OPC UA Configuration Manager

© 2023 PTC Inc. All Rights Reserved.

Table of Contents

OPC UA Configuration Manager 1
Table of Contents 2
OPC UA Configuration Manager 4
Overview 4
OPC UA Configuration Manager 5
Project Properties — OPC UA 5
Server Endpoints 7
Trusted Clients 9
Discovery Servers 10
Trusted Servers 10
Instance Certificates 12
OPC UA Tutorial 15
Connection Examples 25
Troubleshooting Tips 27
Unable to connect to the UA server when trying to import items in the Device Properties dialog 27
Unable to see the UA server when attempting to browse from the UA client 27
The target computer running the UA server is not shown in the network browse from the UA client 28
Unable to connect to the UA server via the correct Endpoint URL 28
Connection attempts to the UA server require authentication (Username and Password) 29
Cannot ping a router that uses port forwarding to send requests to the UA server 29
No OPC UA Specific Error Messages are Posted to the Event Log 29
Event Log Messages 30
Account '<name>' does not have permission to run this application. 30
The UA Server certificate has been reissued. UA clients must trust the new certificate to connect. 30
The UA Client Driver certificate has been reissued. UA servers must trust the new certificate for the client driver to connect. 30
The UA Client certificate '<client name>' has been rejected. The server cannot accept connections from the client. 30
The UA Client certificate '<client name>' has been trusted. The server can accept connections from the client. 30
The UA Server certificate '<server name>' has been rejected. The UA Client Driver cannot connect to the server. 31
The UA Server certificate '<server name>' has been trusted. The UA Client Driver can connect to the server. 31

The UA Server certificate '<server name>' has been added to Trusted Servers. The UA Client Driver can now connect to the server. 31
The UA Client certificate '<client name>' has been added to Trusted Clients. The UA Server can now accept connections from the client. 31
The UA Client certificate '<client name>' has been removed from Trusted Clients. The UA Server cannot accept connections from the client. 31
The UA Server certificate '<server name>' has been removed from Trusted Servers. The UA Client Driver cannot connect to the server. 31
The endpoint '<url>' has been added to the UA Server. 31
The endpoint '<url>' has been removed from the UA Server. 31
The UA Discovery Server '<server name>' has been added. The UA Server endpoints can now register with this UA Discovery Server. 32
The UA Discovery Server '<server name>' has been removed. The UA Server endpoints can no longer register with this UA Discovery Server. 32
The endpoint '<url>' has been disabled. 32
The UA Client Driver certificate has been imported. UA servers must trust the new certificate for the client driver to connect. 32
The UA Server certificate has been imported. UA clients must trust the new certificate to connect. 32
The endpoint '<url>' has been enabled. 32
Add Trusted Client 32
Remove Trusted Client 32
Reject Trusted Client 32
Trust Trusted Client 33
Add Trusted Server 33
Remove Trusted Server 33
Reject Trusted Server 33
Trust Trusted Server 33
Add Endpoint 33
Enable an Endpoint 33
Disable an Endpoint 33
Remove Endpoint 33
Add Discovery Server 33
Remove Discovery Server 34
Reissue Client Certificate 34
Reissue Server Certificate 34
Index **35**

OPC UA Configuration Manager

Help version 1.044

CONTENTS

Overview
What is OPC Unified Architecture and how is it used?

OPC UA Configuration Manager
Where can I find information on the tabs in the OPC UA Configuration Manager?

OPC UA Tutorial
Where can I find a tutorial on how to implement OPC UA?

Connection Examples
Where can I find examples of connections and information on the best OPC UA practices?

Troubleshooting Tips
Where can I find descriptions of common troubleshooting problems?

Event Log Messages
What messages does the Event Log produce?

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 (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.

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 OPC UA Configuration Manager is a user-friendly interface through which the certificate exchange may be performed.

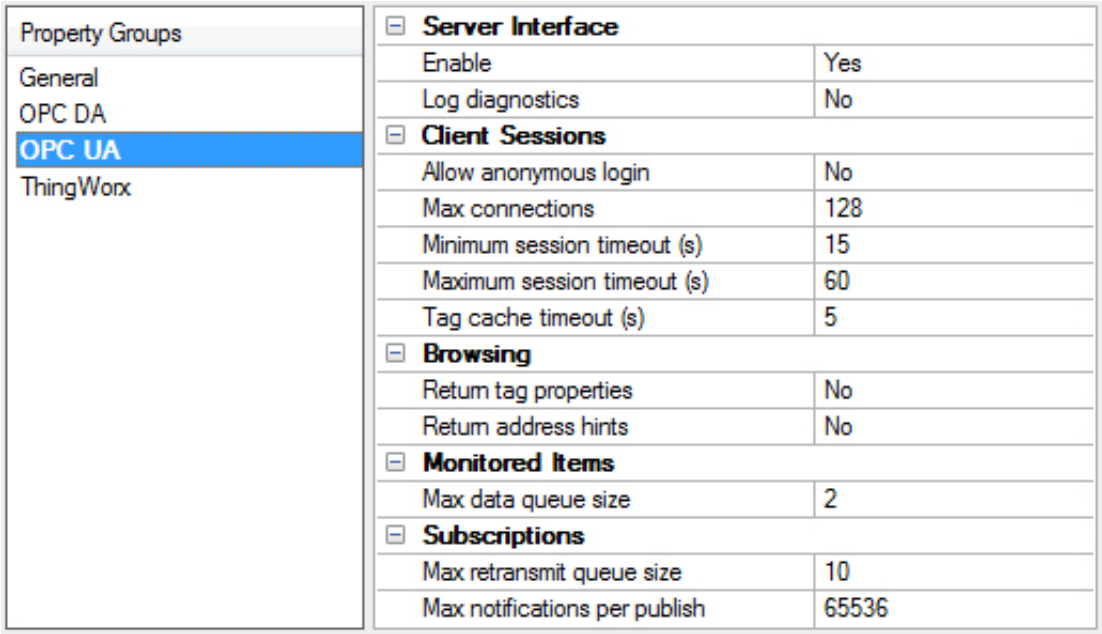
For more information on a specific OPC UA Configuration Manager property, select a link from the list below.

Server Endpoints
Trusted Clients
Discovery Servers
Trusted Servers
Instance Certificates

Project Properties — OPC UA

OPC Unified Architecture (UA) provides a platform independent interoperability standard. It is not a replacement for OPC Data Access (DA) technologies: for most industrial applications, UA complements or enhances an existing DA architecture. The OPC UA Project Properties group displays the current OPC UA settings in the server.

Note: To change a setting, click in the specific property's second column. This invokes a drop-down menu that displays the options available.



Server Interface

Enable: When enabled, the UA server interface is initialized and accepts client connections. When disabled, the remaining properties on this page are disabled.

Log diagnostics: When enabled, OPC UA stack diagnostics are logged to the OPC Diagnostics Viewer. This should only be enabled for troubleshooting purposes.

Client Sessions

Allow anonymous login: This property specifies whether or not a user name and password are required to establish a connection. For security, the default setting is No to disallow anonymous access and require credentials to log in.
Note: If this setting is disabled, users cannot login as the default user in the User Manager. Users can login as the Administrator provided that a password is set in the User Manager and is used to login.
Tip: Additional users may be configured to access data without all the permissions associated with the administrator account. When the client supplies a password on connect, the server decrypts the password using the encryption algorithm defined by the security policy of the endpoint, then uses it to login.
Note: Users can login as the Administrator using the password set during the installation of KEPServerEXOPC AggregatorTOPServerThingWorx Kepware ServerThingWorx Kepware Edge to login. Additional users may be configured to access data without all the permissions associated with the administrator account. When the client supplies a password on connect, the server decrypts the password using the encryption algorithm defined by the security policy of the endpoint, then uses it to login.
When the client supplies a password on connect, the server decrypts the password using the encryption algorithm defined by the security policy of the endpoint.

Max. connections: specify the maximum number of supported connections. The valid range is 1 to 256. The default setting is 128.

Minimum session timeout: specify the UA client's minimum timeout limit for establishing a session. Values may be changed depending on the needs of the application. The default value is 15 seconds.

Maximum session timeout: specify the UA client's maximum timeout limit for establishing a session. Values may be changed depending on the needs of the application. The default value is 60 seconds.

Tag cache timeout: specify the tag cache timeout. The valid range is 0 to 60 seconds. The default setting is 5 seconds.
Note: This timeout controls how long a tag is cached after a UA client is done using it. In cases where UA clients read / write to unregistered tags at a set interval, users can improve performance by increasing the timeout. For example, if a client is reading an unregistered tag every 5 seconds, the tag cache timeout should be set to 6 seconds. Since the tag does not have to be recreated during each client request, performance improves.

Browsing

Return tag properties: Enable to allow UA client applications to browse the tag properties available for each tag in the address space. This setting is disabled by default.

Return address hints: Enable to 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 receives 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 property is disabled. This setting is disabled by default.

Monitored Items

Max. Data Queue Size: specify the maximum number of data notifications to be queued for an item. The valid range is 1 to 100. The default setting is 2.

Note: The data queue is used when the monitored item's update rate is faster than the subscription's publish rate. For example, if the monitored item update rate is 1 second, and a subscription publishes every 10 seconds, then 10 data notifications are published for the item every 10 seconds. Because queuing data consumes memory, this value should be limited when memory is a concern.

Subscriptions

Max. retransmit queue size: specify the maximum number of publishes to be queued per subscription. The valid range is 1 to 100. A value of zero disables retransmits. The default setting is 10.

Note: Subscription publish events are queued and retransmitted at the client's request. Because queuing consumes memory, this value should be limited when memory is a concern.

Max. notifications per publish: specify the maximum number of notifications per publish. The valid range is 1 to 65536. The default setting is 65536.

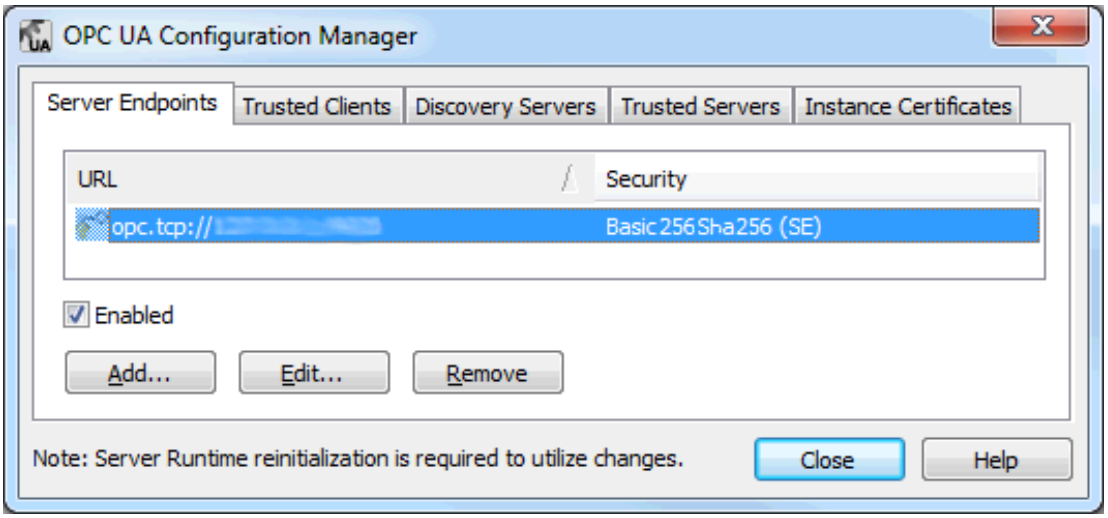
Note: This value may affect the connection's performance by limiting the size of the packets sent from the server to the client. In general, large values should be used for high-bandwidth connections and small values should be used for low-bandwidth connections.

The **Defaults** button restores the settings to the default / pre-set values.

Server Endpoints

Server Endpoint definitions are required by the OPC UA server to create a UA interface with which UA clients can communicate. UA server endpoints are defined as Universal Resource Locators (URLs) and identify the specific instance of a server, transport type, and the security with which it communicates. A server endpoint consists of one URL and one security policy type. A maximum of 100 server endpoints are allowed in the project. The Server Endpoints tab may display multiple server endpoints on one line.

Note: Each newly defined endpoint is enabled by default, but users may disable it if desired. Addition, removal, or modification of the endpoints while the server is running requires re-initialization of the UA server's Runtime.

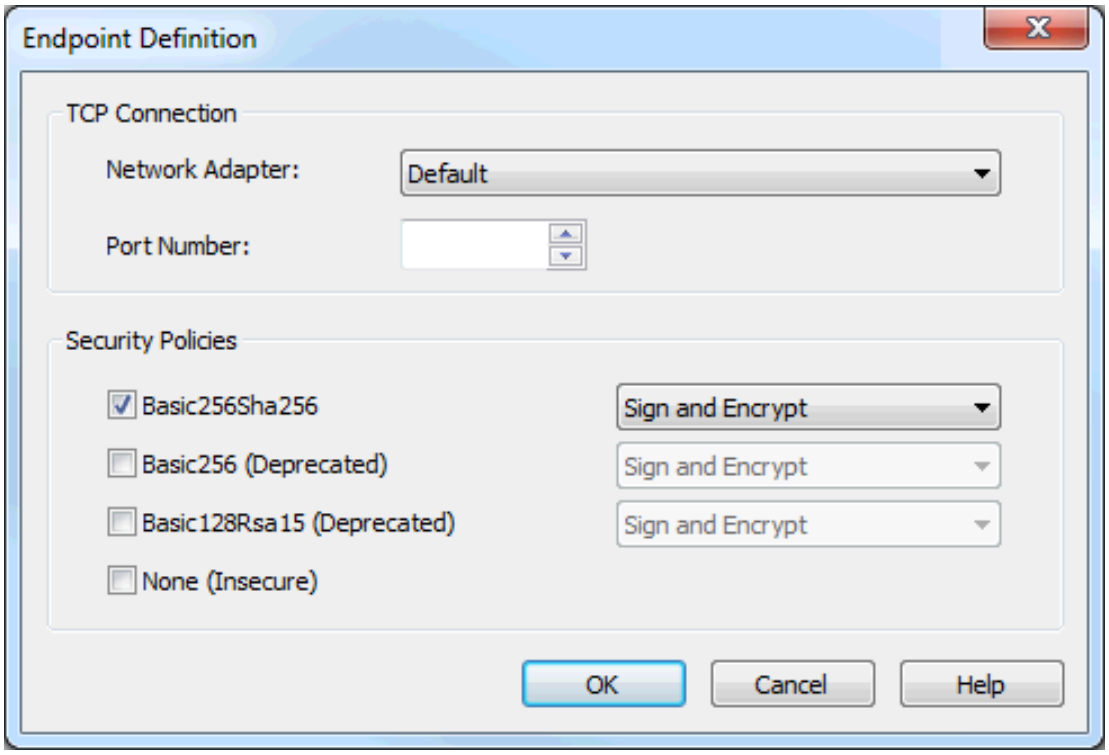


Note: All endpoints within the server instance share the same instance certificate. The UA server uses self-signed certificates by default, but users can import a custom instance in the Instance Certificates tab.

Important: In compliance with OPC UA requirements, a server implementing the Standard UA Server Profile must support user name / password login. 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.



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.
Note: Teamed NICs are not supported at this time.

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 host name 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: These security policy and message mode parameters specify the security algorithms that the UA server supports. Basic256Sha256 is selected by default. The options are as follows:

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

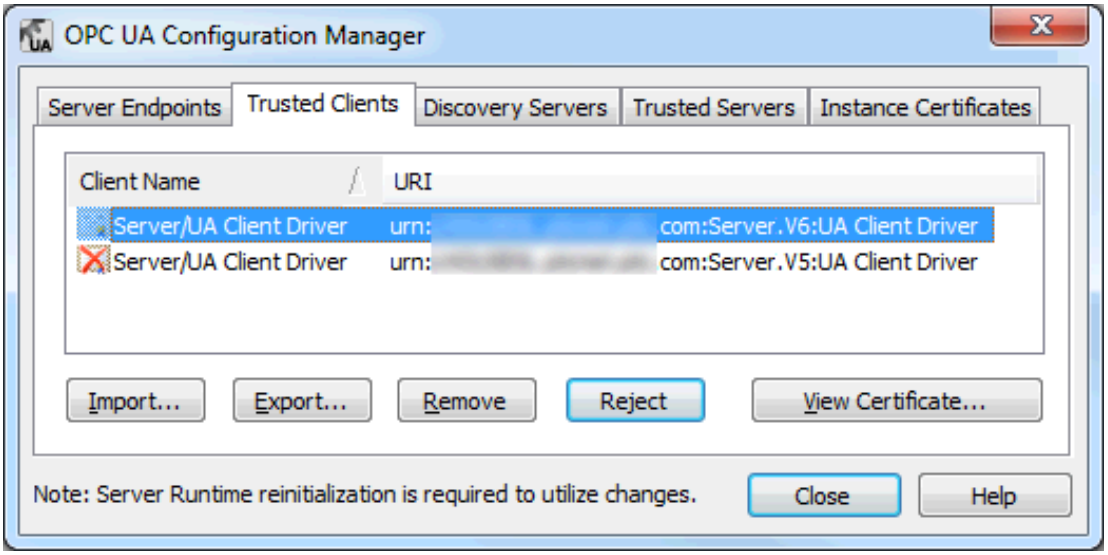
The Security Policy drop-down lists may only be accessed when the corresponding checkbox is checked. If none of the security policies are checked, the default security policy assumption is None, which does not provide protection and is not recommended. Each drop-down lists the modes of encryption of messages supported by the UA server, ordered most secure to least secure. The default selection is Sign and Encrypt. The options are as follows:

- Sign and Encrypt
- Sign; Sign and Encrypt
- Sign

CAUTION: 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 less secure and usage should be limited to providing backward compatibility.

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.



Import... When clicked, this button imports a client certificate to trust.

Export... When clicked, this button exports a trusted client certificate to a desired location.

Remove: When clicked, this button removes trust from the client certificate. It also removes the certificate from the list of Trusted Clients.

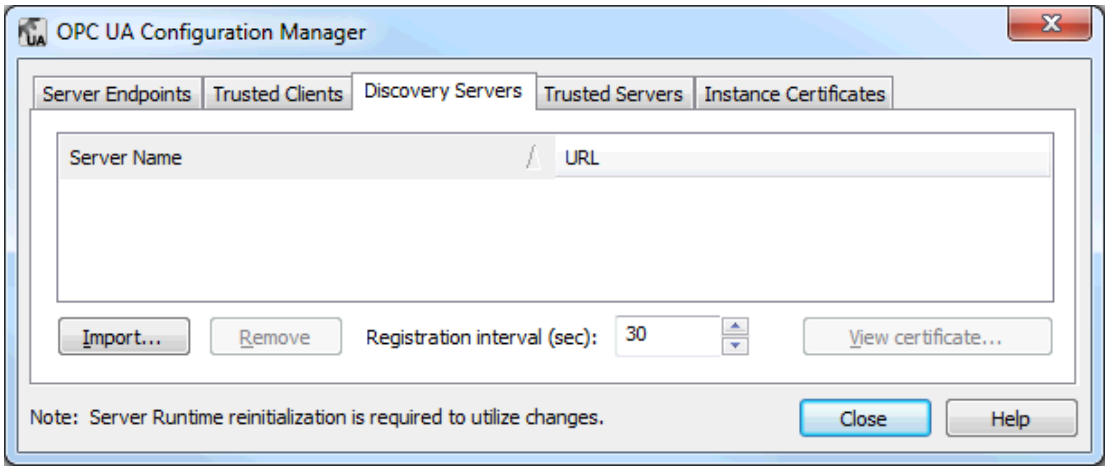
Reject: When clicked, this dynamic button removes trust from a client certificate. Rejected certificates remain in the list of Trusted Clients, marked with a red X.

Trust: When clicked, this dynamic button trusts a client certificate.

View Certificate... When clicked, this button invokes a view of the client certificate's information.

Discovery Servers

Any OPC UA server may register with a UA Discovery Server to make its endpoint information available to clients with access. 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 OPC UA Configuration Manager provides the ability to import, remove and view trusted Discovery Server endpoints that will be identified to the UA server interface.

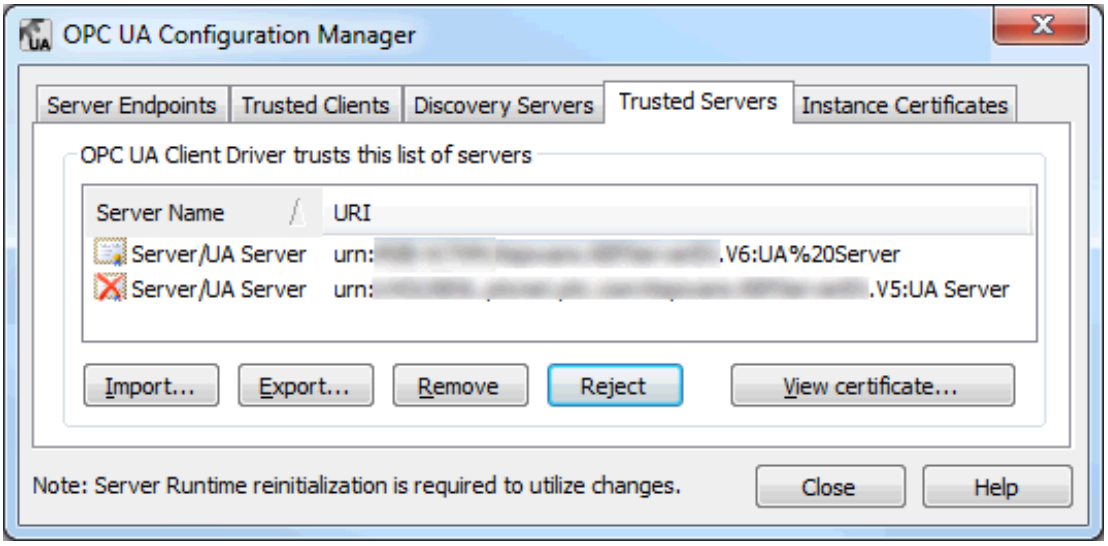


Note: Users may change the registration interval that will be used to refresh the Discovery Server through the **Registration Interval** parameter. The default setting is 30 seconds.

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.

Note: 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.



Import... When clicked, this button imports a server certificate to trust.

Export... When clicked, this button exports a trusted server certificate to a desired location.

Remove: When clicked, this button removes trust from the server certificate. It also removes the certificate from the list of Trusted Servers.

Reject: When clicked, this dynamic button removes trust from a server certificate. Rejected certificates remain in the list of Trusted Servers, marked with a red X.

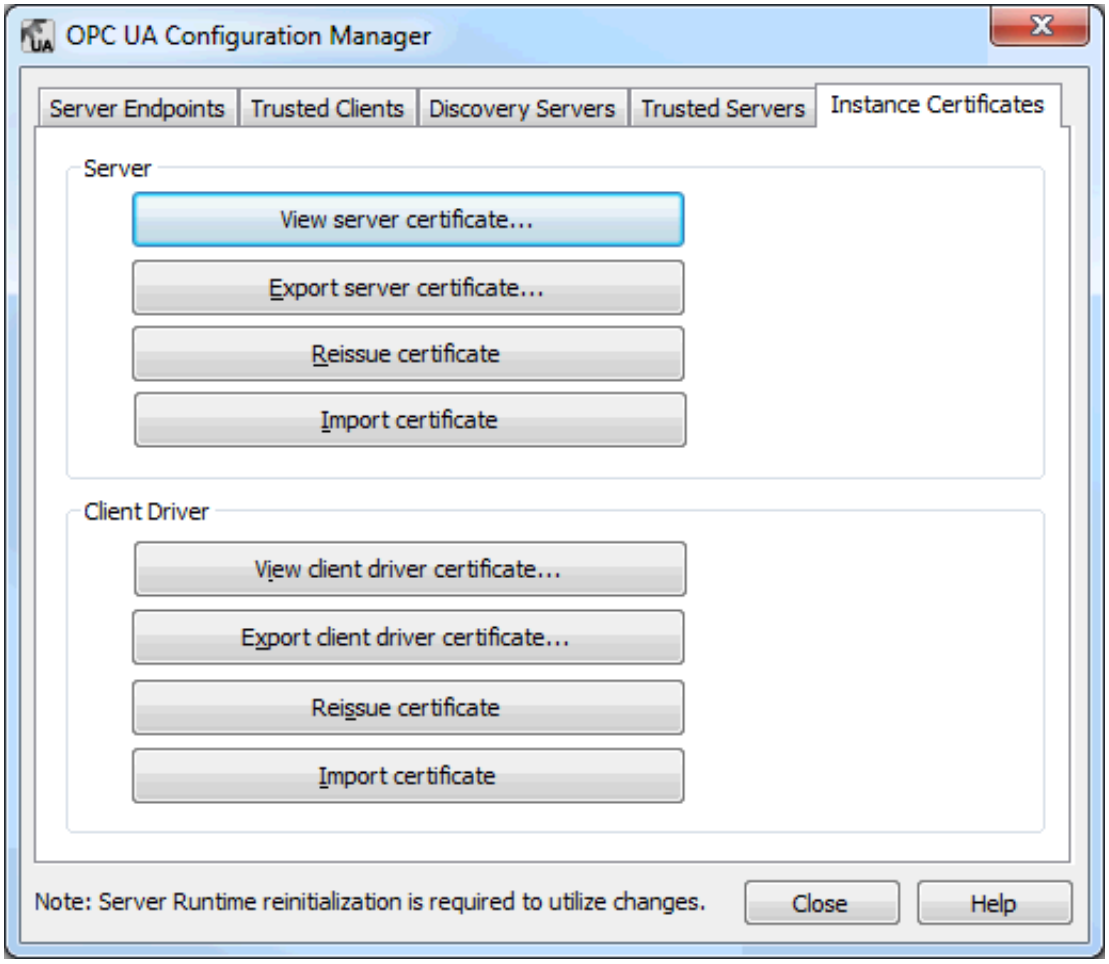
Trust: When clicked, this dynamic button trusts a server certificate.

View Certificate... When clicked, this button invokes a view of the server certificate's information.

For instructions 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.



Server

View server certificate: When clicked, this button invokes the server certificate. The dialog contains both general and detailed certificate information, in addition to the certification path. *For more information, refer to* ***Certificate Display***.

Export server certificate: When clicked, this button exports the server certificate to a desired location.

Reissue certificate: When clicked, this button reissues the server certificate. Certificates generated by the OPC UA Configuration Manager are self-signed, signed using rsa-sha256 algorithm, and expire in three years. Re-issuing invalidates any existing trust relationships.

Import certificate: When clicked, this button imports a certificate. Imported server certificates must be in PKCS12 format (which is a .pfx extension). They must contain both the instance certificate and the private key, and may be password protected.

Client

View client driver certificate: When clicked, this button invokes the client driver's certificate. The dialog contains both general and detailed certificate information, in addition to the certification path. *For more information, refer to* ***Certificate Display***.

Export client driver certificate: When clicked, this button exports the client driver's certificate to a desired location.

Reissue certificate: When clicked, this button reissues the client driver's certificate. Certificates generated by the OPC UA Configuration Manager are self-signed, signed using rsa-sha256 algorithm, and expire in three years. Re-issuing invalidates any existing trust relationships.

Import certificate: When clicked, this button imports a certificate. Imported client certificates must be in PKCS12 format (which is a .pfx extension). They must contain both the instance certificate and the private key, and may be password protected.

Default Self-Signed Certificates

File names:

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

Expiration:

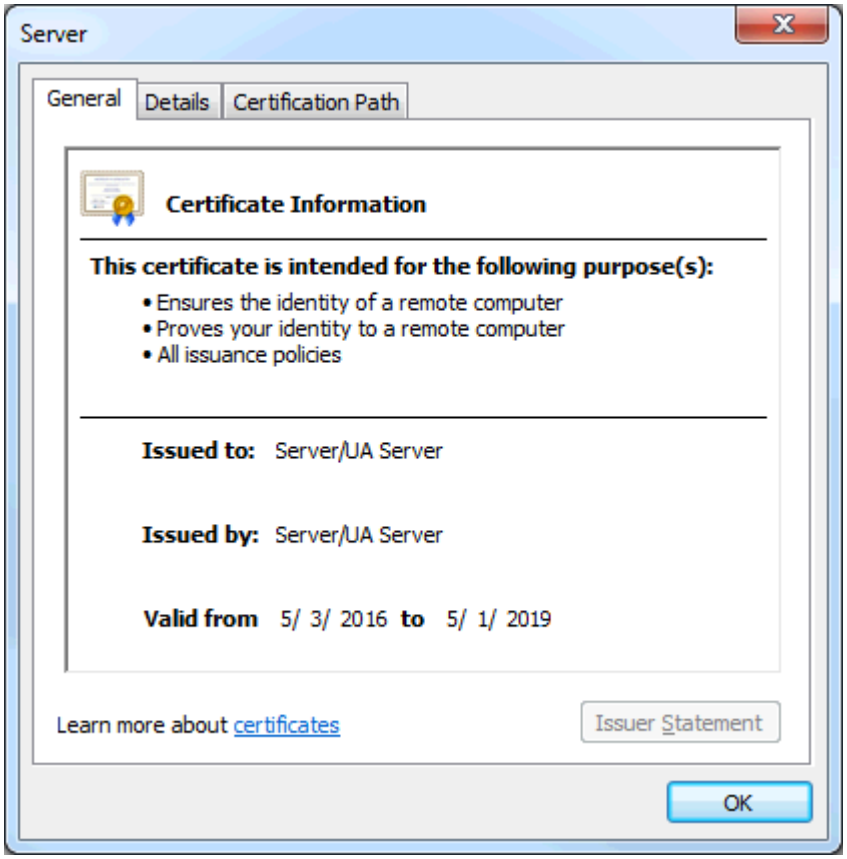
- Three (3) years from date of issue

Signing Algorithm:

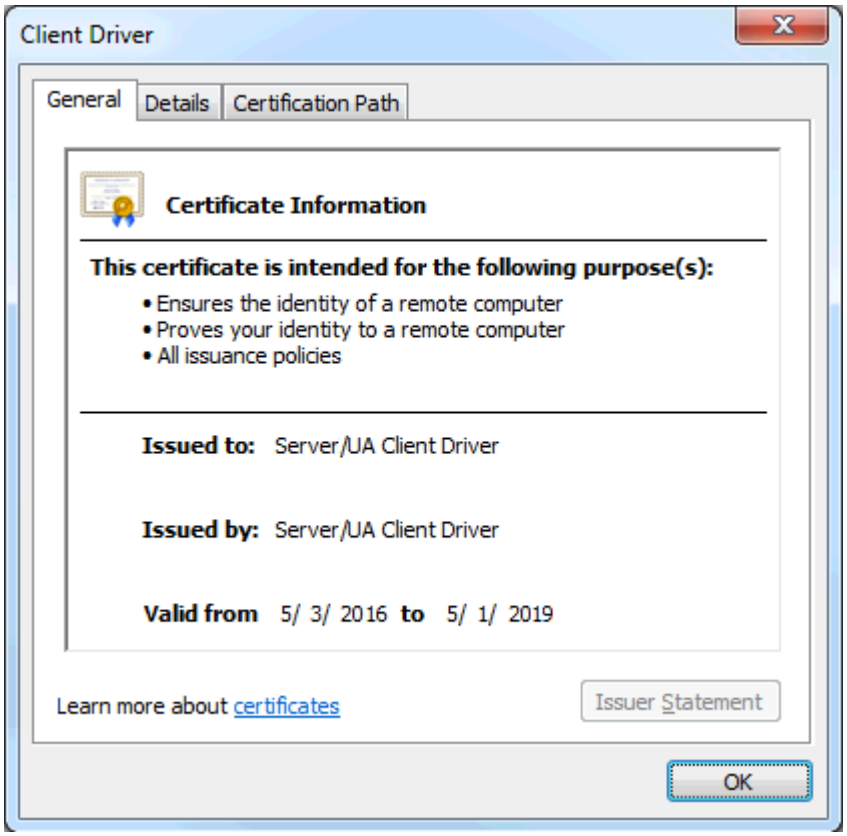
- rsa-sha256

Certificate Display

When viewing the server certificate, the dialog should appear as shown below.

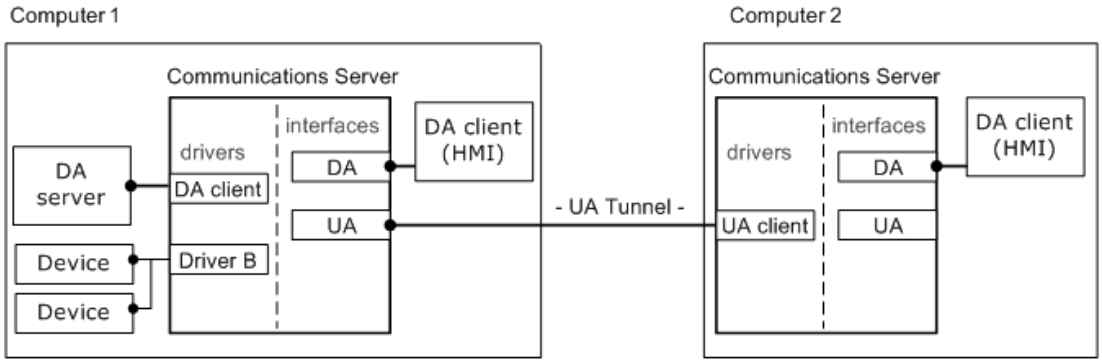


When viewing the client driver certificate, the dialog should appear as shown below.



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 to establish a secure connection. This exchange only has to be done once in the certificate's lifetime.

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 insecure connections, refer to* ***Setting up the Server***.

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

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 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. Select **OPC UA Configuration**.
2. 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. 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 Service**.

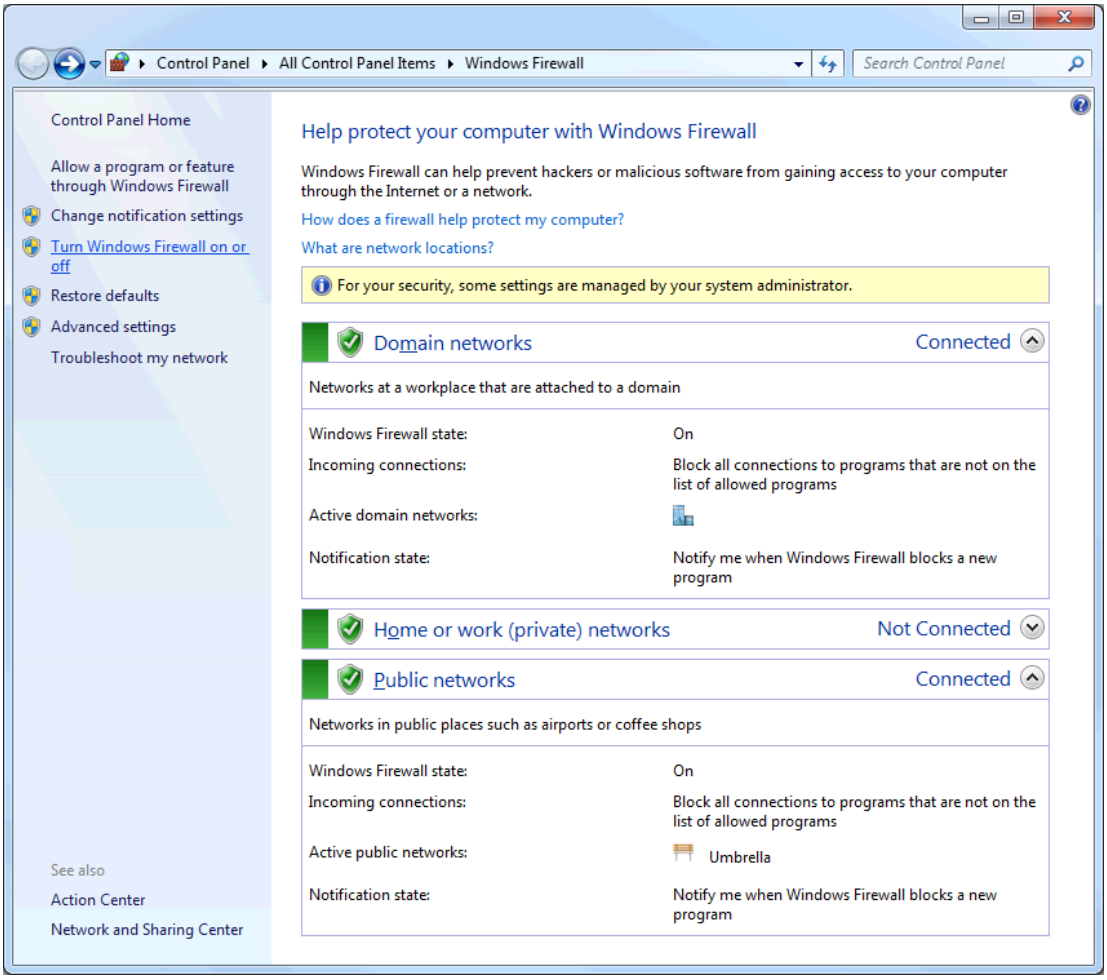
Discovery Service (Optional)
Users familiar with OPC DA may be familiar with OPCEnum, an application that runs locally on the serving computer and exposes available OPC DA servers to the clients connecting remotely. The client only needs to know the serving computer's location on the network.

A service was created that allows OPC UA servers to be discovered at a "well-known" location 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.

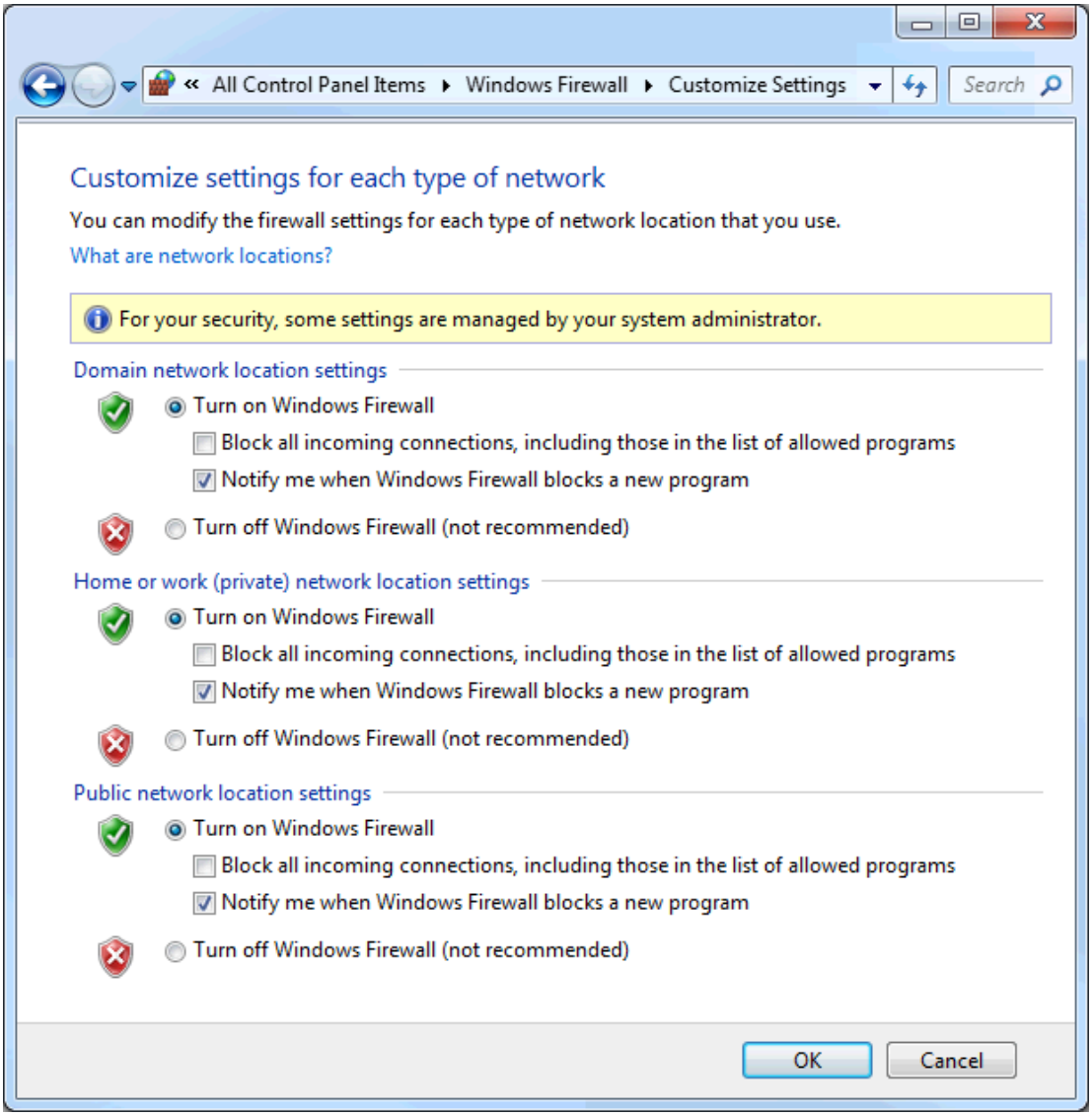
Firewall
The firewall drops incoming traffic that is not expected (called "unsolicited traffic") or traffic that does not correspond to the exceptions set within the firewall (called "excepted traffic"). Since OPC UA does not require callbacks, only the server computer needs to have the exception.

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**.

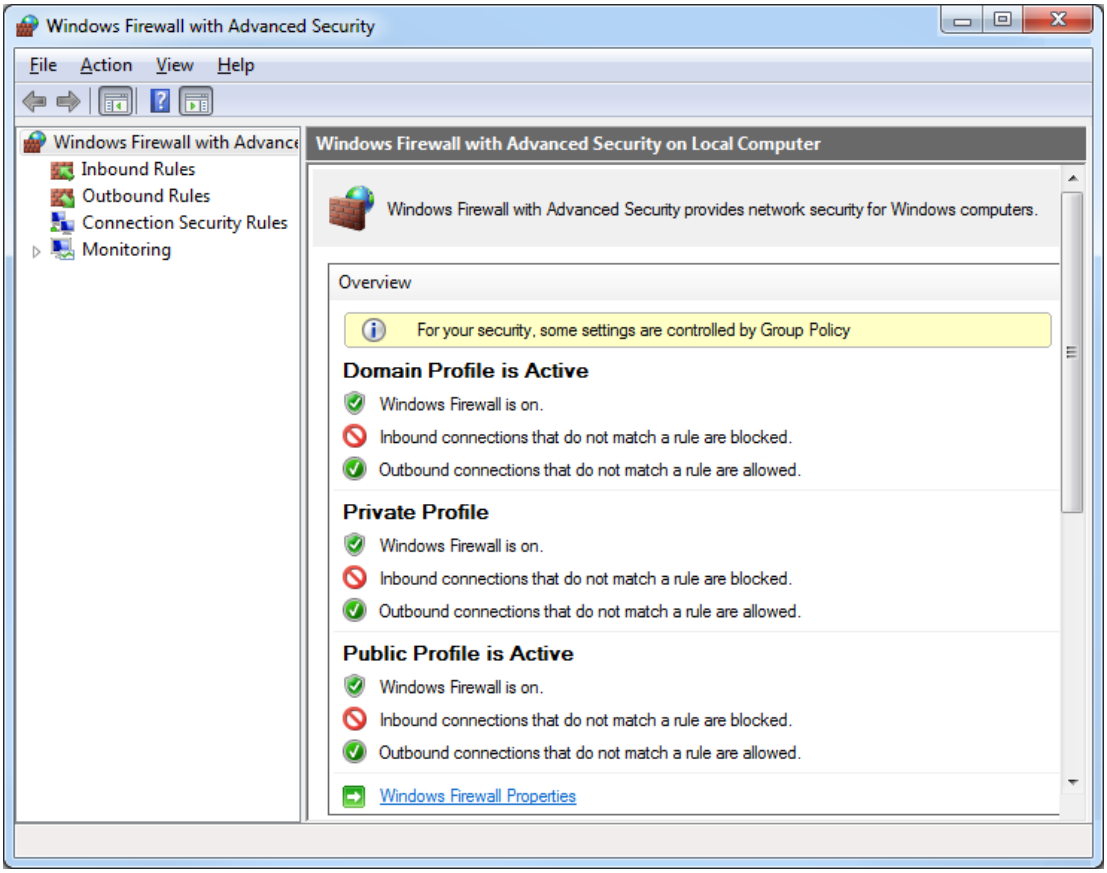

Control Panel ▸ All Control Panel Items ▸ Windows Firewall
Search Control Panel
Control Panel Home
Allow a program or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Action Center
Network and Sharing Center
Help protect your computer with Windows Firewall
Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.
How does a firewall help protect my computer?
What are network locations?
For your security, some settings are managed by your system administrator.
Domain networks
Connected
Networks at a workplace that are attached to a domain
Windows Firewall state: On
Incoming connections: Block all connections to programs that are not on the list of allowed programs
Active domain networks:
Notification state: Notify me when Windows Firewall blocks a new program
Home or work (private) networks
Not Connected
Public networks
Connected
Networks in public places such as airports or coffee shops
Windows Firewall state: On
Incoming connections: Block all connections to programs that are not on the list of allowed programs
Active public networks: Umbrella
Notification state: Notify me when Windows Firewall blocks a new program

2. Click **Turn Windows Firewall on or off**.



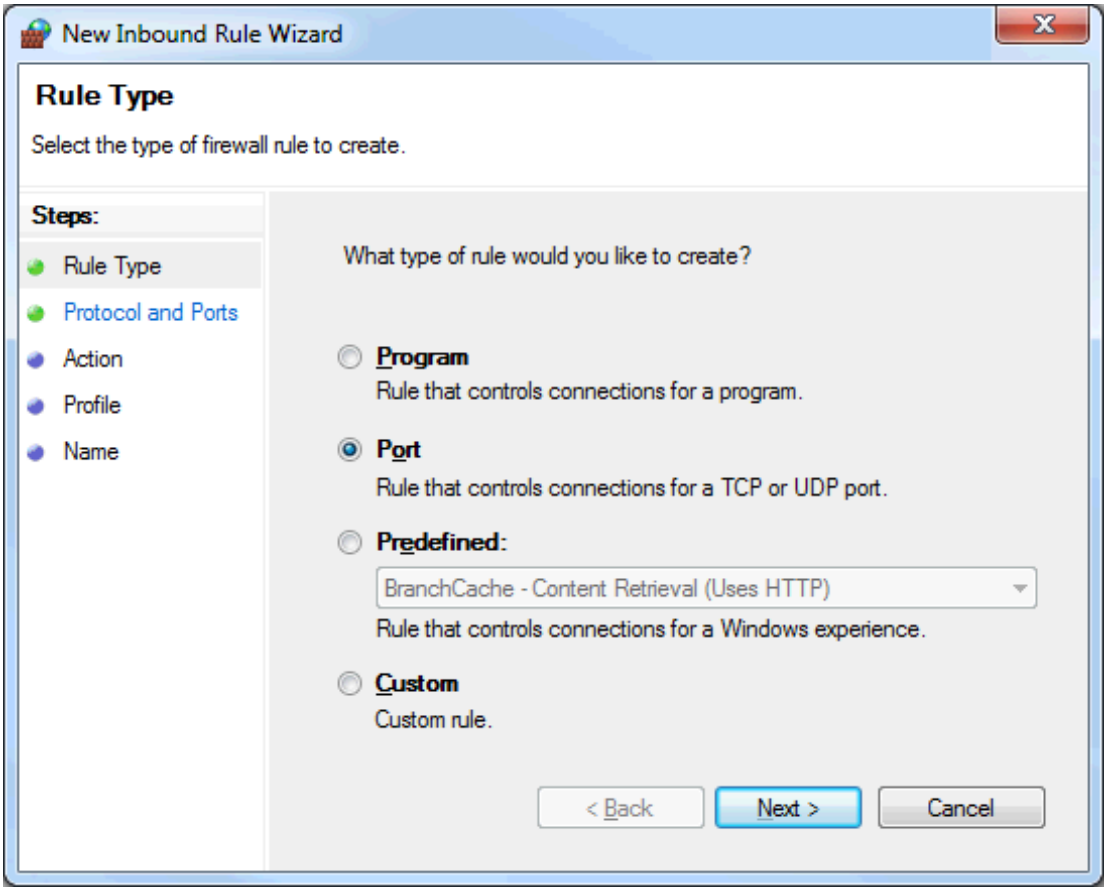
3. Verify that the firewall is enabled.

4. Click on **Advanced Settings**.

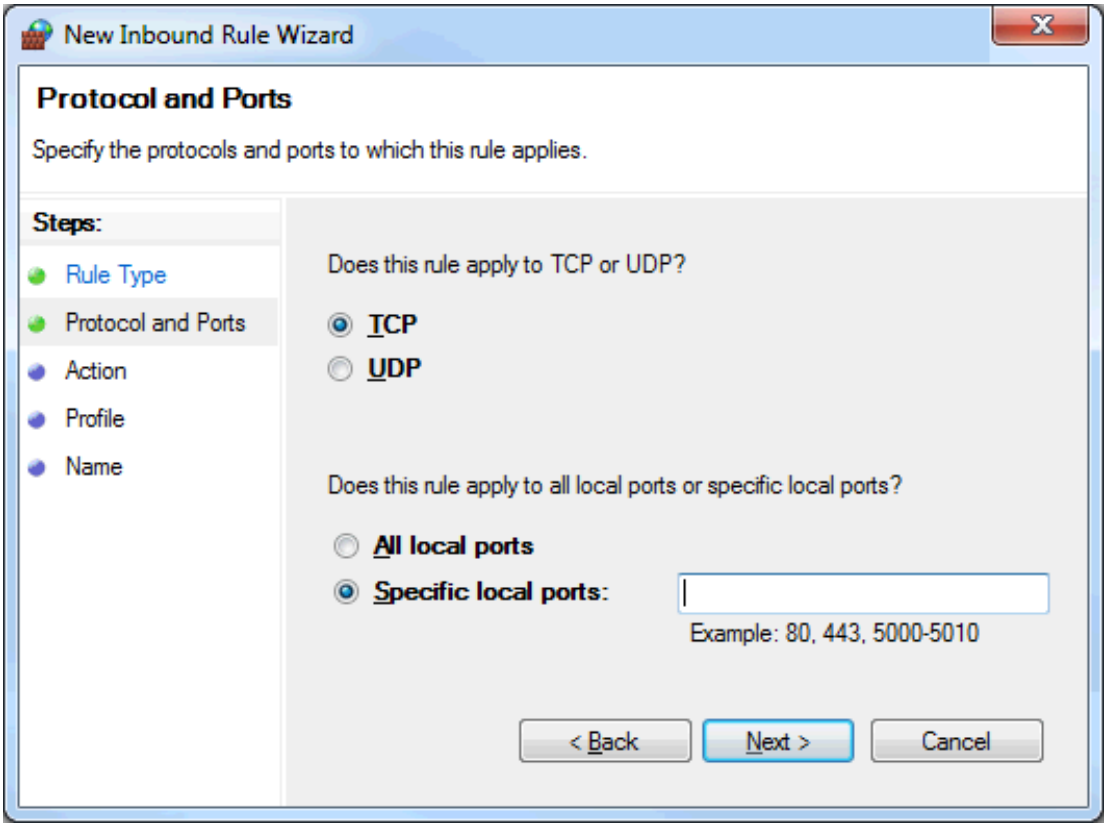


5. Click on **Windows Firewall Properties**.
6. Select **Inbound Rules** in the left pane.
7. Choose **New Rule...** in the right Actions pane.

8. For the Rule Type, select **Port**.



9. Select **Specific local port**.



10. Enter the UA endpoint assigned to the endpoint.
11. Click **Next**.
12. Verify that the correct protocol is selected. The default setting is TCP.
13. Click **OK**.
14. 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. Select **Edit** | **Connectivity**| **New Channel**.
3. In the **Select the type of channel to be created** drop-down, select **OPC UA Client** and then click **Next**.
4. In **Specify the identity of this object**, type a name for the channel and then click **Next**.
5. Keep the default settings in **Write Optimizations** by clicking **Next**.

6. In **UA Server**, manually enter the server's endpoint URL into the **Endpoint URL** field.
7. Alternatively, users can click the **Browse (...)** icon and locate it on the computer.
    a. Verify that **Use Discovery URL** is disabled.
    b. In **Discovery Port**, enter the endpoint port number that was created on the server computer. The default port number should already be assigned and match 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.
    c. If the port number was changed, click **Refresh**.
    d. Locate the server computer. Endpoints that are assigned to "localhost" will only be found under the **Local Machine** branch.
    e. Expand the computer to display a list of available servers, then expand the servers and select the correct endpoint.
    f. 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.
    g. Click **OK**. The endpoint information will appear in the UA Server page. Click **Next**.
8. Keep the default settings in **UA Session** by clicking **Next**. These can be optimized later if desired.
9. Keep the user name and password blank in **Authentication** by clicking **Next**. These may be changed as desired.
10. View the **Summary** and then click **Finish**.

OPC UA Client Device

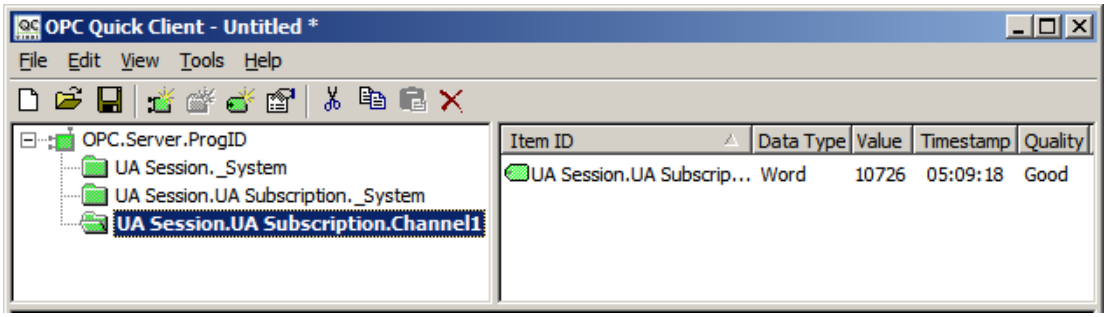
The Device Wizard guides users in setting up a subscription, and also provides a way to browse and import items from the OPC UA Server. All the items in the device will update according to the settings provided. Multiple devices can be added to the same channel to allow for different update intervals 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** | **Connectivity** | **New Device**.
2. In **Name**, type a name for the OPC UA client device and then click **Next**.
3. Keep the default settings and proceed 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 Branches** 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.



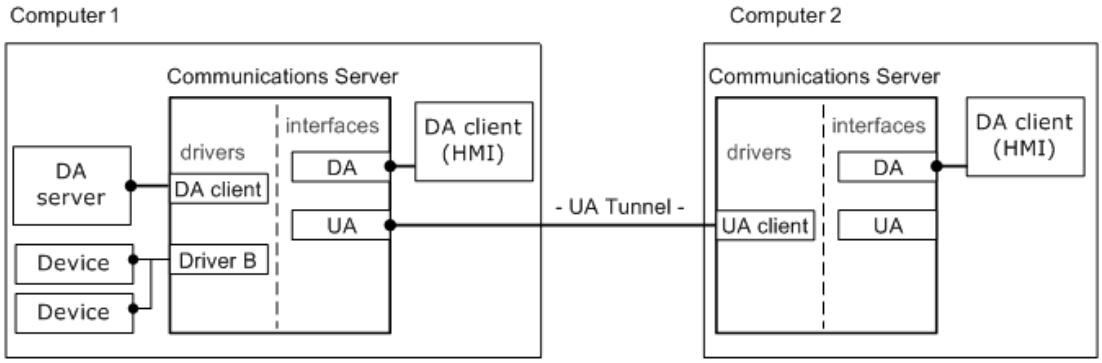
2. Browse for the items in the OPC UA channel. Then, verify that the data quality is good and that the values are updating.

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 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.

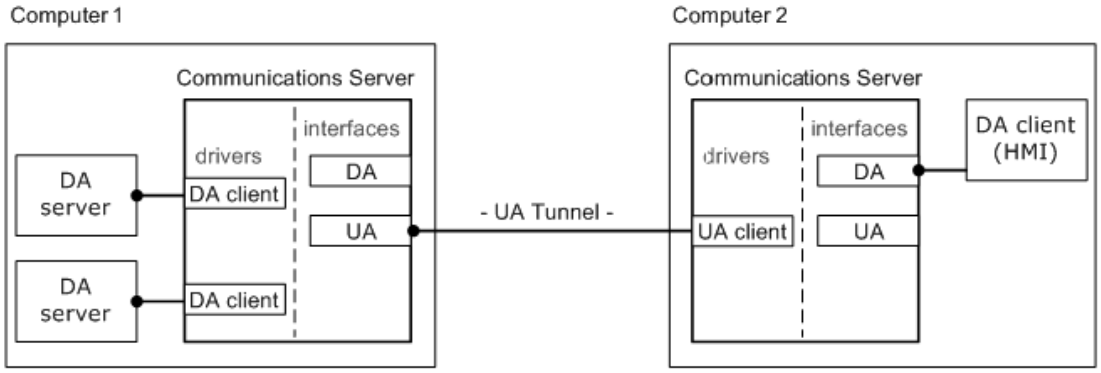
Providing Data from the Factory Floor to Remote Clients

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.



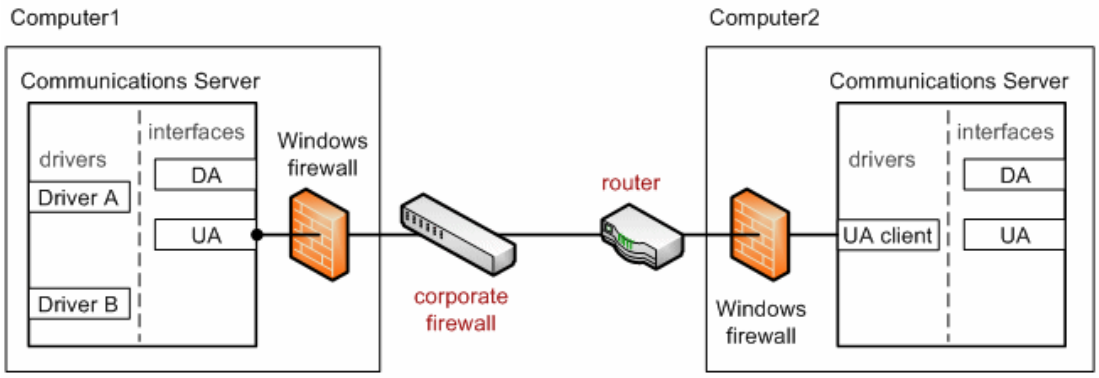
Serving Secure Aggregate Data from External DA Servers

The communications server uses the OPC DA Client Driver 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).


Computer1
Communications Server
drivers
interfaces
DA
Driver A
UA
Driver B
Windows firewall
corporate firewall
router
Computer2
Communications Server
drivers
interfaces
DA
UA client
UA
Windows firewall

Troubleshooting Tips

Click on the link for a description of the problem.

Troubleshooting Tips

Unable to connect to the UA server when trying to import items in the Device Properties dialog
Unable to see the UA server when attempting to browse from the UA client
The target computer running the UA server is not shown in the network browse from the UA client
Unable to connect to the UA server via the correct Endpoint URL
Connection attempts to the UA server require Authentication (Username and Password)
Cannot ping a router that uses port forwarding to send requests to the UA server
No UA specific error messages are posted to the Event Log

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.
3. The UA server and / or UA client certificate has a validity period before the current system date.

Solution:

1. Verify the channel UA server security profile and message mode configurations.
2. If security is not required, select "None" as the security policy in the Channel Properties dialog.
3. Perform a certificate swap.
4. Import a non-expired certificate.
5. Re-issue the certificate to generate a new non-expired certificate.

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 **Edit**| **Project Properties**, check the **OPC UA** property group for the Server Interface settings.
4. Verify that **Enable** is set to **Yes**.
5. 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. The target computer may be in a Work-group only; not in a domain.

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 for-warding 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 select Project in the tree view. In **Edit** | **Properties**, check the OPC UA property group 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 OPC UA Specific Error Messages are Posted to the Event Log

Possible Cause:

OPC UA server diagnostics are not enabled.

Solution:

Launch the server Configuration and select **Project** in the tree view. Choose **Edit**| **Project Properties**. Review the UA tab for the Server Interface and confirm that "Log diagnostics" is set to "Yes."

Event Log Messages

The following information concerns messages posted to the Event Log pane in the main user interface. Consult the OPC server help on filtering and sorting the Event Log detail view. Server help contains many common messages, so should also be searched. Generally, the type of message (informational, warning) and troubleshooting information is provided whenever possible.

Account '<name>' does not have permission to run this application.

Error Type:
Error

Possible Cause:
The current logged in user does not have adequate permissions.

Possible Solution:

1. Log in with an administrator account.
2. Contact the system administrator to verify or update permissions.
3. Verify or correct access rights to the application data directory for this application.

See Also:
Application Data (in server help) and the Application Data User Permissions section of the <a href-f="https://www.kepware.com/getattachment/6882fe00-8e8a-432b-b138-594e94f8ac88/kepserverex-secure-deployment-guide.pdf">Secure Deployment Guide

The UA Server certificate has been reissued. UA clients must trust the new certificate to connect.

Error Type:
Security

The UA Client Driver certificate has been reissued. UA servers must trust the new certificate for the client driver to connect.

Error Type:
Security

The UA Client certificate '<client name>' has been rejected. The server cannot accept connections from the client.

Error Type:
Security

The UA Client certificate '<client name>' has been trusted. The server can accept connections from the client.

Error Type:

Security

The UA Server certificate '<server name>' has been rejected. The UA Client Driver cannot connect to the server.

Error Type:
Security

The UA Server certificate '<server name>' has been trusted. The UA Client Driver can connect to the server.

Error Type:
Security

The UA Server certificate '<server name>' has been added to Trusted Servers. The UA Client Driver can now connect to the server.

Error Type:
Security

The UA Client certificate '<client name>' has been added to Trusted Clients. The UA Server can now accept connections from the client.

Error Type:
Security

The UA Client certificate '<client name>' has been removed from Trusted Clients. The UA Server cannot accept connections from the client.

Error Type:
Security

The UA Server certificate '<server name>' has been removed from Trusted Servers. The UA Client Driver cannot connect to the server.

Error Type:
Security

The endpoint '<url>' has been added to the UA Server.

Error Type:
Security

The endpoint '<url>' has been removed from the UA Server.

Error Type:
Security

The UA Discovery Server '<server name>' has been added. The UA Server endpoints can now register with this UA Discovery Server.

Error Type:
Security

The UA Discovery Server '<server name>' has been removed. The UA Server endpoints can no longer register with this UA Discovery Server.

Error Type:
Security

The endpoint '<url>' has been disabled.

Error Type:
Security

The UA Client Driver certificate has been imported. UA servers must trust the new certificate for the client driver to connect.

Error Type:
Security

The UA Server certificate has been imported. UA clients must trust the new certificate to connect.

Error Type:
Security

The endpoint '<url>' has been enabled.

Error Type:
Security

Add Trusted Client

The UA Client certificate '<certificate name>' has been added to Trusted Clients. The UA Server will now accept connections from the client.

Remove Trusted Client

The UA Client certificate '<certificate name>' has been removed from Trusted Clients. The UA Server will not accept connections from the client.

Reject Trusted Client

The UA Client certificate '<certificate name>' has been rejected. The server will not accept connections from the client.

Trust Trusted Client

The UA Client certificate '<certificate name>' has been trusted. The server will accept connections from the client.

Add Trusted Server

The UA Server certificate '<certificate name>' has been added to Trusted Servers. The UA Client Driver can now connect to the server.

Remove Trusted Server

The UA Server certificate '<certificate name>' has been removed from Trusted Servers. The UA Client Driver cannot connect to the server.

Reject Trusted Server

The UA Server certificate '<certificate name>' has been rejected. The UA Client Driver cannot connect to the server.

Trust Trusted Server

The UA Server certificate '<certificate name>' has been trusted. The UA Client Driver can connect to the server.

Add Endpoint

The endpoint '<endpoint definition>' has been added to the UA Server.

Enable an Endpoint

The endpoint '<endpoint definition>' has been enabled.

Disable an Endpoint

The endpoint '<endpoint definition>' has been disabled.

Remove Endpoint

The endpoint '<endpoint definition>' has been removed from the UA Server.

Add Discovery Server

The discovery server '<certificate name>' has been added. The UA Server endpoints will now register with this discovery server.

Remove Discovery Server

The discovery server '<certificate name>' has been removed. The UA Server endpoints will no longer register with this discovery server.

Reissue Client Certificate

The UA Client Driver certificate has been reissued. UA servers will need to trust the new certificate in order for the client driver to connect.

Reissue Server Certificate

The UA Server certificate has been reissued. UA clients will need to trust the new certificate to connect.

Index

A

Account '<name>' does not have permission to run this application. 30
Add Discovery Server 33
Add Endpoint 33
Add Trusted Client 32
Add Trusted Server 33
Anonymous 6

C

Cannot ping a router that uses port forwarding to send requests to the UA server 29
Certificate 11
Certificate Display 13
Connection attempts to the UA server require authentication (Username and Password) 29
Connection Examples 25
Credentials 6

D

Default Certificate 13
Disable an Endpoint 33
Discovery Servers 10
Discovery Service 17

E

Enable an Endpoint 33
Endpoint Definition 8
Event Log Messages 30
Export 9, 11
External DA Servers 25

F

Firewall 17, 25

H

Help Contents 4

I

Import 9, 11
Import certificate 12-13
Instance Certificates 12

L

Local Discovery Service (LDS) 17

N

Network Adapter 8
No OPC UA Specific Error Messages are Posted to the Event Log 29

O

OPC Data Access (DA) 4
OPC Foundation 4
OPC UA Configuration Manager 5
OPC UA Tutorial 15
OPC Unified Architecture (UA) 4
Overview 4

P

Password 6
Port Number 8
Prerequisites 15

Project Properties — OPC UA 5

R

Registration Interval 10
Reissue certificate 12-13
Reissue Client Certificate 34
Reissue Server Certificate 34
Reject Trusted Client 32
Reject Trusted Server 33
Remote Clients 25
Remove Discovery Server 34
Remove Endpoint 33
Remove Trusted Client 32
Remove Trusted Server 33

S

Security 6, 15
Security Policies 8
Server Endpoints 7

T

The endpoint '<url>' has been added to the UA Server. 31
The endpoint '<url>' has been disabled. 32
The endpoint '<url>' has been enabled. 32
The endpoint '<url>' has been removed from the UA Server. 31
The target computer running the UA server is not shown in the network browse from the UA client 28
The UA Client certificate '<client name>' has been added to Trusted Clients. The UA Server can now accept connections from the client. 31
The UA Client certificate '<client name>' has been rejected. The server cannot accept connections from the client. 30
The UA Client certificate '<client name>' has been removed from Trusted Clients. The UA Server cannot accept connections from the client. 31
The UA Client certificate '<client name>' has been trusted. The server can accept connections from the client. 30
The UA Client Driver certificate has been imported. UA servers must trust the new certificate for the client driver to connect. 32

The UA Client Driver certificate has been reissued. UA servers must trust the new certificate for the client driver to connect. 30

The UA Discovery Server '<server name>' has been added. The UA Server endpoints can now register with this UA Discovery Server. 32

The UA Discovery Server '<server name>' has been removed. The UA Server endpoints can no longer register with this UA Discovery Server. 32

The UA Server certificate '<server name>' has been added to Trusted Servers. The UA Client Driver can now connect to the server. 31

The UA Server certificate '<server name>' has been rejected. The UA Client Driver cannot connect to the server. 31

The UA Server certificate '<server name>' has been removed from Trusted Servers. The UA Client Driver cannot connect to the server. 31

The UA Server certificate '<server name>' has been trusted. The UA Client Driver can connect to the server. 31

The UA Server certificate has been imported. UA clients must trust the new certificate to connect. 32

The UA Server certificate has been reissued. UA clients must trust the new certificate to connect. 30

Troubleshooting Tips 27

Trust 9

Trust Trusted Client 33

Trust Trusted Server 33

Trusted Clients 9

Trusted Servers 10

U

Unable to connect to the UA server via the correct Endpoint URL 28

Unable to connect to the UA server when trying to import items in the Device Properties dialog 27

Unable to see the UA server when attempting to browse from the UA client 27

V

Verification 23

View Certificate 9