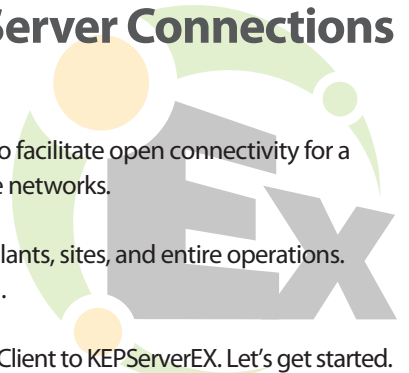




OPC UA Client and Server Connections



OPC UA is the newest open standard from the OPC Foundation to facilitate open connectivity for a variety of systems. Use it to bridge all types of data across remote networks.



OPC UA also effectively aggregates data from multiple devices, plants, sites, and entire operations. Use it to leverage meaningful information on the enterprise level.

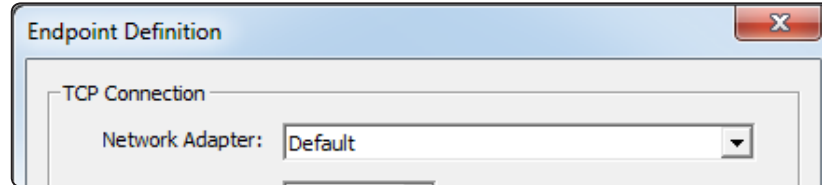
Follow the five steps located in the sidebar to connect an OPC UA Client to KEPServerEX. Let's get started.

Follow the Steps

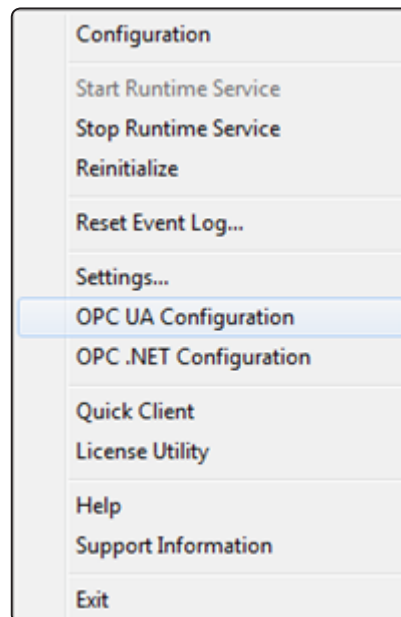
Step 1:

Define an endpoint in KEPServerEX's OPC UA Configuration Manager.

OPC UA connections use endpoint addressing. An endpoint serves as the URL that other OPC UA software applications will use to find and connect to remote applications.

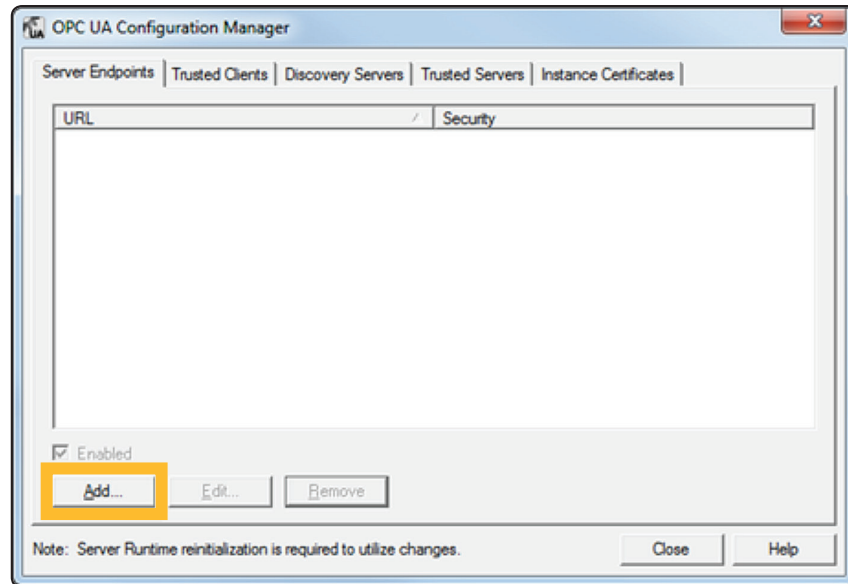


To create an endpoint in KEPServerEX, open the OPC UA Configuration Manager by right-clicking on the Administration icon (located in the System Tray) and selecting OPC UA Configuration.

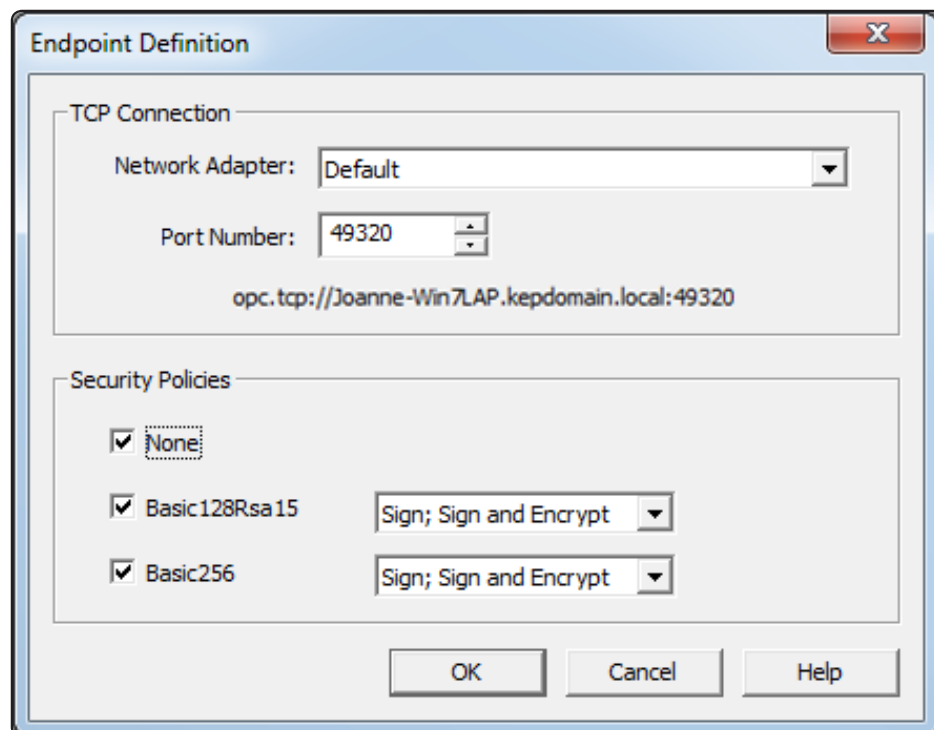




In OPC UA Configuration Manager, open the Server Endpoints tab and then click Add.



In Endpoint Definition, locate Security Policies. Check None if your application does not need to use security certificates for encrypted communication (such as when the environment is already secured by IT). Leave the remaining settings at their default values, and then click OK to create the endpoint.



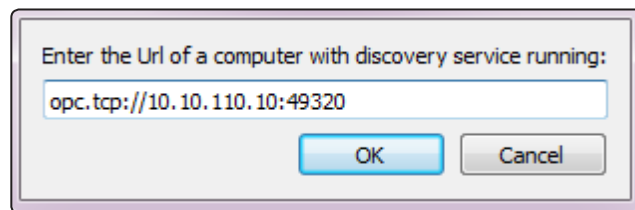


Step 2:

Enter the newly-created server endpoint address in the OPC UA client.

OPC UA clients should support browsing for OPC UA servers. This means you can simply open your client application, add a server connection, and then browse for the KEPServerEX OPC UA server to connect.

If your client cannot find the KEPServerEX OPC UA server, enter the server endpoint address created in Step 1.



Note: This image is from a Third-Party OPC UA client.

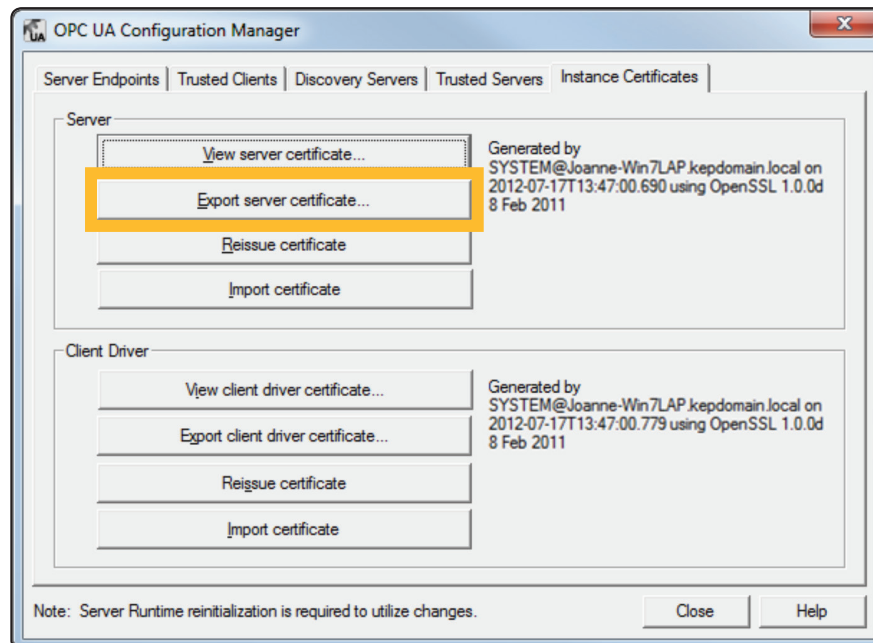
Step 3:

Exchange security certificates between the OPC UA Client and Server.

Note: Skip this step if "None" was selected in the Security Policies section of the Endpoint Dialog in Step 1.

If the OPC UA client does not prompt you to exchange certificates with KEPServerEX automatically, then you must manually generate a certificate from the server and then upload it to the client.

To manually generate a certificate, return to the OPC UA Configuration Manager and open the Instance Certificates tab. Click Export Server Certificate.



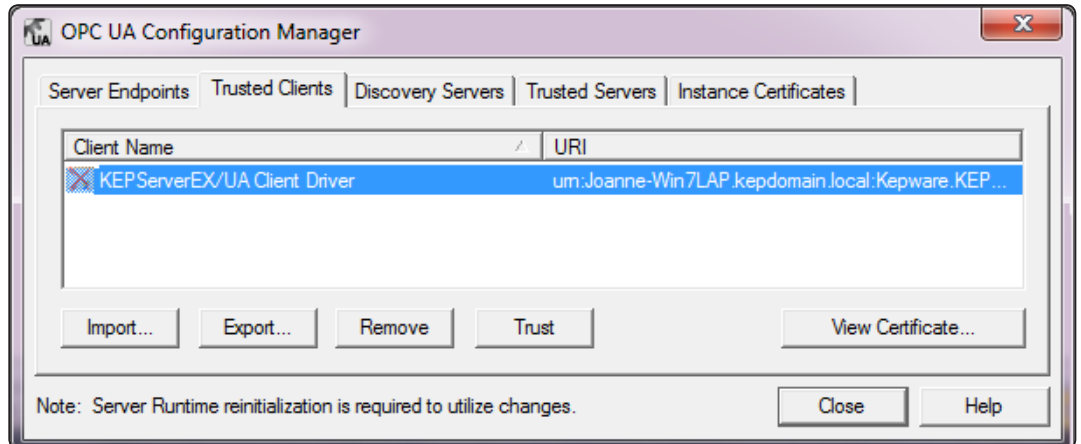
Save the certificate file and transfer it to the OPC UA client according to the client's instructions.



Step 4:

Trust the OPC UA client connection.

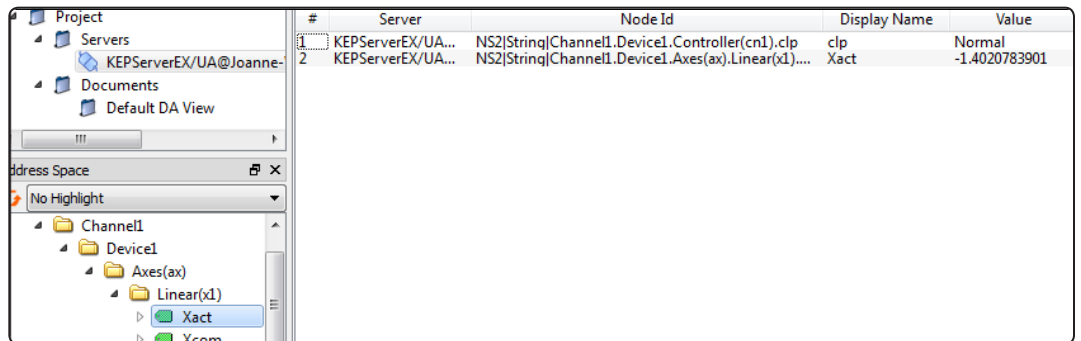
Browse to the Trusted Clients tab in KEPServerEX's OPC UA Configuration Manager. If the client you are trying to connect to has a red X, click on the name of the client and then click "Trust". If the client does not have a red X you may skip this step.



Step 5:

Verify the connection is successful by reading tag values from KEPServerEX in the OPC UA Client application.

In the OPC UA Client, check that tag values can be read and that they show "Good" quality. If KEPServerEX is not connected to a device, use the Simulator Driver to generate a ramp or sine wave function to see if data is changing.



Note: This image is from a Third-Party OPC UA Client.