ARCTEQ
PART OF ENSTO GROUP

AQ 300

Cybersecurity and connectivity guide

TABLE OF CONTENTS

DISCLAIMER AND COPYRIGHT

Please read these instructions 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 the instructions 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 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.

DOCUMENT INFORMATION

Revision	1.00
Date	10 February 2026
Changes	First revision of the document

This document contains important instructions that should be saved for future use. Read the document carefully before installing, operating, servicing, or maintaining this equipment. Please read and follow all the instructions carefully to prevent accidents, injury and damage to property.

"Notice" messages indicate relevant factors and conditions to the concept discussed in the text, as well as to other relevant advice.

"Caution" messages indicate a potentially hazardous situation which, if not avoided, **could** result in minor or moderate personal injury, in equipment/property damage, or software corruption.

"Warning" messages indicate a potentially hazardous situation which, if not avoided, **could** result in death or serious personal injury as well as serious damage to equipment/property.

These symbols are added throughout the document to ensure all users' personal safety and to avoid unintentional damage to the equipment or connected devices.

Please note that although these warnings relate to direct damage to personnel and/or equipment, it should be understood that operating damaged equipment may also lead to further, indirect damage to personnel and/or equipment. Therefore, we expect any user to fully comply with these special messages.

1 INTRODUCTION

The document describes the process for handling cybersecurity when communicating with the AQ 300 device. The document can be used as a technical guideline during the engineering, installation and commissioning phase, and during normal operation. It also provides technical guidance to operate the device locally with the LCD and remotely with a web browser.

The following enhanced security features are available:

- Secure software update with digital signatures via firmware files.
- Encrypted communication protocol available (such as HTTPS) in order to increase security of data transfer.
- User selectable access modes of the built-in web interface: enabled, disabled, read-only modes.
- Remote access could be allowed for dedicated clients only (Whitelist).
- All security-relevant events are logged in a non-erasable security log and these events can optionally be reported through syslog protocol to a remote log server.
- Security alarm indication.
- Device management and SCADA accesses can be controlled individually.
- Restriction of open TCP/UDP ports: all service ports can be managed via the web interface.
- Role-Based Access Control (RBAC) provides a permission model that allows access to AQ 300 series device operations and configurations based on specific roles and individual user accounts configured.
- Used passwords are stored in encrypted form and managed in this process that complies with the BDEW Whitepaper and NERC CIP recommendations.
- User password requirement according to IEEE 1686.
- Secure communication between the AQtivate 300 configuration software and the AQ 300 series device (configuration management via secured channel (HTTPS)).
- Secure configuration via digitally signed configuration file (epcs).
- The complete software for AQ 300 series devices is protected by digital signatures in order to detect malicious changes. Only such officially signed software components can be loaded and are executed in the device.

  - Optional CyberProtect functionality: Available Lightweight Directory Access Protocol (LDAP) to support authentication and authorization functions for Authentication Authorization Accounting (AAA) server.
  - Advanced user management with the ability to create user defined roles to manage user interactions with the device through user accounts.
  - Authentication transfer between devices allowing the user through import/export function.
- Secure IEC 61850 communication through IEC 61850 TLS.

These enhanced cybersecurity features have been developed in accordance with NERC-CIP, IEEE 1686, BDEW Whitepaper and IEC 62351-8 standards and recommendations.

The minimum firmware requirement to cover all cyber security features described herein is 2.10.2.3010. For the connectivity guide, the minimum version is 2.10.2.3013.

2 SECURE SYSTEM SETUP

2.1 AQ 300 malware detection

The AQ 300 device is based on an embedded Linux-based operating system. So far, Linux-based intelligent electronic devices are considered to be safer and less prone to cyber threats than their Windows counterparts. Moreover, the AQ 300 device is equipped with an internal firewall to protect against network attacks. This firewall is turned on by default to increase the device's standard protection.

Nevertheless, the device may contain unknown vulnerabilities. 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.

2.2 AQtivate 300 configuration software tool security

The AQtivate 300 configuration software tool is based on Windows operating systems. Therefore, in order to protect against malware infection, it is recommended to install an anti-virus tool with permanent updated anti-virus patterns.

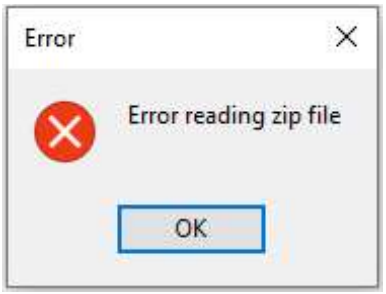
HTTPS with authentication/authorization connection is used to access AQ 300 devices from AQtivate 300 over standard TCP port 443 with secure communication via digitally signed .epcs configuration file. The less secure HTTP can also be used with the standard port 80.

2.3 Configuration file security

A configuration file readable by an AQ 300 device is signed with a .epcs extension and cannot be edited with any software except AQtivate 300. The configuration file is encrypted using CRC code calculation. Any tampering or corruption of the .epcs file is detected by AQtivate 300 and warning messages are given.

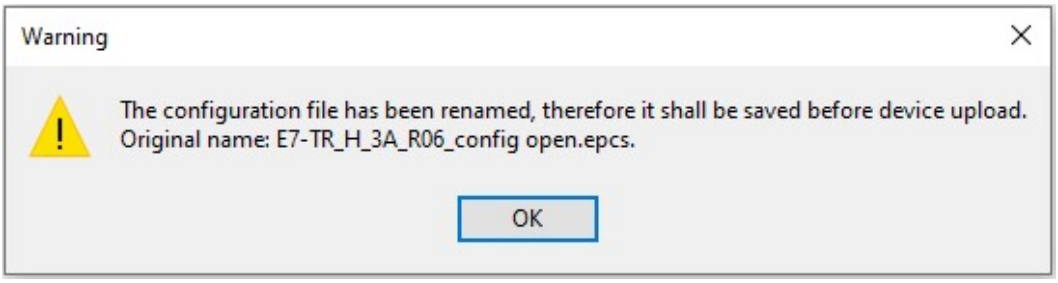
Opening a file whose extension has been wrongly appended and simply changed to .epcs gives the following pop-up window warning (see the figure below).

Figure 1. *Error pop-up when opening a file wrongly appended with the .epcs extension.*



Opening a file whose name was changed externally by a program other than AQtivate 300 gives the following pop-up window warning:

Figure 2. *Error pop-up when opening a file with an externally changed name.*



2.4 Communication ports and services

The device supports several communication ports for operation of multiple network applications.

To set up a network's firewall the following table summarizes all the port numbers being used by AQ 300 devices. All protocols can be individually disabled in device's ***System settings*** menu or in the ***Security settings*** menu.

The dedicated ports which are open by default can be used for protection relay configuration.

Table 1. *Available transport layer ports.*

Port	Direction	Protocol	Default	Service	Comment
22	IN	TCP	Open	SSH/SFTP	Secure file transfer protocol
102	IN	TCP	Closed	IEC 61850	IEC 61850 communication MMS/reporting
3782	IN	TCP	Closed	IEC 61850 TLS	Secure IEC 61850 communication

Port	Direction	Protocol	Default	Service	Comment
80	IN	TCP	Open	HTTP	Configuration and parametrization (redirects to HTTPS if the corresponding security level is selected)
443	IN	TCP	Closed	HTTPS	Configuration and parametrization (recommended)
123	OUT	UDP	Closed	SNTP	Time synchronization (SNTP)
389	OUT	TCP UDP	Closed	LDAP	Lightweight Directory Access Protocol (LDAP)
636	OUT	TCP UDP	Closed	LDAPS	LDAP over SSL
514	OUT	UDP	Closed	syslog	Syslog protocol
4712 4713	IN/OUT	TCP UDP	Closed	SNTP	Synchrophasor
2402	IN	TCP	Closed		IEC 60870-5-104
502	IN	TCP	Open	Modbus	Modbus TCP
20000	IN	TCP		DNP	DNP3 TCP
2405	IN/OUT	UDP			Proprietary protocol for device group backlight control (switch on)
2406	IN/OUT	UDP			Proprietary protocol for device discovery

The following settings, under the tab *Ethernet comm.* are settings utilized to enable different protocols used for substation communication. Some of the ports highlighted above can be opened/closed by changing these parameters.

Table 2. *Substation Ethernet communication protocols in the "Ethernet comm." tab.*

Title	Explanation
IEC 61850 enabled	IEC 61850 can be activated
IEC 104 enabled	IEC 104 can be activated
Modbus TCP enabled	Modbus TCP can be activated
DNP 3 TCP enabled	DNP3 TCP can be activated

In the ***System settings*** menu under the *Time synchronization* tab, the time synchronization port can be enabled.

Table 3. *NTP time synchronization.*

Title	Explanation
Timesync via NTP	Enabling NTP time synchronization

Lightweight Directory Access Protocol (LDAP) related parameters can be found under the ***User manager*** menu (located in the ***Security*** main menu) in the *LDAP authentication, authorization* tab. Find more details in the Server authentication (LDAP server authentication) chapter of this document.

The HTTP/HTTPS and SSH ports can be opened/closed from the ***System services*** menu, located within the ***Security*** main menu and its sub-menu ***Security settings***. Please see the System services chapter of this document.

2.5 Security settings

2.5.1 Secure handling

These parameters are crucial for cyber security and make device handling more secure or convenient. In the ***Security settings*** menu (located In the ***Security*** main menu) and under its *Secure handling* tab, the following three settings can be enabled/disabled according to the operation needs.

Table 4. *Secure handling settings.*

Title	Explanation
Safe settings	When enabled, a confirmation dialogue is displayed on the physical LCD when crucial relay settings are changed.

Title	Explanation
Remote front panel control	When enabled, the front panel buttons LCD and HMI can be controlled from the webpage. Note that the I and O buttons **cannot** be controlled!
LCD mirroring	When enabled, the exact live copy of the LCD can be viewed from the webpage.

2.5.2 System services

In the ***Security settings*** menu (located In the ***Security*** main menu) and under its *System services* tab, these security related communication parameters can be found which can be disabled/enabled according to the operation needs.

Table 5. *Parameters related to the Ethernet ports in the "System services" tab.*

Title	Explanation
HTTP mode	Selecting the access mode of the built-in web interface: "Disabled", "Read-only", or "Full access". Parameter change via web access is disabled in read-only mode.
HTTPS security level	Selection of the security level: "HTTP", "HTTPS", or "HTTPS only".
Network ProtectionHood	Enabling network protectionHood service.
SFTP/SSH enabled	Enabling SFTP/SSH globally.
Enable manufacturer SSH access	Enabling SSH for manufacturer purposes (factory use only).
Enable archive SSH access	Enabling SSH access for disturbance record archiving.
Remote logging	Enabling to send syslog messages. For further details, please refer to the Logging chapter in this document.

2.5.3 Client whitelist

Access to the device can be given to specific IP addresses only. The client whitelist functionality used for this purpose is available in the ***Security settings*** menu (located In the ***Security*** main menu) and under its *Client whitelist* tab.

When the function is enabled, up to eight clients can be configured with different roles.

The following parameters can be set for the client whitelist setup.

Table 6. *Client whitelist parameters.*

Title	Explanation
Enabled	Client whitelist functionality can be activated
Client 1...8 IP	Client IPv4 address can be defined
Client 1...8 Role	The allowed privileges can be set to the client: • "Both": all privileges are allowed. • "SCADA": all communication protocols to SCADA application are allowed. • "Management": HTTP/HTTPS is allowed (web access, config.)

2.6 Authentication

The following types of authentication are supported by AQ 300 devices:

- Device Authentication (local authentication).
- Server Authentication (LDAP server authentication).

No password or security information is displayed in plain text by web interface of the AQ 300 device, nor is such information ever transmitted without cryptographic protection. The number of supported individual users and their passwords is 32.

2.6.1 Role-based access control (RBAC)

With RBAC, the users can view functionalities that are permitted to their assigned roles in the web/HMI. The applied roles and rights are harmonized with the following standards and guidelines: IEC 62351-8, IEEE 1686, BDEW Whitepapers.

2.6.2 User roles

In order to add and/or modify user roles, the user must have the rights for managing users via the "Manage users" right.

The device is initially configured with Guest user rights where all rights are permitted to the Guest. The Guest user rights should be limited after the security setup.

Predefined user roles with different user rights are available in the *Roles* tab, located in the ***User manager*** menu under the ***Security*** main menu.

The IEC 62351-8 standard predefines the following user roles:

- **VIEWER**: A viewer can view what objects are present within an AQ 300 device.
- **OPERATOR**: An operator can view what objects are present within an AQ 300 device and can initiate control actions.
- **ENGINEER**: An engineer can view what objects are present within an AQ 300 device and can initiate control actions. Moreover, an engineer has full access to configure the device locally or remotely (parametrization, configuration update).
- **INSTALLER**: An installer can view what objects and values are present within an AQ 300 device by presenting the type and ID of those objects. Moreover, an installer can write files and can configure the server locally or remotely.
- **SECADM**: Security administrator can change role-to-rights assignments and can manage users. Moreover, they have access to the *Certificate handling*, *Alarm/Logging* menus.
- **SECAUD**: Security auditor can view audit logs and alarms.
- **RBACMNT**: RBAC management can change role-to-rights assignments and can manage users. Note that the RBACMNT role constitutes as a sub-functionality of the SECADM role.

The following predefined user roles are specific to vendors instead of the IEC 62351-8 standard:

- **GUEST**: By default, the device assigns the GUEST role to the user before there are any log-in requirements. Please note that initially all rights are assigned to the guest user. It is therefore important to limit guest user rights after the system security setup!
- **EMERGENCY**: In the case of LDAP server authentication, the emergency user offers an alternative authentication method if for any reason the LDAP server is not available.
- **FULL ACCESS**: Full rights are permitted to the user.

The tables below collect the predefined role-right assignments in the device, when the CyberProtect functionality is not in use.

Table 7. *Predefined role-rights assignments without CyberProtect, part 1.*

Role	Type	View data	View settings	Manage settings	Control
Guest	Guest	Web, LCD	Web, LCD	Web, LCD	Web, LCD
Full access	–	Web, LCD	Web, LCD	Web, LCD	Web, LCD
VIEWER	–	Web, LCD	–	–	–
OPERATOR	–	Web, LCD	Web, LCD	–	–
ENGINEER	–	Web, LCD	Web, LCD	Web, LCD	–
INSTALLER	–	Web, LCD	Web, LCD	Web, LCD	–
SECADM	–	Web, LCD	Web, LCD	Web, LCD	–
SECAUD	–	Web, LCD	Web, LCD	Web, LCD	–
RBACMNT	–	Web, LCD	–	–	–

Table 8. *Predefined role-rights assignments without CyberProtect, part 2.*

Role	Manage configurations	Update firmware	Manage users	Audit	Log
Guest	Web, LCD	Web, LCD	Web, LCD	Web, LCD	Web, LCD
Full access	Web, LCD	Web, LCD	Web, LCD	Web, LCD	Web, LCD
VIEWER	–	–	–	–	–
OPERATOR	–	–	–	–	–
ENGINEER	Web, LCD	–	–	–	–
INSTALLER	Web, LCD	Web, LCD	–	–	–
SECADM	–	–	Web, LCD	–	–
SECAUD	–	–	–	Web, LCD	–
RBACMNT	–	–	Web, LCD	–	–

The CyberProtect functionality allows for advanced user management with user-defined roles. Otherwise, the user roles are defined by the IEC 62351-8 standard as explained above. Note the following two features:

- On the last column, all the roles have an “Edit” button to allow for custom rights management (see the two tables below).
- Additional custom-defined roles can be created using the Add Role button.

The “Emergency” role can only be configured when CyberProtect is activated. This is because the relevance of the “Emergency” role only comes into play when LDAP (a sub-feature of CyberProtect) is enabled.

Table 9. *Predefined role-rights assignments with CyberProtect, part 1 (additions through the CyberProtect functionality in blue).*

Role	Type	View data	View settings	Manage settings	Control
Guest	Guest	Web, LCD	Web, LCD	Web, LCD	Web, LCD
Emergency	Emergency	Web, LCD	Web, LCD	Web, LCD	Web, LCD
Full access	–	Web, LCD	Web, LCD	Web, LCD	Web, LCD
VIEWER	–	Web, LCD	–	–	–
OPERATOR	–	Web, LCD	Web, LCD	–	–
ENGINEER	–	Web, LCD	Web, LCD	Web, LCD	–
INSTALLER	–	Web, LCD	Web, LCD	Web, LCD	–
SECADM	–	Web, LCD	Web, LCD	Web, LCD	–
SECAUD	–	Web, LCD	Web, LCD	Web, LCD	–
RBACMNT	–	Web, LCD	–	–	–

Table 10. *Predefined role-rights assignments with CyberProtect, part 2 (additions through the CyberProtect functionality in blue).*

Role	Manage configurations	Update firmware	Manage users	Audit	Log
Guest	Web, LCD	Web, LCD	Web, LCD	Web, LCD	Web, LCD
Emergency	Web, LCD	Web, LCD	Web, LCD	Web, LCD	Web, LCD
Full access	Web, LCD	Web, LCD	Web, LCD	Web, LCD	Web, LCD

Role	Manage configurations	Update firmware	Manage users	Audit	Log
VIEWER	–	–	–	–	–
OPERATOR	–	–	–	–	–
ENGINEER	Web, LCD	–	–	–	–
INSTALLER	Web, LCD	Web, LCD	–	–	–
SECADM	–	–	Web, LCD	–	–
SECAUD	–	–	–	Web, LCD	–
RBACMNT	–	–	Web, LCD	–	–

The “Guest” and “Emergency” roles cannot be deleted. Only the role name can be modified. The “Type” columns of the table above show the original name of these non-erasable roles.

The factory-defined rights are listed in the table below.

Table 11. *Rights definitions.*

Rights title	Explanation
View data	View IED operational data (voltage, current, power, energy, status, alarms...) that is not intended to be available as general information display.
View settings	View configuration settings of the device, such as scaling, communications addressing, programmable logic routines, and the firmware version numbers.
Manage settings	Managing the system settings of the device.
Control	Access to controllable object handling.
Manage configurations	Download and upload configuration files to the device, and manage parameters.
Update firmware	Performing firmware upgrade.
Manage users	Creating, deleting, or modifying user IDs, passwords, roles and/or role authorizations and configuring LDAP access.
Audit	Viewing and downloading the audit trail.

Rights title	Explanation
Log	Access to the ***Status/log*** menu.
API access	API access to parameters and system settings can be enabled.

2.6.3 Managing user roles

In order to add and/or modify user roles, the user must have the rights for managing users via the “Manage users” right.

Adding a new role

1. Select the **Add Role** button in the *Roles* tab, located in the ***User manager*** menu under the ***Security*** main menu.
2. Define the following items in the “Add Role” pop-up window:
    a. “Role”: name the role.
    b. “LDAP Group”: define the applied LDAP group when using the LDAP user authentication.
    c. “Permissions”: select the applied rights to the new role. The permissions for the web access and the local LCD system can be set separately.
3. Click the **Add Role** button to add the role to the system, or click the **Cancel** button to cancel the process of adding a new role.

Editing an existing role

1. Click the **Edit** button in the selected role entity to edit it.
2. Define the following items in the “Edit Role” pop-up window:
    a. Role name can be modified.
    b. LDAP Group can be modified.
    c. Rights assignment can be modified.
3. Click the **Save** button to save the role modification(s), or click the **Cancel** button to cancel the process of editing the role, or click the **Reset** button to set back to the original values, or click the **Remove Role** button to delete the role from the role list.

2.6.4 Managing users

In the ***User manager*** menu the user profiles of the selected device can be edited. New users can be created, existing users can be deleted, and different user group members can be edited. Please note that in order to add and/or

modify user roles, the user must have the rights for managing users via the "Manage users" right!

The device is initially configured with an "admin" user with a "Full Access". The default admin password is: `C1b3rS3c!`. It is important to remove the admin user or change the admin default password after the system security setup!

Adding a new user

1. Select the **Add User** button in the *Users* tab, located in the ***User manager*** menu under the ***Security*** main menu.
2. Define the following items in the "Add User" pop-up window:
    a. "Username": give the new user a username.
    b. "Role": select the required role from the role list. The defined roles can be seen in the *Users* tab.
    c. "Password": define the user's initial password. For further information about password requirements please refer to the Password requirement chapter in this document.
    d. "Confirm password": type the initial password again to confirm.
3. Click the **Add User** button to add the user to the system, or click the **Cancel** button to cancel the process of adding a new user.

Editing an existing user

1. Click the **Edit** button in the selected user entity to edit it.
2. Define the following items in the "Edit User" pop-up window:
    a. Username can be modified.
    b. Role assignment can be modified. The defined roles can be seen in the *Roles* tab.
3. Click the **Save** button to save the user account modification(s), or click the **Cancel** button to cancel the process of editing the user account, or click the **Reset** button to restore the initial field values, or click the **Remove User** button to delete the user from the user list.

Exporting users from the AQ 300 device

1. Select the **Export** button in the *Import/Export* tab, located in the ***User manager*** menu under the ***Security*** main menu.
2. A PGF file is saved to the PC.

3. The file can now be imported to another device.

Importing users from another AQ 300 device

1. Select the **Import** button in the *Import/Export* tab, located in the ***User manager*** menu under the ***Security*** main menu.
2. Select the exported PGF file from another AQ 300 device.
3. If the import is successful, a pop-up window with the message "Auth imported successfully" appears.
4. The newly added uses are now visible in the *Users* tab.

A device without a CyberProtect license **cannot** accept an authentication file from a device with a CyberProtect license!

2.6.5 Password requirement

The device supports password entry from a local or remote connection. User-created passwords follow a set of rules that must be adhered to in the creation of each password. A minimum of eight (8) characters must be used, and the password must be case-sensitive. The password characters shall contain the following:

- At least one upper case (A, B, C, ...) and one lower case letter (a, b, c, ...),
- At least one digit (0–9),
- At least one non-alphanumeric character (e.g., @, %, &, *, etc.)

Any attempt to create a password that violates these rules will be captured at the time of attempted creation, and the user is notified and prompted to choose another password that conforms to the rules.

2.6.6 User login

To log in to the web interface please follow these instructions:

1. Click the ***Login*** menu.
2. Enter the username and the password to log in to the device.
3. Click the **OK** button to log in, or the **Cancel** button to cancel the login process.

The "Login" pop-up window appears on accessing the device, if all rights for the guest role are disabled!

2.6.7 Session handling

The web and LCD session handling properties can be found in the *Session Handling* tab, located in the ***User manager*** menu under the ***Security*** main menu.

Table 12. *Properties of the "Session Handling" tab.*

Title	Web/LCD	Explanation
Number of login attempts	Web & LCD	The maximum number of allowed unsuccessful login attempts at a time.
Lock time	Web & LCD	After the maximum number of allowed unsuccessful login attempts, the user will be locked out for a time period set here.
Default timeout for session	Web & LCD	Timeout counter starts from this value after login or any user activity.
Maximum timeout for session	Web & LCD	Maximum value until the timeout can be extended in one session.
Maximum number of sessions	Web & LCD	Maximum number of allowed connections to the device (login sessions) at a time.
Maximum number of users	Web & LCD	Maximum number of allowed users connecting to the device at a time.

The actual session remaining time can be seen under the left menu bar.

To extend the session please follow these instructions:

1. Click on the active user/role in menu bar.
2. Extend the active session time in the "Extension Session Timeout" pop-up window with the available buttons: **Extend 10 minutes** or **Extend 1 hour**. Click the **Back** button the cancel the extension process.

The maximum session time cannot exceed the "Maximum timeout for session" setting!

Access automatically reverts to the guest level according to the access level timeout setting values!

2.6.8 Managing password

To change the password, the active user should click the “Change Password” text located below the left menu bar, at the bottom-left of the AQtivate window.

LDAP authenticated user password cannot be changed!

2.6.9 Lost password

If an essential password with “Manage users” right is lost, recovery is possible by resetting the unit to default values and restoring default role-rights assignment.

All relay settings will be reset to the factory defaults as a result of password reset process, not just the passwords!

Resetting the role-rights assignment setup to default

1. Push the **O** button at the device’s front panel six (6) times within 10 seconds while the main LCD screen is active. A reset ID will appear at the top of the screen (see the figure below).
2. Create a support ticket with Arcteq’s customer support (please see the contact details in the Contact information chapter in this document). The ticket information must include the device serial number as well as the displayed reset ID code. Arcteq’s customer support staff can then provide a reset code to reset the relay to its factory settings.
3. Repeat the first step of these instructions again. Additionally, enter the reset password you received from Arcteq.
4. The reset process takes around eight seconds. A dialog box with the text “Factory default in 8 seconds!” appears.
5. Press the **OK** button when it becomes available and the device will automatically restart and restore the default factory settings.

Figure 3. *Error pop-up when opening a file with an externally changed name.*

2.6.10 Server authentication (LDAP server authentication)

In order to set up server authentication, the user must have the rights for managing users via the “Manage users” right.

The relay offers Lightweight Directory Access Protocol (LDAP) support to allow authentication and authorization functions for Authentication Authorization Accounting (AAA) server.

> LDAP server authentication is only available when the optional CyberProtect functionality is activated. Otherwise, only local authentication is possible.

All the relevant parameters for the LDAP setup are collected under the *LDAP authentication, authorization* tab located in the ***User manager*** menu in the ***Security*** main menu. If the pre-configured LDAP server is not available, the device can be accessed with emergency user rights.

Figure 4. *Example of an LDAP configuration shown in the "LDAP" tab.*

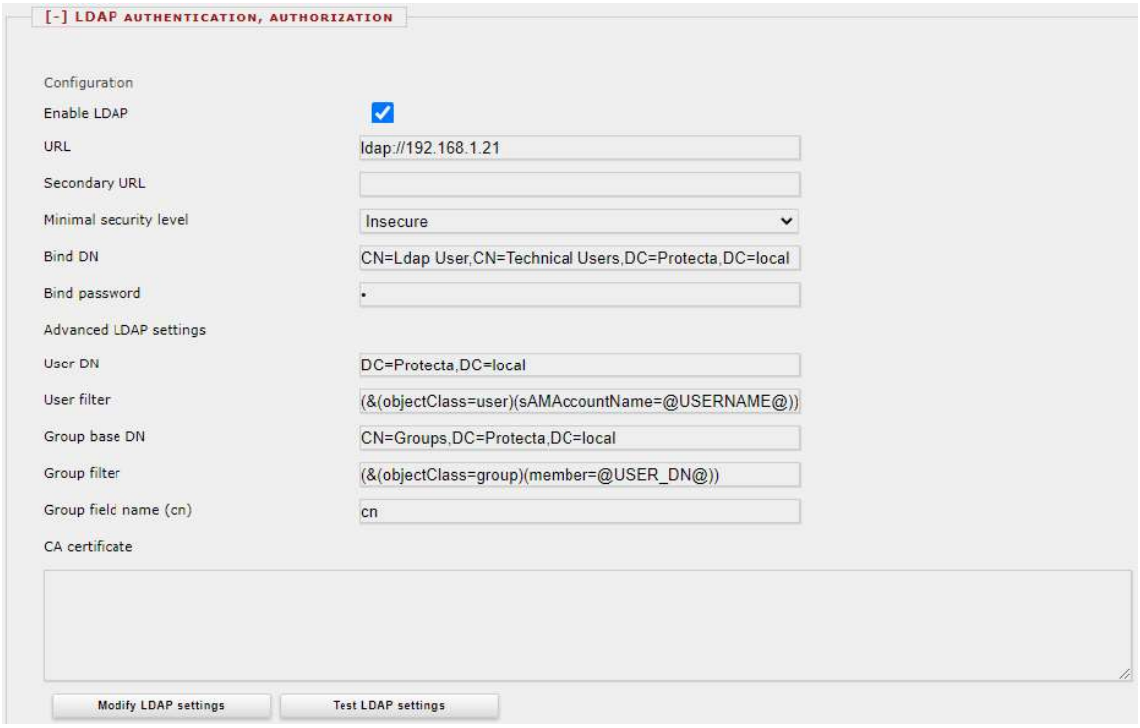


Table 12. *Properties of the "Session Handling" tab.*

Parameter title	Explanation
Basic LDAP settings	
Enable LDAP	Enable LDAP authentication, authorization.
URL	Address or name of the server where LDAP is hosted.
Secondary URL	Address or name of the backup LDAP server.
Minimal security level	Enable/disable TSL over LDAP: "Insecure", "TSL/SSL – No CERT check", and "TSL/SSL".
Bind DN	DN used for password protected connection. This parameter is ignored when the "Bind password" parameter is empty.
Bind password	Password used for connecting to a serve. If left empty, the server is not password protected.
Advanced LDAP settings	
User DN	Base DN for user search.
User filter	Filter expression used for user search. The string "@USERNAME@" will be replaced by the entered username.
Group base DN	Base DN for group search.

Parameter title	Explanation
Group filter	Filter expression used for group search. The string "@USER_DN@" will be replaced by the DN returned by the user search.
Group field name (cn)	Name of the field containing the group name.
CA certificate	CA certificate of the server in PEM format.

Setting up the LDAP connection and registered user authentication

1. Fill the *LDAP authentication, authorization* tab with the relevant data (obtained from your system administrator) and click the **Modify LDAP settings** button.
2. Open the *Roles* tab and refresh the webpage to see the new column titled "LDAP Group".
3. Select the desired role for LDAP authentication and fille the "LDAP Group" field with the proper group ID (obtained from your system administrator).

Figure 5. *Example of LDAP settings test results.*

Role	Type	LDAP Group	View data	View settings
Guest	Guest		Web, Lcd	Web, Lcd
Emergency	Emergency		Web, Lcd	Web, Lcd
Full Access			Web, Lcd	Web, Lcd
VIEWER			Web, Lcd	
OPERATOR			Web, Lcd	Web, Lcd
ENGINEER			Web, Lcd	Web, Lcd
INSTALLER		AddressBook	Web, Lcd	Web, Lcd

The emergency role can be used to access the device when LDAP is enabled but the configured LDAP servers are not available!

Testing the LDAP connection and registered user authentication

1. Click the **Test LDAP settings** button at the bottom of the LDAP authentication, authorization tab to test the LDAP connection and authentication, authorization.
2. Enter the username and the password to log in to the LDAP server, and then click the **OK** button.

3. The “LDAP test result” pop-up window (see the figure below) appears to show the actual result of the connection status to the LDAP server as well as the outcome of the authentication, authorization procedure.

Figure 6. *Example of LDAP settings test results.*

```
Tue Jun 28 07:40:55 2022: Starting RESOLVE test with username 'zsarnaisz'...
Tue Jun 28 07:40:55 2022: ---
Tue Jun 28 07:40:55 2022: SECURITY WARNING: Using insecure connection
Tue Jun 28 07:40:55 2022: Connecting to to ldap://192.168.1.21...
Tue Jun 28 07:40:55 2022: Setting LDAPv3 client version...
Tue Jun 28 07:40:55 2022: Setting timeouts to 2 second(s)...
Tue Jun 28 07:40:55 2022: Connecting with simple authetication...
Tue Jun 28 07:40:55 2022: LDAP connection successful
Tue Jun 28 07:40:55 2022: ---
Tue Jun 28 07:40:55 2022: Lookup user - base: DC=Protecta,DC=local filter:
(&(objectClass=user)(sAMAccountName=zsarnaisz))
Tue Jun 28 07:40:55 2022: User found! dn is: CN=Zsarnai Szabolcs,OU=Users,OU=Application,DC=Protecta,DC=local
Tue Jun 28 07:40:55 2022: ---
Tue Jun 28 07:40:55 2022: Lookup group - base: CN=Groups,DC=Protecta,DC=local filter:
(&(objectClass=group)(member=CN=Zsarnai Szabolcs,OU=Users,OU=Application,DC=Protecta,DC=local))
Tue Jun 28 07:40:55 2022: Checking group CN=GitLab-Users,CN=Groups,DC=Protecta,DC=local
Tue Jun 28 07:40:55 2022: Member of 'GitLab-Users'
Tue Jun 28 07:40:55 2022: Checking group CN=AddressBook,CN=Groups,DC=Protecta,DC=local
Tue Jun 28 07:40:55 2022: Member of 'AddressBook'
Tue Jun 28 07:40:55 2022: Found LDAP 2 group(s)
---
Resolved to role: Full Access
```

2.7 Logging

In order to set up logging service, the user must have the rights for managing settings via the “View settings, manage settings” right.

The relay can use a standard System Logging Protocol (Syslog) to communicate with a logging server (syslog server). Syslog server is designed specifically to make it easy to monitor device in the network. A syslog server might be a physical server, a standalone virtual machine, or a software-based service. The relevant parameters for the syslog setup can be found in the *System services* tab located in the ***Security settings*** menu in the ***Security*** main menu. Up to 2 syslog servers can be activated with “server1” and “server2” parameters.

Table 13. *Parameters for syslog setup.*

Title	Explanation
Remote logging	Enabling the syslog server messaging.
Log server1 IP address	The IP address for the syslog server 1 can be set here.
Log server1 UDP port	Syslog messages are sent via User Datagram Protocol (UDP). Its default port number is 514.

Title	Explanation
Log server2 IP address	The IP address for the syslog server 2 can be set here.
Log server2 UDP port	Syslog messages are sent via User Datagram Protocol (UDP). Its default port number is 514.

Syslog message properties: facility, severity, and priority

The syslog receiver's configuration file processes messages primarily based on their facility and severity. However, when the syslog message is generated, it is sent with a priority value that has been calculated from the facility and severity rather than the individual properties.

The facility and severity can be set in the *Syslog level settings* tab located in the ***Alarms/Logging*** menu in the ***Security*** main menu. Each facility and severity has both a name and a numeric value.

The first table below (Table 14) lists the numeric values, names, and the commonly used abbreviations of the various facility strings used in syslog configuration files. The table further down (Table 15) lists the same parameters for the severity strings.

Table 14. *Facility range.*

Numeric code	Facility	Title
0	Kernel messages	Kernel
1	User-level messages	User
2	Mail system	Mail
3	System daemons	Daemon
4	Security/authorization messages	Auth
5	Messages generated internally by syslogd	Syslog
6	Line printer subsystem	Lpr
7	Network news subsystem	News
8	UUCP subsystem	Uucp
9	Clock	Cron
10	Security/authorization messages	Authpriv
11	FTP daemon	Ftp

Table 15. *Severity range.*

Numeric code	Facility	Title
0	Emergency: system is unusable	Emergency
1	Alert: action must be taken immediately	Alert
2	Critical: critical conditions	Critical
3	Error: error conditions	Error
4	Warning: warning conditions	Warning
5	Notice: normal but significant condition	Notice
6	Informational: informational messages	Info
7	Debug: debug-level messages	Debug

The priority is calculated with the following equation:

$$Priority = Facility \times 8 + Severity$$

2.8 Audit trails

The audit trails facility can store at least 2,048 events before the circular buffer begins to overwrite the oldest event with the latest event. There is no capability to erase or modify the audit trail. It is not possible to remove the storage media of the audit trail without permanently damaging the AQ-300 device beyond field repair.

Furthermore, security-relevant operations (such as failed logins, change of password, etc.) are logged and cannot be deleted within the device. The audit trail structure and logged messages are according to the IEEE 1686 standard.

The audit trail entries can be found under the ***Audit trails*** menu in the ***Security*** main menu. Please note that adding and/or modifying user roles requires the user to have the "Audit" right.

Each audit trail event includes the following parameters:

- Event record number – event ID: the automatically generated sequential number for the event.
- Facility and severity according to the *Syslog level settings* tab (please refer to the Logging chapter above for further details).
- Time and date: the time and date of the event, including the year, month, day, hour, minute, and second.

- User: the username of the client logged into the device at the time of the event.
- Source: the remote client IP address from which the event originates.
- Destination: the IP of the AQ-300 device.
- Activity: several activities cause an entry into the audit trail record (see the table below for the categories).
- Details: detailed information related to the entry.

Table 16. *Activity categories.*

Title	Explanation
Login	Result of a login attempt. This activity category is logged whether the login attempt has been done locally or remotely, and whether it was successful or failed.
Logout	Logout, either user-initiated or automatic (due to the session time having expired).
Upload	File upload.
Settings	Settings changed.
Parameters	Parameters changed.
Options	Options changed.
User Manager	Users added, removed, or modified; user password changed.
Role Manager	User roles added, removed, or modified.
Pfw Upload	Result of a pfw upload, either successful or failed.
Psp Upload	Result of a psp upload, either successful or failed.
Epcs Upload	Result of an epcs upload, either successful or failed.
Restore	Result of a restore process, either successful or failed.
Command	Result of a command to the device from the webpage.
Download	Result of a client downloading a file from the device.
Audit	Result of downloading or viewing audit or alarm entries from the webpage.
Time Sync	Result of an event related to time synchronization.
Startup	Device starting.
Card	Result of a failed card, a pulled-out card, or a difference between the configured and the installed card/module.

Title	Explanation
IO Simulator	Binary input and binary output simulation entries are logged through this tag.
Nameplate	Result of events related to the nameplate, such as deletion, etc.

Alarms

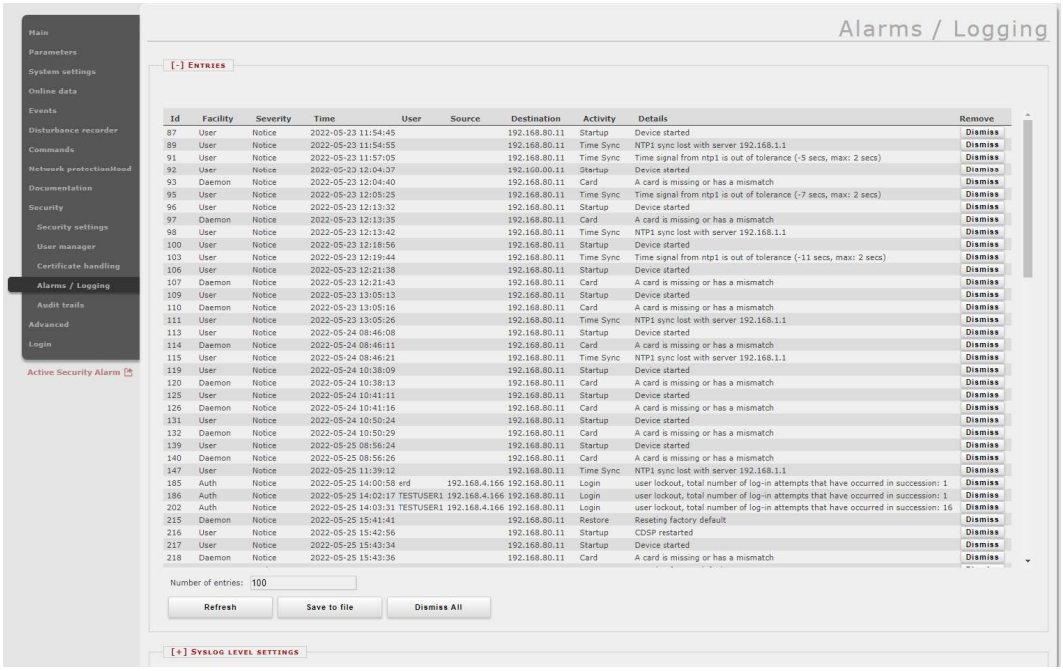
Alarms are defined as activities that may indicate unauthorized activity. The entries in the ***Alarms/Logging*** menu are a subset of audit trail events. While audit trails cannot be deleted, alarm entries can be deleted and/or cleared by clicking on the **Dismiss** button. The following alarm events are logged:

- User locked out
  User can lock themselves out when a pre-defined number of incorrect password attempts are performed in succession during a user login session (the related parameters can be found in the Session handling chapter).
- Attempted use of unauthorized configuration file or firmware
  The device detects when a user attempts to use an unauthorized configuration file or firmware, to access the computer without authorization, or do both. Unless a user, a configuration file, or a firmware file is registered as legitimate for a device, it is considered to be unauthorized.
- Device start or restart
  Any instance of the device starting or restarting will be logged with this alarm entry.
- Time sync signal loss
  Time synchronization events (such as loss of NTP connection, out-of-tolerance time signal, etc.) will be recorded as an entry in the alarms list.
- Missing I/O module
  When there is a mismatch between the configured cards and the detected cards in the device, this type of alarm is raised.

Security alarm activity indicates a security alarm message on the web by showing the “Active Security Alarm” message on the left menu bar. If the user has the access level authorizing them to see alarm messages, they can click the

message to navigate to the *Alarms/Logging Entries* tab in the ***Security*** main menu.

Figure 7. *Example of the Alarms/Logging menu showing alarm entries.*



Audit trails and alarms are recorded according to the time stamp of the device. Accurate readings therefore require that the time synchronization of the device is set correctly!

2.9 Certificate handling

In order to handle certificates, the user must have the “Manage settings” right.

2.9.1 HTTPS certificate

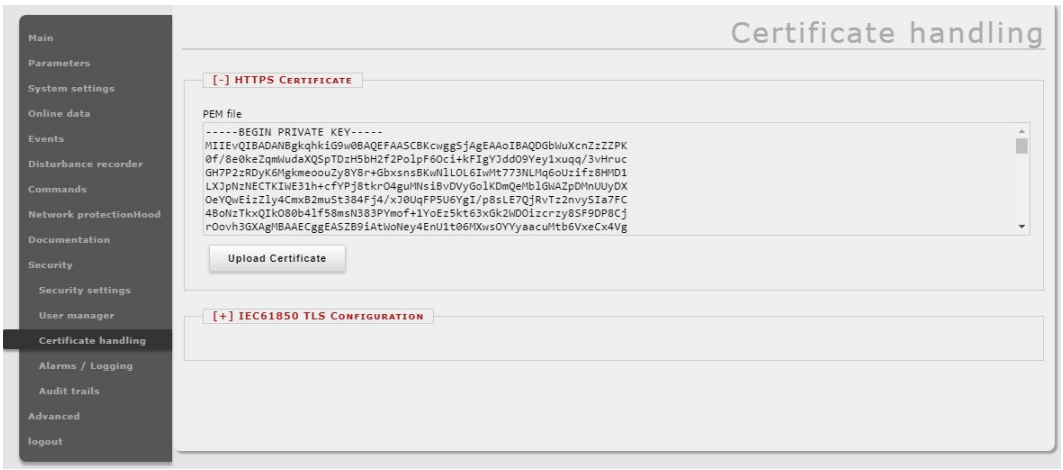
HTTPS includes robust authentication via the SSL/TLS protocol. The SSL/TLS certificate of the device includes a public key that a web browser can use to confirm that the data sent by the server has been digitally signed by someone in possession of the corresponding private key.

By default, the server certificate is a self-signed certificate which is generated and provided by the device itself, instead of being issued by any certification authority (CA).

A self-signed certificate will encrypt communication between your server and any clients. However, because it is not signed by any of the trusted certificate authorities included with web browsers, users cannot use the certificate to validate the identity of your server automatically.

There is an option for uploading a server's certificate, which has been signed by a publicly trusted certificate authority (CA). In this case the browser can accept that any identifying information included in the certificate has been validated by a trusted third party. The certificate can be uploaded from the *HTTPS Certificate* tab located in the ***Certificate handling*** menu within the ***Security*** main menu.

Figure 8. *HTTPS certificate handling window.*



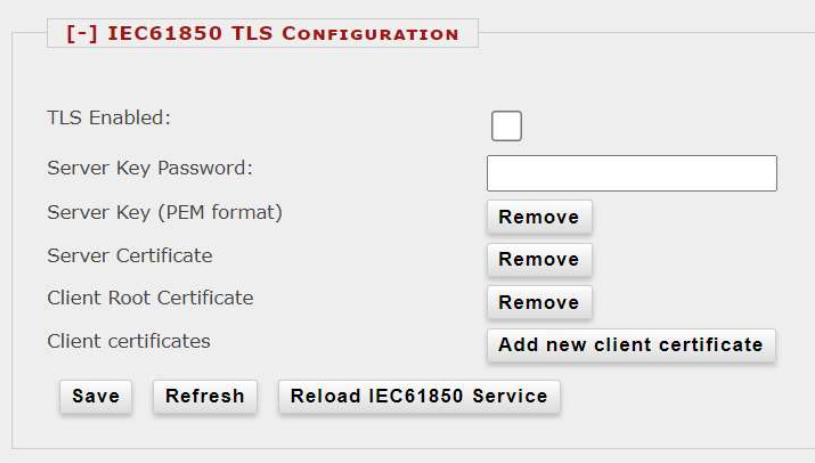
2.9.2 IEC 61850 TLS configuration

TLS (Transport Layer Security) secures IEC 61850 communication: enabling TLS and uploading the required certificates addresses the vulnerabilities in the communication. The table below (Table 17) shows the settings related to IEC 61850 TLS. Two parameters can be set, and certificate files can be uploaded. These settings can be found in the IEC 61850 TLS Configuration tab located in the ***Certificate handling*** menu within the ***Security*** main menu.

Table 17. *IEC 61850 TLS configuration settings.*

Title	Explanation
TLS Enabled	Enables and disables IEC 61850 TLS.
Server key password	Defines the password for the server private key.
Server key (PEM format)	Uploads and removes the server private key. This is required for operation.
Server Certificate	Uploads and removes the server certificate. This is required for operation.
Client Root Certificate	Uploads and removes the root certificate for clients. This is optional for operation.
Client certificates	Uploads and removes individual client certificates. Only clients with these certificates can join.

Figure 9. *IEC 61850 settings tab on the webpage.*

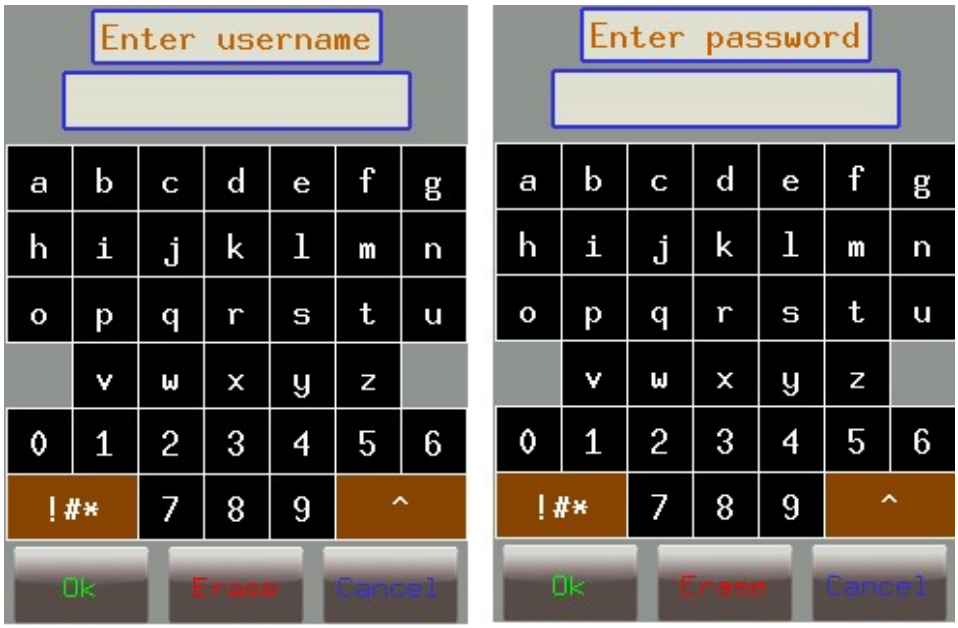


2.10 Using the local HMI

2.10.1 User management

Touching the orange lock icon on the device's main display allows the user to log in to the local HMI. When the login window appears, the username and password should be typed one after the other (see the figure on the following page).

Figure 10. *User authentication on the local HMI.*



The local HMI session can be managed in the session handling window (pictured in the figure below) according to the relevant parameters for local LCD session handling. These parameters have been defined in the Session handling chapter. The local HMI session handling window can be accessed by touching the green unlocking icon on the device's main display.

Figure 11. *Local LCD session handling.*

In the session handling window the user can logout of the device or extend the local HMI session timeout. By using the button with the back arrow icon the user can navigate back to the main user screen.

2.10.2 Security settings

Security settings, similar to the web interface, can be accessed from the LCD screen (pictured in the figure below).

Figure 12. *Security settings screen in the LCD.*

The detailed settings within each of these three menu items are the same as those in the web interface. These are described in the Security settings chapter.

3 CONTACT INFORMATION

3.1 Company

Address	Arcteq Relays Ltd. Kvartsikatu 2 A 1 65300 Vaasa FINLAND
Phone	+358 10 3221 370
Email	sales (at) arcteq.com
Website	www.arcteq.com

3.2 Technical support

Website	arcteq.com/support-login
Phone	+358 10 3221 388 (EET 9:00–17:00)