Firmware Release Note for Security Router model

- IE-SR-2TX-WL (Article No. 2682590000)

Attention: 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 for download from the Weidmüller website.

For information on bug fixes, implementation of new functions and other adjustments to previously released firmware versions, please read below release notes carefully.

Firmware update: If - after starting - the update process stops unintendedly during the initial file upload process file (does not upload 100% or stops after reaching 100%), the currently free RAM memory has reached a critical size for completing the firmware update process. In this case reboot the device (via Webpage 'Administration → Reboot' or Power down/up) to delete temporary files. Then repeat the firmware update process again.

Version 1.52 (RED DA compliant) July 31, 2025

Note: Regarding comparable features and bugfix status this firmware V1.52 corresponds to version V1.67 of router models with integrated cellular modem (IE-SR-2TX-WL-4G-EU / Article No. 2682560000 and IE-SR-2TX-WL-4G-US-V / Article No. 2682580000).

Attention: Firmware version V1.52 (and newer ones) meets the EU RED-DA cybersecurity requirements (EN 18031-1:2024) related to RED Article 3.3(d) for products with connectivity functions that must prevent unauthorized access and misuse of data.

Feature Enhancements / Updates:

- New user accounts 'user' and 'guest' added additionally to existing user 'admin' (Full rights administrator). Can be configured on Website 'Administration → System Settings'.
  - Rights of account 'user': Access/Change of Webpages 'System Info', 'Interface Configuration', 'Network configuration', 'Reboot', 'Diagnostics' and 'Save Configuration' including submenus.
  - Rights of account 'guest': Read-only access to Webpages 'System Info' and 'Diagnostics'.

  Note: After update to V1.52 (or later) from any previous version before V1.52 and taking over the current configuration (no reset to factory defaults), there is no change in terms of user management. Existing 'admin' account is working as before, new accounts 'user' and 'guest' are disabled by default. They can be activated on Webpage Administration → System Settings.
- For a device having factory default settings the default 'admin' password must be changed at first login to ensure legal access security. Accounts 'user' and 'guest' are disabled by default.
- New levels for required cryptographic password strength added (Strong, Medium, Weak). By default, the strong encryption level is set and recommended for use.
- Implementation of a 1-minute blocking time to access the Web interface after repeatedly (5 times) entering the password incorrectly to increase the access security.
- SNMP: Now versions SNMPv1, SNMPv2c and SNMPv3 are supported. Due to security requirements SNMP is disabled by factory default.
- New feature 'DDoS Protection' (Distributed denial-of-service) added for protection against incoming traffic flooding (Webpage Firewall Settings →DDoS Prevention).
- New 'Event Log' (additional to existing 'System Log') added to monitor user- and security-related events.

- Firmware updates (up- or down-grades) starting on a device running a RED DA compliant firmware (V1.52 or newer) require an additional checksum file (provided together with firmware file) to ensure the data integrity of the firmware file.

  Note: If - for any reason - a downgrade is necessary to any previous version before the first RED DA compliant version V1.52 please contact the Weidmüller support for getting the “old” firmware version and the associated checksum file.

Bug Fixes:

- Feature ***‘Send individual Mails based on received content from remote device’***: The Router’s status response message (‘0’ + <CR><LF> or ‘1’ + <CR><LF>) after receiving the “Mail Send information” was mistakenly divided into 2 TCP packets (first with status ‘0’ or ‘1’, second contained <CR><LF>). Now it behaves according to the definition. For more information click ‘Help’ on Router Webpage ‘Event Settings → Mail’.

Version 1.49 Release date: June 12, 2025

Note: Regarding comparable features and bugfix status this firmware V1.49 corresponds to version V1.64 of router models with integrated cellular modem (IE-SR-2TX-WL-4G-EU / Article No. 2682560000 and IE-SR-2TX-WL-4G-US-V / Article No. 2682580000).

Feature Enhancements / Updates:

- Enhancement of runtime stability by implementation of a control function for limiting tasks against excessive memory usage and too high processor load.
- Implementation of new feature ***‘Send individual Mails based on received content from remote device’***: : Via this feature any smart device can transfer a simple data string (containing all relevant information of a mail) to the Router (either via serial interface or TCP connection) to generate and send a mail with individual text and recipient address.
- Website ‘Administration → System Settings’: Checkbox ‘Redirect to HTTPS‘ has been added to force a secure login into the Router’s Web interface using HTTPS.
- Website ‘VPN → Files / Certificates’: If a file without an extension will be uploaded to directory ‘Other Files (Directory /etc/files/)’ then for such a file the action buttons ‘View‘ and ‘Download‘ will be removed. This prevents getting the content of the stored file, for example due to security reasons.

  For example, by storing a file with name 'username_password' in /etc/files it can be used to secure (not readable) the configured 'username' and 'password' for OpenVPN option 'auth-user-pass' (Configure: auth-user-pass /etc/files/username_password).
- Website ‘Firewall Settings → IP Filter (Local Access)’: Parameter ‘*Prioritization over Device Access Rules (Http[s], Telnet, SSH)*’ has been added additionally for creating custom filter rules. All configured rules with enabled priority will be applied topmost over
  - the general device access rules (Http[s], Telnet, SSH, to be enabled/disabled via checkboxes on web page 'Administration ➔ System Settings'),
  - non-prioritized custom rules,
  - and default policy rules.

  For example, this allows to configure an IP-specific device access, if necessary for security reasons.

Bug Fixes:

- If the Router was running as ‘Wireless Client’ (Internet/WAN Connection) and a DNAT rule on WLAN interface with an additional virtual IP has been configured, then this virtual IP has been shown on website ‘System Information → System Overview’ instead of the real WLAN IP address.

- VPN IPsec: An established VPN connection was not re-established automatically, if the connection temporarily was interrupted by the VPN peer (for example after reboot of the VPN peer device). The Router needed to be rebooted also, then everything worked properly again.
- Website ‘Administration → Firmware Update’: Name of selected update file could not be seen completely. For example, after file selection a user could not verify if the version number contained in the selected file name, was the right one which he wanted to select.
- Elimination of security vulnerability **CVE-2025-41661**. Issue: Possibility of arbitrary command injection in Main Web Interface (Endpoint event_mail_test).

  Solution: 1. Remove of the eval command.

  2. Check the input validity of SMTP / Port / Sender and the three Receiver fields to prevent illegal input.
- Elimination of security vulnerability **CVE-2025-41662**. Issue: Possibility of arbitrary command injection in Main Web Interface (Endpoint tls_iotgen_setting).

  Solution: Remove of the eval command.
- Elimination of security vulnerability **CVE-2025-41663**. Issue: Possibility of arbitrary command injection resulting in a stack buffer overflow in the u-link Management API.

  Solution: Check input validity of Network / Subnet and Gateway fields to prevent illegal input.

Version 1.48 Release date: February 24, 2025

Note: Regarding comparable features and bugfix status this firmware V1.48 corresponds to version V1.60 of router models with integrated cellular modem (IE-SR-2TX-WL-4G-EU / Article No. 2682560000 and IE-SR-2TX-WL-4G-US-V / Article No. 2682580000).

Feature Adaptions / Improvements:

- New function “Bootloader update” has been implemented.
  - After firmware upgrade new parameter “Bootloader version” is shown in Webpage “System Overview” → Section “System Data”, additionally new tree menu item “Bootloader Update” has been added in section “Administration”.
  - General information why updating the bootloader to a version >= V1.5 could be necessary:
    - On routers with bootloader version V1.4 both RJ45 ports (LAN and WAN) behave like an **unmanaged 2-Port Ethernet switch** for around 45 seconds after power-up. This can lead to unwanted (uncontrolled) forwarding of network traffic from LAN to WAN ports and vice versa. For example, DHCP broadcast requests incoming at LAN port at this early power-up time can arrive at a possible DHCP server at WAN port resulting in DHCP offers back to LAN devices, though normally they should get an IP address from a LAN DHCP server after power-up.
    - When using bootloader version V1.5 both RJ45 ports (LAN and WAN) are blocked immediately at power-up time and will take over their intended role according to the saved configuration during the boot process.

Version 1.46 Release date: October 21, 2024

Bug Fixes:

- At power-up both Ethernet Ports (LAN and WAN) did behave like an unmanaged switch for about 45 seconds until the Ethernet switching IC has been configured as intended by the kernel settings. During this time window it could happen that broadcast packets unintendedly have been forwarded through the Ethernet ports resulting e.g. in an unwanted DHCP request/offer communication between devices connected to LAN and WAN side. This initial “unconfigured” state of the Ethernet switching IC now has been shortened to a maximum of 12 seconds after power-up.

Version 1.45 Release Date: June 12, 2024

Note: Regarding comparable features and bugfix status this firmware V1.45 corresponds to version V1.58 of router models with integrated cellular modem (IE-SR-2TX-WL-4G-EU / Article No. 2682560000 and IE-SR-2TX-WL-4G-US-V / Article No. 2682580000).

Feature Enhancements / Updates:

- Menu Network Services --> Date & Time / NTP: Parameter “Synchronise” in section "NTP time synchronization" has been removed. This parameter was used to set the synchronization interval of the Real-time clock with the Router's "System Time". This “internal” behaviour now is set to 60 minutes.

Bug Fixes:

- Internal Supercap-buffered Real-time clock now will be synchronised by the Router’s “System Time” each time when the “System Time”’ will be changed, either by manual setting (Menu ‘Network Services --> Date & Time / NTP’) or by periodic update via NTP request. This keeps the Router’s “System Time” up-to-date after power-up, unless the Router is not powered-off for longer than around 7 days. Then the RTC needs to be re-charged at next Router power-on. If this duration will be exceeded, means the storage energy of the supercapacitor is used up, then the Router’s “System Time” will be set at next power-up by the initial RTC time 'Sat Jan 1 2022 00:00:00 (UTC)'.

  The previous behaviour was, that the RTC only has been set by the “System Time” after a reboot (Warm start). This could lead to a wrong value of the Router’s “System Time” when taken over from RTC at power-up and no NTP service was configured or not accessible.

Version 1.43 Release Date: April 17, 2024

Note: Regarding comparable features and bugfix status this firmware V1.43 corresponds to version V1.57 of router models with integrated cellular modem (IE-SR-2TX-WL-4G-EU / Article No. 2682560000 and IE-SR-2TX-WL-4G-US-V / Article No. 2682580000).

Feature Enhancements / Updates:

- Menu Event Settings → E-Mail: Parameter ‘Secure Mode’ for SMTP server settings extended by additional selection value ‘STARTTLS’.
- Menu Event Settings → E-Mail: Implementation of function ‘Send Testmail’ to send a pre-defined test mail based on the configured mail server settings to evaluate if properly configured.

Bug Fixes:

- When restoring the configuration from a backup file (created with another router of the same type) the MAC addresses (LAN and WAN port, not WLAN) of the target router were overwritten with the MAC addresses of the router from which the backup file was created. If this happened, original MAC addresses could be restored by doing a reset to factory default settings.
- Serial interface configuration: Only 7 data bits could be set (instead of 7 or 8 data bits).
- Possible loss of general WLAN function after direct change from operation mode ‘Wireless Client’ to ‘Access Point’ (instead of disabling WLAN first, then enabling WLAN again and selecting Access Point’). Resulting, menu ‘System Overview’ did not show any SSID, the configured SSID was not visible by WLAN clients and in system log has shown that the WLAN interface was not found. A reset to factory settings was necessary to get the WLAN interface working again.
- If WAN / Internet Connection was set to ‘Wireless Client’ then not all active routes were pushed to the u-link Portal.

- Menu Firewall Settings → IP Filter (Local Access): Setting value 'Accept' of 'Default Filter policies' for 'Input LAN' and 'Input WAN' did not allow any input communication without restrictions.
- Menu Network Services → DHCP: No effect on tree menu item 'DHCP' (Expand or collapse sub menus) if 'Plus' or 'Minus' character has been clicked. It was always expanded.
- Menu System Information → System Overview: Correction of wrong status display of parameter 'DHCP Server'. Status of enabled 'DHCP Server' was shown as disabled.
- Menu System Information → System Overview: Correction of wrong status display of parameter 'Port Settings' for RJ45-Ports LAN and WAN if only the WAN port was connected. In this case both 'Port Settings' have wrongly shown status '10 half duplex'.

Version 1.35 Release date: August 15, 2023

Feature Enhancements / Updates:

- NAT Settings: Additional to OpenVPN interface type 'TUN' now Interface 'TAP' can be selected for both DNAT (Incoming Interface) and SNAT (Outgoing Interface).
- OpenVPN: When configuring a pre-defined routed connection type (Routed-Point-to-Point Connection or Routed-Multi-Client Connection) for parameter 'Interface Type' now 'TAP' can be selected additional to 'TUN' (default).
- Extension of Web menu 'System Overview' with new section 'u-link / OpenVPN' showing the status of an active VPN instance (either u-link, OpenVPN Server or OpenVPN Client).
- For WLAN password (Shared Key) the use of blank characters (space) now is allowed for both modes 'Wireless Client' and 'Access Point'.

Bug Fixes:

- If a configuration PC was connected to the Routers WAN port and the Web interface was accessed via WAN port IP and if any parameter in menu 'Interface Configuration → LAN/WAN Port' (e.g., LAN IP, Gateway or DNS entry) has been changed, then after applying the Web interface automatically was redirected to the LAN port IP.
- DNAT Settings (Forwarding): A configured 'Port Forwarding' rule using destination port 80 (www) has overruled other configured 'Port Forwarding' rules.
- IP Filter (Local Access): When configuring a rule, the entered values of parameter 'Source IP / Netmask' sometimes are not taken over correctly into the 'Active IP Filter List (Local Access)'. Resulting in showing wrong entries like 'xxx.xxx.xxx.xxx/undefined' or 'Specify'.

Version 1.34 Release date: May 10, 2023

Note: Due to the major upgrade from V1.32 to V1.34 a reset to factory default settings is recommended!

Feature enhancements / updates:

- Implementation of u-link VPN Client for use with Weidmüller u-link Remote Access Service.
  For configuration new menu item "VPN → u-link" has been added.
  Note: For the 4G models IE-SR-2TX-WL-4G-EU and IE-SR-2TX-WL-4G-US-V of this Router family the support of u-link Remote Access Service already was introduced with 4G-model-related version V1.38 and then adjusted in version V1.40 (including some u-link related bug-fixes). In terms of features and bug-fixes this version V1.34 corresponds to version V1.40 of the 4G Router models.
- Implementation of IPsec VPN configurable as Initiator (Automatic start) or Responder (Waiting). For configuration new menu item "VPN → IPsec" has been added.
- Additional Implementation of these Dynamic DNS Providers:
  - DuckDNS (duckdns.org)

  - NoIP (no ip.biz)
  - DynDNS Service (dyndnss.net)
  - GoIP (goip.de)
  - Dynu (dynu.com)
  - FreeDNS (freedns.afraid.org)
- Adapted behavior of signalizing when pressing ‘Reset’ button. Pressing and holding reset button > 1 second and < 5 seconds initiates a reboot and sets LAN IP to factory default value 192.168.1.110. This is indicated by a short beep and fast blinking of LED ‘DO’. Pressing and holding reset button > 5 seconds initiates a reboot and resets the configuration to factory default values. This is indicated by two short beeps and fast blinking of LED ‘DO’.

Bug Fixes:

- Support of blank characters added for WLAN SSID. Now allowed for both operation modes “Access Point” and “Wireless Client”.
- Fix of u-link registration status display. Previously status “Registered” already was displayed though the registration process was not yet completely done.
- Adaption of u-link registration process in case of trying to register a used activation code. Previously the registration process restarted endless when a used activation code was entered.
- WAN port did not work properly (slow data throughput) when configured as additional (second) LAN port (applicable for Internet/WAN connection via Wireless Client).

Version 1.32 — Release date: October 27, 2022

Feature enhancements / updates:

- Adaption of OpenVPN configuration page for mode ‘Configure via OpenVPN options’ (Input windows now are resizable, additional information for configuration added).

Bug Fixes:

- Configured OpenVPN settings - when entered directly as OpenVPN options - could not be stored after applying.
- OpenVPN logging level selection 10 removed (OpenVPN logging supports only up to level 9).
- Status of OpenVPN client connection to an OpenVPN server now will correctly displayed.
- The selectable behavior for an activated OpenVPN instance (either being Server or Client) now will be done correctly (for example start/stop respectively connect/disconnect automatically at boot time or triggered by digital input).
- Event mail could not be sent when having a space character in parameter ‘Sender name’.

Version 1.30 — Release date: October 18, 2022

- This is the initial firmware version!