: Round trip time to control connected clients (if still alive) now can be set up to 5000 ms as maximum. Old maximum round trip time of 1000 ms was very noisy on 3G links.
- Explicit setting of Ethernet transmission mode like 100 MBit/half duplex was not applied on reboot after power down. Instead auto negotioation was used again.

New feature:
- Function ‘Client monitoring’: Allowing reset of the 3G modem if a client monitoring entry fails. This is very helpful on special M2M APNs which might need a 3G network re-registration after some time.

Version 2.3.0, Build number 63969 Release date: March 14, 2013

Bug Fixes:
- Fixed problem using IP aliases in Forwarding table.
- OpenVPN web interface: Now errors will be displayed if wrong options are entered.
- If a configured “Forwarding entry” was changed all running connected communication streams were not reclassified directly after the change (only after reboot).
- IE 8.0 Java Script error occurred if configuring a “Forwarding entry” by web interface.
- OpenVPN with NTLM Proxy Authentication contained a bug which could lead to not working proxy tunneling depending of the proxy vendor. This issues was described in “Public OpenVPN Ticket 172”.

(https://community.openvpn.net/openvpn/ticket/172)

- "Save Only" mode web interface improvements regarding Reboot and Save buttons.

New features:

- Implementation of new "Forwarding table" with below described features:
  - Optional setting of "Source NAT" for forwardings to hide the original source.
  - Conditional source matching to enable a forward only for special addresses.
  - IP Forwarding with IP aliases on VPN channels like IPsec or OpenVPN to run additional virtual IPs on the VPN which will get forwarded to the local network.
  - No more limitations on the number of forwards (before max. 11 forwardings)
  - Configuration of Port- or IP-Forwardings independent of the IP configuration NAT interface (can now be used without having activated "NAT masquerading" either on LAN- or WAN-Port.

Version 2.2.9, Build number 63331 Release date: January 15, 2013

Bug Fixes:

- If a configured paket filter was changed, all running connected communication streams were not reclassified directly after the change (only after reboot).

Version 2.2.8, Build number 63139 Release date: December 19, 2012

Bug Fixes:

- PPPoE password edit with Firefox 15 was broken.
- Ping test on „save only" mode was broken.
- The VPN LED did not work on other OpenVPN interfaces than VPN1.
- Modbus/TCP API calls for OpenVPN reworked. The OpenVPN connection must now be configured without permanent and Modbus/TCP will switch it on and off like a VPN Key event.

New features:

- Complete new OpenVPN web interface with many new features:
  - Implementation of OpenVPN user authentication and VPN-IP-Address assignment using a RADIUS server.
  - Optionally user authentication by User name / Password (additonally to certificate authentication).
  - OpenVPN server with per Client IP address and common name / user name mapping including per client OpenVPN internal routes - "iroutes".
  - Any TCP/UDP port of OpenVPN-Server instances now can be used.
  - OpenVPN cipher can be configured.
  - Complete support for the OpenVPN "redirect-gateway" feature.

Version 2.2.7, Build number 62350 Release date: September 19, 2012

Bug Fixes:

- Running OpenVPN processes did not recognize changes of the DNS configuration.
- Firmware updates from older versions to version 2.2.7 using packet filter rules with stateful or automatic connection tracking will lead to a malfunctioning packet filter. The bug was introduced in version 2.2.7 Build 62062. This bug also effects NAT and port forwarding. The same problem can occur if a "settings file or "SIM card backup" with an older configuration gets loaded into version 2.2.7 Build 62062.
- Further improved 3G Link Stability

New features:

- Implementation of NTP server relay.
- Higher data throughput if the device runs without statefull filter rules.

Version 2.2.6, Build number 61875 Release date: August 13, 2012

Bug Fixes:

- Behavior of setting capacity-buffered realtime clock changed. At delivery time (before first boot of Router) the real time clock is set to production date of Router. If the Router is running more than 24 hours then each time when 24 hours have been passed, then the current date/time will be flashed into the memory as new initial date/time if the Router will be shutdown and powered on again.

New features:

- Implementation of uploading PEM certificate files of type ".crt".

Version 2.2.5, Build number 61501 Release date: June 13, 2012

Bug Fixes:

- SCEP can now be used with automatic renewing and challenge password in combination.

Version 2.2.4, Build number 61357 Release date: May 23, 2012

Bug Fixes:

- OpenVPN HTTP proxy field was restricted to 15 characters, this has been fixed.
- NAT and port forwarding on L3VPN OpenVPN network devices did not work properly.

New features:

- The port forwarding is now called forwarding and was extended to forward on an IP/IP base too using IP aliases on the public interface.
- The VPN LED can now be configured to either run on one of the OpenVPN connections or on Ipsec.

Version 2.2.3, Build number 61087Release date: April 27, 2012

Bug Fixes:

- Upload of certificate files of type ".pem", was broken in version 2.2.3 Build 61052.
- 3G interface bug fixes on DNS server & SIM card state.

New features:

- The OpenVPN integration now supports the configuration of the OpenVPN parameters lzo, tun/tap device types and UDP.
- 3G web interface GUI is now easier to use.
- Ethernet Link Mode can be configured manually.