OPC UA Configuration Manager Help

Table of Contents

OPC UA Configuration Manager

Help version 1.009

CONTENTS

Overview

OPC Unified Architecture (UA) is an open standard created by the OPC Foundation with help from dozens of member organizations. Although UA intends to provide a platform independent interoperability standard (in order to move away from Microsoft COM) it is not a replacement for OPC Data Access (DA) technologies. For most industrial applications, UA will complement or enhance an existing DA architecture. It will not be a system-wide replacement. OPC UA complements OPC DA infrastructures in the following ways:

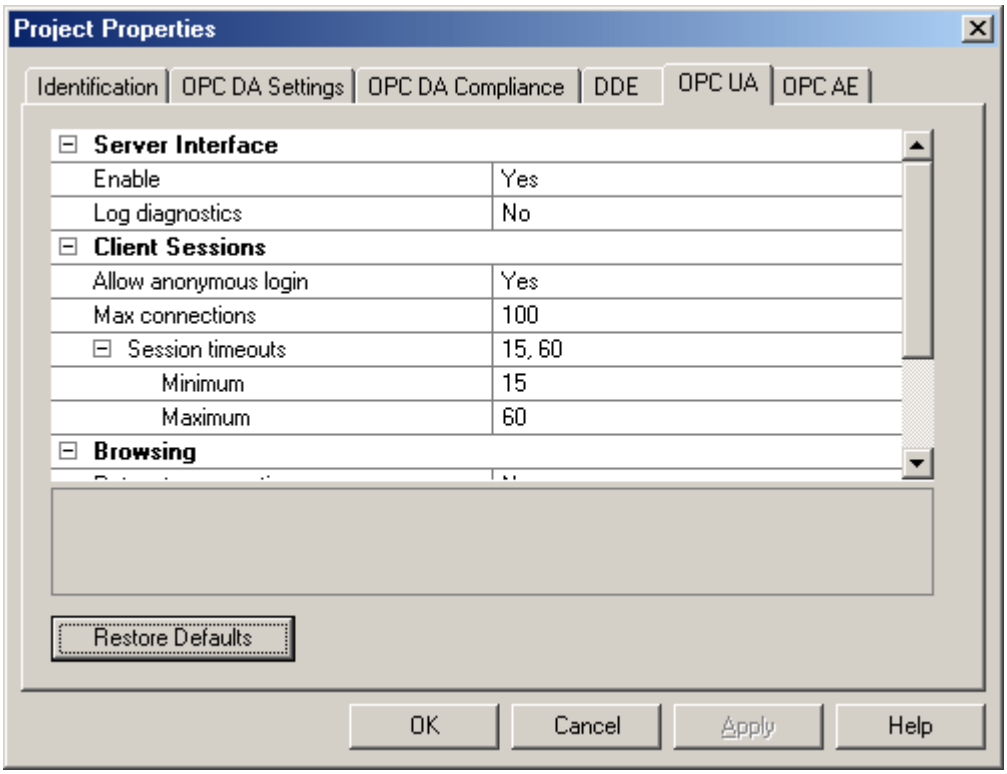
- It offers a secure method of client-to-server connectivity without depending on Microsoft DCOM and has the ability to connect securely through firewalls and over VPN connections. For users connecting to remote computers within the corporate network (inside the firewall) on a domain, an OPC DA and DCOM connection may be satisfactory.
- It provides an additional way to share factory floor data to business systems (shop-floor to top-floor). OPC UA can aggregate data from multiple OPC DA sources into non-industrial systems.

For the majority of user applications, the most relevant components of the UA standard are as follows:

- Secure connections through trusted certificates for client and server endpoints.
- Robust item subscription model to provide efficient data updates between clients and servers.
- An enhanced method of discovering available information from participating UA servers.

Server Settings

The Server Settings dialog may be accessed through the Configuration by clicking **File** | **Project Properties** and then selecting the **OPC UA** tab.



Server Interface

Descriptions of the parameters are as follows:

- **Enable:** When enabled, the UA server interface will be initialized and accept client connections. When disabled, the remaining parameters on this page will also be disabled.
- **Log Diagnostics:** When enabled, OPC UA stack diagnostics will be logged to the Event Log. This should only be enabled for debugging purposes.

Client Sessions

Descriptions of the parameters are as follows:

1. **Allow Anonymous Login:** When disabled, this parameter specifies that user name and password information will be required to establish a connection. The default setting is enabled.
2. **Max Connections:** This parameter specifies the maximum number of supported connections. The valid range is 1 to 100. The default setting is 100.
3. **Session Timeouts:** This parameter specifies the UA client's timeout limit for establishing a session. Values may be changed depending on the needs of the application. The default values are 15 to 60.
   - **Minimum:** This parameter specifies the UA client's minimum timeout limit. The default setting is 15.
   - **Maximum:** This parameter specifies the UA client's maximum timeout limit. The default setting is 60.

Browsing

Descriptions of the parameters are as follows:

1. **Return Tag Properties:** When enabled, this parameter allows UA client applications to browse the tag properties available for each tag in the address space. This setting is disabled by default.
2. **Return Address Hints:** When enabled, this parameter allows UA client applications to browse the address formatting hints available for each item. Although the hints are not valid UA tags, certain UA client applications may try to add them to the tag database. When this occurs, the client will receive an error from the server. This may cause the client to report errors or stop adding the tags automatically. To prevent this from occurring, make sure that this parameter is disabled. This setting is disabled by default.

Advanced Settings

Advanced Settings are stored in the settings.ini file. Although this file may be edited, it is recommended that the default settings be used for most applications.

Name	Description	Default Value	Minimum Value	Maximum Value
MaxAlloc	Maximum serializer memory allocation.	4MB	128K	8MB
MaxStringLength	Maximum string length.	64K	16K	1MB
MaxByteStringLength	Maximum byte string length.	1MB	16K	2MB
MaxArrayLength	Maximum array length.	64K	16K	1MB
MaxMessageSize	Maximum message size.	4MB	128K	8MB

OPC UA Configuration Manager

The OPC UA Configuration Manager assists users in administering the UA server configuration settings. OPC UA's security requires that all endpoints participating in UA communication do so over a secure connection. To comply with this security requirement, each UA server instance and UA client instance must provide a trusted certificate to identify itself. These certificates may be self-signed. As such, they must be added to a local trusted certificate store on both the server and client nodes by a user with Administrator privileges before any secure UA client/server connections may be attempted. The UA Configuration Manager is a user-friendly interface through which the certificate exchange may be performed.

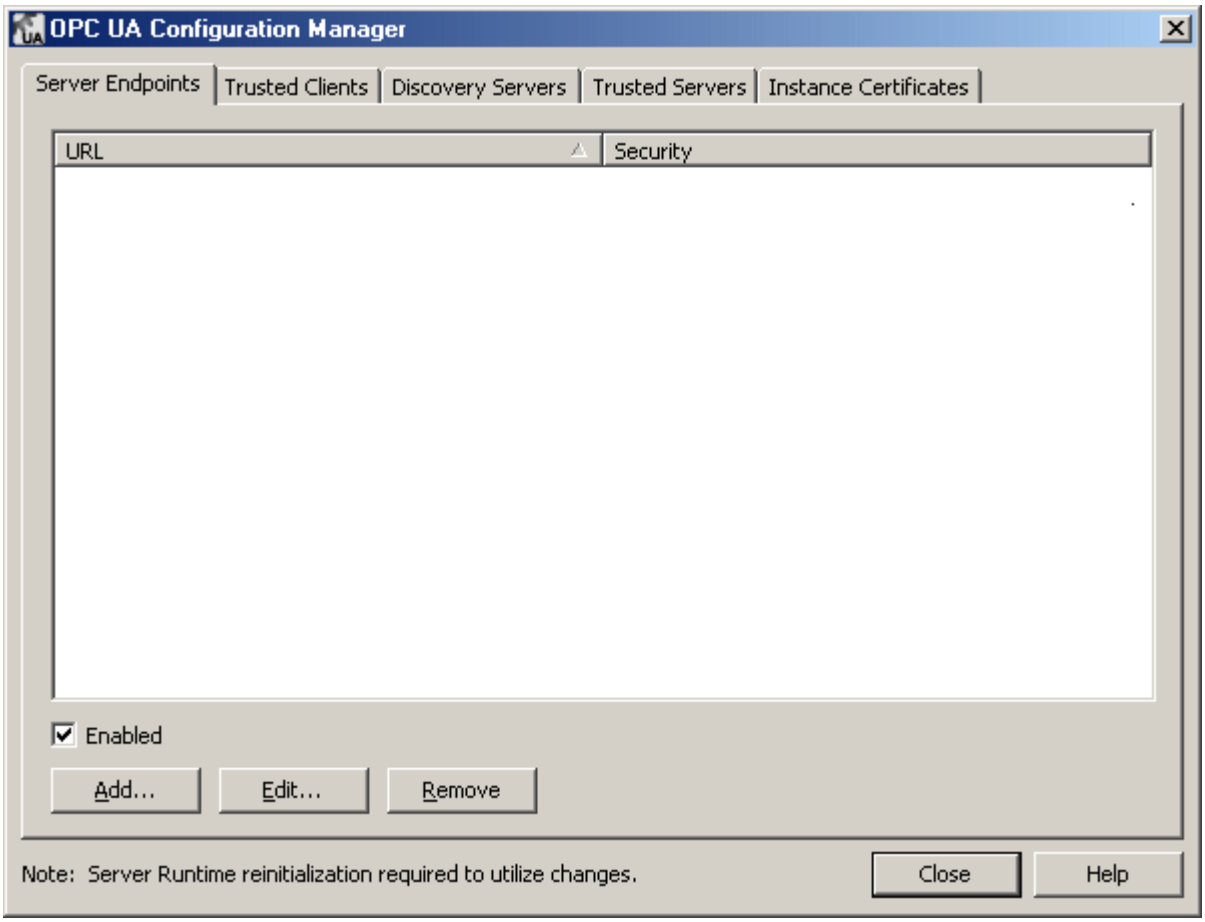
For more information on a specific OPC UA Configuration Manager tab, select a link from the list below.

Server Endpoints
Trusted Clients
Discovery Servers
Trusted Servers
Instance Certificates
Certificate Exchange

Server Endpoints

Server Endpoint definitions are required by the OPC UA server in order to create a UA interface with which UA clients can communicate. UA server endpoints are defined as Universal Resource Locators (URLs). They identify the specific instance of a server, transport type and the security with which it communicates.

Note: Each defined endpoint is enabled by default, but users may disable it if desired. The application of a state change to the running server requires re-initialization of the UA server's Runtime.

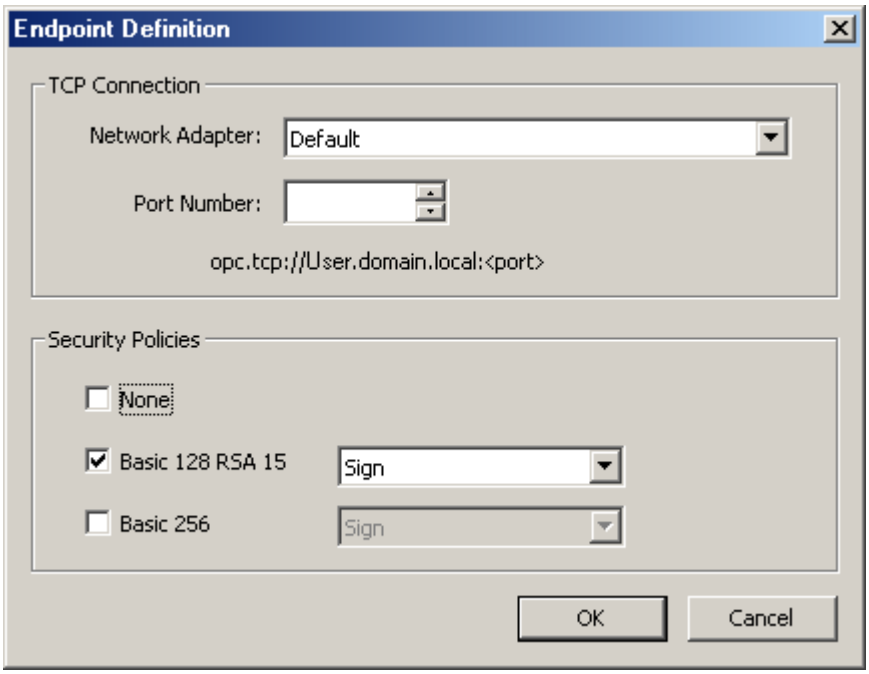


Note: All endpoints within the server instance share the same instance certificate. The UA server uses self-signed certificates: users with administrative privileges must manually place a copy of the UA server's certificate into the trusted store for each UA client that wishes to connect to the UA server.

Important: In compliance with OPC UA requirements, a server implementing the Standard UA Server Profile must support user name/password logon. This UA server will support user information validation on a per server instance basis (instead of per endpoint). Recognized users will come from the User Manager feature within the Server Administration, which is located in the System Tray.

Endpoint Definition

To access the Endpoint Definition dialog, click **Add...** or **Edit...** in the Server Endpoint tab.



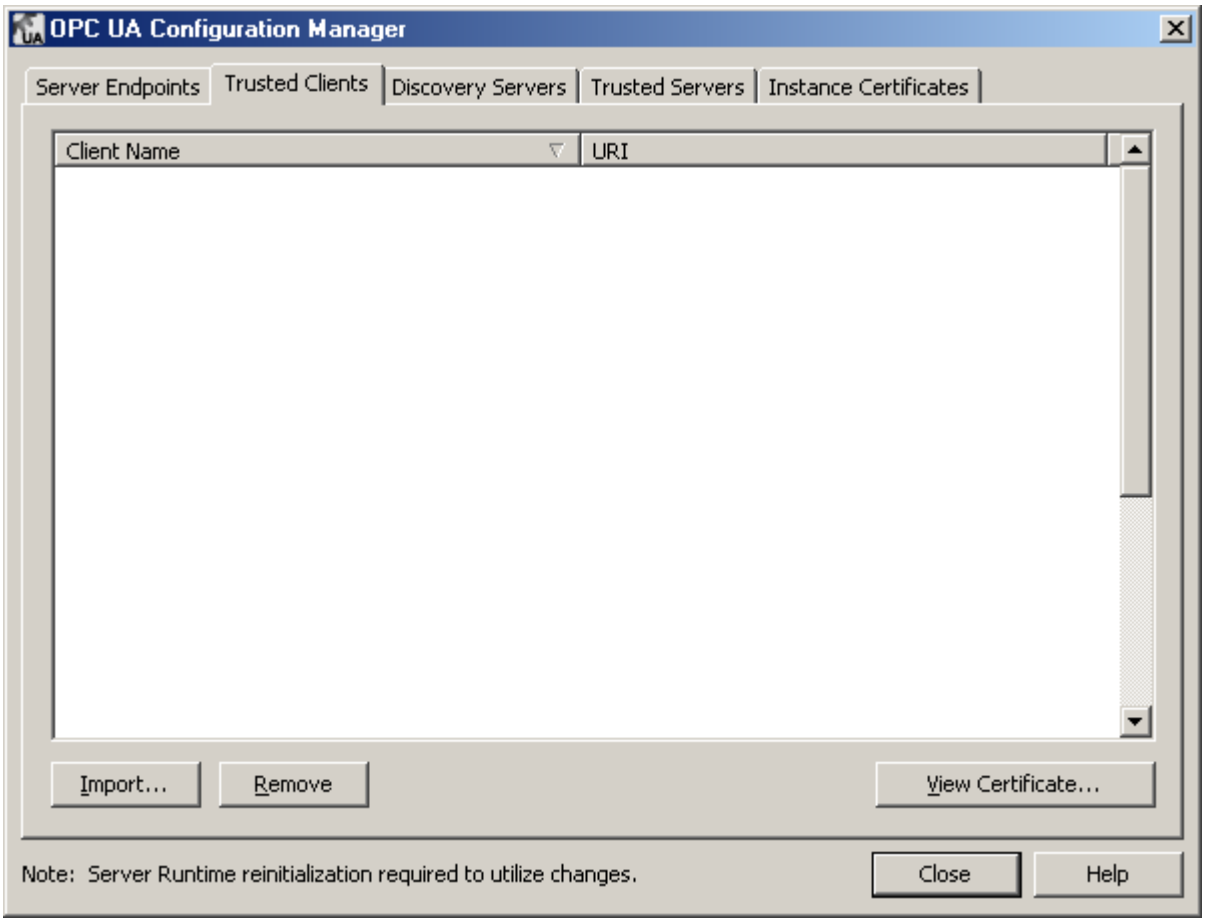
Description of the parameters are as follows:

- **Network Adapter:** This parameter specifies the network adapter to which the connection will be bound. It may be configured to available adapters with IP addresses, Default and Local host only. The initial selection is Default, which maps to the default network adapter.
- **Port Number:** This parameter specifies the port number. This is required in the definition because the remainder of the URL that is constructed to define the endpoint is standardized on the hostname of the computer and the transport protocol. All endpoint URLs defined by this dialog will be of the form *opc.tcp://<hostname>:<port>*. In the event that a fully qualified host name cannot be determined, either the local host or an IP address will be substituted.
- **Security Policies:** The Security Policy drop-down lists may only be accessed when the corresponding checkbox is checked. If both Basic 128 RSA 15 and Basic 256 are not checked, the security policy assumption will default to None.

  Note: The None and Basic 128 RSA 15 security policies are required to support the Standard UA Server profile as defined by the OPC UA Specification, part 7. Basic 256 is provided to implement the highest supported level of security.

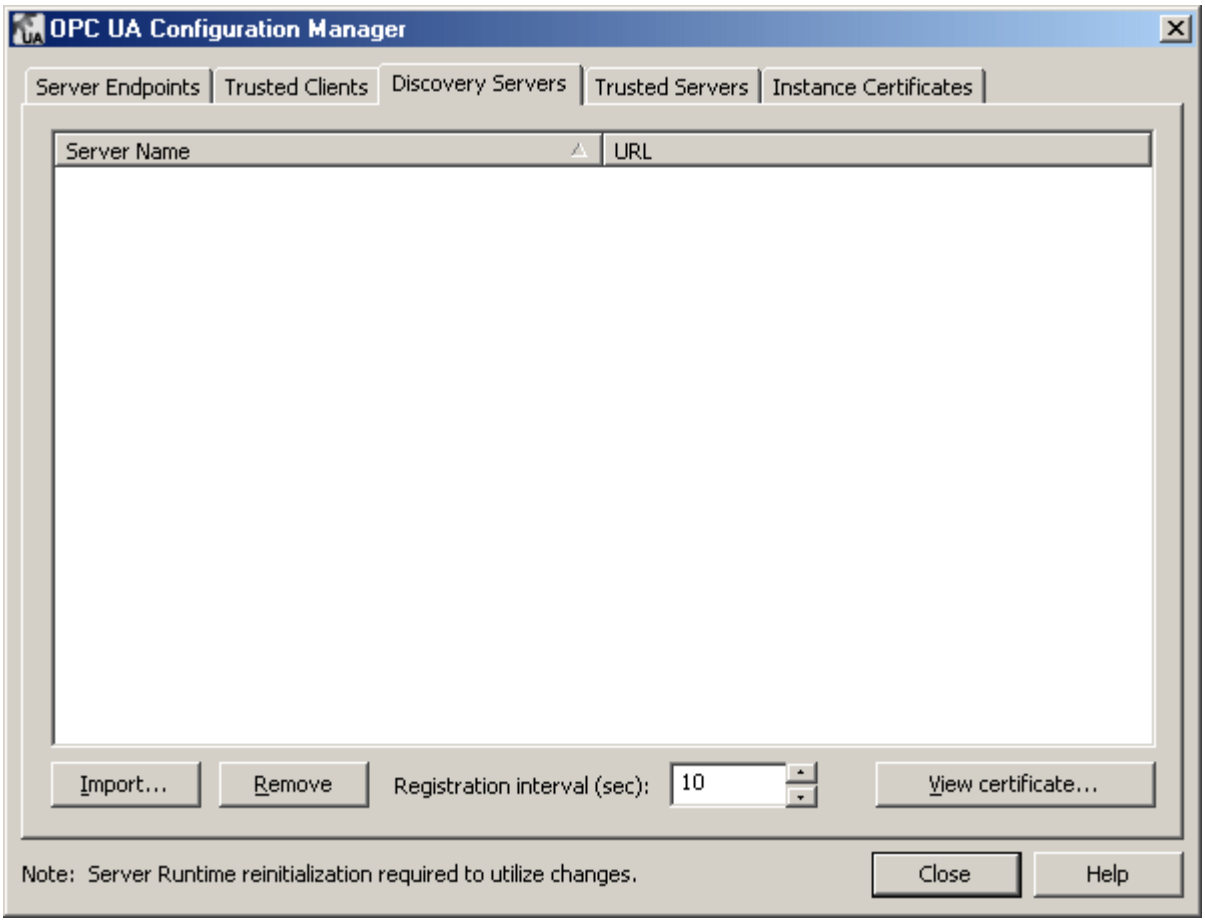
Trusted Clients

UA servers require a certificate to establish a trusted connection with each UA client. In order for the server to accept connections from a client that provides a self-signed certificate, the client's certificate must be imported into the trusted client certificate store used by the OPC UA server interface. To facilitate this function, the UA Configuration Manager has the ability to import, remove and view trusted client certificates.



Discovery Servers

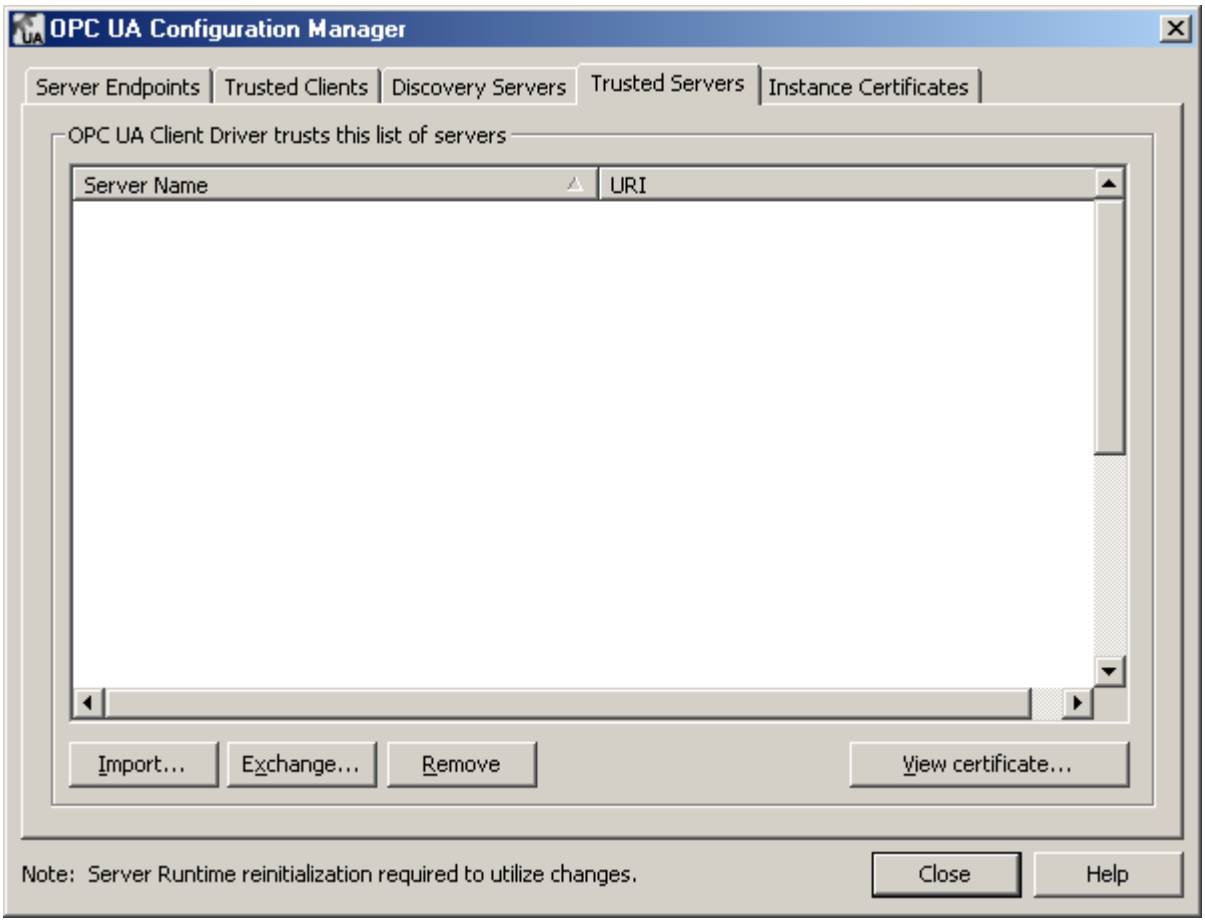
Any OPC UA server may register with a UA Discovery Server in order to make its endpoint information available to clients with access. In order to perform this registration, the UA server interface must know what endpoint or endpoints to use. A Discovery Server with a self-signed certificate must be obtained and stored in the UA server's trusted certificate store. Likewise, the UA server's certificate must be obtained and stored in the UA Discovery Server's trusted certificate store. The UA Configuration Manager provides the ability to import, remove and view trusted Discovery Server endpoints that will be identified to the UA server interface.



Note: Users may change the registration interval that will be used to refresh the Discovery Server through the **Registration Interval (sec)** parameter. The default setting is 10 seconds.

Trusted Servers

The Trusted Servers tab will only be displayed if the UA Client Driver is installed on the computer. This dialog is used to establish the list of trusted servers with which the UA Client Driver can communicate.

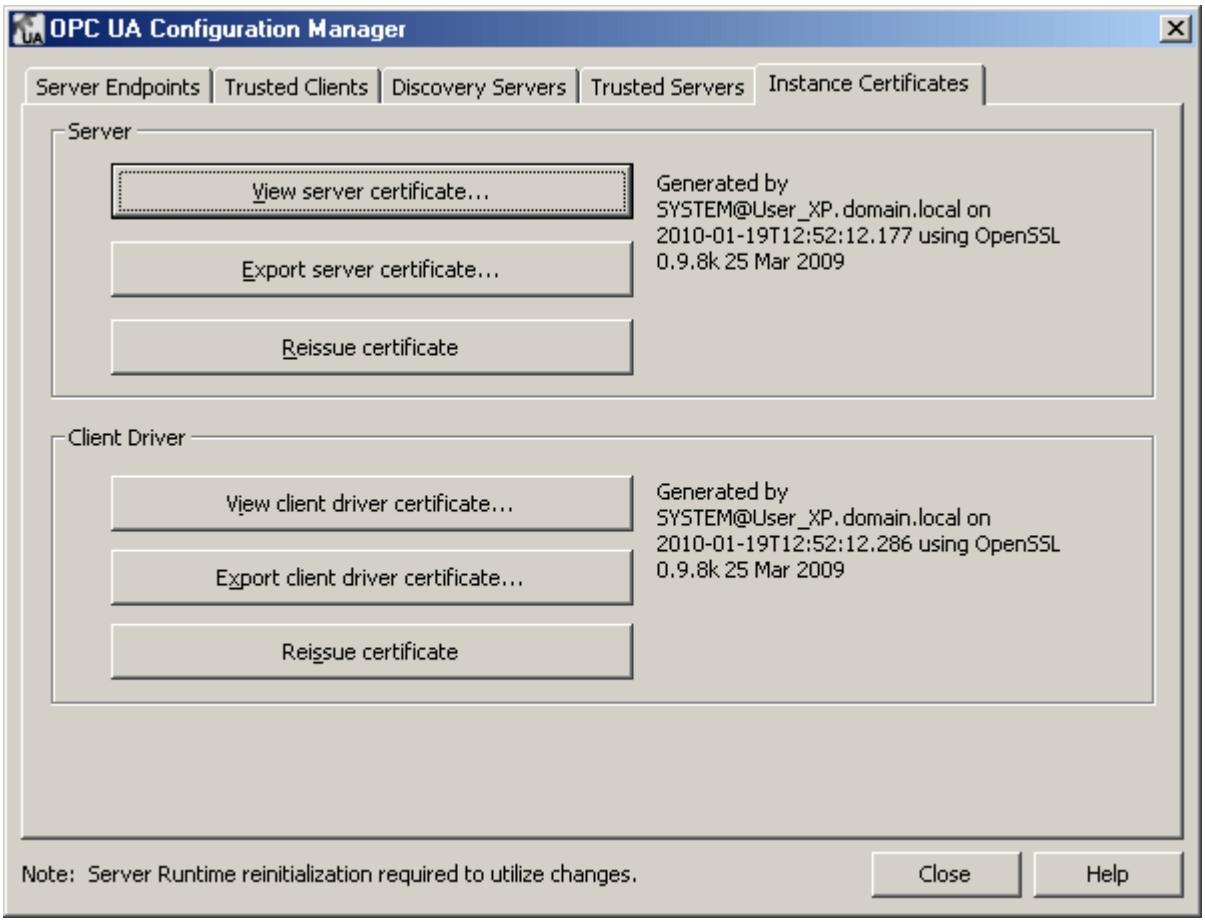


The UA Client Driver requires trusted certificate management for clients that self-sign, just like the UA server. In order for the UA Client Driver to connect to a server that uses a self-signed certificate, users with administrative privileges must import the external UA server's certificate into the UA Client Driver's trusted certificate store. Because the client driver self-signs its certificate, that certificate must be exported and stored to the server's trusted certificate store.

Note: For information on exchanging certificates between the UA Client driver and the UA server, refer to **Manual Exchange**.

Instance Certificates

The self-signed X.509 Instance Certificates are created for the UA Server and the UA Client Driver. They may be accessed through the Instance Certificates tab as shown below.



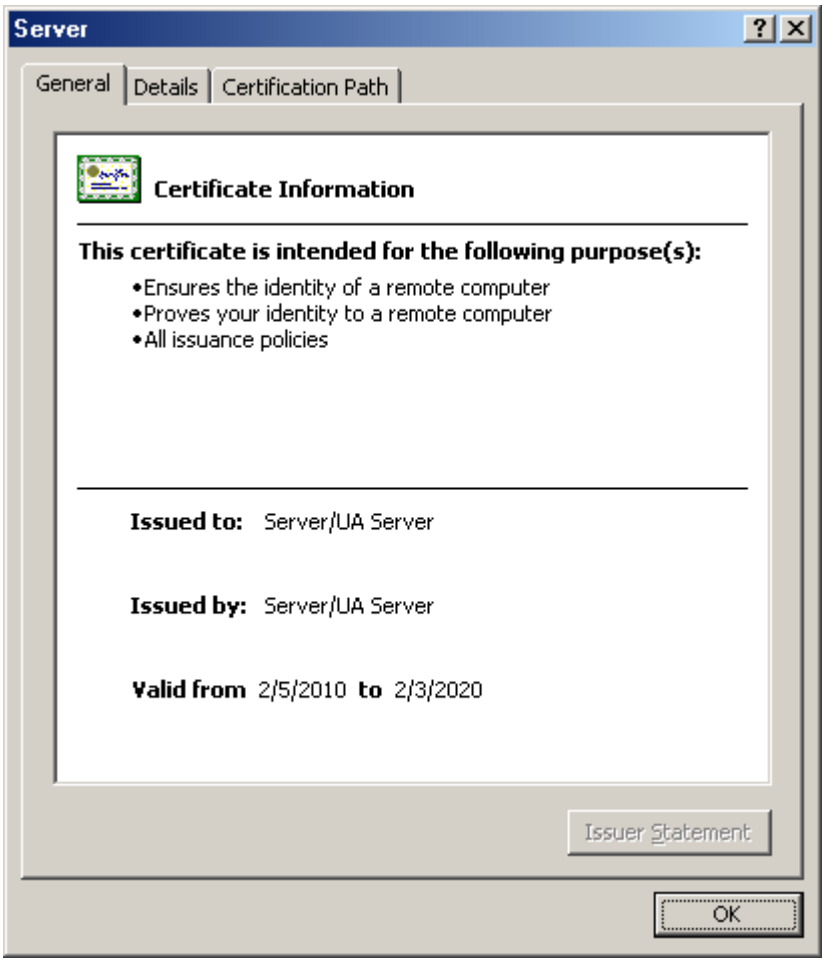
The default names assigned to the certificate files are as follows:

- <product name>_ua_server.der
- <product name>_ua_client_driver.der

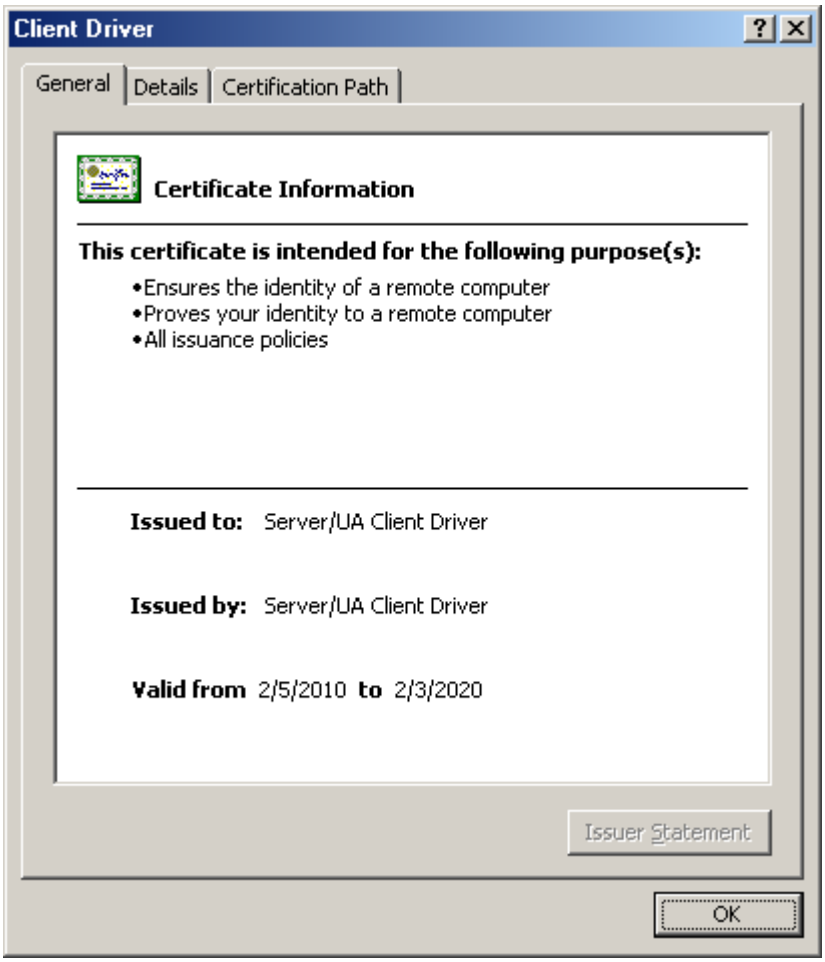
Note: Before a third-party UA client may be connected to the UA server, a manual exchange of certificates must occur. To use the UA Client Driver with a local or remote instance of the UA server, click **Exchange** in the **Trusted Servers** tab of the UA Configuration Manager.

Viewing the Server and Client Driver Certificates

To view the server certificate, click **View Server Certificate** in the **Instance Certificates** tab of the UA Configuration Manager.

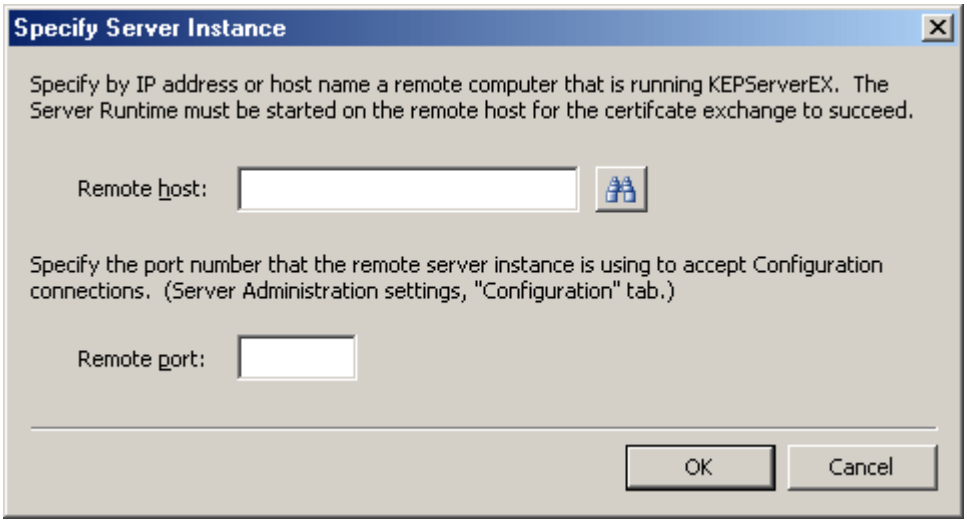


To view the client driver certificate, click **View Client Driver Certificate** in the **Instance Certificates** tab of the UA Configuration Manager.



Certificate Exchange

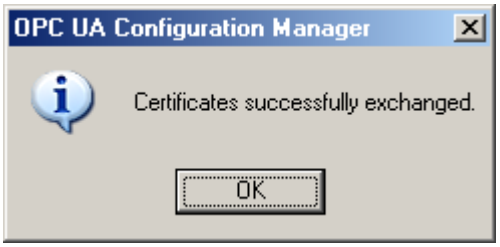
When using OPC UA as a secure and reliable tunnel for remote connectivity (or alternative to DCOM), certificates must be exchanged between the UA Client Drivers and the UA server. To do so, select the **Exchange** button located in the Trusted Servers tab of the UA Configuration Manager.



The following conditions are required in order for the Exchange feature to work:

1. The UA server must be installed on the remote node.
2. Remote connections to the UA server Runtime must be enabled.
3. The server Runtime application must be running on the remote node.
4. The settings on the local exchange property window must be correct.
5. The user must have a working network connection to the remote node.
6. There may not be any firewalls blocking either node.

Users must select the remote node and then click **OK**. If the certificate exchange is successful, the following dialog will be invoked.



Exchanging Certificates Between Third-Party UA Clients and the UA Server

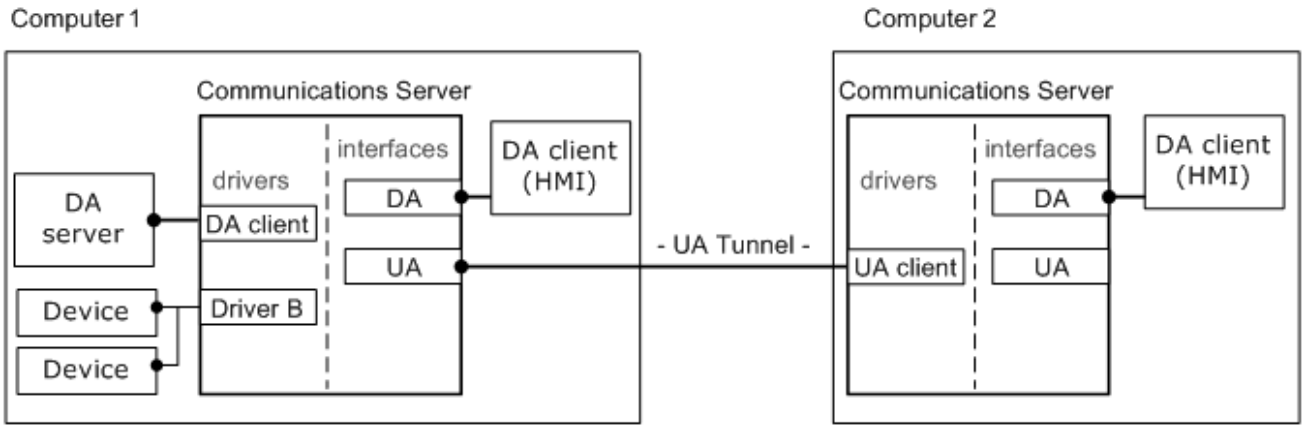
The example below demonstrates how to manually exchange certificates between the UA server running on one computer (PC1) and the server with UA Client Driver running on a second computer (PC2). The example below assumes that users have Administrator privileges on both computers.

1. To start, install the server on PC1. The UA server components will install automatically.
2. In the System Tray, right-click on the Server Administration and then select **OPC UA Configuration**.
3. Click on **Instance Certificates** and then select **Export Server Certificate...**. Accept the default name, noting the save location for future reference.
4. Move the exported server certificate to PC2. This may be accomplished with a USB memory stick.
5. Next, install the server on PC2. The UA server components will install automatically. Be sure that the OPC UA Client Driver is selected when install components are selected.
6. Next, launch the OPC UA Configuration utility through the System Tray (as mentioned above).
7. Click on **Trusted Servers** and then select **Import...**.
8. Import the server certificate created on PC1. Accept the default import location.
9. Next, click on **Instance Certificates** and then select **Export client driver certificate...**. Accept the default name, noting the save location for future reference.
10. Move the exported client certificate to PC1. This may be accomplished with a USB memory stick.
11. From PC1, launch the OPC UA Configuration Utility through the System Tray.
12. Click on **Trusted Clients** and then select **Import...** in order to import the client certificate created on PC2. Accept the default import location.
13. Next, stop and restart the server Runtime. To do so, right-click on the Administration's icon in the System Tray and then select **Stop Runtime Service** | **Start Runtime Service**.
14. From PC2, launch the server configuration from the Administration utility. Configure a project that uses the UA Client Driver including channel, device and items. When creating the channel, users should be able to browse to the UA server endpoints on PC1.

Note: If unable to browse or establish a connection to the UA server, refer to **Troubleshooting Tips**.

OPC UA Tutorial

This tutorial provides instructions on configuring a secure OPC UA connection between two remote computers running the communications server.



The following Runtime components are required:

- The communications server with UA server interface on Computer 1.
- The communications server with UA Client Driver on Computer 2.

Note: The OPC DA Client Driver (shown in the image above as Computer 1) is an optional component used to connect to external OPC DA servers.

Prerequisites

Before continuing, users must do the following:

1. Install the server application on the client computer. In the **Select Features** dialog, include the OPC UA Client Driver (located beneath **Communication Drivers**).

2. Install the server application on the server computer. Since UA functionality is included, no additional features need to be selected during the install.

Note: Certain user applications may require that each computer act as a server as well as a client. If so, install the OPC UA Client Driver on each computer that needs to access items remotely.

Security

Instead of relying on the computer's operating system to secure the applications, OPC UA uses X.509 authentication technology. This technology consists of a set of public and private keys for each entity wishing to establish a trust. The private key is protected while the public key is placed into a certificate for distribution. The client and server must exchange certificates in order to establish a secure connection. This exchange only has to be done once in the certificate's lifetime.

There are two methods of exchange: **Automated** and **Manual**. The automated exchange is performed from the client side and only takes an instant to complete. In order to do so, however, the server computer must have an open port in the firewall and the Runtime must be allowed to accept remote configuration on that port. The manual exchange includes the export and import of a certificate file on each computer. Removable media (or another form of file transfer) must be used in order for the exchange to take place. The manual process also allows for certificates to be exchanged between clients and servers that are beyond the scope of this application.

If security is not compulsory, the certificate exchange can be skipped. The level of security is set by users when defining the server endpoints. When "None" is selected, certificates will not be checked for validation. For more information on unsecure connections, refer to **Setting up the Server**.

Automated Exchange

1. To start, right-click on the **Administration** icon in the System Tray. Then, click **Settings** | **Configuration**.

2. To enable remote configuration, check **Allow runtime to accept remote connections**.

   Note: The change will be applied once the Configuration interface is shutdown, because the same port is used to configure the Runtime locally.

3. Next, add an exception to the Windows firewall for the port that is specified in the **Communicate using port ___** parameter. Users may temporarily turn off the firewall before the exchange is performed and then return the firewall back to its secure state once the process is complete. This will prevent unauthorized users from exchanging certificates in the future.

4. From the client computer, launch the OPC UA Configuration Manager by right-clicking on the **Administration** icon in the System Tray. Then, select **OPC UA Configuration**.

5. Click **Trusted Servers** | **Exchange**.

6. In the **Server Instance** dialog, click the **Browse** icon (located to the right of the **Remote Host** field).

   Note: Newer operating systems may be required to enable discovery and file sharing.

7. Browse to the server and then select the computer name. Click **OK**.

8. Next, verify that the correct port is identified in the **Remote Port** field. This port is used for the server's remote configuration. The value should match the value on the server computer (visible when the exception was made to the firewall).

9. Click **OK**. A message will be invoked, stating that the exchange was successful. The server certificate should appear in the **Trusted Servers** window and can be identified by the URI.

10. Launch the OPC UA Configuration Manager on the server computer. The client certificate should be in the **Trusted Clients** window and can be identified by the URI.

Manual Exchange

1. To start, launch the OPC UA Configuration Manager on the server computer by right-clicking on the **Administration** icon in the System Tray. Then, select **OPC UA Configuration**.

2. Next, select **Instance Certificate**. Under the **Server** group, click **Export Server Certificate**. Select an easily accessible location for the certificate file. Users may change the default file name as desired.

3. Manually copy the server certificate file from the server computer and move it onto the client computer.

4. Next, launch the OPC UA Configuration Manager on the client computer.

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

6. Locate the server certificate file and then click **Open**. The server certificate should appear in the **Trusted Servers** window and can be identified by the URI.

7. Next, select **Instance Certificate**. Under the **Client Driver** group, select **Export Client Driver Certificate**. Select an easily accessible location for the certificate file. Users may change the default file name as desired.

8. Manually copy the client certificate file from the client computer and return it to the server computer.

9. Next, launch the OPC UA Configuration Manager on the client computer.

10. Select the **Trusted Clients** tab and then click **Import**.

11. Locate the client certificate file and then click **Open**. The client certificate should appear in the **Trusted Clients** window and can be identified by the URI.

Setting Up the Server

Endpoints

In order for an OPC UA client to connect to an OPC UA server, the client must know the server location and security requirements. In its complex form, the client will use a location and port number (called a discovery endpoint) to discover information about the server. In turn, the server will return all configured endpoints along with the security requirements that are available to the client. To simplify the process, the discovery endpoint and the server endpoint

may reside in the same location (as is the case with this server application).

An initial endpoint is created during the server application installation for local connections. Minor configuration changes are required in order to allow remote clients to discover and connect to the server. The server does not require any changes to make local connections. For information on adding and changing the existing endpoints, follow the instructions below.

1. To start, launch the OPC UA Configuration Manager by right-clicking on the **Administration** icon in the System Tray. Then, select **OPC UA Configuration**.

2. Next, click **Server Endpoints** and then select the default endpoint that was created during the install for non-local connections.

3. Click **Edit**.

   Note: Be sure to note the port number so that it can be added to the firewall later.

4. If necessary, modify the **Security Policies** settings. Since these are server settings, this particular endpoint will allow all connections with the enabled policies. This means that the default endpoint will only allow secure connections using signing and encryption. If security is not required, select "None." Users making this selection may want to disable the security policies completely.

5. Once the policies have been adjusted accordingly, click **OK**.

6. To enable the endpoint, select it in the list and then check **Enable**.

7. Next, apply the changes to the server Runtime by right-clicking on the **Administration** icon in the System Tray and then selecting **Reinitialize**. If the server is not running, right-click on the **Administration** icon and then select **Start Runtime**.

Discovery Service (Optional)
Users familiar with OPC DA may be familiar with OPCEnum, an application that runs locally on the serving computer and exposes available OPC DA servers to the clients connecting remotely. The client only needs to know the serving computer's location on the network.

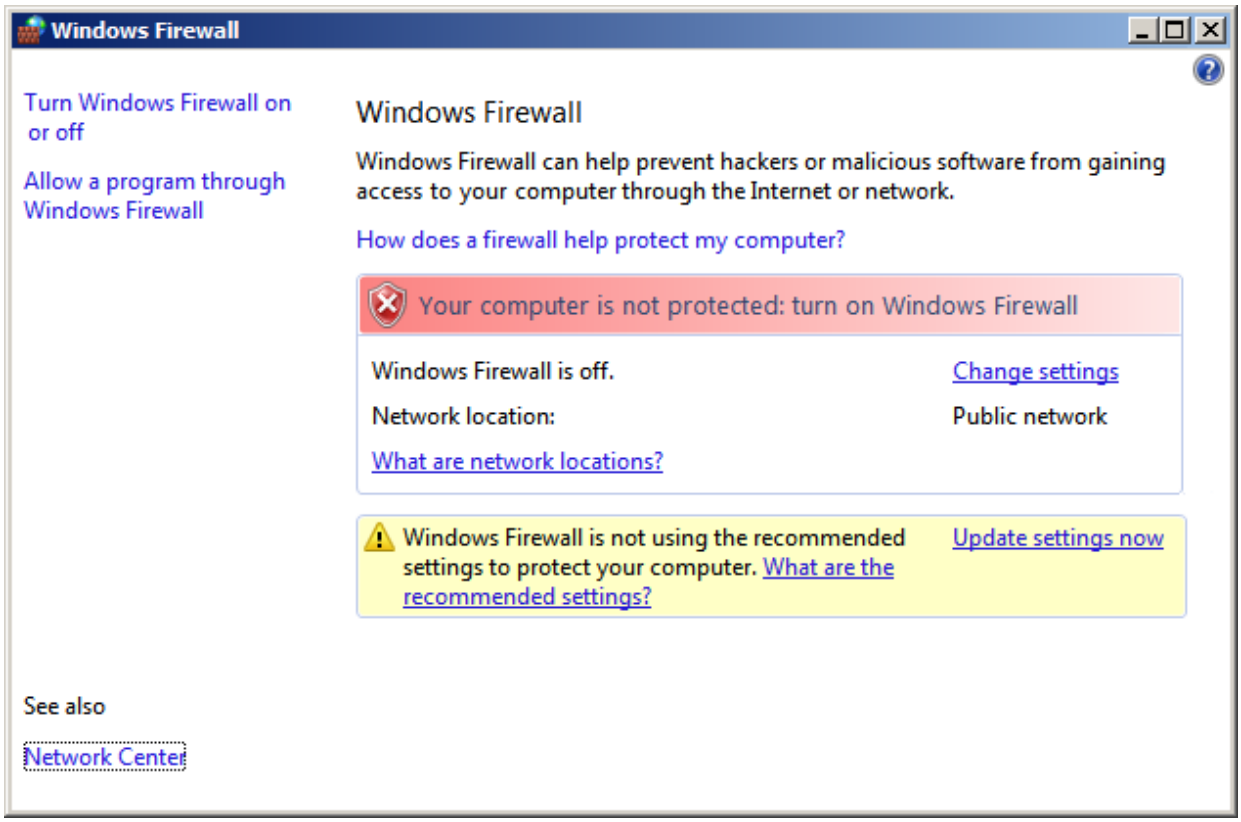
A service was created that allows OPC UA servers to be discovered at a "well-known" location, in order to provide similar usability while being platform independent. Called **Local Discovery Service (LDS)**, this service is expected to be installed on every computer that is running an OPC UA server (in the same way that OPCEnum is installed alongside most classic OPC servers). Since the development and implementation of LDS has not come as far as OPC UA itself, the actual usage of the service will vary.

Note: This server application does not provide an LDS, but may be configured to register with one.

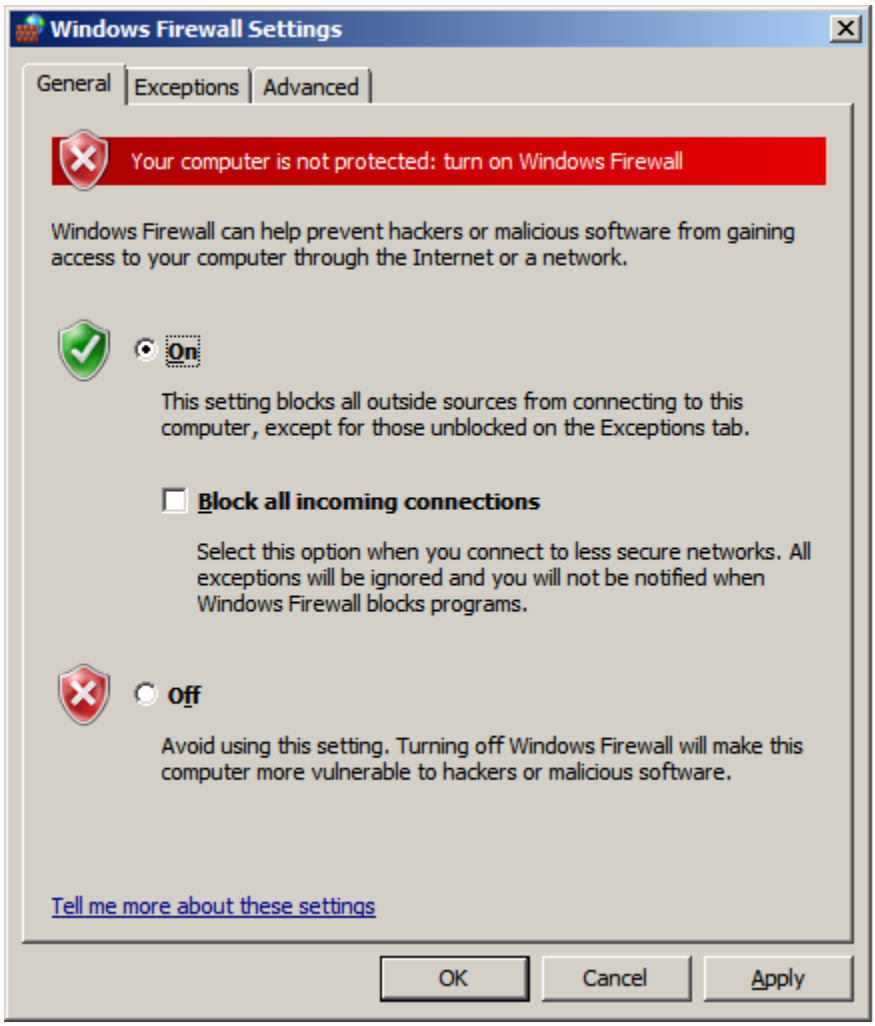
Firewall
The firewall drops incoming traffic that is not expected (called "unsolicited traffic") or traffic that does not correspond to the exceptions set within the firewall (called "excepted traffic"). Since OPC UA does not require callbacks, only the server computer needs to have the exception.

To add an exception, follow the instructions below on the server computer.

1. To start, launch the Windows Firewall by selecting **Start** | **Run**. Then, type **firewall.cpl**.



2. Since Windows Vista and Windows Server 2008 will not directly display the Settings dialog, click **Change Settings**.
3. Next, click **General**.



4. Verify that the firewall is enabled by clicking **On**. Then, select the **Exceptions** tab.
5. Click **Add Port** and then enter the UA endpoint in the **Name** field. Enter the port number that is assigned to the endpoint in the **Port Number** field.
6. Verify that the correct protocol is selected. The default setting is TCP.
7. Next, click **OK**.
8. If multiple endpoints have been assigned to the server, add them now. When finished, click **OK** to exit.

Setting Up the Client

OPC UA Client Driver Channel

The Channel Wizard is used to locate and identify the OPC UA server, configure session timeouts and provide user information when applicable. For information on adding a UA Client channel, follow the instructions below.

1. To start, launch the Configuration by right-clicking on the **Administration** icon in the System Tray. Then, select **Configuration**.
2. Next, select **Edit** | **Devices** | **New Channel**.
3. In **Identification**, type a name for the OPC UA client channel and then click **Next**.
4. In **Device Driver**, select **OPC UA Client** and then click **Next**.
5. Keep the default settings in **Write Optimization** by clicking **Next**.

6. In **UA Server**, manually enter the server's endpoint URL into the **Endpoint URL** field. Alternatively, users can click the Browse icon and locate it on the computer.
7. Verify that the **Use Discovery URL** parameter is disabled.
8. 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. Thus, if a discovery server is being used, it is not necessary to enter the correct port number in this field.
9. If the port number was changed, click **Refresh**.
10. Next, locate the server computer. Endpoints that are assigned to "localhost" will only be found under the **Local Machine** branch.
11. Expand the computer to display a list of available servers. Then, expand the servers and select the correct endpoint.
12. 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.
13. Next, click **OK**. The endpoint information will appear in the UA Server page. Click **Next**.
14. Keep the default settings in **UA Session** by clicking **Next**. These can be optimized later if desired.
15. Keep the username and password blank in **Authentication** by clicking **Next**. These may be changed as desired.
16. View the **Summary** and then click **Finish**.

OPC UA Client Device

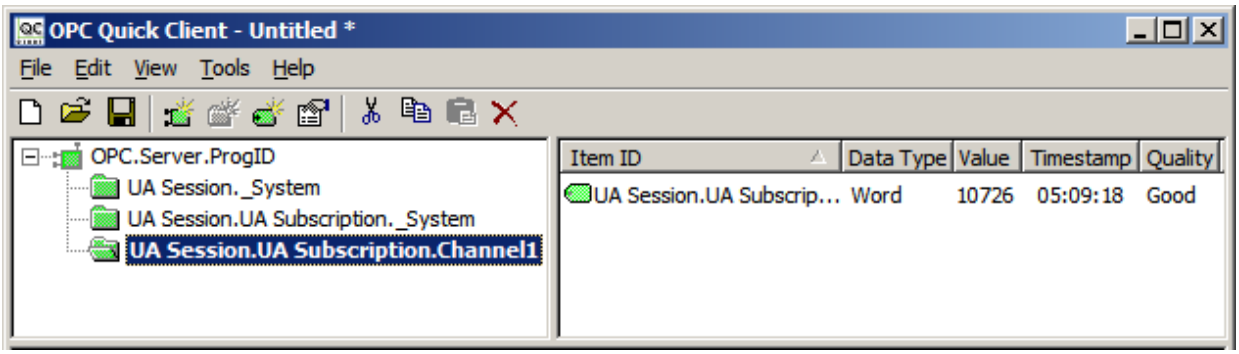
The Device Wizard guides users in setting up a subscription, and also provides a way to browse and import items from the OPC UA Server. All the items in the device will update according to the settings provided. Multiple devices can be added to the same channel in order to allow for different update intervals and modes. For information on adding a UA Client device, follow the instructions below.

1. To start, select the new channel and then click **Edit** | **Devices** | **New Device**.
2. In **Name**, type a name for the OPC UA client device and then click **Next**.
3. Keep the default settings for **Subscription**, **Keep Alive**, **Priority and Timeout**, **Monitored Items** and **Deadband** by clicking **Next**. These can be optimized later if desired.
4. In **Import**, click **Select import items**. The server's available items should appear in the browsing window. If not, the security configuration may be incorrect. For more information, refer to **Troubleshooting Tips**.
5. Select the desired items and then 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** and then click **Finish**. The imported items will populate beneath the device, using the server's channel and device names as groups.

Verification

The items added in the OPC UA Client can now be browsed by an OPC DA client. For easy verification, follow the instructions below.

1. Select **Tools** | **Launch OPC Quick Client**. A connection will be established to the local OPC DA server and items will populate the view.



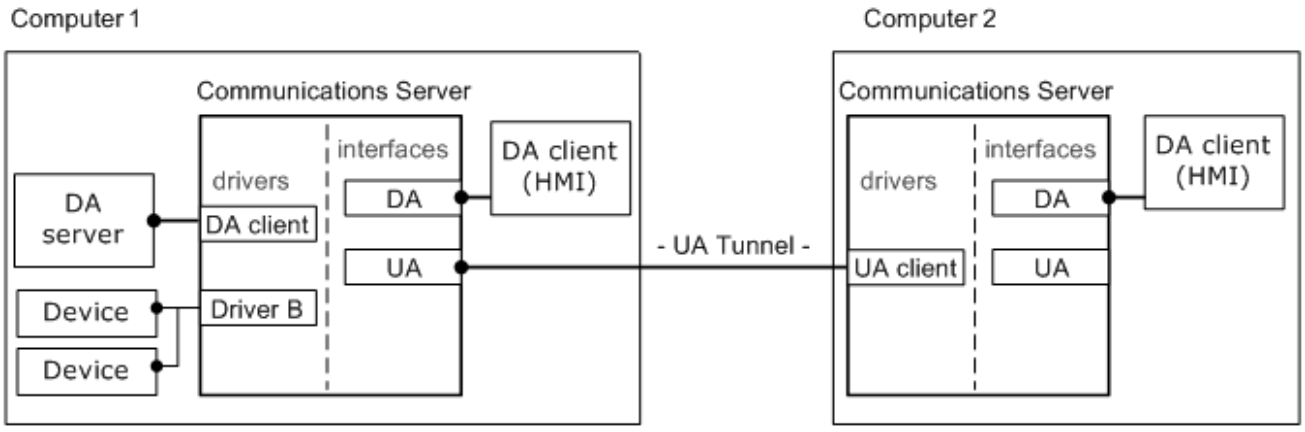
2. Browse for the items in the OPC UA channel. Then, verify that the data's quality is good and that the values are updating.

Connection Examples

The OPC UA Tunnel is not a product in itself, but rather a remote connectivity solution created from existing available components. On the server side of the tunnel, the OPC UA server is an interface packaged beside OPC DA in the overall communications server product. On the client side of the tunnel, the OPC UA Client Driver is a driver plug-in that can be added along with other device channels. The OPC UA Configuration Manager is a tool that provides easy management of trusted certificates and UA server endpoints. The DA Client Driver is an additional driver plug-in that further enhances the UA Tunnel solution. Since the communications server is a "server," this driver provides connectivity to other OPC DA servers.

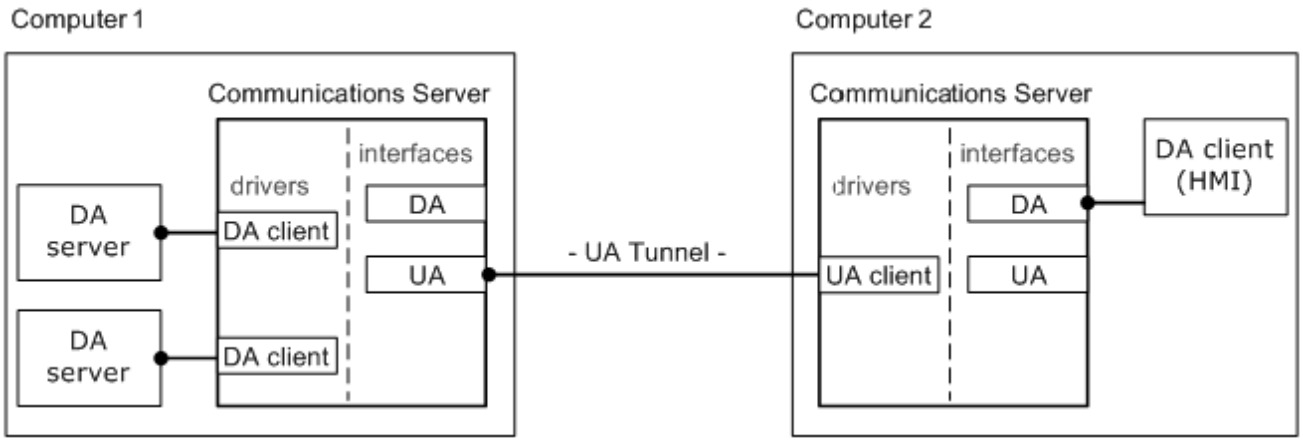
Providing Data from the Factory Floor to Remote Clients

The communications server provides data to local OPC DA clients as well as to remote OPC DA clients. The UA Tunnel solution provides the secure remote connection.



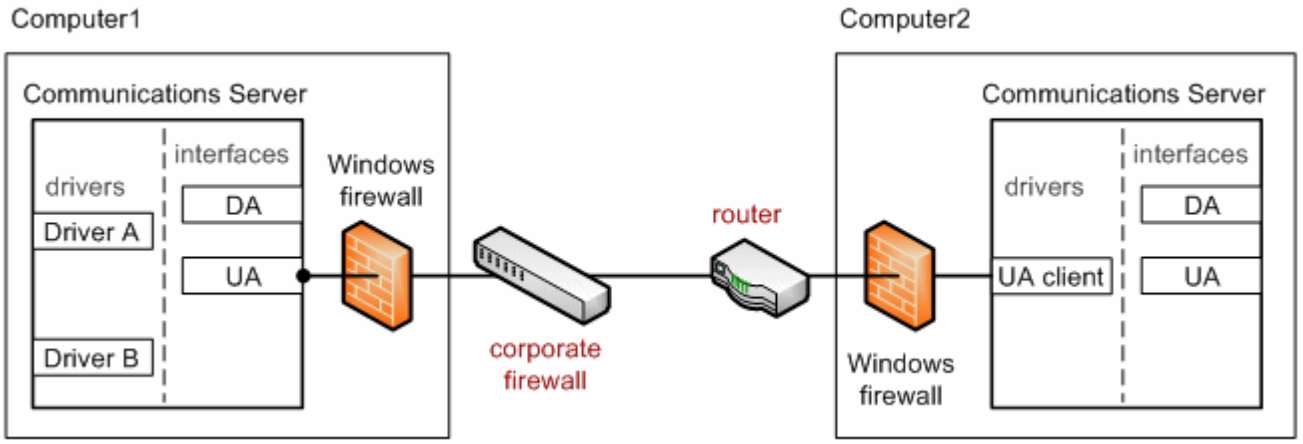
Serving Secure Aggregate Data from External DA Servers

The communications server uses the OPC DA Client Driver plug-in to connect to OPC DA servers. It then securely serves aggregate data to remote OPC DA clients.



Example Firewall and Routing Architecture

It is likely that users will need to allow a port exception (such as the UA server endpoint port) to the Windows firewall on Computer 1, in addition to opening a port in the corporate firewall. There should not be any changes required for the Windows firewall on Computer 2. The router on the client side of the connection, however, may require that a port be opened (or a port forwarding option be enabled).



Troubleshooting Tips

Click on the link for a description of the problem.

Unable to connect to the UA server when trying to import items in the Device Properties dialog

Possible Cause:

1. An incorrect security profile was selected.
2. Certificates are invalid or not present.

Solution:

1. If security is not required, select "None" as the security policy in the Channel Properties dialog.
2. Perform a certificate swap.

Unable to see the UA server when attempting to browse from the UA client

Possible Cause:

1. The endpoint port listed in the Discovery Port field is incorrect.
2. The endpoint is not enabled on the UA server.
3. The UA server interface is disabled in Project Properties.
4. The UA server and endpoint are enabled and correct; however, changes have not been saved to the server Runtime.

Solution:

1. Confirm the endpoint port defined in the UA server and enter the correct port in the Discovery Port field. Then, refresh the view.
2. Launch the OPC UA Configuration Manager on the UA server computer to verify that the endpoint is enabled.
3. Launch the server Configuration. In **File** | **Project Properties**, check the **UA** tab for the Server Interface settings. Enable should be set to "Yes."
4. Save the project from the Configuration, and click "Yes" when prompted to save the changes to the Runtime.

The target computer running the UA server is not shown in the network browse from the UA client

Possible Cause:

The target computer has not been added to the network domain. This may be Workgroup only.

Solution:

Confirm the Endpoint URL from the UA Configuration Manager on the UA server computer. Then, manually enter the Endpoint URL in the UA Client Driver channel.

Unable to connect to the UA server via the correct Endpoint URL

Possible Cause:

1. The corporate firewall on the client side of the connection may only allow connections through a single port (such as 8080).
2. The server side router/switch needs to be configured to forward incoming client requests to the UA server computer.
3. The Windows firewall is blocking the incoming request from the UA client.

Solution:

1. Open a port in the corporate firewall for the UA tunnel connection. Alternatively, reset the endpoint port on the UA server to match the port allowed in the corporate firewall.
2. Configure port forwarding in the router. The UA client's URL would then use the router's IP address with the port number used for the UA server endpoint (which is the port number used for port forwarding in the router).
3. Add an exception for the endpoint port to the Windows firewall.

Connection attempts to the UA server require authentication (Username and Password)

Possible Cause:

The UA server's Client Sessions parameter "Allow anonymous login" has been set to "No."

Solution:

Launch the server Configuration and then click **File** | **Project Properties**. Check the UA tab for the Client Session settings and confirm that "Allow anonymous login" is set to "Yes."

Note:

If Authentication is required, access the User Manager from the server Administration menu (located in the system tray) to set Username and Password.

Cannot ping a router that uses port forwarding to send requests to the UA server

Possible Cause:
The default setting in the router may be set not to respond to ping.

Solution:
Temporarily enable "Respond to Ping" in server side's router. After a successful ping response, disable this setting.

No UA specific error messages are posted to the Event Log

Possible Cause:
UA server diagnostics are not enabled.

Solution:
Launch the server Configuration and then click **File** | **Project Properties**. Review the UA tab for the Server Interface and confirm that "Log diagnostics" is set to "Yes."

Index