Connectivity Guide

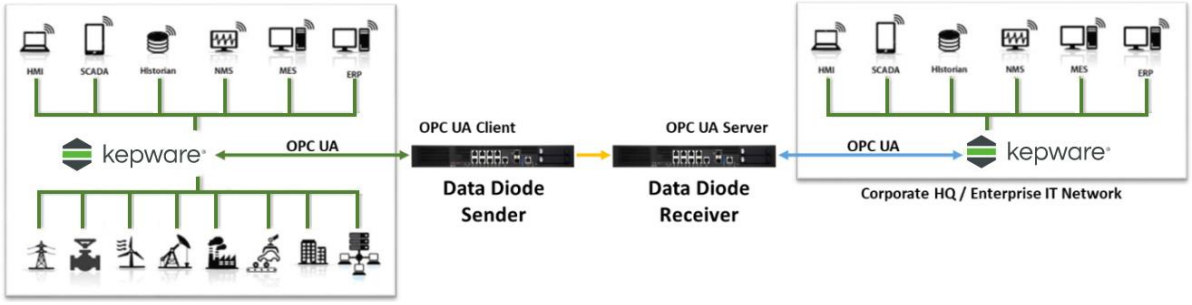
KEPServerEX® and ST Engineering Data Diode

September 2021
Ref. 1.001

Table of Contents

1. Overview and Requirements

This guide demonstrates the use of the ST Engineering Data Diode in between a pair of KEPServerEX OPC servers to secure the industrial network and provide one-way traffic between a typical OT and IT network layer.



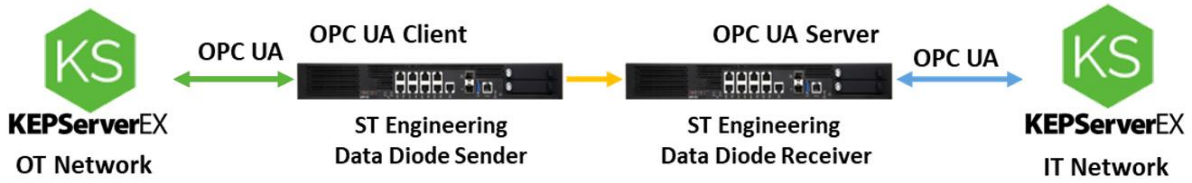
A data diode is a unidirectional communication hardware that enforces one-way data transfers across the networks. The ST Engineering Data Diode has been tested for up to 40,000 tags (word) at one second data change rate.

Find out more about the product at https://www.stengg.com/cross-domain-cybersecurity.

1.1 Integration Benefits

- Ensures unidirectional (physical layer one way) data transfer to protect critical OT system.
- Supports all OPC UA built-in data types.
- Configures with KEPServerEX Automatic Tag Creation.
- Real-time without data loss:
  - Real-time value update based on subscription
  - Periodically queries of every monitored nodes' values with re-transmit to ensure no loss
- Broad range device integration with more than 150 device drivers, client drivers, and advanced plug-ins.

1.2 Test Deployment Scenario



On the OT network, a copy of KEPServerEX was installed and connected to various OT assets using various drivers. A pair of the data diodes sits between and data is transferred internally across the data diode sender and receiver via the built-in OPC UA clients in the data diode sender and exposed via the UA server on the data diode receiver.

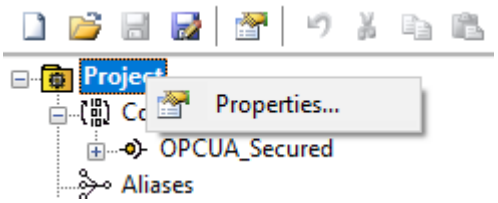
The data diodes constructs and the model and sends across the network by iteratively defining two parameters, namely the NodeID (data leaf) and its parent (Node Reference). *Refer to information below about defining the [parent NodeID](#).*

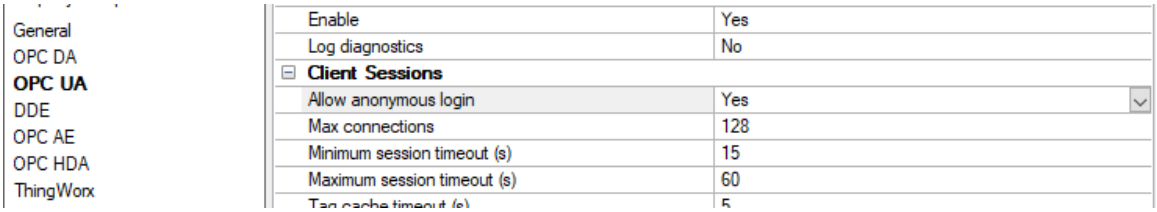
2. Preparing the Kepware UA Server

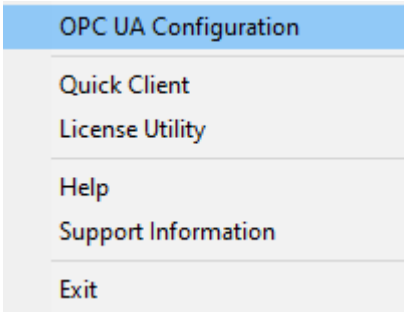
CAUTION: This guide uses the anonymous security policy and anonymous login (NOT secure for use in production).

Refer to Secure OPC UA Tunneling with KEPServerEX for instructions on how to create an authenticated version of the UA connection.

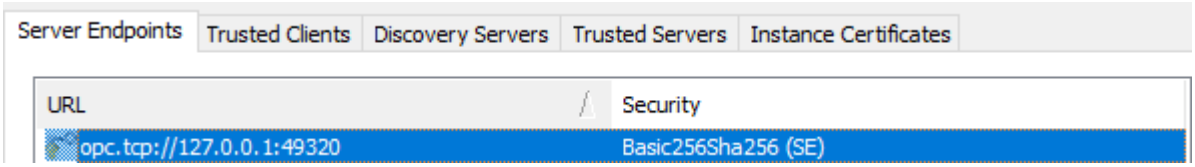
1. In KEPServerEX, right click on the **Project** and select **Properties...**.
2. Set the property to **Allow Anonymous Login** for client session to **Yes**.



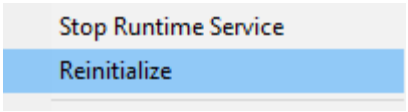




3. Enable the server endpoint by right clicking the admin icon and selecting **OPC UA Configuration**.



4. Under **Server Endpoints**, add in the appropriate NIC binding and select **None**.



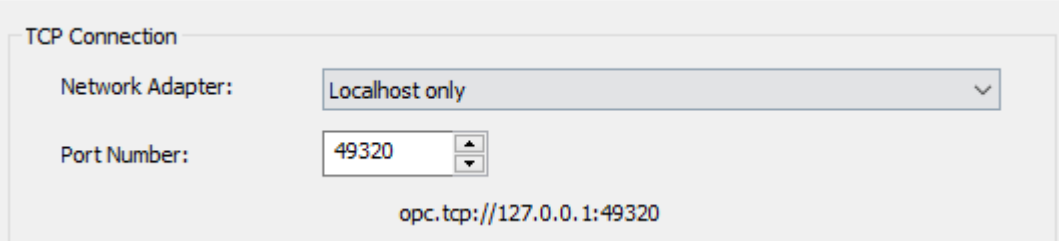
5. Reinitialize the server via the KEPServerEX Administrator tool.

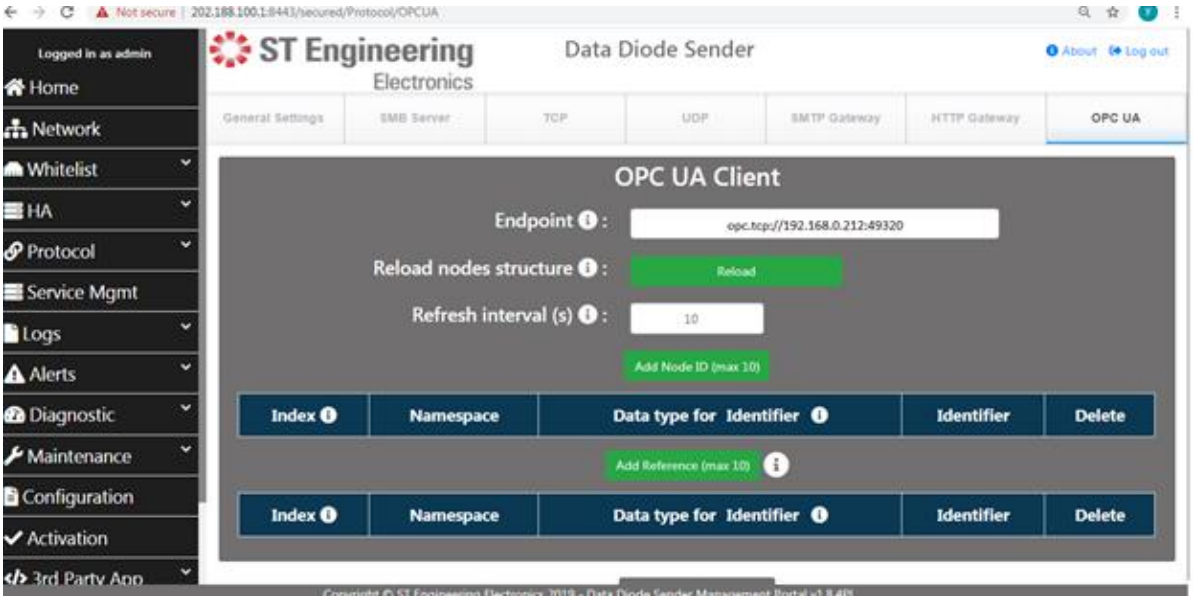
3. Data Diode Sender Configuration

Configure the OPC UA Client and KEPServerEX with the following steps.

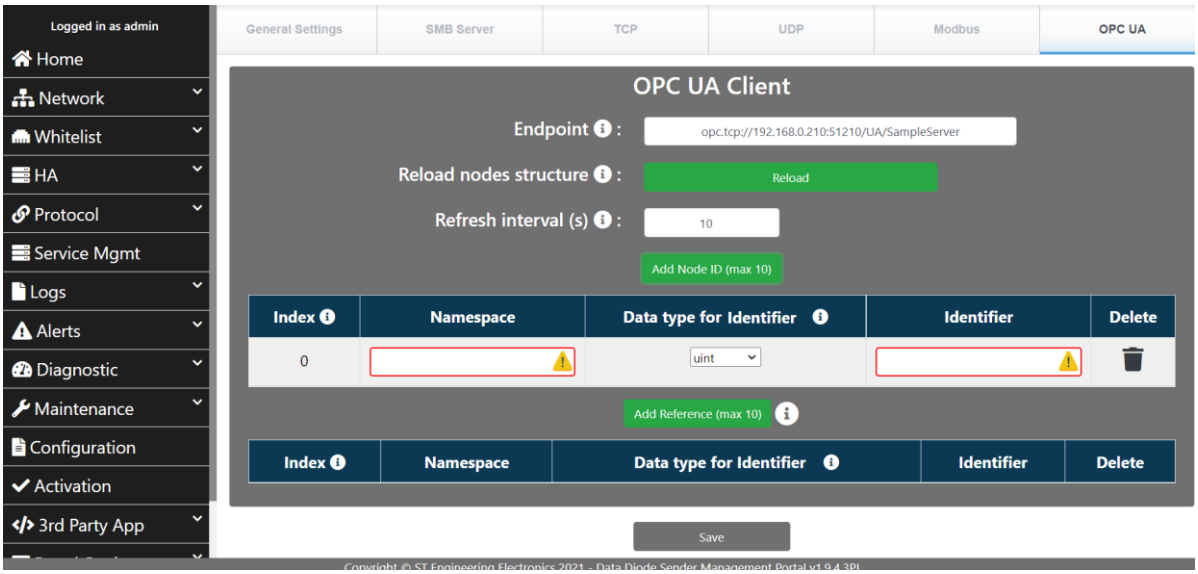
1. Access the management portal via the management and login.
2. Under the data diode sender, select **Protocol > OPC UA**.
3. Set KEPServerEX **Endpoint** URL (typically, in the format of opc.tcp://<IP>:49320).

- From the UA Configuration steps above where the UA Endpoint is enabled.

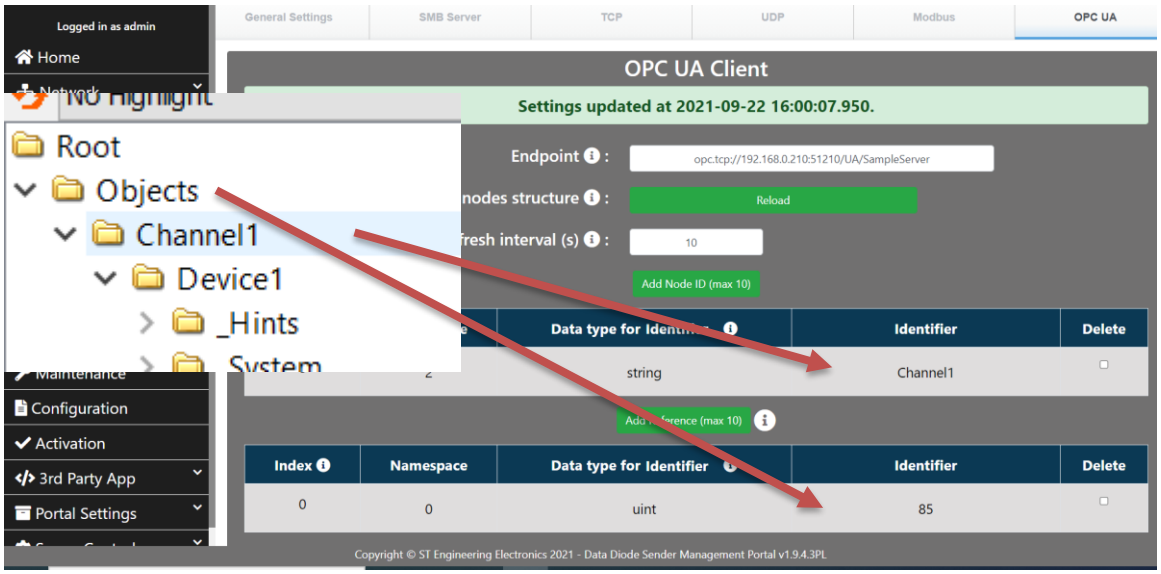




4. To add the data to the sender node of the data diode pair, click **Add Node ID** button**.**
5. Enter the namespace, data type and the identifier string for the respective hierarchy. For example, for Kepware. To add all data under Channel1:
    a. namespace = 2 (provided by UA Server)
    b. Datatype of identifier = select from dropdown (uint, guid, string , bytearray)
    c. identifier = Channel1

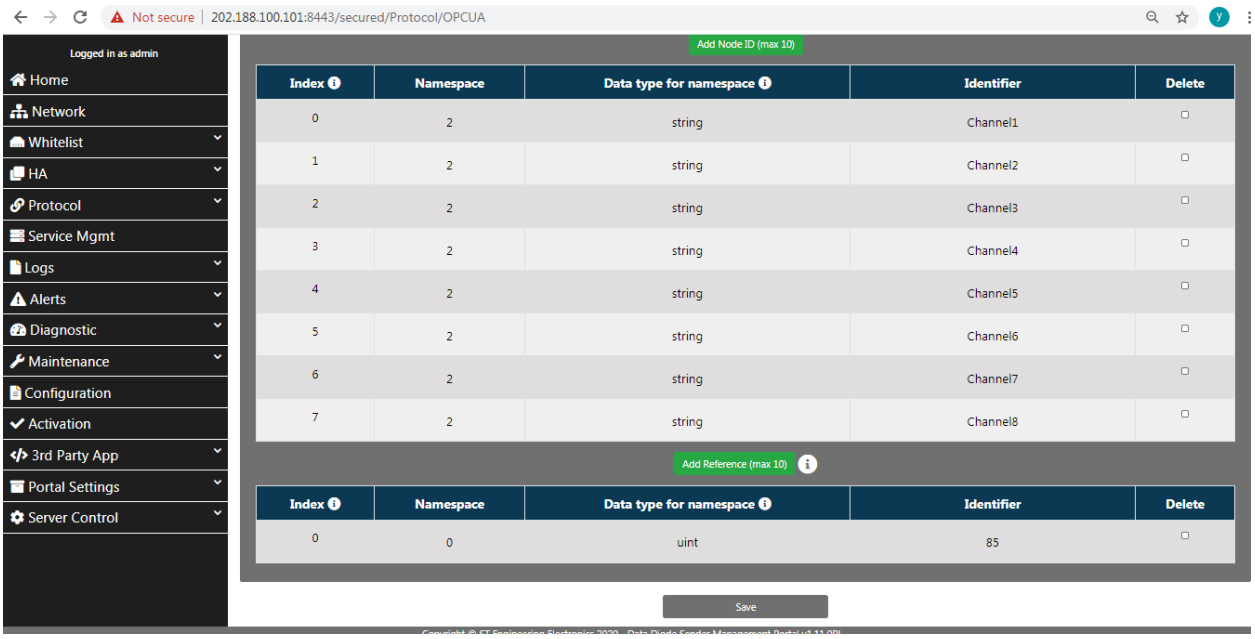


6. Now, define its parent node of the NodeID. In this case, the parent object is the root object folder (namespace = 0, NodeID type = uint, identifier = 85).
    a. Namespace = 0
    b. Datatype = uint
    c. Identifier = 85



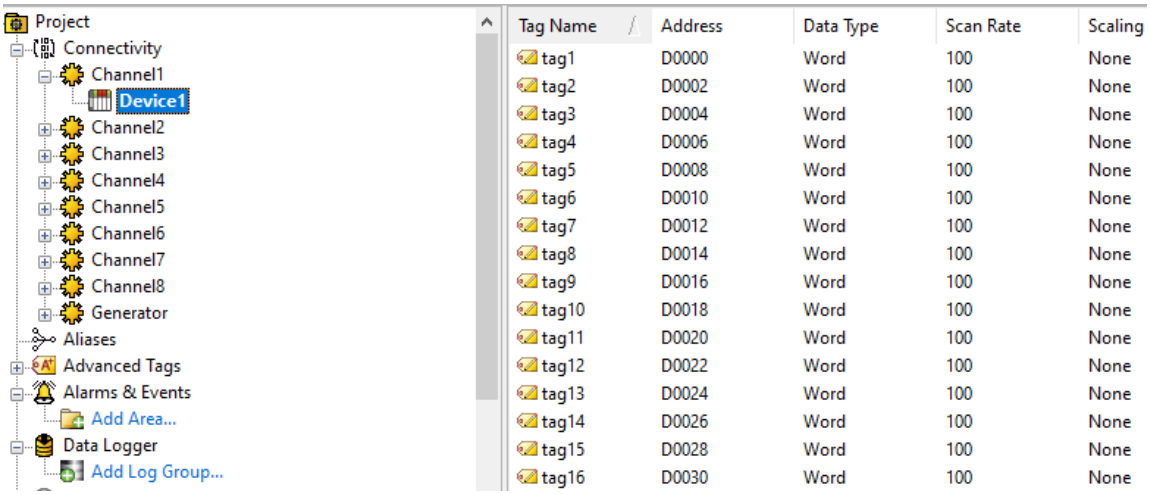
Notes:

- The data diode subscribes to the configured node and all its sub nodes. Once any node's value is changed, the value is sent to the data diode receiver. In this case, all monitoring node parent nodes.
- A poll is periodically issued as a watchdog mechanism.
- Load node structure is only required during the first-time setup.



7. From service management, choose **Stop OPC UA Service**.
8. Click the button to **Reload** node structure.
9. From service management, choose **Start OPC UA Service**.
10. Check the log to ensure the node structure is loaded.

11. The sample scenario is a project of 40,000 tags over eight channels using the Memory Based driver as the device simulator. The data is driven by Advanced Tags collected through the _system.time_second tag. Each of the channel has 1 device and 5000 tags.

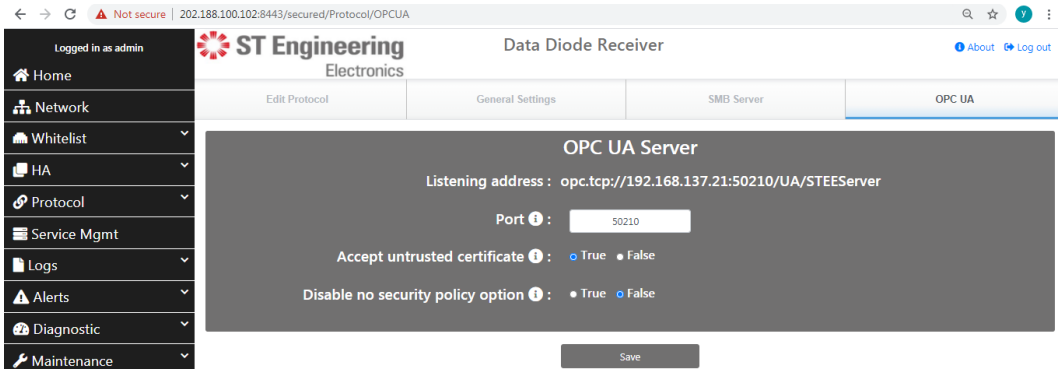


4. Connecting the Data Diode Receiver

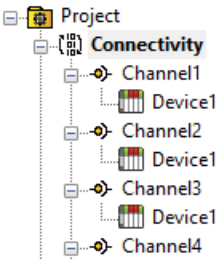
The data diode receiver is connected through the OPC UA server interface.

1. Start the OPC UA service by choosing **Service Management... Start OPC UA Service**.
2. The UA endpoint of the device is listed under OPC UA tab under **Protocol... OPC UA**.

Tip: In the screen below, the OPC UA URL is opc.tcp://192.168.137.21:50210/UA/STEEServer.



3. The load test leveraged another KEPServerEX OPC UA client to connect the end point.
4. Similarly, the exact same project was set up with eight OPC UA channels, one device per channel, with 5000 tags inside to replicate the Kepware data source project.



5. Lab Test Result

- All monitored nodes and sub nodes' hierarchical structures are successfully transferred to receiving site.
- Kepware's OPC UA Client can display the node hierarchical structure.
- The values of the 40,000 tags at 1 second sampling rate are updated with no data loss.