

Firmware Change Log (new features and bug fixes) 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

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 on IE-SR-4TX* reported seemingly valid values for IE-SR-4TX* whereas this product 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 on an IE-SR-4TX*.
- 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.
- The u-link VPN could not be established due to a regression bug which was introduced in IE-SR-4TX* 1.3.1.
- 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.
- Devices using a web server certificate with RSA512 keys will experience a web server error starting with version in IE-SR-4TX* 1.3.1 firmware versions. In these cases, the web server goes completely offline (also on HTTP, port 80!). As of version 1.3.4, this is intercepted and all RSA512 certificates are automatically exchanged for the device's self-signed factory certificate.
- 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. Bug was introduced with version 1.0.0 on IE-SR-4TX*.
- 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. Bug was introduced with version 1.0.0 on IE-SR-4TX*.
- 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 got 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 due to a regression error since version 1.0.0 on IE-SR-4TX*.
- 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 since version 1.0.0 due to a regression bug.
- 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
- 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 regression bug was introduced with version 1.0.0 on IE-SR-4TX*.
- 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 through 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
- 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 were 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****Feature updates:**

-

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**