How to enable the OPC UA server in Kepware (KEPServerEX) for remote access

The OPC UA server interface in KEPServerEX lets remote systems connect to the server for client connections, diagnostics, or linking two OPC servers. This guide shows you how to enable the OPC UA server in Kepware for remote clients. You enable the host name endpoint, open the OPC UA port in Windows Defender Firewall, trust the client certificate, and then browse and monitor tags from a remote OPC UA client.

Prerequisites

Before you begin, make sure you have the following:

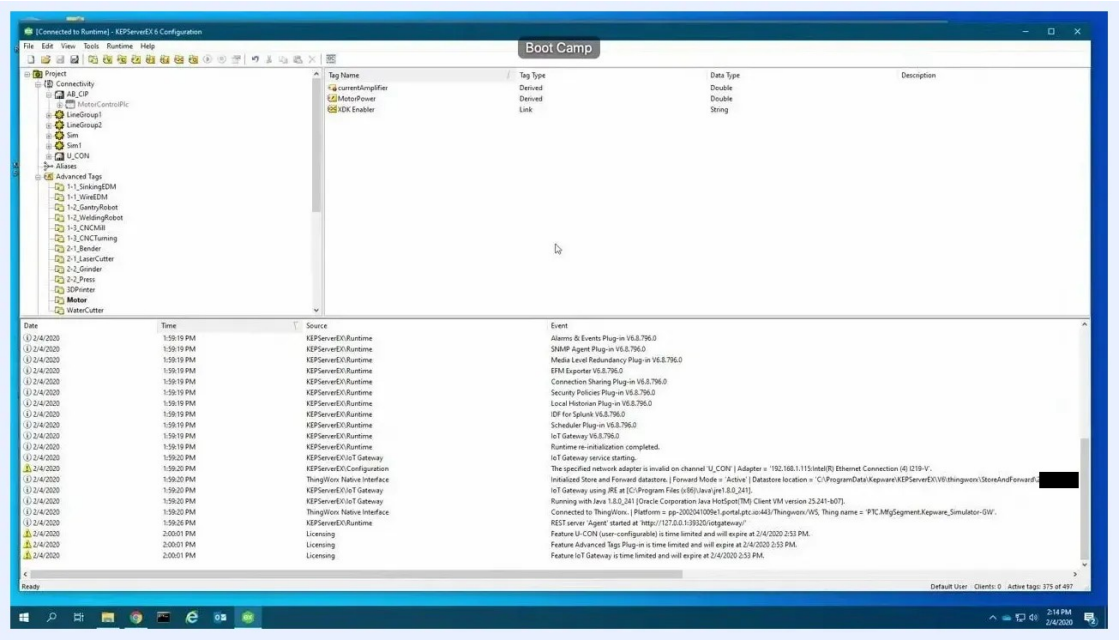
- The KEPServerEX Configuration application and a project that contains simulated or real data, with devices and tags already configured.
- Access to the Windows Start menu on the KEPServerEX machine. You may need to run the OPC UA Configuration utility as an administrator.
- Access to Windows Defender Firewall with Advanced Security on the same machine.
- A remote machine with an OPC UA client application, such as Prosys OPC UA Client. The client machine can run Mac, Windows, or Linux.

Enable the OPC UA server interface

Step 1: Open KEPServerEX and review your project

1. Launch the KEPServerEX Configuration application.
2. Open the project that contains your simulated or real data.

3. Review the project tree and confirm that your devices and tags are configured.



KEPServerEX Configuration application with a project loaded, showing the device and tag structure, the event log at the bottom, and the menus and toolbars at the top

Step 2: Check the OPC UA server channel status

1. In the project tree, right-click your project.
2. Locate the "OPC UA Server Channel" entry.
3. Confirm that the "Server Interface" is enabled.

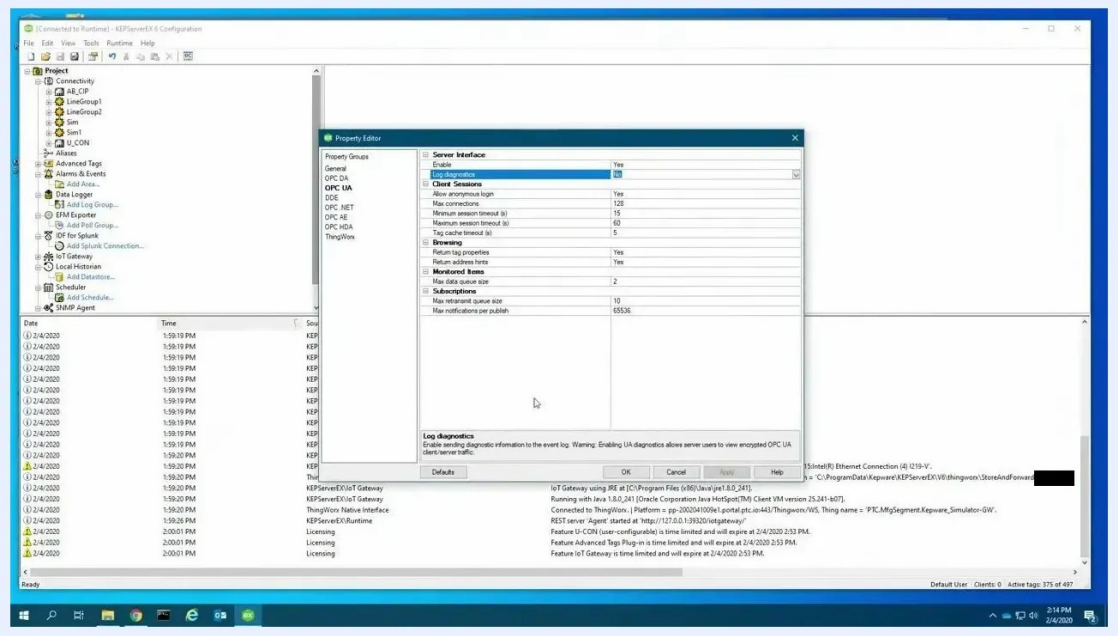
This area controls logging information only. It does not provide the full OPC UA server setup.

Step 3: Launch the OPC UA Configuration utility

You don't configure the OPC UA server interface in the KEPServerEX Configuration application. Minimize or close that window if needed, and then open the separate OPC UA Configuration utility.

1. Open the Windows Start menu.
2. Go to **All Programs > Kepware**.
3. Select **OPC UA Configuration**.

4. If prompted, right-click and choose "Run as administrator".



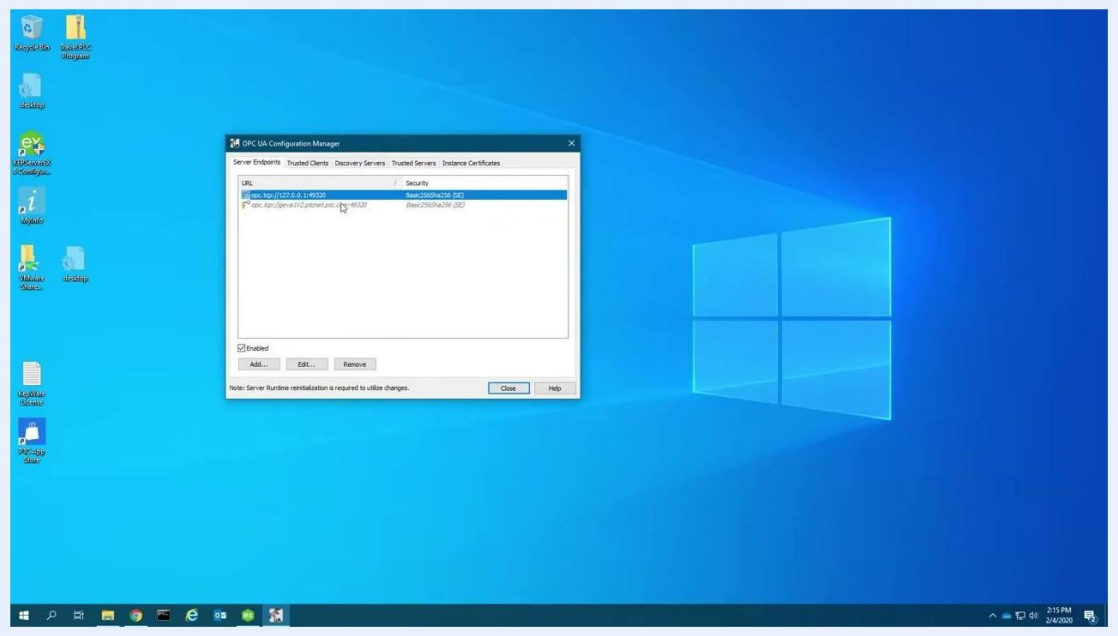
Windows desktop with the Start menu open, highlighting the OPC UA Configuration utility in the Kepware program group

Step 4: Review the default OPC UA endpoints

In the OPC UA Configuration Manager, open the **Server Endpoints** tab. Two default endpoints appear:

- opc.tcp://127.0.0.1:49320: the localhost endpoint, enabled by default. It allows local access to the OPC UA server interface and is used by OPC Quick Client.

- A second endpoint that uses the actual host name of your machine. It is disabled by default for security.

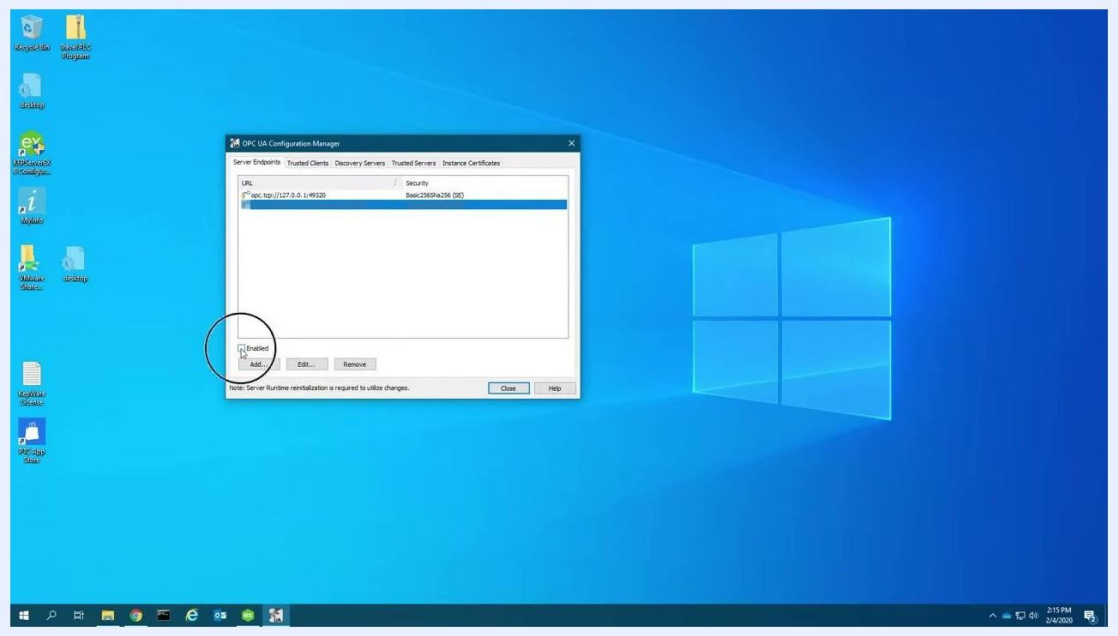


OPC UA Configuration Manager showing two server endpoints, with the localhost endpoint enabled and the host name endpoint disabled

Step 5: Enable the host name endpoint for remote access

1. In the **OPC UA Configuration Manager**, locate the endpoint with your computer's host name, for example opc.tcp://[hostname]:49320.

2. Select the **Enabled** check box next to this endpoint so remote clients can connect.

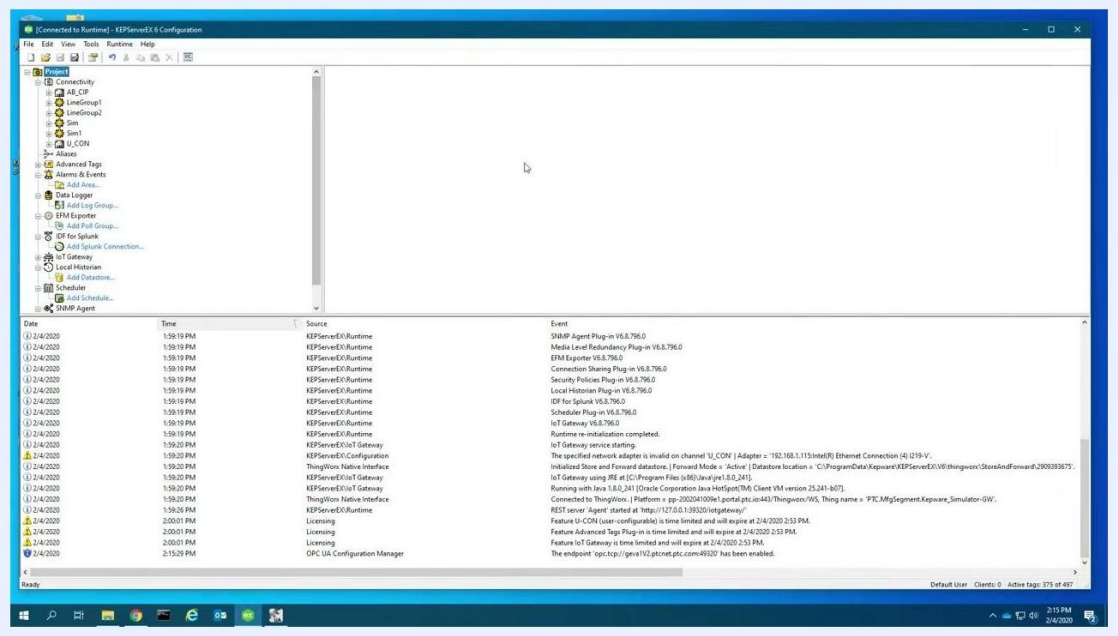


OPC UA Configuration Manager with the Enabled check box selected for the host name endpoint

Step 6: Review trusted clients

1. Click the **Trusted Clients** tab in the OPC UA Configuration Manager.

2. Confirm that no trusted clients are listed. This means no remote clients have been approved yet.



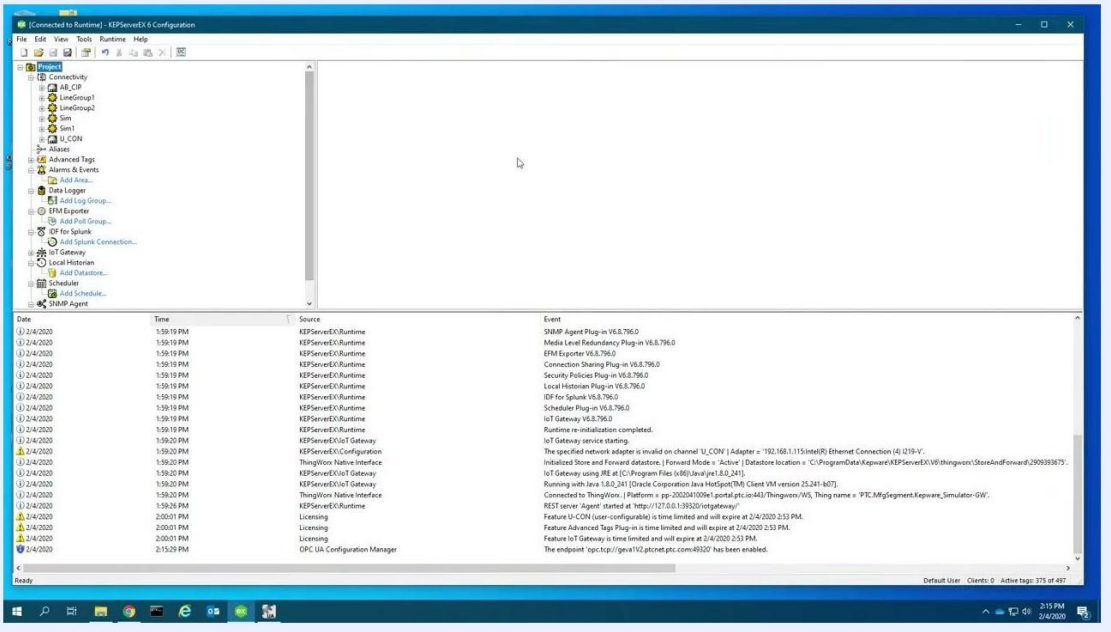
Trusted Clients tab in the OPC UA Configuration Manager with no entries

Step 7: Reinitialize the OPC UA server runtime

After you enable the host name endpoint, you must restart the OPC UA server instance for the change to take effect.

1. In the OPC UA Configuration Manager, select the endpoint and start a **runtime reinitialize**.

2. Wait for the process to complete.

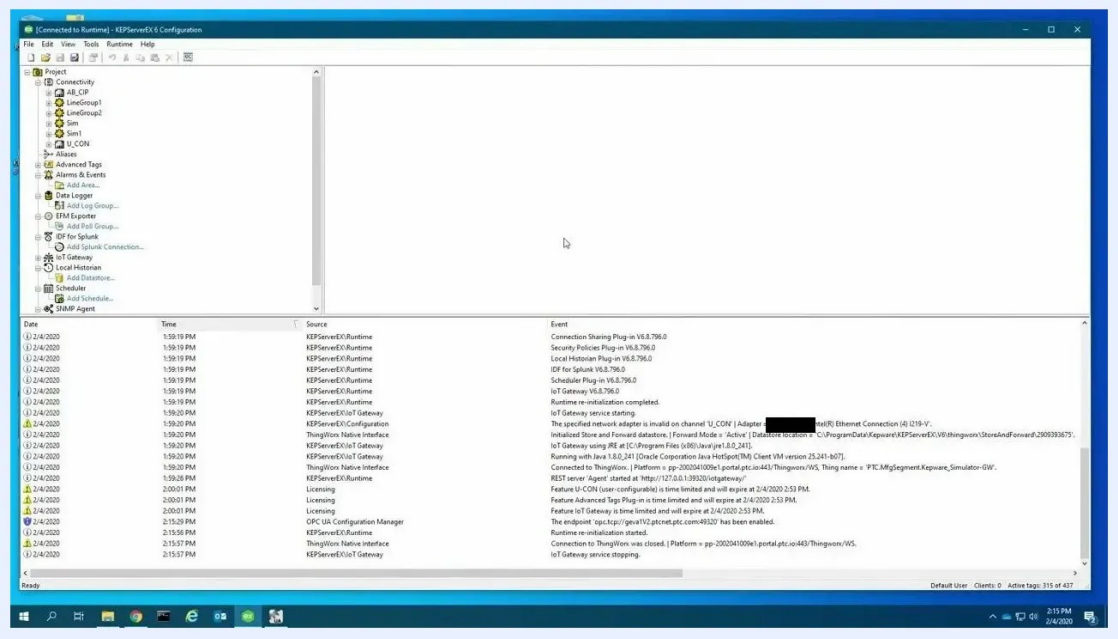


KEPServerEX Configuration application showing the event log while the runtime reinitializes

Step 8: Verify the runtime reinitialization

1. Check the event log in the KEPServerEX Configuration application.

2. Confirm that an entry shows the endpoint (for example, opc.tcp://[hostname]:49320) is enabled and that runtime reinitialization is complete.



KEPServerEX Configuration event log confirming the endpoint is enabled and runtime reinitialization is complete

Step 9: Note the OPC UA server port

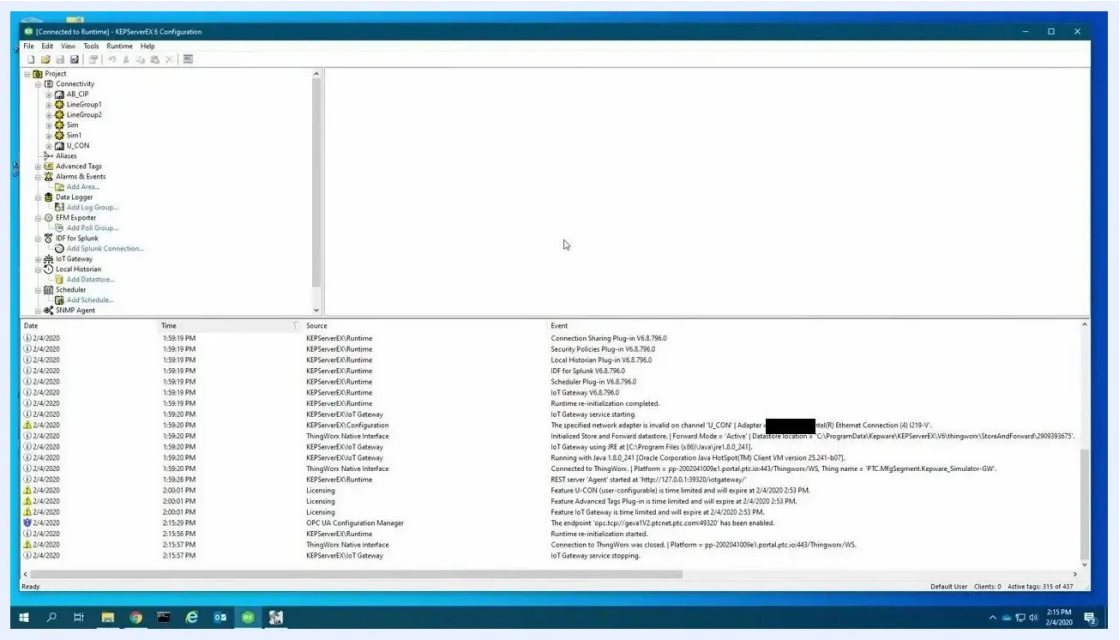
Identify the port the OPC UA server uses. The default is **49320**. Write it down, because you need it for both client configuration and the firewall rule.

Allow the OPC UA port in Windows Defender Firewall

Step 10: Open Windows Defender Firewall with Advanced Security

1. Launch **Windows Defender Firewall with Advanced Security** from the Start menu or Control Panel.

2. Make sure the firewall is active for the Domain, Private, and Public profiles.

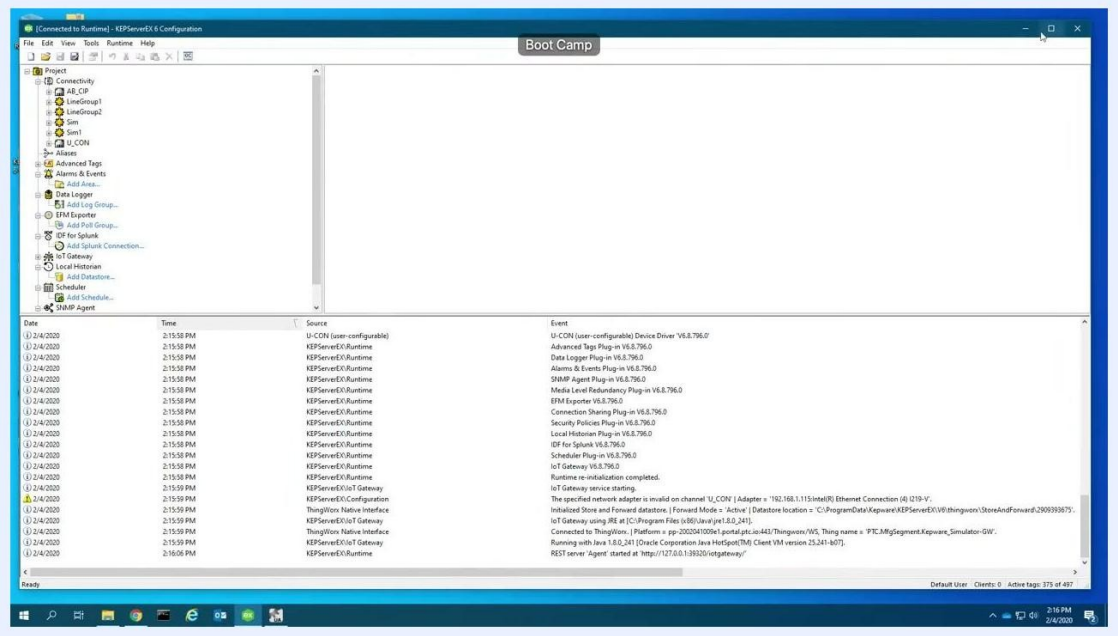


Windows Defender Firewall with Advanced Security showing the firewall status for all profiles

Step 11: Create a new inbound rule

1. Select **Inbound Rules** in the left pane.

2. Click **New Rule...** in the Actions pane on the right.

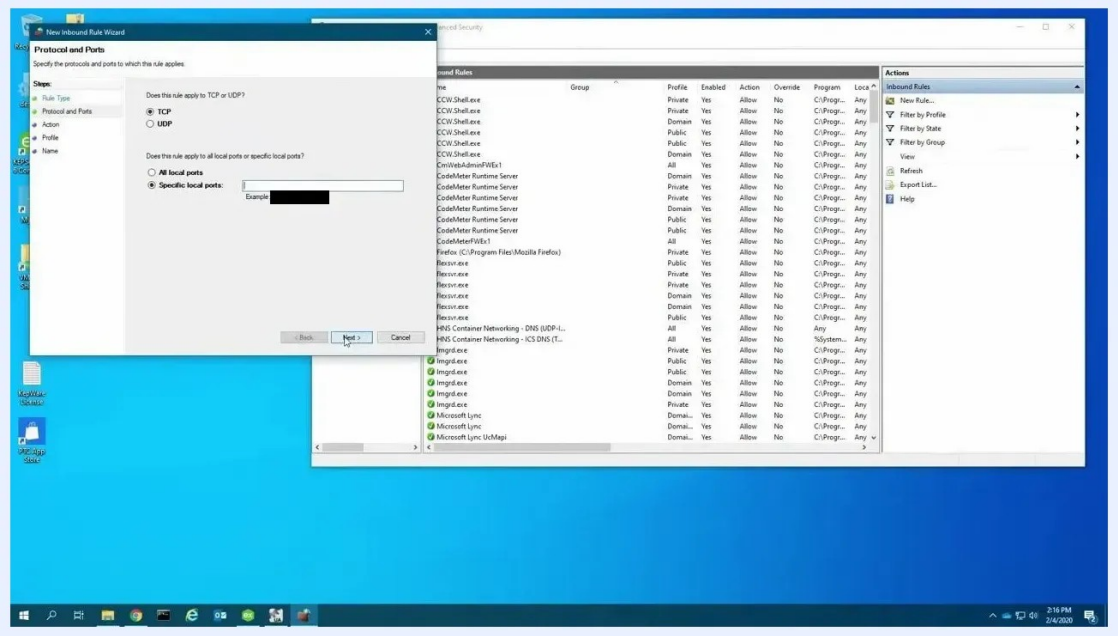


Windows Defender Firewall with Advanced Security with Inbound Rules selected and the New Rule option highlighted

Step 12: Configure the rule for the OPC UA port

1. In the **New Inbound Rule Wizard**, select **Port** as the rule type.
2. Choose **TCP** as the protocol.
3. Select **Specific local ports** and enter **49320**.

4. Click **Next**.

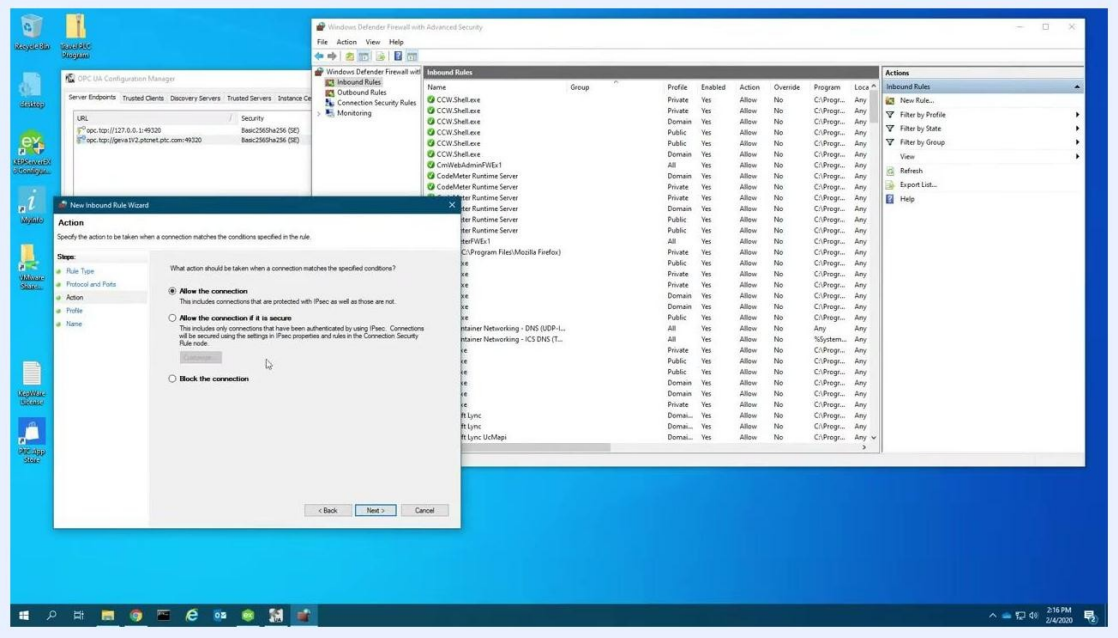


New Inbound Rule Wizard with TCP and specific local port 49320 entered and the Next button highlighted

Step 13: Allow the connection

1. In the **Action** step, select **Allow the connection**.

2. Click **Next**.



New Inbound Rule Wizard with "Allow the connection" selected and the Next button highlighted

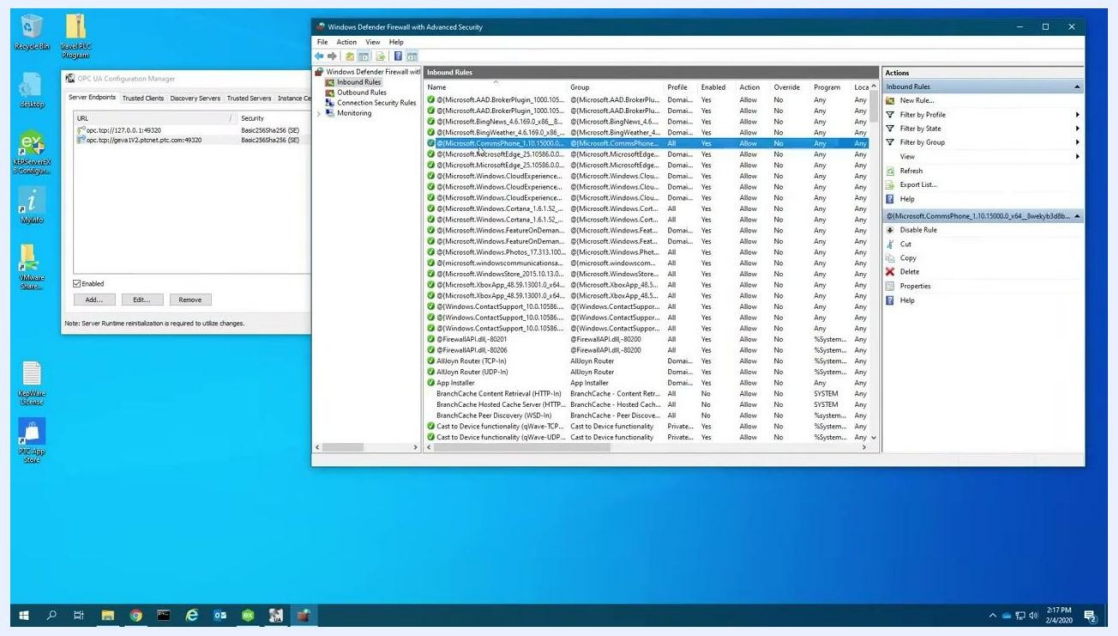
Step 14: Restrict the rule to private and domain networks

1. In the **Profile** step, make sure only **Private** and **Domain** are selected.
2. Clear **Public** to avoid exposing the OPC UA server on internet-facing interfaces.
3. Click **Next**.

Step 15: Name the firewall rule

1. In the **Name** step, enter a descriptive name such as **OPC UA Server Interface (KepWare)**.
2. Optionally, add a description.

3. Click **Finish** to create the rule.

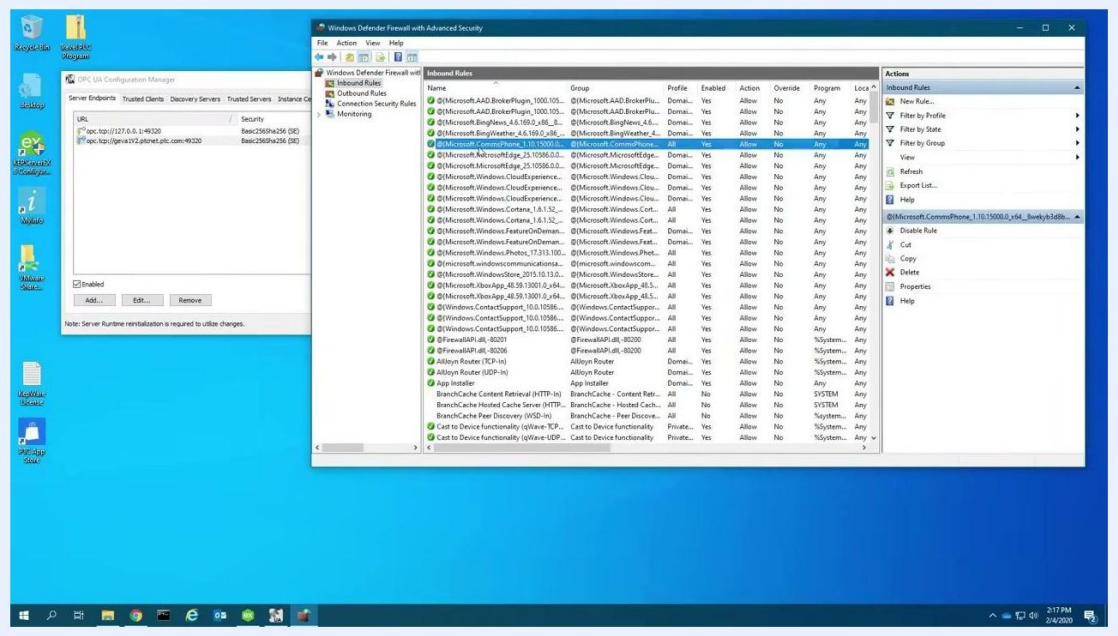


New Inbound Rule Wizard with the rule named "OPC UA Server Interface (KepWare)" and the Finish button highlighted

Step 16: Verify the new firewall rule

1. In **Windows Defender Firewall with Advanced Security**, sort the **Inbound Rules** list by name.
2. Locate **OPC UA Server Interface (KepWare)**.

3. Confirm that the rule is enabled and set to **Allow** for the correct profiles.



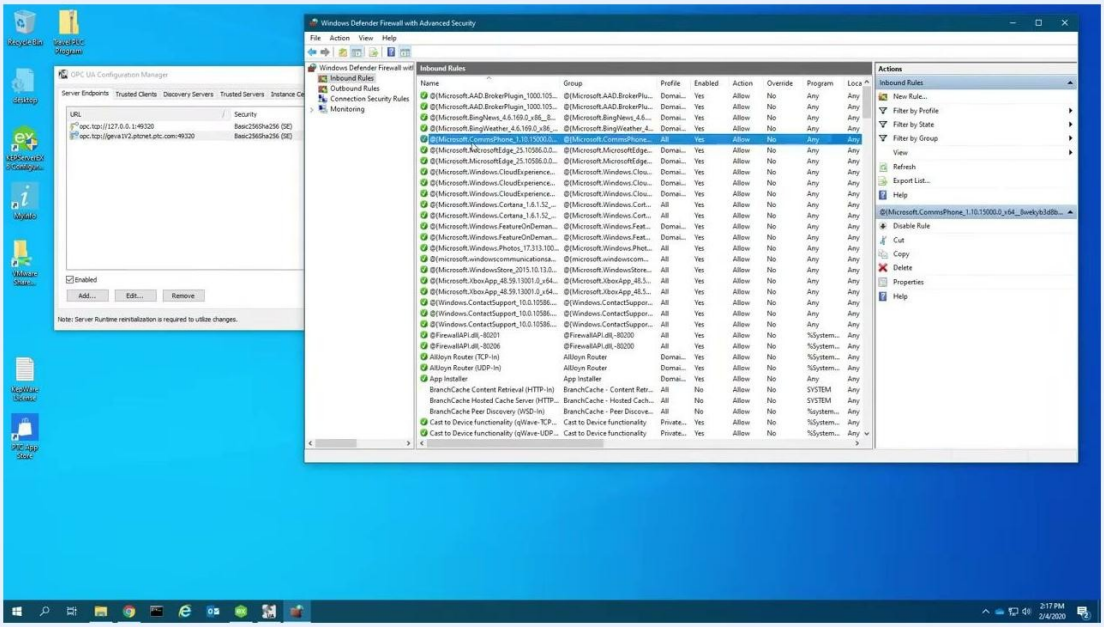
Windows Defender Firewall with Advanced Security listing the new "OPC UA Server Interface (KepWare)" rule as enabled

Connect a remote OPC UA client

Step 17: Connect to the OPC UA server

1. On a remote machine, open your OPC UA client application, for example Prosys OPC UA Client.
2. Enter the server endpoint in the format opc.tcp://[hostname]:49320, for example opc.tcp://geva1v2:49320.

3. Start the connection.

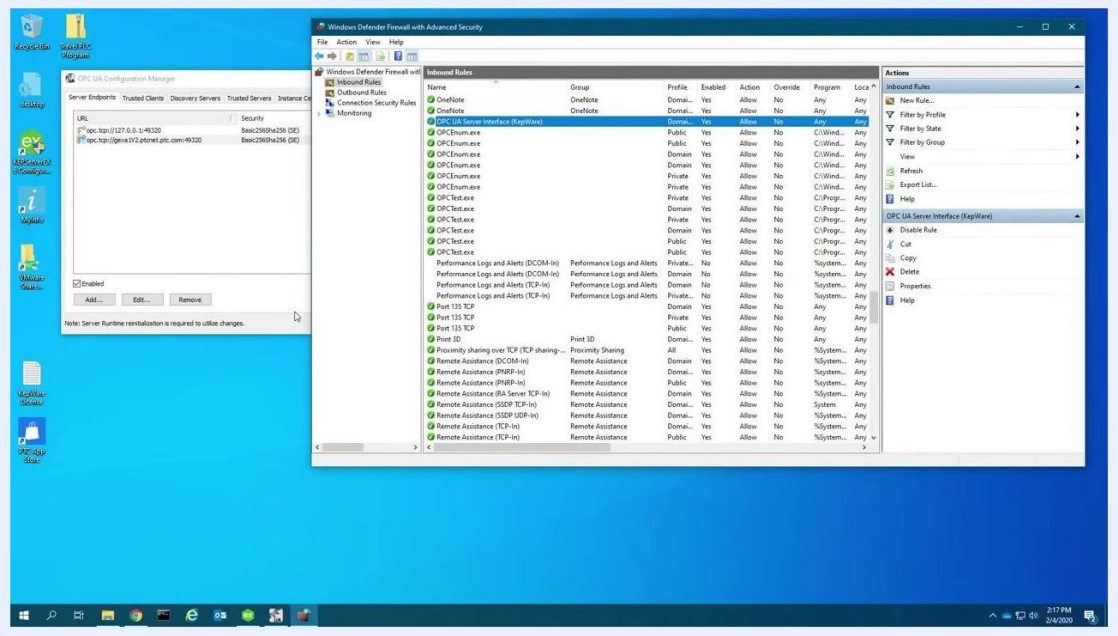


Prosys OPC UA Client with the server endpoint entered for connection

Step 18: Select security settings in the client

1. When prompted, choose the available security mode and policy, for example **Sign & Encrypt** with **Basic256Sha256**.

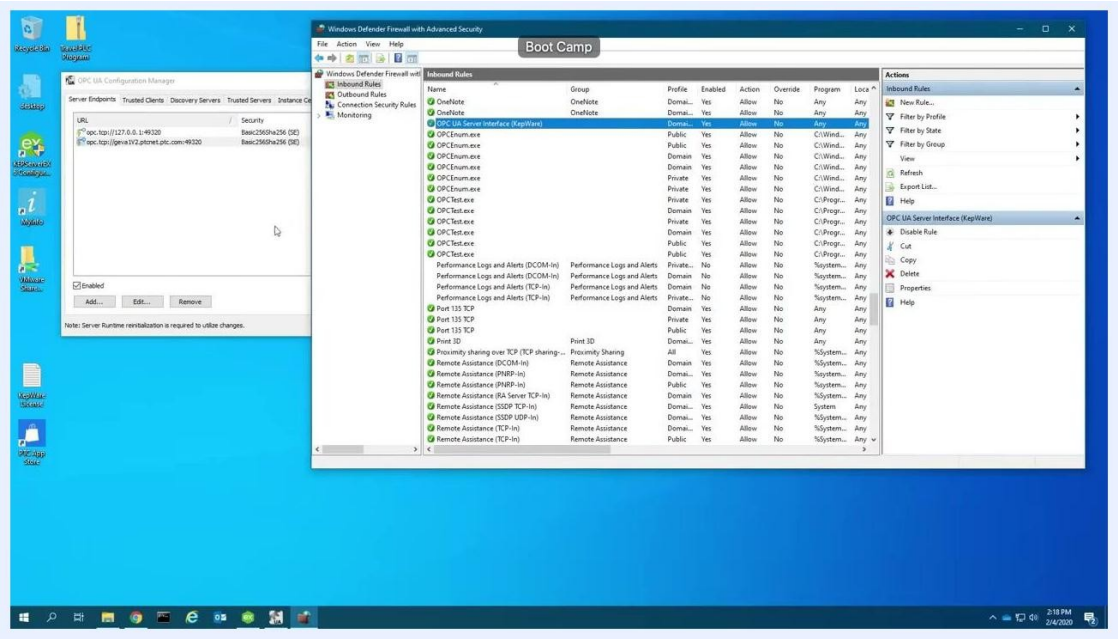
2. Click **OK** to continue.



Prosys OPC UA Client Security Settings dialog with Sign & Encrypt and Basic256Sha256 selected

Step 19: Handle the certificate error

If the server doesn't accept the client's application certificate, an error appears, for example "The server does not accept this application's certificate. Error=Bad_SecurityChecksFailed". Note the message and click **Close**. You trust the certificate on the server in the next steps.

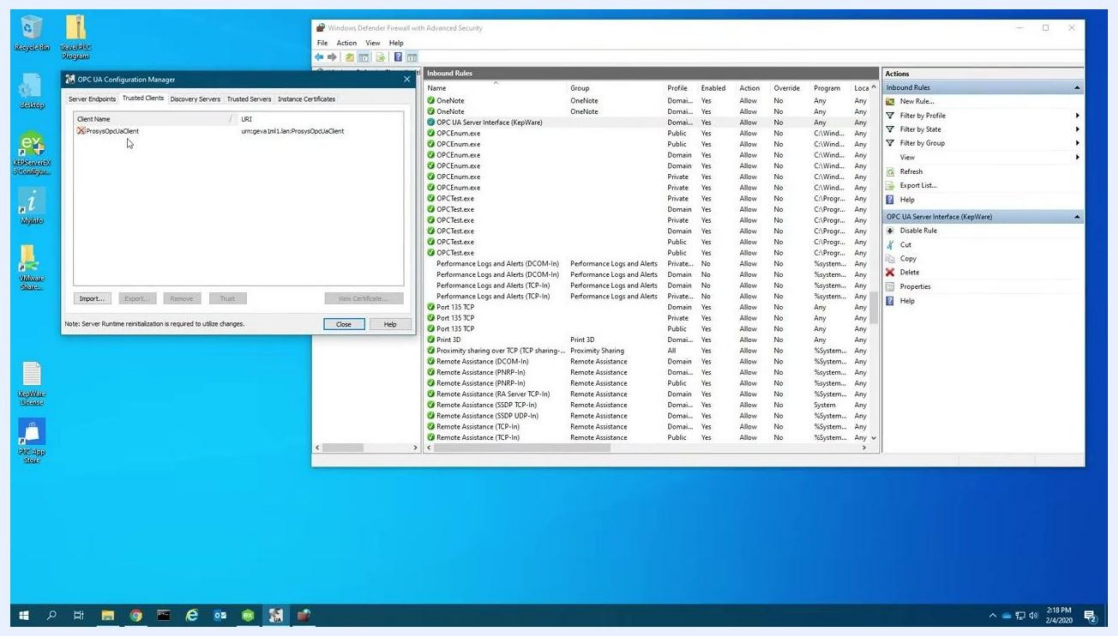


Prosys OPC UA Client showing the untrusted certificate error dialog

Step 20: Find the client in the OPC UA Configuration Manager

1. On the KEPServerEX machine, launch the "OPC UA Configuration Manager".
2. Open the "Trusted Clients" tab.
3. Verify that the client (for example, ProsysOpcUaClient) appears in the list with its URI, for example urn:geva1v1:Jan-ProsysOpcUaClient.

The client may appear with a red X, which means its certificate is not yet trusted.

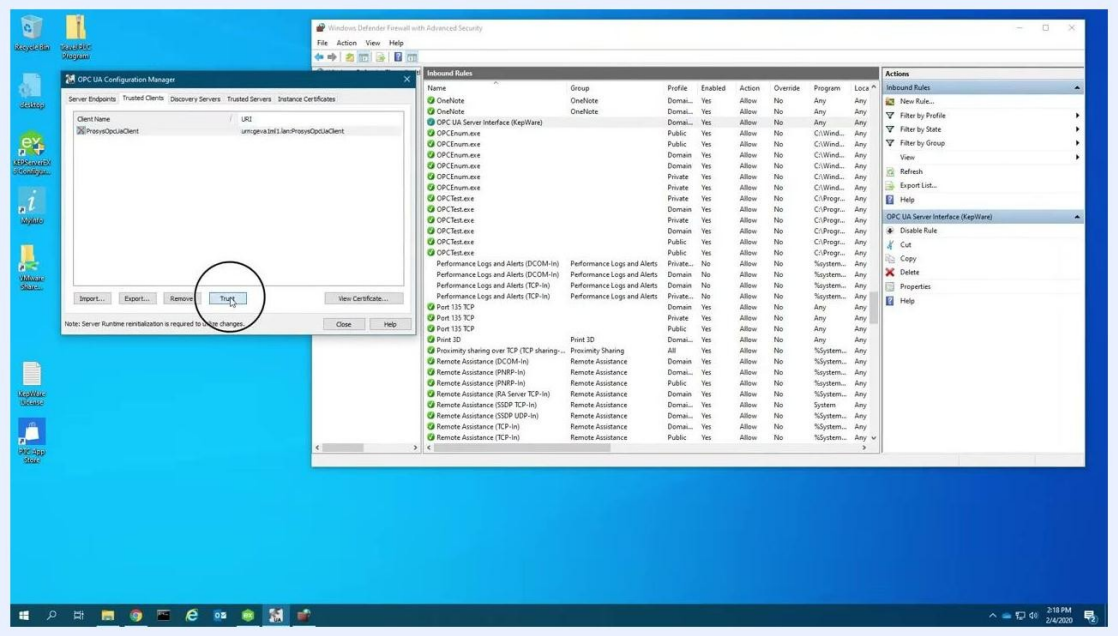


OPC UA Configuration Manager Trusted Clients tab showing ProsysOpcUaClient with a red X and its URI, with Windows Defender Firewall with Advanced Security open in the background

Step 21: Trust the client certificate

1. Select the client entry, for example ProsysOpcUaClient.
2. Click the "Trust" button at the bottom of the window.

A message at the bottom of the window states that you must reinitialize the server runtime to use the changes.

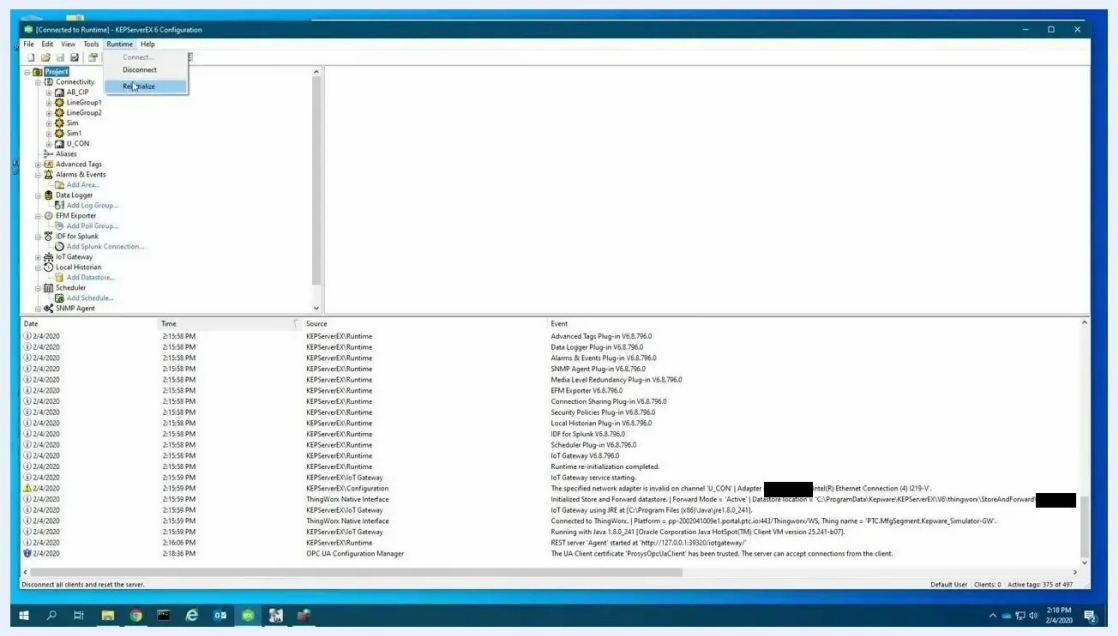


OPC UA Configuration Manager with the Trust button highlighted for the selected client certificate

Step 22: Reinitialize the KEPServerEX runtime

1. Open the KEPServerEX Configuration application.
2. On the menu bar, select Runtime, then choose Reinitialize.

This step disconnects all clients and resets the server, which applies the new certificate trust settings.



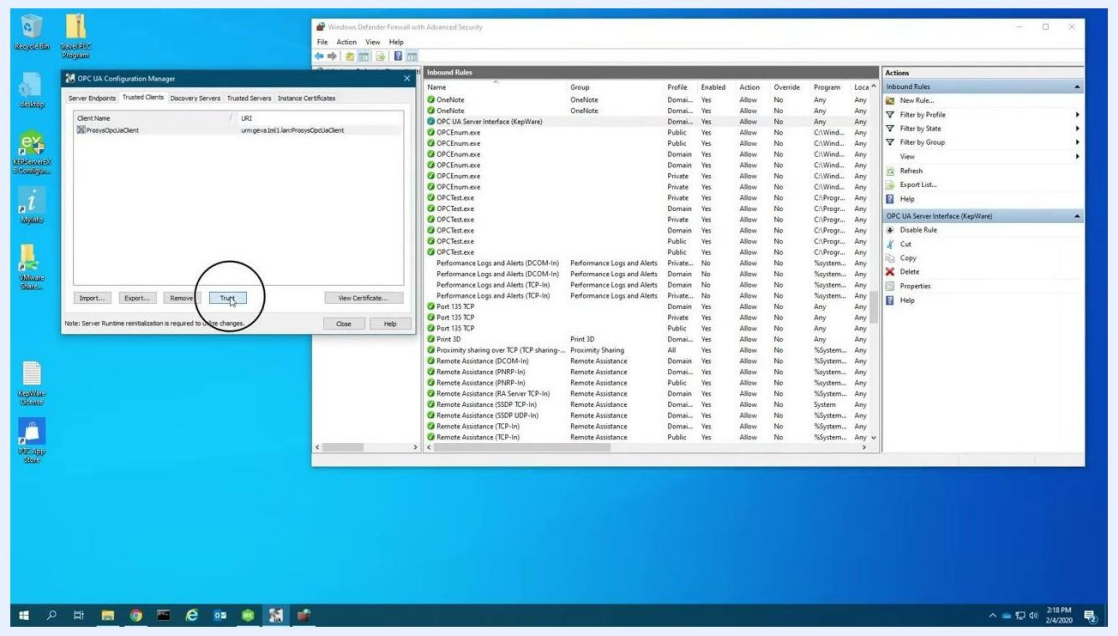
KEPServerEX Configuration window with the Runtime menu open and Reinitialize selected, with the project tree and event log visible

Browse and monitor tag data

Step 23: Reconnect and browse the address space

1. Switch to the Prosys OPC UA Client on your client machine.
2. Connect to the KEPServerEX OPC UA server using the endpoint URL, for example opc.tcp://geva1v2.ptcnet.ptc.com:49320.
3. In the left pane, review the hierarchical tree of objects, types, and views.

4. Select "Objects" to begin browsing available tags and nodes.

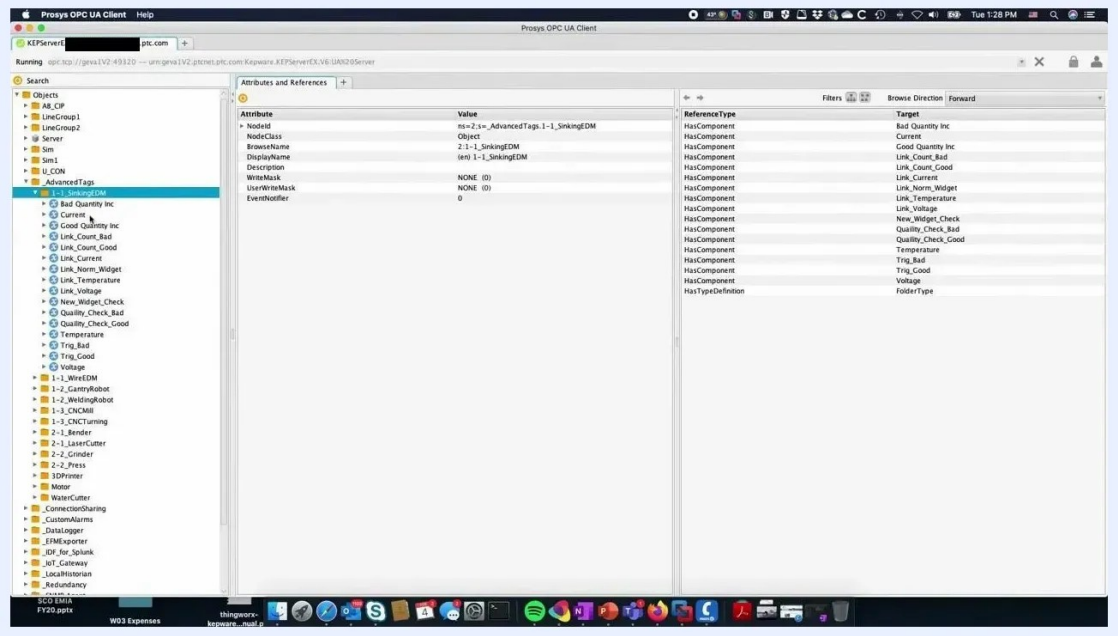


Prosys OPC UA Client connected to KEPServerEX with Objects selected and attributes and references displayed

Step 24: Select tags to monitor

1. Expand the "Objects" tree and go to the group you want, for example AdvancedTags > 1-1_SinkingEDM.
2. Select a tag such as Current to view its attributes and references.

The right pane lists all components and their relationships.



Prosys OPC UA Client with the Current tag under 1-1_SinkingEDM selected, showing its attributes and references

Step 25: Monitor tag data and trends

Add tags such as Current to the data view. The upper section shows these details for each tag:

- **NodeId**, for example ns=2;s=...AdvancedT...Current
- **DisplayName**, for example Current
- **Value**, for example 1.4960392
- **DataType**, for example Float
- **SourceTimestamp** and **ServerTimestamp**, for example 04.02.2020 14:19:52.592
- **StatusCode**, for example GOOD (0x00000000)
- **MonitoringMode**, for example Reporting
- **Graph**, a check box that is selected for each tag

The lower section shows a real-time trend graph:

- Each monitored "Current" tag appears as a colored line, such as red or blue, over a 60-second window.
- The X-axis shows time, for example 14:19:25 to 14:19:50.
- The Y-axis shows tag values, for example 1.4700 to 1.5225.
- The legend at the bottom identifies each line as "Current".

Confirm that the graph updates in real time. Use the "Show data for (seconds)" field to adjust the time window. Make sure the "Subscription Enabled" and "Reporting" modes are active for all monitored tags so the data stays live.

Summary

You now know how to enable the OPC UA server in Kepware for remote access. You enabled the host name endpoint in the OPC UA Configuration Manager, reinitialized the runtime, and opened TCP port 49320 for Private and Domain networks. You then trusted the remote client's certificate and used Prosys OPC UA Client to browse and monitor live tag data.