OPC-UA Tutorial

A Guide to Configuring the TOP Server for OPC-UA
Setting up the Server
  Setting up the Endpoints

Setting Up the Client
  Verification

APPENDIX

Discovery Service (Optional)

Firewall

CONTACT US
Introduction

Introduction to OPC UA

The OPC Unified Architecture, also known as OPC-UA, is the latest open-standard architecture developed by the OPC Foundation to improve and expand interoperability standards in the Industrial Automation Industry.

Why do we need a new architecture to begin with? OPC-UA was the result of several advancements and changes in the way data was commonly being accessed and exchanged. Some changes that lead to the need for a new architecture include:

- Microsoft’s COM and DCOM (the basis for previous standards) were deprecated and are now considered legacy technologies
- Web services gained importance in data exchange between machines and for communications to factory floor devices
- Earlier specifications were decoupled and did not integrate well, e.g. items in a Data Access server could not communicate directly with items in an Alarms and Events server.

OPC-UA is designed for exchanging information in an object-oriented manner, rather than as isolated data points. This increases the accessibility of your plant floor data by letting you re-use information stored in a common object. OPC-UA also incorporates a service-oriented model, which increases interoperability with other platforms and improves security.

OPC-UA is not a replacement for existing OPC-DA standards. Because of the layered design of this architecture, it includes all the functionality of existing OPC-DA servers, but expands upon their functionality with a common interoperability layer. This interoperability layer unifies information exchange and provides a common interface for controlling processes.

What are the benefits of the new architecture? OPC-UA provides a way to connect clients and servers in a secure manner, without relying on Microsoft DCOM. This is a big advantage because it means that you are no longer saddled with the headaches associated with having to configure DCOM. This is because DCOM plays no role in data transport. OPC-UA can also allow users to make secure connections through
firewalls and over VPN connections. In addition, it expands the ability to provide factory floor information to other business systems, as a result of the object-oriented model described above.

**Introduction to TOP Server**

The TOP Server is an OPC-UA server, but it also supports other interfaces such as OPC DA, SuiteLink/FastDDE, DDE and PDB. The purpose of the server is to establish a connection with a device to access information in the device’s memory space. It can then serve this data up to a client application.

The TOP Server functions as an OPC-UA server but it also has the ability to function as an OPC-UA client, by using the OPC UA Client driver, which will be demonstrated in this paper.

**Intended Audience**

This paper is intended for general audiences, including process control engineers and systems integrators, who are interested in learning more about utilizing the OPC-UA Server and Client capabilities of the TOP Server. This tutorial will show you how to configure the TOP Server to allow an OPC UA client to connect to it. It will also demonstrate how to configure a secure OPC UA tunnel between two TOP Server machines.
Prerequisites

For the first part of this document, it will be necessary to have the TOP Server installed on your machine.

In order to successfully configure the OPC UA Tunnel demonstrated in the third section of the document, the TOP Server must be installed on both the server and the client machines. When installing the TOP Server on the client machine, make sure that you elect to install the OPC UA Client Driver.

![TOP Server Installation](image)

**Figure 1: TOP Server Installation**
Configuring the TOP Server for Client Connections

General Project Settings

This section will discuss the general project properties that can be configured in the TOP Server. You can access these property settings by going to File | Project Properties in the TOP Server user interface and then clicking on the OPC UA tab. Let us take a look at some of the categories and discuss what these properties mean.

Server Interface

- **Enable**: The UA server interface must be enabled in order to accept client connections. If this setting is disabled, then the rest of the properties will also be disabled.

- **Log Diagnostics**: If this setting is enabled, then the OPC UA stack diagnostics will be shown in the Event Log. You only want to enable this setting if you are debugging your configuration.

Client Sessions

- **Allow Anonymous Login**: By default, this setting is enabled, which means that any OPC UA client will be able to connect. By disabling this parameter a username and password will be required to establish a connection. This username and password corresponds to the users set up in the TOP Server User Manager. You can simply use the default Administrator username and password if you do not have any other user specifically set up. You can find more information on the User Manager and the security settings on the TOP Server website.


- **Max Connections**: This sets the maximum number of client connections that can be made to the TOP Server. This value can range from 1 to 100. The default is 100 connections.

- **Session Timeouts**: This parameter is the amount of time a UA Client has to make a connection to the TOP Server before it times out. This is set as a range of values. The default minimum timeout is 15 seconds and the maximum is 60 seconds. The minimum accepted value is 5 seconds.
Browsing

- **Return Tag Properties**: This parameter allows a UA Client to browse the tag properties for each tag. By default, this property is not enabled.

- **Return Address Hints**: If this parameter is enabled, the UA client applications can browse the address formatting hints available for each item. This setting is disabled by default.

  **Note**: Unless you have a very good reason for enabling this, it should remain disabled, because some UA clients may try to add these hints to the tag database. This will result in an error from the server.

**OPC UA Configuration Manager**

This utility is essential to being able to successfully establish connections between your OPC UA client and the TOP Server. We will take a look at several properties in this utility that you may need to configure to communicate with your OPC UA client.

**Server Endpoints**

With the OPC-DA Specification, servers were identified by their ProgID. In OPC-UA, this is done through what is called a discovery endpoint, which more closely resembles a URL than the OPC-DA ProgIDs. This discovery endpoint uses a location and a port number to discover information about existing servers. The server will then return all the configured endpoints, and their security requirements, that are available to the client. Any one particular server can have multiple server endpoint definitions. You may want to define multiple endpoints if you want certain clients to connect on certain ports, or if you want some clients to only be able to connect locally, and some to be able to connect remotely.

All endpoints within a particular server will share the same instance certificate. An instance certificate (which will be discussed in more detail below) is a security certificate that grants permissions to clients to be able to connect to the server. This means that user validation is done on a per server instance basis, not per endpoint. Therefore, a client that has the server’s instance certificate will be able to connect to any endpoint configured in the server, provided that the client supports the type of encryption that the endpoint employs.
Any users you wish to have validated must be configured in the User Manager utility. You can access the User Manager by right-clicking on the Administration icon in the System Tray and then selecting User Manager. The server certificate will be discussed in more detail in the section on Instance Certificates.

A default server endpoint is automatically created in the TOP Server during the installation. All endpoints are enabled by default. You can disable them by un-checking the Enabled checkbox. You can configure an endpoint as described below.

1. Launch the **OPC UA Configuration Manager** by right-clicking on the Administration icon in the System Tray. Select **OPC UA Configuration** [Figure 2]. You can also start the Configuration Manager by going to **Start | All Programs | Software Toolbox | TOP Server 5 | OPC UA Configuration** [Figure 3].

   ![Figure 2: Configuration from Administration Icon](image-url)
2. On the **Server Endpoints** tab select the default endpoint that was created for you and click **Edit**.

3. At this point, you can modify the **Security Policies** settings if necessary. Since these settings are on the server side, any configured endpoint will allow all client connections with enabled policies. This means that, by default, only secure connections using signing and encryption (Basic126Rsa and/or Basic256) will be allowed. You can also select the type of encryption that the endpoint will support. If you do not care to implement the security, you can simply select “None”. If you are not using security certificates, you will want to disable the security policies completely (by unchecking the Basic128Rsa15 and Basic256 boxes).
You can also set the Network Adapter and the Port Number at this time. As mentioned above, there may be instances when you want clients to connect on a particular point, or you want clients to only be able to connect locally. These changes can be made here. The default Network Adapter is Default, and the default port is 49380. Click OK to save the configuration [Figure 5].

![Figure 5: Endpoint Definition](image)

4. To enable the endpoint, select it in the list and verify that the Enabled box is checked.
5. The Runtime service must be re-started in order for the changes to take effect. You can do this by right-clicking on the Administration Icon and selecting Stop Runtime Service, and then select Start Runtime.

**Instance Certificates**

Each application that wants to establish a trust with the OPC-UA server or client must have the appropriate public and private keys. The private key is protected, while the public key is placed into a certificate of distribution, called the Instance Certificate. Establishing a secure connection requires the client to have the server’s certificate, and the server to have the client’s certificate. This exchange is only required once for the duration of the certificate’s lifetime. The expiration date of the certificate is set by the issuer. You can determine the expiration date by selecting the certificate in your Trusted Clients tab in the OPC UA Configuration Manager, and select View Certificate.

In order for an OPC UA client to be able to connect to the TOP Server, you will need to export the Server Certificate and transfer it to your client.

1. Launch the **OPC UA Configuration Manager** on the server computer by right-clicking on the Administration icon in the System Tray. Select OPC UA Configuration. If the Administration Icon
in not running, you can start this service by going to Start | All Programs | Software Toolbox | TOP Server 5 | TOP Server 5- Administration. You could also launch the Configuration Manager directly from the start menu.

2. On the Instance Certificates tab, click Export Server Certificate under the Server group. Save the certificate to a location that can be easily accessed.

![Figure 7: Export Server Certificate](image)

3. Manually copy the server certificate file from the server computer to the client computer. You can do this by using a removable media device, or copy the certificate to a network drive that can be accessed by the client computer.

**Trusted Clients**

Just as the server generates its own Instance Certificate, the OPC UA client will also have a security certificate that is uploaded to the TOP Server. This can be done under the Trusted Clients tab in the OPC UA Configuration Manager. Simply click on the Import button, and browse to the location where you saved the Client Instance Certificate.

1. On the server computer, launch the OPC UA Configuration Manager.

2. On the Trusted Clients tab, click Import.
3. Browse to the client certificate and click Open. You should now see this certificate in the Trusted Clients window.
Configuring the TOP Server as an OPC UA Client

The TOP Server OPC UA Client driver will allow the TOP Server to act as an OPC UA Client to another OPC UA server.

Setting up a Channel

You can use the TOP Server Channel Wizard to locate and identify an OPC UA server and make any configuration changes necessary. Generally, the default selections are acceptable for most applications.

1. Launch the Configuration by right clicking on the Administration icon in the System tray and selecting Configuration, or by double clicking on the icon. You can also start the configuration by going to Start | All Programs | Software Toolbox | TOP Server 5 | TOP Server 5 – Configuration.

![Figure 10: Launch TOP Server Configuration](image)

2. Create a new project by going to File | New or clicking on the icon.

3. You can start the Channel Wizard by selecting Edit | Devices | New Channel or by clicking on the Click to add a Channel link as shown in the figure below.
4. Type a name for the OPC UA client channel in the **Channel name** field. The channel name for this demonstration will be OPC UA Client. If you do not specify a name, TOP Server will create one for you. Click **Next**.

5. In the **Device Driver** drop-down, select **OPC UA Client** and click **Next**.
6. In the **Write Optimization** window, selecting **Write all values for all tags** as the Optimization Method will add all write requests to the internal Write queue and then write all of the points out to the device as quickly as possible.

Selecting **Write only latest value for non-boolean** tags will only write out the value of the last write request that was received. This will apply to all non-boolean tags. Selecting **Write only latest value for all tags** will write the last received value, including Booleans. This is the default setting. The Duty Cycle determines the number of write operations that are performed per read. The default value is 10, which means that 10 write requests will be performed for every single read request that is processed.

You can use the default settings for the **Optimization Method** and **Duty Cycle** in the **Write Optimization** window. Click **Next**
7. In **UA Server** window, manually enter the server’s endpoint URL into the **Endpoint URL** field. Make sure the Security Policy and Message Mode settings match what you set up when configuring the security in Step 3 of topic **Server Endpoints** above.

![Figure 14: Enter Endpoint URL](image)

8. You could also browse for the URL by clicking on the **Browse** icon to the right. This will allow you to browse to other TOP Servers, with which you have exchanged certificates, on the network. If
you do have a Discovery Service, see the section called Discovery Service in the Appendix for more information on how to browse with this feature.

**Note:** When browsing for other TOP Servers, verify that the Use Discovery URL checkbox is disabled. When this checkbox is disabled the tree view will be populated with nodes on the network. When enabled, it will show UA servers found through the discovery URL.

**Note:** In order for the TOP Server UA client to browse to a remote TOP Server UA server, the remote server must have a server endpoint set up, specifying either the default network adapter, or a specific network adapter. If you only have a server endpoint set up for LocalHost as the adapter, your UA client will not be able to find the UA server.

9. You can use all of the default settings in UA Session window. The **Timeout on connect in** parameter specifies the maximum amount of time the channel will wait to connect to the UA server after making a connect call. The default is 30 seconds. The **Timeout inactive session in** parameter sets the maximum number of minutes that a session will remain open without activity. The default is 20 minutes. The **Channel is renewed every** property establishes how long the TOP Server will wait between channel renewals. The default is 60 minutes. The **Retry failed connect every** parameter specifies how often the channel will attempt to reconnect if the connection fails. The default is 5 seconds. Click **Next**.
10. If you left the OPC UA settings at the default in the Project properties you can keep the username and password blank in the Authentication Window and click Next. If you made changes to the Allow Anonymous Login, the username and password will need to match what is defined in the User Manager as described above. More information can also be found here: http://www.toolboxopc.com/html/security.html. Click Next.

11. View the Summary to ensure that all settings are correctly configured and click Finish.
Setting Up a Device

The TOP Server Device Wizard will guide you through setting up a subscription. It also provides a way to browse and import items from the OPC UA Server. All the items in the device will update according to the settings provided. Multiple devices can be added to the same channel in order to allow for different update intervals and modes.

1. Select the new channel you just created and click Edit | Devices | New Device. You can also click on the Click to add a device link that appeared after you completed your channel set-up.
2. Type a name for the client device in the **Device Name** field and click **Next**. We have called the Device TOP Server, since we will be connecting to another TOP Server running as a UA server.

![New Device - Name](image)

**Figure 18: Device Name**

3. You can use the default settings for next several configuration Windows, including **Subscription**, **Connection**, **Communications Parameters**, **Monitored Items**, and **Deadband**. You can accept the defaults on all of these windows by clicking **Next**.

4. On the Import screen, click **Select import items**. You will see a list of the server’s available items populated in the browsing window. If you do not see the items, your security settings may not be configured correctly.

**Note:** Security policies need to match on the client and server, and certificates need to be exchanged if they are being used.
5. Select the desired items and click **Add Items** or **Add Branch** to import them into the client. When all the items have been imported, click **OK** and then click **Next**.

6. View the Summary to ensure that all settings are correctly configured and click **Finish**.
Figure 21: Device Summary
Configuring the TOP Server for Tunneling

This section will cover how to create a secure tunnel between remote TOP Server machines. We will make use of some of the topics we have already discussed above. The TOP Server has some special features that make connecting from a TOP Server UA Client to a TOP Server UA Server easier, such as automated exchange of the certificates, and the ability to browse to the TOP Server UA Server without needing a Discovery Service.

Security

Tunneling security is set through the exchange of Instance Certificates. This exchange can be done automatically, or manually.

It is important to note, that although the OPC-UA specifications require applications to support the security certificates, it is by no means necessary that you implement this feature. If you are not concerned with the security certificates, you can deactivate this validation when defining the server endpoints by setting the security to “None” as was discussed in the section on setting up the Server Interface.

Automated Exchange of Instance Certificates

When connecting a TOP Server UA Server to a TOP Server UA Client, it is not necessary to manually perform the certificate exchange. This process can be handled automatically, as described below. This makes establishing a secure tunnel between TOP Servers simple and quick. The following conditions are required in order for the Exchange feature to work:

- The UA server must be installed on the remote node.
- Remote connections to the UA server Runtime must be enabled.
- The server Runtime application must be running on the remote node.
- The settings on the local exchange property window must be correct.
- The user must have a working network connection to the remote node.
- There may not be any firewalls blocking either node.
1. Right-click on the **Administration** icon (Figure 22) in the System Tray. Select **Settings** and then select the **Configuration** tab. If the Administration Icon is not running, you can start this service by going to **Start | All Programs | Software Toolbox | TOP Server 5 | TOP Server 5 – Administration**.

![Figure 22: Administration Icon](image)

2. To enable the remote configuration check **Allow runtime to accept remote connections**. This is unchecked by default. Click **Apply**.

![Figure 23: Administration from Start Menu](image)
Figure 24: TOP Server Settings

**Note:** The configuration interface must be shut down in order for the changes to be applied.

3. Add an exception to the Windows firewall for the port that is specified in the *Communicate using port* field. Information on how to add an exception can be found in this document in the topic called *Firewall* in the Appendix.

**Note:** You could also temporarily turn off the Windows firewall before doing the exchange and then turn it back on once the exchange is complete. Since this method does not require opening a port, it can help prevent unauthorized users from exchanging certificates in the future.

4. On the TOP Server machine that we want to set up as the client, right click on the *Administration* icon in the System Tray and select *OPC UA Configuration*. You can also open the configuration by going to *Start | All Programs | Software Toolbox | TOP Server 5 | OPC UA Configuration*. 
5. On the **Trusted Servers** tab, click on the **Exchange** button.

**Note:** Be aware that this function is only for acquiring the instance certificate for a remote TOP Server for the UA tunnel. This will not allow you to automatically import certificates for other UA servers.

6. In the Specify Server Instance dialog, enter the machine name where the server is located in the **Remote Host** field. You can also click on the **Browse** Icon, as shown in the screenshot below.
Figure 27: Browse for Remote Server

7. Browse to the server and select the computer name. Click OK. Verify that the correct port is identified in the Remote Port field. This is the port that is used for the server’s remote configuration. This value should match what is on the server computer. Click OK. You will receive a message confirming that the exchange was successful. You can confirm the exchange by looking at the Trusted Servers window.

Figure 28: Successful Certificate Exchange

Figure 29: Trusted Servers
8. On the TOP Server machine that you have designated to act as the OPC UA server, launch the **OPC UA Configuration Manager** from the Administration Icon or from the Start menu. You should see the client certificate in the **Trusted Clients** window.

![Figure 30: Trusted Clients](image)

**Manual Exchange**

1. Launch the **OPC UA Configuration Manager** on the TOP Server machine acting as a UA server by right-clicking on the **Administration** icon in the System Tray. Select **OPC UA Configuration**. You can also open the Configuration Manager by going to **Start | All Programs | Software Toolbox | TOP Server 5 | OPC UA Configuration**.

2. On the **Instance Certificates** tab click **Export Server Certificate** under the Server group. Save the certificate to a location that can be easily accessed.

**Note:** If you disabled your firewall, do not forget to enable it again now.
3. Manually copy the server certificate file from the server computer to the client computer. You can do this by using a removable media device, or copy the certificate to a network drive that can be accessed by the client computer.

4. On your designated TOP Server UA Client machine, launch the **OPC UA Configuration Manager**.

5. Select the **Trusted Servers** tab and click **Import**.

**Figure 31: Export Server Certificate**
6. Browse to the server certificate and click **Open**. You should then see the server certificate in the **Trusted Servers** window.

7. On the **Instance Certificates** tab, select **Export Client Driver Certificate** under the Client Driver group. Save the file to a location that is easily accessible.
8. Copy the client certificate from the client computer to the server computer. You can do this by using a removable media device, or copy the certificate to a network drive that can be accessed by the server computer.

9. On the TOP Server OPC UA server computer, launch the **OPC UA Configuration Manager**.

10. On the **Trusted Clients** tab, click **Import**.
11. Browse to the client certificate and click **Open**. You should now see this certificate in the **Trusted Clients** window.

**Setting up the Server**

**Setting up the Endpoints**

On the TOP Server machine that we have designated to act as the UA server, we now need to set up the server endpoint. Refer to the section **Server Endpoints** above for instructions.

**Setting Up the Client**

For more information on how to configure the TOP Server on the client machine, refer to the section called **Configuring the TOP Server as an OPC UA Client** in this document.

**Verification**

The items you just added in the OPC UA Client can now be browsed by an OPC DA client. You can verify the configuration by the following:
1. Launch the OPC QuickClient by selecting **Tools | Launch OPC Quick Client** or clicking on the QuickClient icon in the menu bar. A connection will be established to the local OPC UA server and the items will populate the view.

![Quick Client Icon](image)

**Figure 35: Quick Client Icon**

2. Browse for the items in the OPC UA Channel. Verify that the data’s quality is good and that the values are being updated.

![UA data with Quick Client](image)

**Figure 36: Displaying UA data with Quick Client**
Appendix

Discovery Service (Optional)

The intent of the Discovery Service is to allow your OPC UA Client to browse the PC with an OPC UA Server and discover its Server Endpoint.

If you have a Discovery Service, the TOP Server supports the registration and certificate exchange with this Service. At the time of this writing, the OPC UA specifications for the Discovery Service are not complete. Based on the current specification drafts it would be expected that the Discovery Service would be installed on the same PC as the TOP Server. The TOP Server does not supply this Discovery Service.

NOTE: When using the TOP Server OPC UA Client driver to connect to a TOP Server UA Server you can browse for the Server endpoints without the need for this discovery service.

The following instructions are only to be used if you have an available Local Discovery Service (LDS).

1. In the Discovery Port parameter, enter the endpoint port number that was created on the server computer. The default port number should already be assigned and agree with the default endpoint.

   Note: Port 4840 will always be scanned by the browser. If the port number was changed, click Refresh.

2. Browse to the network computer where the server is installed. Endpoints that are assigned to "localhost" will only be found under the Local Machine branch.

3. Expand the computer to display a list of available servers. Then, expand the servers and select the correct endpoint.
4. To continue to use this endpoint to discover UA servers, enable the **Use Discovery URL** in the Discovery parameter at the top of the dialog. This is a global change and will affect all other UA Client Drivers.

5. Click **OK**. The endpoint information will appear in the UA Server Window. Browsing to the URL will auto-fill the Security Policy and Message Mode fields. Click **Next**

**Firewall**

The purpose of the firewall is to block incoming traffic that is unsolicited or traffic that does not correspond to the exceptions that are set in the firewall. With OPC-UA, only the server computer requires a firewall exception, since OPC-UA does not require callbacks.

You can add an exception to the firewall on your server machine by following these steps:

1. Launch the **Windows Firewall** configuration by selecting **Start** | **Run** and then typing `firewall.cpl` or by browsing on your machine to **Start** | **Control Panel** | **Windows Firewall**.
Note: If you are using Vista or Server 2008 the Settings will not be directly displayed in this dialog box. You can access these settings by clicking on **Change Settings**.

2. Under the **General Tab**, verify that the firewall is enabled (the On button is checked).

3. Under the **Exceptions** tab click **Add Port** and then enter the UA endpoint in the **Name** field. Enter the port number for the endpoint (found in step 3 of the **Endpoints** section above) in the **Port Number** field. Verify that the correct protocol is selected. The default setting is TCP. Click **OK**.
4. You can add additional endpoints by repeating step 3 above. Click **OK** to exit when you are finished configuring the exceptions.
Contact Us

If you have any questions or are seeking further assistance, please contact us at:

Online Support:  http://support.softwaretoolbox.com

Email Support:  support@softwaretoolbox.com

Phone Support:  +1 (704) 849-2773

Fax:  +1 (704) 849-6388

Mailing Address:  Software Toolbox, Inc.  148A East Charles Street, Matthews, NC 28105, USA