Connectivity Guide

Secure OPC UA Tunneling with KEPServerEX®

January 2020
Ref. 1.04

Table of Contents

1. Introduction

The purpose of a tunnel is to traverse networks or satisfy the requirements for layered networks as defined by ISA95 and Purdue. This guide describes how to set up a secure tunnel between two instances of KEPServerEX® using user authentication with signed and encrypted messages.

2. Getting Started

This document does not cover the installation and licensing of KEPServerEX. For instructions, visit the Resource Library and Licensing pages on www.kepware.com.

The OPC UA server is the instance of KEPServerEX where the data sources reside. These data sources can be PLCs, databases, or other OPC servers where the data is accessed using communication drivers with KEPServerEX. This instance is typically installed on the controls side of the network.

The OPC UA client is the instance of KEPServerEX on the other end of the tunnel or on the enterprise side of the network. This is where other OPC clients, both OPC DA and OPC UA, access KEPServerEX or where KEPServerEX publishes data to the cloud using the IOT Gateway or Splunk.

3. Firewall

OPC UA does not use unsolicited callbacks, making it “firewall friendly”. This document does not include firewall configuration. Organizations have their own security policies dictating firewall configuration, which should be as secure as possible. For this exercise, please ensure external client applications can securely access the server instance with a TCP connection using the port configured in the steps below.

4. Certificates

When a secure OPC UA connection is attempted, a certificate exchange between the client and the server occurs. This certificate is validated and used for signing and encrypting the payload. This document makes use of the pre-loaded self-signed certificate created during the installation process and should be used *ONLY* for testing and proof-of-concept work. In KEPServerEX Version 6.7 and higher, this self-signed certificate is valid for three years and must be managed by the user.

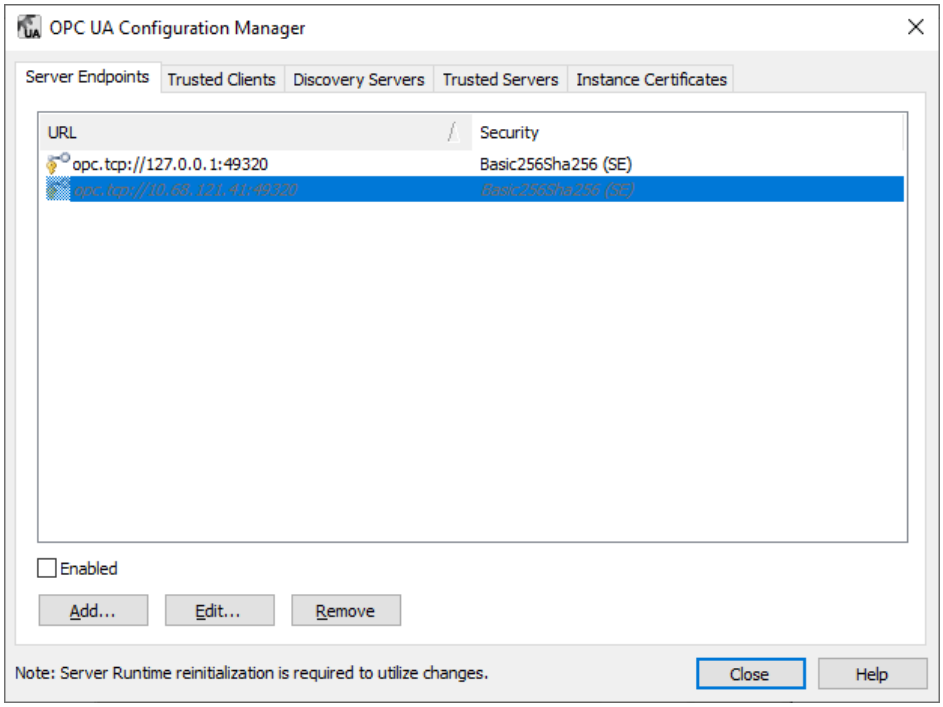
5. Setting up the Server Side

5.1 Server Endpoints

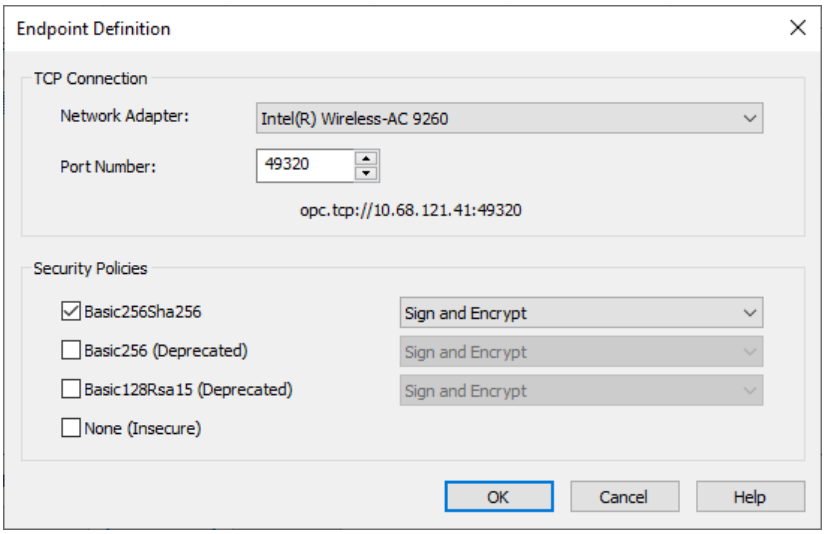
During the install of KEPServerEX, two endpoints are created, but only one is enabled for local connections. To set up a tunnel, an additional endpoint referencing a network card must be created or enabled to allow a remote connection from a client.

Enable an endpoint to allow remote connections:

1. Launch the OPC UA Configuration Manager by right-clicking on the **Administration** icon in the system tray and selecting **OPC UA Configuration**.
2. Select the **Server Endpoints** tab.

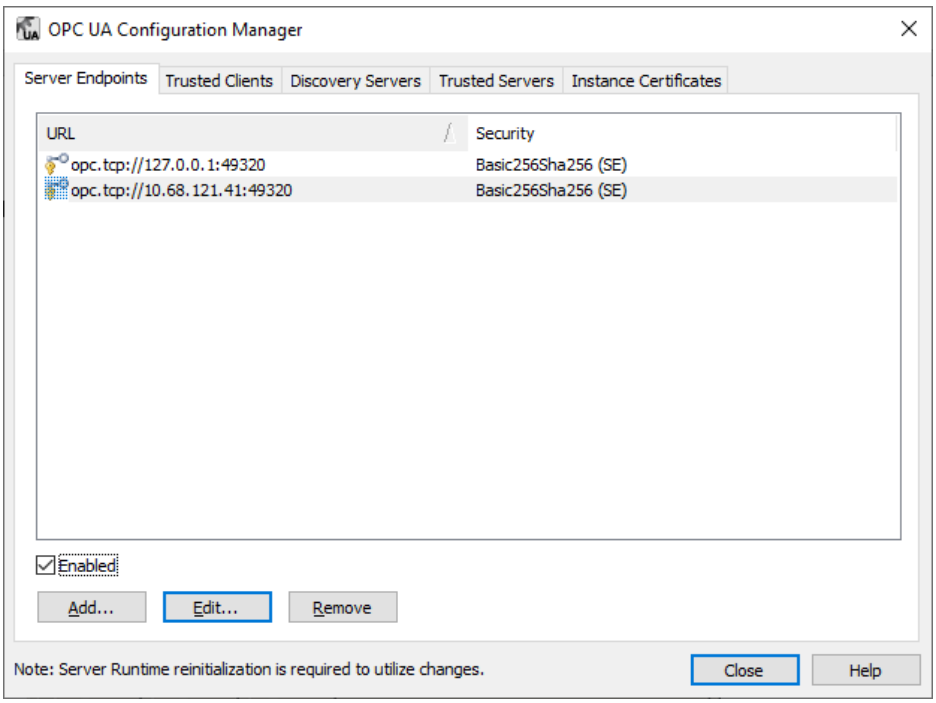


3. Select the default endpoint created during the install for non-local connections. This endpoint can be identified by having a PC name or IP in the endpoint URL.
4. Select **Edit**.
5. Choose the correct network from the **Network Adapter** drop down.
6. For the most secure connection possible, ensure that only **Basic256Sha256** security policy is checked.

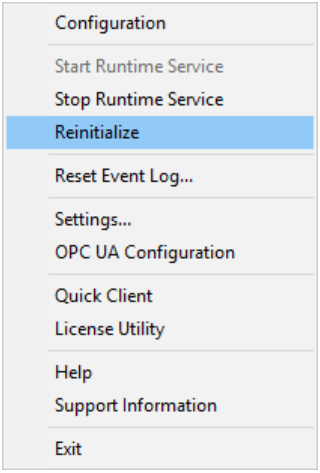


7. Make note of the **port** number so that it can be added to the firewall.
   - For increased security, change the port number to something other than 49320.

8. Click **OK** to close the dialog and apply the changes.
9. Enable the endpoint by selecting it in the list and checking the **Enabled** checkbox.



10. Apply the changes to the server Runtime by right-clicking on the **Administration** icon and selecting **Reinitialize**.

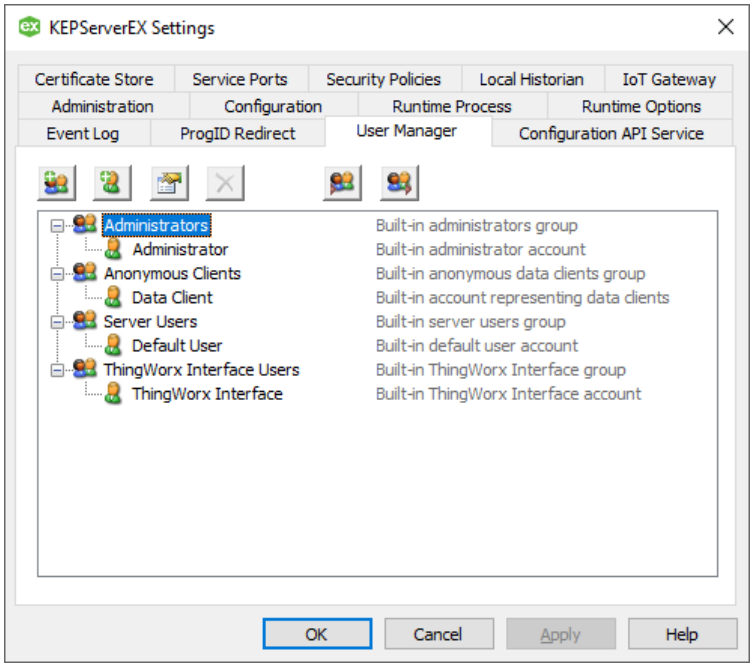


5.2 User Manager

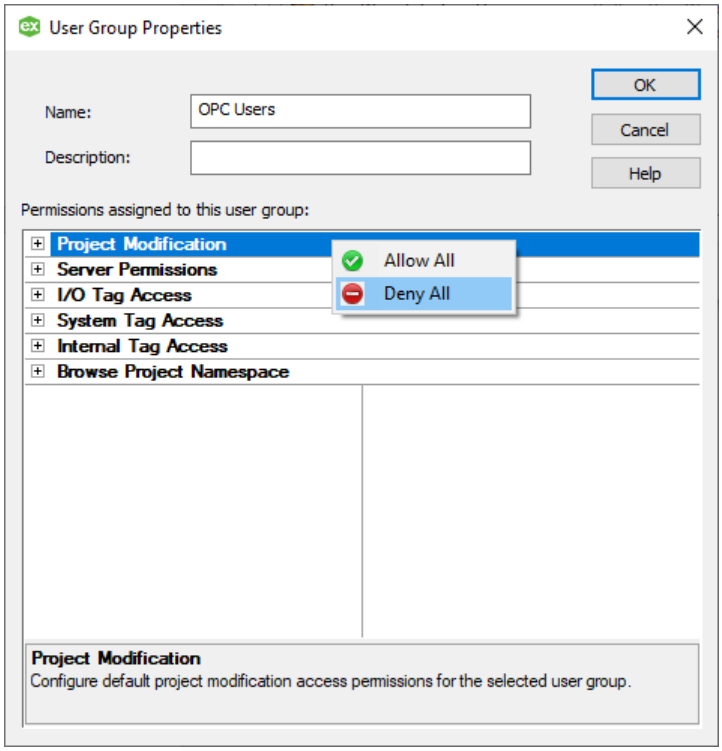
OPC UA supports user authentication using username and password. Users are created and edited using the User Manager within KEPServerEX.

Create an OPC UA specific user and allow tag access:

11. Access the **User Manager** by right-clicking on the **Administration** icon in the system tray and selecting **Settings**.
12. Select the **User Manager** tab.

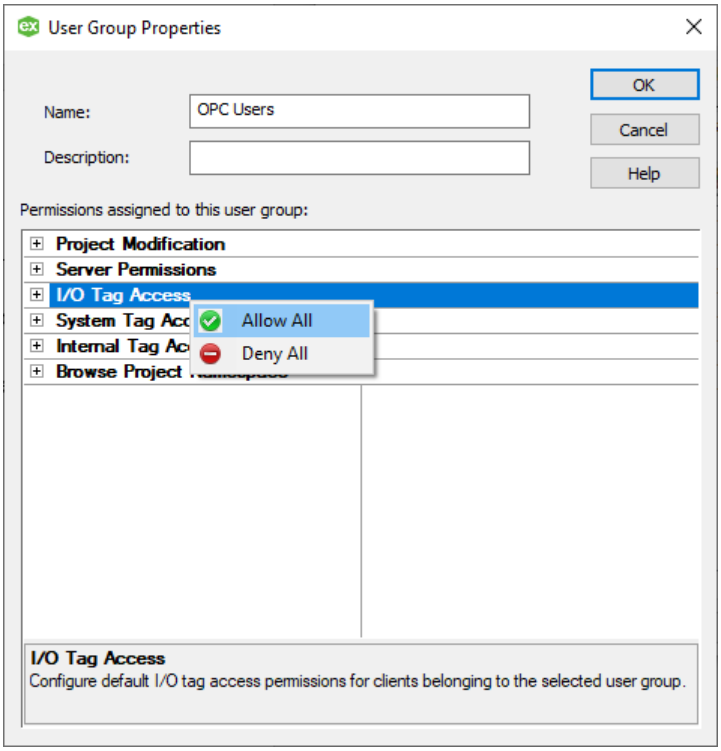


13. Create a group by clicking on the **New Group** icon.
14. Permissions are categorized so that a group can be customized to match the user's intended persona. Since this user is being created specifically for accessing data, administrative permissions should be denied while data access must be allowed.
15. Right-click on **Project Modification** and select **Deny All**.
16. Right-click on **Server Permissions** and select **Deny All**.



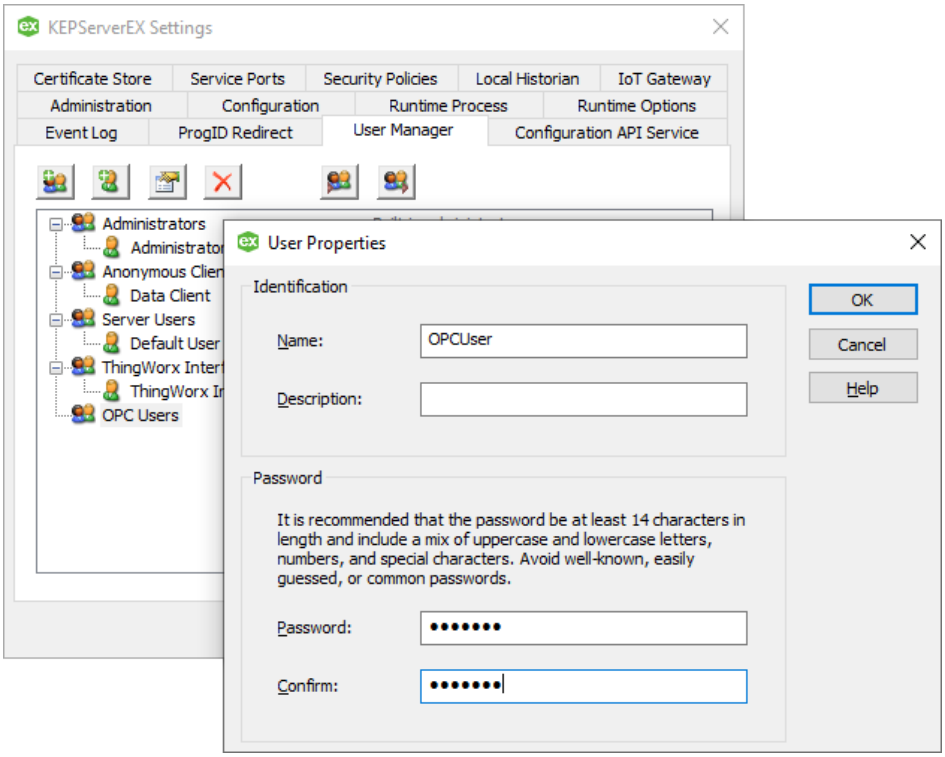
17. Right-click on **I/O Tag Access** and select **Allow All**.

18. Repeat for **System Tag Access**, **Internal Tag Access**, and **Browse Project Namespace**, choosing **Allow All** to each.

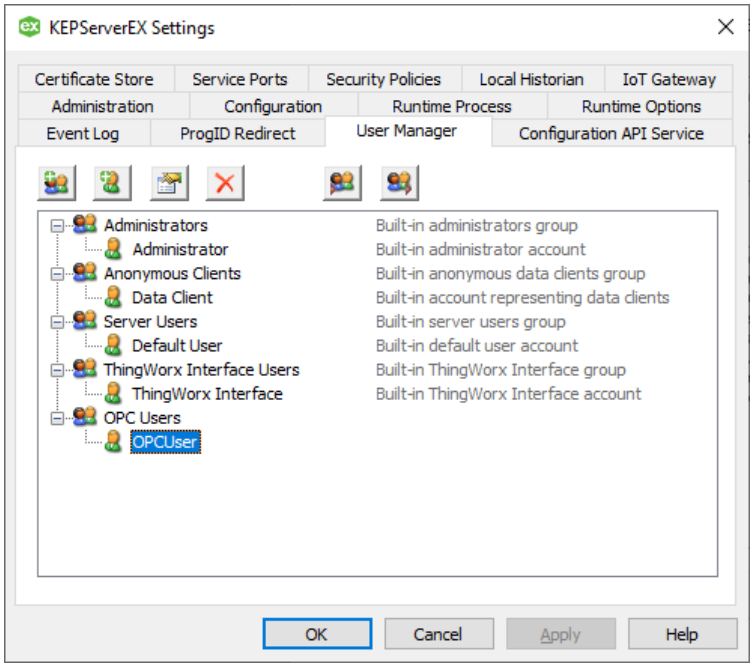


19. Select **OK** when finished.

20. Right-click on the newly created group and select **Add User**.



21. Enter a Name, Description, and Password and select **OK**.
    - This name and password will be used when configuring the OPC UA Client driver on the client PC in later steps.



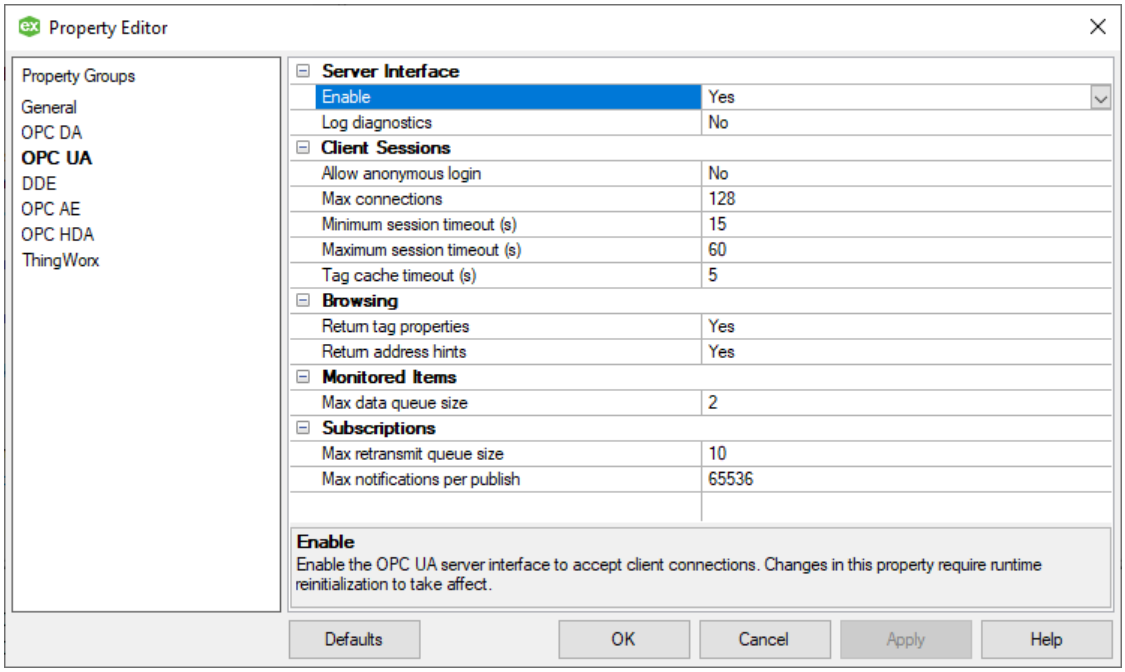
22. Select **OK** to close the **Settings** dialog.

5.3 Server Interface

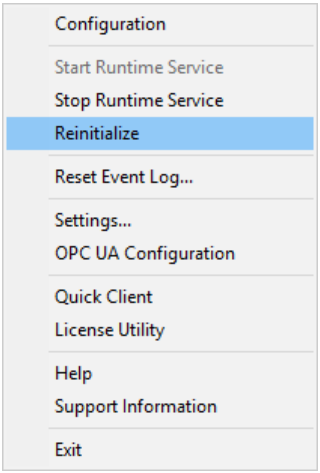
The project file contains information about the OPC UA interface that should be verified using the KEPServerEX Configuration.

Enable the OPC UA interface and disable anonymous login:

23. Launch the KEPServerEX Configuration and select **Project | Properties**...
24. Select the **OPC UA** tab.
25. Set Enable to **Yes**.
26. Set Allow anonymous login to **No**.



27. Select **OK** to close the dialog.
28. Right-click on the **Administration** icon and select **Reinitialize**.



6. Setting up the Client

Data sources configured on the server are accessed by the OPC UA Client driver on the client.

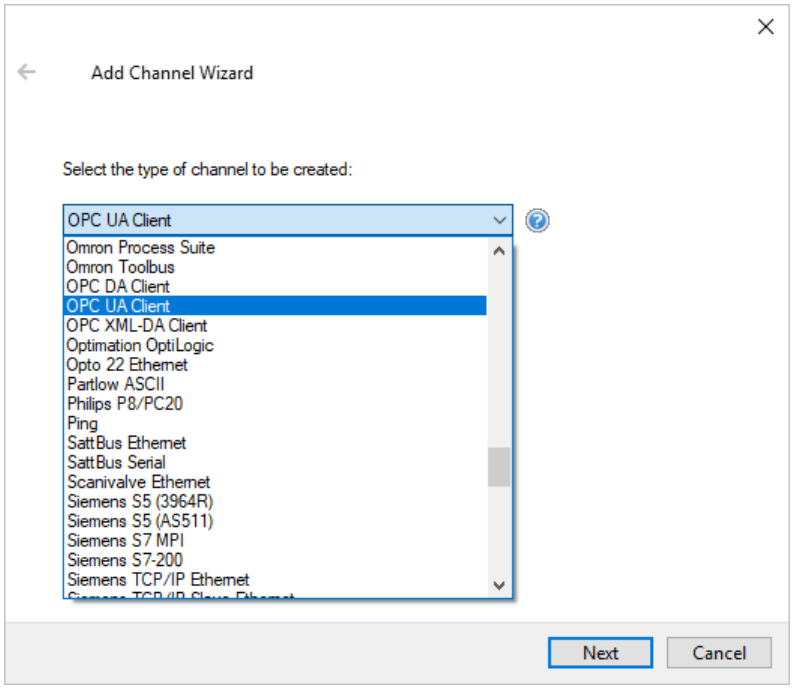
6.1 Creating a Session

A **Channel** in KEPServerEX is used to identify the OPC UA server, configure session timeouts, and provide user credentials for creating an OPC UA session.

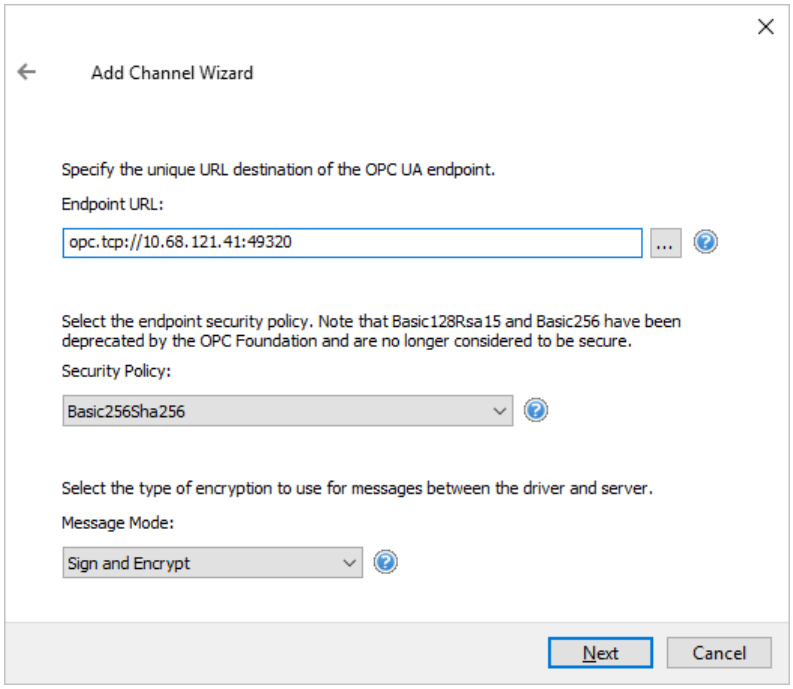
Add a UA Client channel by following these steps:

29. Launch the **KEPServerEX Configuration** by right-clicking on the **Administration** icon and selecting **Configuration**.
30. Right-click on **Connectivity** in the project tree and select **New Channel**.

31. Locate **OPC UA Client** in the list and click **Next**.

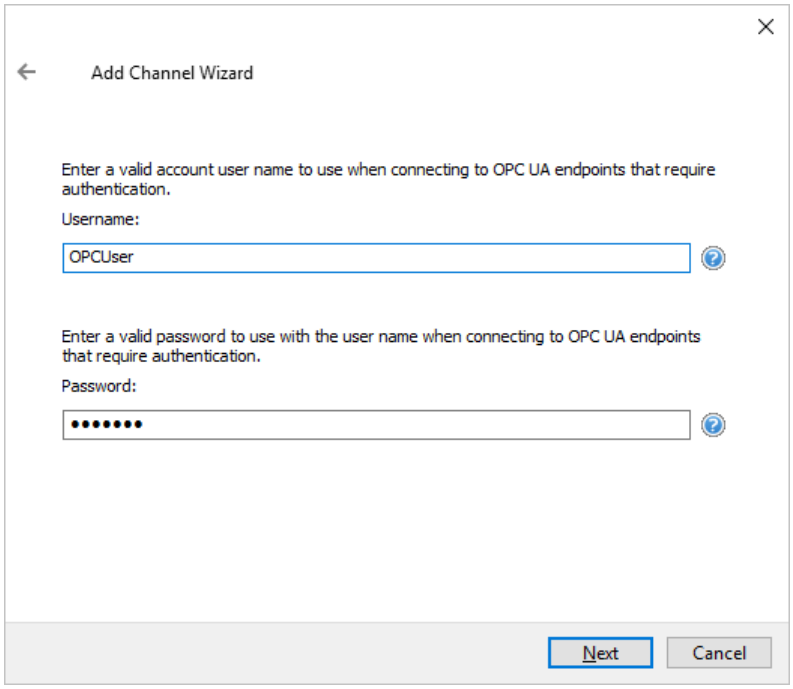


32. Provide a channel Name and click **Next**.
33. Accept the defaults for Optimization Method and Duty Cycle by clicking **Next**.
34. Enter the **Endpoint URL** of the endpoint created on the server PC, set Security Policy to **Basic256Sha256**, and set Message Mode to **Sign and Encrypt**.

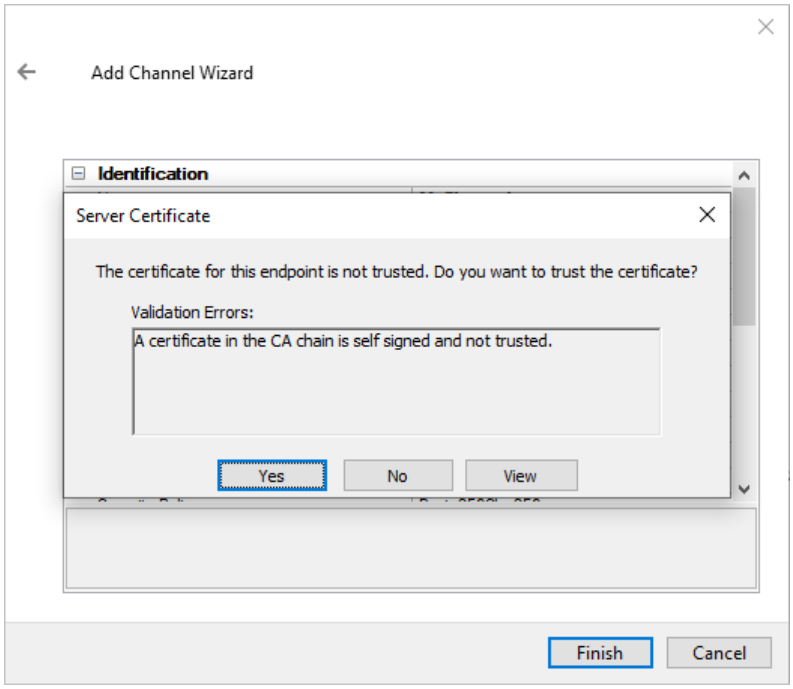


35. Click **Next**.
36. Accept default Timeout Settings by clicking **Next**. These can be edited after the channel has been created if desired.

37. Enter the **Username** and **Password** for the OPC user created on the server.



38. Click **Next**.
39. Click **Finish** on the summary page.
40. If the client can establish a connection to the server, a prompt appears allowing the user to accept and trust the server's certificate. If prompted, select **Yes**.



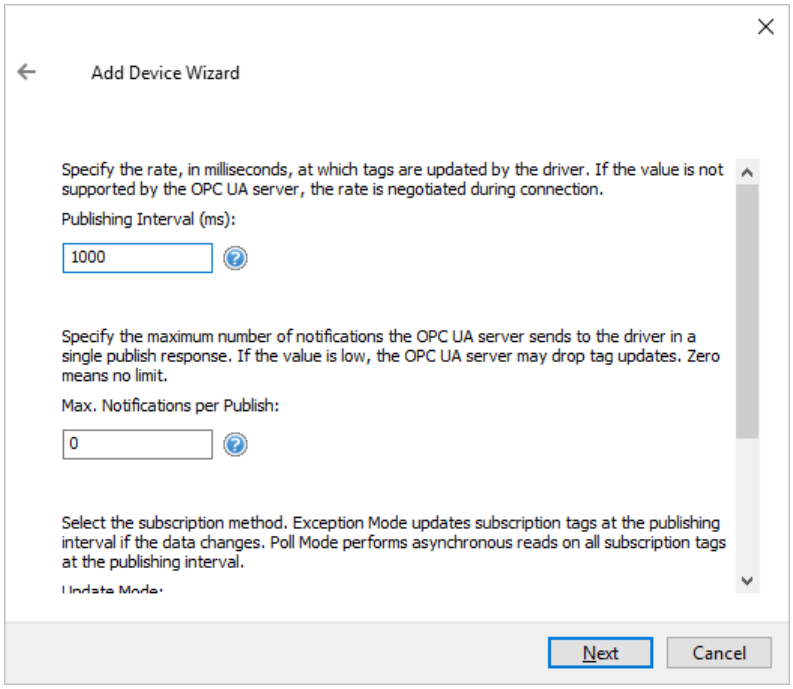
41. Channel configuration is complete. All settings can be adjusted by right-clicking on the channel and selecting **Properties**.

6.2 Adding a Subscription

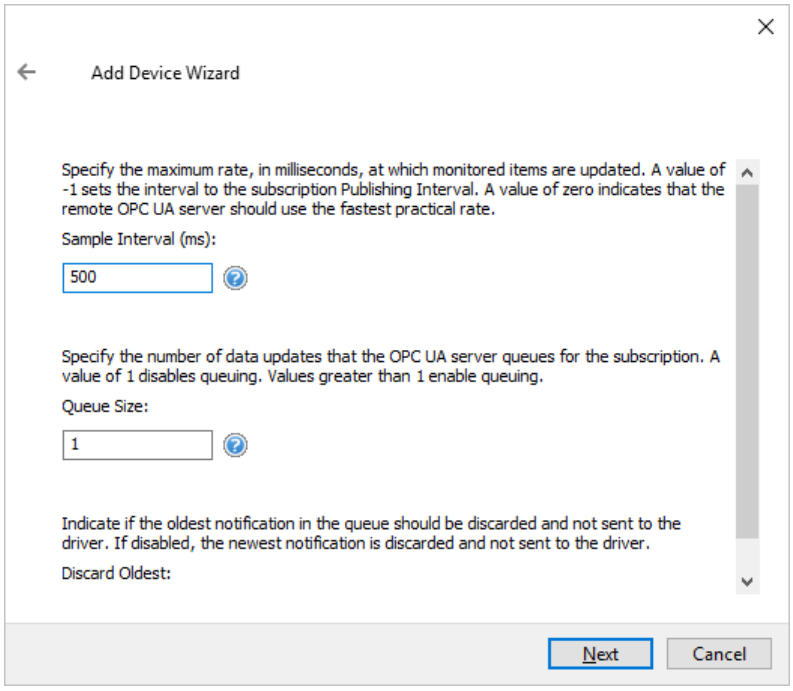
A device defined in KEPServerEX is used to browse and import items from the OPC UA server and acts as an OPC UA subscription. The settings configured in the device dictate how the data source is polled. Multiple devices can be added to the same channel with different update intervals and modes.

Add a UA Client device by following these steps:

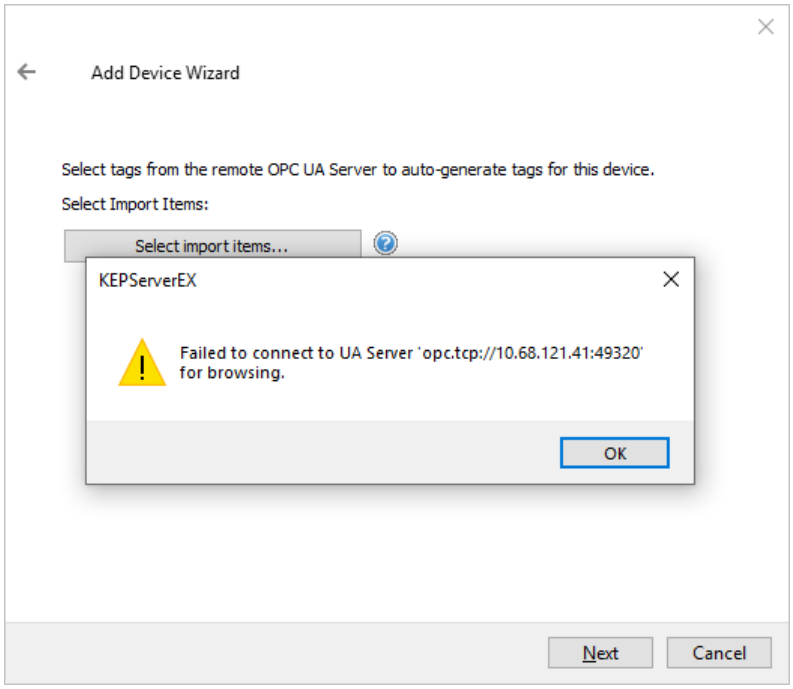
42. Right-click on the new channel in the project tree and select **New Device**.
43. Provide a device Name and click **Next**.
44. Accept the defaults for Scan Mode and Initial Updates from Cache by clicking **Next**.
45. Set the **Publishing Interval** to the rate at which the clients expect to receive updates (default is 1000 ms).



46. Accept the defaults for Lifetime Count and Keep-Alive Count by clicking **Next**.
47. Accept the defaults for Max. Notifications per Publish by clicking **Next**.
48. Set the **Sample Interval** to half the **Publish Rate** to ensure no updates are missed. The Sample Interval is the rate at which the server polls the data source (default is 500 ms).



49. Accept the defaults for Deadband by clicking **Next**.
50. Click **Select import items**.
    NOTE: This is expected to fail because the server has not yet trusted the client certificate. This is corrected in the steps below.



51. Click **OK**.
52. Click **Next**
53. Click **Finish** on the summary page.

7. Establish Trust

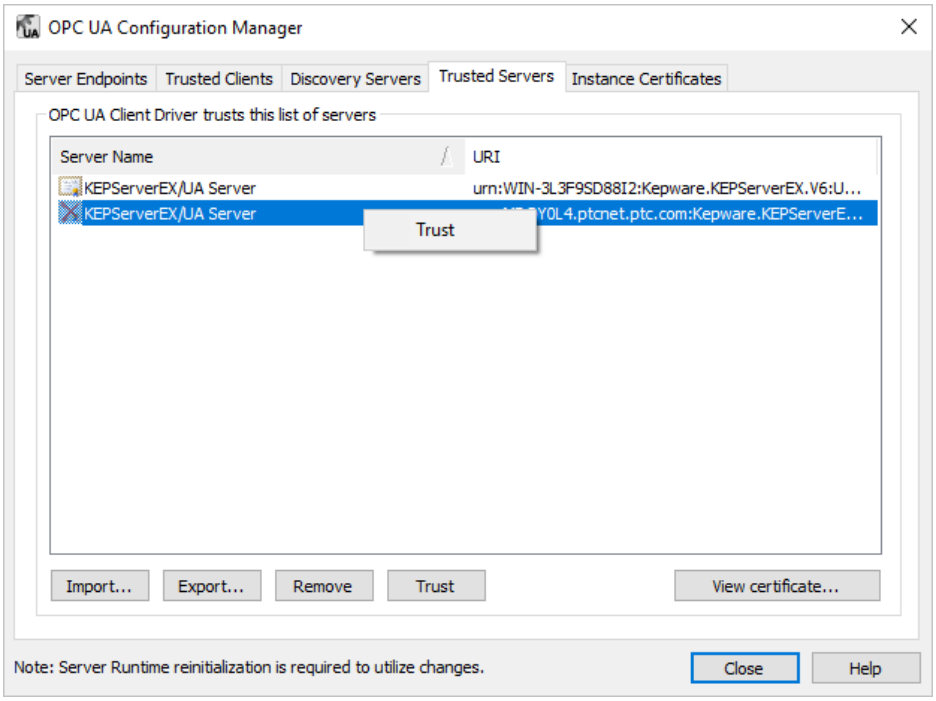
User intervention is required to establish trust between two applications. This is by design.

7.1 Trust Server Certificate

During the creation of the channel, a prompt appears to trust the server certificate. This can also be done after the channel has been created, as shown below.

To trust the server certificate on the client:

54. On the client, launch the **OPC UA Configuration Manager** by right-clicking on the **Administration** icon in the system tray and selecting **OPC UA Configuration**.
55. View the **Trusted Servers** tab.
56. If the server's certificate is not trusted, right-click on it and select **Trust**.

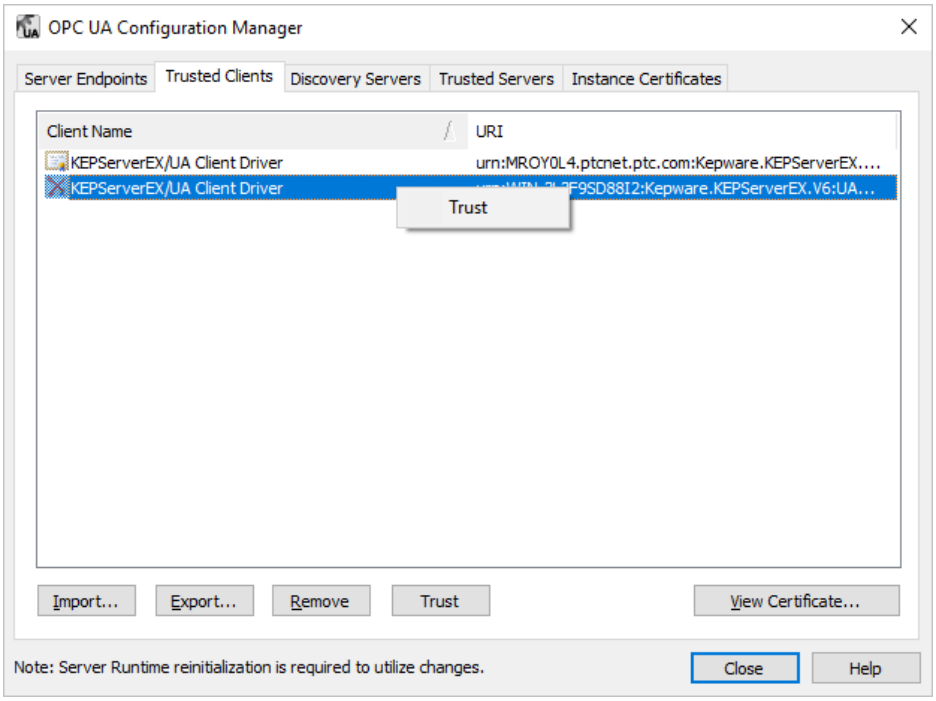


7.2 Trust Client Certificate

The Server Runtime does not have a user interface to prompt the user to accept the client certificate. The certificate must be trusted after the client attempts to connect for the first time (usually when browsing for tags).

To trust the client certificate on the server:

57. On the server, launch the **OPC UA Configuration Manager** by right-clicking on the **Administration** icon in the system tray and selecting **OPC UA Configuration**.
58. View the **Trusted Clients** tab.
59. Right-click on the un-trusted client certificate and select **Trust**.



8. Finalize Tunnel

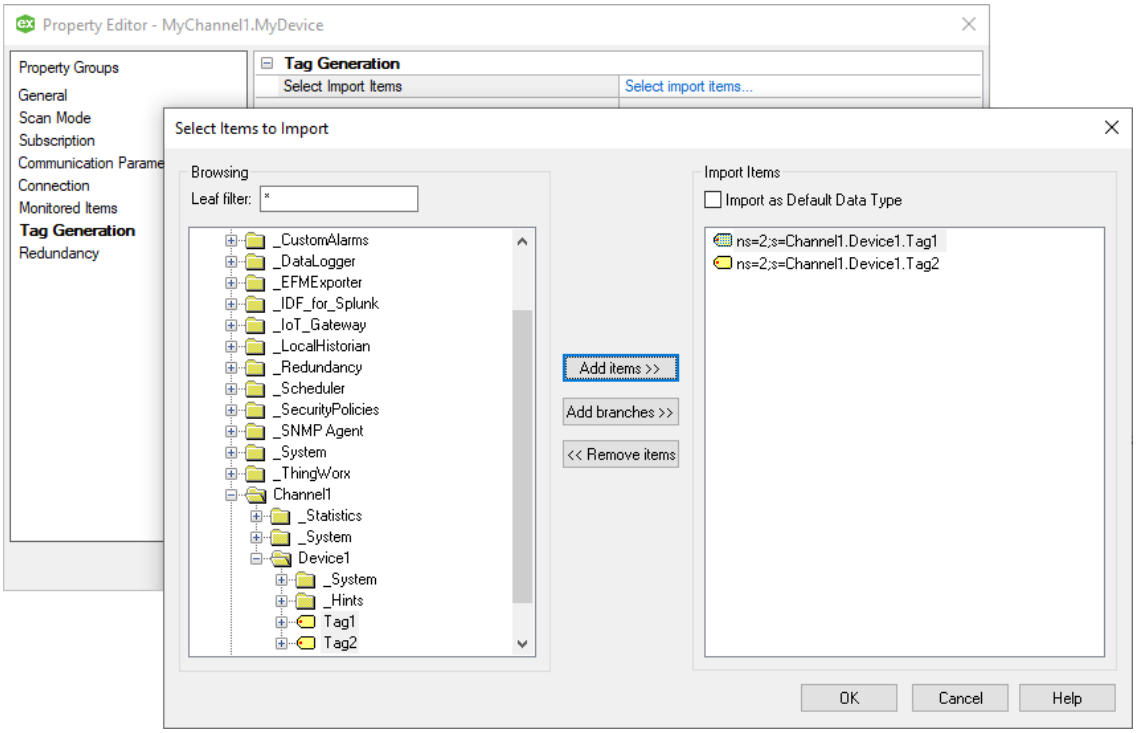
Now that a trust has been established, return to the client PC to import items and test connectivity through the tunnel.

8.1 Import Items

OPC UA supports tag browsing, but items may also be added manually, as described below.

Browse and add tags to the OPC UA Client driver:

60. View the **KEPServerEX Configuration** on the client PC.
61. Right-click on the device in the project tree and select **Properties...**.
62. View the Tag Generation group and click **Select import items...**.



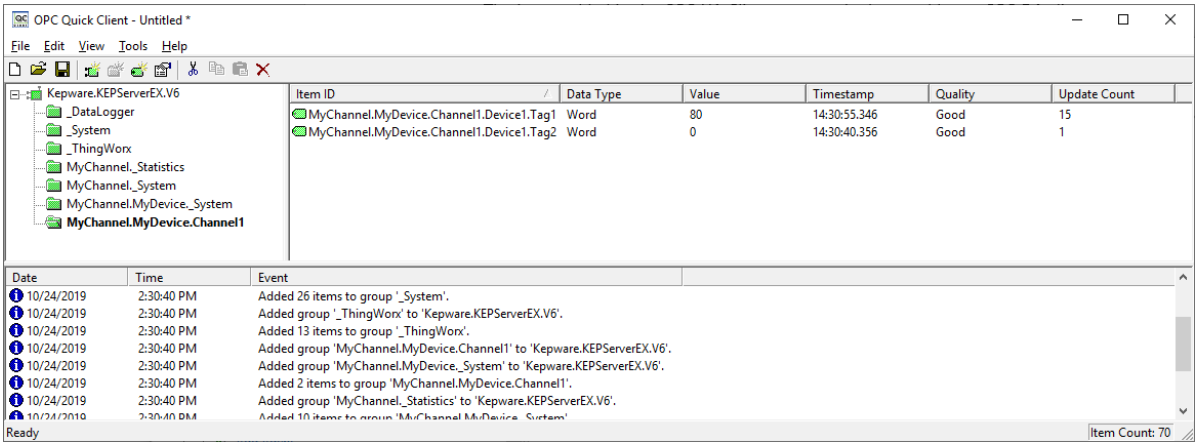
63. Browse the tree and locate the tags to be polled in the tunnel.
64. Select the desired items on the left pane and click **Add Items** or **Add Branch** to import them into the client.
65. When finished, click **OK** (tags will appear in the project file).

8.2 Verification

The items added in the OPC UA Client can be viewed by a local OPC DA client.

To verify connection and data flow, follow these steps:

66. From the **KEPServerEX Configuration**, select **Tools | Launch OPC Quick Client**. A connection to the local OPC DA server is established and items should populate the Detail View pane.



67. Browse for the items in the OPC UA Client group and verify that the data quality is “Good” and values are updating as expected.

