Cyberlogic OPC UA Server Help

OPC UA Connectivity for Cyberlogic OPC Servers

Version 1

CYBERLOGIC OPC UA SERVER HELP

Version 1

Document last revision date September 3, 2020

TABLE OF CONTENTS

INTRODUCTION

The Cyberlogic OPC UA Server is a free software add-on to all Cyberlogic OPC Server Suite products, which allows the OPC Unified Architecture (OPC UA) client applications access to the Cyberlogic OPC Server data. Prior to installation, make sure that at least one of the Cyberlogic OPC Server Suite products is installed, and the Cyberlogic OPC Server is configured.

The Cyberlogic OPC UA Server can work with any version of the Cyberlogic OPC Server if both are installed on one of the supported Windows platforms.

OPC UA Protocols

The OPC UA standard supports two protocols: the binary protocol (opc.tcp) and the Web Service protocol (http/https).

The binary protocol offers the best performance, least overhead, takes the least amount of resources, and offers the best interoperability. It uses a single arbitrarily selected TCP port for communication, which simplifies tunneling or passing through a firewall.

The Web Service (SOAP) protocol is a simpler protocol and is intended for lower performance applications. It is also firewall-friendly since it is using standard http(s) ports.

In order to achieve the best interoperability and performance, the Cyberlogic OPC UA Server supports the binary protocol (opc.tcp).

OPC UA Security

The OPC UA was designed with security being one of the main pillars of its architecture. OPC UA security consists of authentication, authorization, encryption, and data integrity via digital signatures. For authentication, encryption and signatures, X.509 v3 certificates are used on both the server and the OPC UA client side. A username and password can also be used for authentication, and access to the server can be restricted to authorized users only.

Security Policies

A security policy specifies which security mechanisms are to be used. The OPC UA Server announces which mechanisms it supports, and the UA Client selects one to use with the secure channel it wishes to open or for the session-less connection it wishes to make. A security policy determines the algorithms for signing, encryption, and key derivation.

The choice of allowed security policies is normally made by the administrator typically during or right after the OPC UA applications are installed. Here are the security policies supported by the Cyberlogic OPC UA Server:

- None
- Basic128Rsa15 (Deprecated)
- Basic256 (Deprecated)
- Basic256Sha256

Caution! The security policies, Basic128Rsa15 and Basic256, have been deprecated by the OPC Foundation as of OPC UA Specification, version 1.04. The encryption provided by these policies is not considered secure and usage should be limited to providing backward compatibility.

For most applications, it is recommended that the Basic256Sha256 security policy is used. The security policy, None, provides no security and should normally be disabled.

Each security policy supports the selection of several security modes: None, Sign, and SignAndEncrypt. Security mode, None, is only used with security policy, None. For high-security applications, SignAndEncrypt should be used. In some applications, where data confidentiality is not required, Sign might be sufficient.

Authentication Policies

Authentication policies define the ways users are authenticated when UA clients connect to the server. Users can be authenticated by a username and password, or a digital certificate. Authentication can also be disabled by selecting, Anonymous. When using a certificate for authentication, the certificate must also be trusted and placed on the Client Certificates list.

Authorized Users

OPC UA provides user authorization based on the authenticated users. The Authorized Users list defines the users that have access to the server when username and password authentication is used.

Application Instance Certificates

OPC UA uses a concept for application authentication that allows applications, which intend to communicate, to identify each other. Each OPC UA application instance (client or server) has a certificate (Application Instance Certificate) assigned that is exchanged during secure channel establishment. The receiver of the certificate checks whether it trusts the certificate, and based on this check, it accepts or rejects the request or response message from the sender.

Server Certificate

OPC UA server has a single Application Instance Certificate, which is used to identify itself to the client applications. It is also used for signing and or encrypting messages. To simplify discovery of the server by UA Clients, this certificate is typically registered with the Local Discovery Server (LDS).

Client Certificates

Each OPC UA server has a list of Application Instance Certificates for each trusted client. These certificates are used when a security policy requires signed and/or encrypted messages. The Cyberlogic OPC UA Server also uses the same list to include certificates that are used for authenticating users.

The Client Certificates list is typically created by a system administrator. An administrator determines if the certificate is signed, validated and trustworthy before placing it in this list.

Compatibility and Compliance

The Cyberlogic OPC UA Server provides full compliance with the OPC Foundation’s OPC UA Specification, version 1.04.

WHAT SHOULD I DO NEXT?

The links below will take you directly to the section of this manual that contains the information you need to configure, use and troubleshoot the Cyberlogic OPC UA Server.

Read a Quick-Start Guide

First-time users of the Cyberlogic OPC UA Server will want to read the Quick-Start Guide, which walks through a typical configuration session, step-by-step.

Get Detailed Information on the Configuration Editor

Experienced users who want specific information on features of the configuration editor will find it in the Configuration Editor Reference section.

Verify That It's Working or Troubleshoot a Problem

If you have already configured the server, you should verify that it operates as expected. Refer to the Validation & Troubleshooting section for assistance. In case of communication problems, this section also provides problem-solving hints.

Print a Copy of This Document

The content of this document is also provided in PDF format. PDF files can be viewed using the Adobe® Reader program and can also be used to print the entire document.

Contact Technical Support

To obtain support information, click on the Server Control/Product Info tab. The contact information is provided there.

QUICK-START GUIDE

Before the Cyberlogic OPC UA Server can be used, it must be properly configured. The server is installed with the most common settings already set, but some manual configuration is still required.

OPC UA clients and servers must match their security and authentication settings before connections can be established. That typically means that you must configure the security policies, set authorized users, and add digital certificates to validate users and/or client applications.

The following shows a typical configuration session. Use it only as a guideline of how to configure the most common features. For detailed descriptions of all the available features, refer to the Configuration Editor Reference section.

Note Before configuring the Cyberlogic OPC UA Server, one of the Cyberlogic OPC Server products must be installed and configured.

The procedure is broken down into several short segments:

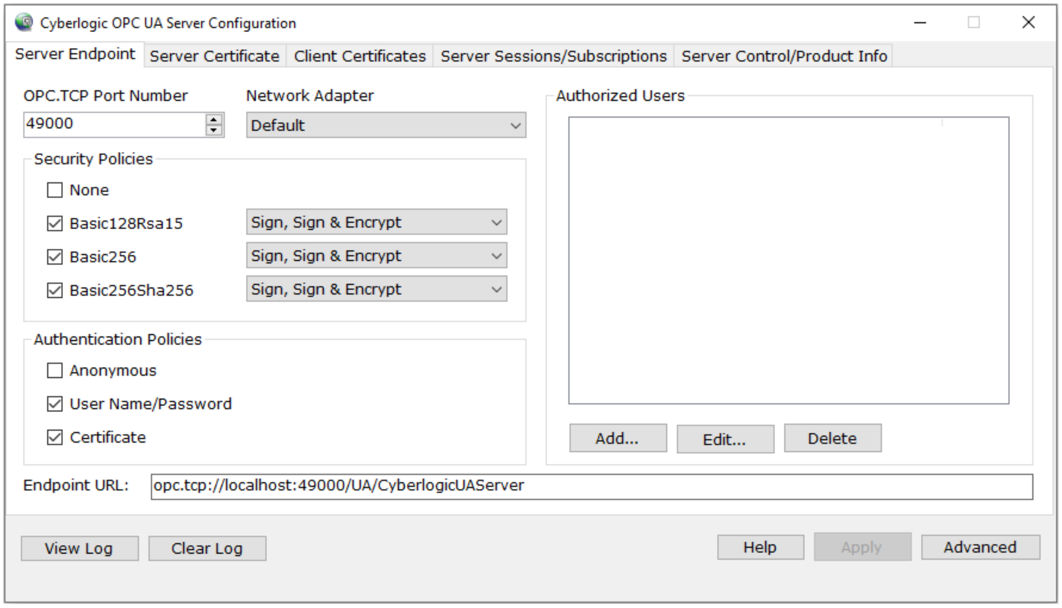
- Server Endpoint and Security
- Server Certificate
- Client Certificates
- Server Control

We will start with Server Endpoint and Security.

Server Endpoint and Security

The first step in configuring the UA Server is defining the server endpoint and the security settings that the server will enforce. Each OPC UA client must match these settings for the server to allow connections.

1. From the Windows ***Start*** menu open the ***Cyberlogic OPC UA Server*** submenu. From there select ***Configuration & Status***.



OPC.TCP Port Number: 49000

Network Adapter: Default

Security Policies

☐ None

☑ Basic128Rsa15 — Sign, Sign & Encrypt

☑ Basic256 — Sign, Sign & Encrypt

☑ Basic256Sha256 — Sign, Sign & Encrypt

Authentication Policies

☐ Anonymous

☑ User Name/Password

☑ Certificate

Authorized Users

Endpoint URL: opc.tcp://localhost:49000/UA/CyberlogicUAServer

Running the editor for the first time displays the screen above.

2. First, you need to configure the ***OPC.TCP Port Number*** and ***Network Adapter*** the UA server will use. By default, port 49000 and the ***Default*** network adapter is selected. These settings will work for most installations. However, your network administrator may require you to change them. Notice the ***Endpoint URL*** shown at the bottom of this screen. This string may be required when configuring your OPC UA client application.

3. Second, the ***Security Policies*** must be configured. By default, all policies, other than ***None***, are enabled, and security mode ***SignAndEncrypt*** is selected. This means that all messages between the server and clients are secured by encryption and digital signatures. You should only enable the policies you intend to use.

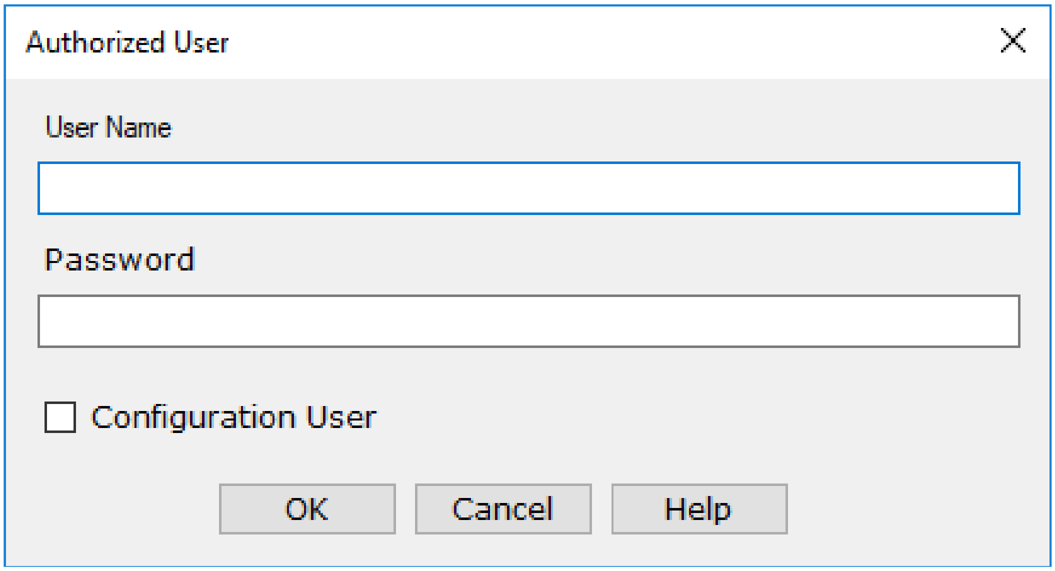
Caution!

> The security policies, Basic128Rsa15 and Basic256, have been deprecated by the OPC Foundation as of OPC UA Specification, version 1.04. The encryption provided by these policies is not considered secure and usage should be limited to providing backward compatibility.

For most applications, it is recommended that the ***Basic256Sha256*** security policy is used. The security policy, ***None***, provides no security and should normally be disabled.

4. In most cases, access to the UA server is restricted to only certain authorized users. The ***Authentication Polices*** define how these users will be validated. By default, user authentication by ***User Name/Password*** and ***Certificate*** are enabled. If you are planning on authenticating users, make the correct selections here. When using ***Certificate*** for authentication, the certificate must also be trusted and placed on the Client Certificates list.

5. If you selected the ***User Name/Password*** authentication in the previous step, you need to create the authorized users list. To do that, click the ***Add...*** button in the ***Authorized Users*** section. Otherwise continue to step 7.



6. Enter the ***User Name*** and ***Password*** for an authorized user. You can also select the ***Configuration User*** checkbox. Configuration users have the rights to execute some of the OPC UA methods that expose the server configuration information. Select this checkbox only if this functionality is required. Click ***OK*** button to finish. If you need to add more users, go back to step 5.

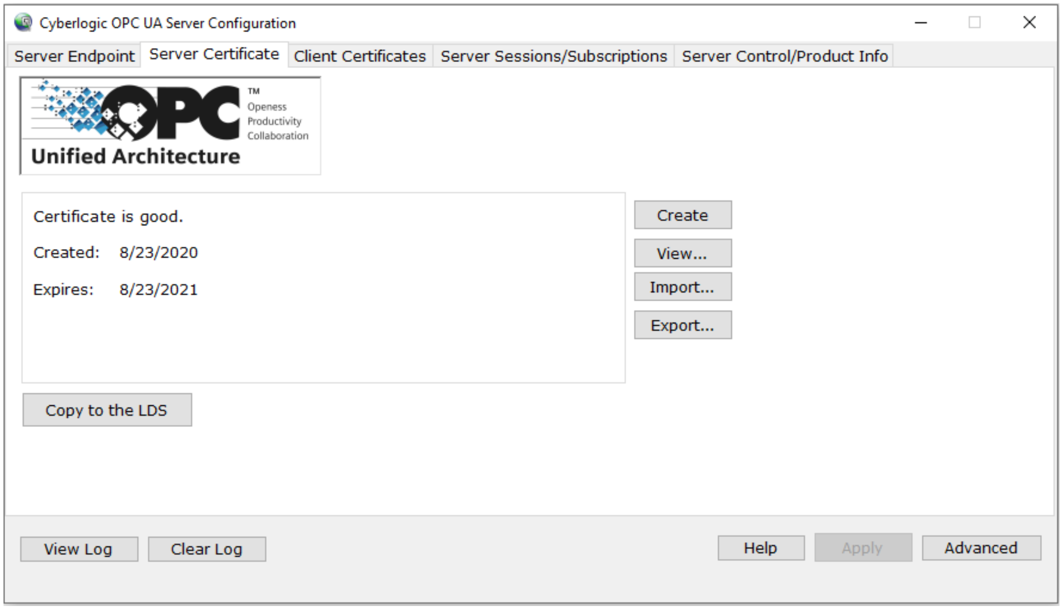
7. Click the ***Apply*** button to accept the changes.

The server endpoint and the security settings are now configured. To continue, go to Server Certificate.

Server Certificate

OPC UA server has a single Application Instance Certificate, which is used to identify itself to the client applications. To simplify discovery of the server by UA Clients, this certificate is typically registered with the Local Discovery Server (LDS).

1. Select the ***Server Certificate*** tab.



Certificate is good.

Created: 8/23/2020

Expires: 8/23/2021

2. By default, the self-signed certificate is created during installation, and you do not need to create it here again. However, if you would rather use a more secure CA issued certificate, press the ***Import*** button to replace it. The certificate must be in the PFX format.

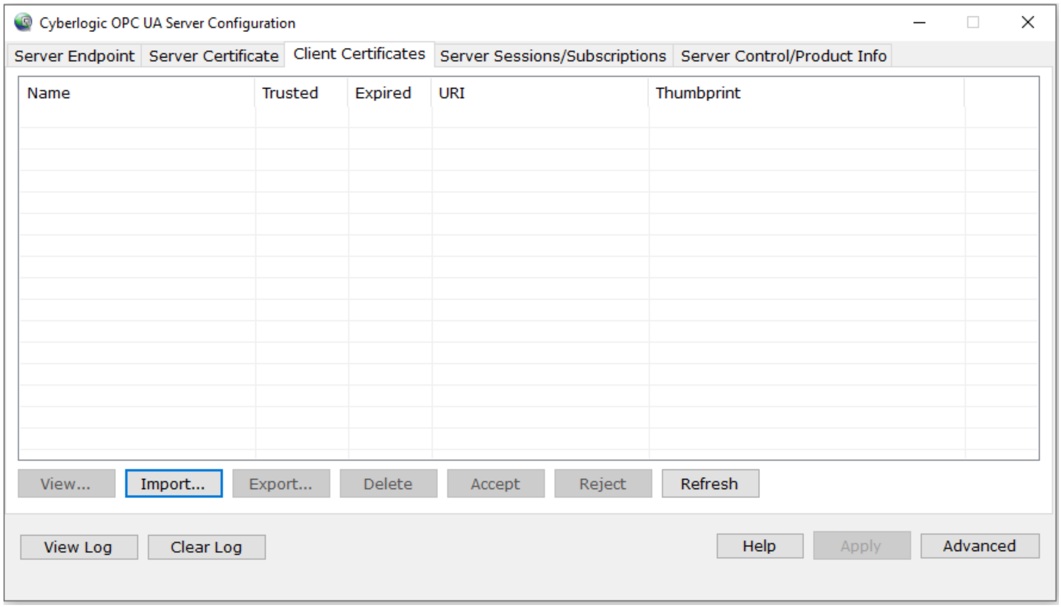
3. Click the ***Copy to the LDS*** button to copy the server's certificate to the Local Discovery Server certificate store. This will register the server with the LDS and make it easier for clients to connect to the server.

To continue, go to Client Certificates.

Client Certificates

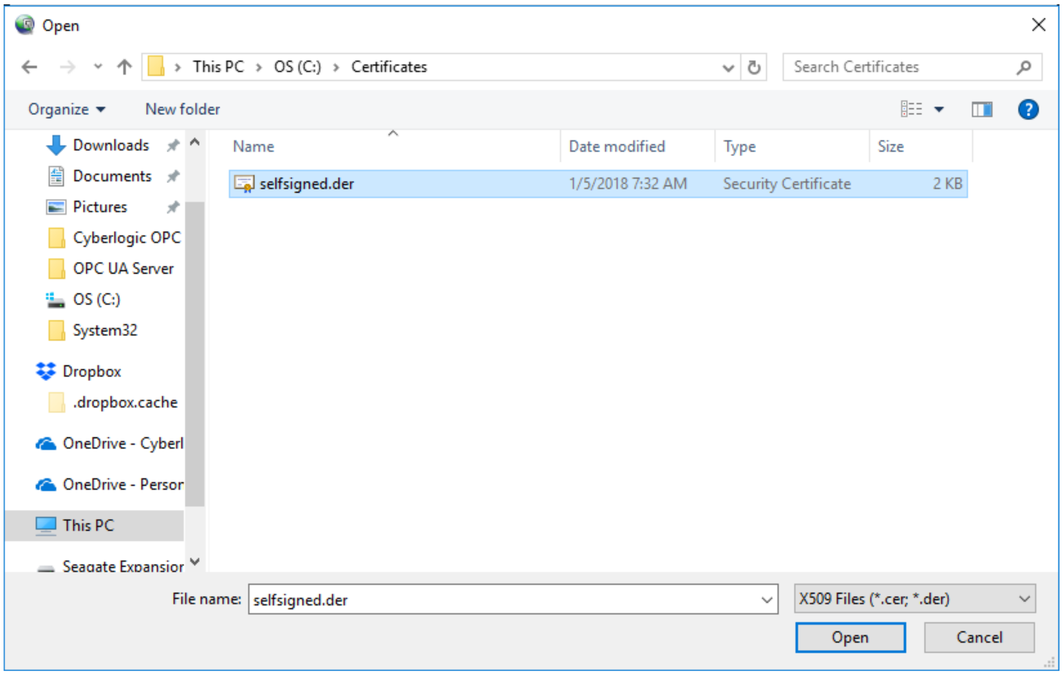
The server maintains a list of trusted certificates to identify both client applications (Application Instance Certificates) and users that have access to the UA Server. If the security and authentication policies that you configured require these types of certificates, you will need to add them to the ***Client Certificates*** list.

1. Select the ***Client Certificates*** tab.



Name	Trusted	Expired	URI	Thumbprint

2. If you have already tried connecting to the server, your client’s certificate may already be placed on the list (press the ***Refresh*** button to make sure that all new certificates are shown). However, initially, all newly added certificates are set as not trusted and need to be validated. If you see your certificate on the list, select it and press the ***Accept*** button, then continue to step 4. Otherwise, click the ***Import...*** button and browse to the client certificate you want to import. The certificate must be in either the SER or DER format.

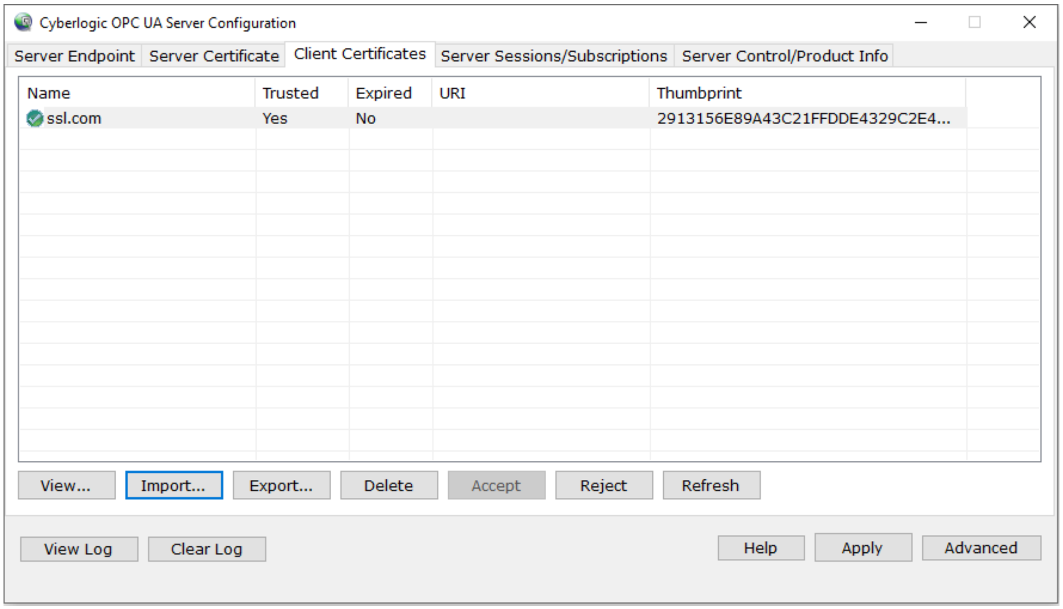


Name	Date modified	Type	Size
selfsigned.der	1/5/2018 7:32 AM	Security Certificate	2 KB

File name: selfsigned.der

X509 Files (*.cer; *.der)

3. Click ***Open*** to complete the import.



Name	Trusted	Expired	URI	Thumbprint
ssl.com	Yes	No		2913156E89A43C21FFDDE4329C2E4...

4. The certificate is now in the list of trusted client-side certificates. If you need to add more certificates to this list, go back to step 2.

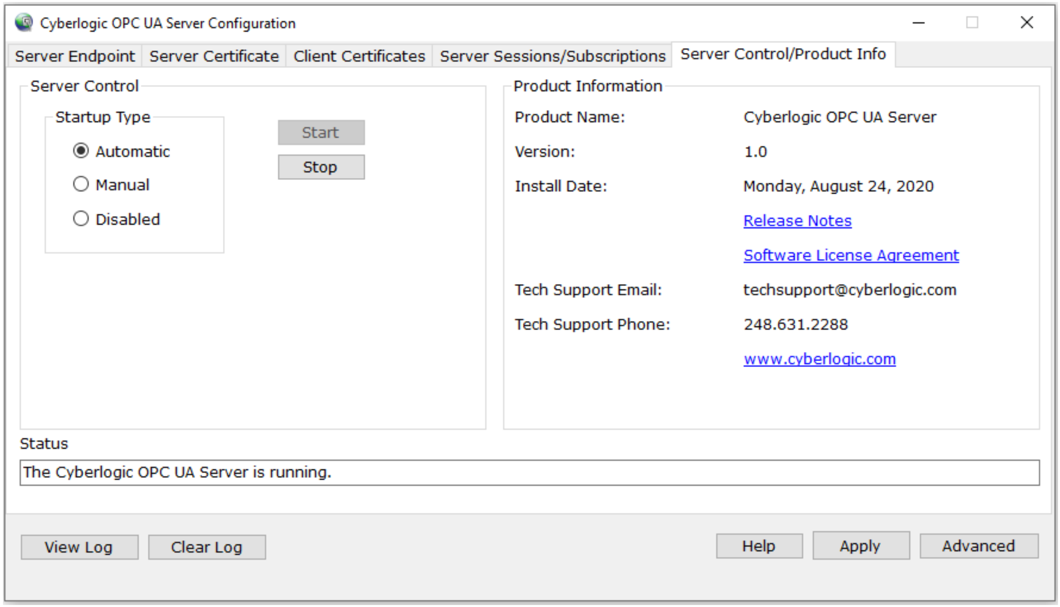
5. Click ***Apply*** to accept the changes.

To continue, go to Server Control.

Server Control

The ***Server Control/Product Info*** tab allows you to select the startup type and monitor the current server status. The server needs to be running before clients can connect to it. To always start the server when Windows boots up, we recommend the ***Automatic*** setting.

1. Select the ***Server Control/Product Info*** tab.



Server Control

Startup Type

● Automatic

○ Manual

○ Disabled

Product Information

Product Name:	Cyberlogic OPC UA Server
Version:	1.0
Install Date:	Monday, August 24, 2020
	Release Notes
	Software License Agreement
Tech Support Email:	techsupport@cyberlogic.com
Tech Support Phone:	248.631.2288
	www.cyberlogic.com

Status

The Cyberlogic OPC UA Server is running.

2. Select ***Automatic*** in the Startup Type.

3. Click the ***Start*** button to start the server.

The UA server is now ready for the OPC UA clients to connect.

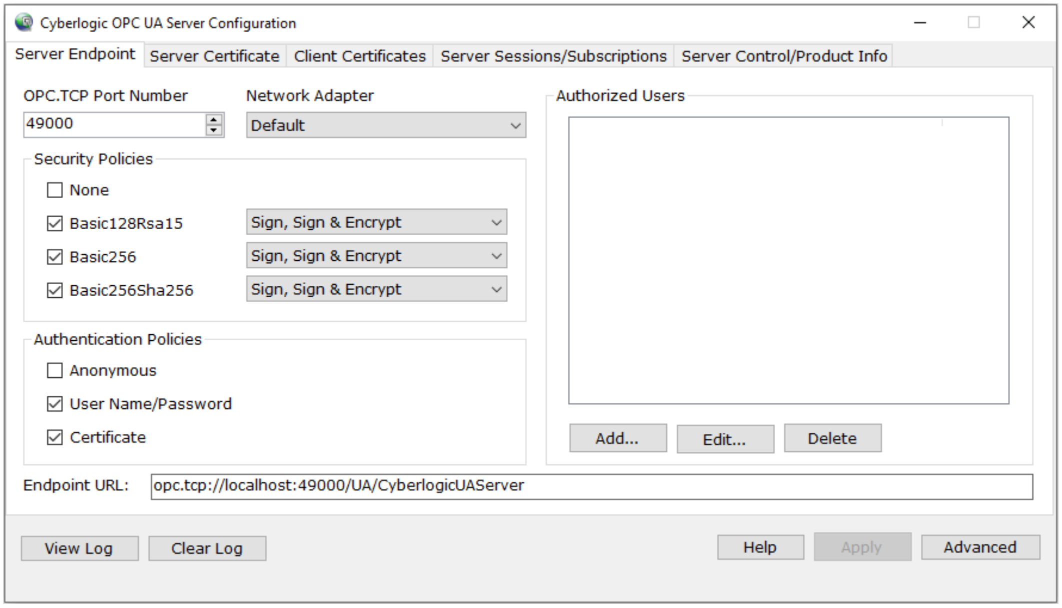
CONFIGURATION EDITOR REFERENCE

The Cyberlogic OPC UA Server Configuration editor allows you to configure the settings and monitor the status of the Cyberlogic OPC UA Server. The server is installed with the most common settings already set, but some manual configuration is still required.

Note Before configuring the Cyberlogic OPC UA Server, one of the Cyberlogic OPC Server products must be installed and configured.

This section provides a detailed description of each of the configuration editor features. If you are a new user and want a procedure to guide you through a typical configuration session, refer to the Quick-Start Guide.

To launch the editor from the Windows Start menu, go to ***Cyberlogic OPC UA Server*** submenu, then select ***Configuration & Status***.



Cyberlogic OPC UA Server Configuration

Server Endpoint | Server Certificate | Client Certificates | Server Sessions/Subscriptions | Server Control/Product Info

OPC.TCP Port Number: 49000

Network Adapter: Default

Security Policies

- ☐ None
- ☑ Basic128Rsa15 — Sign, Sign & Encrypt
- ☑ Basic256 — Sign, Sign & Encrypt
- ☑ Basic256Sha256 — Sign, Sign & Encrypt

Authentication Policies

- ☐ Anonymous
- ☑ User Name/Password
- ☑ Certificate

Authorized Users

Endpoint URL: opc.tcp://localhost:49000/UA/CyberlogicUAServer

The Cyberlogic OPC UA Server Configuration editor, shown above, will open. There are five buttons at the bottom:

View Log

Pressing this button displays the server's log file. This can be useful for troubleshooting. To configure the logging options, press the ***Advanced*** button and go to the ***OPC UA Server Log File Configuration*** section.

Clear Log

Pressing this button clears the server's log file.

Help

Based on the tab that you are on, pressing this button opens a context sensitive help file.

Apply

Any time you make configuration changes, pressing this button applies changes to the server.

Advanced

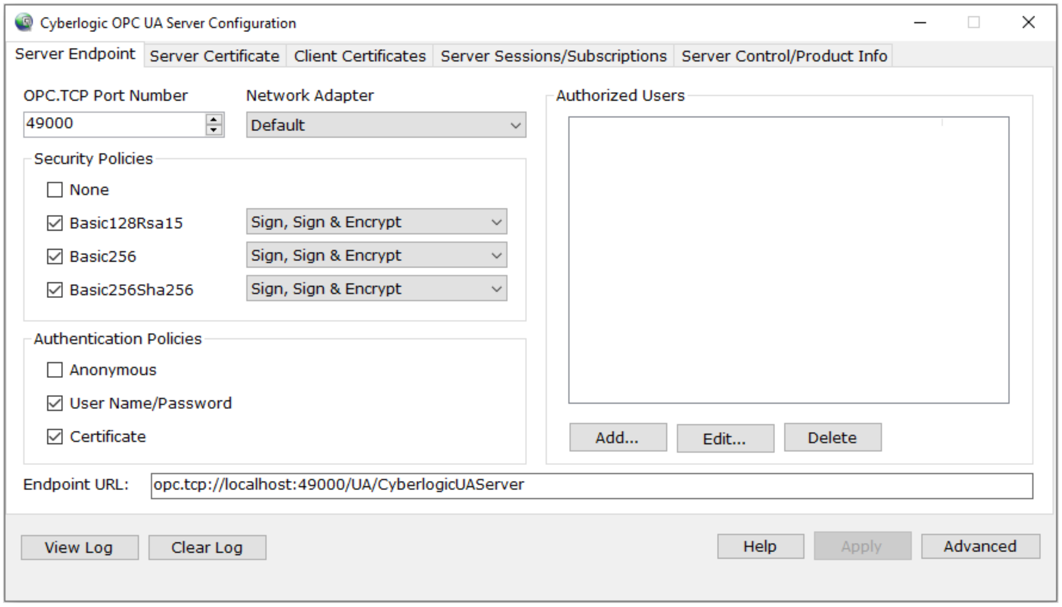
Pressing this button gives access to the advanced configuration settings. For more information, click here.

At the top of the editor there are five tabs that give you access to the various configuration settings:

- Server Endpoint Tab
- Server Certificate Tab
- Client Certificates Tab
- Server Sessions/Subscriptions Tab
- Server Control/Product Info Tab

The following sections provide complete descriptions of these tabs.

Server Endpoint Tab



OPC.TCP Port Number: 49000

Network Adapter: Default

Security Policies

☐ None

☑ Basic128Rsa15 — Sign, Sign & Encrypt

☑ Basic256 — Sign, Sign & Encrypt

☑ Basic256Sha256 — Sign, Sign & Encrypt

Authentication Policies

☐ Anonymous

☑ User Name/Password

☑ Certificate

Authorized Users

Endpoint URL: opc.tcp://localhost:49000/UA/CyberlogicUAServer

This tab defines the security and authentication policies that UA clients can use when connecting to the server. Notice the ***Endpoint URL*** shown at the bottom of this screen. This string may be required when configuring your OPC UA client application.

The Cyberlogic OPC UA Server supports the OPC UA binary protocol (opc.tcp). The binary protocol offers the best performance, least overhead, takes the least amount of resources, and offers the best interoperability. It uses a single arbitrarily selected TCP port for communication, which simplifies tunneling or passing through a firewall.

OPC.TCP Port Number

This is the port number that is required for the opc.tcp protocol. The default port number is 49000.

Network Adapter

This is the network adapter that will be used for the client connections. You can specify a network adapter with a specific IP address, limit the connections to the local host, or select the default network adapter. The default selection is ***Default***.

Security Policies

A security policy specifies which security mechanisms are to be used. The OPC UA Server announces which mechanisms it supports, and the UA Client selects one to use with the secure channel it wishes to open or for the session-less connection it wishes to make. A security policy determines the algorithms for signing, encryption, and key derivation.

Caution!

> The security policies, Basic128Rsa15 and Basic256, have been deprecated by the OPC Foundation as of OPC UA Specification, version 1.04. The encryption provided by these policies is not considered secure and usage should be limited to providing backward compatibility.

For most applications, it is recommended that the ***Basic256Sha256*** security policy is used. The security policy, ***None***, provides no security and should normally be disabled.

Each security policy supports the selection of several security modes: ***None***, ***Sign***, and ***SignAndEncrypt***. For high-security applications, ***SignAndEncrypt*** should be used. In some applications where data confidentiality is not required, ***Sign*** might be sufficient.

By default, ***Basic128Rsa15***, ***Basic256***, and ***Basic256Sha256*** policies are enabled, and each is set to ***Sign***, and ***SignAndEncrypt***.

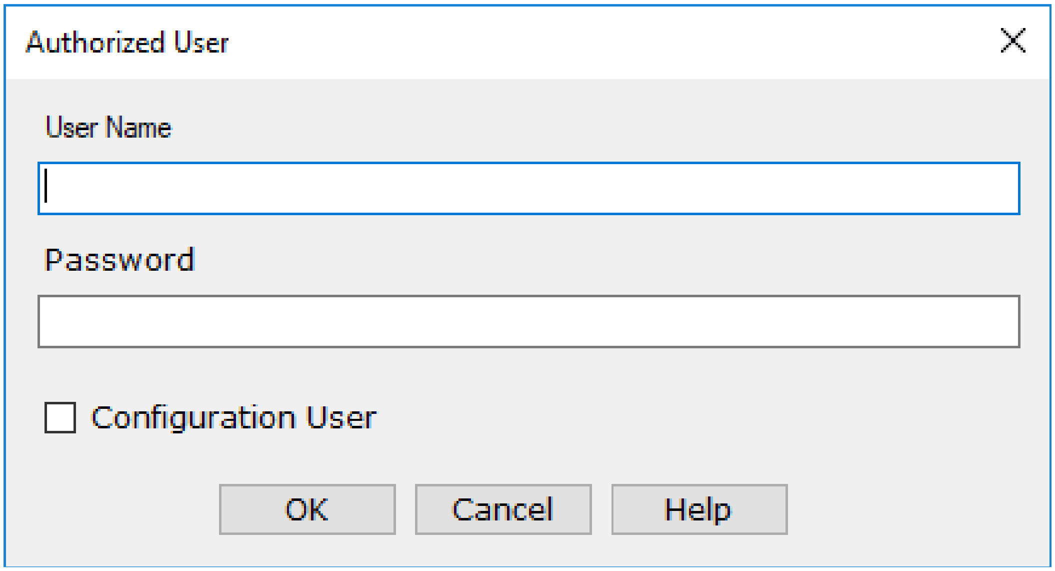
Authentication Policies

Authentication policies define the ways users are authenticated when UA clients connect to the server. Users can be authenticated by a username and password, or a digital certificate. Authentication can also be disabled by selecting, ***Anonymous***. When using a certificate for authentication, the certificate must also be trusted and placed on the Client Certificates list.

By default, ***User Name/Password*** and ***Certificate*** are enabled.

Authorized Users

OPC UA provides user authorization based on the authenticated users. The ***Authorized Users*** list defines the users that have access to the server when a username and password authentication is used. You can ***Add***, ***Edit***, and ***Delete*** users. When adding or editing users, the dialog below appears.



User Name

This is the username part of the username and password combination.

Password

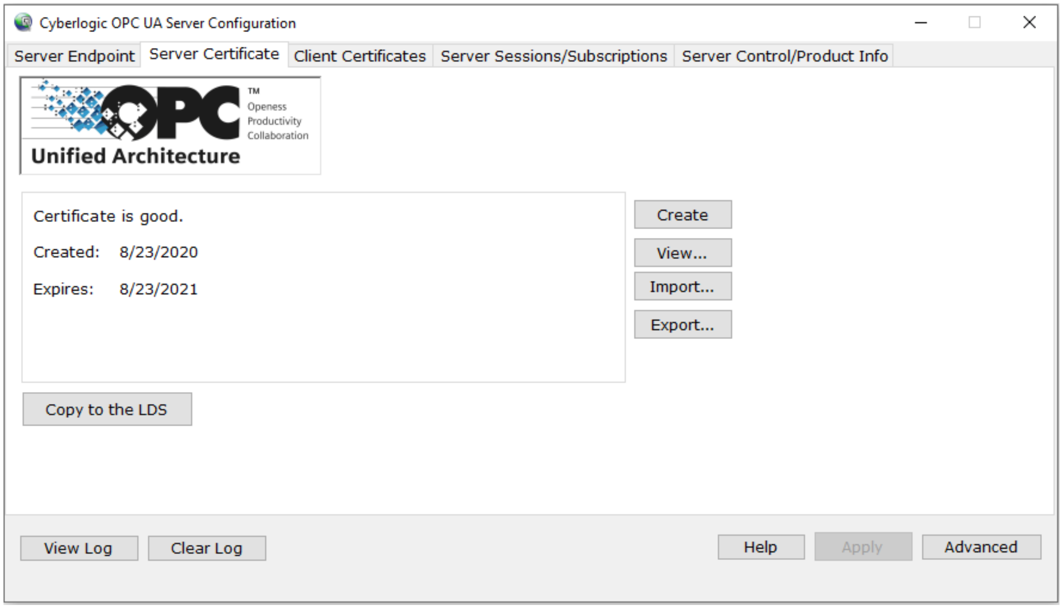
This is the password part of the username and password combination.

Configuration User

Configuration users have the rights to execute some of the OPC UA methods that expose the server configuration information. Select this checkbox only if this functionality is required.

Note When changes are made on this screen, the changes must be applied to the server by clicking ***Apply*** before they go into effect.

Server Certificate Tab



Certificate is good.

Created: 8/23/2020

Expires: 8/23/2021

The OPC UA server has a single Application Instance Certificate, which is used to identify itself to the client applications. It is also used for signing and/or encrypting messages. To simplify discovery of the server by UA Clients, this certificate is typically registered with the Local Discovery Server (LDS).

During the installation, a self-signed certificate is automatically generated and is valid for one year. On this tab, you can ***Create***, ***View***, ***Import***, and ***Export*** the server certificate.

Create

Click this button to create a new self-signed server certificate.

View

Click this button to view the current server certificate.

Import

Click this button to import a server certificate. This would typically be done to replace the self-signed certificate with a more secure, certification authority (CA) issued, certificate. The certificate must be in the PFX format.

Export

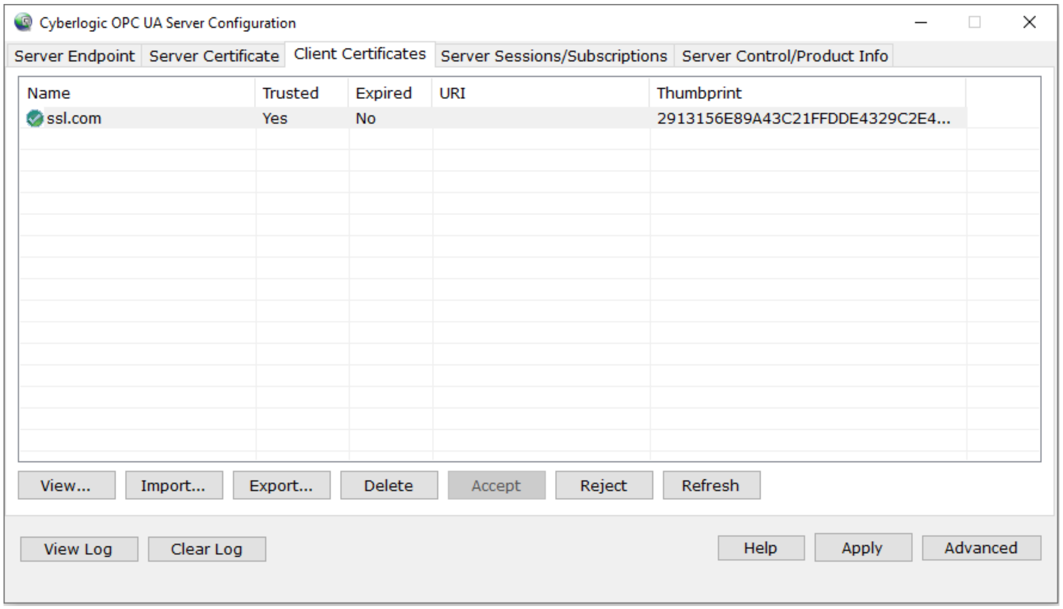
Click this button to export the server certificate as a DER file. Select this if you need to transfer the certificate to another system for a UA client to validate.

Copy to the LDS

Click this button to copy the server certificate to the Local Discovery Server (LDS) certificate store. This will register the server with the LDS and make it easier for clients to connect to the server.

Note When changes are made on this screen, the changes must be applied to the server by clicking ***Apply*** before they go into effect.

Client Certificates Tab



Name	Trusted	Expired	URI	Thumbprint
✓ ssl.com	Yes	No		2913156E89A43C21FFDDE4329C2E4...

Each OPC UA server has a list of Application Instance Certificates for each trusted client. These certificates are used when a security policy requires signed and/or encrypted messages. The Cyberlogic OPC UA Server also uses the same list to include certificates that are used for authenticating users.

The Client Certificates list is typically created by a system administrator. An administrator determines if the certificate is signed, validated and trustworthy before placing it in this list.

View...

Click this button to view the selected certificate.

Import...

Click this button to import a certificate to the list. You can import client certificates that are not automatically exchanged when connecting to the server. You may also need to import user certificates when using certificate authentication. The certificate must be in either the CER or DER format.

Export…

Click this button to export the selected certificate. Once exported, you can transfer the certificate to other systems.

Delete

Click this button to delete the selected certificate from the list.

Accept

Click this button to accept the selected certificate as trusted.

Client certificates that are automatically received during the first connection attempt to the server are not initially trusted. For the connect to be allowed, the certificate must be manually accepted as trusted.

Reject

Click this button to reject a previously accepted certificate.

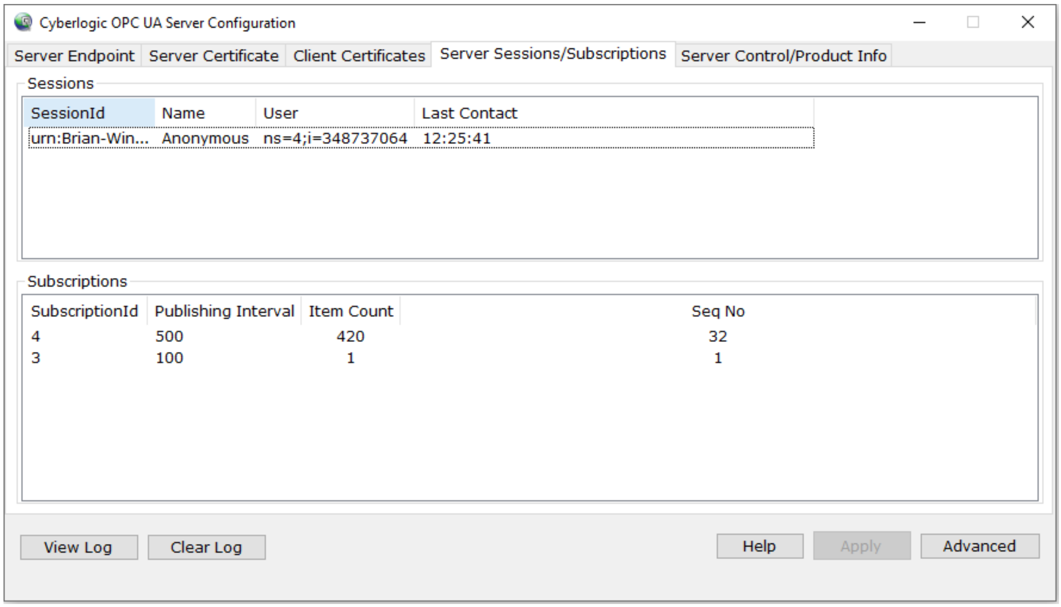
Refresh

Click this button to refresh the list of certificates.

When a client certificate is received during the first connection attempt to the server, it may not be shown until the list is refreshed.

Note When changes are made on this screen, the changes must be applied to the server by clicking ***Apply*** before they go into effect.

Server Sessions/Subscriptions Tab


Cyberlogic OPC UA Server Configuration
Server Endpoint
Server Certificate
Client Certificates
Server Sessions/Subscriptions
Server Control/Product Info
View Log
Clear Log
Help
Apply
Advanced

Sessions

SessionId	Name	User	Last Contact
urn:Brian-Win...	Anonymous	ns=4;i=348737064	12:25:41

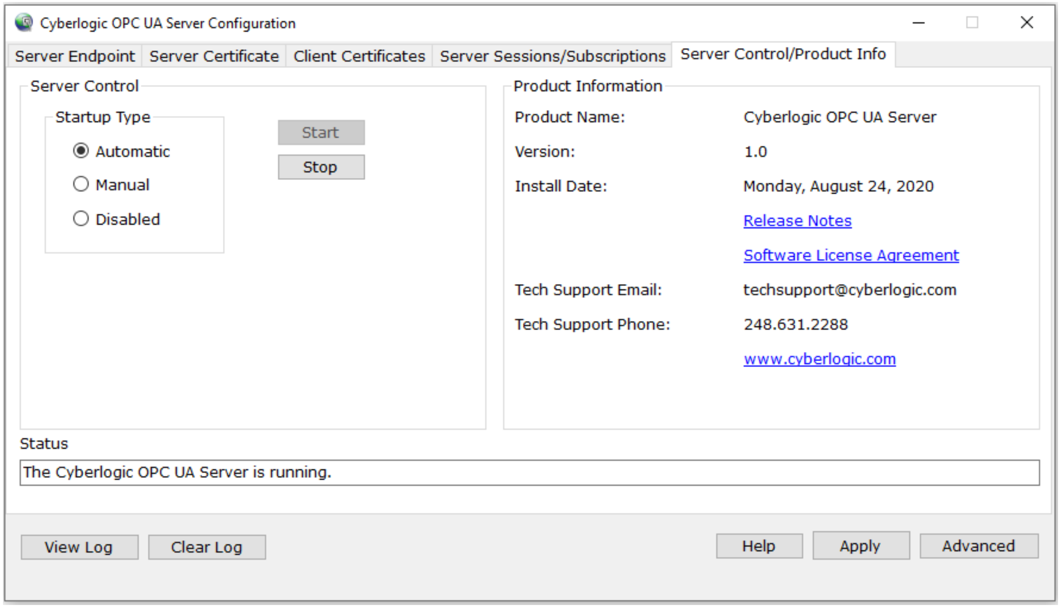
Subscriptions

SubscriptionId	Publishing Interval	Item Count	Seq No
4	500	420	32
3	100	1	1

When clients connect to the server, they create a session. Once the session is established, the clients can create subscriptions to obtain data from the server.

The Sessions area of this screen shows the currently active sessions and their last contact time. The Subscription area shows the details of the open subscriptions in the server.

Server Control/Product Info Tab



Server Control

Startup Type

● Automatic
○ Manual
○ Disabled

Product Information

Product Name:	Cyberlogic OPC UA Server
Version:	1.0
Install Date:	Monday, August 24, 2020
	Release Notes
	Software License Agreement
Tech Support Email:	techsupport@cyberlogic.com
Tech Support Phone:	248.631.2288
	www.cyberlogic.com

Status

The Cyberlogic OPC UA Server is running.

This screen is divided into two areas: Server Control and Product Information.

Server Control

This area of the screen allows you to select the startup type and monitor the current server status.

Automatic

When the option is selected, the UA Server will start when Windows boots up.

Manual

When this option is selected, the UA Server will not start when Windows boots up, but you can control it manually using the start and stop buttons.

Disabled

When the option is selected, the UA Server will not run.

Start

In Automatic or Manual mode, click this button to start the UA Server.

Stop

In Automatic or Manual mode, click this button to stop the UA Server.

Status

This tell you whether the UA Server is running, stopped, starting or stopping.

Selecting the Startup Type

Select the desired mode among the Startup Type choices.

If you want the UA Server to start whenever the system is booted, select ***Automatic.*** This is the recommend setting for systems that will use the UA Server.

If you want to use the UA Server and want to control it manually, choose ***Manual.*** The server will not start on boot-up; instead, you must use the ***Start*** and ***Stop*** buttons to control it.

If you do not want to use the UA Server, choose ***Disabled.***

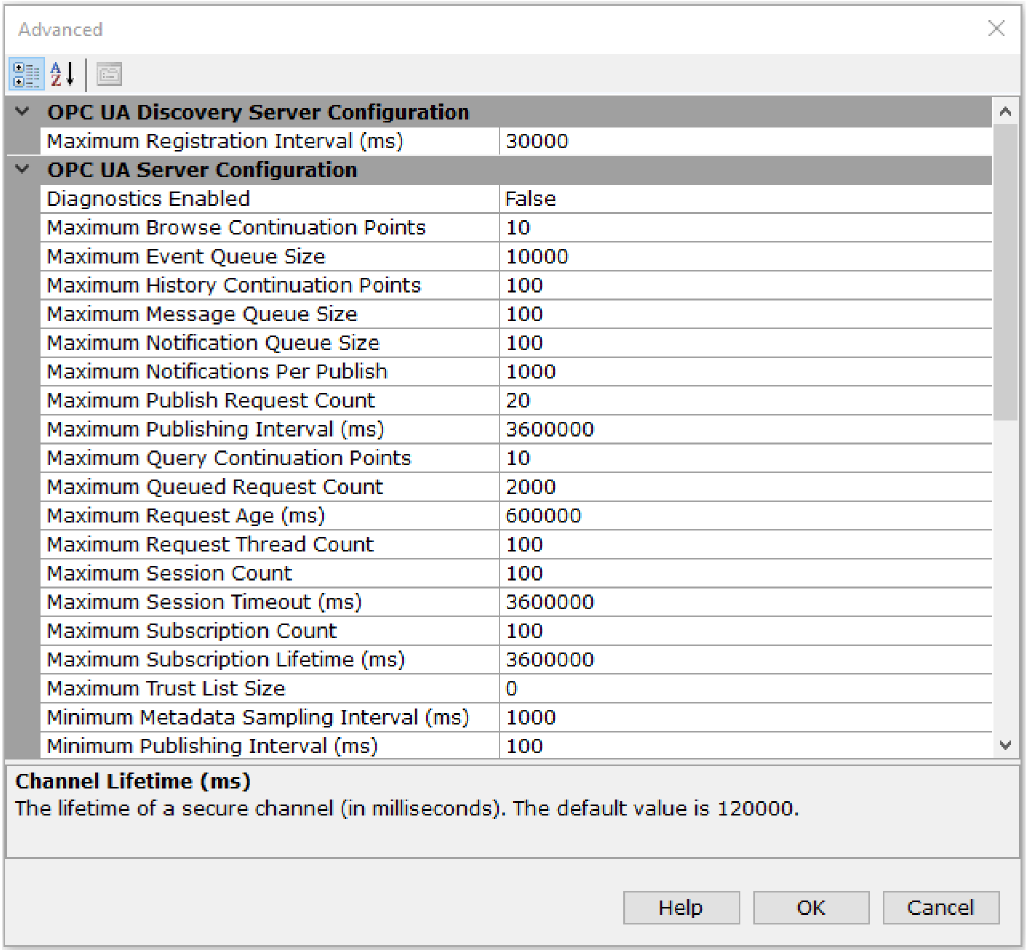
Start/Stop the UA Server

Click the ***Start*** or ***Stop*** button.

Product Information

This area of the screen shows the version number of the Cyberlogic OPC UA Server, the software installation time, and the Cyberlogic contact information. This may be helpful when calling for technical support.

Advanced Settings



OPC UA Discovery Server Configuration	
Maximum Registration Interval (ms)	30000
OPC UA Server Configuration	
Diagnostics Enabled	False
Maximum Browse Continuation Points	10
Maximum Event Queue Size	10000
Maximum History Continuation Points	100
Maximum Message Queue Size	100
Maximum Notification Queue Size	100
Maximum Notifications Per Publish	1000
Maximum Publish Request Count	20
Maximum Publishing Interval (ms)	3600000
Maximum Query Continuation Points	10
Maximum Queued Request Count	2000
Maximum Request Age (ms)	600000
Maximum Request Thread Count	100
Maximum Session Count	100
Maximum Session Timeout (ms)	3600000
Maximum Subscription Count	100
Maximum Subscription Lifetime (ms)	3600000
Maximum Trust List Size	0
Minimum Metadata Sampling Interval (ms)	1000
Minimum Publishing Interval (ms)	100

Channel Lifetime (ms)
The lifetime of a secure channel (in milliseconds). The default value is 120000.

This screen give you access to many advanced UA Server related settings. Most of them are set to the optimum values and do not need to be changed.

OPC UA Discovery Server Configuration

Maximum Registration Interval (ms)

The maximum time between registration attempts (in milliseconds). 0 means do not register. The default value is 30000.

OPC UA Server Configuration

Diagnostics Enabled

This sets whether diagnostics are enabled. If diagnostics are enabled some clients may be able to display this information. The default value is False.

Maximum Browse Continuation Points

The maximum number of continuation points used for Browse/BrowseNext operations. The default value is 10.

Maximum Event Queue Size

The maximum size of the event queue. The default value is 10000.

Maximum History Continuation Points

The maximum number of continuation points used for HistoryRead operations. The default value is 100.

Maximum Message Queue Size

The maximum number of messages saved in the queue for each subscription. The default is 100.

Maximum Notification Queue Size

The maximum number of notifications saved in the queue for each monitored item. The default value is 100.

Maximum notifications Per Publish

The maximum number of notifications per publish. The default value is 1000.

Maximum Publish Request Count

The maximum publish request count. The default value is 20.

Maximum Publishing Interval (ms)

The maximum publish interval supported by the server (in milliseconds). The default value is 3600000.

Maximum Query Continuation Points

The maximum number of continuation points used for Query/QueryNext operations. The default value is 10.

Maximum Queued Request Count

The maximum number of requests that will be queued waiting for a thread. The default value is 2000.

Maximum Request Age (ms)

The maximum age of an incoming request in milliseconds (old requests are rejected). The default value is 600000.

Maximum Request Thread Count

The maximum number of threads assigned to processing requests. The default value is 100.

Maximum Session Count

The maximum number of open sessions. The default value is 100.

Maximum Session Timeout (ms)

The maximum duration of time a session can remain open without communication from the client (in milliseconds). The default value is 3600000.

Maximum Subscription Count

The maximum subscription count. The default value is 100.

Maximum Subscription Lifetime (ms)

The maximum time the subscription will remain open without a publish from the client. The default value is 3600000.

Maximum Trust List Size

The maximum size of the trust list in bytes. 0 means unlimited. The default value is 0.

Minimum Metadata Sampling Interval (ms)

The minimum sampling interval for metadata. The default value is 1000.

Minimum Publishing Interval (ms)

The minimum publishing interval supported by the server (in milliseconds). The default value is 100.

Minimum Request Thread Count

The minimum number of threads assigned to processing requests. The default value is 5.

Minimum Session Timeout (ms)

The minimum amount of time a session can remain open without communication from the client (in milliseconds). The default value is 10000.

Minimum Subscription Lifetime (ms)

The minimum lifetime for a subscription (in milliseconds). The default value is 10000.

Multi Cast DNS Enabled

A boolean value used to identify whether the server announces itself using multicast DNS. The default value is False.

Publishing Resolution (ms)

The minimum difference between the supported publishing interval (in milliseconds). The default value is 50.

Shutdown Delay (sec)

The delay before shutdown (in seconds). The default value is 5.

OPC UA Server Security Policies

Reject SHA1 Signed Certificates

If True, the server will reject SHA1 signed certificates. The default value is True.

OPC UA Server Log File Configuration

Delete On Load

Deletes the log file when the server loads. The default is True.

Log Output File

The log output file path.

Log Output File Size (bytes)

The maximum size of the log file. Once the maximum size is reached, the current file is deleted, and a new empty file is created.

Log Settings

The type of values to log. The default value is ***Security, Errors and Trace***.

OPC UA Server Transport Quotas

Channel Lifetime (ms)

The lifetime of a secure channel (in milliseconds). The default value is 120000.

Maximum Array Length

The maximum length of an array encoded in a message body. The default value is 65535.

Maximum Byte String Length

The maximum length of a byte string encoded in a message body. The default value is 65535.

Maximum Message Size

The maximum length of a message body. The default value is 1048576.

Maximum String Length

The maximum length of a string encoded in a message body. The default value is 65535.

Operation Timeout (ms)

The default timeout to use when sending requests (in milliseconds). The default value is 60000.

Security Token Lifetime (ms)

The lifetime of a security token (in milliseconds). The default value is 3600000.

VALIDATION & TROUBLESHOOTING

The following sections describe how to validate that the Cyberlogic OPC UA Server has been configured correctly. If you are having difficulties communicating to the server, refer to the Frequently Asked Questions section for guidance.

OPC UA Demo Client

The easiest way to verify that the UA Server has been configured correctly is to try to connect to it using one of the many free demo OPC UA client applications. One of the most popular of them is the UaExpert from Unified Automation. Follow the link below to find more information on how to download and install this software. The included help file provides a free tutorial with step-by-step instructions on how to use it.

https://www.unified-automation.com/products/development-tools/uaexpert.html

Note Third-party products mentioned in this document are posted for informational purposes only. Cyberlogic is not affiliated with Unified Automation. Cyberlogic does not endorse, promote or warrant the operation of the UaExpert software, or any other products or services offered by Unified Automation, for any purpose or fitness. Other software with similar or equivalent features and functions may be available on the market.

Configuration Editor Diagnostics

The Cyberlogic OPC UA Server editor provides some built-in diagnostics. To monitor all active client sessions and subscriptions, refer to the Server Sessions/Subscriptions tab.

The server can also produce a log file with various error and trace messages. To view the content of this file, press the ***View Log*** button. To configure the logging options, press the ***Advanced*** button and go to the ***OPC UA Server Log File Configuration*** section.

Also, to make sure that the server is running, go to the Server Control/Product Info tab and check the server ***Status*** line.

Frequently Asked Questions

I've installed the software. What's next?

Before the Cyberlogic OPC UA Server can be used, it must be properly configured. The server is installed with the most common settings already set, but some manual configuration is still required. Refer to the Quick-Start Guide section for more help.

I'd like to add my UA client application's certificate to the trusted client certificates list. What do I need to do?

Select the Client Certificates tab in the editor. If you have already tried connecting to the server, your client's certificate may already be placed on the list (press the ***Refresh*** button to make sure that all new certificates are shown). However, initially, all newly added certificates are set as not trusted and need to be validated. If you see your certificate on the list, select it and press the ***Accept*** button.

You can also add your client's certificate offline by importing it. Click the ***Import*** button and browse to the certificate you want to import. The certificate must be in either the SER or DER format.

The server is not registering with the Local Discovery Server. What do I need to do?

Make sure the server certificate is copied to the local discovery server directory by clicking the ***Copy to the LDS*** button on the Server Certificate tab.

I have been running for over a year and my client can no longer connect to the OPC UA Server. What do I need to check?

Check the Server Certificate tab and see if the certificate expired. The original certificate that is created after the installation is only good for one year. If it has expired, click the ***Create*** button to create a new one. You may also have to copy it to your clients allowed list.

I want to temporarily block a client from connecting without deleting the client certificate from my system. What do I need to do?

Select the Client Certificates tab in the editor. Find the client certificate in the list and select it. Click the ***Reject*** button and then ***Apply*** to accept the change. The server will now reject connections from the client. To reenable connections from the client, select the certificate and click the ***Accept*** button and then ***Apply*** to accept the change.

How are the NodeId's created for tags in the OPC UA Server?

A *NodeId* is composed of three elements that identify a *Node* within a UA server, the *NamespaceIndex*, *IdentifierType*, and *Identifier*. It has the form of *NamespaceIndex*;*IdnetifierType*;*Identifier*. For the Cyberlogic OPC UA Server, the *NamespaceIndex* is always 2, and the *IdentifierType* is always *String*. The *Identifier* is the *ItemID* of a tag inside the Cyberlogic OPC DA server. For example, an *ItemID* of ***NewDevice.Simple_Types.TestValue6_INT*** would have a corresponding *NodeId* of ***ns=2;s=0:NewDevice.Simple_Types.TestValue6_INT***.