

KF Comm 2 Software: OPC UA Port Setup

Abstract:

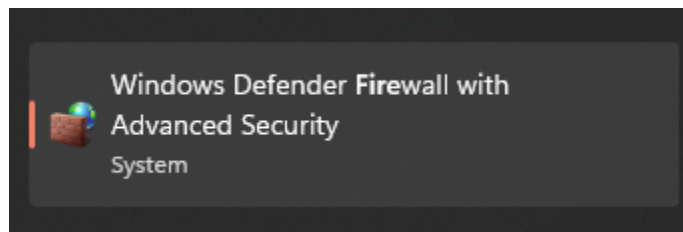
This article describes how to connect KF Comm 2 Software to an external client through an OPC UA server for monitoring purposes.

Applicability:

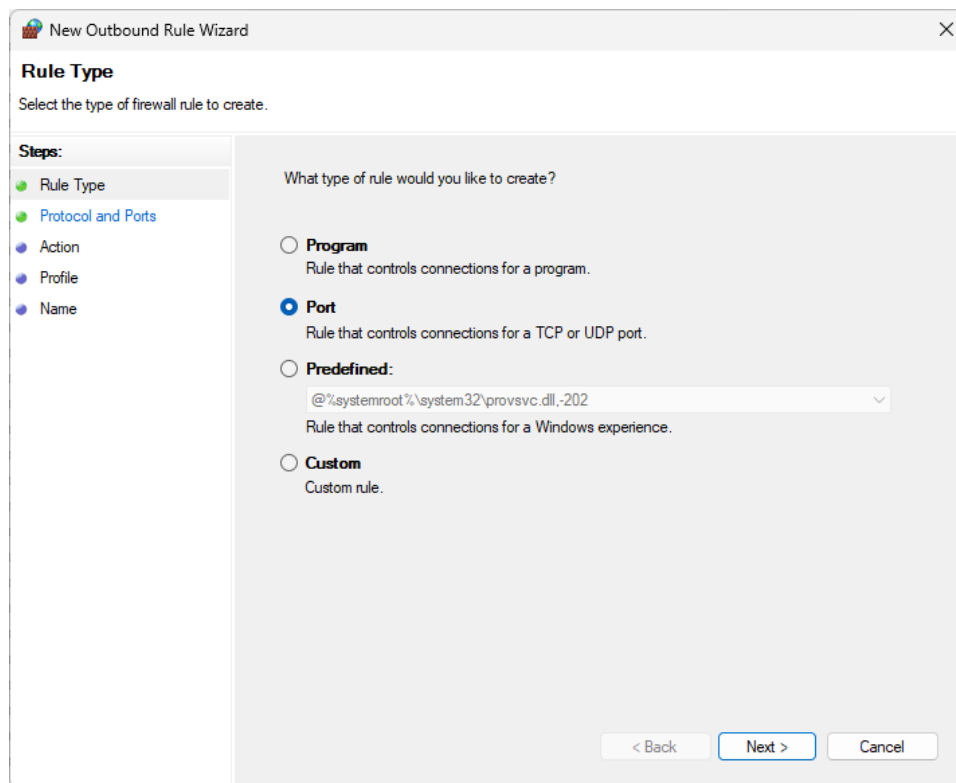
This functionality is available in KF Comm 2 software version 3.2.7 or newer.

KF Comm PC

1. On the PC running KF Comm 2 software, open Windows Defender Firewall with Advanced Security. You may need to run as administrator.



2. Click on Outbound Rules in the left sidebar.
3. Click New Rule... in the right sidebar.
4. **Rule Type:** Select Port.



5. **Protocol and Ports:** Leave the first choice as TCP. Choose Specific remote ports for the second and enter “20794” in the text field.

The screenshot shows the 'New Outbound Rule Wizard' dialog box, specifically the 'Protocol and Ports' step. The title bar reads 'New Outbound 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, a 'Steps:' pane lists 'Rule Type', 'Protocol and Ports' (highlighted), 'Action', 'Profile', and 'Name'. The main area contains two questions: 'Does this rule apply to TCP or UDP?' with 'TCP' selected, and 'Does this rule apply to all remote ports or specific remote ports?' with 'Specific remote ports:' selected. A text field next to 'Specific remote ports:' contains '20794|' with a blue border. Below it, an example text reads 'Example: 80, 443, 5000-5010'. At the bottom right are '< Back', 'Next >', and 'Cancel' buttons.

6. **Action:** Choose Allow the connection.

The screenshot shows the 'New Outbound Rule Wizard' dialog box, specifically the 'Action' step. The title bar reads 'New Outbound 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:' pane lists 'Rule Type', 'Protocol and Ports', 'Action' (highlighted), 'Profile', and 'Name'. The main area contains the question 'What action should be taken when a connection matches the specified conditions?' with three options: 'Allow the connection' (selected), 'Allow the connection if it is secure', and 'Block the connection'. The 'Allow the connection' option has a description: 'This includes connections that are protected with IPsec as well as those are not.' The 'Allow the connection if it is secure' option has a description: 'This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.' Below this is a 'Customize...' button. At the bottom right are '< Back', 'Next >', and 'Cancel' buttons.

7. **Profile:** At a minimum, check Domain and Private. To reduce troubleshooting, it is recommended to check Public as well.

The screenshot shows the 'New Outbound Rule Wizard' window at the 'Profile' step. The title bar reads 'New Outbound 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 is titled 'When does this rule apply?' and contains three checked options: 'Domain' (Applies when a computer is connected to its corporate domain.), 'Private' (Applies when a computer is connected to a private network location, such as a home or work place.), and 'Public' (Applies when a computer is connected to a public network location.). At the bottom right are buttons for '< Back', 'Next >', and 'Cancel'.

8. **Name:** This will not affect the software functionality, but enter a descriptive name to identify this rule in case it needs to be modified later.

The screenshot shows the 'New Outbound Rule Wizard' window at the 'Name' step. The title bar reads 'New Outbound Rule Wizard'. The main heading is 'Name' with the instruction 'Specify the name and description of this rule.' On the left, a 'Steps:' list includes 'Rule Type', 'Protocol and Ports', 'Action', 'Profile', and 'Name' (highlighted). The main area has a 'Name:' label followed by a text box containing 'KFCComm OPC'. Below it is a 'Description (optional):' label followed by a larger text box. At the bottom right are buttons for '< Back', 'Finish', and 'Cancel'.

Client PC

9. On the client PC, open Windows Defender Firewall with Advanced Security. You may need to run as administrator.
10. Click on Inbound Rules in the left sidebar.
11. Repeat steps 3 through 8 above.
12. Get the IP address of the PC running KF Comm 2 software. This can be done by opening the Command Prompt and typing the command "ipconfig" under the IPv4 address.
13. Run the Command Prompt as an administrator on the server.
14. Enter the following command, replacing **PUBLIC_IP** with the IP address of the PC running KF Comm 2 software:

```
netsh interface portproxy add v4tov4 listenaddress=*PUBLIC_IP* listenport=20794  
connectaddress=127.0.0.1 connectport=20794
```

15. On the client PC, try to connect using DataFeed or UA Expert. If successful, connect using your OPC UA client.

Prepared By:

Repligen Corporation

Process Analytics

685 Route 202/206 Bridgewater, NJ 08807

☎ +1 908-707-1009

✉ analytics-support@repligen.com