

Instructions for how to upgrade the firmware of an AQ 200 series device



Version: 2.00 EN

Revision	1.00
Date	September 2014
Changes	N/A
Revision	1.01
Date	April 2018
Changes	Added the table of contents.Added the "Troubleshooting" chapter.
Revision	2.00
Date	September 2023
Changes	 Updated the guide to the new visual layout. Text rewritten to increase readability. Content expanded where necessary to increase usability. Updated all images. Added the "Downloading the firmware file" chapter.

Version: 2.00 EN

TABLE OF CONTENTS

Upgrading process	3
1.1 Downloading the firmware file	3
1.2 Connecting the device and the PC	3
1.3 Upgrading the firmware	5
Troubleshooting	9
2.1 Allowing inbound ping	9
2.2 Whitelisting the AQtivate 200 application	. 14
2.3 Adding a new TFTP rule	. 17
Reference information	.20
	Upgrading process

Instruction on how to upgrade the firmware of an AQ 200 series device

Version: 2.00 EN

1 UPGRADING PROCESS

1.1 Downloading the firmware file

You can download the latest firmware file at Arcteq's website: <u>arcteq.com/customer-corner</u>. Go to the *Product releases* section and click "Read more". This opens a new page that lists various product releases in chronological order, with the latest at the top. Determine the series of your device: for example, "AQ-x21x and AQ-x20x" for an AQ-F205 or an AQ-T216, "AQ-x25x" for an AQ-G257A. Find the latest firmware release for your device series and open the files related to the release by clicking the title line.

All releases include the release notes which gathers all the relevant information about the release: fixes and new features, the latest instruction manual revisions, all available option cards, the minimum requirements for the AQtivate 200 software, and other related instructions. Additionally, the release files also include a link to install the latest version of AQtivate 200, a communication map and signal list file, instructions for firmware upgrading (this document), as well as the firmware file or files. All firmware files are named in the following style: "Firmware .zip file (v2.5.7.1-85-g5656f58.zip)".

For the AQ 250 series, all the firmware files are within the one .zip file; with AQ-210 (and AQ-x20x) there are separate files depending on the protection type of the device: for example, T for transformer protection devices and FVSPE for feeder, voltage alarming, power, and energy protection devices. When you have located the correct file, click on the download link for the firmware file and wait for the downloading to be complete. This may take a while depending on the size of the file.



Even though all firmware files are zipped files, do <u>not</u> unzip the firmware file! The AQtivate 200 setting and configuration tool does this automatically during the upgrade process.

1.2 Connecting the device and the PC

If possible, we recommend that you disconnect your AQ 200 series device from the network for the duration of the upgrading process. Although all AQ 200 series devices have an Ethernet port at the device's front panel, the front panel Ethernet port <u>cannot</u> be used for upgrading the firmware! Additionally, you <u>cannot</u> upgrade the firmware while a configuration file is open! Save and close your configuration file before you begin upgrading the device firmware.

Instruction on how to upgrade the firmware of an AQ 200 series device

Version: 2.00 EN

- 1. Connect your device to a computer with a standard RJ-45 Ethernet cable, plugging it in the device's rear Ethernet port. Make sure the computer you are connecting to has the AQtivate 200 setting and configuration tool installed!
- 2. Go to your computer's network settings, and manually set its IP address (see the figure below):



Figure 1-2-1. Setting the IP manually in your PC.

- a. Open the Control panel application with Windows Search.
- b. Select the following path: Network and Internet \rightarrow Network Connections.
- c. Right-click the "Ethernet" block and select "Properties" from the command window that appears.
- d. Select the "Use the following IP address" option, and set an IP address manually. Remember to note it down as you will need it soon!
- 3. Connect your device to a suitable power source and wait for your device to power up.
- 4. When the device is on, set its IP address for the same area as your PC (= the IP addresses in both the PC and the device have identical first, second, and third octets in the IP address, only the fourth one is different!):
 - a. Go to the device's Communication main menu, and select "Connections".
 - b. Use the front panel's navigation buttons to highlight the "IP address" in the *Ethernet* panel, and press the **OK** button to the right of the navigation buttons.
 - c. A keypad window opens in the device display: use the navigation buttons to set the IP address in this keypad window.
 - d. Press OK on the keypad window to save the new IP address.



Please note that if your device is already connected to the network, you can connect your computer to the hub with the corresponding IP settings!

Version: 2.00 EN

 Open the AQtivate 200 software, type the device IP address into the text field at the top of the software's main window, and click **Connect** or press **Enter** (see the figure below). You can also press **F11** on your keyboard and find the device in the device listing provided by the software.

Figure 1-2-2. Location of the IP address text field in AQtivate 200.



6. When the Arcteq logo on the device begins to blink and when the AQtivate 200 software shows a green "Online" text in its top-left corner, you are connected to the device and can begin upgrading its firmware.



For a more detailed description of connecting your device and your computer, please refer to the AQtivate 200 instruction manual. It is available at Arcteq's website on the "Documents & Software" page (<u>https://www.arcteq.com/documents-and-software/</u> \rightarrow Software \rightarrow "Instruction manuals").

1.3 Upgrading the firmware

1. Go to AQtivate 200 and select "Upgrade firmware" from the *Tools* main menu (see the figure below).

🖌 AQtivate	<u> </u>			-	
File Commands Disturbance Recorder	Tools Print Help	192.168.100.100	- Disconnect 🛛 I	ive Edit ###	ARCTEQ
~ 1	💧 Run Script	Ctrl+R			
<	Mimic Editor	F6			
Online Edit	250 Mimic Editor	FS			
		F7			
Sevice name: Unithante Sevice Jumphone 00170110517		F7			
Location: Unitionation					
IP Address: 192.168.100.100		er			
AM2-F255-	Project Editor				
HW Conf: PHDAAAA-	😔 Wizard				
	Events And Logs	•			
LRF:	Communication	•			
DIAG:	Misc				
	Settings				
	🗰 Upgrade Firmware				
	불 FTP	F2			
	Device List	F11			

Figure 1-3-1. Opening the "Upgrade firmware" window in AQtivate 200.

Instruction on how to upgrade the firmware of an AQ 200 series device

Version: 2.00 EN

2. A dialog window named "Upgrade firmware" opens. Click the ... button to the right of the text field for "Firmware file" (see the figure below) and browse the firmware package location. Select the correct firmware .zip file and click **OK**.

🖌 Upgrade Fi	rmware			? ×
Device:			250 Series	•
Firmware file:				
				Upgrade
Relay IP:			Back mac:	
Back IP:			Server IP:	
Subnet mask:			Gateway IP:	
				Close
#	Time	Error/Warning		

Figure 1-3-2. Selecting the firmware ZIP file.

3. When you have selected the correct firmware .zip file, click the **Upgrade** button below the text field to begin the upgrading process (see the figure below).

Figure 1-3-3. Starting the firmware upgrade process.

Upgrade Firmware		? ×
Device:	250 Series	-
Firmware file: C:/Users/EsimErkki/Down	ads/v2.5.7.1-85-g5656f58.zip	
		Upgrade
Relay IP:	Back mac:	
Back IP:	Server IP:	
Subnet mask:	Gateway IP:	
		Close
# Time	Error/Warning	

Upgrading into a newer software sometimes results in a notification for a failed attempt ("Firmware upgrade failed"). The most common cause for this message is that an anti-virus protection or a firewall software is interfering with the upgrading process. Please refer to the "Troubleshooting" chapter of this document to see how to disable anti-virus and/or firewalls for the duration of the upgrading process.

4. AQtivate 200 shows you a progress bar for the upgrade (see the figure at the top of the following page). During the upgrading process your device will reboot several times, and show a black and/or distorted display. This is normal. At some point AQtivate 200 informs you that the connection was closed; this is also normal.

Instruction on how to upgrade the firmware of an AQ 200 series device

Version: 2.00 EN

Figure 1-3-4. Selecting the firmware ZIP file.



5. At some point during the upgrading process the "Upgrade firmware" dialog window will show you information related to the process, such as IP addresses and the subnet mask (see the figure below).

🖌 Upgrade Firmware ? \times 250 Series Device: Firmware file: C:/Users/EsimErkki/Downloads/v2.5.7.1-85-g5656f58.zip 192.168.100.100 Relay IP: Back mac: 192.168.100.99 Back IP: Server IP: Subnet mask: 255.255.255.0 Gateway IP: 192.168.100.1 Frror/Warning

Figure 1-3-5. Information regarding the process displayed in the dialog window.

6. When the upgrading process is finished, the dialog window displays the message "Firmware upgrade complete" (see the figure below).

Figure 1-3-6. I	Information	regarding	the process	displayed in	the dialog window.
-----------------	-------------	-----------	-------------	--------------	--------------------

🖌 Upgrade Fi	rmware			?	\times
Device:			250 Series		•
Firmware file:	C:/Users/EsimErkki/Dowr	nloads/v2.5.7.1-85-g5656f58.z	ip		
				Upgra	de
Relay IP:			Back mac:		
Back IP:			Server IP:		
Subnet mask:			Gateway IP:		
				Close	e
#	Time	Error/Warning			
1 🚹	31.8.2023 14.30	Connection closed.			
2 🔔	31.8.2023 14.35	Connection closed.			
3 🔔	31.8.2023 14.37	Connection closed.			
4 🚺	31.8.2023 14.39	Firmware upgrade complete			

Instruction on how to upgrade the firmware of an AQ 200 series device

Version: 2.00 EN

- 7. After you have upgraded your device, its display will fully reboot after a few minutes. Once AQtivate 200 informs you that its firmware upgrade has been completed, reboot the device itself: cycle the auxiliary power supply by turning the device off and on again.
- 8. Finish the process: verify all setting parameters and do recommissioning tests (we recommend using a secondary injection for the transformer).

Instruction on how to upgrade the firmware of an AQ 200 series device

Version: 2.00 EN

2 TROUBLESHOOTING

The following sections explain three solutions to the most common problems in firmware upgrading. However, if you continue to have difficulties after trying these solutions, please contact Arcteq (see the contact information at the end of this document).

2.1 Allowing inbound ping

1. Open "Firewall & network protection" in the Windows Security application and select "Advanced settings" in the new dialog window (see the figure below).

Windows Security		- 🗆 X
←	(የን Firewall & network protection Who and what can access your networks.	Have a question?
Home Virus & threat protection Account protection	Domain network (active) Firewall is on.	Get help Who's protecting me? Manage providers
(m) Firewall & network protection Image: App & browser control Image: Device security	Private network Firewall is on.	Help improve Windows Security Give us feedback
 Device performance & health Family options Protection history 	S Public network Firewall is on.	Change your privacy settings View and change privacy settings for your Windows 11 Pro device.
ঞ্টি Settings	Allow an app through firewall Network and Internet trouble-shooter Firewall notification settings Advanced settings Restore firewalls to default	Privacy dashboard Privacy Statement

Figure 2-1-1. Advanced settings for firewall protection in Windows Security.

2. Another new dialog window opens. First, click on "Inbound rules" on the left-side pane and then on "New rule..." on the right-side pane (see the figure below).

P Windows Defender Firewall wit	h Advanced Security		— 🗆	\times
File Action View Help				
🗢 🏟 🗖 🖬 🗟 🖬				
Windows Defender Firewall with	Inbound Rules		Actions	
Inbound Rules	Name	Profile	Inbound Rules	
Connection Security Rules	Allow Ping from SFIIT	All	🙀 New Rule	
> 🖳 Monitoring	S AQtivate	Domain	Filter by Profile	•
	🚫 AQtivate	Domain		
	S Arcteq Relay Configuration and Setting	Domain '	Y Filter by State	•
	S Arcteq Relay Configuration and Setting	Domain	Filter by Group	•
	BarTender Licensing Service	Domain	View	•
	BarTender Licensing Service Discovery	Domain		
	🖉 BarTender System Administration Console	Domain	Q Refresh	
	Ø BarTender System Administration Console	Domain	📑 Export List	
	Corel PHOTO-PAINT 2017 (64-Bit)	All	7 Help	
	CorelDRAW 2017 (64-Bit)	All		

Figure 2-1-2. Adding a new rule to allow inbound ping.

Version: 2.00 EN

3. Select "Custom" as the type for the new firewall rule, and click Next (see the figure below).

Figure 2-1-3	Selecting	the rule	type	"Custom".
--------------	-----------	----------	------	-----------

Prew Inbound Rule Wiza	ard	\times
Rule Type		
Select the type of firewall rule to	o create.	
Steps:		
Rule Type	What type of rule would you like to create?	
Program		
Protocol and Ports	O Program	
Scope	Rule that controls connections for a program.	
Action	○ Port	
Profile	Rule that controls connections for a TCP or UDP port.	
Name	O Predefined:	
	AllJoyn Router 🗸	
	Rule that controls connections for a Windows experience.	
	O Custom	
	Custom rule.	
	< Back Next > Canc	el

4. Select "All programs" to specify that the new rule applies to all programs, and click Next (see the figure below).

Prew Inbound Rule Wizard		\times
Program		
Specify the full program path and e	xecutable name of the program that this rule matches.	
Steps:		
Rule Type	Does this rule apply to all programs or a specific program?	
Program		
Protocol and Ports	All programs Rule applies to all connections on the computer that match other rule properties.	
Action		
 Profile 	○ This program path:	
Name	Browse	
	%ProgramFiles%\browser\browser.exe	
	Services Customize	
	Specify which services this rule applies to.	
	< Back Next > Cancel	

Figure 2-1-4. Selecting applicable programs.

Instruction on how to upgrade the firmware of an AQ 200 series device

Version: 2.00 EN

5. Open the dropdown menu for the *Protocol type* parameter and select "ICMPv4". Then, click **Customize...** to specify the ICMP settings for this rule (see the figure below).

6	New Inbound Rule Wizard				×					
Р	rotocol and Ports									
Sp	ecify the protocols and ports to w	hich this rule applies.								
St	eps:									
۲	Rule Type To which ports and protocols does this rule apply?									
۲	Program									
۲	Protocol and Ports	Protocol type:	ICMPv4	\sim						
۲	Scope	Protocol number:	1 🜲							
۲	Action									
۲	Profile	Local port:	All Ports	~						
۲	Name									
			Example: 80, 443, 50	000-5010						
		Remote port:	All Ports	~						
			5	200 5010						
			Example: 80, 443, 50	00-5010						
		Internet Control Mess (ICMP) settings:	age Protocol	Customize						
		(10111)								
				< Back Next >	Cancel					

Figure 2-1-5. Selecting the protocol type "ICMPv4".

6. In the new dialog window, select "Specific ICMP types" to apply the new rule to specific ICMP connections, check the box in front of "Echo Request", and click **OK** (see the figure below).

Figure 2-1-6.	Customizing	the ICMP	settings.
---------------	-------------	----------	-----------

Customize ICMP Settings	×
Apply this rule to the following Internet Control Message Protocol (ICMP) connections:	
All ICMP types	
Specific ICMP types	
Packet Too Big Destination Unreachable Source Quench Bedirect Echo Request Router Adventsement Router Solicitation Time Exceeded Parameter Problem Timestamp Request Address Mask Request	
This ICMP type:	
Type: 0 V Code: Any V Add	
OK Cancel	

Instruction on how to upgrade the firmware of an AQ 200 series device

Version: 2.00 EN

7. Returning to the previous dialog window (see the figure below), select whether the new rule applies to any IP addresses ("Any IP address"), or to specific IP addresses ("These IP addresses:"). You must select this for both local and remote IP addresses separately. If you do not allow all IP addresses, you must specify the exact IP addresses you want to allow in the text field below the option and click Add for each of them. When you are finished, click Next.

Scope		
Specify the local and remote IP	addresses to which this rule applies.	
Steps:		
Rule Type		
Program	Which local IP addresses does this rule apply to?	
Protocol and Ports	 Any IP address 	
Scope	O These IP addresses:	
Action		Add
Profile		Edit
Name		Remove
	Customize the interface types to which this rule applies:	Customize
	Which remote IP addresses does this rule apply to?	
	Which remote IP addresses does this rule apply to? Any IP address	
	Which remote IP addresses does this rule apply to? Any IP address These IP addresses:	
	Which remote IP addresses does this rule apply to? Any IP address These IP addresses:	Add
	Which remote IP addresses does this rule apply to? Any IP address These IP addresses:	Add Edt
	Which remote IP addresses does this rule apply to? Any IP address These IP addresses:	Add Edit Remove

Figure 2-1-7. Defining applicable IP addresses.

 Select "Allow the connection" to allow the connection (both IPsec-protected and not) to occur when the conditions for the new rule have been met, and click Next (see the figure below).

Figure 2-1-8. Allowing connections.

Prev Inbound Rule Wizard		\times						
Action Specify the action to be taken when a connection matches the conditions specified in the rule.								
Specify the action to be taken whe	n a connection matches the conditions specified in the rule.							
Steps: Pub Type Program Producol and Pots Scope Action Profile Name	What action should be taken when a connection matches the specified conditions?							
	< Back Next > Cancel							

Instruction on how to upgrade the firmware of an AQ 200 series device

Version: 2.00 EN

9. Select the profile or profiles ("Domain", "Private", and/or "Public") to which you want this new rule to apply, and click **Next** (see the figure below).

Figure 2-1-9. Selecting the profile(s).

Prew Inbound Rule Wizard	1	\times
Profile		
Specify the profiles for which this r	ule applies.	
Steps:		
Rule Type	When does this rule apply?	
Program		
Protocol and Ports	🕑 Domain	
Scope	Applies when a computer is connected to its corporate domain.	
Action	Private	
Profile	Applies when a computer is connected to a private network location, such as a home or work place.	
Name	Public Applies when a computer is connected to a public network location.	el

10. Finally, give your new rule a name and (optionally) a description; click **Finish** (see the figure below).

Pow Inbound Rule Wizard	1	\times
Name		
Specify the name and description	of this rule.	
Steps:		
Rule Type		
Program		
Protocol and Ports		
Scope	Name:	
Action	ICMP - Echo	
Profile	Description (optional):	
Name	Enable ping	
	< Back Finish Cancel	

Figure 2-1-10. Naming the new rule.

Version: 2.00 EN

11. Your new rule is now displayed at the top of all inbound rules (see the figure below).

Figure 2-1-11. The new rule in the inbound rules list.

🔗 Windows Defender Firewall wit	th Advanced Security				- 0	\times
File Action View Help						
🗢 🌩 🔰 📰 📑 🚺 🗊						
Hindows Defender Firewall with	Inbound Rules			Actions		
Inbound Rules	Name	Group	Profile	Inbound Rules		
Connection Security Rules	🔇 ICMP - Echo		All	🚉 New Rule		
> 🔍 Monitoring	Allow Ping from SFIIT		All	Filter by Profile		•
	S AQtivate		Domain	Filter by State		
	O AQtivate		Domain			
	Arcteq Relay Configuration and Setting		Domain	Y Filter by Group		•
	Arcteq Relay Configuration and Setting		Domain	View		•
	Barlender Licensing Service		Domain	Refresh		
	BarTender System Administration Console		Domain	Export List		
	BarTender System Administration Console		Domain			
	Corel PHOTO-PAINT 2017 (64-Bit)		All	1 Help		
	O CorelDRAW 2017 (64-Bit)		All	ICMP - Echo		
	🖉 DameWare Mini Remote Control Service		All	Disable Rule		
	🧭 DameWare Mini Remote Control Service		All	🖌 Cut		
	🧭 DameWare Remote Control		All	D Com		
	🔇 Dropbox		All	Сору		
	🔮 Dropbox		All	X Delete		
	V Firefox (C:\Program Files\Mozilla Firefox)		Private	Properties		
	V Firefox (C:\Program Files\Mozilla Firefox)		Private	🕜 Help		
	🛛 👽 Microsoft Lync		Domain			

2.2 Whitelisting the AQtivate 200 application

1. Open "Firewall & network protection" in the Windows Security application and select "Allow an app through firewall" (see the figure below).

Figure 2-2-1. Allowing an application through firewall protection in Windows Security.

Windows Security		- 🗆 X
← ≡ ŵ Home	(প) Firewall & network protection Who and what can access your networks.	Have a question? Get help
Virus & threat protection Crossed and the protection Virus & Account protection Virus & network protection Virus & network protection	Domain network (active) Firewall is on.	Who's protecting me? Manage providers
App & browser control Device security	Private network Firewall is on.	Help improve Windows Security Give us feedback
 Device performance & health Family options Protection history 	Public network Firewall is on.	Change your privacy settings View and change privacy settings for your Windows 11 Pro device.
🕸 Settings	Allow an app through firewall Network and Internet trouble-shooter Firewall notification settings Advanced settings Restore firewalls to default	Privacy dashboard Privacy Statement

Instruction on how to upgrade the firmware of an AQ 200 series device

Version: 2.00 EN

- 2. In the new dialog window, click on the following buttons in this order (see the figure below):
 - a. **Change settings** (please note that this requires administration rights on the computer you are using!)
 - b. Allow another app....

Figure 2-2-2. Adding a new application through the firewall.

Allowed application	5								-	\times
$\leftarrow \ \ \rightarrow \ \ \lor \ \ \uparrow$	🖮 > Control Panel	> System and Security > Windows Defender Firewall > A	Allowed ap	plications			\sim	С	Search Control Panel	P
		Allow apps to communicate through Window To add, change or remove allowed apps and ports, cick CI What are the risks of allowing an app to communicate? For your security, some settings are managed by you Allowed apps and features:	vs Defer hange setti r system av	nder Fire ngs. dministrati	ewall Dr.	🗣 Change setti	ngs	la	•	
		Name	Domain	Private	Public	Group Policy				
		✓ @{Microsoft.DesktopAppInstaller_1.18.2691.0_x64	•	~		No	1			
		☑ @{Microsoft.DesktopAppInstaller_1.18.2691.0_x64	1	•		No				
		☑ @{Microsoft.MicrosoftStickyNotes_4.5.7.0_x648	•	-		No				
		☑ @{Microsoft.MicrosoftStickyNotes_4.5.7.0_x648	•	•		No				
		@{Microsoft.Windows.Photos_2022.30070.26007.0		✓	•	No				
		@{Microsoft.Windows.Photos_2022.30070.26007.0	7	~	✓	No				
		@{Microsoft.Windows.Search_1.14.1.19041_neutra		•		No				
		@{Microsoft.Windows.Search_1.14.7.19041_neutra	⊻	✓		No				
		☑ @{Microsoft.Windows.Search_1.14.7.19041_neutra		⊻		No				
		✓ @{Microsoft.Windows.Search_1.16.0.22000_neutra				No				
		@{Microsoft.Windows.SecHealthUI_10.0.19041.18	M			No				
		@{Microsoft.Windows.SecHealthUI_10.0.19041.18	⊻			INO				
					Details.	. Remove	:)	b	•	
					OK	Canc	el			

3. Click Browse... in the new dialog window (see the figure below).

Figure 2-2-3. Browsing for an application to add.

Add an app		\times
Select the app that you want to add or dick Brow listed and then dick OK.	wse to find o	one that is not
Applications:		
Path:		Browse
What are the risks of unblocking an app?		
You can choose which network types to add this a	app to.	
Network types	Add	Cancel

Version: 2.00 EN

4. Find the folder where you have AQtivate 200 installed, select the application, and click Open (see the figure below).

in Browse					×				
\leftrightarrow \rightarrow \checkmark \uparrow	→ This PC → Windows (C:) → P	rogram Files (x86) > Arcteq > AQtivate	,	 C Search AQtivate 	Q				
Organise Vew folder									
	Name	Date modified	Туре	Size					
🛄 Desktop 🏾 🖈	color_themes	11/04/2023 10.32	File folder						
🛓 Downloads 🖈	늘 manuals	11/04/2023 10.32	File folder						
🝯 Documents 🖈	🚞 platforms	11/04/2023 10.32	File folder						
🚬 Pictures 🔹 🖈	🚞 sqldrivers	11/04/2023 10.32	File folder						
🕖 Music 🔹 🖈	🚞 styles	11/04/2023 10.32	File folder						
🛂 Videos 🔹 🖈	1 7z	21/10/2021 15.49	Application	574 KB					
📒 IM00085 🔹 🖈	🛃 AQtivate	13/03/2023 12.19	Application	18 024 KB					
	🛄 AQviewer	10/03/2023 17.30	Application	1 521 KB					
> o Creative Cloud F	🖌 unins000	11/04/2023 10.31	Application	2 989 KB					
> This PC									
File n	ame: AQtivate			 Applications (*.ex 	e;*.com;*.icd) ∨				
				Open	Cancel				

Figure 2-2-4. Selecting the AQtivate 200 application.

5. Select Add (see the figure below).

Figure 2-2-5. Adding AQtivate 200 to the whitelisted applications.

Add an app		\times
Select the app that you want to add or click i listed and then click OK.	Browse to find or	ne that is not
Applications:		
AQtivate		
Path: C:\Program Files (x86)\Arcteq\	AQtivate\AQtiv	Browse
What are the risks of unblocking an app?		
You can choose which network types to add t	his app to.	
Network types	Add	Cancel

Instruction on how to upgrade the firmware of an AQ 200 series device

Version: 2.00 EN

6. The AQtivate 200 application is now whitelisted in the list of allowed apps and features (see the figure below).

Figure 2-2-6. AQtivate 200 listed among other applications that are allowed to communicate through the firewall.

P Windows Defender Firewall with	🔐 Windows Defender Firewall with Advanced Security							
File Action View Help								
🗢 🄿 🙋 🖬 🔒 🛛 🖬								
P Windows Defender Firewall witi Inbound Rules								
Inbound Rules	Name	Group	Profile	Enabled	Action	Override	Program	
Connection Security Rules		Domain	Yes	Allow	No	C:\program files (x86)\arcteq\aqtivate\aqtivate.exe		
> 🖳 Monitoring	Arcteq Relay Configuration and Setting		Domain	Yes	Allow	No	C:\program files (x86)\softreal\aqtivate300\aqtivate300.exe	
S BarTender Licensing Service			Domain	Yes	Allow	No	Any	

2.3 Adding a new TFTP rule

- 1. Open "Firewall & network protection" in the Windows Security application and select "Advanced settings" (see Figure 2-1-1 above).
- 2. Another new dialog window opens. First, click on "Inbound rules" on the left-side pane and then on "New rule..." on the right-side pane (see Figure 2-1-2 above).
- 3. Select "Port" as the type for the new firewall rule, and click **Next** (see the figure below).

Figure 2-3-1. Selecting the rule type "Port".

1	New Inbound Rule Wizard		\times				
F	tule Type						
Se	elect the type of firewall rule to crea	te.					
S	eps:						
۲	Rule Type	What type of rule would you like to create?					
•	Protocol and Ports Action Profile	Program Rule that controls connections for a program.					
•	Name	 Port Rule that controls connections for a TCP or UDP port. Predefined: 					
		AllJoyn Router V					
		Hule that controls connections for a Windows experience.					
		Custom rule.					
		< Back Next > Cancel					

Instruction on how to upgrade the firmware of an AQ 200 series device

Version: 2.00 EN

4. Select "UDP", specify that the rule only applies to the local port "69", and then click **Next** (see the figure below).

Figure 2-3-2.	Defining	the	protocols	and	ports	for the	new rule
I Igui o Z o Z.	Demining	uiic	p10100015	ana	porto		new rule.

🔗 New Inbound Rule Wizard			×						
Protocol and Ports									
Specify the protocols and ports to	which this rule applies.								
Steps:		_							
a Rule Type	Does this rule apply to TCP or UD)P?							
Protocol and Ports	○ тср								
Action	O UDP								
Profile									
Name	Does this rule apply to all local ports or specific local ports?								
	Specific local ports:	69							
	· · ·	Example: 80, 443, 5000-5010	-						
		< Back Next > Ca	ncel						

- 5. Select "Allow the connection" to allow the connection (both IPsec-protected and not) to occur when the conditions for the new rule have been met, and click **Next** (see Figure 2-1-8 above).
- 6. Select the profile or profiles ("Domain", "Private", and/or "Public") to which you want this new rule to apply, and click **Next** (see Figure 2-1-9 above).

Version: 2.00 EN

7. Finally, give your new rule a name and (optionally) a description; click Finish (see the figure below).

Figure 2-3-5. Naming the new rule.

6	New Inbound Rule Wizard		×
N	ame		
Sp	ecify the name and description of	this rule.	
St	eps:		
۲	Rule Type		
۲	Protocol and Ports		
۲	Action		
۲	Profile	Name:	
۲	Name	IF IP server	
		Description (optional):	
			_
		< Back Finish	Cancel
			Ganool

8. Your new rule is now displayed at the top of all inbound rules (see the figure below).

Figure 2-3-6. The new TFTP rule in the inbound rules list.

Windows Defender Firewall with	th Advanced Security				- 0	×
File Action View Help						
🗢 🄿 🙍 📰 🗟 🚺						
🔗 Windows Defender Firewall witl	Inbound Rules			Actions		
🔜 Inbound Rules	Name	Group	Profile	Inbound Rules		
Outbound Rules	TFTP server		All New Bule			
Monitoring	Allow Ping from SFIIT			S Eilter hu Drefile		
y and the state of	S AQtivate		Domain	The Price by Profile		
	S AQtivate			Filter by State		•
	SArcteq Relay Configuration and Setting		Domain 🛛 🐨 Filter by Group	Filter by Group		•
	SArcteq Relay Configuration and Setting		Domain	View		•
	Ø BarTender Licensing Service		Domain	O Refresh		
	SarTender Licensing Service Discovery	g Service Discovery				
	BarTender System Administration Console BarTender System Administration Console Corel PHOTO-PAINT 2017 (64-Bit) CorelDRAW 2017 (64-Bit)		Domain	Export List		
			Domain	🛛 🛛 Help		
			All	TETD conver		
			All			-
	🔮 DameWare Mini Remote Control Service			Disable Rule		
	🔮 DameWare Mini Remote Control Service		All	🔏 Cut		
	🔇 DameWare Remote Control			Copy		
	🔮 Dropbox		All			
	🔮 Dropbox		All	Delete		
	Firefox (C:\Program Files\Mozilla Firefox)		Private	Properties		
	Firefox (C:\Program Files\Mozilla Firefox)		Private	P Help		
	🛛 🕑 ICMP - Echo		All			

Instruction on how to upgrade the firmware of an AQ 200 series device

Version: 2.00 EN

3 REFERENCE INFORMATION

Manufacturer:

Arcteq Relays Ltd.

Visiting and postal address:

Kvartsikatu 2 A 1 65300 Vaasa FINLAND

Contacts:

Phone for general and commercial issues (office hours GMT +2): +358 10 3221 370 Website: <u>www.arcteq.com</u> E-mail (sales): <u>sales@arcteq.fi</u>

Arcteq technical support:

E-mail (technical support): <u>helpdesk@arcteq.fi</u> Website (technical support): <u>https://support.arcteq.fi</u> Phone (EET 9:00 – 17:00): +358 10 3221 388