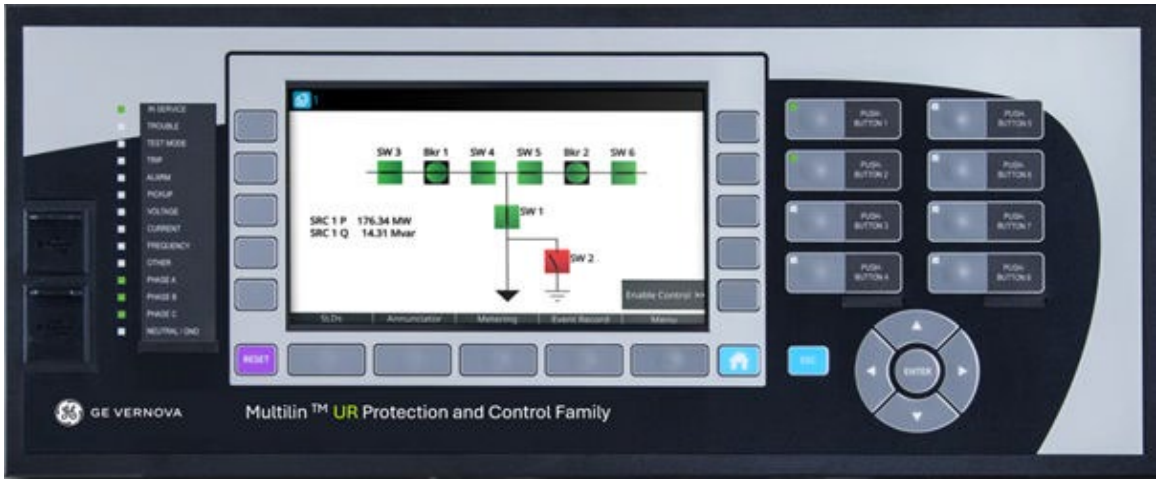
GE VERNOVA

Secure Deployment Guide

UR Family version 8.7x

GE Publication Number: SDG-1601-0910-87x-1

Publication Date: December 2025



Cybersecurity disclaimer

The UR family of products are intelligent electronic devices (or relays), designed to be installed and operated in utility substations and industrial plant environments and connected to secure private networks. These products should not be connected to the public internet.

We strongly recommend that you protect your digital devices using a **Defence-in-Depth** strategy. This will protect your products, your network, your systems and your interfaces against cyber security threats. This includes, but is not limited to:

- Placing digital devices 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.

The relays are available with an optional software option, which provides additional cybersecurity mechanisms to help you protect against cybersecurity intrusion. We strongly recommend using this “CyberSentry” option.

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

As a user, it is your sole responsibility to make sure that all UR Family relays 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 best practices to securely install and operate your product with the relevant setup software. It also provides an overview of the supported cybersecurity features.

There are three cybersecurity options: Basic, CyberSentry Lvl-1 (level 1), and CyberSentry Lvl-2 (level 2). This document covers all security variations with information on the recommended configurations.

With the basic cybersecurity option, the product provides a range of effective advanced security controls including:

- Lockout
- Dual permission security access

The UR Family of relays with a CyberSentry order code option offers enhanced security. This is a software option that provides advanced security features with role-based access control, centralized authentication and system level syslog reporting.

With CyberSentry level 1, the product supports:

- Centralized authentication
- Encrypted data transmission over Ethernet
- Security event reporting through the Syslog protocol
- Logging security events in the syslog format and configured syslog server

With CyberSentry level 2, the product supports:

- All the features provided by CyberSentry level 1
- Communication using Secure R-GOOSE supporting authentication and encryption of machine-to-machine (M2M) communication, as described in IEC 62351-9

1.1. Intended Audience

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

1.2. Additional Documentation

Along with 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.
- Password and user account policies, to prevent use of weak passwords.
- 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).
- In relays with CyberSentry, role-based access control, to enforce correct privileges in accordance with the area of responsibility.
- In relays with CyberSentry, centralized user management (using RADIUS), to allow prompt removal of user accounts.

To complement the defence-in-depth strategy, the product must be installed in a secure environment.

3. Environment

The product and associated setup 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.

We recommend that your security concept considers the whole system, in which the relays 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 devices, such as the UR 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 device must be done from a secure engineering workstation through a trusted network link.
- 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 devices.

4. Secure Installation - Hardening

4.1. Verifying software integrity

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

GE 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.

As part of the “Secure Firmware Upgrade”, the firmware integrity and authenticity are verified before upgrading the firmware in the relay.

4.2. Upgrading firmware to the latest version

We 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.

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

4.2.1. Disable unused protocols and ports

The relay 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 settings screen at the path:

`SETTINGS > PRODUCT SETUP > COMMUNICATIONS`

In compliance with NERC-CIP, most of the logical ports can be configured (they can be enabled or disabled). We recommend that you disable the protocols and logical ports that will not be used. The logical port details can be found in the section “Supported Protocols”

4.3. CyberSentry Level 1 and Level 2

4.3.1. Modify default passwords

UR relays with the CyberSentry Level 1 and 2 (CyberSentry Lvl 1 and Lvl 2) security option supports pre-defined user roles: Administrator, Engineer, Supervisor, Operator, Observer.

For device authentication, role passwords are stored securely on the device. The usernames are the same as the roles when the user accounts are maintained on the relay. All accounts, except Observer, have default password as **ChangeMe1#**.

When you receive a UR relay, we recommend that you log into the relay using the default password and change the passwords using unique strings for all the accounts using the path:

`SETTINGS > PRODUCT SETUP > SECURITY`

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

Relays with the CyberSentry security option support device 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 RADIUS server. In such a case, the password can be modified directly on the RADIUS server.

4.3.2. Create non-shared user accounts

UR relays with the CyberSentry (Level 1 as well as Level 2) security option support centralized or server authentication using a RADIUS server. This enables users to have non-shared accounts with

restricted privileges. You can configure each user account with any of the roles: Administrator, Engineer, Supervisor, Operator, Observer.

We recommend that you remove unused accounts from the server configuration. Only active accounts should be maintained.

4.4. Basic security: Configure Settings & Commands password

Relays with basic security support password security. This allows you to configure setting and command passwords.

4.4.1. Setting Password

This defines whether a user is permitted to make any changes to any of the setting values:

- Change any setting
- Test mode operation

There are two setting passwords based on the interface used for connecting to the relay.

- ***Local Settings*** password
- ***Remote settings*** password

4.4.2. Command Password

This defines whether a user is permitted to perform the following operations:

- Change the state of virtual inputs
- Clear the event records.
- Clear the oscillography records.
- Change the date and time.
- Clear the breaker arcing current.
- Clear the data logger.
- Clear the user-programmable pushbutton states.

There are two command passwords based on the interface used for connecting to the relay.

- ***Local Commands*** password
- ***Remote Commands*** password

With the basic security option, we recommend that you set unique passwords in compliance with password complexity rules.

Settings and Command passwords can be modified from EnerVista from the setting screen.

`SETTINGS > PRODUCT SETUP > SECURITY` by clicking the **CHANGE** button for the Command Password or Setting Password. The type of connection to the relay, local (RS232 or USB) or remote (Ethernet or RS485), determines whether the local or remote settings and commands passwords are changed, respectively.

5. CyberSentry: (Lvl-1 & Lvl-2) Secure Installation

5.1. Security recommendations

The UR relays offer flexible modification possibilities for the security configuration based on the user's setup and policies. We recommend the following configuration:

- Supervisor Role: When suitable, enable the "Supervisor" role.
- Serial Inactivity timeout: We recommended a value of at least 3 minutes.
- Ethernet inactivity timeout: Fixed at 2 minutes.
- Maximum number of failed logins attempts before account locking (Setting name: "Session Lockout"): We recommend a value of 3.
- Session Lockout Period: This is the duration that a user is prevented from logging in after being locked out. We recommend a value of 3 minutes.
- Factory Service Mode: Set to "Disabled" during normal operations.
- Lock Firmware: Set to "Enabled" to ensure that undesired firmware upgrade attempts are avoided.
- Communication ports: Disable communications ports and protocols when not used.
- Security bypass option: Do not use this during normal operation.
- Remote / centralized authentication server: Use this where possible.
- With Cyber Sentry level 2, we recommend configuration of redundant KDC servers for uninterrupted, encrypted and signed Routable GOOSE messages.

All security settings are explained in the product manual.

5.2. Bypass access:

The **Bypass Access** feature provides access to all users without any authentication and access control for special situations (when this is considered secure". If ***Bypass Access*** is set to "Remote" or "Local & Remote" then communication between the URPC and the UR relay is without any encryption.

By default, this feature is disabled and only the Supervisor, or the Administrator (when the Supervisor role is disabled), can enable this feature.

We strongly recommend that you keep the **Bypass Access** setting disabled when the UR relay is in service. It is important to ensure role-based access control is in place and unauthorized personnel are not allowed to modify the configuration or enter commands.

If **Bypass access** is enabled, you can configure this setting to the following options:

- *Local*: Bypasses authentication for the push buttons, the keypad, and the RS232 and RS485 communication ports.
- *Remote*: Bypasses authentication for the Ethernet ports
- *Local and Remote*: Bypasses authentication for both the above
- *Pushbuttons*: Bypasses authentication for the front panel push buttons only. On the graphical front panel, this also bypasses the authentication for the side pushbuttons, which control the breakers and disconnect switches.

5.3. Reset Key Access

When enabled, this setting allows the execution of the RESET key on the front panel without user authentication.

Note: The Reset key resets the LED and latched target messages on the front panel.

By default, the ***Reset Key Access*** setting is disabled. In this case, you will need to be authenticated and authorized to execute the RESET command.

We strongly recommend keeping the ***Reset Key Access*** setting disabled and enable it only for necessary limited time periods (when it is secure to do so).

5.4. Device Authentication

The ***Device Authentication*** setting is enabled by default. When enabled, device authentication uses local predefined users and roles. If a match is not found and centralized authentication is configured, then the device will attempt to authenticate users on the RADIUS server.

If this setting is disabled, the device only uses the centralized authentication server (RADIUS). It is important to ensure that the RADIUS server is configured and reachable before disabling device authentication.

When device authentication is disabled, only the Administrator and Supervisor have the permission to re-enable it.

We recommend that you set this to `Yes`.

Notes:

In Device Authentication mode, the Observer role does not have a password associated with it.In Server Authentication mode the Observer role requires a password.

5.5. RADIUS authentication

UR relays with the CyberSentry security option support both device level authentication and server authentication. We recommend using the server authentication feature as this offers easier user database management and helps with the maintenance of non-shared user accounts.

You can use Enervista URPC Setup configuration software to configure RADIUS authentication (settings: ***Server IP***, ***Port***, ***Vendor ID***, ***Timeout and Retries***, ***Shared Secret***).

You can configure user credentials directly in the authentication server.

Note: Relays using basic security do not support this feature.

5.6. Secure event logging

5.6.1. Syslog server

The advanced security option supports Syslog over UDP.

The device captures security-related events and sends these to a centralized syslog server (assuming a syslog server is configured and reachable). We recommend 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. All severity levels follow RFC 5424.

For a list of security events and their severity, please refer to the product manual.

5.6.2. Security events storage on relay

Security events are saved in the following files:

- `SECURITY_EVENTS.CSV`
- `SETTING_CHANGES.LOG`

Both files store 1024 events in a circular buffer format. Once the file reaches its maximum capacity, the oldest event gets overwritten by the newest event.

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

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

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

Please refer to the instruction manual of the product for further information.

The `SETTINGS_CHANGES.Log` file captures all setting changes performed, along with the Date and Time stamp, Old Value, New Value, & Modbus address.

Due to capacity limitations and the nature of the circular buffer, we recommend that you download and archive these files in a secure place for auditing purposes, at regular intervals.

5.7. Self-tests

The UR CyberSentry Level 1 option provides the following user-configurable self-tests:

FAILED AUTHENTICATE: If this setting is enabled, the number of failed authentications is compared with the Session Lockout threshold. When the Session Lockout threshold is exceeded, a minor alarm indication is asserted.

FIRMWARE LOCK: If this setting is Enabled, then any firmware upgrade operation attempt when the Lock Relay setting is enabled brings up this self-test alarm.

SETTINGS LOCK: If this setting is Enabled then an unauthorized write attempt to a setting for a given role activates this self-test

5.8. Maximum user connections to relay

At any given time, a single user with role “Administrator”, “Engineer” or “Operator”, or multiple users with the role “Observer” can connect to relay. A user with role “Observer” is only permitted to view actual values and the relay configuration. The maximum number of connections to relay are limited by the number of total Modbus connections supported, up to 4.

5.9. Role permission mapping

The following roles are supported:

- Administrator
- Engineer
- Supervisor
- Operator
- Observer

For details of permissions associated with each role, refer to the relevant product manual.

6. Cyber Sentry level 2 (Secure R-GOOSE):

A UR relay with Cyber Sentry level 2 software option supports the same set of security features as CyberSentry level 1 plus various protocols allowing the IED to connect to a Key Distribution Centre (KDC) Server. This allows:

- Verification of the KDC certificate
- The use of Retrieve Keys
- Establishment of a secure channel
- Transmission of R-GOOSE traffic using symmetric keys for encryption and signature (based on the user configuration).

The UR instruction manual contains all the details concerning this process, including:

- Configuration settings for SCEP (Simple Certificate Enrollment Protocol) server
- OCSP (Online Certificate Status Protocol)
- KDC (Key Distribution Center) servers.
- Supported algorithms

GOOSE messages are at Layer 2 of the OSI model and are therefore not recognised by routers, which operate at Layer 3. The GOOSE messages are therefore confined to the substation local network (LAN).

R-GOOSE messages, on the other hand, are GOOSE messages encapsulated within Layer 3 protocols (UDP/IP). R-GOOSE messages are therefore designed for multicasting over different networks (WAN). For WAN communication, confidentiality and authenticity of messages becomes even more important, because important information is sent beyond the local area network using applications that work at Layer 3. The necessary level of security is achieved by encryption and signature. The IEC62351-9 standard covers key management aspects in power systems.

The security configuration of R-GOOSE messages is available at ***SETTINGS > PRODUCT SETUP > SECURITY > SECURITY M2M***. Details are covered in the UR instruction manual.

We strongly recommend using the secure version of routable GOOSE messages when transferring information in a Wide Area Network.

7. Basic Security: Secure Installation

The Products provide “basic security” as the default security option. This supports password security, access timeout and user lockout features.

Products with basic security offer flexible modification possibilities for the security configuration based on the user’s setup and policies. We recommend the following configuration:

- Maximum number of failed logins attempts before account locking (Setting name: “Session Lockout”): We recommend a value of 3.
- Password Lockout Period: This is the duration that a user is prevented from logging in after being locked out. We recommended a value of 5 minutes.
- Factory Service Mode: Set to “Disabled” during normal operations.
- Lock Firmware: Set to “Enabled” to ensure that undesired firmware upgrade attempts are avoided.
- Access level timeout: We recommend a value of 30 minutes.
- Command access level timeout We recommend a value of 5 minutes.
- Communication ports: Disable communications ports and protocols when not used.

Each security setting and corresponding functionality is explained in the product manual.

UR relays with basic security support separate passwords for communication over “local” interface and “remote” interface. This applies for modification of settings and execution of commands.

- Local interface is defined as access to settings or commands via the front panel. This includes both keypad entry and the RS232 port or USB port.
- Remote access is defined as access to settings or commands via any rear communications port. This includes both Ethernet and RS485 connections.

7.1. Local Setting Authorized:

This configuration can be set at ***SETTINGS > PRODUCT SETUP > SECURITY > DUAL PERMISSION SECURITY ACCESS***.

You can configure any flex-operand to this setting. If the configured flex-operand value is “On” then local password-based authentication is needed for any setting change through the local interface.

By default, this setting is set to “On”.

7.2. Remote Setting Authorized:

This configuration can be set at ***SETTINGS > PRODUCT SETUP > SECURITY > DUAL PERMISSION SECURITY ACCESS***.

You can configure any flex-operand to this setting. If the configured flex-operand value is “On” then remote password-based authentication is needed for any setting change through remote interface.

By default, this setting is configured to “On”

7.3. Access Level:

This setting allows you to select the level of access required from the front panel. You can select one of the following options:

- Restricted
- Setting
- Command
- Factory

The access level is set to “Restricted” by default. The "Restricted" option means that settings and commands can be accessed, but there is no access to factory configuration.

The access level” automatically reverts to the restricted level according to the access level timeout setting value.

There are two user security access levels for which you can set a password for each: “setting” and “command”. Using a password for each level controls whether users can enter commands or change settings. Another option is to specify setting and command access for individual user accounts.

The "Factory Service" level is not available for customers and intended for factory use only.

8. Setup Software

The EnerVista Setup software is configuration and monitoring software designed to be used with the relays. With this, you can manage offline projects, connect to the relay, update the device configuration, monitor system data and conveniently view diagnostics sequence of events and COMTRADE. You can also upgrade the relay's firmware.

Enervista Setup is digitally signed software.

8.1. Secure firmware upgrade

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

The relays have a "Lock firmware" setting, which is enabled by default. In this scenario, firmware upgrades cannot be initiated. Before initiating a firmware upgrade, you must set this to "Disabled".

Firmware upgrades can only be performed by users with role "Administrator".

For relays with basic security, firmware upgrades can only be performed after providing the Settings password if it is set.

8.2. Secure Communication

When UR relay is with CyberSentry security option, Enervista URPC setup software tool communicates with the relay via a secure tunnelled channel using SSHv2. This makes sure that sensitive information cannot be disclosed to unauthorized personnel.

8.3. SSH server authentication

UR Setup 8.60 onwards provides SSH (Secure Shell) server authentication.

SSH provides a mechanism for establishing a cryptographically secured connection between the server (the relay, in our case) and the client (EnerVista UR Setup configuration SW tool). The user must provide a username and password to communicate with the relay. After successful authentication, the user is assigned a ROLE with predefined permissions.

From UR Setup 8.60 onwards, the first time you connect to a device, you will be asked to confirm validity of the UR device, based on a SSH key fingerprint. After a positive response, EnerVista UR Setup stores the SSH key fingerprint in the Windows registry. On subsequent connections, it compares the SSH key fingerprint with the stored value from the Windows registry and prompts the user if they are different.

The SSH server authentication function can be disabled through the Enervista menu, in ***File > Preferences > SSH Communication***. We highly recommend keeping it enabled to avoid Enervista communicating with rogue SSH servers.

9. Maintaining Security

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

9.1. 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.

9.2. 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.

9.3. Vulnerability monitoring and firmware updates

GE responsibly discloses vulnerabilities found on its products.

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

Users should define a security update policy.

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

9.4. Reporting a vulnerability

Providing a legitimate pathway for vulnerability disclosure is an essential link between GE 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.gevernova.com/security. Please do not include identifiable sensitive data (e.g. personal data, specific system configuration) within the body of the communication or any attachments (e.g. screenshots, images, or log files).

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

We 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 quickly.
- 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 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.

10. Decommissioning

10.1. Secure decommissioning: Configuration and Sensitive Data

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

The UR relay can be decommissioned by turning off the power and disconnecting the wires.

To clear files and settings in the in a relay with CyberSentry:

- On the UR front panel, navigate to `SETTINGS > PRODUCT SETUP > SECURITY > RESTORE DEFAULTS` and execute.
  The relay restarts and loads the factory default configuration, including communication settings and security passwords.

For CyberSentry UR relays, an Administrator role is needed to change this setting, and a supervisor role (if not disabled) approves it.

Alternatively:

- On the UR HMI, navigate to `COMMANDS > RELAY MAINTENANCE > SERVICE COMMAND`
- Enter the value 20511 and press the ENTER key.
  This can be used with basic security as well as CyberSentry UR order-code relay.

On execution of this service command, the relay configuration (including user passwords) is reset to its default values.

To clear the records in the relay

Navigate to `SETTINGS > PRODUCT COMMANDS` and select the `CLEAR RELAY RECORDS` command.

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

UR relays allow easy restoration of existing configurations. The UR Manual provides additional information about backing up and restoring configurations.

11. Secure Operation Guidelines

To ensure secure operation of the relay, we 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 device into operation.
- Users log out of their session when finished (although an inactivity timeout can be set to automatically terminate user sessions).
- GE certificates are replaced with certificates provided by the end user.
- The product is never connected to a public network, or to the Internet.
- Only the required services are configured and enabled.
- Periodically review all user accounts and disable / remove those accounts that are not active.

12. Appendices

12.1. The Secure Development Life Cycle process: IEC62443-4-1

The IEC62443-4-1:2018 is an internationally and widely recognized standard, which specifies 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.

12.2. Certification: IEC27001

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 has a culture of cybersecurity and is committed to protect its own and its customers data. Our UR relay manufacturing site is IEC27001:2013 compliant.

12.3. Achilles ACC Level 1 certification

The UR family of relays have obtained Achilles ACC Level 1 certification.

The certification acknowledges that UR relay operation goes back to normal when the communication stress test stops. During all the tests (storm as well as non-storm), control operation does not get impacted.

12.4. List of supported Protocols

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

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 device. 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 Numbers	Default Port Status	Configurable Port Numbers	Assigning 0 disables the port	Software Option Dependency
1	Modbus / TCP	502	Enabled	Yes	Yes	Not dependent on SW option
2	HTTP / TCP	80	Enabled	Yes	Yes	Not dependent on SW option
3	IEC 61850 (ISO-TSAP) / TCP	102	Disabled	No	No	IEC61850 option
4	PMU / TCP	4712	Enabled	Yes	Yes	PMU option
5	PMU / UDP1	4713	Enabled	Yes	Yes	PMU option
7	TFTP / UDP	69	Enabled	Yes	Yes	Not dependent on SW option
8	TFTP Data port / UDP (2)	0	Enabled	Yes	When not configured (default value = 0), the ephemeral port range of 49152 to 65535 is used.	Not dependent on SW option

S. No.	Services	Port Numbers	Default Port Status	Configurable Port Numbers	Assigning 0 disables the port	Software Option Dependency
9	DNP / TCP	20000	Disabled	Yes	Yes	Not dependent on SW option
10	DNP / UDP	20000	Disabled	Yes	Yes	Not dependent on SW option
11	IEC 60870-5-104 / TCP	2404	Disabled	Yes	Yes	Not dependent on SW option
12	SNTP1 / UDP	123	Disabled	Yes	No	Not dependent on SW option
13	SNTP2 / UDP	123	Disabled	Yes	No	Not dependent on SW option
14	EGD Data port / UDP	18246	Disabled	No	No	EGD option
15	SFTP/ SSH Port	22	Enabled	No	No	7.1x, 7.2x: Cybersentry option 7.3x and above: Not dependent on SW option
16	RADIUS	1812	Disabled	Yes	0 is out of range	Cybersentry option
17	Syslog/UDP	514	Disabled	Yes	0 is out of range	Cybersentry option
18	GDOI(ISAKMP)	500	Enabled	No	No	CyberSentry Level 2 (with GDOI)
19	GDOI	848	Enabled	No	No	CyberSentry Level 2 (with GDOI)

12.5. Resource Management

By using the following features, the UR family makes sure that the security function does not interfere with operations:

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

12.6. IEC62443-4-1 mapping.

This SDG (Secure Deployment Guide) provides alignment with IEC62443-4-1 requirements as shown in the table below.

SG-1 Product defence in depth	Section 2 Product Defence-in-Depth strategy
SG-2 Defence in depth measures expected in the environment	Section 3 Environment
SG-3 Security hardening guidelines	Section 4 Secure Installation - Hardening Section 9 Maintaining Security
SG-4 Secure disposal guidelines	Section 10 Decommissioning
SG-5 Secure operation guidelines	Section 11 Secure Operation Guidelines
SG-6 Account management guidelines	Section 4 Secure Installation - Hardening
SG-7 Documentation review	Covered by NPI process and quality processes.