Firmware Release Notes

Advanced Line Switch

IE-SW-L3-AL20M-8GT-12GESFP (Article No. 3109750000)

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.

After updating the device at **first** commissioning (having still initial factory default settings) to the latest firmware, we strongly recommend performing a reset to factory defaults additionally after the new firmware is running.

Attention 2: Since version V1.37 the switch uses for the saved configuration (Flash) a different storing format. This requires an additional saving of the configuration immediately after firmware update to V1.37 (or newer) when the switch comes up again with new firmware after the reboot process. For user support not to forget to save again the running configuration as startup configuration, an information message appears immediately after first reboot/start-up with new firmware.

This additional required manual saving of the configuration is only necessary for upgrading switch firmware from any version **<= V1.35** to a version **>= V1.37**. For an update from versions **>= V1.37** to **any newer version** there will be no need to do this.
After updating and first reboot the system automatically checks if the current configuration needs to be saved to Flash memory again. Only in this case the message for saving will be displayed. The user information for saving the configuration appears for firmware update via Web interface as well for doing this via command line interface (CLI).

Version 1.37	Release Date: November 27, 2025

Feature Enhancements / Updates:

- Adaption of internal storage format of running and startup configuration (Flash Memory). This requires an additional saving of the configuration immediately after firmware update from a version <= V1.35 to version V1.37. An information message is displayed as a hint for the user when the switch comes up again with new firmware after the reboot process. The note will be displayed for both procedures of firmware update, via Web interface as well as for the command line interface (CLI).
  - *Note Web GUI: The internal format for saving the configuration data has been changed with this firmware update and requires the running configuration to be saved as startup configuration again. To avoid losing the current configuration, go to webpage "Save/Manage Configuration" and press button "Save as Startup Configuration".*
  - *Note CLI: Attention: The internal format for saving the configuration data has been changed with this firmware update and requires the running configuration to be saved as startup configuration again. To avoid losing the current configuration, apply command 'copy running-config startup-config' now.*
- Improvement of the command line interface (CLI):
  - Support of RADIUS and TACACS+ options 'unencrypted' and 'encrypted' for parameter 'key'. The commands have been adapted as below described:
    - radius-server key { [unencrypted] <unencrypted_key> | encrypted <encrypted_key> }
    - tacacs-server key { [unencrypted] <unencrypted_key> | encrypted <encrypted_key> }
    - radius-server host <host_name> [auth-port <auth_port>] [acct-port <acct_port>] [timeout <seconds>] [retransmit <retries>] [key { [unencrypted] <unencrypted_key> | encrypted <encrypted_key> }]
    - tacacs-server host <host_name> [port <port>] [timeout <seconds>] [key { [unencrypted]
    - <unencrypted_key> | encrypted <encrypted_key> }]
    Note: <Unencrypted_key> is a readable plain text. <Encrypted_key> is the encrypted hash-code of readable plain-text. The hash-code can be seen in the configuration backup file (e.g. created via Web interface) if RADIUS respectively TACACS+ have been configured.
  - New command 'configuration paste' implemented to be used for pasting a complete configuration command sequence as one step.
    - Short information about the procedure: Copy the text-based content of a backup file, establish a CLI session, and enter command 'configuration paste'. Then paste the copied data into the command line.
  - When using a SSH connection via PuTTY now the backspace key works out of the box. Previously for deleting a character the key sequence 'Strg + H' must be entered.

- Improvement SNMP related features:
  - Menu 'SNMP → Trap → Section Events': Implementation of new SNMP trap events on configuration changes.
  - Support of new private OIDs to query CPU and memory status via section 'switchInfoTable'.
    - Note: Needs downloadable device specific private MIB file dated from 2025-11-26 or later.
  - Support of OID 1.3.6.1.2.1.2.2 (Standard MIB-2 → Section 'interfaces' → ifTable → ifAdminStatus) allowing port disabling and enabling.
  - Support of OID 1.3.6.1.2.1.3.1 (Standard MIB-2 → Section 'at' → atTable) allowing to retrieve the address translation table.
  - Adaption of OID 1.3.6.1.2.1.17.1.4.1.2.1 (Standard MIB-2 → Section dot1dBridge' → dot1dBase → dot1dBasePortTable → dot1dBasePortIfindex) which now shows the retrieved port numbers beginning from number 1. Previously the numbering of the port interface index has started from 1000001, 1000002, 1000003, etc.

Bug Fixes:

- Weidmüller Gigabit SFP transceiver IE-SFP-1GE-RJ45 (Article No.2766120000) could not establish a link to Fast Ethernet devices being only capable to run at 100 Mbit/s.

- Adaptions related to RADIUS and TACACS+ configuration:
  - When upgrading from firmware **V1.31 or previous version** to **V1.33 or V1.35** the RADIUS and TACACS+ configuration settings were deleted. This was caused by changing the storing mechanism of RADIUS and TACACS+ server keys. Due to security requirements the server keys have been stored since version V1.33 as encrypted hash-code while in the older versions the keys were stored as readable plain-text both in the flash memory and in the backup file.
  - An upgrade from firmware **V1.31 or previous version** to **V1.37 or a newer version** no longer causes any problem, the configured RADIUS and TACACS+ settings are adopted correctly. During update process the RADIUS/TACACS+ keys stored as readable plain-text are converted to encrypted hash-code.
  - **Attention:** Due to change of key storing above described an upgrade from firmware **V1.33 or V1.35** to **V1.37 or a newer version** still causes the problem, that configured RADIUS and TACACS+ key settings are interpreted wrongly.
    - The reason is that for V1.33/1.35-based startup configurations the keys already are stored as encrypted hash-code but are not saved with key option 'Encrypted'. However, V1.37 or a newer version expects - when upgrading – either key option 'Encrypted' or 'Unencrypted' to interpret a stored key correctly. If no key option is found, then the key will be handled as plain text. Resulting, at update process the encrypted hash-code in the startup configuration will be encrypted again and stored as supposedly encrypted plain text. This can be recognized, that after update on Web pages 'RADIUS Server Configuration' and 'TACACS Server Configuration' the de-crypted key of the twice encrypted hash-code will be shown (which is the original hash-code before it was encrypted again).
  - Resulting, after update from firmware **V1.33 or V1.35** to **V1.37 or a newer version** the RADIUS/TACACS+ server keys are corrupted and must be re-entered manually.

Version 1.35	Release Date: June 30, 2025

Feature Enhancements / Updates:

- Adaption of 'Profinet' protocol stack to pass the Profinet conformance test according to version V2.45.
- Private SNMP command 'switchProfinetMgt' implemented for enabling/disabling industrial protocol 'Profinet'.
  - Note: Needs downloadable device specific private MIB file dated from 2025-06-11 or later.
- Information about flash memory size added on webpage 'System Information'.

Bug Fixes:

- After configuration restore via backup file the switch started correctly with imported configuration, but after power down and up again the device has lost the configuration and came up with factory defaults. This issue was introduced in firmware version V1.33.
- Field 'System Name' could not start with a numeric value, although allowed according to input definition.
- Command Line Interface (CLI): Using command 'Show spanning-tree' could cause an unintended device reboot.

- Webpage 'Warning/Events → Event Selection': Switch has done an unintended automatic reboot if checkbox 'Configuration Changed and Saved' for SNMP has been enabled and applied.

Version 1.33	**Release Date: March 27, 2025**

- This is the initial firmware version for market launch!