AQ 200 firmware upgrade guide

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

AQ 200 firmware upgrade guide

Instruction on 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.

AQ 200 firmware upgrade guide

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

Version: 2.00 EN

TABLE OF CONTENTS

1   UPGRADING PROCESS

1.1   Downloading the firmware file

You can download the latest firmware file at Arcteq's website: arcteq.com/customer-corner. 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.

> **i** Even though all firmware files are zipped files, do **not** 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

> **i** 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 **cannot** be used for upgrading the firmware! Additionally, you **cannot** upgrade the firmware while a configuration file is open! Save and close your configuration file before you begin upgrading the device firmware.
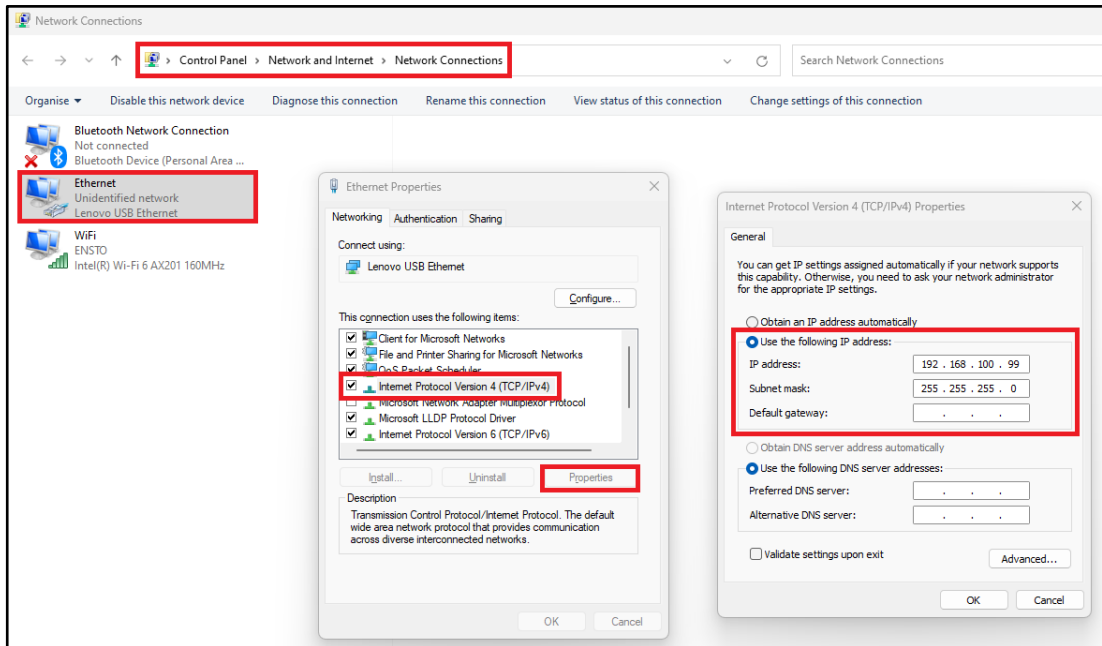
1. Connect your device to a computer with a standard RJ-45 Ethernet cable, plugging it in the device's rear Ethernet port. Make sure the computer you are connecting to has the AQtivate 200 setting and configuration tool installed!
2. Go to your computer's network settings, and manually set its IP address (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 → 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.

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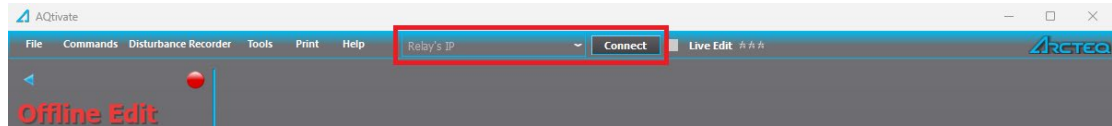
5. Open the AQtivate 200 software, type the device IP address into the text field at the top of the software's main window, and click **Connect** or press **Enter** (see the figure below). You can also press **F11** on your keyboard and find the device in the device listing provided by the software.

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 (https://www.arcteq.com/documents-and-software/ → *Software* → "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).

Figure 1-3-1. Opening the "Upgrade firmware" window in AQtivate 200.
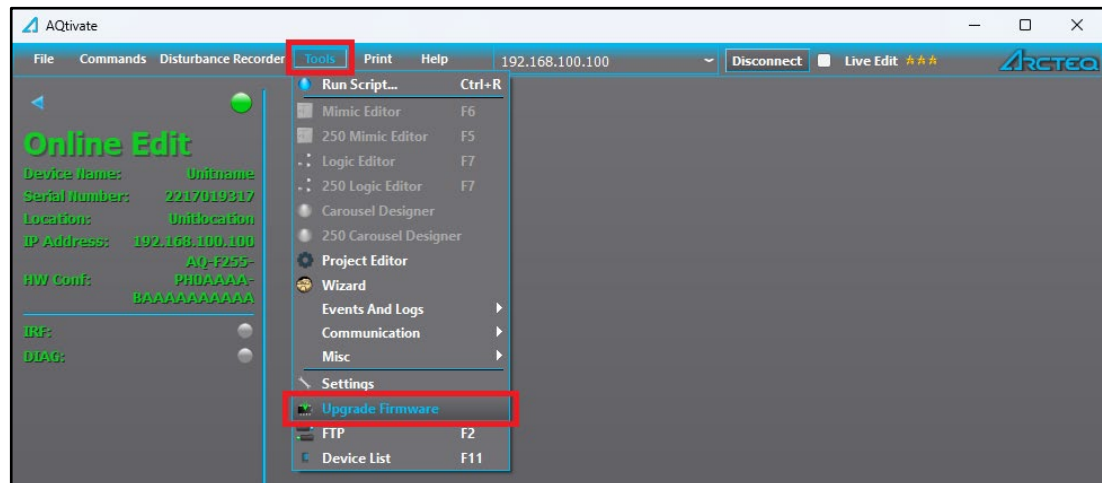
2. A dialog window named "Upgrade firmware" opens. Click the **...** button to the right of the text field for "Firmware file" (see the figure below) and browse the firmware package location. Select the correct firmware .zip file and click **OK**.

Figure 1-3-2. Selecting the firmware ZIP file.
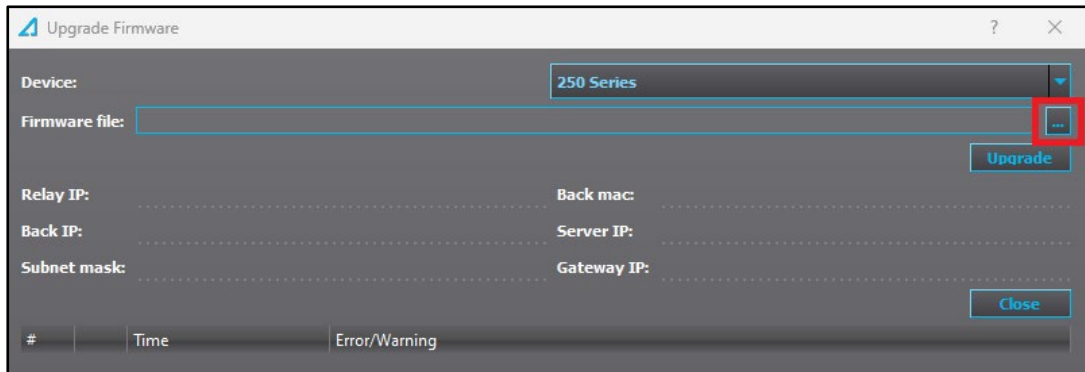
3. When you have selected the correct firmware .zip file, click the **Upgrade** button below the text field to begin the upgrading process (see the figure below).

Figure 1-3-3. Starting the firmware upgrade process.
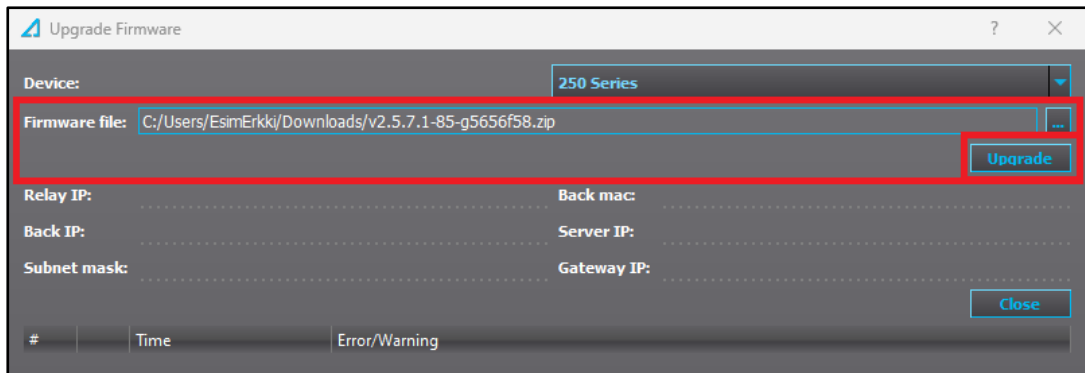
> Upgrading into a newer software sometimes results in a notification for a failed attempt ("Firmware upgrade failed"). The most common cause for this message is that an anti-virus protection or a firewall software is interfering with the upgrading process. Please refer to the "Troubleshooting" chapter 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.

Figure 1-3-4. Selecting the firmware ZIP file.
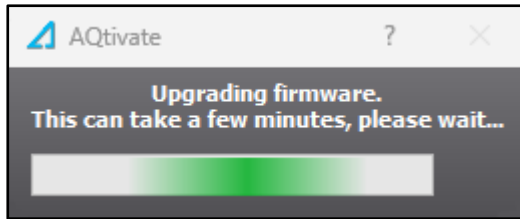
5. At some point during the upgrading process the "Upgrade firmware" dialog window will show you information related to the process, such as IP addresses and the subnet mask (see the figure below).

Figure 1-3-5. Information regarding the process displayed in the dialog window.
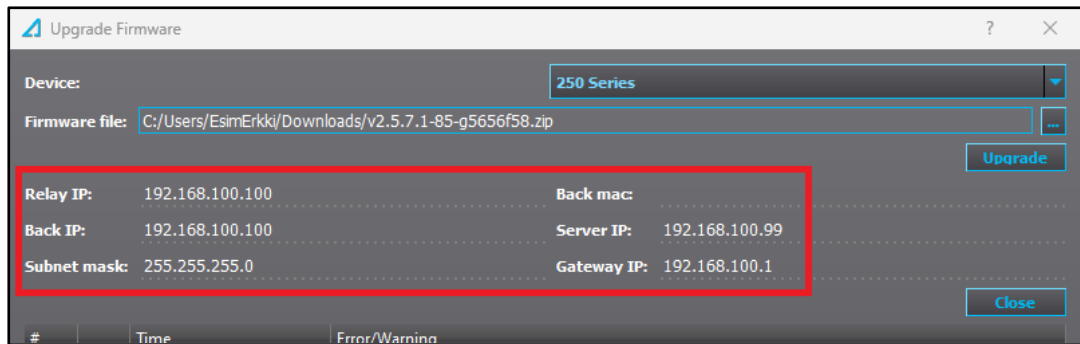
6. When the upgrading process is finished, the dialog window displays the message "Firmware upgrade complete" (see the figure below).

Figure 1-3-6. Information regarding the process displayed in the dialog window.
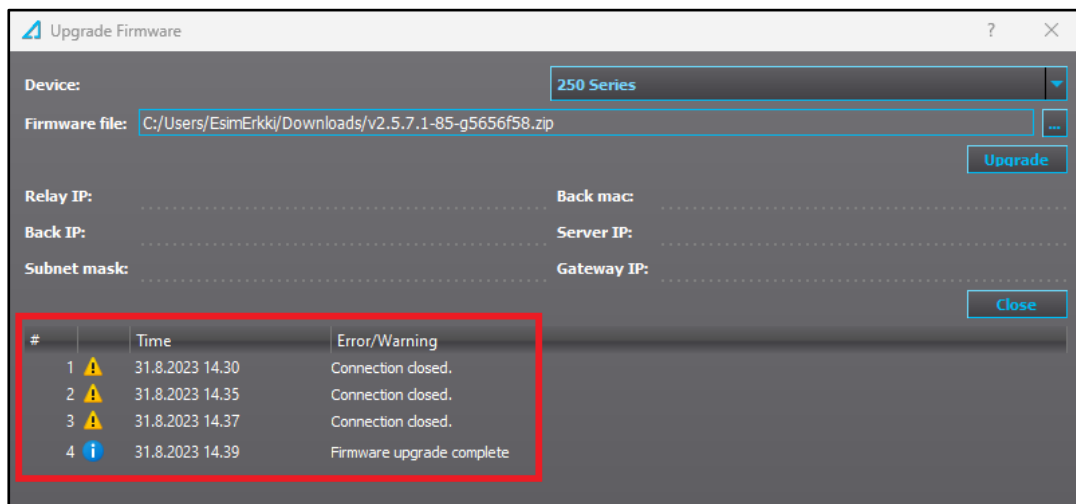
7. After you have upgraded your device, its display will fully reboot after a few minutes. Once AQtivate 200 informs you that its firmware upgrade has been completed, reboot the device itself: cycle the auxiliary power supply by turning the device off and on again.
8. Finish the process: verify all setting parameters and do recommissioning tests (we recommend using a secondary injection for the transformer).

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).

Figure 2-1-1. Advanced settings for firewall protection in Windows Security.
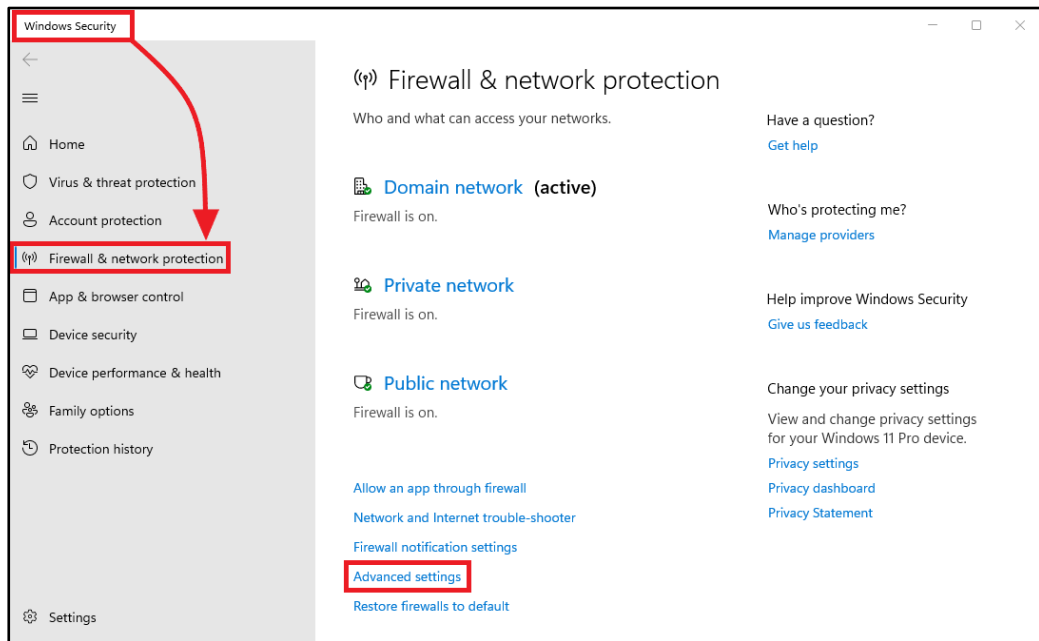
2. Another new dialog window opens. First, click on "Inbound rules" on the left-side pane and then on "New rule…" on the right-side pane (see the figure below).

Figure 2-1-2. Adding a new rule to allow inbound ping.
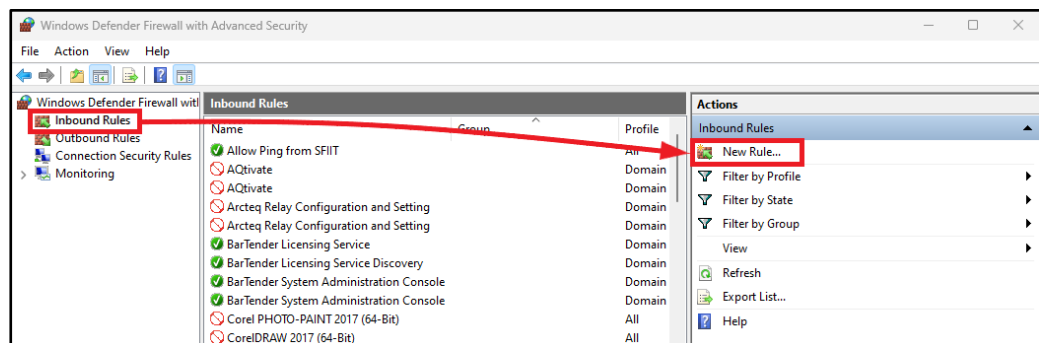
© Arcteq Relays Ltd.

Document ID: IM00085

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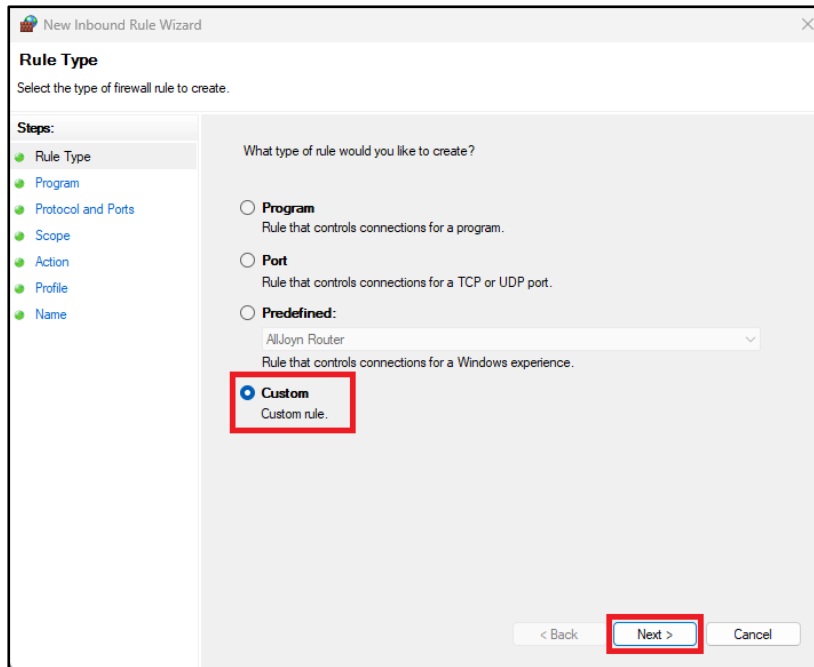
4. Select "All programs" to specify that the new rule applies to all programs, and click **Next** (see the figure below).

Figure 2-1-4. Selecting applicable programs.
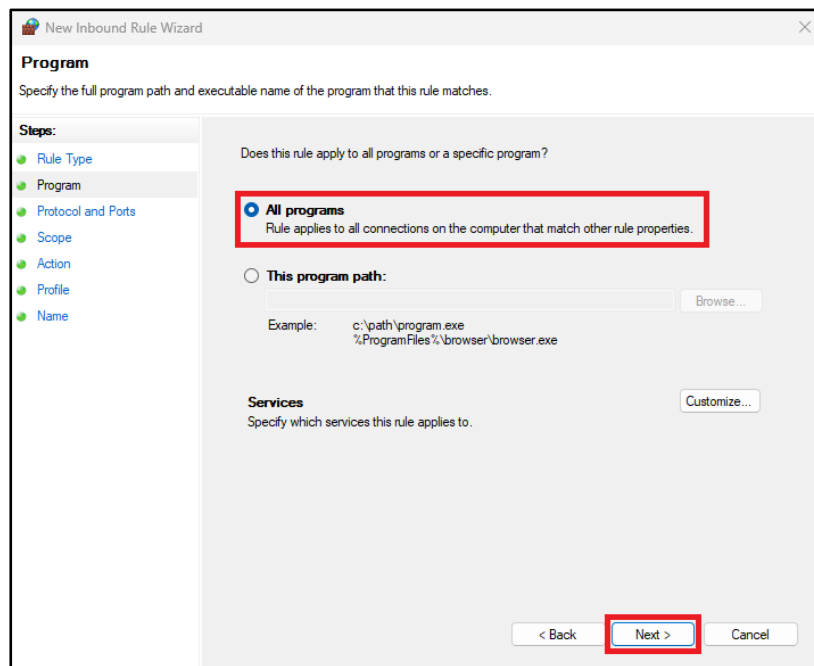
5. Open the dropdown menu for the *Protocol type* parameter and select "ICMPv4". Then, click **Customize…** to specify the ICMP settings for this rule (see the figure below).

Figure 2-1-5. Selecting the protocol type "ICMPv4".
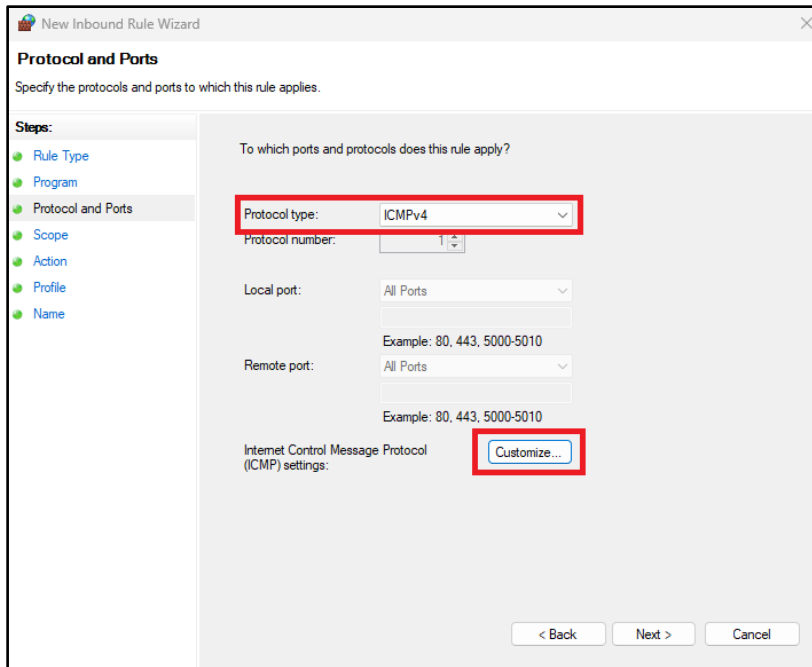
6. In the new dialog window, select "Specific ICMP types" to apply the new rule to specific ICMP connections, check the box in front of "Echo Request", and click **OK** (see the figure below).

Figure 2-1-6. Customizing the ICMP settings.
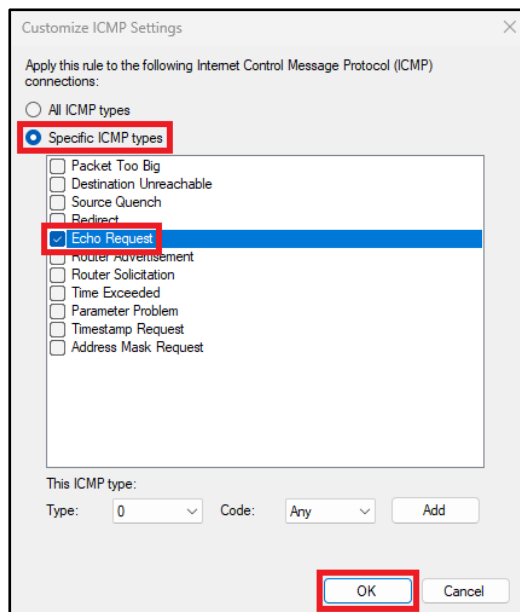
7. Returning to the previous dialog window (see the figure below), select whether the new rule applies to any IP addresses ("Any IP address"), or to specific IP addresses ("These IP addresses:"). You must select this for both local and remote IP addresses separately. If you do not allow all IP addresses, 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**.

Figure 2-1-7. Defining applicable IP addresses.
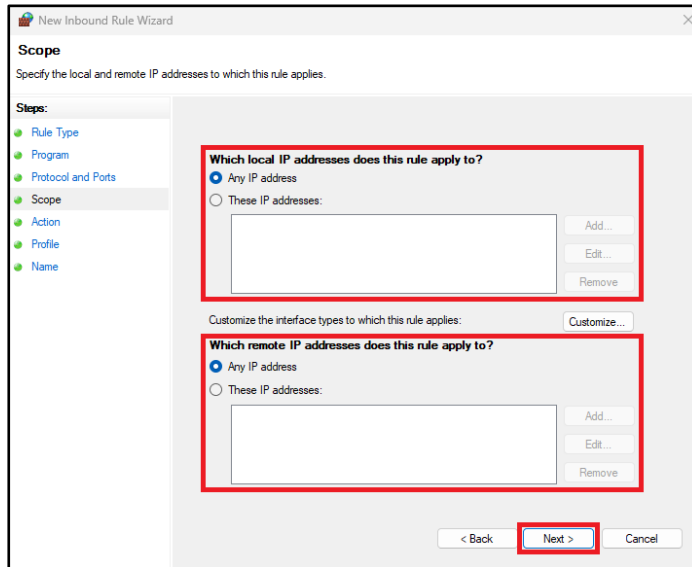
8. Select "Allow the connection" to allow the connection (both IPsec-protected and not) to occur when the conditions for the new rule have been met, and click **Next** (see the figure below).

Figure 2-1-8. Allowing connections.
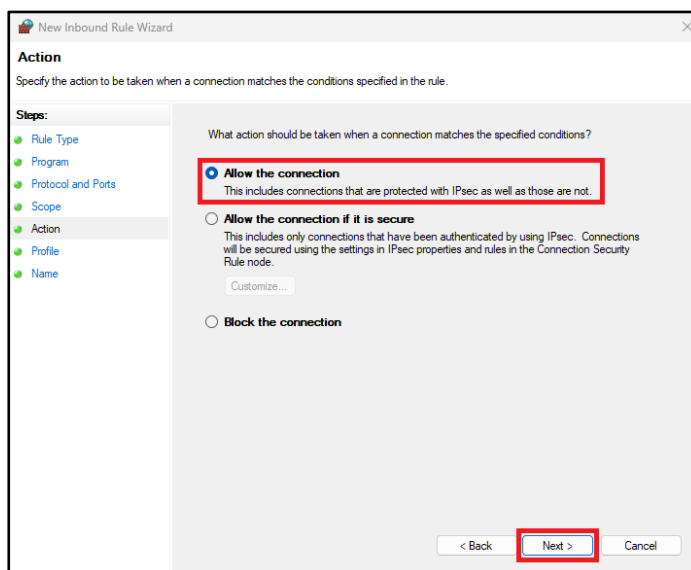
9. Select the profile or profiles ("Domain", "Private", and/or "Public") to which you want this new rule to apply, and click **Next** (see the figure below).

Figure 2-1-9. Selecting the profile(s).
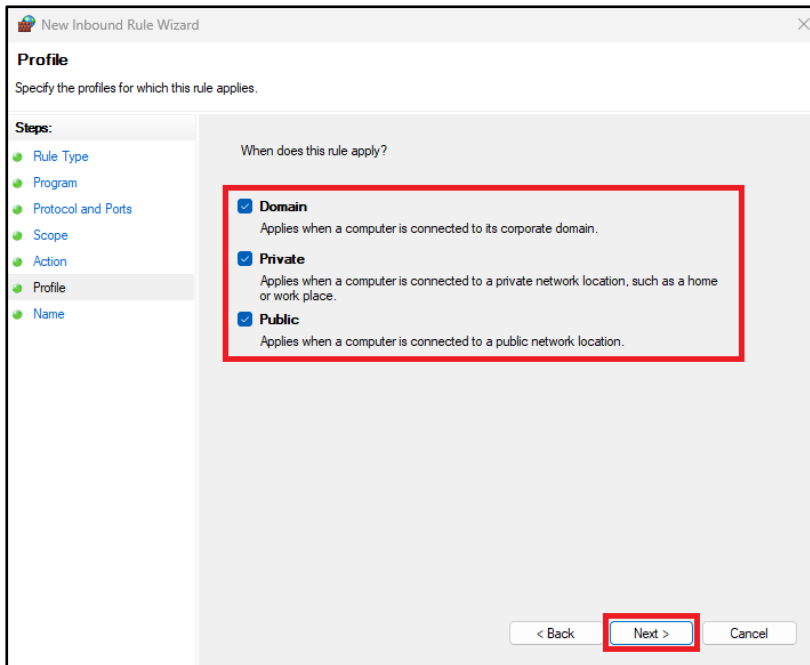
10. Finally, give your new rule a name and (optionally) a description; click **Finish** (see the figure below).

Figure 2-1-10. Naming the new rule.
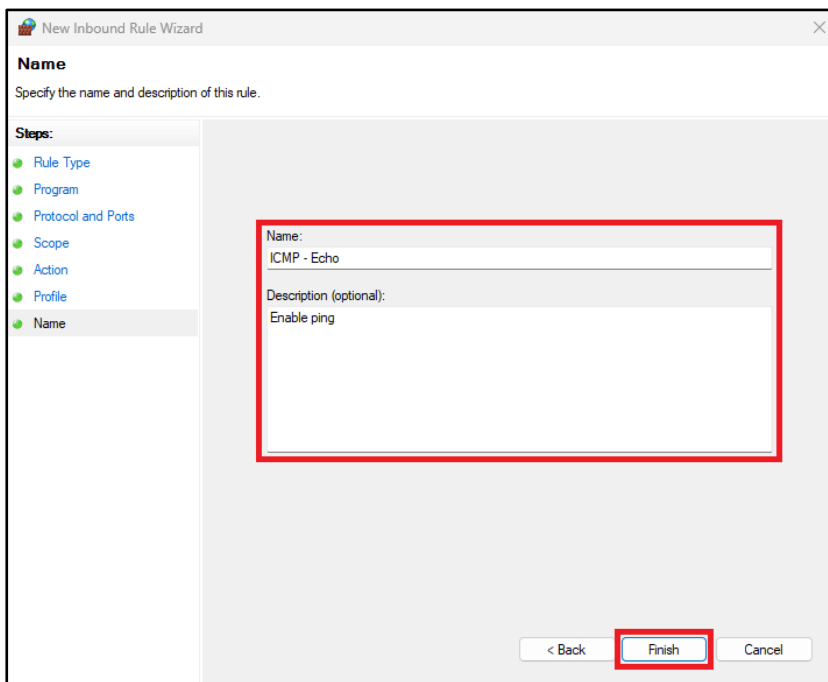
11. Your new rule is now displayed at the top of all inbound rules (see the figure below).

Figure 2-1-11. The new rule in the inbound rules list.
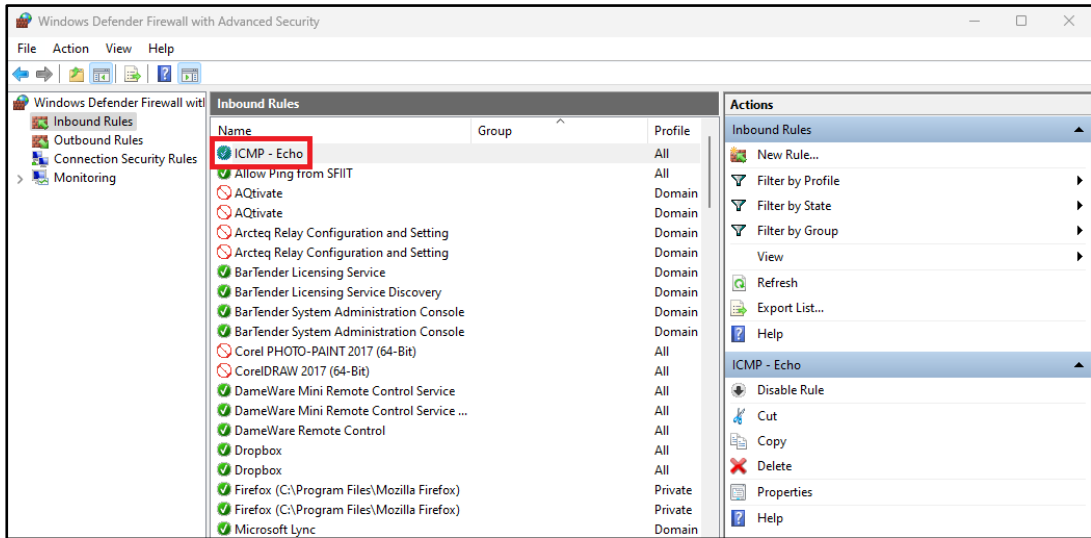
2.2 Whitelisting the AQtivate 200 application

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.
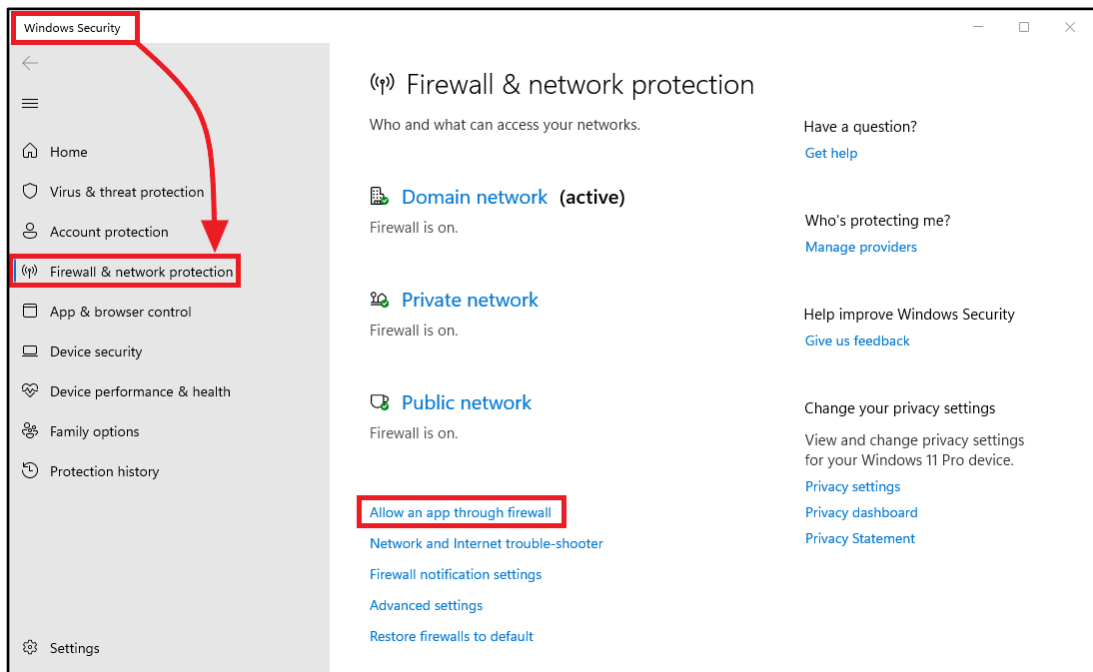
© Arcteq Relays Ltd.

Document ID: IM00085

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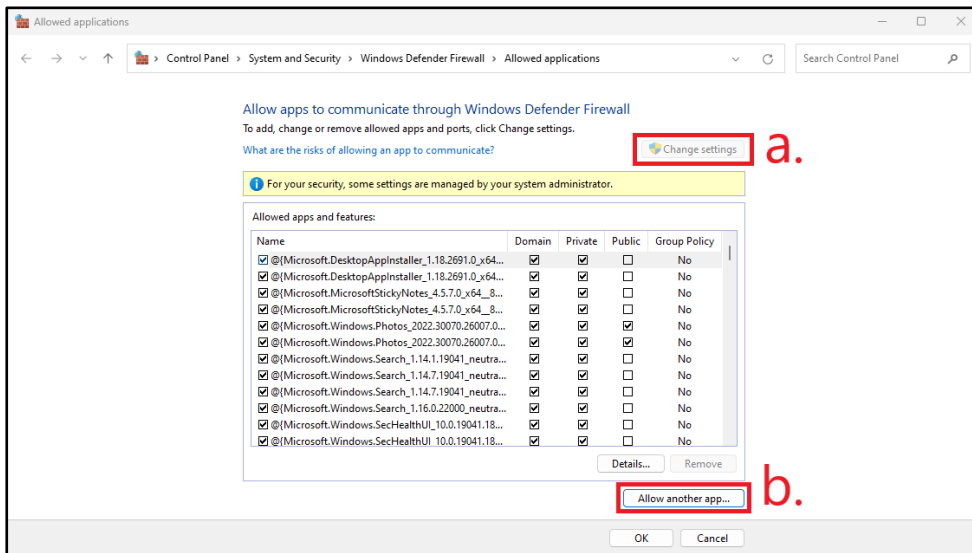
3. Click **Browse…** in the new dialog window (see the figure below).

Figure 2-2-3. Browsing for an application to add.
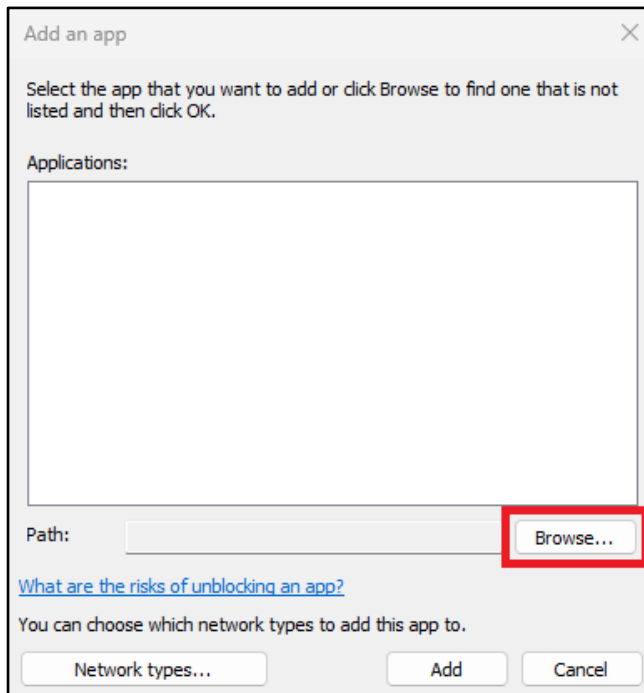
4. Find the folder where you have AQtivate 200 installed, select the application, and click **Open** (see the figure below).

Figure 2-2-4. Selecting the AQtivate 200 application.
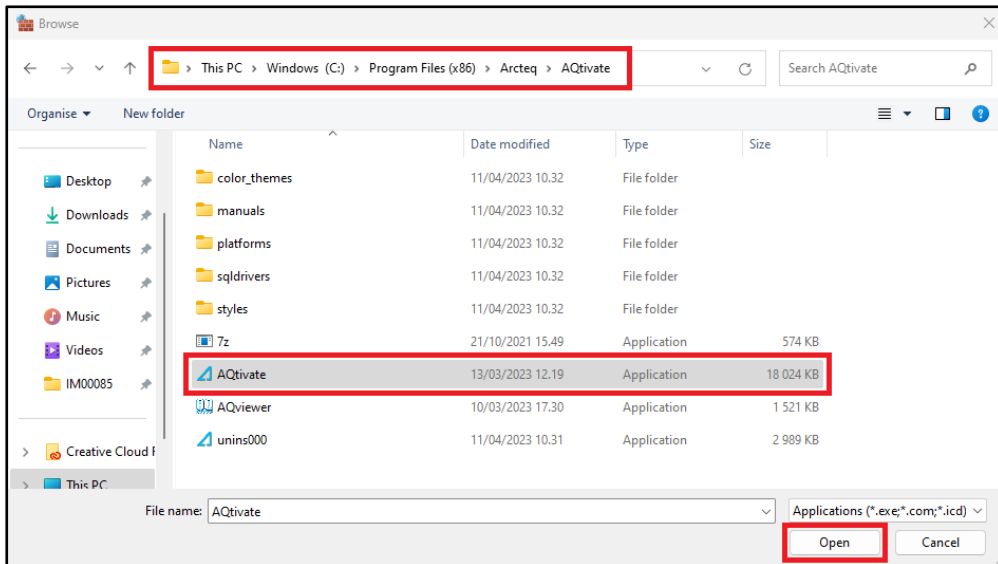
5. Select **Add** (see the figure below).

Figure 2-2-5. Adding AQtivate 200 to the whitelisted applications.
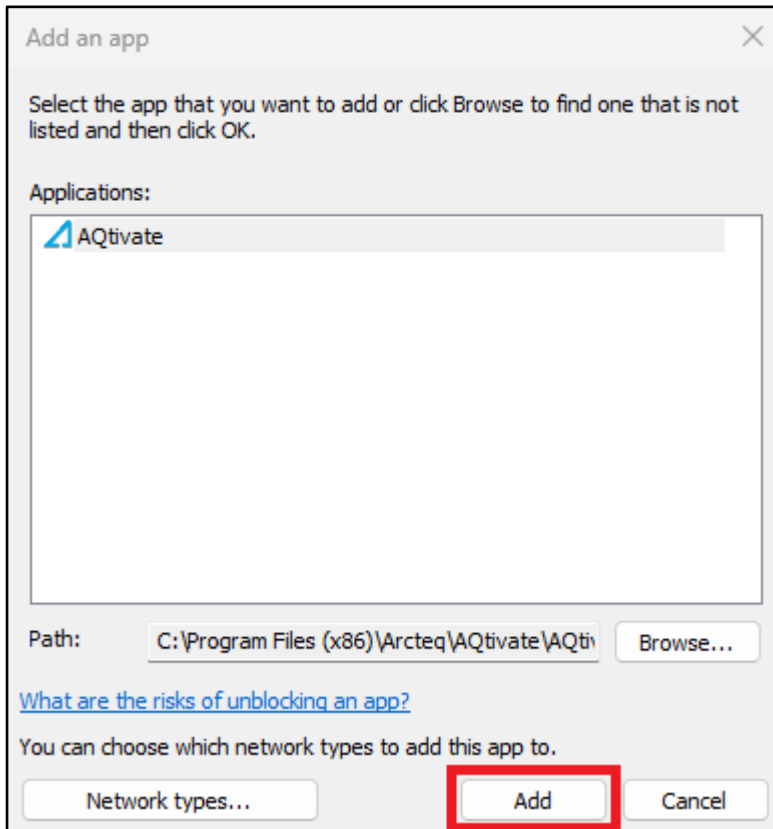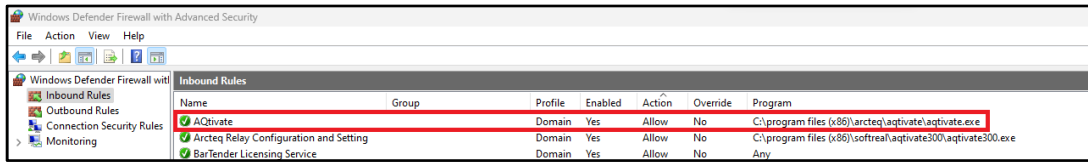
6. The AQtivate 200 application is now whitelisted in the list of allowed apps and features (see the figure below).

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

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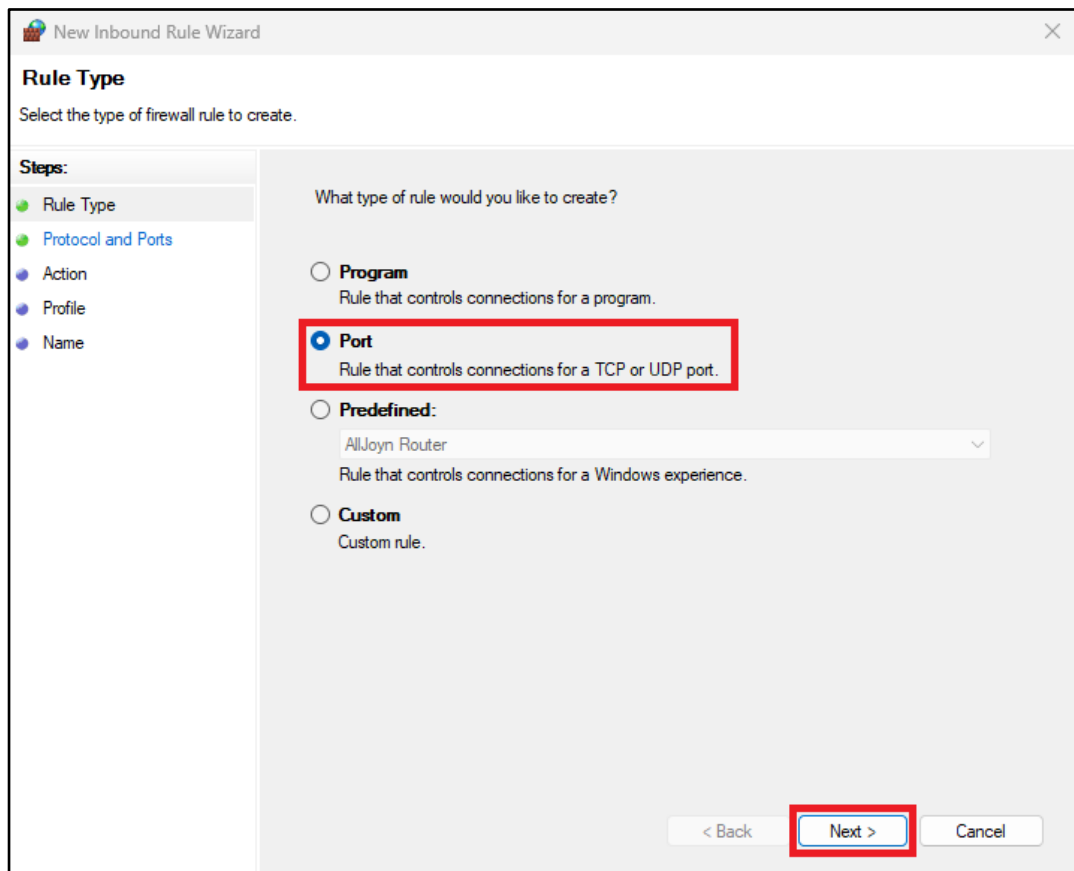
4. Select "UDP", specify that the rule only applies to the local port "69", and then click **Next** (see the figure below).

Figure 2-3-2. Defining the protocols and ports for the new rule.

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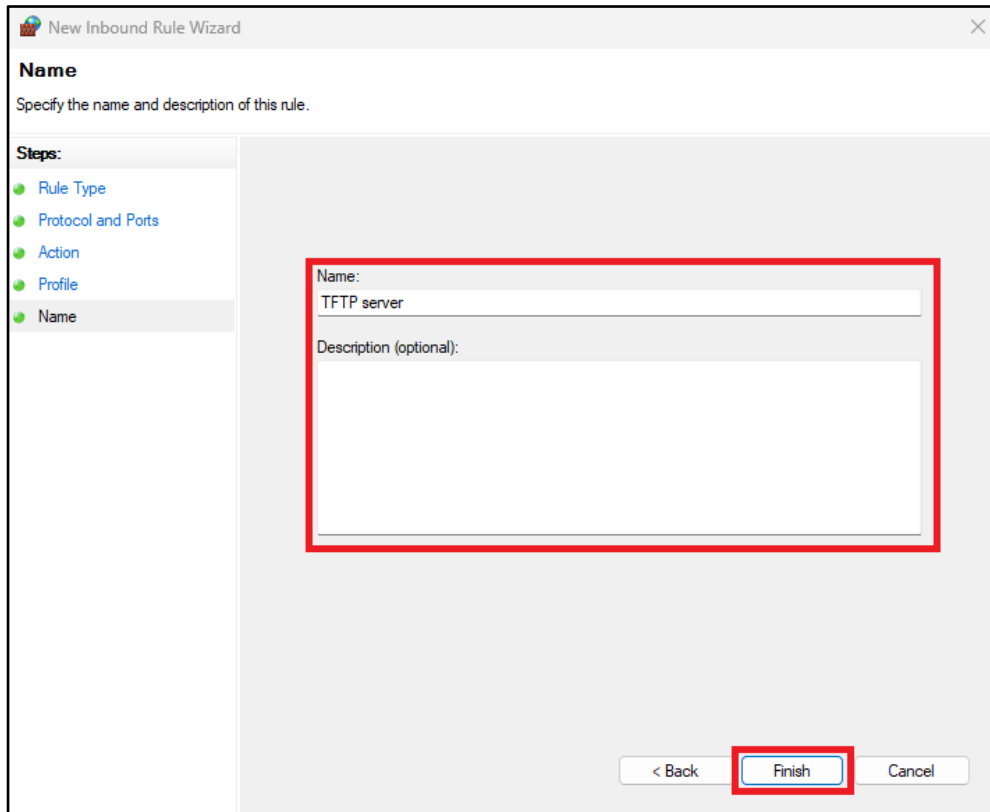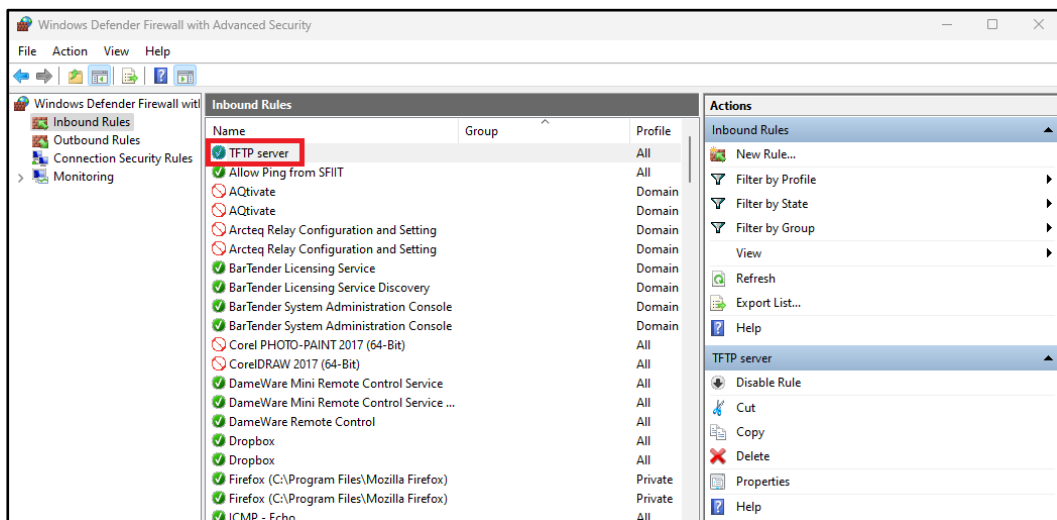
7. Finally, give your new rule a name and (optionally) a description; click **Finish** (see the figure below).

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

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.

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: www.arcteq.com
E-mail (sales): sales@arcteq.fi

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