# EtherNet/IP™ to Modbus® TCP/IP to OPC UA Server Gateway FAQ

**I understand this gateway allows EtherNet/IP and Modbus TCP/IP PACs and devices to share OPC UA data with OPC clients, but what distinguishes this gateway from other OPC UA gateways?**

Currently, this is the only stand-alone protocol gateway that simultaneously supports the following:

- 8 EtherNet/IP Class 1 server connections
- Multiple EtherNet/IP Class 3 client and server connections
- 10 Modbus TCP clients and 10 Modbus TCP server connections
- 10 OPC UA Server connections
- 64,000 tag limit

**Is this OPC UA gateway compatible with OPC Classic?**

No. As OPC Classic is quickly becoming obsolete, we've chosen not to support it. If access from classic OPC Client is required, you can use products available in the market that convert OPC UA to OPC Classic.

**OPC UA offers several types of methods for securely passing data between OPC UA clients and OPC UA servers. What types of security methods are implemented in this OPC UA server?**

The PLX32-EIP-MBTCP-UA currently implants the following security modes and policies:

- **None**
- **Signed**
  - Basic128Rsa15
  - Basic256
  - Basic256Sha256
- **Encrypted and Signed**
  - Basic128Rsa15
  - Basic256
  - Basic256Sha256

### Can the server support all these security policies simultaneously?

Yes. Note that in order to support all listed above policies, 2 different certificates are required, and the server supports the use of the proper certificate for the security policy requested by the client.

### What kind of certificates does the server use: self-signed, or signed by the Certificate Authority (CA)?

Initially the server generates a self-signed certificate. During provisioning of the gateway, it is replaced by a certificate signed by CA.

### Is a third-party public key infrastructure (PKI) management system required? Where can we get a CA Certificate, and how can the server's certificate be replaced by a CA signed certificate?

Management of certificates is implemented using the Configuration Manager Application. It supports the importing of the CA Certificate, created by a third-party PKI management system. You can also create your own CA Certificate, and install the certificate signed by that CA, via GUI (graphical user interface).

### Is it possible to install into the gateway a certificate created by a third-party PKI management system?

Yes. Import of the certificate from a file and installation of it in the gateway is also supported.

### How are tags configured? Is it possible to generate a tag configuration file by some script and then import? Is there GUI to configure tags?

The Configuration Manager of the gateway provides GUI to configure tags and download it into the gateway. In addition, the import/export of tags from/to the XML file is supported.

### How can tags be organized in the OPC UA address space? Is it a flat list, or is it possible to organize them into groups?

Tags can be organized into folders, and can be listed under the root folder of tags.

### Does the server support restriction of access to data?

Yes, the server implements access control based on user name and password provided by the client. There are predefined groups such as Operators and Users, and depending on what groups the user is a member of, tag values can be read only or writable too. Access rights are configured from the Configuration Manager GUI.