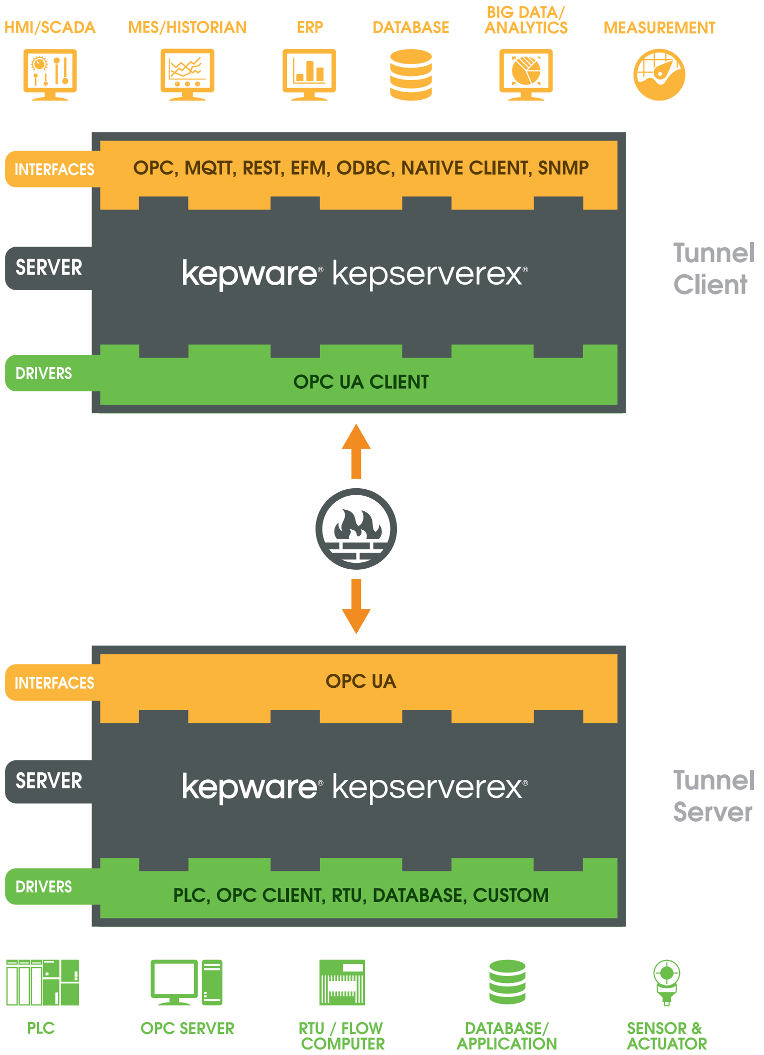
Secure Data Tunneling with KEPServerEX®

Easy Guide

The **KEPServerEX** connectivity platform leverages **OPC Unified Architecture** (UA) to provide a secure tunnel for device communications through networks barriers (like firewalls) and over the Internet.

A secure data tunnel is formed between one instance of KEPServerEX that functions as the **tunnel client** and another instance of KEPServerEX that functions as the **tunnel server.** The **OPC UA Client driver** pairs with the UA Server interface of a KEPServerEX implementation to transfer data securely and reliably.

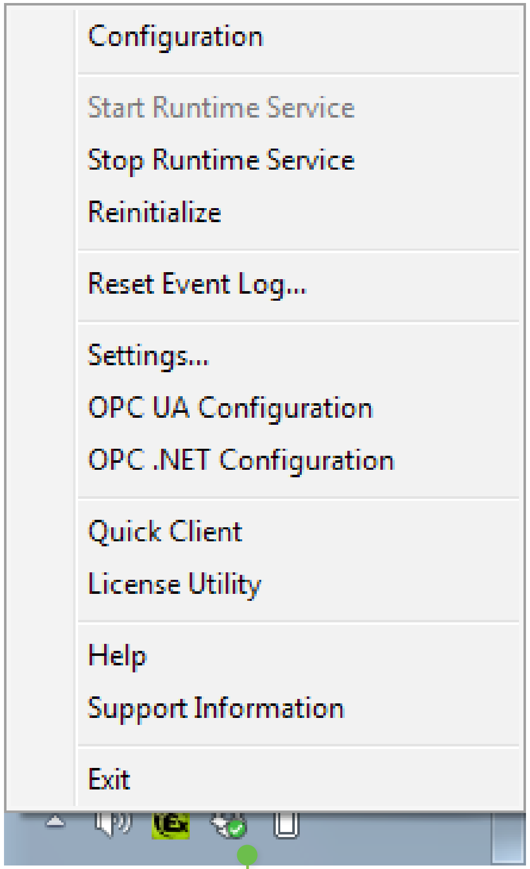
Follow the steps on the next page to configure a secure and encrypted data tunnel between two instances of KEPServerEX.



This guide applies to KEPServerEX V5.20 and above.

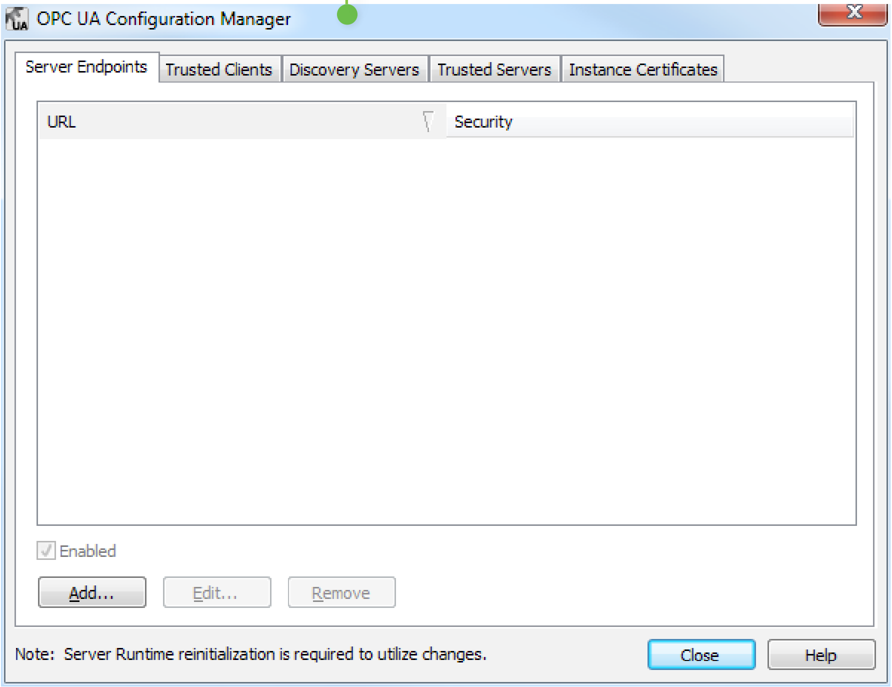
Follow the Steps

Step 1:
Configure the Tunnel Server



Open the **OPC UA Configuration Manager** by right-clicking on the **Administration** icon located in the **System Tray** and selecting **OPC UA Configuration.**

Next, create an endpoint, which is a point of access to the OPC UA server. To do so, select the **Server Endpoints** tab and then click **Add.**

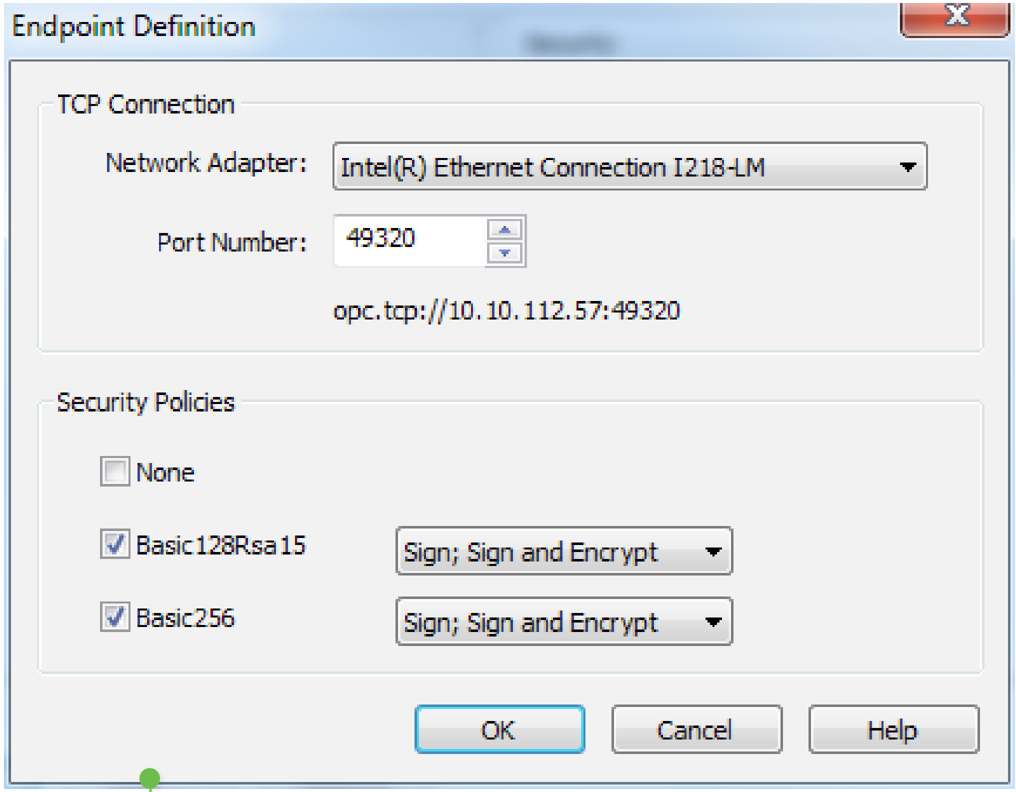


Note: Server Runtime reinitialization is required to utilize changes.

In **Endpoint Definition**, do the following:

- Select the network adapter on which to create the access point to the **tunnel server**. Using the “default” setting will create an endpoint that uses the computer name in place of an IP address.
- Record the “opc.tcp:// ...” string displayed below the **Port Number** setting for use in a future step.
- Choose a security policy of **Basic256** and then select **Sign and Encrypt** from the corresponding drop-down menu. These settings are the most secure, and will uniquely identify and encrypt each message exchanged between the **tunnel client** and **tunnel server**.
- Deselect the other **Security Policies** options.

Certificates will be exchanged automatically in a future step.



Endpoint Definition

TCP Connection

Network Adapter: Intel(R) Ethernet Connection I218-LM

Port Number: 49320

opc.tcp://10.10.112.57:49320

Security Policies

☐ None

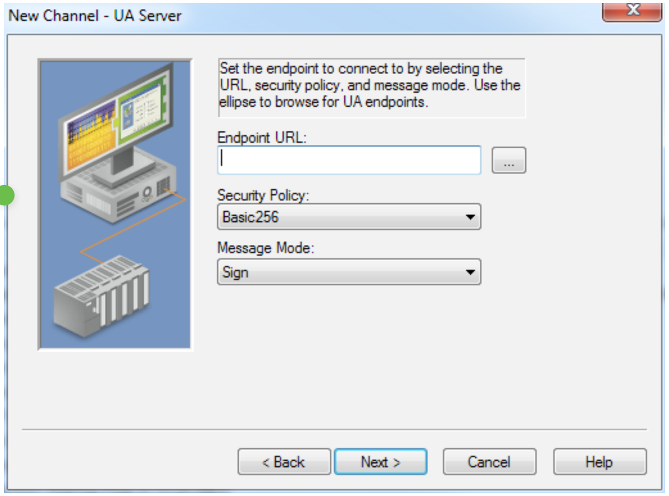
☑ Basic128Rsa15 — Sign; Sign and Encrypt

☑ Basic256 — Sign; Sign and Encrypt

Next, reinitialize the KEPServerEX Runtime service to register the newly-created endpoint. To do so, right-click on the **Administration** icon located in the **System Tray** and select **Reinitialize**.

Step 2:
Configure the Tunnel Client

On the **tunnel client**, open the KEPServerEX Configuration tool and add a channel to the KEPServerEX project. In **Device Driver**, select the **OPC UA Client** driver from the drop-down list and then click **Next** until you reach the **UA Server** dialog.



New Channel - UA Server

Set the endpoint to connect to by selecting the URL, security policy, and message mode. Use the ellipse to browse for UA endpoints.

Endpoint URL:

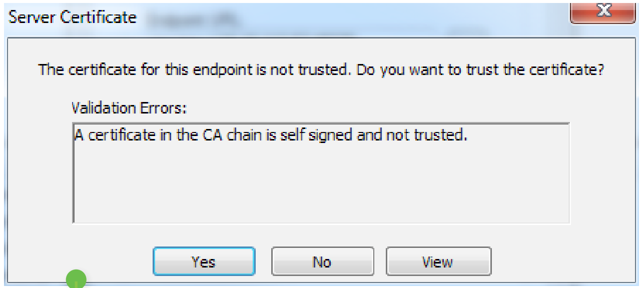
Security Policy: Basic256

Message Mode: Sign

In **Endpoint URL**, enter the newly-created server endpoint address recorded from Step 1.

In **Security Policy**, select **Basic256**. In **Message Mode**, select **Sign and Encrypt**, which are the settings selected for the endpoint that was created in Step 1.

Once you have entered the endpoint address, click **Apply**. The OPC UA Client driver acting as the **tunnel client** will now automatically attempt to connect to the **tunnel server** for the purpose of sourcing the tunnel server's certificate. The certificate is used for message signing and message encryption.



Server Certificate

The certificate for this endpoint is not trusted. Do you want to trust the certificate?

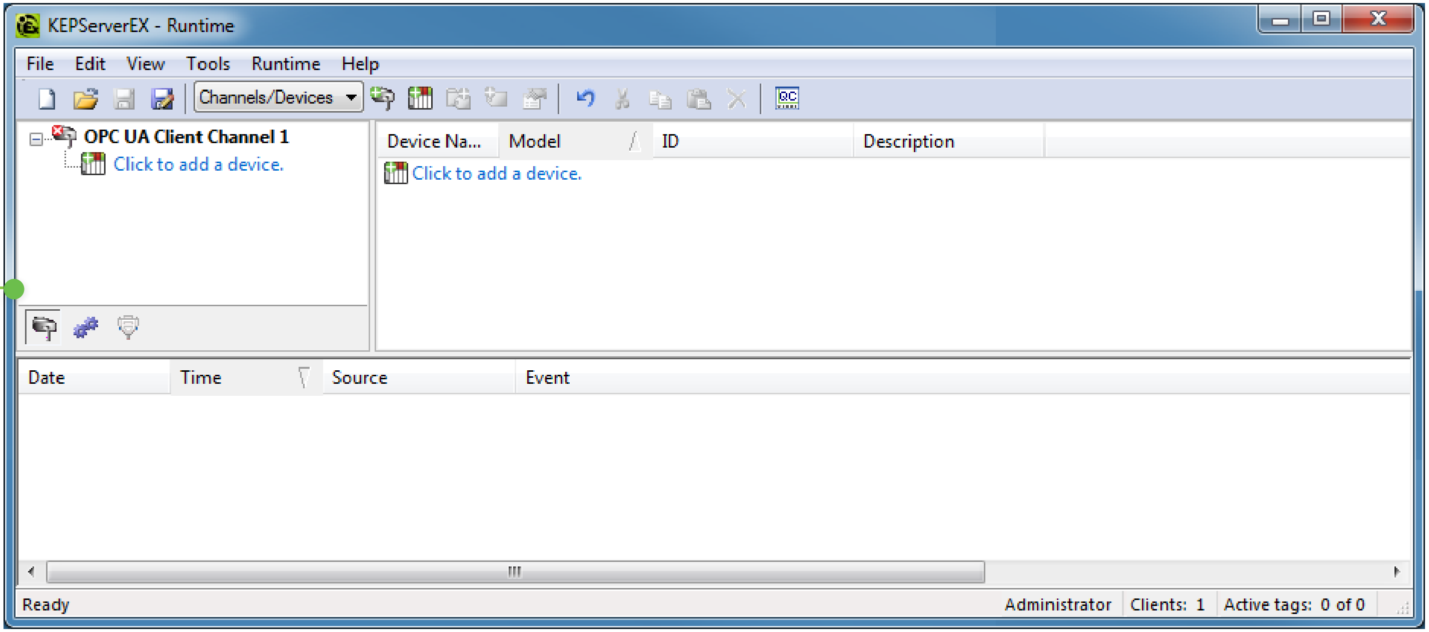
Validation Errors:

A certificate in the CA chain is self signed and not trusted.

If successful, a dialog will be presented that asks if you would like to trust the server certificate. Click **Yes** or select **View** in order to review the OPC UA server certificate and ensure that it originates from your **tunnel server**.

Once complete, click **Next** through the remaining channel settings. Then, select **Finish**.

Continuing in the **tunnel client,** in the KEPServerEX Configuration tool, select **Click to add a device** beneath the newly-created channel.



Click through the **Device Wizard**, selecting the default settings to create the device. Do not import tags yet; that will be done in a future step.

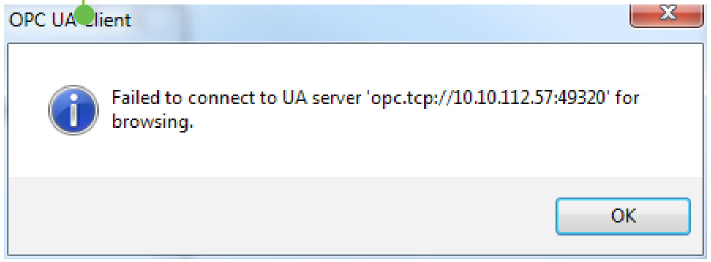
Note: In the OPC UA Client driver, a device represents a collection of tags (data points) in the **tunnel server** that should be sampled from connected devices at the same rate. By default, the **tunnel client** will direct the **tunnel server** to sample all tags at a rate of 500 milliseconds.

It will send the last observed value or quality change for each tag back to the **tunnel client** at a maximum rate of once per second. These settings can be adjusted in the **Device Properties** through the **Monitored Items** and **Subscription** tabs.

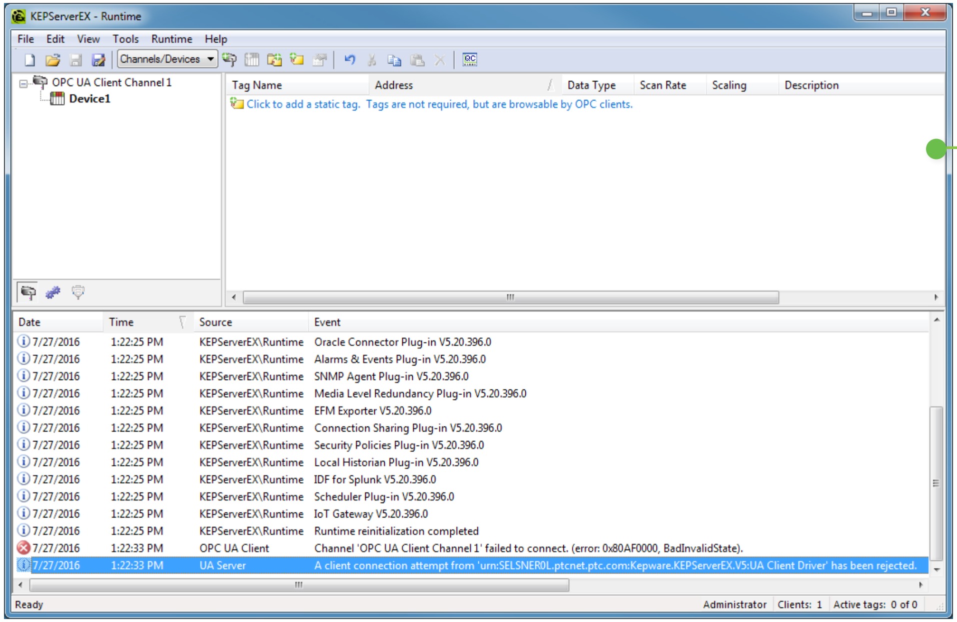
Step 3:
Share the Tunnel Client Certificate with the Tunnel Server

Having successfully exchanged the **tunnel server** certificate with the tunnel **client during** channel creation in a prior step, we can now use this device object to force the **tunnel client** certificate to be exchanged with the **tunnel server**. Upon successful exchange, the device object will be used to import tags into the **tunnel client** from the **tunnel server**.

To force the exchange, double-click on the device in the **tunnel client** and click **Import | Select import items**. Do not be alarmed when this import fails.



Failed to connect to UA server 'opc.tcp://10.10.112.57:49320' for browsing.



Tag Name	Address	Data Type	Scan Rate	Scaling	Description

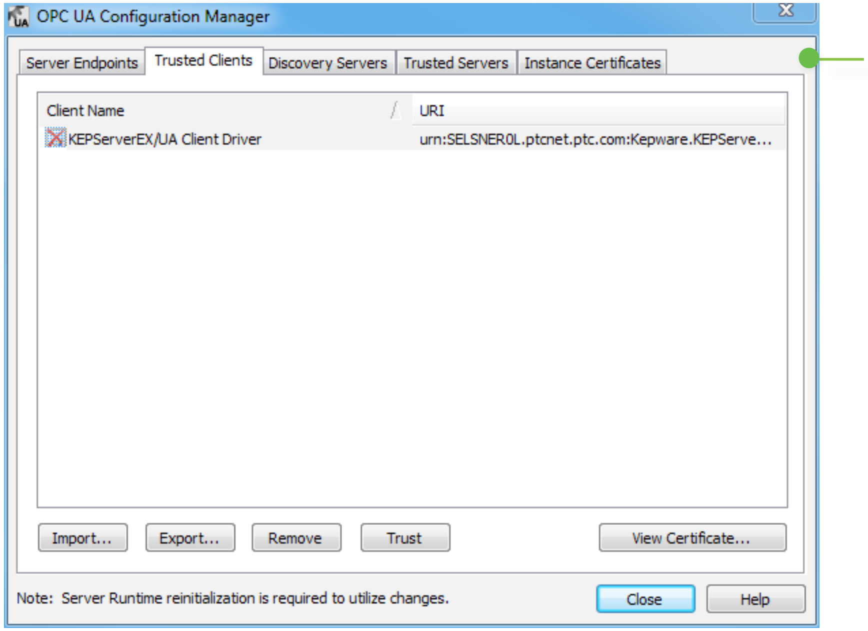
Click to add a static tag. Tags are not required, but are browsable by OPC clients.

Date	Time	Source	Event
7/27/2016	1:22:25 PM	KEPServerEX\Runtime	Oracle Connector Plug-in V5.20.396.0
7/27/2016	1:22:25 PM	KEPServerEX\Runtime	Alarms & Events Plug-in V5.20.396.0
7/27/2016	1:22:25 PM	KEPServerEX\Runtime	SNMP Agent Plug-in V5.20.396.0
7/27/2016	1:22:25 PM	KEPServerEX\Runtime	Media Level Redundancy Plug-in V5.20.396.0
7/27/2016	1:22:25 PM	KEPServerEX\Runtime	EFM Exporter V5.20.396.0
7/27/2016	1:22:25 PM	KEPServerEX\Runtime	Connection Sharing Plug-in V5.20.396.0
7/27/2016	1:22:25 PM	KEPServerEX\Runtime	Security Policies Plug-in V5.20.396.0
7/27/2016	1:22:25 PM	KEPServerEX\Runtime	Local Historian Plug-in V5.20.396.0
7/27/2016	1:22:25 PM	KEPServerEX\Runtime	IDF for Splunk V5.20.396.0
7/27/2016	1:22:25 PM	KEPServerEX\Runtime	Scheduler Plug-in V5.20.396.0
7/27/2016	1:22:25 PM	KEPServerEX\Runtime	IoT Gateway V5.20.396.0
7/27/2016	1:22:25 PM	KEPServerEX\Runtime	Runtime reinitialization completed
7/27/2016	1:22:33 PM	OPC UA Client	Channel 'OPC UA Client Channel 1' failed to connect. (error: 0x80AF0000, BadInvalidState).
7/27/2016	1:22:33 PM	UA Server	A client connection attempt from 'urn:SELSNER0L.ptcnet.ptc.com:Kepware.KEPServerEX.V5:UA Client Driver' has been rejected.

Ready | Administrator | Clients: 1 | Active tags: 0 of 0

The **tunnel client** has now shared its certificate with the **tunnel server**. On the tunnel server, you will notice a message in the server's Event Log resulting from the previous step.

Step 4:
Trust the Certificate from the Tunnel Client

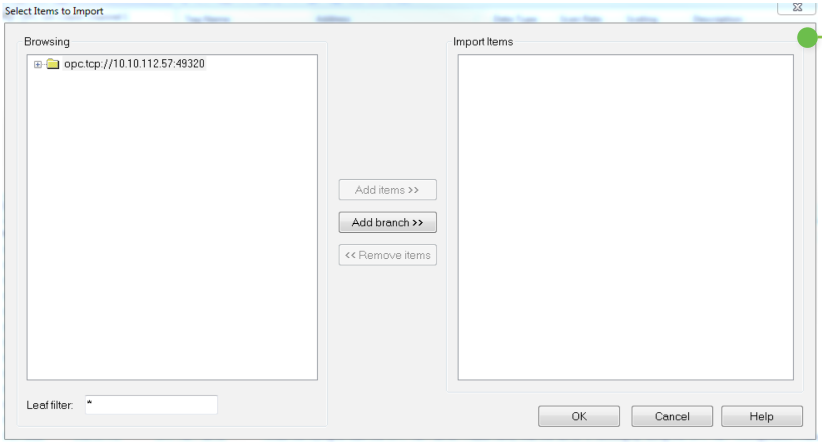


Client Name	URI
KEPServerEX/UA Client Driver	urn:SELSNER0L.ptcnet.ptc.com:Kepware.KEPServe...

Note: Server Runtime reinitialization is required to utilize changes.

As a layer of security, you must manually trust the certificate from the **tunnel client** on the **tunnel server**. On the tunnel server, open the **OPC UA Configuration Manager** and then select the **Trusted Clients** tab. Select the certificate from the **tunnel client** and then click **Trust**.

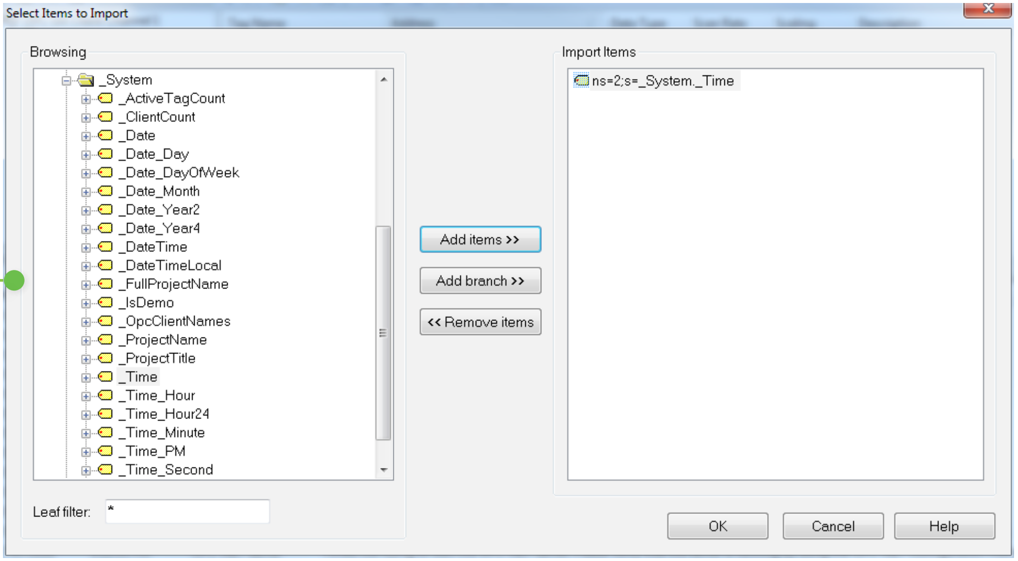
Step 5:
Test the Data Tunnel



Return to the **tunnel client** and then open **Device Properties**. Click **Import | Select import items** to invoke a dialog that enables you to browse available tags in the **tunnel server.**

Expand the server's address space by clicking the plus sign symbol.

Locate and expand the **_System** folder. Then, select the **_Time** item and click **Add items** to load the data point into the **tunnel server**.

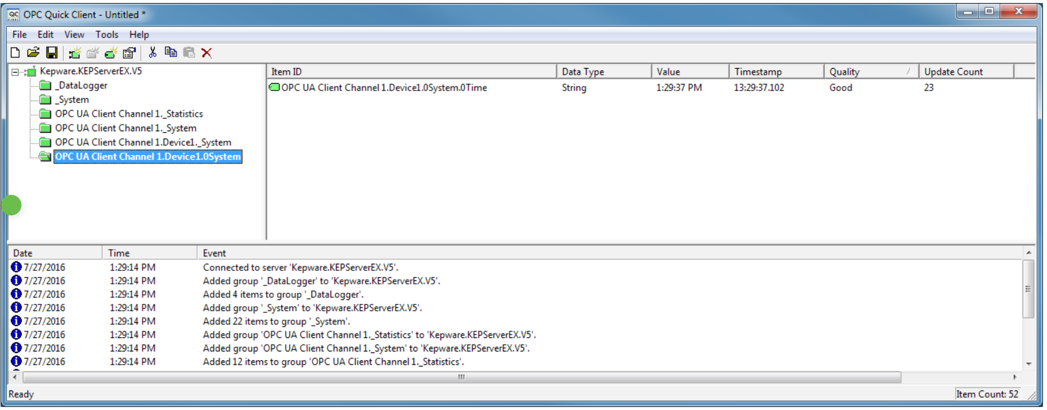


Import Items: ns=2;s=_System._Time

Leaf filter: *

Next, click **OK** and then read the imported tag using the **OPC Quick Client**. The imported tag should display a time with good quality and be updating every one second.

You've now configured a secure data tunnel between two instances of KEPServerEX.


OPC Quick Client - Untitled *
File
Edit
View
Tools
Help
Kepware.KEPServerEX.V5
_DataLogger
_System
OPC UA Client Channel 1._Statistics
OPC UA Client Channel 1._System
OPC UA Client Channel 1.Device1._System
OPC UA Client Channel 1.Device1.0System
Ready
Item Count: 52

Item ID	Data Type	Value	Timestamp	Quality	Update Count
OPC UA Client Channel 1.Device1.0System.0Time	String	1:29:37 PM	13:29:37.102	Good	23

```
Date        Time         Event
7/27/2016   1:29:14 PM   Connected to server 'Kepware.KEPServerEX.V5'.
7/27/2016   1:29:14 PM   Added group '_DataLogger' to 'Kepware.KEPServerEX.V5'.
7/27/2016   1:29:14 PM   Added 4 items to group '_DataLogger'.
7/27/2016   1:29:14 PM   Added group '_System' to 'Kepware.KEPServerEX.V5'.
7/27/2016   1:29:14 PM   Added 22 items to group '_System'.
7/27/2016   1:29:14 PM   Added group 'OPC UA Client Channel 1._Statistics' to 'Kepware.KEPServerEX.V5'.
7/27/2016   1:29:14 PM   Added group 'OPC UA Client Channel 1._System' to 'Kepware.KEPServerEX.V5'.
7/27/2016   1:29:14 PM   Added 12 items to group 'OPC UA Client Channel 1._Statistics'.
```

Tips and Tricks

1. When communicating to a **tunnel server** that is behind a router (for example, from a **tunnel client** across the Internet to a **tunnel server**), you will need to configure the router to conduct port forwarding. This will protect the internal network while permitting the tunnel to function. The required configuration is as follows:

   - Configure the router to listen for incoming TCP traffic on port ***x*** (where ***x*** is a port you select) and to forward all TCP traffic arriving on port ***x*** to the IP address of the machine running the **tunnel server**. In this configuration, you will need to specify the router to forward the incoming traffic to the specific port selected for use with the endpoint created in the **Server Endpoints** tab of the **OPC UA Configuration Manager** on the **tunnel server**.

   - On the **tunnel client**, the target endpoint (specified in **Channel Properties | UA Server**) needs to use the router's IP address instead of the IP address of the machine running KEPServerEX. Additionally, the port must be changed to reflect port x selected for use in the router.

2. You do not need to import tags into the **tunnel client** in order to read and write data through the tunnel. It is possible for an application using the **tunnel client** to dynamically address items in the **tunnel server** without importing tags into the **tunnel client** beforehand.

   To read the _Time tag from the **tunnel server** without first importing the tag, use the following syntax:

   OPC UA Client Channel 1.Device1.ns=2;s=_System._Time

   If the _Time tag were located in a device connected to the **tunnel server** instead of in the server-generated _System folder, the syntax would change as follows:

   OPC UA Client Channel 1.Device1.ns=2;s=<AnyChannelName>.<AnyDeviceName>._Time

Learn More

- To discover how OPC UA protects message integrity and confidentiality through message encryption and signing, read the **How OPC UA Protects Your Data** blog post.
- To gain detailed product information, access the **OPC UA Client driver** product manual.

J7860–SecureDataTunnelingwithKEPServerEX–EN–1016