

Port 4004 Status Check and Closure Procedure

■ Purpose of this document

This document provides instructions on how to check firewall settings and steps to close specific ports to address vulnerabilities in environments with Xerox FreeFlow Core running in your environment.

■ Procedure

Please check the following three in order.

1. [Check your firewall settings.](#)
2. [Check the status of a specific port.](#)
3. [Close firewall ports.](#)

1. Check your firewall settings.

Open “Windows Settings” and select “Privacy & Security” on the left.
(For Windows Server 2022, it is “Update & Security”.)

Click “Windows Security” to open the “Windows Security dialog”.

Open “Home” in the “Windows Security dialog”, you can see the status of your firewall and network protection.

If “Firewall & Network Protection” has a green checkmark and says No action required, there is no problem.

Click “Firewall & Network Protection” on the left, and check the configuration status of domain, private, and public networks.

If your network says Firewall is enabled, the firewall is enabled.

Note

Even if it says “Firewall is disabled”, it doesn’t mean there’s an immediate problem.

If your network environment has integrated security management services in place, it may be protected by services other than Windows Firewall.

In this case, please check the configuration status of the specific port in the next step.

2. Check the status of a specific port.

You can use PowerShell, which is standard with Windows OS, to check if a specific port is allowed to connect.

Launch “Windows PowerShell” from the Windows search menu.

Enter the IP address into the < IP >.

Enter the port number into the < PortNumber>, and press Enter.

```
Test-NetConnection -ComputerName <IP> -Port <PortNumber>
```

If you get a response like the following, <PortNumber> is closed and cannot be connected.

```
Warning: TCP connect to (<IP> : <PortNumber>) failed
```

```
ComputerName           : <IP>
RemoteAddress          : <IP>
RemotePort             : <PortNumber>
InterfaceAlias         :
SourceAddress          : <IP>
PingSucceeded          : True
PingReplyDetails (RTT) : 0 ms
TcpTestSucceeded       : False
```

When <PortNumber> the connection is allowed, you will see the following.

```
ComputerName           : <IP>
RemoteAddress          : <IP>
RemotePort             : <PortNumber>
InterfaceAlias         :
SourceAddress          : <IP>
PingSucceeded          : True
PingReplyDetails (RTT) : 0 ms
TcpTestSucceeded       : True
```

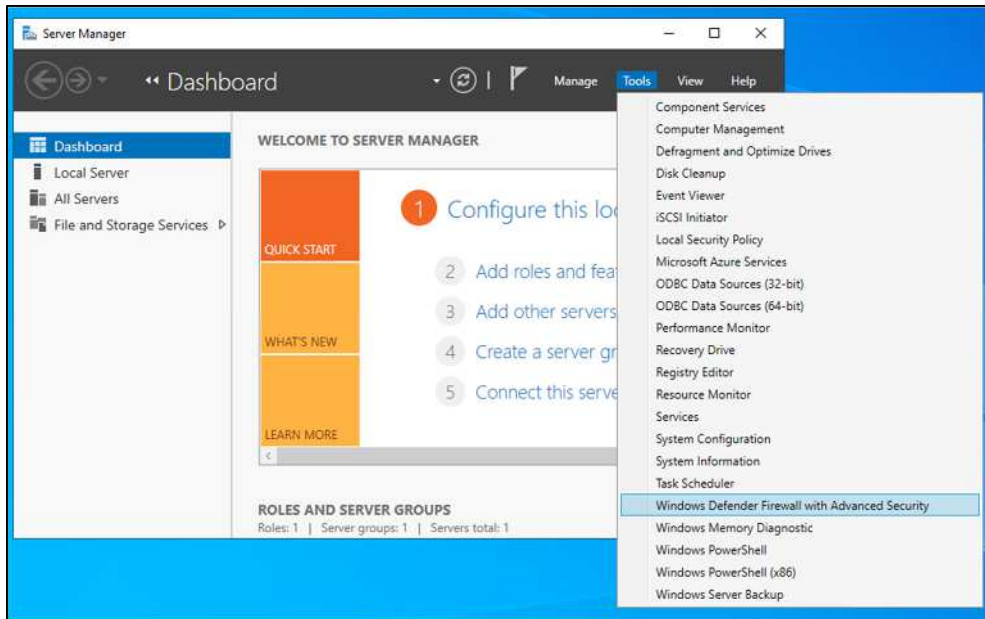
If the above checks allow a port that should not be allowed to be connected, follow the steps to close the specific port in the next step.

3. Close firewall ports.

The following is an example of Windows Server 2022.

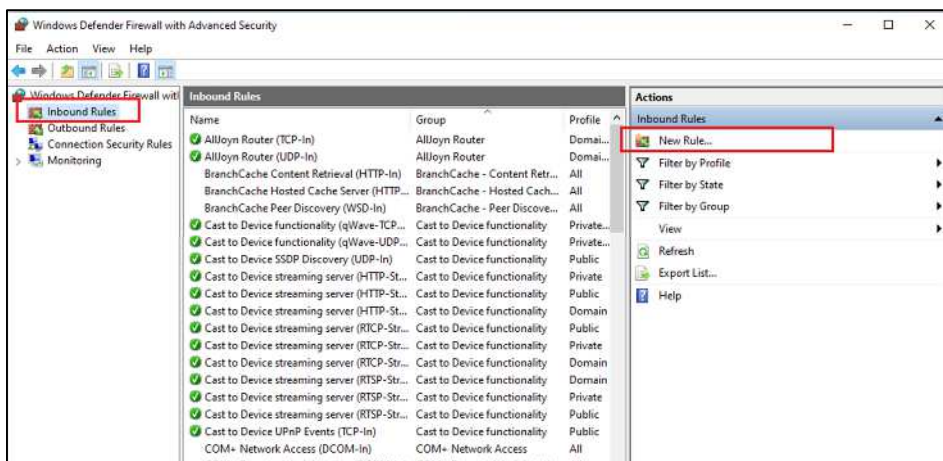
Select “Start” and select “launch Server Manager”.

Select “Tools” and select “Windows Defender Firewall with Advanced security”.



In the left window of “Windows Defender Firewall with Advanced security” click “Inbound Rules”.

Then in the right window click “New Rule...”.



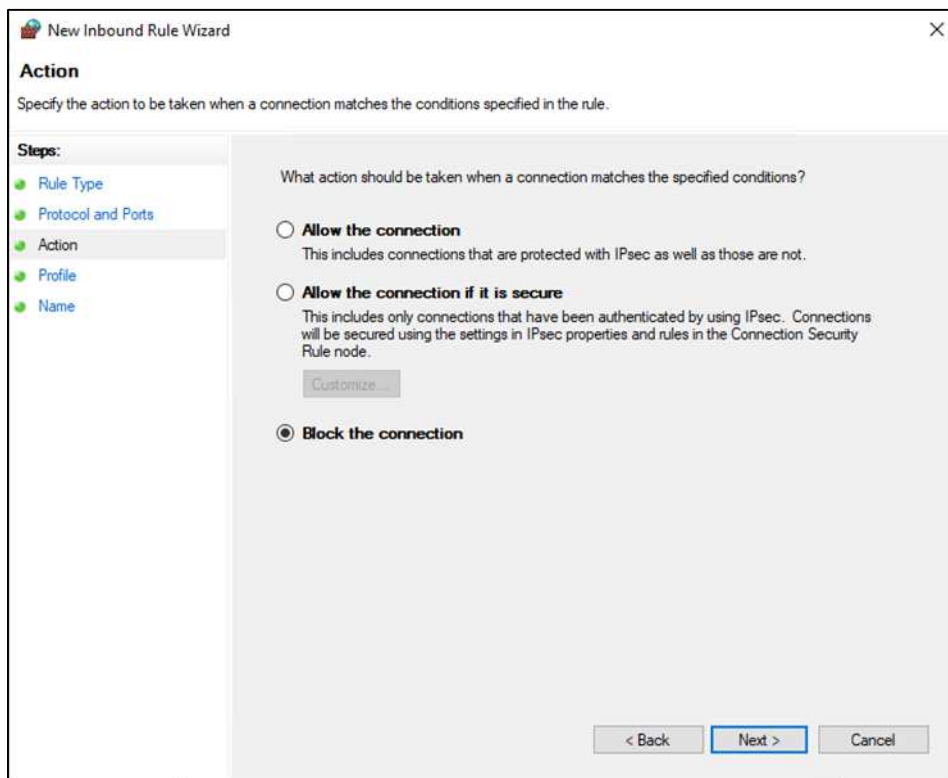
In the “Rule Type”, select “Port”, and then click ”Next”.

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

In the “Protocols and Ports”, select “TCP”, “Specific local ports”, enter the port number xxx, and click “Next”.

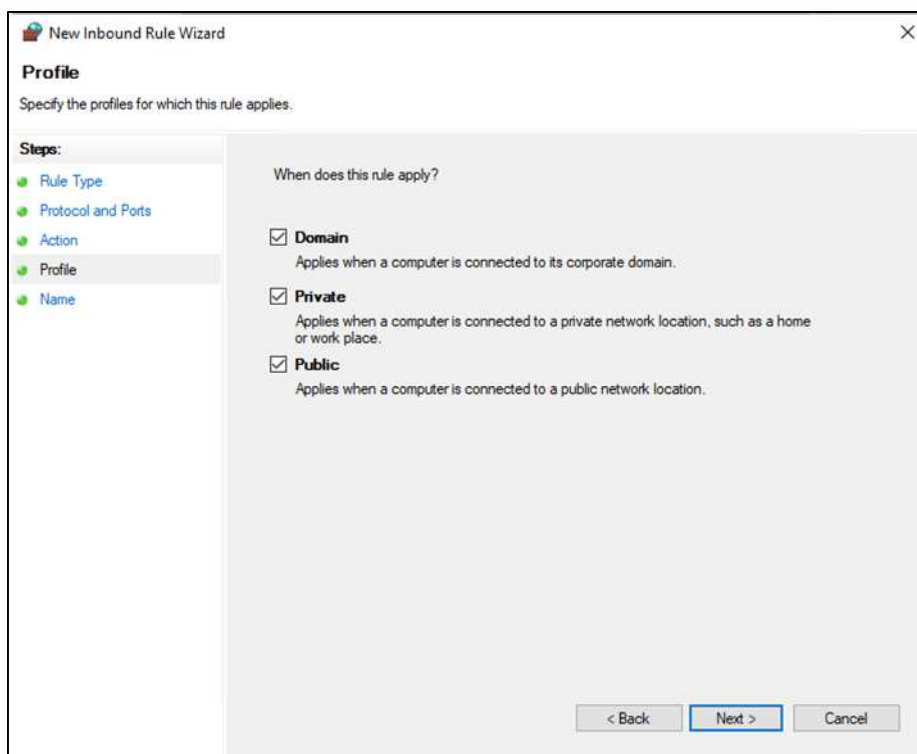
The screenshot shows the 'New Inbound Rule Wizard' window at the 'Protocol and Ports' step. The title bar reads 'New Inbound Rule Wizard'. The main heading is 'Protocol and Ports' with the instruction 'Specify the protocols and ports to which this rule applies.' On the left, the 'Steps:' pane shows 'Rule Type' and 'Protocol and Ports' as completed steps. The main area asks 'Does this rule apply to TCP or UDP?' with 'TCP' selected. Below, it asks 'Does this rule apply to all local ports or specific local ports?' with 'Specific local ports:' selected. A text input field is provided for specific ports, with an example '80, 443, 5000-5010' shown below it. At the bottom right are '< Back', 'Next >', and 'Cancel' buttons.

In the “Action”, select “Block the connection”, and click “Next”.



The screenshot shows the 'New Inbound Rule Wizard' window at the 'Action' step. The title bar reads 'New Inbound Rule Wizard'. The main heading is 'Action' with the instruction 'Specify the action to be taken when a connection matches the conditions specified in the rule.' On the left, a 'Steps:' list includes 'Rule Type', 'Protocol and Ports', 'Action' (highlighted), 'Profile', and 'Name'. The main area asks 'What action should be taken when a connection matches the specified conditions?' and offers three radio button options: 'Allow the connection' (with a description about IPsec), 'Allow the connection if it is secure' (with a description about IPsec authentication and a 'Customize...' button), and 'Block the connection' (which is selected). At the bottom right are '< Back', 'Next >', and 'Cancel' buttons.

In the “profile”, check “Domain”, “Private”, and “Public”, and click “Next”.



The screenshot shows the 'New Inbound Rule Wizard' window at the 'Profile' step. The title bar reads 'New Inbound Rule Wizard'. The main heading is 'Profile' with the instruction 'Specify the profiles for which this rule applies.' On the left, a 'Steps:' list includes 'Rule Type', 'Protocol and Ports', 'Action', 'Profile' (highlighted), and 'Name'. The main area asks 'When does this rule apply?' and features three checked checkboxes: 'Domain' (with description: 'Applies when a computer is connected to its corporate domain.'), 'Private' (with description: 'Applies when a computer is connected to a private network location, such as a home or work place.'), and 'Public' (with description: 'Applies when a computer is connected to a public network location.'). At the bottom right are '< Back', 'Next >', and 'Cancel' buttons.

In “Name”, enter a name and description of your choice, and click “Finish”.

The screenshot shows a Windows-style dialog box titled "New Inbound Rule Wizard" with a close button (X) in the top right corner. The dialog is divided into two main sections. On the left is a "Steps:" sidebar containing a list of steps: "Rule Type", "Protocol and Ports", "Action", "Profile", and "Name". The "Name" step is currently selected and highlighted. The main area of the dialog is titled "Name" and contains the instruction "Specify the name and description of this rule." Below this instruction are two input fields: a single-line text box labeled "Name:" and a larger multi-line text box labeled "Description (optional):". At the bottom right of the dialog are three buttons: "< Back", "Finish" (which is highlighted with a blue border), and "Cancel".

- Eligible products and versions
Xerox FreeFlow Core All versions

September 2025
FUJIFILM Business Innovation Corp.