GE VERNOVA

Secure Deployment Guide

Multilin Agile

P14D, P14N, P94V

Hardware Version: E
Firmware Version: 8.0

GE Publication Number: GER-4991

Publication Date: March 2025

Cybersecurity Disclaimer

The Multilin Agile (P14D, P14N, P94V) products are intelligent electronic devices (or IEDs), designed to be installed and operated in utility and industrial plant environments and connected to secure private networks. These products should not be connected to the public internet.

GE Vernova strongly recommends that users protect their digital IEDs using a **Defence-in-Depth** strategy which will protect their products, their network, their systems and interfaces against cybersecurity threats. This includes, but is not limited to:

- Placing digital IEDs inside the control system network security perimeter
- Deploying and maintaining access controls, monitoring and intrusion detection
- Security awareness training
- Security policies
- Network segmentation and firewalls installation
- Strong and active password management
- Data encryption
- Antivirus and other mitigating applicable technologies

Multilin Agile IEDs are available with an optional software option, providing additional cybersecurity mechanisms to help protect against cybersecurity intrusion. GE Vernova strongly recommends using this 'advanced security' option.

For additional details and recommendations on how to protect Multilin Agile IEDs, please see the ***Hardening Setup*** section below. From time to time, we may also provide additional instructions and recommendations relating to the Multilin Agile family and cybersecurity threats or vulnerabilities.

As a user, it is your sole responsibility to make sure that all Multilin Agile IEDs are installed and operated in accordance with its cybersecurity capabilities, security features, and the instructions and recommendations. Users assume responsibility for all risks and liabilities associated with damages or losses incurred in connection with any cybersecurity incidences.

Contents

1. Introduction

This document describes the Initial Hardening setup and best practices to securely configure Multilin Agile family IEDs with EnerVista configuration software. It also provides an overview of the supported cybersecurity features.

Multilin Agile IEDs offer various order code options to enable the selection of a product suited to the customer's need and application. For Cybersecurity, it offers two options - basic, and advanced security.

Multilin Agile IEDs with basic security options offers:

- Role based access
- Inactivity timeout and lockout based on authentication failure
- Encrypted communication channel with configuration tool (EnerVista D&I Setup)
- Logging of security events and storage in a separate file on the IED
- Security events reporting to the configured syslog server

Multilin Agile IEDs with advanced security order code options offer:

- Centralized authentication (RADIUS/LDAP)
- Configurable permissions for roles

This document provides recommended configurations for both security variations. Prior to ver 08A, the Multilin Agile IED only supported RADIUS for centralized authentication. From release 08A, Multilin Agile also supports LDAP.

1.1. Intended audience

This document is a helpful resource for utility personnel responsible for deploying the products in a secure manner. This document assumes that the reader is familiar with the product.

1.2. Additional documentation

Alongside this document, you can also refer to the product manual for a detailed understanding of the supported security features.

2. Product Defence-in-Depth Strategy

The product implements the following security features:

- Secure design process to ensure that cybersecurity is part of the design process and not an afterthought.
- Security and penetration testing to detect, as far as possible, vulnerabilities at the design stage.
- Digital signature of firmware and software, to allow verification of integrity and authenticity before installation.
- Monitoring of software components vulnerabilities and security bulletins, to inform users of newly discovered vulnerabilities and threats.
- User authentication.
- Role-based access control, to enforce correct privileges in accordance with the area of responsibility.
- Password and user account policies, to prevent use of weak passwords and password brute force attack.
- In IEDs with advanced cybersecurity, centralized user management (using RADIUS or LDAP), to allow prompt removal of user accounts.
- Security event logging for post-incident analysis.
- Centralized security event logging using SYSLOG protocol. This allows events to be sent to a Security Operations Centre (SOC) for close to real time security monitoring.
- Hardening to reduce the attack surface (making it more difficult for cybersecurity attacks).

To complement the defence-in-depth strategy, the product must be installed in a secure environment. The product cannot mitigate DoS attack through network interface overload.

3. Environment

The Multilin Agile IED and EnerVista D&I Setup configuration software is designed to be installed and operated in a utility and industrial environment with connection to a private network inside the Electronic Security Perimeter (ESP).

Although the rest of this guide describes security measures at the product level, requirements to achieve good security go beyond just the product.

GE Vernova recommend that your security concept considers the whole system, in which the IEDs are installed, in accordance with a **Defence-in-Depth** approach. Security includes (but is not restricted to):

- Physical security such as building access control and locked cabinets.
- Security policies.
- Access control.
- Network security measures, such as IP segmentation, use of firewalls and use of secure protocols. Consider employing an Operations Technology (OT) next generation firewall. This would enforce OT policy at the protocol level and monitor and block malicious activity and unintended disruptions.
- Protection/Control system IEDs, such as the Multilin Agile family, should not be connected directly to the internet.
- Configure appropriate firewall rules to allow only legitimate user connections to the product.
- Security monitoring, such as network intrusion detection systems, security event logging using a centralized server.
- System hardening by disabling unused processes and ports, and removal of unused connection links.
- Remote configuration/monitoring of the IED must be done from a secure engineering workstation through a trusted network link.
- Use secure methods for remote access, such as a Virtual Private Network (VPN), dual authentication, recognizing that the VPN is only as secure as the connected IEDs.

4. Secure Installation - Hardening

4.1. Verifying software integrity

Before installing any software, the installation package integrity must be verified.

GE Vernova software is digitally signed. You verify a piece of software by right-clicking on the filename and selecting the **Digital Signature** tab in the **Properties** menu. The signature details must read "This digital signature is OK".

The software must not be installed if the signature verification fails. If this happens, please contact your support organization.

4.2. Upgrading firmware to the latest version

GE Vernova strongly recommend you upgrade the firmware to the latest sub-version of the major version used, to take advantage of all the fixed known vulnerabilities.

As part of the 'Secure Firmware Upgrade', the firmware integrity and authenticity are verified before upgrading the firmware in the IED.

The firmware upgrade procedure can be found in the main product manual.

4.3. Disable unused protocols and ports

The Multilin Agile IED supports several communication ports (based on order code). By default, all physical ports are enabled. The network traffic on each of the Ethernet ports can be disabled or enabled by setting the **Function** to Disabled for the respective Ethernet port. This setting can be configured from the settings screen at path:

SETTINGS > DEVICE > COMMUNICATIONS

In compliance with NERC-CIP, most of the Multilin Agile logical ports are user-configurable - they can be enabled or disabled. GE Vernova recommend that you disable the protocols and logical ports that will not be used. The logical port details can be found in the section 'List of Supported Protocols'.

4.4. User authentication and roles

4.4.1. Modify default passwords

Multilin Agile IEDs with the advanced security option supports pre-defined user accounts with roles: ADMINISTRATOR, ENGINEER, OPERATOR, VIEWER. It also supports roles: INSTALLER, RBACMNT, SECADM, SECAUD as defined in standard IEC62351-8:2020. Permissions to each of these roles can be modified. The default user accounts password is "**ChangeMe1#**".

For IED authentication, role passwords are stored securely on the IED. The usernames are the same as the roles when the user accounts are maintained on the IED. All accounts, except OBSERVER, have the default password as "**0**".

When you receive a Multilin Agile IED, GE Vernova recommend that you log into the IED using the default password, and change the passwords using unique strings for all the accounts using the path:

SETTINGS > RBAC User Management

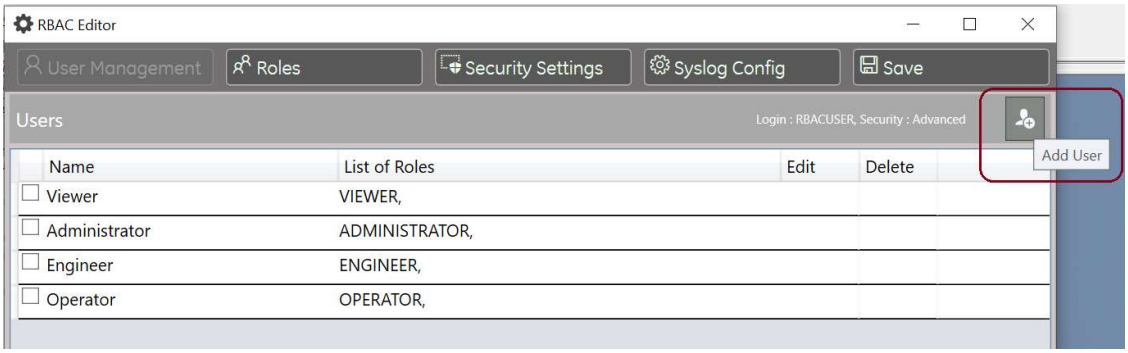
Privileged users with ADMINISTRATOR roles can change passwords for all local accounts.

Multilin Agile IEDs with the advanced security option support IED authentication as well as centralized or server authentication. When server authentication is used, each user account username, password and role information is stored on the authentication server. In such a case, the password can be modified directly on the authentication server.

4.4.2. Non-shared user accounts (advanced security variant)

Multilin Agile IEDs with the advanced security option, supports both the IED and centralized or server authentication. In both cases, users can configure and define non-shared accounts with restricted privileges.

You can configure each user account with any of the roles: ADMINISTRATOR, RBACMNT, SECADM, SECAUD, INSTALLER, ENGINEER, OPERATOR, VIEWER. It also supports defining a new role with user defined permissions. The RBAC Management screen appears in the EnerVista configuration tool, as shown below:



GE Vernova recommends that you remove unused accounts from the user configuration. Only active accounts should be maintained.

5. Multilin Agile Secure Installation

This section outlines recommendations for secure installation of the Multilin Agile family of IEDs security recommendations.

5.1. Security recommendations

Multilin Agile IEDs offer flexible modification possibilities for the security configuration based on the user's setup and policies. GE Vernova recommends the following configuration:

- **Serial inactivity timeout:** (Setting name: `Access Timeout`). Recommended value: 5 minutes
- **Password complexity:** Recommended value: Enabled
- **Maximum number of failed logins attempts before account lockout:** (Setting name: `Access Lockout`): Recommended value: 3 Attempts Limit
- **Communication ports:** Disable/Disconnect communication ports and protocols when not in use
- **Security bypass option:** Avoid use of security bypass option
- **Remote/centralized authentication server:** Use this where possible

All security settings are explained in the product manual.

5.2. Bypass access

This can be configured by the user with 'ADMINISTRATOR' privileges to any digital operand. When activated, access control for the HMI interface is bypassed. That means any user with ADMINISTRATOR privileges can access the HMI.

It is available in both security variants of Multilin Agile - basic and advanced security IED. By default, the "Bypass access" is disabled.

It is strongly recommended that this option is activated when HMI access is limited to a small number of personnel or where assessments are carried out on all users. Otherwise, it is recommended that Bypass Access is disabled when the Multilin Agile IED is in service, to ensure proper RBAC is in place, and unauthorized personnel are unable to modify the configuration or give commands in any circumstances.

5.3. Required password for D/T change

The date/time can be set by any role if this setting is disabled. If this setting is enabled the date/time can only be set by the allowed users.

This configuration is available in both basic and advanced security IEDs. By default, it is "Enabled".

Timestamping all events and oscillography is crucial, and it is advisable to only grant a small number of users permission to change the date and time on the IED.

When IED authentication is disabled, only the ADMINISTRATOR and SUPERVISOR have the permission to re-enable it.

5.4. Require password for control

This setting is applicable for controls performed from the HMI of the IED.

If this setting is disabled, then a password is not required for performing controls from the HMI. If this setting is enabled, then a privileged user's password is required.

This configuration is available in both basic and advanced security IEDs. By default, "Require PW (Password) for Control" is enabled.

GE Vernova recommends that this setting remains enabled in normal operation.

5.5. Require password for remote control

This setting is applicable for controls operations performed remotely. It can be configured as On or Off.

This setting is only available in basic security.

If this setting is On, Operator controls performed from remote communications do not require a password. If this setting is Off, a password is required. By default, this setting is configured as Off.

5.6. Server authentication

Multilin Agile IEDs with advanced security support IED-level authentication and centralized authentication. The use of centralized authentication is recommended as it offers easier user database management and helps in the maintenance of non-shared user accounts.

From ver 08A onwards, Multilin Agile supports RADIUS and LDAP for server authentication. Configuration for server authentication (Settings: `Server IP`, `Port`, `Vendor ID`, `Timeout and Retries`, `Shared Secret`) can be done using EnerVista D&I Setup configuration software. The RADIUS server also needs a 'CA Certificate' to be available with the Multilin Agile IED. The 'CA Certificate' needs to be uploaded to the Multilin Agile IED using the EnerVista configuration tool -"RBAC editor" screen.

The following protocols and servers are supported by the Multilin Agile 08A IED:

RADIUS: Servers used as a central authentication server can be:

- FreeRADIUS server
- RSA Authentication Manager

Implementation supports the authentication protocols:

- PEAPv0 with inner authentication method MS-CHAPv2
- EAP-TTLS with inner authentication method PAP (to support RSA AM)
- PAP (unsecured, to support any RADIUS server)

LDAP: Servers used as a central authentication server can be:

- Microsoft Active Directory server
- OpenLDAP

Implementation supports the authentication protocols:

- TCP
- STARTTLS

Note: IEDs with basic security order code do not support this feature.

5.7. Secure event logging

5.7.1. Syslog server

Mutilin Agile IEDs support the **syslog over UDP** and **TCP** in ver 08A. It supports redundant syslog server configuration. Multilin Agile IEDs capture security-related events and sends them to a centralized syslog server (assuming a syslog server is configured and reachable). If both the primary syslog server and the secondary syslog server are configured, and both are reachable then the IED sends syslog messages to both the configured servers. If that is also unreachable then the security events are buffered.

GE Vernova recommends using a syslog server for event logging as it provides a centralized view of all system events, and it enforces long term storage of logs. Depending on the level of severity, a syslog server (or a reporting tool gathering information from a syslog server) can produce reports and charts etc.

For a complete list of supported security events, please refer to product manual; section 19.4.6 SYSLOG.

GE Vernova strongly recommends that customers install the advanced security option.

5.7.2. Security events storage on IED

Security events are saved in the files: `securelog.CSV` and `log.txt`

This file stores events until it reaches 1MB size. Once the file reaches 1MB the file is renamed as securelog1.txt, and a new file "securelog.txt" starts storing newly generated security events.

Details about these files and how to retrieve them are available in the instruction manual.

The securelog.CSV file stores the following fields for each security event:

- Event number
- UTC Date & time stamp
- Username
- Role
- IP address
- Activity value

The security events file can be accessed by role with the appropriate privileges. It can be viewed from EnerVista D&I software on the following path: ***online device\Records\Security events***.

Please refer to the product manual for further information.

Due to capacity limitations, Ge Vernova recommends that you download and archive these files in a secure place for auditing purposes, at regular intervals.

5.8. Maximum user connections to IED

Based on the order code, the maximum number of connections is five (5).

At any given time, only one user with a 'NON-VIEWER' role can connect to an IED. However, multiple users with the 'VIEWER' role can connect to an IED at any given time. The 'VIEWER' role allows those users to view actual values, and the configuration of the IED. The maximum number of connections to the IED is limited by the total number of MODBUS connections supported.

5.9. Role permission mapping

The following pre-defined roles are supported by the Multilin Agile IED with 'basic' security:

- ADMINISTRATOR
- ENGINEER
- OPERATOR
- VIEWER

Multilin Agile IEDs support fixed permissions for each pre-defined role in the case of basic security.

5.10. Non-Encrypted MODBUS

Due to customers' requests to use 'plain' or 'non-encrypted' MODBUS communication with SCADA applications for certain scenarios, Multilin Agile is supporting the clear-text MODBUS.

Under the path: ***DEVICE\COMMUNICATIONS\MODBUS***, the user can find "`MODBUS TCP`" setting.

If a Multilin Agile IED has 'basic security' then the setting "`MODBUS TCP`" can be configured to one of the following options:

- **Disabled:** When the `MODBUS TCP` setting is set to Disabled, the port 502 will be closed.
- **Enabled:** When the `MODBUS TCP` setting is set to Enabled, the legitimate user can read or write over plain MODBUS using port 502 on successful authentication.
- **Read-Only (*):** When the `MODBUS TCP` setting is set to Read-Only, the legitimate user can only read over plain MODBUS using port 502.

By default, the `MODBUS TCP` Setting is set to Enabled. A user with 'ADMINISTRATOR' role can configure this setting. Once the setting is configured to other than disabled, the IED will allow communication with a 3rd party SCADA application in plain text MODBUS over port 502. For a configuration change, the Multilin Agile IED will register a security event to identify the user.

If a Multilin Agile IED has 'advanced security' then the setting "`MODBUS TCP`" can be configured to one of the following options: **Disabled** or **Enabled**.

6. Setup Software

EnerVista Setup software is configuration and monitoring software, designed to be used with the IEDs. With this the user can manage offline projects, connect to the IED, update the IED configuration, monitor system data, and conveniently view diagnostics sequence of events and COMTRADE. The user can also upgrade the IEDs firmware.

EnerVista Setup is digitally signed software.

6.1. Secure firmware upgrade

The configuration software can validate the firmware file's digital signature to ensure the authenticity (publisher verification) and integrity of the firmware file. The configuration software prohibits the firmware upgrade process if the file verification fails. This behaviour complies with the NERC-CIP 10 requirement.

Firmware upgrades can only be performed by users with a role with appropriate permission. By default role definition, 'INSTALLER' can upgrade the firmware.

For IEDs with basic security, firmware upgrades can only be performed by a user with 'ADMINISTRATOR' role.

The IED also validates the firmware file's authenticity. This ensures that no unauthorized personnel can harm the IED even if they manage to bypass the EnerVista setup for firmware upgrade.

6.2. Secure communication

When the EnerVista D&I setup software tool communicates with the Multilin Agile IED via a secure tunnelled channel, using GRPC over TLS, it ensures that sensitive information cannot be disclosed to unauthorized personnel. TLS ensures that both the server and client have a valid certificate for proper communication.

7. Maintaining Security

Once good security has been properly configured, it is important to create procedures to maintain security over time.

7.1. Periodic security audits

The configuration applied in the secure installation paragraph must be recorded.

Periodically, particularly after maintenance activity, the security configuration must be audited, and deviations tracked and fixed.

7.2. Backup and restore procedures

Firmware installation packages and configuration files must be backed up following any configuration/maintenance activity.

A restore procedure must be prepared for quick service restoration following an incident.

7.3. Vulnerability monitoring and firmware updates

GE Vernova responsibly discloses vulnerabilities found in its products.

Users should periodically check for newly published vulnerabilities and available firmware updates.

Users should define a security update policy.

All GE Vernova software packages are digitally signed. Digital signatures must be verified before installation.

7.4. Reporting a vulnerability

Providing a legitimate pathway for vulnerability disclosure is an essential link between GE Vernova and the cybersecurity community.

To submit a vulnerability in a Grid Solutions product to the GE Vernova PSIRT team, please fill in the form at https://www.ge.com/security. Please do not include identifiable sensitive data (e.g. personal data and specific system configuration) within the body of the communication or any attachments (e.g. screenshots, images, or log files).

GE Vernova actively encourage reports to be sent to us for remediation prior to a public disclosure, so that we can properly address any vulnerabilities.

GE Vernova request the following when you report a vulnerability:

- Please provide your report in English.
- Include specific information about affected products, including model or serial numbers, geographic location, software version, and the means of obtaining the product.
- If you have developed a proof-of-concept for exploiting the vulnerability, please include the code and explanation.
- If you are aware of any incidents of this vulnerability being exploited on equipment in the field (e.g. a Grid Solutions' customer was directly impacted by this vulnerability), please inform us.
- Information on how you discovered the vulnerability, your thoughts on impact or CVSS scoring, and potential remediations will help us to triage the vulnerability more efficiently.
- Please include relevant information about yourself or the company/organization you are representing, or whether you prefer to remain anonymous.
- Please let us know if you have a preferred method of contact during our internal triage process.
- Please include your intentions for disclosing the vulnerability to us, or if you intend to disclose the vulnerability to the public.

In response, you can expect the following from us:

- We will acknowledge receipt of your message within 48 hours.
- In the following phase of initial triage and assessments, an appropriate member of the GE Vernova PSIRT may reach out to you to:
    - Request additional information, or
    - Communicate an expected process and timeline, or
    - Notify you that the report is either out of scope or will not be triaged for other reasons
- Once we have conducted our own assessment of the vulnerability, we will communicate our process and findings after investigation.
- We will provide public recognition for the security researcher (if requested) and if the report results in a public disclosure.

By submitting a request, you acknowledge that Grid Solutions may use in an unrestricted manner (and allow others to do the same) any data or information that you provide to Grid Solutions. Your submission does not grant you any rights under Grid Solutions intellectual property or create any obligations for Grid Solutions.

8. Decommissioning

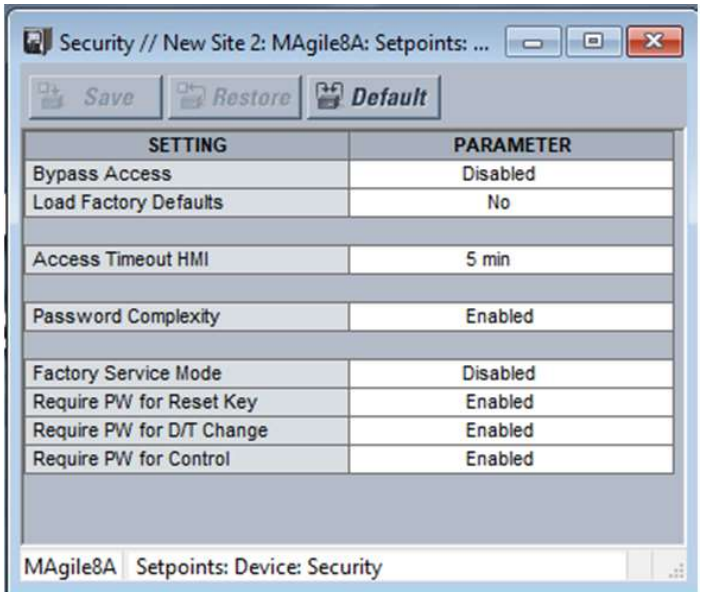
8.1. Secure decommissioning - configuration and sensitive data

The goal of secure decommissioning is to prevent unauthorized disclosure of information.

The Multilin Agile IED can be decommissioned by turning off the power and disconnecting the wires.

To clear files and settings in an IED the privileged user can navigate to ***Setpoints/Device/Security***. And select “Load Factory Defaults“ = Yes.

The IED restarts and loads the factory default configuration, including communication settings and security passwords.



Note: For Multilin Agile IEDs, an ADMINISTRATOR role is needed to change this setting.

To clear the records in the IED

To clear files from the IED, the Multilin Agile IED supports various commands. For accessing these commands, navigate to ***Setpoints > Device > Clear Records*** and select the “CLEAR” command.

There are commands to clear individual files for (events, transient waveforms, fault report, data logger files). A single “CLEAR ALL RECORDS” command removes all files from the IED.

This behaviour is compliant with cybersecurity requirements in that it removes all customer-specific data from the IED.

Multilin Agile IEDs allow easy restoration of existing configurations. The Multilin Agile manual provides additional information about backing up and restoring configurations.

9. Secure Operation Guidelines

To ensure secure operation of the Multilin Agile IED, GE Vernova recommend that:

- Users are assigned a specific role at a level sufficient for the tasks they must perform.
- Users change their passwords when they believe there might be a possibility of unwanted disclosure.
- Default account passwords are changed before putting the IED into operation.
- Users log out of their session when finished (although an inactivity timeout can be set to automatically terminate user sessions).
- GE Vernova certificates are replaced with certificates provided by the end user.
- The product is never connected to a public network, nor the Internet.
- Only the required services are configured and enabled.
- Periodically review all user accounts and disable/remove those accounts that are not active.

10. Appendices

10.1. The secure development life cycle process: IEC 62443-4-1

The IEC 62443-4-1:2018 is an internationally and widely recognized standard, which specifies the process requirement for the secure development of products used in industrial automation and control systems. The life-cycle description includes security requirements definition, secure design, secure implementation (including coding guidelines), verification and validation, defect management, patch management and product end-of-life.

In ongoing efforts to support our customers and their challenges, Grid Solutions is pleased to announce that it has achieved IEC 62443-4-1 certification. This certification ensures that a secure development lifecycle process is well defined, implemented and enforced across all the product's lifespan - from the design to the end-of-life cycle.

10.2. Certification: IEC 27001

ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system within the context of the organization.

GE Vernova has a culture of cybersecurity and is committed to protect its own and its customers data. The Multilin Agile IED manufacturing site is IEC 27001:2013 compliant.

10.3. Achilles ACC Level 1 certification

The D&I IED platform have obtained Achilles ACC Level 1 certification.

The certification acknowledges that this IED operation goes back to normal when the communication stress test is removed. The Multilin Agile IED is part of the D&I platform.

10.4. List of supported protocols

For Multilin Agile IEDs, communication protocols are supported based on software options in the order code. The following table shows protocols, ports used, and their default configuration.

The IED supports the ability to turn off any of the following specific physical ports:

- Front USB port
- Rear port RS485
- Ethernet port

The IED supports the ability to turn off any of the following specific communication protocols:

- IEC 61850 (MMS and GOOSE)
- MODBUS RTU
- MODBUS TCP
- DNP3oE
- DNP3 Serial
- IEC 60870-5-103
- TFTP

Time synchronization protocols can be selectively enabled/disabled based on the configuration.

- IRIG-B
- PTP-1588
- SNTP

All the ports that are enabled by default cannot be disabled by design as they are a core service required for the reliable function of the IED. The following table details the port/service list that would enable a user to facilitate port control through a firewall device found in their ESP.

S. No.	Services	Port Type	Port Numbers	Default	Configurable Port Numbers
1	MODBUS/TCP	TCP	502	Enabled	Yes
2	DNP3oE	TCP	20000	Disabled	Yes
3		UDP	20000	Disabled	Yes
4	IEC61850 (MMS)	TCP	102	Enabled	No
5	TFTP	UDP	69	Enabled	No
6	SFTP (SSH)	TCP	22	Enabled	No
7	GRPC/TLS	TCP	10000	Enabled	No

Note: *TFTP is only available in the basic security cortec. It is not available in the advanced security cortec.*

10.5. Resource management

The Multilin Agile ensures that the security function does not interfere with operations, by using the following features:

- Circular local security events file (protect against filesystem over usage)
- Multiple Ethernet ports which allow for setting a dedicated management interface

10.6. IEC 62443-4-1 mapping

This SDG (Secure Deployment Guide) provides alignment with IEC 62443-4-1 requirements as shown in the table below:

SG-1	Product defense-in-depth	Section 2: Product Defence-in-Depth strategy
SG-2	Defense-in-depth measures expected in the environment	Section 3: Environment
SG-3	Security hardening guidelines	Section 5: Secure Installation Hardening Section 7: Maintaining Security
SG-4	Secure disposal guidelines	Section 8: Decommissioning
SG-5	Secure operation guidelines	Section 9: Secure Operation Guidelines
SG-6	Account management guidelines	Section 4: Secure Installation - Hardening
SG-7	Documentation review	Covered by NPI process and quality processes

11. List of Acronyms

ESP - Electronic Security Perimeter
PSIRT - Product Security Incident Response Team
RBAC - Role Based Access Control
OC - Order Code