Firmware Change Log for Industrial Security Router Series IE-SR-4TX

List of affected Router variants:

Article name	Article number
IE-SR-4TX	2751270000
IE-SR-4TX-LTE/4G-EU	2751280000
IE-SR-4TX-LTE/4G-USEMEA	2739630000

General Upgrade/Downgrade information:

Downgrades from version 2.2.2 or higher to version 2.1.2 or below are no longer possible on devices with cellular modems (2751280000, 2739630000) due to EN 18031-1 / RED compliance.

Before commissioning the device for the first time, we strongly recommend checking the installed firmware version and updating to the latest version, if a newer one is available. Please check and download the newest version from the Weidmüller website.

Please note that software maintenance, corrections, and support activities are generally focused on the latest firmware release. Earlier firmware versions may be subject to limited maintenance and may no longer receive updates, fixes, or support over time.

Upgrade to version 2.0.10 or higher is only possible from version 1.6.9. For Routers with versions < 1.6.9 first update to version 1.6.9 followed by a final update to latest version.
For downgrades from version 2.0.10 or higher to version 1.6.9 or below it is necessary to bring the router into compatibility mode. Refer to the manual to find out how to activate compatibility mode.

Version 2.3.4, Build number 189047 — Release date: November 3, 2026

Security Patches:

- This firmware release includes security fixes for a vulnerability tracked under the Weidmüller security advisory **WMSA-2600006**. The update resolves the following CVE:
  - **CVE-2026-109618:** Improper Handling of Exceptional Conditions

Bug Fixes:

- 1:1 NAT: Fixed an issue where ports with 1:1 NAT enabled received a new random MAC address each time the interface was brought up. They now retain their original MAC address.
- Device discovery (ADSDP): Fixed an issue where discovery replies for ports with 1:1 NAT enabled showed the internal interface IP address. They now show the 1:1 NAT address under which the device is reachable.
- Resolved an issue that could cause firmware updates from u-link via WWHv1 to fail. That error started with firmware 2.3.1.
- Improved mobile connection stability when u-link is used for connection monitoring, preventing repeated modem resets.
- Corrected an issue where imported packet filter rules were not applied immediately.
- Fixed port forwardings (DNAT) to a virtual IP address that stayed inactive until reboot when they were added at runtime while traffic to that address was already running.
- The “Start update” button is now available once the required server and file information has been entered.
- Time zone changes now take effect immediately without restarting the device.
- Improved private APN connectivity when username and password authentication (PAP/CHAP) is used.
- Fixed WWAN connection loss with Sierra Wireless EM7455 modem: after a modem reset the WWAN interface could no longer obtain an IP address.

Feature updates:

- strongSwan 6.1.0 is now included, providing the latest security fixes contained in this version.
- u-link diagnostics: Added pre-registration connectivity checks for DNS, proxy, TLS, WWH, VPN, and SCEP endpoints.
- The CA trust store has been refreshed, adding new trusted root CAs and removing certificates that are no longer trusted.
- Web interface, audit log: Improved audit log performance with newest-first sorting, page navigation, entry count, and on-demand loading of older entries.

Copyright © 2026 Weidmüller Interface GmbH & Co. KG
All rights reserved. Reproduction without permission is prohibited.

- Enhanced web interface security by handling unauthorized requests more strictly before their content is processed.
- PHP 8.3.36 is now used, including additional security fixes.

Version 2.3.1, Build number 186119 — Release date: July 28, 2026

Security Patches:

- This firmware release includes security fixes for multiple vulnerabilities tracked under the Weidmüller security advisory **WMSA-2600004**. The update resolves the following CVEs:
  - **CVE-2025-68160**: OpenSSL Line-Buffering BIO DoS Vulnerability
  - **CVE-2025-69418**: OpenSSL OCB Information Disclosure Flaw
  - **CVE-2025-69419**: OpenSSL Buffer Overflow Vulnerability
  - **CVE-2025-69420**: OpenSSL TimeStamp DoS Vulnerability
  - **CVE-2025-69421**: OpenSSL PKCS#12 DoS Vulnerability
  - **CVE-2026-22795**: OpenSSL PKCS#12 Parsing DoS Vulnerability
  - **CVE-2026-22796**: OpenSSL PKCS#7 Signature DoS Vulnerability
  - **CVE-2026-14167**: Privilege escalation during configuration import
  - **CVE-2026-14168**: Vertical privilege escalation via configuration table write
  - **CVE-2026-14169**: Account lockout via non-atomic user creation
  - **CVE-2026-14171**: Post-login open redirect in the web interface
  - **CVE-2026-2291**: dnsmasq Buffer Overflow Vulnerability
  - **CVE-2026-4893**: dnsmasq Information Disclosure Vulnerability
  - **CVE-2026-5172**: dnsmasq Buffer Overflow Vulnerability
  - **CVE-2026-40510**: OpenSC Buffer Overflow Vulnerability
- We strongly recommend updating to this firmware version to ensure optimal security and system integrity.

Bug Fixes:

- Improved SMS Service page usability: Fixed layout inconsistencies, including trap notification checkbox alignment and configuration group formatting.
- Fixed LTE/WWAN authentication issue: Resolved a problem introduced in firmware 2.2.7 that prevented connections when passwords contained question marks (?) or certain other special characters. Existing configurations that worked in earlier firmware versions are now supported again.
- Enhanced Web Access configuration safety: Added clear warning messages and an explicit confirmation step when disabling web access on the currently active management interface or when disabling all remote access interfaces, helping to prevent accidental lockouts.
- Re-added missing SMS feature to the Webinterface of the WWAN products (IE-SR-4TX-LTE/4G-EU & IE-SR-4TX-LTE/4G-USEMEA).
- Removed a legacy packet-filter cleanup routine that could trigger a spurious SQL startup log error ("no such column: ICMP"). The routine had been inactive since version 2.0.10.

Feature updates:

- The Web Interface was refactored to improve Usability. Most noteable this includes a new Startpage, Firmware Update Section and IPsec config page.
- Enhanced modem watchdog functionality: A secondary monitoring IP address can now be configured to improve connection supervision. The modem is restarted only if all configured monitoring targets are unreachable for the defined offline timeout. The timeout is now configurable in seconds (default: 60 seconds). Alternatively, the u-link WWH heartbeat can be used as the monitoring criterion, triggering a modem restart if the heartbeat is unavailable for the configured timeout period.
- Added GCM cipher (AES-256-GCM) and EC Diffie-Hellman groups (ecp256, ecp384, ecp521, curve25519) to the IPsec configuration options for BSI TR-02102 compliance.
- The IPsec configuration page has been redesigned with an improved layout. In addition, IPsec connection entries can now be edited directly within the connection table for easier configuration and management.
- Starting with this firmware version, u-link VPN WWHv3 is the default protocol for devices restored to factory settings. **The new primary server address is wwh2-we.aw-cp.de**. Customers using border firewalls should allow connections to the new server. Existing installations are not migrated automatically during firmware updates; WWHv3 must be enabled manually if desired. Migration to WWHv3 is recommended.
- Added DHCP server support for PXE boot (UEFI x86_64) and NTP server distribution to DHCP clients.

Version 2.2.8, Build number 183820 — Release date: May 27, 2026

Copyright © 2026 Weidmüller Interface GmbH & Co. KG
All rights reserved. Reproduction without permission is prohibited.

Bug Fixes:

- Fixed Ethernet link failures on power-up when connected to systems with certain Intel network controllers. The IE-SR-4TX integrated Ethernet switch now disables Energy Efficient Ethernet (EEE) earlier during boot to prevent a timing-related issue that could cause link negotiation to fail.
- Improved input validation for mobile network (UMTS/LTE) username and password fields. The allowed character set is now restricted to commonly used characters, and the maximum length is limited to 64 characters.
- The built-in DNS resolver no longer returns IPv6 records, as IPv6 is not supported on the device.
- New passwords can no longer contain German umlauts (ä, ö, ü). This restriction is required because umlaut characters may be encoded differently depending on the browser, which can cause the password to be stored in a different form than entered — making it impossible to log in afterwards. Existing passwords containing umlauts remain valid and can still be used to log in.
- The firmware now provides the ability to configure the MTU (Maximum Transmission Unit) for cellular/WWAN connections via the web interface. The configurable range is 1300 to 1500 bytes, with 1500 bytes as the default value. This setting is particularly useful when using VPN connections or tunnels over private APNs where the underlying cellular link has a smaller MTU.
- Packet filter rules are no longer reset to factory defaults when switching the operating mode. Previously, all user-defined packet filter rules were replaced with default rules upon an operating mode change. This was originally intended behavior, as packet filter rules may depend on network interfaces that differ between operating modes. However, this automatic reset has been removed. Note: After switching the operating mode, existing packet filter rules that reference network interfaces not available in the new mode may become invalid and should be reviewed and cleaned up manually by the user.
- PKCS#12 certificate files with embedded private key can be uploaded correctly now.
- The IPsec VPN configuration now accepts the wildcard (*) as remote IP address for roadwarrior setups
- Switching the WAN uplink from DHCP to a static configuration previously caused the Configuration Wizard to ignore the defined interface settings. This issue has been fixed.
- NTS authentication status is displayed in the web interface in the correct way.
- Resolved an issue where NTS (Network Time Security) configuration options were missing from the user permissions settings page. Administrators can now control per-user visibility of NTS settings such as NTS service, trusted CA, relay and relay certificate.
- Improved stability of the configuration wizard by ensuring the apply request is sent only once after all validation checks complete, instead of once per checked element.
- Fixed an issue in the web interface where repeatedly clicking the login button during a lockout period caused the countdown timer to accelerate visually. The security lockout mechanism itself was not affected - only the displayed countdown was incorrect. The login button now remains properly disabled throughout the entire lockout period, accurately reflecting the remaining wait time.
- Changes made to the custom navigation menu were not saved and were silently discarded. This behavior has been corrected.
- The Configuration Wizard could become unresponsive when applying WWAN uplink settings. In addition, error handling has been improved to better manage network link losses during uplink configuration changes.
- Configuring a gateway in the setup wizard could trigger an incorrect redirect to the IP configuration page due to a connection timeout. This has been resolved.
- Authenticated users were unable to see network traffic and packet filter statistics graphs on the start page. The graphs are now displayed correctly.
- The “Fallback Monitoring Address” field previously accepted only plain IP addresses. It now also supports valid hostnames and hostname:port combinations.
- The UMTS roaming option on the IP configuration page sometimes showed an incorrect state after the page was loaded. The display issue has been fixed.
- When multiple authentication entries were configured, the NTS (Network Time Security) status table was displayed incorrectly. The layout has been corrected.

Feature updates:

- It is now possible to select which local network interfaces are pushed as routes through the u-link VPN tunnel. The configuration is available under Configuration -> VPN -> u-link -> Network route push to u-link VPN. Only interfaces with a static IP assignment are pushed. Interfaces using DHCP are excluded automatically, even if the checkbox is enabled.
- Empty lines in the event log are no longer displayed. The log display area has been enlarged — more entries are directly visible without scrolling. The layout has been widened for a better overview.
- Improved permission handling on configuration pages with interface access lists. Users with partial write permissions can now still apply permitted settings, while non-writable options are shown disabled and are excluded from submission.
- Added support for up to three SNMP trap receivers, enabling redundancy when the primary trap receiver is unavailable.
- The u-link Web Access function, which allows local network services to be accessed directly via u-link, can now be enabled or disabled in the web interface. A new option is available under Configuration ->

Copyright © 2026 Weidmüller Interface GmbH & Co. KG
All rights reserved. Reproduction without permission is prohibited.

VPN -> u-link -> Allow dynamic port forwardings. Note: The Web Access function requires an active WWH3 connection.
- The NAT (Source NAT) option is now enabled by default for LAN and WAN interfaces, simplifying initial network configuration.

Version 2.2.6, Build number 181925 **Release date: January 5, 2026**

Bug Fixes:
- Improved error message display for password changes in the Configuration Wizard and Users page. Error messages are now properly shown when passwords do not match or validation fails.
- The OpenVPN Client will not reject any IPv6 settings and continue with the IPv4 settings if a OpenVPN server pushes both IP settings.
- Previously, users with restricted write permissions needed full write access to all settings on a page in order to make any changes. This has been improved for the Date & Time page: input fields without write permission are now disabled, while the remaining fields can still be modified.
- The 1:1 NAT functionality for u-link VPN connections has been fully restored. Earlier firmware versions had unintentionally removed both configuration variables and the related web interface elements, which made the feature unavailable. Now all components have been reintroduced and 1:1 NAT operation is fully functional again.
- IP forwarding rules configured with IP-alias addresses (Local IP field specified) were not applied directly; they only became active after saving the configuration and rebooting in older Versions. This is fixed now.
- Improved error handling for certificate uploads. Invalid or unsupported file formats are now correctly detected and reported.
- Updated the password strength help text to clearly describe all password policy requirements, improving usability and security transparency for users.
- Improved handling of WWH protocol switching for u-link (WWHv1 / WWHv3). Switching between protocol versions is now processed more reliably, ensuring stable reconnection and consistent VPN operation.
- Fixed a JavaScript error on the USB access configuration page that previously prevented applying settings. The page now operates as expected.
- Resolved an issue where the Remote Capture service (Port 2002) was not starting correctly after being enabled. The service now operates as expected.
- When importing a cf2 file created with the exact same software version, the routers rules cache was not rebuilt, which could leave stale data and cause incorrect packet filtering until the filter configuration is changed or the device is switched to a different software version. The cache is a local copy of the active Linux kernel rules, used to speed up boot, and it is normally refreshed when changes are applied or firmware versions change. In this bug scenario, the import skipped regeneration, leaving data from a previous configuration. In 2.2.3, the cache will always be regenerated on import to avoid the issue. Until then, clicking Apply and then Save, or creating the cf2 file from an older firmware version, ensures a correct cache.
- The rule name input field now enforces the backend‘s 16-character limit, preventing unnecessary configuration errors and improving usability.
- Added a clear warning message to prevent unintentional lockout when disabling all remote access interfaces.
- Fixed a bug where the hostname was not sent correctly in a DHCP request.
- In version 2.2.2 to 2.2.3, a regression caused the device’s web interface to no longer show the SNMP network service configuration. This issue has now been resolved. Importantly, previously configured SNMP options and overall functionality were not affected; the bug was limited to the web interface display.

Feature updates:
- The Audit-Log functionality has been significantly extended. The system now records a comprehensive range of hardware and network-related events, including USB device connections, Ethernet link changes, VPN key or CUT signal transitions, and u-link VPN connection states. These enhancements improve transparency and traceability for system administrators and are fully integrated into the web interface for clear and structured visualization of all relevant Audit-Log entries.
- The Audit Log system will now log changes of date and time and jumps in a new section "System".
- The Audit Log can now be forwarded to a Remote Syslog Server. Use the Eventlog Configuration web page to configure this function.
- The firmware now allows uploading a custom CA certificate including its private key. This enables operators to integrate the device into an existing PKI or OT-wide trust hierarchy instead of relying on the automatically generated self-signed CA. When a custom CA is provided, the device automatically issues its HTTPS server certificate from this CA, including the current DNS hostname and all assigned IP

Copyright © 2026 Weidmüller Interface GmbH & Co. KG
All rights reserved. Reproduction without permission is prohibited.

addresses as X.509 Subject Alternative Names (SANs). If the uploaded CA is a subordinate CA of a higher-level organizational root, multiple devices within the same OT environment can share the same trust anchor. This significantly improves interoperability and security by enabling mutual trust between systems and simplifying certificate management across installations.
- A strong password policy is now enforced by default when the device is reset or started with factory defaults. Existing installations are not affected by updates.
- The web interface now includes security headers in its HTTP responses to improve browser protection. These headers help prevent content type spoofing and unauthorized embedding of the web interface, increasing resilience against common web-based attack vectors. The options set are: "X-Frame-Options: SAMEORIGIN" and " X-Content-Type-Options: nosniff".
- Introduced a session limit to prevent excessive concurrent logins. This improves system stability and protects memory resources during intensive operation.
- Allow dynamic port forwarding on u-link with WWH3.
- Added Secure NTP (NTS-KE) for Client and Server/Relay operations.
- OpenVPN: Allow minimum version TLS 1.3 from now on.
- I/O Settings are added to the menu of the web interface.

Version 2.2.3, Build number 180042 Release date: September 16, 2025

Bug Fixes:
- IP forwarding rules configured with IP-alias addresses (“Local IP” field specified) were not applied directly; they only became active after saving the configuration and rebooting.
- When importing a cf2 file created with the same software version, the firewall rules cache was not rebuilt, which could leave stale data and cause incorrect packet filtering until the filter configuration is changed or the device is switched to a different software version. The cache is a local copy of the active Linux kernel rules, used to speed up boot, and it’s normally refreshed when changes are applied or firmware versions change. In this bug scenario, the import skipped regeneration, leaving data from a previous configuration. In 2.2.3, the cache will always be regenerated on import to avoid the issue. Until then, clicking Apply and then Save, or creating the cf2 file from an older firmware version, ensures a correct cache.
- In version 2.2.2, a regression caused the device’s web interface to no longer show the SNMP network service configuration. This issue has now been resolved. Importantly, previously configured SNMP options and overall functionality were not affected; the bug was limited to the web interface display.

Feature updates:
- By default, the password strength policy is now enforced on all newly deployed devices as well as on devices that have been reset to factory defaults. Consequently, the configuration wizard prevents completing setup with a weak password.
- The Web Interface is now using "Content Security Policy" options in the HTTP header as far as possible.

Version 2.2.2, Build number 179544 Release date: August 18, 2025

Bug Fixes:
- Fixed a regression in the Layer 2 Packet Filter introduced in version 2.0.10. Manual TCP Flags (field name: "state") filter rules at Layer 2 were not accepted and were inadvertently removed during updates from version 1.6.9 to 2.x.y.
- A regression bug introduced in version 2.0.10 that affected stateful ICMP rules in the Packet Filter was fixed. These rules were unintentionally removed by a new database consistency check during update. ICMP rules can be created using three methods: "automatic", "stateful", and "manual" — only the "stateful" method was affected by this issue. This has now been fixed. Note: If you previously used stateful ICMP rules, please verify they are still present and valid after updating.
- The Filter Wizard database once again supports names up to 32 characters for background processes such as updates from older versions or the import of settings via API. Therefore, the upload of older configurations will no longer fail because of longer names. The user interface will continue to enforce a 14-character limit due to internal Linux kernel topics.
- When the Remote Capture Service was enabled, it started correctly, but the Web Interface UI failed to return to its normal state after clicking the Apply button. This regression bug was introduced with version 2.0.10.
- Fixed a regression affecting the diagnostic data download feature. After clicking the "Download" button, the interface became unresponsive, and the button remained disabled. This issue was introduced in firmware version 2.1.0. The download function now works as intended.
- The OpenVPN Server configuration table for clients was fixed. There was no clear error message if no password was supplied, this could lead to the impression that it is impossible to add ad entry into the table. The UI was fixed to enforce the password.
- No message was displayed regarding saving when a user account was deleted.

Copyright © 2026 Weidmüller Interface GmbH & Co. KG
All rights reserved. Reproduction without permission is prohibited.

Feature updates:

- Added a fail to ban mechanism based on the source IP address. By default, a ban time of 60 seconds after 10 wrong passwords attempts from a same IP is active after software update to 2.2.0. The ban is issued on the source IP independent of the tried username. The login ban behavior is configurable.
- A new Denial-of-Service (DoS) protection mechanism has been implemented. This enhancement safeguards the router against local network DoS attacks, particularly on Ethernet segments, ensuring greater reliability and resilience during device discovery and configuration.
- Added a Network Monitoring Mechanism which will detect ARP cache poisoning attacks to the devices own IP and report them as Anomaly in the Audit system.
- Added auditability of configuration changes.
- Added auditability of Packet Filter matches. The logging is limited to one message for each rule per minute.
- WWH 3.0 protocol version can now be enabled for early adopters.
- Enhanced SNMPv3 Support:
    - New cryptographic hash algorithms have been added, now supporting up to SHA-512.
    - SNMPv3 traps have been fixed and are now functioning correctly. The SNMP Engine ID can now be configured manually as well.
    - User synchronization: SNMPv3 usernames and their write permissions are now synchronized with the main user database. This reflects the requirements of upcoming IEC62443 4-2 functional requirements. However, due to differing password algorithm requirements, SNMPv3 service passwords must be configured separately.
    - Security Note: SNMPv3 user passwords are stored in clear text on the device, as required by the SNMPv3 authentication algorithm.
    - The SNMP service (UDP Port 161) can now be restricted to selected interfaces.
    - The password policy and lifetime mechanisms are not enforced to the SNMPv3 passwords to keep update compatibility.
- The Status LED will now signal the new commissioning mode (Use of the Config Wizard) in case of factory default settings. Please note that the devices will no longer forward IP traffic between the different network interfaces LAN/WAN or ETH1/ETH2-4 if it is not yet configured and running in commissioning mode.
- The NTP server interface and the Remote Capture Server interface can now be configured with a network interface input filter.
- When initially setting up the router or after a factory reset, a secure new password must be assigned.

Features disabled:

- SNMPv1 and v2 have been removed to comply with the upcoming EN18031-1/RED regulatory standard. When updating or importing older settings that contain SNMP configurations:
    - SNMPv2 settings will be automatically removed and disabled.
    - SNMPv3 usernames that do not exist in the main user database will be created automatically with randomly generated passwords. These will be assigned read-only permissions in the permissions database or write-all permissions for the SNMP read/write user. This reflects the behavior of previous versions.
    - SNMPv3 usernames already existing in the user database will be enabled if they were previously disabled. Their SNMPv3 service password will be set to a new random value. No changes will be made to their existing user account permissions.
    - All network interfaces will listen for SNMPv3 requests if the service was enabled.
    - **SNMP Traps will get disabled on update and must be reconfigured.**

Version 2.1.2, Build number 177014 — Release date: May 15, 2025

Bug Fixes:

- Resolved an issue where packet filter rules using negated interfaces (e.g., != WAN) were mishandled. This regression, introduced in version 2.0.10, caused such rules to be incorrectly removed during updates and prevented them from being added through the configuration interface.
- Fixed Login via u-link Web Access to the device itself, which was broken due to a regression bug starting with version 2.1.0.
- **Fixed:** Restored u-link dynamic forwarding for VNC and other protocols when the device operates in legacy MD5 password mode. This functionality was previously broken due to a regression introduced in version 2.1.0.
- Improved IPsec certificate-based ID handling which could lead to incompatibilities with other vendors.

Feature updates:

- Added the possibility to display a custom text on the login screen.

Version 2.1.1, Build number 175935 — Release date: Apr 22, 2025

Copyright © 2026 Weidmüller Interface GmbH & Co. KG
All rights reserved. Reproduction without permission is prohibited.

Bug Fixes:

- The new password policy and password storage migration buttons on the User Accounts web page have been redesigned for improved clarity and ease of use.
- In versions prior to 2.0.10, it was possible to disable HTTPS entirely. However, starting from version 2.0.10, HTTPS is mandatory as it is the only supported interface. Devices that had HTTPS disabled in previous versions and were upgraded to 2.0.10 or higher experienced a complete loss of web UI access—neither HTTP nor HTTPS was available due to the old setting preventing HTTPS from being enabled. To prevent this issue, the option to disable HTTPS has been removed from the internal configuration.
- Resolved a regression bug introduced in versions 2.0.10 of the Filter Wizard that prevented users from adding new rules to existing rule sets. While newly created rule sets appeared in the UI, they were not actually applied and would disappear after a reboot if more than 14 characters have been used for the ruleset name.
- Fixed u-link routing issue affecting 1:1 NAT configurations, which was introduced by a regression bug in version 2.0.10.

Feature updates:

- Enhanced IPsec Policy Configuration. Feature: Allow 0.0.0.0/0 as the IPsec remote subnet for IPsec policies. Note: When configuring an IPsec policy with 0.0.0.0/0 as the remote subnet, ensure you add appropriate static IP routes targeting the IPsec device. These routes are necessary to direct the traffic into the IPsec tunnel for this special case.
- The IPsec configuration web page has been enhanced to provide a clearer and more intuitive DH group selection process.
- Added the ability to specify the maximum password reuse limit to ensure compliance with IEC 62443-4-2 FR 1.
- Integration of a new Security Audit system. In the first step it will record all failed and successful logins into the administrative web interface and APIs in a persistent internal database. The feature is designed to comply with IEC62443 4-2 CR 2.8, CR 2.9 and CR 2.10.
- The password lifetime can now be configured according to IEC62443 4-2 CR 1.7.
- Network interfaces that obtain their IP address via DHCP will now perform a DHCP refresh when the Ethernet link is disconnected and reconnected. If the interfaces are part of an internal Ethernet bridge, this refresh will only occur when all connected interfaces lose their Ethernet link.
- Added the possibility to hide or show menu entries for specific users in the web interface.

Version 2.0.10, Build number 174437 — 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 1.6.9.
- 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 1.3.4.
- 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

Copyright © 2026 Weidmüller Interface GmbH & Co. KG
All rights reserved. Reproduction without permission is prohibited.

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.
- 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.

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 1.6.9, Build number 163587 — Release date: Feb 06, 2024

Bug Fixes:
- The PPPoE settings on the web interface had been invisible due to a regression bug introduced with version 1.6.4
- The remote syslog was not working correctly after a system reboot.
- The date and time settings did not allow dates after 2023.
- Removed the VPNUP I/O signal toggle option as the device has no output signals.
- Fix SMS service on IE-SR-4TX-LTE/4G-USEMEA model with Sierra Wireless EM7455 modems
- 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.
- 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.

Feature updates:
- Added the possibility to upload a WWAN modem update in the device web interface. Use the web interface and navigate to: System -> Software Update -> Tab:WWAN. Please contact Weidmüller support for new firmware files if needed
- Enable the SMS features and the WWAN network scan for IE-SR-4TX-LTE/4G-EU models with Fibocom NL668EAU modem. Additionally the mobile phone number and ICCID of the SIM card have been added to the WWAN status page for all modems.

Version 1.6.4, Build number 157902 — Release date: Sep 25, 2023

Bug Fixes:
- Config files from IE-SR-4TX-LTE could not be loaded into an IE-SR-4TX-LAN and vice versa. This has been fixed.
- 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

Copyright © 2026 Weidmüller Interface GmbH & Co. KG
All rights reserved. Reproduction without permission is prohibited.

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.
- 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 1.6.3, Build number 156152 — 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 1.6.0. 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.

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 1.6.2, Build number 154726 — 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 1.6.1.

Version 1.6.1, Build number 154276 — Release date: May 30, 2023

Bug Fixes:
- 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 1.5.0 and 1.5.1.
- 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 1.5.0 and 1.5.1 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:

Copyright © 2026 Weidmüller Interface GmbH & Co. KG
All rights reserved. Reproduction without permission is prohibited.

- 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 1.5.1, Build number 151683 — 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 1.5.0.
- Fixed a regression bug regarding transparent bridge mode on the device web interface introduced with version 1.5.0. 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 1.5.0.
- 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 1.5.0.
- The HTTP API (get.php) did respond with wrong multiline formating on "statuslong" calls due to a regression bug introduced with version 1.5.0.

Version 1.5.0, Build number 150459 — Release date: Apr 13, 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)

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 1.4.7, Build number 148034 — Release date: Jan 18, 2023

Bug Fixes:

- 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 reestablished faster or the following integrated WWAN modems: EM7455, EM73x4, MC7455, MC73x4 and SIM8202G
- Fixes an internal memory leak that occurs while u-link VPN is active. The leak is cleaned up when the VPN is down and occurs when the VPN is up. While the leak is present, the overall performance of the system slowly decreases. An update is recommended if u-link VPN is used as a permanent connection or over longer periods of time. The bug was introduced with versions 1.3.4
- The IP route pushing of additional static routes with u-link VPN client was broken. The bug was introduced with 1.3.4
- In some cases, the embedded web server was terminated when a user reconfigured the date and time. This has been fixed.
- Improved values for multiple interface dropdowns within the device web interface
- Removed an empty item in the packet filter interface drop-down lists.
- The current date and time were displayed differently on the home page than on the date and time page.
- New switch chip did not disable the WAN port if a digital in CUT signal was configured to do so.
- Added the possibility to disable the ports LAN1-LAN3
- Update of integrated software package dnsmasq to version 2.86. (see CVE-2021-3448)
- Status call nslookup4 crashes when static configured DNS server is not available
- 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.
- IPsec Update to strongSwan 5.9.6
- 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.
- IPsec connections with certificates suffered from a race condition at system startup. This could lead to no IPsec connection being established immediately after booting.

Copyright © 2026 Weidmüller Interface GmbH & Co. KG
All rights reserved. Reproduction without permission is prohibited.

- If the default gateway was changed on devices with 1:1NAT configuration, the 1:1 NAT IP addresses of the device could be temporarily lost. Only a reconfiguration or a device restart could rectify the situation.
- HTTPS connections to the device's web server could drop for several hours if the device's date and time were changed abruptly, such as when the NTP client was enabled.
- Fix 1:1 NAT on u-link or OpenVPN interfaces

Feature updates:

- Improved WWAN SIM card exchange on all 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.
- Added Support of new memory cards using the SCM slot.

Version 1.3.4, Build number 140962 Release date: October 14, 2022

Bug Fixes:

- Complete rewrite of the Modbus/TCP Service for controlling and monitoring the VPNs of the device. Please see the updated manual for details. It is - for example - now possible to use the u-link acknowledge by API with Modbus/TCP.
- The Modbus/TCP API reported seemingly valid values for whereas this product dos does not have the CUT and ALARM feature. This has been changed. There will be a Modbus Exception if these registers are read or written.
- The 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.
- 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.
- 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.
- 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
- The JSON/RPC method alarm.get() did not work as expected. This has been fixed.
- The internal WWAN connection monitor process was not stopped when the feature was disabled. A save and reboot cycle was required to stop the feature.
- The WWAN MMC and MNC settings were only applied when they git configured for the first time but not anymore after a reboot.
- Updated integrated zlib library regarding CVE-2018-25032
- 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 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 unwanted 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
- 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.
- 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.
- The internal time zone database has been updated.
- The various u-link checks in the start-up wizard, configuration page and status page have been synchronized.
- The Web interface Eventlog is now a "read only" HTML element.
- u-link was not available on the forwarding page

Copyright © 2026 Weidmüller Interface GmbH & Co. KG
All rights reserved. Reproduction without permission is prohibited.

- 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
- Security Update of the integrated libcurl to version 7.83.1
- 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.
- 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.

Feature updates:

- IPsec: It is now possible to use wildcards to match remote identities (e.g.*@<your _domain.de>, *.<your _domain.de>, or C=DE, O=<your _domain>, CN=*)
- Support for hardware with new 4G WWAN modem: Fibocom NL668EAU

Removed features:

- 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 1.2.9, Build number 136467 — Release date: March 22, 2022

Bug Fixes:

- Fixed a bug which caused the web interface to behave very slowly especially on the "Save Settings" page. The bug is only present on the latest devices with a slightly different hardware.

Version 1.2.6, Build number 132889 — Release date: December 02, 2021

Feature updates:

- Support for IE-SR-4TX* with alternative Ethernet switch chip. These routers cannot be downgraded to older firmware versions than 1.2.6.
- JSON/RPC API has been extended with a new config.import_config() call.

Bug Fixes:

- A very rare error which can occur when restoring the factory settings has been fixed. In the event of an error, the affected devices no longer show a valid configuration and can then no longer be reached via the network. In these cases, the only thing that helped was a new factory reset.

Version 1.1.2, Build number 125086 — Release date: August 25, 2021

Bug Fixes:

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

Version 1.1.0, Build number 123476 — 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.
- 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 1.0.12. Improved fallback to work even if SNAT is not active on the monitoring interface. Monitoring with ICMP was not affected.
- Write permissions for u-link configuration and SMS service configuration can now be changed using the web interface permissions page.
- Fixed dynamic routing with RIP

Copyright © 2026 Weidmüller Interface GmbH & Co. KG
All rights reserved. Reproduction without permission is prohibited.

- Config-Wizard did not enable u-link completely, the user had to enable it additionally on the u-link web 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.

Version 1.0.12, Build number 116627 — Release date: March 28, 2021

Feature updates:

- The Forwarding feature has been extended to forward UDP or TCP port ranges.

Bug Fixes:

- Fix of an internal race condition of IP forwarding feature in cases of configuration changes with parallel traffic. In seldom cases this could lead to some running TCP streams to not get forwarded as expected.
- Fix of regression bug introduced with 1.0.7. NATing and filtering of active FTP was broken.
- Bugfix in case of problems with IPsec connection establishment with user supplied CA certificates.
- IP forwarding with IP aliases could be influenced by OpenVPN or u-link connection events due to an internal race condition in terms of connection tracking with parallel traffic.
- Fix of issue referenced by CVE-2021-3156: Integrated FOSS component 'sudo' has been updated to version 1.9.5p2. Prior to that version there was a privileged escalation bug weakening the internal security chain.
- 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.

Version 1.0.9, Build number 112614 — Release date: November 23, 2020

Feature updates:

- IPsec IKEv2 can now be activated.By default, active connections are now initiated using IKEv2, but IKEv1 connections are passively accepted.
- Update of the integrated lighttpd web server from 1.4.33 to 1.4.55.Note: none of the known CVEs had any security effect to any Weidmüller security routers as the faulty components or configurations where not enabled at any time:CVE-2013-4508, CVE-2013-4559, CVE-2013-4560,CVE-2014-2323, CVE-2014-2324

Bug Fixes:

- The mobile WWAN connection was not monitored for connection loss on IE-SR-4TX-LTE/4G-EU version. In case of a long-time interrupt (hours) of mobile connectivity the connection was not reestablished automatically even on the configuration setting "permanent" was enabled.
- Fixed IPsec status web page.
- Fixed IPsec logging into the Eventlog
- Fix new WWAN fallback using TCP ping which was introduced in the previous version.

Version 1.0.7, Build number 109487 — Release date: October 8, 2020

Bug Fixes:

- Fixed function of the Digital Input to initiate VPN connection

Version 1.0.7, Build number 106548 — Release date: July 7, 2020

Initial Release

Copyright © 2026 Weidmüller Interface GmbH & Co. KG
All rights reserved. Reproduction without permission is prohibited.