Security Datasheet

Full Gigabit Switches Advanced Line series
Full Gigabit Switches Substation Line series

Firmware 2.02 or higher

Weidmüller Interface GmbH & Co. KG
Klingenbergstraße 26
D-32758 Detmold
Germany
Fon: +49 5231 14-0
Fax: +49 5231 14-292083
www.weidmueller.com



Advanced Line series



Substation Line series

Full Gigabit Switches Advanced Line and Substation Line series

This Security Data Sheet provides you with a condensed overview of the security functions of the devices. It is an addition to the following documents:

- Hardware Installation Guide
- User manual
- Industrial Product Security Guideline

Security intended use:

The devices are intended for the realization of managed Ethernet communication networks within industrial automation and substation automation environments. They shall be installed in a restricted-access location, for example a locked control cabinet, and shall not be connected directly to the public Internet.

To protect equipment, systems, machines and networks against cyber threats, the asset owner shall implement and maintain a complete, risk-based and state-of-the-art industrial cybersecurity concept. The asset owner is responsible for preventing unauthorized access to equipment, systems, machines and networks. Connections to enterprise networks, DMZ segments, remote-service networks or the Internet shall only be established where necessary and shall be protected by dedicated security

devices, for example industrial firewalls and VPN gateways, with appropriate filtering, monitoring and logging.

In architectures aligned with IEC 62443 and the Purdue reference model, the devices are intended primarily for use inside Level 1 or Level 2 application zones. The devices segment and interconnect automation components within controlled industrial or substation networks.

Most models operate as managed Layer 2 switches. The IE-SW-L3-AL20M-8GT-12GESFP and IE-SW-L3-SL28M-HV/LV additionally provide Layer 3 functions. These routing functions do not replace a dedicated zone-boundary firewall. The switches are not intended to be the sole boundary-protection component towards higher-level networks or the public Internet.

Supported SubstationLine models additionally provide substation-specific communication functions such as MMS. Such application protocols shall only be enabled where required and shall be restricted to the intended network zone and authorized communication partners.

Products covered by this data sheet

AdvancedLine:

IE-SW-AL06M-4GTPoE-2GESFP (2682430000)

IE-SW-AL08M-8GT (2682350000)

IE-SW-AL08M-8GTPoE (2682420000)

IE-SW-AL12M-8GT-4GESFP (2682340000)

IE-SW-AL12M-8GTPOE-4GESFP-120W (3109760000)

IE-SW-AL12M-8GTPOE-4GESFP-240W (3109770000)

IE-SW-AL14M-12GT-2GESFP (2682360000)

IE-SW-AL24M-16GT-8GESFP (2682370000)

IE-SW-AL26M-22GTPOE-2GCPOE-2GESFP (3109780000)

IE-SW-L3-AL20M-8GT-12GESFP (3109750000)

SubstationLine:

IE-SW-SL20M-8GT-12GESFP-HV/LV (HV: 2778970000 / LV: 2778980000)

IE-SW-SL26M-24TX-2GC-HV/LV (HV: 2778990000 / LV: 2779000000)

IE-SW-SL28M-HV/LV (HV: 2779010000 / LV: 2779020000)

IE-SW-L3-SL28M-HV/LV (HV: 2875580000 / LV: 2875590000)

Weidmüller PSIRT (Product Security Response Team)

Comment	Link
Weidmueller has established a PSIRT and provides information on product-specific security vulnerabilities and their elimination on the Weidmüller website "Security Advisory Board“	https://support.weidmueller.com/support-center/popular-resources/security-advisory-board
Weidmueller publishes security vulnerabilities of its products at VDE @CERT.	https://cert.vde.com/en/
Weidmueller offers a detailed **Industrial Product Security Guideline.** This document provides guidance on building a robust cybersecurity system and integrating Weidmüller components into that system.	Industrial security

Weidmüller security activities

The Full Gigabit Switches AdvancedLine and SubstationLine series listed in this Security Data Sheet provide the cybersecurity feature set introduced with firmware 2.02. This feature set is compliant with the component requirements of IEC 62443-4-2 at Security Level 1. The individual component capabilities and the available functions supporting additional SL-C requirements are shown in the IEC 62443-4-2 mapping chapter of this document.

Weidmüller offers "Secure by Design" products in accordance with IEC62443-4-2. If required, please contact our sales staff.

How to find product information

Device type	**Physical/optic:** Type plate on device, Label on packaging **Web interface:** „Device Name“ on device homepage **Command Line Interface:** „show version“ -> „System Name“ **SNMP:** „sysName“ (mib-2.system) **Fieldbus:** „Product Name“ via Modbus/TCP, PROFINET, EtherNet/IP and for SubstationLine series MMS **u-netops:** Device discovery and identification in the switched network
Software version	**Web interface:** „Software Version“ on device homepage **Command Line Interface:** „show version“ -> „Software Version“ **SNMP:** „swFwVer.1“ (private mib) **u-netops:** Device and firmware information
Hardware version	**Physical/optic:** Type plate on device, Label on packaging

MAC address	**Physical/optic:** Type plate on device, Label on packaging **Web interface:** „MAC Address“ in menu „System Information“ **Command Line Interface:** „show version“ command
Serial number	**Physical/optic:** Type plate on device, Label on packaging **Web interface:** „Serial Number“ in menu „System Information“

Technical information

Interfaces

Type	No	Default	Can be changed	Comment
Ethernet	Device type dependent	Active	Yes	Disable unused ports
Console	1	Active	Yes	In Basic Settings > Access Management > Authentication Methods, select the Console login method. Where available, no prevents console login. Restrict physical access and retain an authorized recovery path.
Reset button	1	Active	Yes	Factory Default > Behavior External Reset Button sets the short-press action and whether a long press also resets Startup Configuration. A long press resets Running Configuration.
External Backup & Restore module	1	Active	Yes	The external module uses the serial interface. Under Basic Settings > Ext. Backup/Restore Module, enable or disable backup and restore independently.

Function	Default	Can be changed	Comment
Port usage	Active	Yes	Set unused ports to Disabled under Port Settings > Port Configuration. Verify the selected port and keep management access available.
Static MAC-address table	Disabled	Yes	Add the required static VLAN, MAC and port entries under Security > MAC Table. Use Secure learning to drop frames from unlisted sources. Add the management path to the table before enabling Secure learning on its port.
Device Binding	Disabled	Yes	Under Security > Device Binding, enable the feature and set the expected port, IP and MAC address. Alive Check can log, cycle or shut down a link when the peer stops responding. Stream Check detects low traffic. DDOS Prevention monitors selected traffic and applies the configured response.
Device authentication via RADIUS server (IEEE 802.1X)	Disabled	Yes	Configure RADIUS under Security > AAA. Enable NAS globally and select the required Port-based, Single or Multi 802.1X mode per port. Check NAS > Switch or Port for authorization status.
Access Control Lists	Disabled	Yes	Apply ordered Access Control Entries under Security > ACL. Select the match and Permit or Deny action. Under ACL > Ports, set the action for traffic that matches no specific entry. Check ACL Status and counters.
IP Source Guard	Disabled	Yes	Enable IP Source Guard globally and on the intended access ports. Use static port, VLAN, IP and MAC bindings or dynamic DHCP snooping bindings. Back up the ACLs first, because enabling global IP Source Guard removes existing access control entries.
DHCP Port and IP Binding	Disabled	Yes	Bind the lease address to the intended port under DHCP Server > IP port binding. To block replies from unauthorized DHCP servers, enable DHCP Snooping and mark only allowed server-facing ports Trusted.
Limit control on ports	Disabled	Yes	Enable Limit Control globally and on the intended ports. Set the permitted number of learned MAC address and VLAN pairs and choose None, Trap, Shutdown or Trap & Shutdown. Configure a trap receiver and a recovery procedure where applicable.

Port Storm Control/rate limiting	Disabled	Yes	Use Traffic Prioritization > Storm Control to limit unknown unicast, multicast or broadcast traffic. Use port or queue policing for ingress rates. Set limits for the intended traffic and verify that essential communication remains available.
DoS/DDoS automatic prevention	Disabled	Yes	Use Security > Device Binding and enable DDOS Prevention for a bound port. Select sensitivity, packet type and action. For TCP or UDP, configure the source or destination socket filter.
VLAN segmentation	Disabled	Yes	Configure the management VLAN, allowed VLANs and access, trunk or hybrid port membership under VLAN > VLAN Membership. Use Private VLAN and Port Isolation where direct communication between selected ports must be restricted.
Layer 3 routing functions		Yes	Static routing, RIP and VRRP are available only on designated L3 models. Routing shall be configured according to the zone-and-conduit design and does not replace firewall-based boundary protection

To ensure controlled communication and protect against unauthorized network activity, the following configuration practices shall be applied:

- **VLANs** shall be used to separate management, automation and office networks.
- **Access Control Lists (ACLs)** shall follow a “deny-all, permit-by-exception” principle. Rule order shall consider first-match behavior to avoid unintended access.
- **IEEE 802.1X** authentication with a RADIUS server should be enabled on access ports to prevent untrusted devices from connecting.
- **Port Security (Limit Control)** shall restrict learned MAC addresses to the count required on each port. Choose the limit response and trap destination according to site policy.
- **Rate Limiting** shall be applied on untrusted interfaces to limit abnormal or excessive traffic and mitigate denial-of-service risks.

Function	Default	Can be changed	Comment
Login & Password	Active	Yes	For firmware version V2.02 or higher, set the administrator password at first login. When upgrading from V1.xx, first login requires a change if the factory password is still set. Use Basic Settings > Users > Password Policy to select the password rules.
User Management	Active	Yes	Create named users in User List and assign groups with the required privilege level in Group List. Use Privilege Levels to configure read and write access to configuration and status functions.
User authentication via external server	Disabled	Yes	Configure authorized RADIUS or TACACS+ servers under Security > AAA. Select login methods per interface under Authentication Methods. The next method is used after a remote server timeout. Use a controlled local fallback where required.
Web via HTTPS	Active	Yes	Use Only HTTPS under Login Configuration. In Certificate Maintain, upload the approved PEM certificate and private key through the protected Web interface. Confirm that management clients trust the device certificate.
Web via HTTP	Disabled	Yes	Select Only HTTPS to restrict management to HTTPS. Where supported and required, select HTTPS with HTTP auto-redirect and verify that the browser trusts the device certificate.
CLI via Console	Active	Yes	Use the serial console for authorized local maintenance. Restrict physical access and configure the Console login method under Access Management.
CLI via Ethernet port with SSH	Active	Yes	Enable SSH in Login Configuration only where required. Restrict management sources and confirm device host identity.
CLI via Ethernet port using TELNET	Disabled	Yes	Not recommended for security reasons. Use SSH for remote CLI access.
SNMP (V1,V2c, V3)	V2c active	Yes	SNMPv2c is enabled by default for u-netops access. Disable SNMP if unused. Use SNMPv3 with authentication and privacy where supported by the management tools.

Modbus/TCP	Disabled	Yes	Use Modbus TCP Slave under Basic Settings > Industrial Protocols only for authorized clients and the applicable register map.
EtherNet/IP	Disabled	Yes	Enable EtherNet/IP under Industrial Protocols only when needed. On models with mutually exclusive modes, disable PROFINET before enabling EtherNet/IP. Use the model-specific EDS.
PROFINET	Active	Yes	Enable PROFINET only for the intended automation network. Check the effect of VLAN configuration on PROFINET traffic and of disabling PROFINET on MRP and traffic shaping.
MMS		Yes	Enable only on supported SubstationLine models when required for the intended substation application. Restrict TCP port 102 by VLAN, ACL and authorized communication partners.
Specific IP addresses	Disabled	Yes	Specify the IP address (or IP address range) that can access to the management of the switch
Specific VLAN ID	VLAN ID: 1	Yes	Program a specific VLAN ID to access to the management of the switch. It will only be possible to manage the switch using ports where this specific VLAN ID is accepted
Brute-force protection		Yes	Configure Allowed Retries, Allowed Retry Period, and Block Time under Access Management > Login Configuration.
Automatic session logout		Yes	Set separate Web Interface Inactivity Time and CLI Inactivity Time values under Access Management > Login Configuration.
Concurrent web sessions	5 simultaneous users, 1 active session per user	No	A new Web login by the same user replaces their previous session.

For secure operation, individual user accounts shall be created for each administrator. Shared accounts are not permitted. User privileges shall follow the principle of least privilege and correspond to the assigned responsibilities (e.g. Administrator, Operator, or Read-Only). Where supported, authentication should be linked to a centralized AAA service such as TACACS+ or RADIUS to ensure consistent access control and auditing. Unused or outdated user accounts shall be disabled or removed. All login and configuration activities shall be logged for traceability.

On firmware version V2.02 or higher, set the administrator password during first login. Select the required rules under Basic Settings > Users > Password Policy.

- Enable the minimum-length rule to require at least 12 characters.
- Select mixed-case, digit and special-character rules required by the site.
- Use an individual password and follow site policy for rotation and reuse.

Treat configuration exports as sensitive. Verify the protection of stored credentials and the handling of exported credentials on the selected firmware.

Management access shall be restricted to encrypted channels.
Web management shall use HTTPS, and CLI management shall use SSH.
Unencrypted protocols such as HTTP and TELNET shall remain disabled.
Access to management interfaces should be limited to defined IP addresses and a dedicated management VLAN.
If SNMP is required, SNMPv3 with authentication and encryption shall be used, while SNMPv1/v2c should remain disabled.
Management sessions should automatically log out after a period of inactivity (recommended: 5 minutes).

Set Allowed Retries, Allowed Retry Period and Block Time in Login Configuration. Check Blocked IP Addresses and unsuccessful login events in System Log Information. Configure Web and CLI inactivity logout for the installation.

Before login, a system banner should be displayed stating that access is restricted to authorized users and that unauthorized use is prohibited.

IEC 62443-4-2 capability mapping

The FR overview shows the manufacturer-declared SL-C 1 baseline for FR 1 to FR 7. Use the firmware release and conformity information for the specific model, firmware version and intended deployment. The detail table describes the security functions of the listed switches with firmware V2.02 or later.

IEC 62443-3-3 defines system requirements and the capability levels of a control system. Use those requirements to specify the installation, including the boundary controls and external services needed for its zones and conduits.

Highest SL Covered shows the highest level documented here for each requirement. A dash means that no security level is stated for this requirement. See Product Support for the documented functionality. For a base CR or NDR, the level includes the applicable enhancements at that level. An RE row describes that enhancement. SL 1 baseline denotes coverage under the model-specific SL-C 1 declaration, with the stated configuration, system measures and applicability. An FR-level claim is shown in the overview and requires coverage of all applicable requirements for the FR. Level selection follows ANSI/ISA-62443-4-2-2018.

Status terminology

Product Support	Meaning
Supported	The switch provides the stated function.
Supported with configuration	Configure the stated function on the switch.
Supported with external integration	The switch contributes to the control and requires the specified external service or device.
Provided by the system	The installation is responsible for providing the control.
Not applicable (N/A)	The requirement falls outside the stated device type or intended use or applies only at system level.
Partially supported	The switch provides part of the required function. The row states what is covered.

Security Level Capability Overview

FR	Capability area	SL-C	Controls	Comment
FR 1	Identification and authentication control	SL 1	Local and external authentication	Use named accounts, an approved password policy, failed-login limits and a pre-login notice. Apply the required peer authentication and credential protections.
FR 2	Use control	SL 1	Privileges, sessions and auditing	Assign least privilege. Configure Web and CLI logout, trusted time and audit retention. Check the session and audit behavior required in the installation.
FR 3	System integrity	SL 1	Secure management and integrity	Use HTTPS and SSH and keep firmware and configuration integrity checks enabled. Verify any additional trust and boot requirements for the installation.

FR 4	Data confidentiality	SL 1	Confidentiality and data handling	Use approved secure management settings and protect exported configurations. Follow the secure disposal procedure.
FR 5	Restricted data flow	SL 1	Segmentation and filtering	Configure VLANs, port isolation and ACLs. Enforce inter-zone policies at the designated boundary device.
FR 6	Timely response to events	SL 1	Audit access and central monitoring	Restrict local audit access and configure the approved collector where required. Check audit delivery and access.
FR 7	Resource availability	SL 1	Availability and recovery	Configure traffic limits and protect configuration backups. Validate recovery and provide emergency power where required.

FR	Requirement ID	Requirement headline	Product SL Coverage	Product Support	Implementation / supporting feature	Required configuration / comment
FR1	CR 1.1	Human user identification and authentication	SL 2	Supported with configuration	Named accounts and per-interface authentication methods are available for Web, SSH, Telnet and Console.	Enable only required interfaces. Require individual local or external identities on each path. See RE1 for unique identities and RE2 for MFA.
FR1	CR 1.1 RE1	Unique identification and authentication	SL 4	Supported	Each local account has a unique user name and an assigned group.	Create an individual account for each administrator. Use individual identities with external AAA.
FR1	CR 1.1 RE2	Multifactor authentication for all interfaces	-	Partially supported	The switch can delegate login authentication to RADIUS or TACACS+ on configured interfaces. Local authentication uses passwords.	Use an approved MFA-capable access service for the management paths that require MFA. Include console and fallback access in the access policy.
FR1	CR 1.2	Software process and device identification and authentication	-	Partially supported	In NAS authenticator mode, the switch relays IEEE 802.1X authentication of attached devices to RADIUS. Device Binding restricts traffic by port, IP and MAC address.	Configure NAS on access ports that require attached-device authentication. Use approved HTTPS device certificates and SSH host keys for the corresponding management connections.
FR1	CR 1.2 RE1	Unique software process and device identities	-	Partially supported	HTTPS certificates and SSH host keys identify the switch on supported management paths.	Assign credentials unique to each switch. Configure management clients to authenticate the

					Policy rules can restrict attached devices.	switch using its HTTPS certificate or SSH host key.
FR1	CR 1.3	Account management	SL 4	Supported	User List and Group List manage local users and groups. RADIUS and TACACS+ provide central authentication.	Create, change and remove named accounts as responsibilities change. Define the approved local fallback for server outages.
FR1	CR 1.4	Identifier management	SL 4	Supported	Local identities are managed by unique user name and group.	Use distinct names and remove or revoke unused identities.
FR1	CR 1.5	Authenticator management	SL 1	SL 1 baseline	The switch requires initial administrator password setup and supports credential changes and password rules. Local passwords are stored as hashes. Supported RADIUS and TACACS+ key settings are protected in configuration storage and backups.	Use individual credentials and secure management channels. Restrict access to configuration backups and protect the credential material they contain.
FR1	NDR 1.6	Wireless access management	N/A	Not applicable (N/A)	The listed switch interfaces are wired.	Apply wireless access management to any wireless infrastructure used in the installation.
FR1	NDR 1.6 RE1	Unique wireless identities	N/A	Not applicable (N/A)	The listed switches provide wired networking.	Apply this enhancement to any external wireless equipment.
FR1	CR 1.7	Strength of password-based authentication	SL 2	Supported with configuration	Password Policy can require at least 12 characters, mixed case, digits and special characters.	Apply the policy to local accounts. For externally managed accounts, apply the approved credential policy at the AAA service.
FR1	CR 1.7 RE1	Human password generation and lifetime limits	-	Partially supported	Password Policy applies password length and composition rules. The firmware provides an expiration reminder.	Set local password length and composition in Password Policy. Apply required password generation and lifetime limits in the approved account service.
FR1	CR 1.8	Public key infrastructure certificates	-	Partially supported	Login Configuration supports HTTPS certificate upload, generation and deletion.	Install an approved HTTPS device certificate and protect its private key. Apply the approved certificate trust and revocation policy in the PKI and management clients.

FR1	CR 1.9	Strength of public key-based authentication	-	Partially supported	HTTPS and SSH use public-key mechanisms. The Web interface can generate a self-signed RSA certificate.	Use approved HTTPS certificates, SSH host keys and cryptographic settings. Configure management clients to authenticate the switch.
FR1	CR 1.9 RE1	Hardware protection of private keys	-	Partially supported	The Web interface handles HTTPS certificates and PEM private keys.	Restrict certificate administration and use protected storage for private keys during provisioning.
FR1	CR 1.10	Authenticator feedback	SL 1	SL 1 baseline	The Web login masks password entry. Use the designated secure management interfaces for human login.	Use HTTPS or SSH for remote administration. Keep passwords concealed when entering credentials in the Web interface.
FR1	CR 1.11	Unsuccessful login attempts	SL 4	Supported with configuration	Login Configuration provides configurable limits and a temporary login block. Blocked IP Addresses shows blocked sources.	Set Allowed Retries, Allowed Retry Period and Block Time in Login Configuration. Apply the installation's login limits to any external AAA service in use.
FR1	CR 1.12	System use notification	SL 4	Supported with configuration	Basic Settings > Access Management > Banner Setting configures the pre-login notice.	Enter the authorized-use notice in Banner Setting for presentation before login.
FR1	NDR 1.13	Access via untrusted networks	SL 2	Supported with external integration	Access Security restricts management by source IP, VLAN and service. MAC-based ACLs and VLAN membership can restrict forwarded Layer 2 traffic.	Configure permitted management and access paths. Use a firewall or VPN gateway for access from untrusted networks and monitor allowed and denied traffic.
FR1	NDR 1.13 RE1	Explicit approval of untrusted access	-	Provided by the system	Access Security can allow configured networks and services. The intended deployment uses dedicated boundary devices for untrusted access.	Provide explicit per-request approval by an authorized role at the system boundary where required.
FR1	CR 1.14	Strength of symmetric key-based authentication	-	Partially supported	RADIUS, TACACS+ and SNMPv3 accept protocol-specific shared secrets or authentication keys.	Assign distinct secrets to each service. Use approved authentication algorithms and manage keys according to the site's credential lifecycle policy.

FR2	CR 2.1	Authorization enforcement	SL 1	Supported with configuration	Groups are assigned privilege levels. The switch distinguishes read and write privileges for configuration and status operations.	Configure Users > Privilege Levels and assign least privilege. Use TACACS+ CLI command authorization and accounting where required.
FR2	CR 2.1 RE1	Least privilege for all user types	-	Partially supported	User groups and Privilege Levels control user actions. SNMPv3 access and views restrict management objects and NAS applies port access policy.	Assign only the permissions required by each human, software or device identity. Apply the policy to all enabled management and network access paths.
FR2	CR 2.1 RE2	Permission mapping to roles	SL 4	Supported with configuration	User groups and Privilege Levels associate permissions with configurable privilege levels.	Use Privilege Levels to assign read and write permissions to each group according to its responsibilities.
FR2	CR 2.1 RE4	Dual approval for critical actions	-	Partially supported	Role-based privileges control who can change the switch configuration.	Apply independent approval by two authorized users in the system change workflow for actions that could seriously affect the industrial process.
FR2	CR 2.2	Wireless use control	N/A	Not applicable (N/A)	The listed switch interfaces are wired.	Apply wireless use controls to any external wireless infrastructure.
FR2	CR 2.3	Use control for portable and mobile devices	N/A	Not applicable (N/A)	Portable and mobile device use is governed by IEC 62443-3-3 SR 2.3. NAS and VLAN membership can restrict network access by service devices.	Use authorized service equipment and restrict access to the cabinet, console and configured service ports.
FR2	NDR 2.4	Mobile code	SL 1	SL 1 baseline	The switch serves the management Web interface over HTTPS. Management privileges restrict access to upload functions.	This requirement applies where the device uses mobile code. Apply the controls for execution, transfer and integrity that are specified for the applicable model and deployment.
FR2	CR 2.5	Session lock	SL 1	SL 1 baseline	The switch can end idle Web and CLI management sessions after separately configurable timeouts. A user must authenticate again after termination.	Configure inactivity logout where it is used to pre-empt session locking. If the installation requires a retained session, provide the applicable lock and reauthentication controls.

FR2	CR 2.6	Remote session termination	SL 4	Supported with configuration	Login Configuration provides separate Web Interface Inactivity Time and CLI Inactivity Time settings. The Web interface also provides Logout.	Set Web Interface Inactivity Time and CLI Inactivity Time under Login Configuration. Use Logout to end a Web session after administration.
FR2	CR 2.7	Concurrent session control	-	Partially supported	The documented Web design allows five simultaneous users and one session per user. A newer login replaces the same user's earlier Web session.	Use individual accounts for simultaneous Web management. Set the Web inactivity timeout in Login Configuration.
FR2	CR 2.8	Auditable events	SL 4	Supported	System Log Information displays security events such as successful and failed logins, user changes and backup or restore operations. Audit records carry a time and source.	Use System Log Information for available audit events and configure external accounting or event forwarding for the enabled services as required.
FR2	CR 2.9	Audit storage capacity	SL 1	SL 1 baseline	The switch has dedicated flash storage for audit records, displays available capacity and supports forwarding to a central Syslog collector.	Size audit retention for the installation. Monitor free space and use an approved collector as required. Apply the documented behavior for storage limits.
FR2	CR 2.10	Response to audit processing failures	SL 1	SL 1 baseline	Audit records are buffered and processed for flash storage or Syslog forwarding. The firmware can alert the administrator on audit processing failure and stop flash writes after an integrity error.	Monitor audit failure alerts. Export existing flash records before clearing the buffer and forward audit records to the approved collector where required.
FR2	CR 2.11	Timestamps	SL 3	Supported with configuration	Audit entries carry timestamps and Time Settings offers SNTP client, server and manual clock settings.	Set the intended time zone under Time Settings. Synchronize the clock with a trusted time source on the management network.
FR2	CR 2.11 RE1	Internal time synchronization	SL 4	Supported with configuration	SNTP Client synchronizes the switch clock to a configured time server for audit timestamps.	Enable SNTP Client and specify a trusted system time source on the management network.
FR2	CR 2.11 RE2	Integrity of time synchronization	-	Partially supported	SNTP Client supports designated time server addresses. The time settings expose	Restrict SNTP traffic to approved time sources on the management

					client, server and manual modes.	network. Apply the installation's time integrity controls.
FR2	CR 2.12	Non-repudiation	SL 3	Supported with configuration	The audit log associates recorded administrative actions with the responsible named user and source. TACACS+ accounting can record CLI commands.	Assign individual accounts, retain administrative audit records and configure TACACS+ command accounting for CLI access where required.
FR2	NDR 2.13 RE1	Monitoring of factory diagnostic interfaces	-	Partially supported	The serial management console supports configurable login authentication.	Install the switch in a restricted-access enclosure. Limit access to applicable factory test interfaces to authorized service personnel.
FR3	CR 3.1	Communication integrity	SL 4	Supported with configuration	HTTPS, SSH and authenticated SNMPv3 protect management communications against alteration when selected and correctly configured.	Disable cleartext management protocols. Restrict any required legacy industrial protocols to a protected conduit and protect their communications at the appropriate endpoints.
FR3	CR 3.1 RE1	Authentication of received management traffic	SL 4	Supported with configuration	Authenticated HTTPS, SSH and SNMPv3 sessions verify the origin of received management messages for the corresponding established sessions or security identities.	Configure management clients to authenticate the switch using trusted HTTPS certificates and SSH host keys. Enable SNMPv3 authentication and restrict unauthenticated management services. Protect any required legacy path separately.
FR3	NDR 3.2	Protection from malicious code	SL 1	SL 1 baseline	The switch supports firmware integrity checks and ACLs for limiting network traffic. The intended installation provides additional safeguards against malicious code.	Provide the compensating protection required by the model and deployment, such as malware filtering at the designated system boundary. Restrict update privileges and use approved firmware.
FR3	CR 3.3	Security functionality verification	SL 4	Supported with configuration	System Log Information shows audit records. Access statistics, ACL hit counters and port status show activity	Use access statistics, ACL counters and audit records to track management access and rule activity. Schedule disruptive maintenance in the

					on the configured network paths.	planned service window.
FR3	CR 3.3 RE1	Operational verification of security functions	SL 4	Supported with configuration	Access Management Statistics shows received, allowed and discarded requests. ACL Status shows rule counters and System Log Information shows audit events while the switch is in service.	Use Access Management Statistics, ACL Status and System Log Information to view allowed and denied requests, rule matches and audit records during operation.
FR3	CR 3.4	Software and information integrity	SL 1	Supported with configuration	V2.02 and later use SHA-256 to check the integrity of supported firmware, configuration and audit log data.	Use approved firmware and configuration files. Keep the standard integrity checks enabled.
FR3	CR 3.4 RE1	Verification of data and software origin	-	Partially supported	Firmware and configuration imports can perform integrity checks.	Obtain firmware from the official download channel for the switch model. Restrict upload permissions and protect configuration import files.
FR3	CR 3.4 RE2	Automatic notice of integrity violations	-	Partially supported	The firmware detects integrity errors in security-related data and can stop writes after an audit flash integrity failure.	Use the approved audit monitoring setup. Preserve available flash records before clearing the audit buffer after a flash integrity error.
FR3	CR 3.5	Input validation	SL 1	SL 1 baseline	Firmware, configuration and HTTPS certificate imports use dedicated interfaces. The standard V2.02 backup restore path performs an integrity check before restoring the configuration.	Restrict management access, use approved files and keep the standard integrity check enabled during backup restoration.
FR3	CR 3.6	Deterministic output	N/A	Not applicable (N/A)	In the intended network role the switch forwards traffic and provides equipment alarms. It does not drive actuator or process-control outputs.	Define the safe state at the process controller. Where a switch relay or logical output is used in a process action, specify its behavior in the installation's safety design.
FR3	CR 3.7	Error handling	SL 1	SL 1 baseline	System Log Information and management screens provide diagnostic messages for local operation and service.	Use System Log Information for security-relevant errors. Restrict access to diagnostic and audit information to authorized roles.

FR3	CR 3.8	Session integrity	-	Partially supported	V2.xx assigns a session identifier to Web logins and associates the session with user and source information. Web logout and inactivity termination are available.	Use HTTPS and configure the Web inactivity timer. End the Web session with Logout after administration.
FR3	CR 3.9	Protection of audit information	-	Partially supported	The switch uses dedicated audit flash and integrity checking. Log display, export and clear operations are available separately.	Restrict permissions to view, export and clear audit logs. Forward required records to the approved collector and protect retained records there.
FR3	CR 3.9 RE1	Hardware-enforced write-once audit storage	-	Provided by the system	Local RAM and flash logs have authorized clear controls. Syslog can forward records externally.	Provide hardware-enforced write-once retention at the approved collector where required. Restrict access to retained audit records.
FR3	NDR 3.10	Support for updates	SL 1	Supported	Basic Settings > Upgrade Firmware uploads the model-specific image and offers deferred activation.	Back up the approved configuration and schedule the restart. System Information displays the active firmware version.
FR3	NDR 3.10 RE1	Update authenticity and integrity	-	Partially supported	The firmware update path checks the integrity of supported images.	Install model-specific firmware from the official download channel and keep the standard integrity check enabled.
FR3	NDR 3.11	Physical tamper resistance and detection	-	Provided by the system	Install the switch in a restricted-access location. A locked cabinet provides physical access control.	Install the switch in a locked enclosure. Provide any tamper resistance or detection required by the installation design.
FR3	NDR 3.11 RE1	Tamper attempt notification	-	Partially supported	Event settings and the fault relay report configured equipment faults.	Route enclosure tamper alarms to the designated monitoring system where the installation requires them.
FR3	NDR 3.12	Provisioning product supplier roots of trust	-	Partially supported	V2.xx and later provide firmware integrity checks.	Use the vendor-approved update process and approved firmware for the installed model.
FR3	NDR 3.13	Provisioning asset owner roots of trust	-	Partially supported	Login Configuration accepts an operator-provided HTTPS	Use an approved HTTPS device certificate. Restrict certificate

					device certificate and PEM private key.	administration and protect the PEM private key.
FR3	NDR 3.14	Integrity of boot process	SL 1	SL 1 baseline	The V2.xx firmware provides SHA-256 integrity protection for the bootloader and critical data partitions.	Use approved firmware and keep the normal integrity validation enabled. Follow the model-specific response procedure for an integrity failure.
FR3	NDR 3.14 RE1	Authenticity of the boot process	-	Partially supported	V2.xx provides SHA-256 integrity protection for the bootloader and critical partitions.	Use approved firmware and follow the model-specific recovery procedure after a boot integrity failure.
FR4	CR 4.1	Information confidentiality	SL 4	Supported with configuration	HTTPS and SSH protect management data in transit. SNMPv3 privacy is available. Management and log access can be restricted through configured privileges.	Use encrypted management modes and restrict access to stored settings and logs. Protect exported configurations and keys in approved storage.
FR4	CR 4.2	Information persistence	-	Partially supported	Factory Default can reset the running and startup configurations. Options are available to retain IP settings and user credentials.	For decommissioning, clear Keep IP and Keep User/Password and reset both configurations. Handle residual audit data, keys, credentials and removable backups under the secure disposal procedure.
FR4	CR 4.2 RE1	Protection of released shared memory	-	Partially supported	The switch can reset its configuration during decommissioning.	Apply the installation's secure data handling and disposal procedures. Handle removable backup media separately.
FR4	CR 4.2 RE2	Verification of data erasure	-	Partially supported	Management pages can be inspected after clearing configuration or logs.	Use the installation's approved disposal procedure for protected credentials, keys and data retained in flash storage.
FR4	CR 4.3	Use of cryptography	SL 4	Supported with configuration	The switch offers HTTPS, SSH and SNMPv3 authentication and privacy.	Use secure management modes, approved certificates, trusted SSH host keys and cryptographic parameters permitted by the installation policy.

FR5	CR 5.1	Network segmentation	SL 4	Supported with configuration	VLAN membership, management VLAN, private VLAN, port isolation and ordered ACLs separate and filter traffic inside a zone.	Assign VLANs and tags to the required ports. Restrict management access and apply ACLs to permit only the intended traffic paths.
FR5	NDR 5.2	Zone boundary protection	N/A	Not applicable (N/A)	The intended deployment is inside a protected zone. VLANs and ACLs segment and filter traffic inside the zone.	Where the installation uses a network device at a zone boundary, use a dedicated boundary control to monitor and enforce the zone and conduit policy.
FR5	NDR 5.2 RE1	Default deny at zone boundaries	N/A	Not applicable (N/A)	The intended deployment is inside a protected zone. The switch supports ordered ACLs within that zone.	Configure default-deny and exceptions at the designated boundary device.
FR5	NDR 5.2 RE2	Isolation at a zone boundary	N/A	Not applicable (N/A)	The switch is intended for in-zone segmentation.	Use the designated boundary device to isolate the control zone when required.
FR5	NDR 5.2 RE3	Fail-closed zone boundary	N/A	Not applicable (N/A)	The intended deployment assigns boundary protection to a separate device.	Use a designated boundary device configured to block communications under the failure conditions defined for the zone boundary.
FR5	NDR 5.3	General purpose person-to-person communication restrictions	N/A	Not applicable (N/A)	The requirement applies to a device at a zone boundary. The switch is intended for use inside a protected zone.	Apply the boundary policy to restrict general-purpose messaging from outside the control system.
FR5	CR 5.4	Application partitioning	N/A	Not applicable (N/A)	Application partitioning is governed by IEC 62443-3-3 SR 5.4.	Separate application workloads on the components that host or execute them.
FR6	CR 6.1	Audit log accessibility	SL 4	Supported with external integration	Authorized users can view and download audit records from System Log Information. Syslog can send records to a central collector.	Restrict local log access by role. Configure the collector as described in RE1 for the higher levels.
FR6	CR 6.1 RE1	Programmatic access to audit logs	SL 4	Supported with external integration	Syslog can send selected audit records automatically to a centralized collector over UDP.	Select Client(Local) and Server(Remote). Set the approved collector address and port and select Audit severity as required. Use a protected management network and restrict read access at the collector.

FR6	CR 6.2	Continuous monitoring	SL 4	Supported with external integration	Syslog, SNMP notifications and counters can feed continuous centralized monitoring.	Configure authorized collectors and monitor for interrupted delivery and security events. Define detection, triage and response at the monitoring system.
FR7	CR 7.1	Denial of service protection	SL 1	SL 1 baseline	Storm Control, port and queue policers, ACL rate limiters and traffic prioritization help maintain essential traffic during overload.	Configure traffic limits and priority for essential communications using Storm Control, policing and ACL rate limits as required.
FR7	CR 7.1 RE1	Manage communication loads	SL 4	Supported with configuration	Storm Control limits broadcast, multicast and unknown-unicast flooding. Port and ACL policers limit selected ingress traffic.	Set storm and ingress rate limits for the expected traffic. Prioritize essential communications according to the deployment's traffic policy.
FR7	CR 7.2	Resource management	SL 1	SL 1 baseline	Login retry limits, Web session limits and traffic policers constrain resource use on management and traffic paths.	Set management retry and session controls and configure traffic rate limits for the expected deployment load.
FR7	CR 7.3	Control system backup	SL 4	Supported	Backup & Restore exports the active or startup configuration. Restoration can target RAM, flash or both. Supported models can use external backup hardware.	Use Running Configuration to back up active settings. Protect backups and keep the integrity validation described under RE1 enabled for this coverage.
FR7	CR 7.3 RE1	Backup integrity verification	SL 4	Supported with configuration	V2.xx validates the SHA-256 integrity of supported configuration backups. A legacy V1.xx import option bypasses that check for old files.	Keep backup integrity validation enabled for current backups. Use the legacy import option only for a planned migration from V1.xx.
FR7	CR 7.4	Control system recovery and reconstitution	SL 4	Supported with configuration	The switch can load an approved configuration and save it as Startup Configuration.	Restore the approved configuration with the required accounts, management settings, VLANs, logging and services. Save it as Startup Configuration for use after restart.
FR7	CR 7.5	Emergency power	N/A	Not applicable (N/A)	Emergency power is governed by IEC 62443-3-3 SR 7.5. Variants with	Provide emergency power at system level. Connect the approved feeds and

					redundant feeds can signal power faults through the available fault relay.	route available power-fault alarms to the monitoring system.
FR7	CR 7.6	Network and security configuration settings	SL 2	Supported	The management interface exposes active network and security settings. Save/Manage Configuration identifies whether the active settings match startup configuration.	Apply the approved settings and save the intended configuration. The running export format is described under RE1.
FR7	CR 7.6 RE1	Machine-readable reporting of security settings	-	Partially supported	Backup & Restore exports Running Configuration as a .cfg file of CLI commands. The export contains settings that differ from factory defaults.	Use the export to review changed settings. Include the model- and firmware-specific factory defaults in a complete inventory of active security settings.
FR7	CR 7.7	Least functionality	SL 4	Supported with configuration	Ethernet ports and optional services can be disabled. Management can be restricted by VLAN and source IP.	Keep only required ports and services active. Retain the approved management access restrictions during network and firmware changes.
FR7	CR 7.8	Control system component inventory	SL 4	Supported	System Information shows firmware, serial number and MAC address. LLDP provides neighbor information. The type plate identifies the exact hardware.	Maintain asset records using System Information and the type plate. Enable LLDP only where neighbor discovery is required.

Function	Default	Can be changed	Comment
Backup & Restore	On demand	No	The configuration of the switch can be stored in a file; similarly, a configuration file can be uploaded on a switch. It is possible to execute this operation through a PC or through our EBS (External Backup & Restore) module type 2682610000. Furthermore, this can be executed using Weidmueller's network management software "u-netops"
Firmware update	On demand	No	From the management of the switch the user can easily upgrade its firmware (FW) whenever any new version is available. This can also be done using Weidmueller's network management software "u-netops" Latest FW version of every product will always be available at Weidmüller's online catalogue.
Logging	Active	No	Use Monitor and Diagnostics > System Log Information to filter and download local events. On supported firmware, configure additional flash retention and verify time before relying on timestamps.
Syslog	Disabled	Yes	In Warning/Event Settings > SYSLOG Setting, select local and remote logging and set the collector, UDP port and severity. Verify event receipt. UDP provides no delivery acknowledgement.

Event logging and time synchronization

Use System Log Information to check relevant security events. Set the time zone and configure SNTP Client with a trusted time server in the management network. For manual time, verify the clock after restart. Protect local records and forward required events to the approved collector.

Firmware management

Firmware updates shall be performed exclusively via the management interface.
The following principles apply to maintain software integrity:

- Use the dedicated import options for approved firmware images, configuration files and HTTPS certificates.
- Keep normal firmware integrity validation active. Verify the active version after the activation restart.
- Configuration exports contain readable CLI commands. Protect them as sensitive files and verify the handling of exported credentials on the installed firmware.
- Before each update, the current configuration shall be backed up - either to a file or via the **External Backup & Restore module (type 2682610000)**.

- Backup files shall be stored securely to prevent unauthorized access.
- For replacement hardware, install the approved firmware and restore a compatible configuration. Verify administrative access, VLANs, services and logging before commissioning.

The product does not support automatic over-the-air (OTA) firmware updates. All firmware images must be downloaded from official Weidmüller sources and installed manually via the device management interface. This ensures that firmware deployment remains under the control of the operator, including testing in a staging environment, change approval, and rollback where required.

Vulnerability management
Operators shall maintain a defined process to regularly check for **firmware updates and security advisories** published by Weidmüller (e.g. via the Security Advisory Board or PSIRT). Discovered vulnerabilities shall be mitigated promptly by applying available updates or implementing compensating controls until a fix is released.

Secure decommissioning
Disconnect the switch from the operational network. Reset Running Configuration and Startup Configuration with Keep IP and Keep User/Password cleared. Verify removal of certificates, keys and retained audit data separately. Remove backup media and device entries from administration and monitoring systems. Dispose of the device and any remaining data according to site policy.

Function	Port	Protocol	Default	Can be changed	Comment
HTTP	80	TCP	Closed	Yes	Restrict Web management to HTTPS. Where required, use a supported HTTPS redirect.
HTTPS	443	TCP	Opened	Yes	Use an HTTPS certificate trusted by the management clients.
TELNET	23	TCP	Closed	Yes	Leave disabled and use SSH for remote CLI access.
SSH	22	TCP	Opened	Yes	CLI access secure
SNMP	161	UDP	Opened	Yes	Disable when unused. Use SNMPv3 with authentication and privacy when required.
SNTP Client	123	UDP	Disabled	Yes	Outbound synchronization to a trusted time server.
SNTP Server	123	UDP	Closed	Yes	Allow synchronization requests only from approved clients.
Modbus/TCP	502	TCP	Closed	Yes	Access to Modbus registers
Profinet	49152, 49153, 49154, 49155, 49156	UDP	Model dependent	Yes	PROFINET Conformance Class B on supported models. Verify UDP and Ethernet-layer flows for the selected model and controller.
EtherNet/IP	44818 / 2222	TCP / UDP	Closed	Yes	TCP/44818 for explicit messaging and UDP/2222 for I/O where applicable. Verify UDP/44818 discovery for the selected controller and device.
MMS	102	TCP	Model dependent	Yes	On supported Substation Line products, permit only authorized IEC 61850 peers.
Syslog	514	UDP	Disabled	Yes	Outbound to the authorized collector. Check the configured port and event delivery.
RADIUS	1812 / 1813	UDP	Disabled	Yes	Outbound authentication and accounting to approved AAA endpoints. Verify configured server ports.

TACACS+	49 (typ.)	TCP	Disabled	Yes	Outbound AAA to approved servers. Verify the configured destination port.
SNMP trap	162 (typ.)	UDP	Disabled	Yes	Outbound to configured managers. Verify destination, SNMP version and event selection.

All unused or unnecessary services and ports shall remain disabled to minimize the attack surface. Unencrypted management and application protocols shall not be enabled.
When network services such as time synchronization or monitoring are required,
access shall be restricted to trusted source IP addresses, and encrypted communication shall be preferred wherever possible.

Additional Support Center information

Headline	Comment	Reference
General	Further product-specific information and help can be found in the Weidmueller Support Center. Use the product type (e.g. IE-SW-AL12M-8GT-4GESFP) in the search field.	https://support.weidmueller.com/support-center/
Industrial Product Security Guideline	A downloadable document on the Weidmueller Industrial Security website providing guidance on building a robust cybersecurity system and integrating Weidmueller components into that system.	Industrial security