Firmware Release Notes

Advanced Line Switch

IE-SW-AL12M-8GT-4GESFP (Article No. 2682340000)

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**

Feature Enhancements / Updates:

- Default user 'admin' (with full administration rights) now can be deleted in favor of any new defined user being the device administrator.
- For Web-based configuration of redundancy protocol MRP (Media redundancy protocol) the role 'MRP Manager' has been implemented additional to role 'MRP Client'.
- For Profinet-related configuration of redundancy protocol MRP via TIA Portal the role 'MRP Manager' has been implemented additional to role 'MRP Client'.
  - Note: For selecting role 'MRP Manager' you need to update your project (TIA Portal) with downloadable file *GSDML-V2.43-Weidmueller-IE-SW-ALM-series-20250212*.xml or newer one.
- Device serial number now can be requested via new SNMP OID 'swSerialNo'.
  - Note: Needs downloadable device specific private MIB file dated from 2025-01-27 or later.
- Improvement of firmware upgrade via command line interface (CLI):
  - When using command *firmware upgrade <tftp://<IP TFTP server>/<firmware filename>* now additional messages are displayed in terms of progress and status of the firmware update process.
  - Additionally, new option *no-reboot* has been implemented for firmware upgrade command *<tftp://<IP TFTP server>/<firmware filename> no-reboot*. This option prevents an automatic reboot after completion of the upgrade process and using the upgraded firmware. When used, the new firmware needs to be activated either by next power down/up, via external reset button, via Web interface reboot or by rebooting via a CLI command (*reload cold*).
- Firmware upgrade via Web interface:
  - New option *'Do not reboot after upgrade process has been completed'* has been implemented. If activated, after successful upload/upgrade the device needs to be rebooted manually (e.g. via Web interface) or powered down/up (Cold start) that new firmware will become active.
- Command line interface (CLI): New command *Show startup-config* has been added.
- Enhancement of security settings of RADIUS / TACACS+ server configuration:
  - Keys/Passwords no longer will be displayed as readable content. To read the entry a button must be pressed.
  - Additionally, due to security reasons the used keys/passwords now will be stored in the backup file as an encrypted hash code.
    Important note about following incompatibility behavior between firmware versions <= V1.31 and >= V1.33 when restoring the configuration by importing a backup file:
    Scenario 1: Backup file was created with firmware versions <= V1.31 and will be used for configuration restore on a switch running a firmware version >= V1.33.
    - Switch recognizes the readable keys/passwords as not encrypted (no hash code) and ignores the RADIUS/TACACS related commands. Resulting, the file-based configuration restore succeeds, except that RADIUS/TACACS Server configuration could not be imported. This needs to be done manually after configuration restore.
    Scenario 2: Backup file was created with firmware versions >= V1.33 and will be used for configuration restore on a switch running a firmware version <= V1.31
    - Switch interprets the hash code of keys/passwords as direct useable key/password and the RADIUS/TACACS related commands will be conducted without any failure. Resulting, the file-based configuration restore succeeds, but the RADIUS/TACACS Server configuration does have set the hash codes as wrong keys/passwords for authentication. This needs to be corrected manually in the Web interface after configuration restore.
    Note: Detailed information about different storing of keys for RADIUS / TACACS server configuration (clear text versus hash code) since V1.33 is also contained in the help text of menu 'Backup & Restore' of the Web interface.

Bug Fixes:

- When activating SNMPv3 a memory overflow could happen caused by unintentional use of too much memory. This could lead to a functional freeze of the device. Now a SNMP agent related size check prevents a memory overflow.
- When an O-Ring redundancy was <u>configured, applied and saved</u> using 'Port 2' as **1ˢᵗ** ring port, and as **2ⁿᵈ** ring port any other port except 'Port 1' then <u>after reboot</u> 'Port 1' automatically was set as **1ˢᵗ** ring port instead of configured 'Port 2'. This issue happened only for this constellation, means 'Port 2' was configured as 1ˢᵗ ring port and any other port except 'Port 1' was configured as 2ⁿᵈ ring port.
- Fix of wrong O-Ring status display shown at O-Ring master switch when any connection of the ring cabling was wrongly connected to a port of an O-Ring slave switch not configured as O-Ring port.
- When configuring an O-Ring redundancy and activating additionally a 'Dual-Homing-port' for redundant connection of the O-Ring to a RSTP network then in some cases only default 'Dual-Homing-port' 4 could be used (other ports could not be selected).
- Fix of the issue that some specific passwords could not be taken over (applied) though only allowed characters has been entered.
- When performing a factory reset, the currently set admin password always reverts to the default one, even if the user intends to keep the current password.
- Fix of industrial protocol EtherNet/IP issues:
  - Switch could not be loaded as EIP device in Rockwell's engineering tool Studio 5000 V33 (or newer) when using EDS file with modification date 2021-08-12.
    → *Use downloadable adapted EDS file with modification date 2025-02-07.*
  - Since firmware version(s) > V.1.31 additional port settings ('Enable/Disable', 'Autonegotiate', 'Speed' and 'Duplex Mode') can be configured with Rockwell's engineering tool Studio 5000.

Version 1.31	Release Date: August 15, 2024

Feature Enhancements / Updates:

- Enhancement of security level for HTTPS and SSH based device access.
  - Cipher suites considered as weak have been removed and some new recommended TLS 1.2 cipher suites have been added.
  - Size of RSA encryption key (Certificate) has been enlarged from 1024 to 2048 bits.
    Important note: The enlarged RSA encryption key only becomes effective if the device will be reset to factory defaults followed by a manually initiated reboot or power-down/up. If after update no reset to factory defaults will be done, the key length of 1024 bits will continue to be used. The cipher suites adaption is independent from factory default settings and becomes immediately effective after firmware update.
- Menu 'System Information': Recommendation note added to disable industrial protocol Profinet (default active) if the switch is not used as Profinet IO device (e.g. configured in TIA Portal). Disabling is recommended to deactivate Profinet-related traffic-shaping rules to avoid any impact on traffic when used in non-Profinet applications.
- Menu 'Warning/Event Settings → Syslog Setting': Parameter 'Server UDP Port' (Default 514) added for variable port selection when sending log messages to a remote Syslog server.
- SNMP: Generation of Device Engine ID for SNMPv3 has been changed from 'IPv4 Address format scheme' to 'MAC Address format scheme'. This ensures a unique SNMP Engine ID for each device in contrast to the previous behavior, where always the same Engine ID were generated for all devices due to the 'IPv4 Address format scheme' based on factory default IP 192.168.1.110.

Bug Fixes:

- SNMP request for power input status did not work properly. The issue was that only the information of power input 1 could be retrieved.

- Menu 'VLAN Membership Configuration': Content of parameter 'Allowed Access VLAN' could be overwritten unintendedly by content of parameter 'Management VLAN ID' after restoring a saved configuration via file restore. This issue only could occur for a value of 'Management VLAN ID' unequal 1 and if - after import and following reboot - the device had no link connection at any port for at least 40 seconds after power-up.

Version 1.29   **Release Date: October 17, 2023**

Bug Fixes:

- A configured and saved 'Dual Homing' redundancy (additional function to O-Ring redundancy) automatically was disabled after reboot or power-up. As result a loop could raise to the redundant connected RSTP network (via the 'Dual Homing' function).

Version 1.28   **Release Date: September 26, 2023**

Feature Enhancements / Updates:

- O-Ring redundancy: Previously hidden O-Ring parameters 'Hello Time' and 'Max. Age Count' now can be configured, same as already configurable for managed Weidmüller Advanced-Line Fast Ethernet switches.
- Use of 2 independent device identifiers 'System Name' and 'PROFINET Device Name'. The 'System Name' will be configured via the web interface for device identification, while the 'PROFINET Device Name' will be configured exclusively via the PROFINET engineering software (e.g., TIA Portal). Parameter 'PROFINET Device Name' is only displayed if industrial protocol PROFINET is enabled.
- SNMP: Parameters of section 'dot1dStp' as part of standard MIB file 'Bridge.mib' now can be used.
- VLAN membership configuration: Additional column added showing the port description which normally is set in menu "Port Configuration". The port-related description can be edited in both menus 'VLAN Membership Configuration' and 'Port Configuration'.
- Password management: An inserted password now can be displayed as readable text or with encrypted characters.
- External Backup and Restore Module: The factory default settings of both parameters 'Backup via EBR Module' and 'Restore via EBR Module' have been changed to enabled. Now a replacement of a defective switch can be done with a new switch having factory default settings by using an EBR module with a backup configuration. There is no need for an initial Web interface configuration of the replacement switch.
- New tree menu item 'Logout' has been added for explicit logoff from the web interface.

Bug Fixes:

- SNTP: 'System Date/Time' no longer has been be updated for activated SNTP modes 'Client' or 'Server' when in the meantime 'System Date/Time' has been updated manually (via corresponding Apply button). Now manual update is no longer possible as long any of the SNTP modes ('Client' or 'Server') is activated (Manual update of 'System Date/Time' is locked).
- The hash code of a configured password with length > 20 characters was not saved correctly in the startup configuration (Flash memory). As result after reboot or power-up a login using such a password was no longer possible.

Version 1.26   **Release date: July 03, 2023**

Feature Enhancements / Updates:

- DNS support added. For example, hostnames now can be used for addressing an NTP time server.
- Extension of settings for 'Daylight Saving Time'. Now recurring and non-recurring 'Daylight Saving Time' can be selected.

- SNTP mode 'Server' now supports to get date and time from a remote (S)NTP server if any time server IP or hostname is configured.
- Relocation of tree menu item 'MAC Table' from section 'Monitoring and Diagnostics' to section 'Security'. Reason: Sub menu 'MAC Address Table Configuration' mainly is used for configuration of MAC-based port access which is a security topic.

Bug Fixes:

- Update of fix in terms of **unintended device reboot** respectively **short-time port link down (for about 20 seconds)** after several weeks of uninterrupted operation time. This was caused by RAM memory overflow due to a programming failure in terms of not releasing discarded memory. Note: This error only appeared for PROFINET-enabled applications.
- Fix regarding port based LLDP settings which have not been taken over after reboot, though the configuration previously was saved as 'Startup' configuration. Note: Disabling port related LLDP only is possible if industrial protocol PROFINET is disabled.
- Fixed issue that HTTPS-based Web interface access no longer was possible after update to firmware version V1.25, though access configuration was set to 'HTTP/HTTPS. This issue was introduced in version V1.25.

Version 1.25	Release date: May 08, 2023

Feature Enhancements / Updates:

- New private SNMP parameters in terms of fault relay alarms have been implemented. Use private MIB file IE-SW-AL12M-8GT-4GESFP_v125_2023-05-17.mib for use of these parameters (Refer to section 'faultAlarm').
- Web menu adaption: Configuration of "Management VLAN ID" moved from menu "Basic Settings → IP Configuration" to menu "VLAN → VLAN Membership".
- Adaption of "Access Control List" settings. Due to default enabled industrial protocol 'PROFINET' the ACL contained 12 exclusively to PROFINET related default filter rules which could not be deleted. Now the ACL is empty by factory default and explicitly useable for user-specific filter rules. The PROFINET related filter functions have been separated from the ACL and are only active if industrial protocol PROFINET is enabled. If enabled. the PROFINET filter functions run first before user-specific configured ACL rules will be applied.

Bug Fixes:

- Fix of **unintended device reboot** respectively **short port link down (for about 20 seconds)** after several operation days. This was caused by a stack overflow which could occur in special circumstances.
- After change of the device IP address and applying the configuration change was not signalized. Now for any IP address related adaption the blue-colored hint message (Running configuration changed but not saved as startup configuration!) will be shown.
- Menu "Basic Settings → IP configuration": When setting parameter "DHCPv4" via drop-down box to "Enabled" then after applying the selection unintendedly changed back to value "Disabled".
- Redundancy protocol O-Ring failed, if VLAN IDs for the trunk ports (used as ring ports) have been configured different than '1'. Now any VLAN ID may be used.
- Fix of bug when restoring a saved file configuration to both the "Running configuration" and the "Startup configuration". The failure was that only parts of the loaded configuration file have been restored to the Startup configuration.
- Proper recognition and behavior of plugged-in RJ45 SFP transceiver modules. Previous versions showed wrong SFP type (Fiber SFP) and did not signalize a port link down when the RJ45 cable was removed.

Weidmüller ϡϾ

Version 1.23 — Release date: December 05, 2022

Feature Enhancements / Updates:

- Hint texts regarding dependencies to be considered when configuring a ring redundancy protocol (O-Ring, O-Chain, MSTP/RSTP, Fast Recovery or MRP) have been updated.

Bug Fixes:

- In certain constellations Ports 1 and 2 could block some Ethernet traffic, resulting in discarding Ethernet packets. This bug was introduced in Version1.20.
- Wrong status data of inserted RJ45 SFP transceivers have been displayed. Now only DDM-capable SFP transceivers show status data when plugged in.

Version 1.22 — Release date: November 10, 2022

Feature Enhancements / Updates:

- Support for upcoming RJ45-SFPs implemented for models having SFP slots.

Version 1.20 — Release date: August 29, 2022

Feature Enhancements / Updates:

- Implementation of MRP redundancy configuration via Web interface and now applicable independent of the industrial protocol PROFINET. In previous version - if protocol PROFINET was enabled - MRP only could be managed and activated via a PROFINET engineering tool (like TIA Portal). Only role MRC (Client) is supported.
- Declaration for used Open Source Software added (GNU General Public License). New menu item "License Information" added.

Version 1.19 — Release date: July 01, 2022

Feature Enhancements / Updates:

- Passed test specifications according to PROFINET version 2.42.
- Improvement of Web interface appearance.
- Extended information in the Help-Webpages for menus VLAN and Redundancy (O-Ring, Ring Coupling, Dual Homing and O-Chain).
- Provision of new SNMP parameters for checking status data of O-Ring and O-Chain redundancy.
  Note: For new SNMP parameters use private MIB file IE-SW-AL12M-8GT-4GESFP_v119_2022-07-01.mib (or a newer version with higher firmware version number).

Bug Fixes:

- PROFINET: Fix of issue for Netload test (Occasionally some connection interrupts could occur when requesting diagnostic data).
- Device description parameters could not be configured after PROFINET has been disabled.
- Adaption of Modbus Register table (Vendor name and device model name now will be retrieved correctly).

Version 1.16 — Release date: March 28, 2022

Feature Enhancements / Updates:

- External Reset button: Extended settings of reset button behavior configurable via Web Interface (only Warm start, Keep IP, Reset Startup Configuration to Factory Defaults, etc.).

- External Backup/Restore Module: Additional restore settings configurable via Web Interface (Replace Running and/or Startup Configuration).
- Security check that model-specific firmware only can be installed on the associated model.
- Activation of function 'Automatic Link Speed Downshift' which is useful for operation in cabling environments that are incompatible with 1000BASE-T with the result of no link establishment. This happens when e.g. 4-wire Ethernet PROFINET cables are used as a link between 2 1000BASE-T ports working in auto-negotiation mode.
  For link recognition between 2 1000BASE-T ports in mode auto-negotiation, the switch automatically changes its 1000BASE-T auto-negotiation advertisement to the next slower speed (100Base-TX) after a set number of failed attempts at 1000BASE-T.

Bug Fixes:

- If O-Ring redundancy was configured and running, Master switch could hang-up and stops communication if Web Interface was opened and used intensively.
- A defined and applied gateway setting has not taken over after saving to flash memory and reboot.
- When reading Modbus registers wrong values of registers "Vendor number", "Vendor name" and "Model name" has been retrieved.

Version 1.11	Release date: January 21, 2022

Feature Enhancements / Updates:

- Implementation of PROFINET protocol stack (Conformance Class B).
- Implementation of Media Redundancy Protocol (MRP) configurable via PROFINET engineering tool.
- Industrial protocol stack EtherNet/IP now can be used again (Was disabled in version V1.10 due to security vulnerability described under section bug fixes).
- SFP transceiver monitoring added for models having ports with SFP slots.

Bug Fixes:

- Elimination of security vulnerability CVE-2020-25159. EtherNet/IP adaptor source code (ENIP / 499ES) was vulnerable to a stack-based buffer overflow, which could allow an attack by sending a specially crafted packet resulting in a denial-of-service condition or code execution.

Version 1.10	Release date: November 04, 2021

- This is the initial firmware version!