ARCTEQ
PART OF ENSTO GROUP

Application Note

Cybersecurity for AQ-ONE and AQ 250 series devices



TABLE OF CONTENTS

1 Document information 3
1.1 Revision history 3
1.2 Notation 3
1.3 Notices, cautions, and warnings 3
2 Purpose and scope 5
3 Device identity and trust levels 6
4 Secure commissioning and initial configuration 8
5 Communication ports and services 9
6 Time synchronization 11
7 User Access Control (UAC) and role management 12
8 Firmware updates 14
9 Logging and auditing 15
10 Recovery Plan 16
11 Summary of recommendations 17
12 Contact information 18

©Arcteq Relays Ltd.

DISCLAIMER AND COPYRIGHT

Please read this document carefully before using the equipment or taking any other actions with respect to the equipment. Only trained and qualified persons are allowed to perform installation, operation, service or maintenance of the equipment. Such qualified persons have the responsibility to take all appropriate measures, including e.g. use of authentication, encryption, anti-virus programs, safe switching programs etc. necessary to ensure a safe and secure environment and usability of the equipment. The warranty granted to the equipment remains in force only provided that any instructions and additional information contained in this document have been strictly complied with.

Nothing contained in this document shall increase the liability or extend the warranty obligations of the manufacturer Arcteq Relays Ltd. The manufacturer expressly disclaims any and all liability for any damages and/or losses caused due to a failure to comply with the instructions and additional information contained herein or caused by persons who do not fulfil the aforementioned requirements. Furthermore, the manufacturer shall not be liable for possible errors in this document.

Please note that you must always comply with applicable local legislation and regulations. The manufacturer gives no warranties that the content of this document is in all respects in line with local laws and regulations and assumes no liability for such possible deviations.

You are advised to notify the manufacturer in case you become aware of any errors in this document or of defects in the equipment.

The manufacturer reserves the right to update or amend this document at any time.

Copyright © Arcteq Relays Ltd. 2026. All rights reserved.

1 DOCUMENT INFORMATION

1.1 Revision history

Table 1. *Revision history for this document.*

Revision	**1.0**
Date	22 May 2025
Changes	▪ (N/A; the first revision of the document.)
Revision	**1.1**
Date	19 May 2026
Changes	▪ Updated the layout. ▪ Added the following pages: cover, Table of contents, Disclaimer and copyright, Document information, & Contact information. ▪ Added the chapter “Recovery Plan”. ▪ Added notices, cautions, and warnings throughout the document where necessary. ▪ Added Figures 1 and 6.
Revision	**1.2**
Date	3 November 2026
Changes	▪ Updated the cover to include AQ-ONE. ▪ Updated the text to include AQ-ONE throughout the document. ▪ Updated the “AQtivate 200” name to “AQtivate” throughout the document.

1.2 Notation

This document uses the following notation for the various sections in the AQtivate 200 configuration and setting software as well as the keyboard:

- Navigation paths are in italics (e.g. *Tools → Events and Logs → Event History*).
- AQtivate 200 main menus are in bold (e.g. the **Protection** menu).
- Tabs are in italics (e.g. the *Line Protection Module* tab).
- Section names within tabs are in single quotation marks (e.g. the ‘CB control block’ support functionality)
- Parameter names are in bold and italics (e.g. the ***Master node status*** parameter).
- Parameter drop-down menu items and text values are in double quotation marks (e.g. “Sub-unit”).

1.3 Notices, cautions, and warnings

This document uses the following notices, cautions, and warnings to highlight information that is especially important for the user.

Table 2. *Highlighting symbols that can be used in this document.*

Symbol	Description
	**NOTICE!** These messages indicate relevant factors and conditions to the concept discussed in the text, as well as other relevant advice.
	**CAUTION!** These messages indicate a potentially hazardous situation which, if not avoided, could result in personal injury, equipment/property damage, or software corruption.
	**DANGER!** These messages indicate a hazardous situation which, if not avoided, could result in serious personal injury or death.

2 PURPOSE AND SCOPE

This document provides technical guidance for securely configuring and operating both AQ-ONE and AQ 250 series devices. It is intended for system integrators, control engineers, and commissioning technicians responsible for deploying and maintaining the device in industrial control systems.

The guide covers cybersecurity practices during engineering, installation, and commissioning phases, as well as ongoing operations. It includes instructions for securing both local access through the Human-Machine Interface (HMI) and remote access through the AQtivate software.

The device is designed for use in isolated networks which have no direct internet connectivity. The device should be installed behind a firewall and only communicate with equipment within the same zone.

If you have discovered a security vulnerability in any of our products, services, or systems, we encourage you to report it to us according to our Vulnerability Disclosure Policy.

Firmware updates are released as frequently as necessary based on exposed vulnerabilities. The latest firmware update must be applied as soon as possible to minimize the risk of a possible cyberattack.

The minimum firmware requirement to cover all cybersecurity features described herein is **v2.5.7.1-AP2**. The minimum AQtivate software requirement is **v1.5.4.**

3 DEVICE IDENTITY AND TRUST LEVELS

All new devices are shipped with factory-installed host certificates, which are used to establish the device's authenticity during communication with the configuration software. Each certificate is unique and signed by Arcteq's root certificate authority. These host certificates serve as a trusted identity for the device. When a connection is established, the configuration software verifies the device's certificate signature against the embedded root key.

Devices that have been updated from non-secure firmware versions (prior to v2.5.7.1-AP2) were not provisioned with a secure identity at the time of manufacture. Although these devices can be upgraded to a secure firmware version, they lack verifiable certificate chains and instead rely on self-signed certificates. Self-signed certificates allow encrypted communication and integrity checks, but they do not prove the authenticity of the device. The configuration software cannot verify whether the device is genuine or potentially compromised.

Only devices that either shipped with secure firmware and factory certificates, or have been correctly re-provisioned by Arcteq, are recognized as compliant with the current security model.

Information about the certificates of the currently connected device can be seen from the lock icon next to the IP address (see Figure 1 below).

Figure 1. *Location of the certificate icon in AQtivate.*



There are three different levels of trust for the communication, as shown in the thermometer to the right of the lock icon. When the lowest third of the thermometer is white, the device has an older firmware; when the both the bottom and the middle parts are in yellow, the device has been updated from a non-secure firmware version; and when all three parts are in green, the device has been signed by Arcteq's production team. Please refer to the following page for Figure 2–4 for examples of each situation.

Figure 2. *Device with older firmware.*

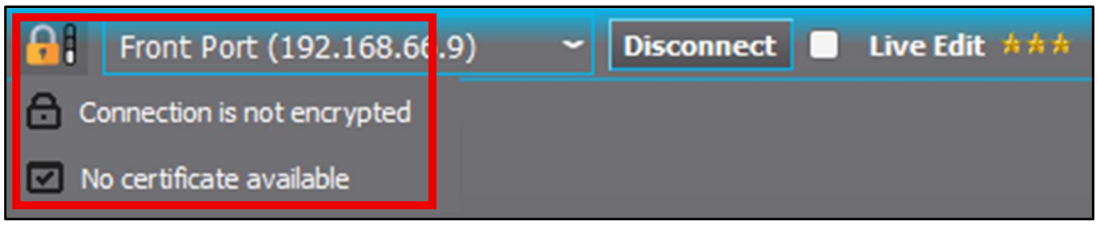


Figure 3. *Device which has been updated from a non-secure firmware version.*

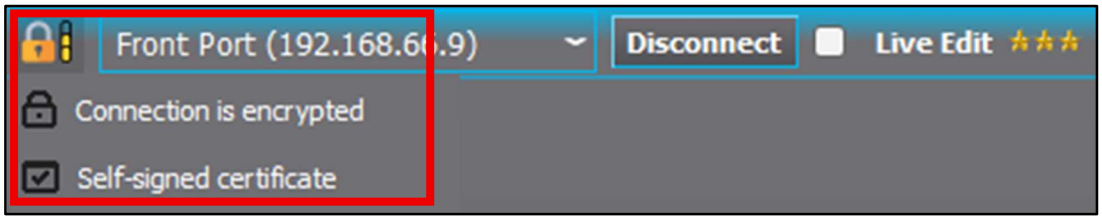
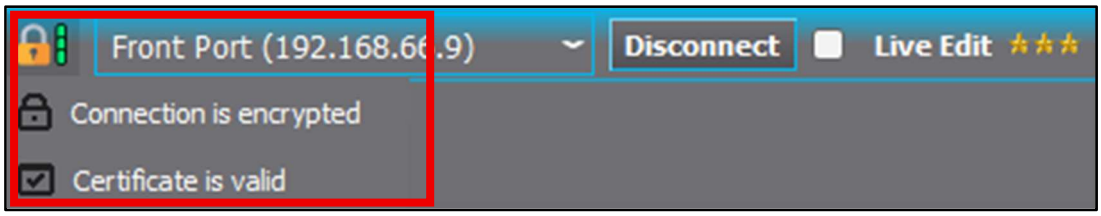


Figure 4. *Device which has been signed by Arcteq.*



4 SECURE COMMISSIONING AND INITIAL CONFIGURATION

Upon receiving the device, the first step is to ensure that both the AQtivate software and the device's firmware are up to date. The latest software for both are available in the Customer corner section of our website (arcteq.com/customer-corner/).

During setup, connect to the device via the configuration software using an isolated engineering workstation. Ensure that the workstation is clean, patched, and not connected to any internet-facing networks.

To ensure best security practices during initial configuration, use the front service port for this connection, as it provides a direct and controlled interface to the device. All other external communication interfaces should remain disconnected until the device has been fully configured and secured. The communication channel between the configuration software and the device is protected using TLS 1.3.



CAUTION!
The front port should never be connected to any external systems!

5 COMMUNICATION PORTS AND SERVICES

During engineering, only the necessary ports required for operation should be enabled, and unused interfaces should remain disabled throughout the lifecycle of the device.

The device uses the following ports by default, as listed in Table 3 below:

Table 3. *Default ports.*

Port	Direction	Protocol	Service	Comment
21	IN	TCP	FTP	Disturbance record transfer, read-only
6969	IN	TCP	SSH / SFTP	Arcteq maintenance access (on front port only)
1551	IN	TCP		Configuration/parametrization (AQtivate 200) with TLS 1.3
1552	IN	TCP		AQPro with TLS 1.3 (disabled by default)
4321	IN	UDP		Arcteq proprietary protocol for device discovery and network loop detection

These services can be configured in AQtivate (**Communication** main menu → *Connections* tab → 'Ethernet Security Settings' section) as shown in Figure 5 below. Each service can be disabled independently. Additionally, you can disable the Ethernet interfaces completely.

Figure 5. *Ethernet security settings in AQtivate.*



All communication protocols are disabled by default. They can be enabled from the **Communication** main menu, in the *Protocols* tab. The default communication ports have been listed in Table 4 on the following page:

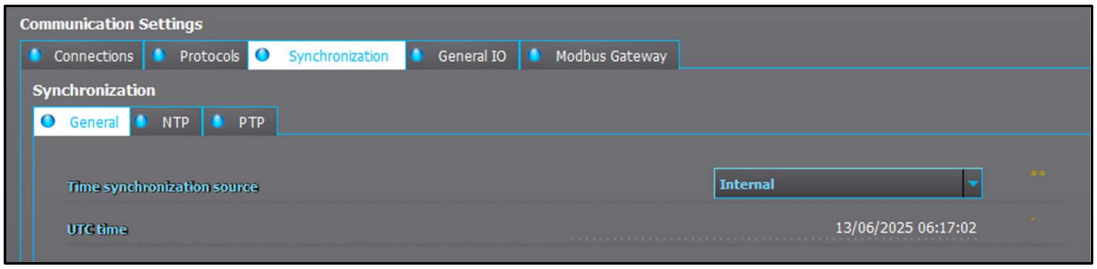
Table 4. *Default communication ports.*

Port	Direction	Protocol	Service	Comment
102	IN	TCP	IEC 61850	IEC 61850
502	IN	TCP	Modbus	Modbus TCP
2404	IN	TCP	IEC 104	IEC 60870-5-104
20000	IN	TCP	DNP	DNP3 TCP
		NA	GOOSE	IEC 61850 GOOSE, Layer 2

6 TIME SYNCHRONIZATION

Different time synchronization methods can be enabled in the **Communication** main menu, in the *Synchronization* tab (see Figure 6 below).

Figure 6. *Time synchronization settings in AQtivate.*



Accurate time is essential for security functions like logging and certificate validation. On boot, the device attempts to sync with the configured NTP server. For higher precision, PTP is also supported.

The time synchronization ports have been listed in Table 5 below:

Table 5. *Time synchronization ports.*

Port	Direction	Protocol	Service	Comment
123	OUT	UDP	NTP	Time synchronization
		NA	NTP	Precision Time Protocol, Layer 2

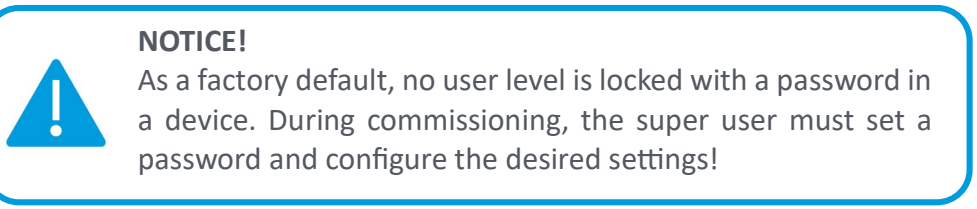
NOTICE!
The protection device also uses Layer 2 for services like GOOSE and PTP time synchronization, which should be considered in the network design!

7 USER ACCESS CONTROL (UAC) AND ROLE MANAGEMENT

The device supports a four-tier User Access Control (UAC) model.

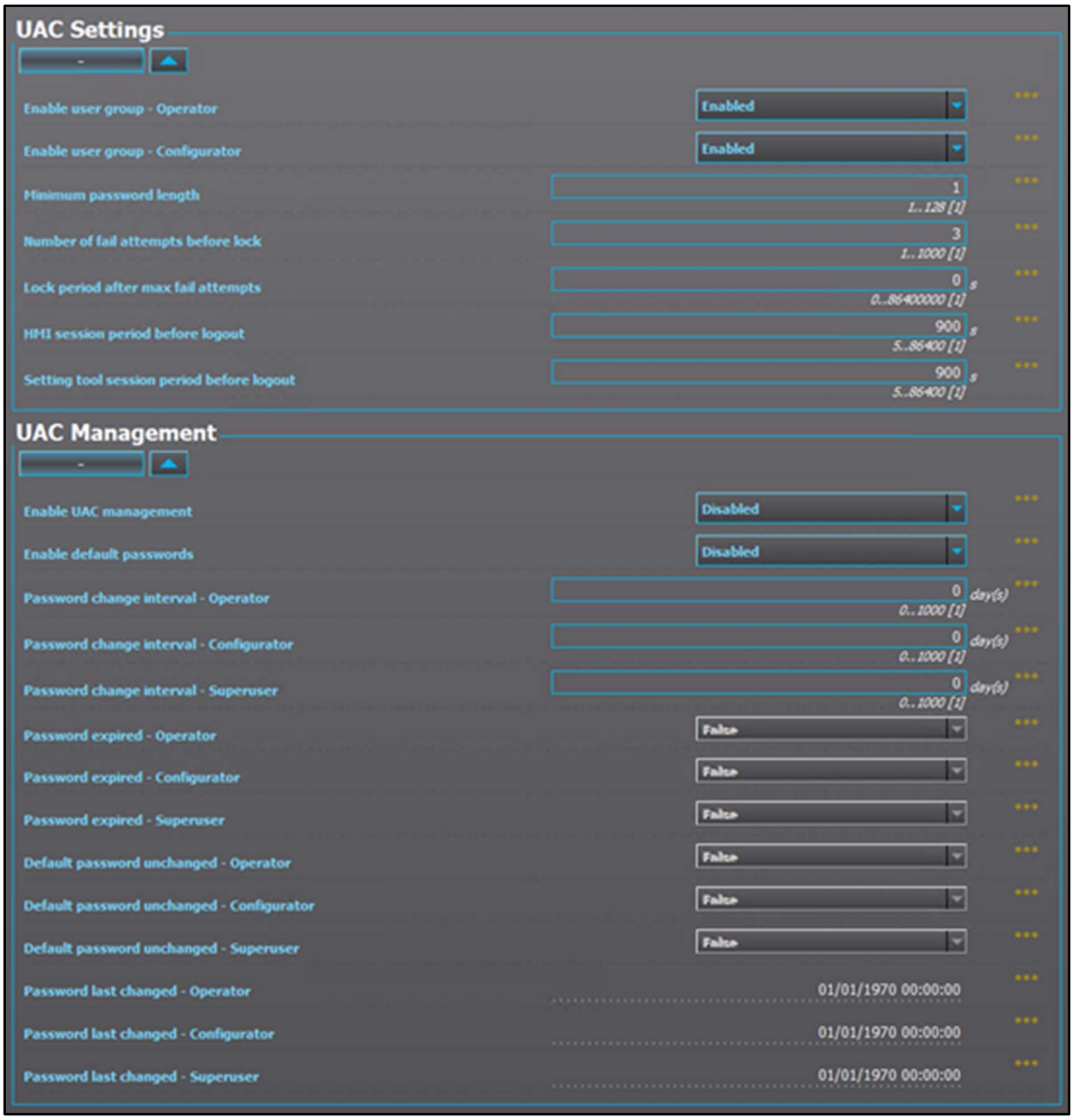
The following roles are predefined:

- User: Can view any menus and settings but cannot change any settings. Cannot operate breakers or other equipment.
- Operator: Can view any menus and settings but cannot change any settings. Can operate breakers and other equipment.
- Configurator: Can change most settings such as basic protection pick-up levels or time delays, breaker control functions, signal descriptions etc. and can operate breakers and other equipment.
- Super user: Can change any setting and can operate breakers and other equipment.



User Access Control settings can be found in the **Monitoring** main menu, in the *User Access Control* tab (see Figure 7 on the following page).

Figure 7. *User Access Control settings in AQtivate.*



8 FIRMWARE UPDATES

The devices can only be updated using digitally signed packages issued by Arcteq. Updates are installed through the configuration software. Before applying any update, the device performs a chain-of-trust validation using embedded cryptographic keys. Any update that fails signature verification is rejected.



NOTICE!
Before updates, back up the configuration settings to a secure workstation. After an update the settings should be thoroughly reviewed to ensure that the device operates according to the intended configuration and security requirements!

9 LOGGING AND AUDITING

The device maintains an internal log of system events, security actions, and user access records. These logs are accessible through the configuration software.

Audit logs should be reviewed periodically to identify anomalies. Engineers should also verify that the internal clock is synchronized with an external time synchronization to maintain accurate timestamping.

10 RECOVERY PLAN

In the event of a suspected compromise or malicious attack against a device, follow the recovery procedure below.

1. Isolate the device. Disconnect the device from all networks. Do not power it off.
2. Document symptoms. Note what triggered suspicion (unexpected behavior, unusual traffic, tamper evidence) with timestamps. Note the device serial number and firmware version.
3. Contact us and ship the device to us for hardware-level inspection and re-provisioning. This is the only way to fully ensure the device is safe.
4. If return is not possible perform a field reset.



NOTICE!
Field reset doesn't detect hardware tampering or modifications below the firmware layer. Factory hardware inspection is the only way to fully verify device integrity.

   - Using an isolated laptop not connected to any networks, try to obtain the current configuration from the device using AQtivate software for forensics analysis.
   - Perform a factory reset.
   - From a separate trusted computer, download the latest firmware from our website. Transfer it to the isolated laptop via USB drive and re-flash using the "Upgrade firmware" functionality in AQtivate. Do not reuse local copies of the firmware, always download fresh to ensure the files have not been tampered with.
   - Rotate all credentials and keys used.
5. Revoke access. Regardless of path chosen, revoke all credentials and keys the device had access to and monitor connected systems for anomalous activity.

11 SUMMARY OF RECOMMENDATIONS

To maintain a secure deployment of your devices, configuration engineers must:

- Disable all unused services and ports.
- Define and implement user access control policies.
- Regularly update firmware using signed packages issued by Arcteq.
- Back up configuration settings before applying updates.
- Review settings after an update to ensure they align with security requirements.
- Periodically review audit logs to identify and address anomalies.
- Ensure device clock is synchronized with external time sources for accurate logging.
- If you suspect a device has been compromised, follow the recovery plan

By following the procedures in this document, you will ensure the device operates securely and remains resilient against internal threats and misconfigurations.

12 CONTACT INFORMATION

Support portal: arcteq.com/support
Support line: +358 10 3221 388 (EET 9:00–17:00)
Address: Kvartsikatu 2 A 1
65300, Vaasa, FINLAND
Phone: +358 10 3221 370 (EET 9:00–17:00)
Email address: sales@arcteq.com