

How to allow UBio Alpeta Server & Ports from the Windows firewall

Support Team

www.unioncomm.co.kr

How to allow UBio Alpeta Server & Ports from the Windows firewall

Step1> Open the Windows Firewall in the Control Panel and then select the “Allow an app or feature through Windows Firewall”

Windows Defender Firewall

Control Panel > All Control Panel Items > Windows Defender Firewall

Control Panel Home

[Allow an app or feature through Windows Defender Firewall](#)

Change notification settings

Turn Windows Defender Firewall on or off

Restore defaults

Advanced settings

Troubleshoot my network

Help protect your PC with Windows Defender Firewall

Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Update your Firewall settings

Windows Defender Firewall is not using the recommended settings to protect your computer.

[Use recommended settings](#)

[What are the recommended settings?](#)

Private networks Connected

Networks at home or work where you know and trust the people and devices on the network

Windows Defender Firewall state:	Off
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active private networks:	네트워크
Notification state:	Notify me when Windows Defender Firewall blocks a new app

Guest or public networks Not connected

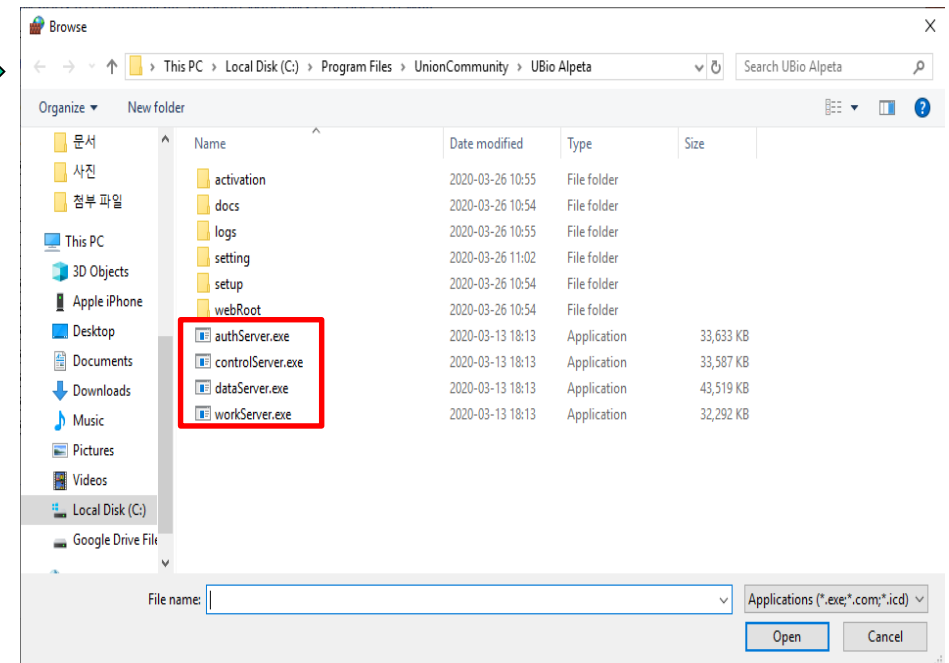
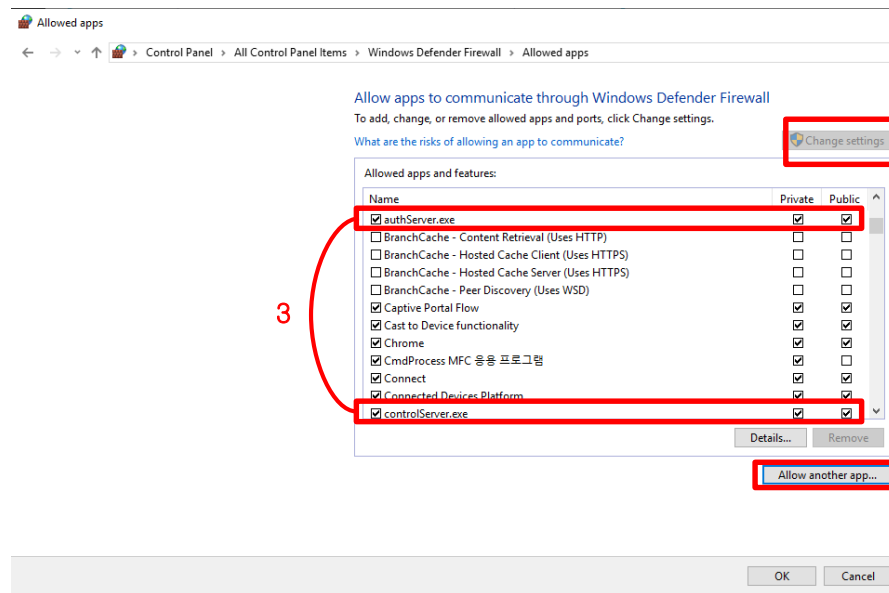
See also

Security and Maintenance

Network and Sharing Center

How to allow UBio Alpeta Server & Ports from the Windows firewall

Step2> Allow “authServer”, “controlServer”, “dataServer”, and “workServer” on the exception of the Windows Firewall in the Control Panel



How to allow UBio Alpeta Server & Ports from the Windows firewall

Step3> Open the Windows Firewall in the Control Panel and them select the “Advanced settings”

Windows Defender Firewall

Control Panel > All Control Panel Items > Windows Defender Firewall

Control Panel Home

- Allow an app or feature through Windows Defender Firewall
- Change notification settings
- Turn Windows Defender Firewall on or off
- Restore defaults
- Advanced settings**
- Troubleshoot my network

Help protect your PC with Windows Defender Firewall

Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Update your Firewall settings

Windows Defender Firewall is not using the recommended settings to protect your computer.

[What are the recommended settings?](#)

[Use recommended settings](#)

Private networks

Connected

Networks at home or work where you know and trust the people and devices on the network

Windows Defender Firewall state:	Off
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active private networks:	네트워크
Notification state:	Notify me when Windows Defender Firewall blocks a new app

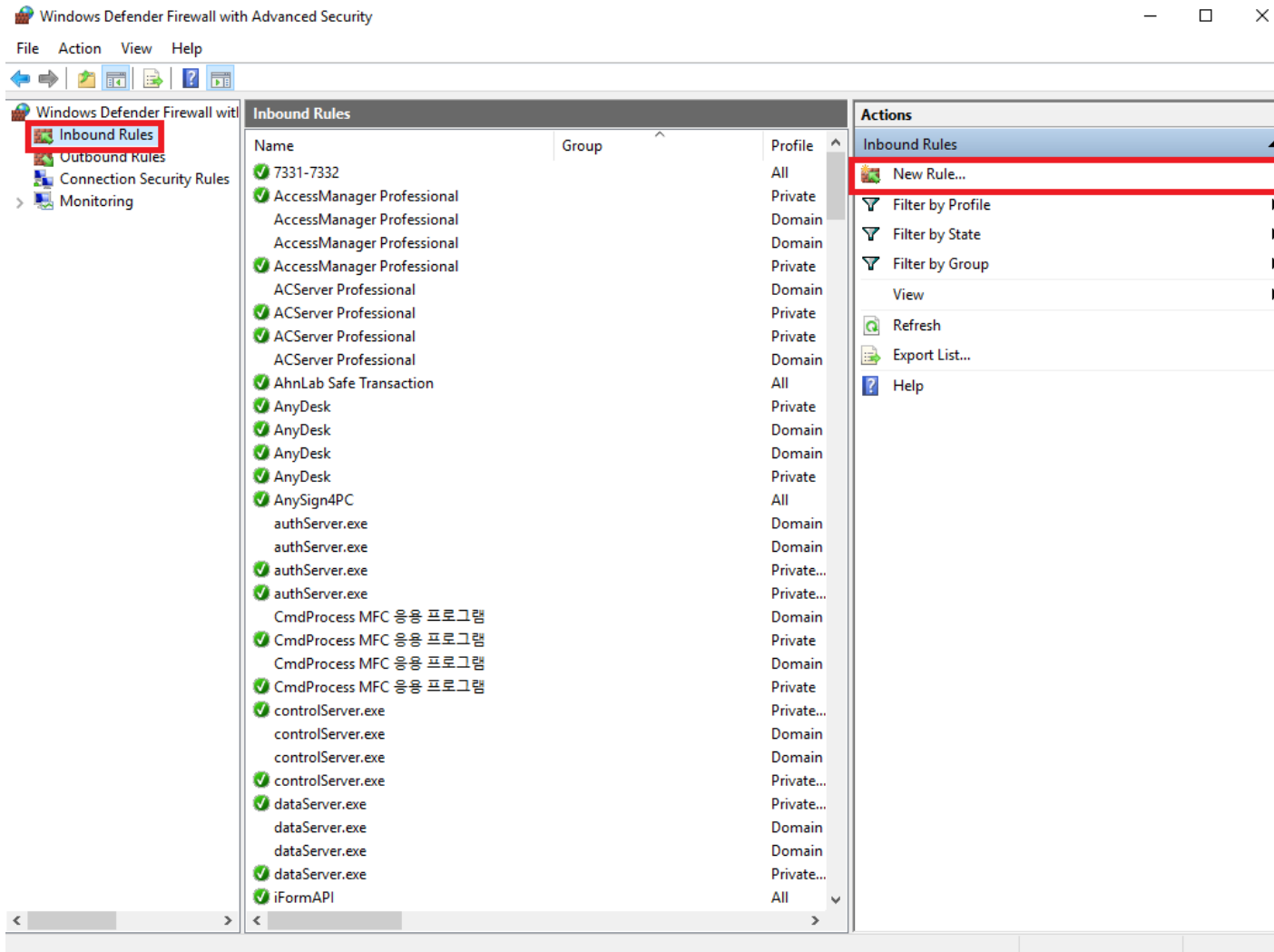
Guest or public networks

Not connected

See also

- Security and Maintenance
- Network and Sharing Center

Step4> Create the new rule in the “Inbound Rules”



How to allow UBio Alpeta Server & Ports from the Windows firewall

Step5> Select the “Port” and then click to “Next”

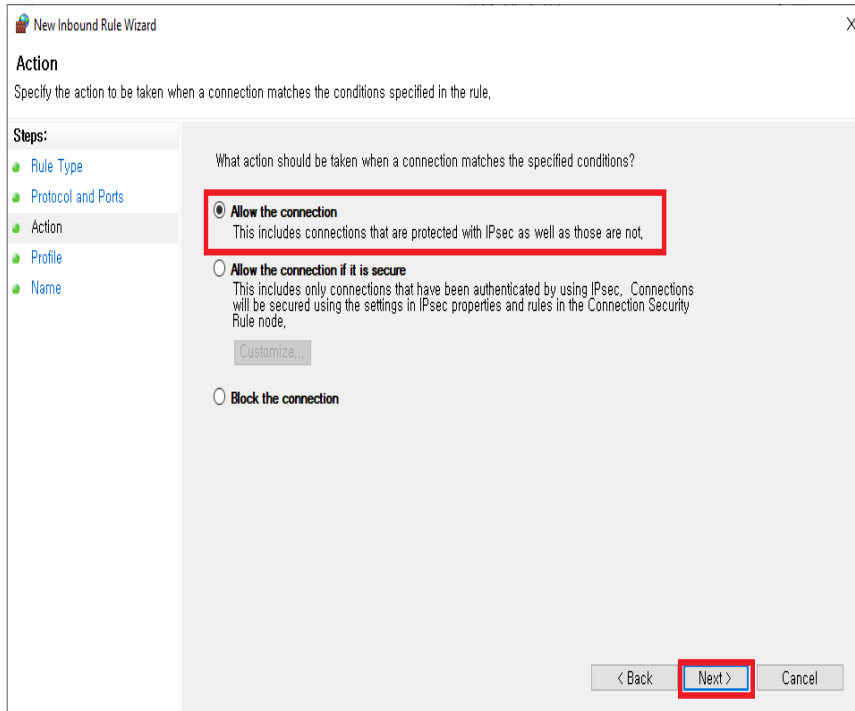
The screenshot shows the 'New Inbound Rule Wizard' window at the 'Rule Type' step. The left sidebar lists 'Steps: Rule Type', 'Protocol and Ports', 'Action', 'Profile', and 'Name'. The main area asks 'What type of rule would you like to create?' with three radio button options: 'Program' (Rule that controls connections for a program), 'Port' (Rule that controls connections for a TCP or UDP port), and 'Predefined:' (with a dropdown menu showing 'AllJoyn Router' and the description 'Rule that controls connections for a Windows experience'). The 'Port' option is selected and highlighted with a red rectangle. At the bottom, there are '< Back', 'Next >', and 'Cancel' buttons, with 'Next >' highlighted by a red rectangle.

Step6> Select the “TCP” and then insert the port number from 9001 to 9004 and then click to “Next”

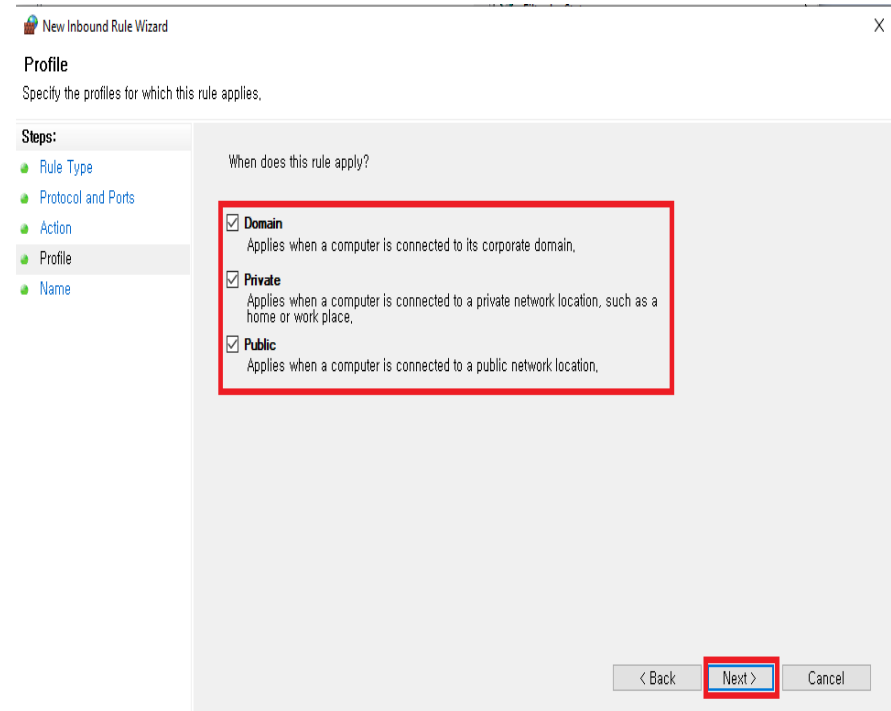
The screenshot shows the 'New Inbound Rule Wizard' window at the 'Protocol and Ports' step. The left sidebar lists 'Steps: Rule Type', 'Protocol and Ports', 'Action', 'Profile', and 'Name'. The main area asks 'Specify the protocols and ports to which this rule applies.' It has two sections. The first section asks 'Does this rule apply to TCP or UDP?' with radio button options for 'TCP' and 'UDP'. The 'TCP' option is selected and highlighted with a red rectangle. The second section asks 'Does this rule apply to all local ports or specific local ports?' with radio button options for 'All local ports' and 'Specific local ports:'. The 'Specific local ports:' option is selected and highlighted with a red rectangle, and its text box contains '9001-9004'. Below the text box is the example text 'Example: 80, 443, 5000-5010'. At the bottom, there are '< Back', 'Next >', and 'Cancel' buttons, with 'Next >' highlighted by a red rectangle.

How to allow UBio Alpeta Server & Ports from the Windows firewall

Step7> Select the “Allow the connection” and then click to “Next”

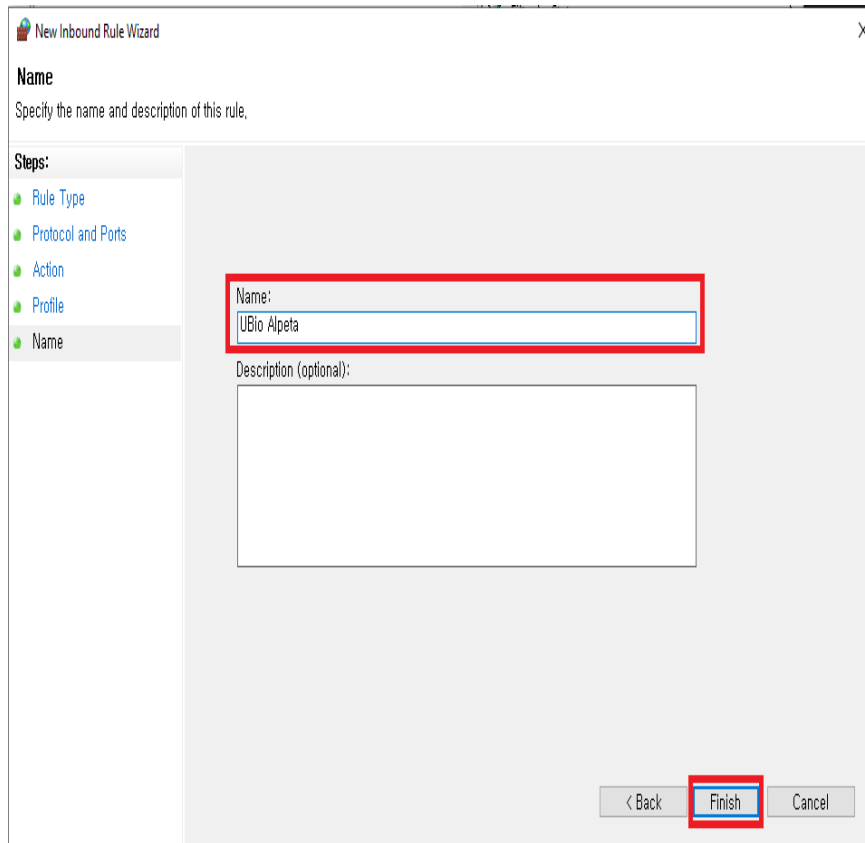


Step8> Select all of the “Profiles” and then click to “Next”



How to allow UBio Alpeta Server & Ports from the Windows firewall

Step9>Give the name of the rule and then click to “Finish”



Step10> Check the created rule in the Inbound Rules List

