

Switch Series

Full Gigabit Advanced- and Substation-Line



Information about major firmware upgrade from any version 1.3x to cybersecurity version 2.xx compliant to IEC 62443-4-2

This document refers to following Full Gigabit managed switch models:

Article name	Article number	Article name	Article number	Article name	Article number
IE-SW-AL08M-8GT	2682350000	IE-SW-AL06M-4GTPoE-2GESFP	2682430000	IE-SW-L3-SL28M-HV	2875580000
IE-SW-AL12M-8GT-4GESFP	2682340000	IE-SW-AL08M-8GTPoE	2682420000	IE-SW-L3-SL28M-LV	2875590000
IE-SW-AL14M-12GT-2GESFP	2682360000	IE-SW-AL12M-8GTPoE-4GESFP-120W	3109760000	IE-SW-SL20M-8GT-12GESFP-HV	2778970000
IE-SW-AL24M-16GT-8GESFP	2682370000	IE-SW-AL12M-8GTPoE-4GESFP-240W	3109770000	IE-SW-SL20M-8GT-12GESFP-LV	2778980000
IE-SW-L3-AL20M-8GT-12GESFP	3109750000	IE-SW-AL26M-22GTPoE-2GCPOE-2GESFP	3109780000	IE-SW-SL26M-24TX-2GC-HV	2778990000
				IE-SW-SL26M-24TX-2GC-LV	2779000000
				IE-SW-SL28M-HV	2779010000
				IE-SW-SL28M-LV	2779020000

1. General information about the major upgrade:

Firmware version 2.02 meets the cybersecurity requirements according to IEC 62443-4-2 SL1 providing below listed additional security features compared to previous non-cybersecure versions 1.3x:

- No predefined (factory-default) password.
 - At first login (at factory defaults) a new administrator password needs to be set.
- Configurable password policy.
- Role-based user and group management.
- Temporary account lockout following failed password login attempts.
 - Access blocking for 30 minutes after 5 failing login attempts within 5 minutes.
- Provision of audit logging in terms of recording of system activities and user actions to ensure accountability, safety, and regulatory compliance.
- New dedicated flash storage for audit logs.
 - Log content will remain after power-down/up.
- Automatic logout for inactive sessions.
- Session-based web interface authentication and concurrent login control.
- Configurable pre-login security banner support.
 - Intended for the advance display of warnings regarding misuse of the device.
- Password change reminder mechanism.
 - Displays a user message to change the password after three months (Works only if NTP time synchronization is activated).
- Enabled HTTPS, SSH, and LLDP by default while disabling non-essential services like SNMP.
- SHA-256 integrity validation for security-related data.
- SHA-256 integrity protection for the bootloader and critical data partitions.

2. Notes regarding the upgrade process:

- 2.1 Start the upgrade process as usual via webpage "Basic Settings → Upgrade Firmware" by selecting device specific firmware file V2.02 and clicking the "Upgrade" button.
- 2.2 The upgrade process takes approximately 5 minutes, normally followed by an automatic device restart (user selectable).
- 2.3 After reboot message "Corrupt data link" appears in the web interface. This is a correct message due to new security feature "Session-based web interface authentication and concurrent login control". Close this browser tab and open a new session.
- 2.4 If the switch is in its factory default state or still uses the factory default password "Detmold," a new password for the "admin" user must be entered after accessing the web interface, in accordance with the default password policy.
If an already configured switch is updated and the currently set password is not the factory default password "Detmold" (for versions 1.xx), the existing password is retained, even if it does not comply with the default password policy.

- 2.5 Following the initial successful login, the storage area for the permanent system log (audit data) must be initialized once. Depending on the switch's storage capacity, this process takes between 1 and 5 minutes. Once initialization is complete, the "System Information" landing page appears.
- 2.6 The upgrade process is now complete, and the device is ready for operation again.

3. Additional important considerations:

3.1 What to consider regarding a firmware downgrade from any cybersecure firmware version ($\geq V2.xx$) to a firmware version non-compliant with IEC62443 cybersecurity requirements ($\leq V1.xx$):

1. Generally, after downgrade, from any version $\geq 2.xx$ to a version $\leq 1.xx$ without preparatory measures it is no longer possible to login into the switch. This is caused by a different user information storage format inside in the startup configuration which cannot be interpreted by a non-secure firmware version. As result, the switch needs to be reset to factory defaults via the external reset button (pressing > 5 secs) and the previous configuration before downgrade is lost. As next step the switch either needs to be configured again manually, or you can restore a configuration via import of a backup file created with a non-secure firmware version 1.xx.
2. Alternatively, and to avoid a factory reset, you need - before doing the downgrade - to restore a configuration as 'Startup Configuration' by using a backup file created with a non-secure firmware version 1.xx. Then, after downgrading to any version 1.xx version and reboot, the switch is able to read the startup configuration and comes-up according to the backup file settings. When doing this, consider the information on webpage 'Backup & Restore', how to restore a backup file created with a non-secure firmware version 1.xx.

In terms of a downgrade related to this topic 2 the procedure is as follows:

- a. Go to webpage 'Backup & Restore'
- b. In section 'Restore Configuration' select the backup file created with a non-secure firmware version 1.xx for restoring.
- c. Enable checkbox 'Replace Startup Configuration'.
- d. Enable checkbox 'Selected backup file was created with an earlier firmware version $\leq 1.xx$ non-compliant with IEC62443 cybersecurity requirements'.
- e. Press button 'Import Configuration'.
- f. Next following message will be displayed: *'Loaded Configuration has been stored as Startup Configuration successfully.'*
- g. Now change to webpage 'Firmware Upgrade' and perform the firmware upgrade process by using a firmware version 1.xx for downgrading. Keep in mind that checkbox 'Selected firmware is non-compliant with IEC62443 cybersecurity requirements.' needs to be enabled.

3.2 What to consider when running a cybersecure firmware version 2.xx and you will restore a configuration using a backup file created with a previous non-cybersecure version 1.xx:

Since the major upgrade to a cybersecure firmware version 2.xx being compliant with IEC62443 cybersecurity requirements, the format of the backup file has been changed in terms of storing the configuration commands of the user management. When restoring an 'old' backup file created with a non-cybersecure firmware version 1.xx to a switch, having installed any cybersecure firmware version $\geq 2.xx$ following aspects need to be considered:

1. An 'old' backup file does not have the matching entries for the user management implemented with cybersecure firmware versions. For this reason, after import and activation (import as startup configuration and doing a reboot), the switch immediately requires setting a new 'admin' password. All other configuration settings of the 'old' backup file will be taken over as intended.
2. After entering the new 'admin' password, this running configuration will be saved automatically as new startup-up configuration containing the new 'admin' password.

Procedure when using an 'old' backup file (created with firmware version 1.xx):

1. Select a backup file for restoring via button 'Select File'.
2. Enable checkbox 'Replace Startup Configuration'.
3. Enable checkbox 'Selected backup file was created with an earlier firmware version ($\leq V1.xx$) non-compliant with IEC62443 cybersecurity requirements'.
 ➤ This disables the SHA256 file integrity check of 'old' backup files not created with any cybersecure firmware version.
4. Press button 'Import Configuration'.
5. Next message 'Loaded Configuration has been stored as Startup Configuration successfully.' appears.
6. After pressing button 'Okay' the switch reboots and comes back requesting the setting of a new 'admin' password according to cybersecure requirements.

3.3 Note regarding the integration of the switch into the Weidmüller network management software 'u-netops':

If the switch is not detected during device discovery in **u-netops** after a firmware update from version 1.3x to version 2.xx (using an existing configuration), a further restart must be performed to initialize the u-netops communication protocol.