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.

```
Warnning: 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
```

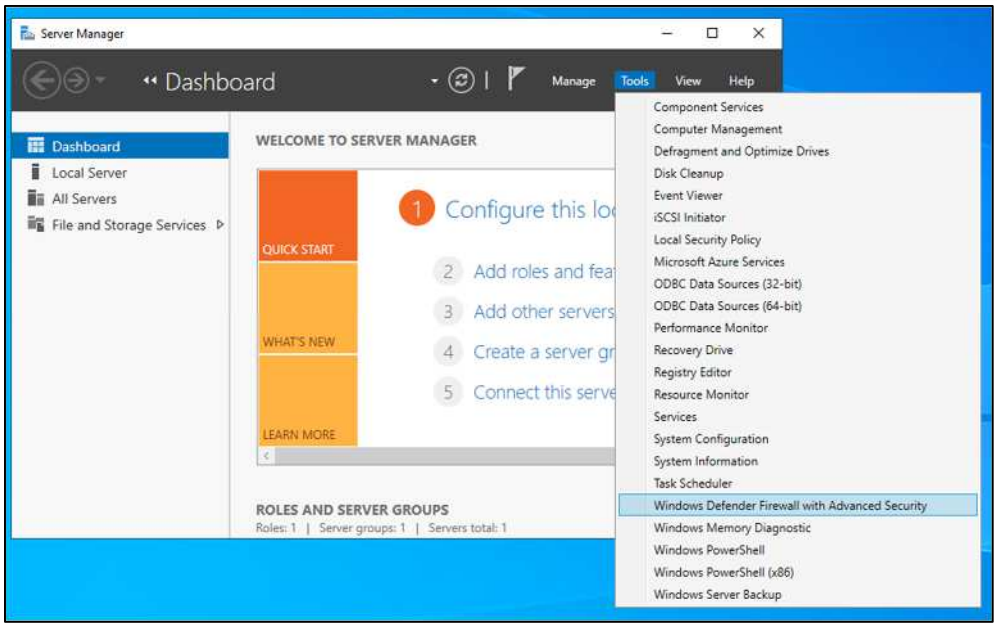
If the above checks allow a port that should not be allowed to be connected, follow the steps to close the specific port in the next step.

3. Close firewall ports.

The following is an example of Windows Server 2022.

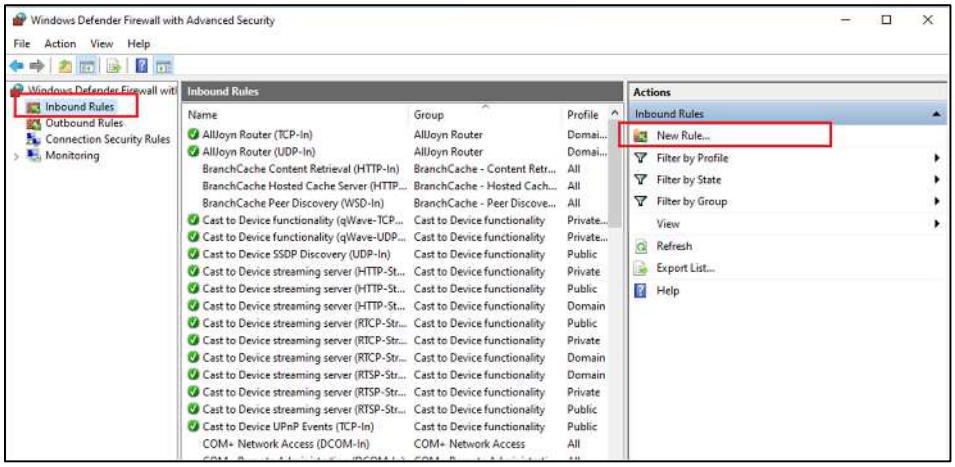
Select “Start” and select “launch Server Manager”.

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

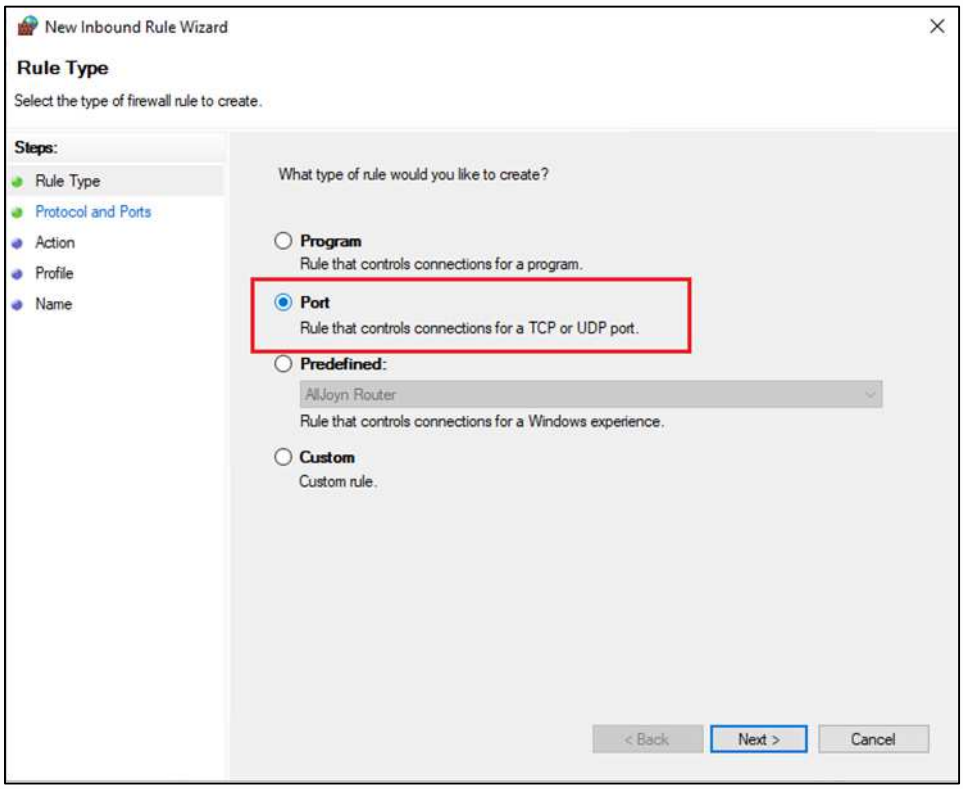


In the left window of “Windows Defender Firewall with Advanced security” click “Inbound Rules”.

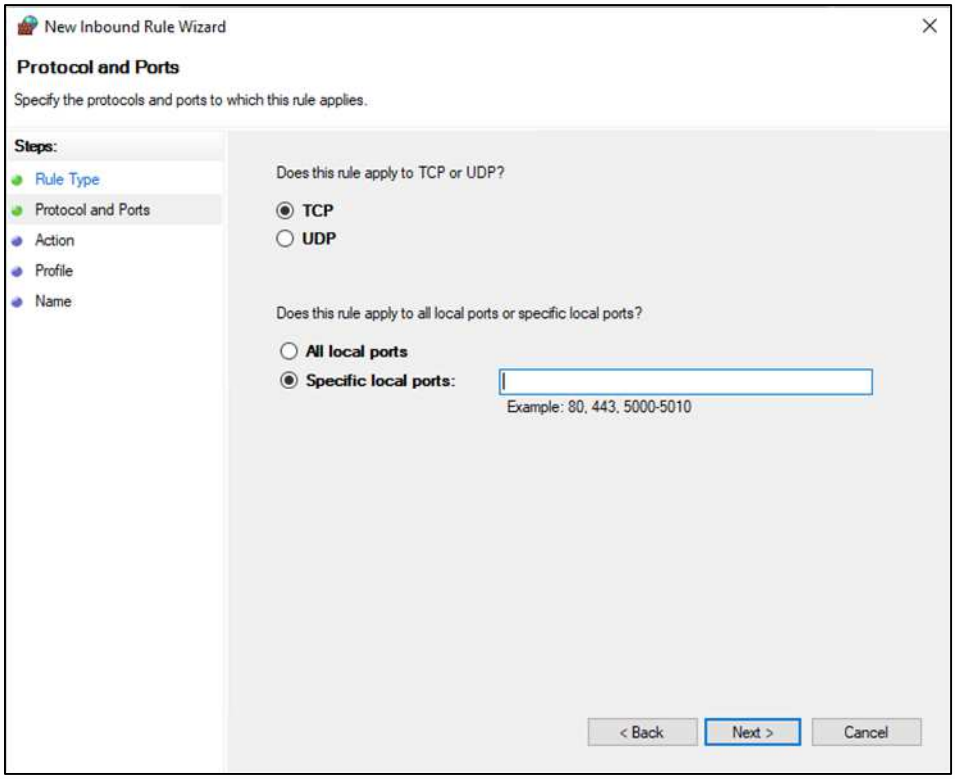
Then in the right window click ”New Rule...”.



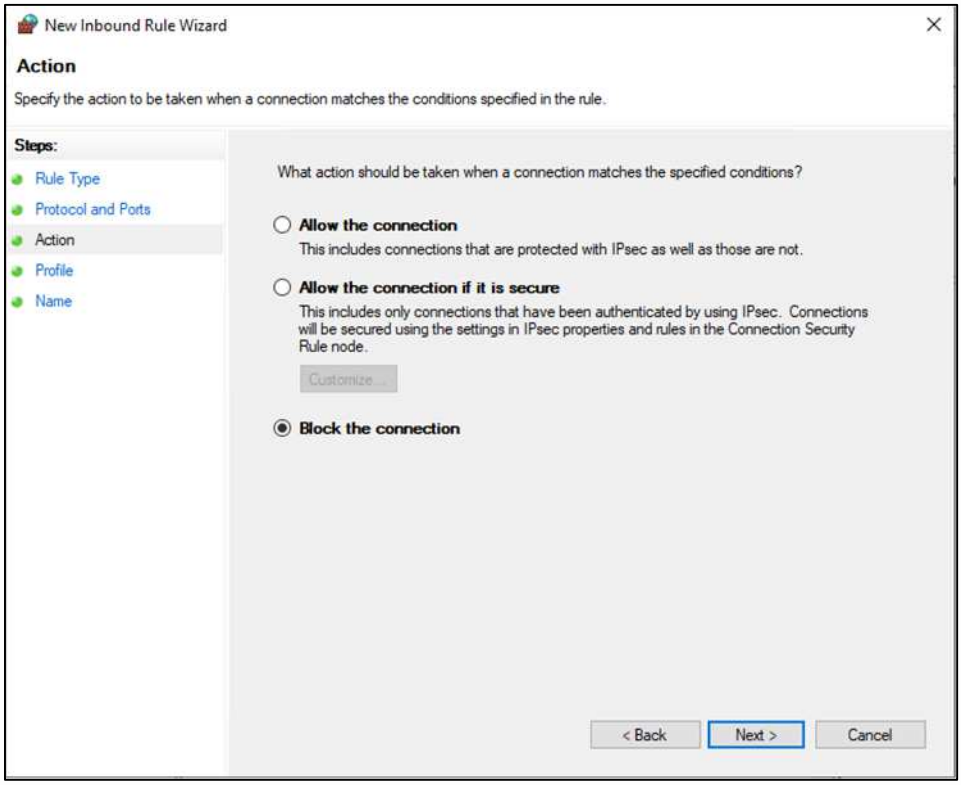
In the “Rule Type”, select “Port”, and then click ”Next”.



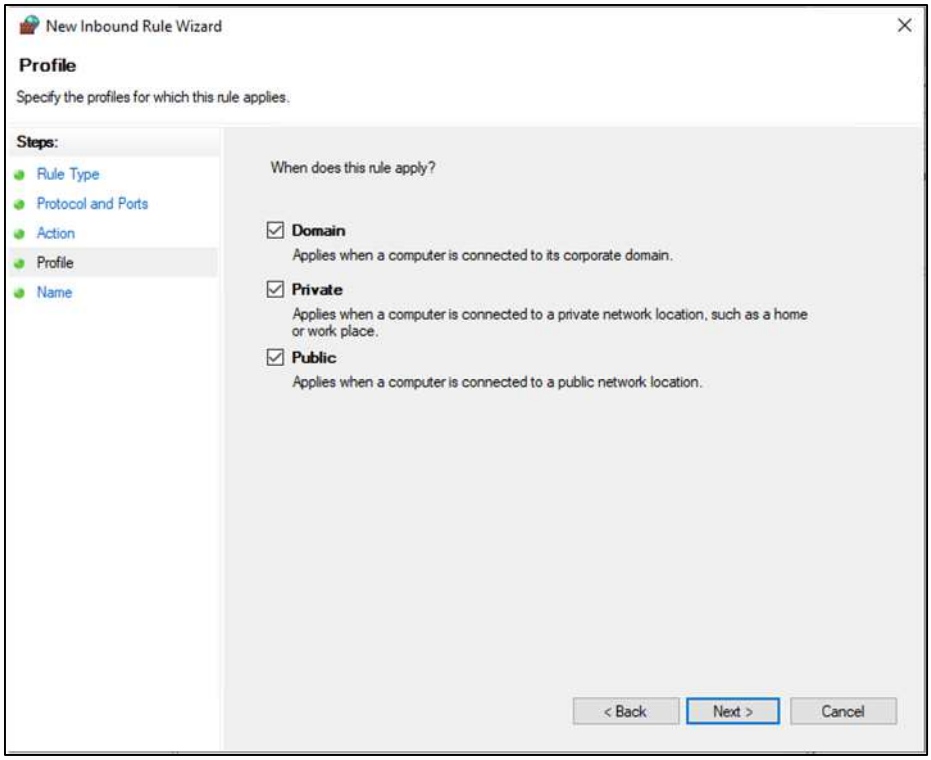
In the “Protocols and Ports”, select “TCP”, “Specific local ports”, enter the port number xxx, and click “Next”.



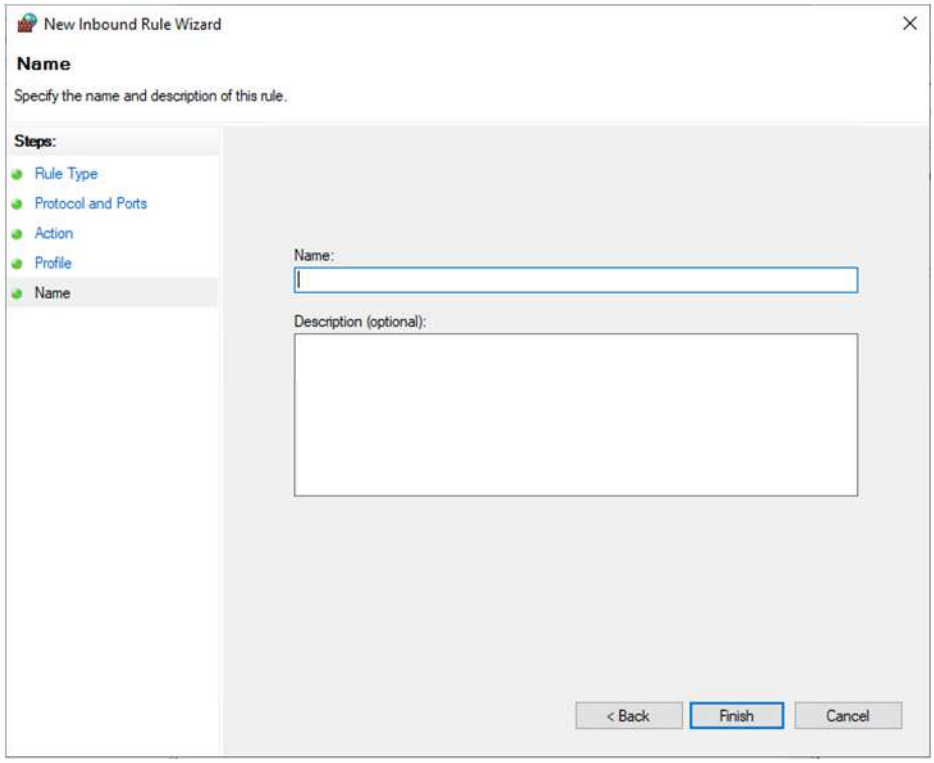
In the “Action”, select ”Block the connection”, and click ”Next”.



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



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



■Eligible products and versions

Xerox FreeFlow Core All versions

September 2025

FUJIFILM Business Innovation Corp.