OPC Unified Architecture - Connectivity Guide

January, 2010
Ref. 01.02

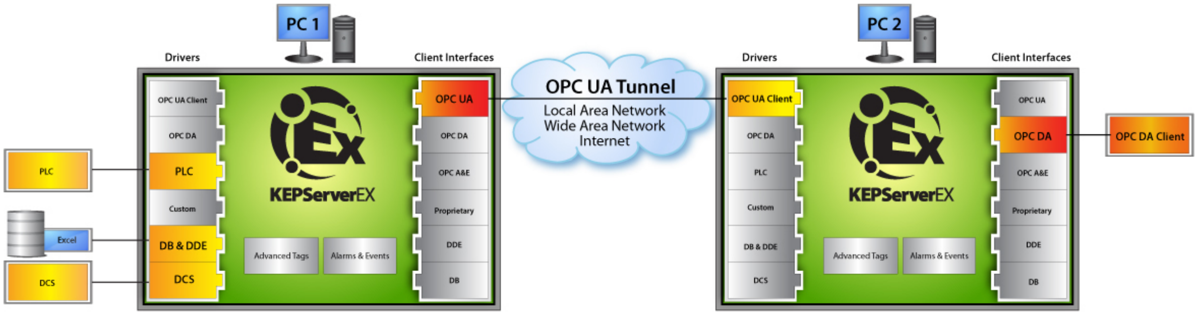
Table of Contents

1. Overview

The idea of setting up a remote OPC connection can even bring fear to those who are vastly familiar with DCOM and classic remote OPC. Out of desperation, it may even be common practice to disable firewalls and also expose the computer to unauthorized or anonymous users. Even if a firewall is in place, DCOM requires that port 135 be added to the exception list by default. This port is used for Microsoft's Remote Procedure Call and has been the target of many malicious attacks. So how can a safe and secure remote OPC connection be established?

The solution comes in the form of a new specification known as OPC Unified Architecture (OPC UA). OPC UA does not require callbacks and the use of DCOM for remote connections. This greatly simplifies firewall configuration and completely eliminates the headache known as DCOM.

The OPC Tunnel is not a product in itself, but rather a feature that is created out of existing components that are available. The tunnel requires the same client-server architecture as any OPC product; however, the client and server both need to have OPC UA support. In this case, it happens that the client and the server are part of the same product package.



The OPC UA server is packaged in with the OPC DA, native interface and, in some cases, DDE servers. By default, the OPC UA server is running and waiting for local connections immediately after the product has been installed. Minor configuration changes are required to allow remote connections. The OPC UA client is actually a driver channel that can be added along with any other device channel. If required, an OPC UA client and an OPC UA server can both be running on the same computer and be sharing data with a remote computer with the same configuration. The result is a connection between two remote servers with the ability to easily share items in a secure way.

2. Prerequisites

Install the server application on the client computer and include OPC UA Client on the Select Features page under Communication Drivers.

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

Some situations are going to 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.

3. Security

In place 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. In order to establish a secure connection between a client and the server, their certificates must first be "swapped" and also "trusted". The swap is only required to be done once for the lifetime of the certificate.

There are a few options when deciding how to swap certificates: automatic, exchange, and manual. The **automatic** trust can be established during runtime when the client first attempts to connect to the server. Several UA client and server applications support this feature and most present a dialog requesting that the user trust or reject the incoming certificate. Because the Runtime doesn't interact with the desktop, an extra step may be required on the server to "Trust" the certificate once it has been swapped. The **exchange** is preformed from the client side and only takes an instant to complete; 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** method consists of exporting and importing a certificate file on each computer using removable media or another form of file transfer for the exchange to take place. The manual process also allows for swapping certificates between client and server applications that do not support automatic exchange.

If security is not necessary, the certificate swap can be skipped. The level of security is set by the server when defining the endpoints. If **None, None** is selected as the a **Security Policy**, certificates are not checked for validation. For unsecure connections, move on to Setting up the Server.

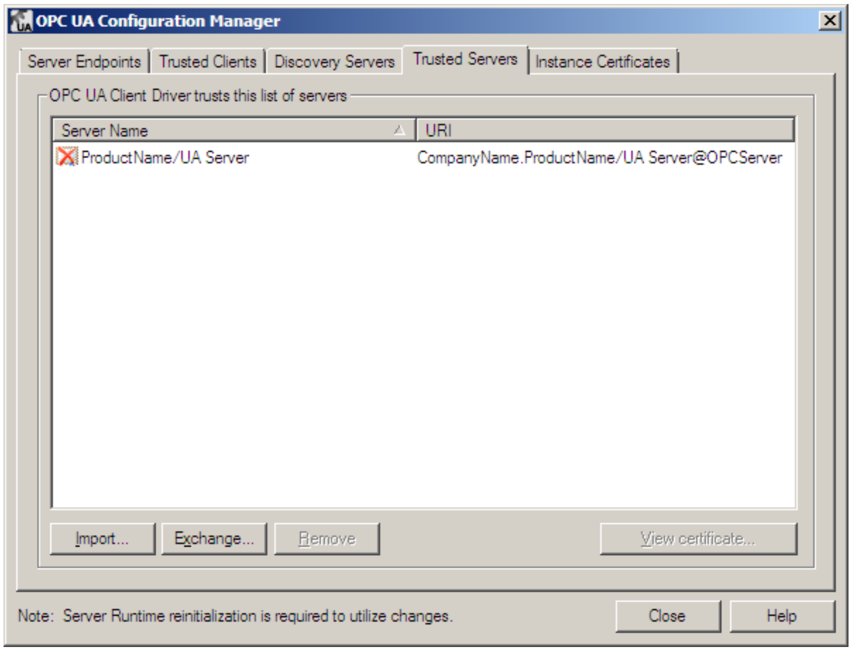
3.1 Automatic

The automatic swapping of the certificates only happens when it is required. For instance, adding an OPC UA Client channel and selecting a secure server endpoint will prompt the user to allow the server to be trusted. Once a device is added to the OPC UA Client and user attempts to import items, the server will first need to trust the client. By design, this server cannot post a dialog to the desktop so a method of trusting swapped certificates was implemented.

First, let's assume the project was already configured for this application's own client and server. The client has attempted to connect for the first time so the certificates have swapped, but are not yet trusted.

1. Right-click on the **Administration** icon and select **OPC UA Configuration**.

2. View the Trusted Servers tab.



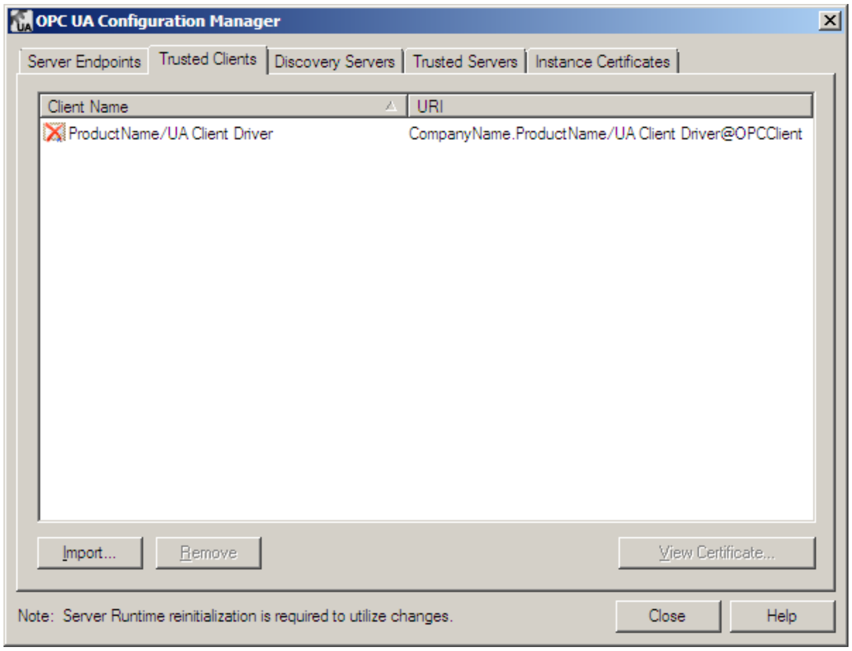
OPC UA Client Driver trusts this list of servers

Server Name	URI
☒ ProductName/UA Server	CompanyName.ProductName/UA Server@OPCServer

Note: Server Runtime reinitialization is required to utilize changes.

3. If the server's certificate appears with a red 'X' it is also not yet trusted. Right-click on the certificate and select **Trust**.

4. View the Trusted Clients tab.



Client Name	URI
☒ ProductName/UA Client Driver	CompanyName.ProductName/UA Client Driver@OPCClient

Note: Server Runtime reinitialization is required to utilize changes.

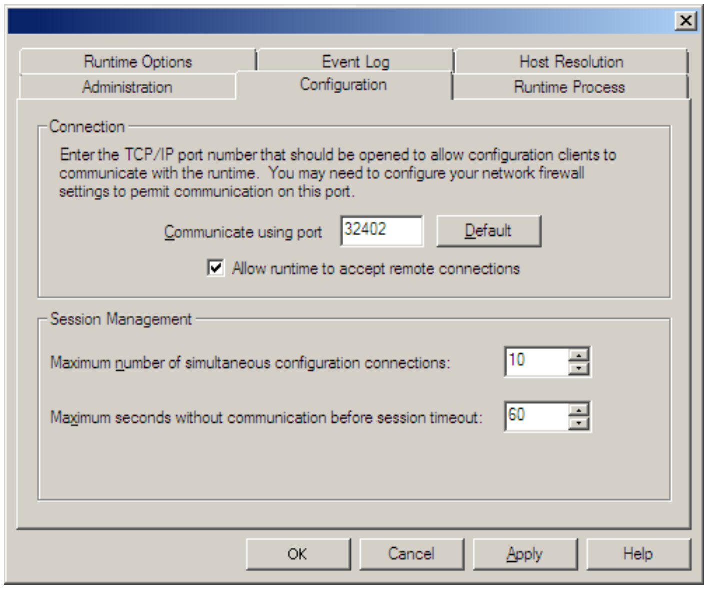
5. If the client's certificate appears with a red 'X' it is not yet trusted. Right-click on the certificate and select **Trust**.

3.2 Exchange

1. Right-click on the **Administration** icon, select **Settings** and choose the **Configuration** tab.

2. Enable remote configuration by checking **Allow runtime to accept remote connections**. The change will only be applied when the Configuration

interface is shutdown since it is using the same port to configure the Runtime locally.



Connection

Enter the TCP/IP port number that should be opened to allow configuration clients to communicate with the runtime. You may need to configure your network firewall settings to permit communication on this port.

Communicate using port: 32402

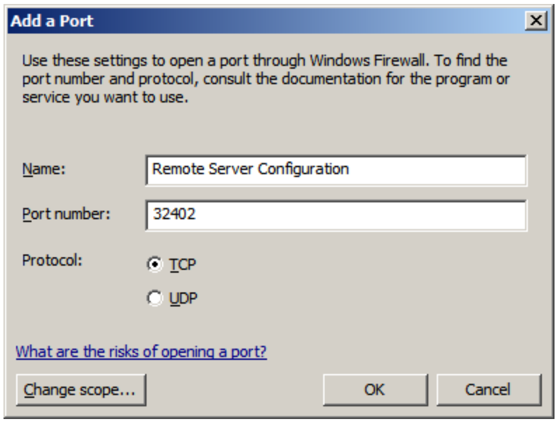
☑ Allow runtime to accept remote connections

Session Management

Maximum number of simultaneous configuration connections: 10

Maximum seconds without communication before session timeout: 60

3. Add an exception to the windows firewall for port that is specified in **Communicate using port** property on the **Configuration** tab. Another option is to temporarily turn off the firewall before the exchange is performed and return the firewall back to its secure state when the process is complete. This method also prevents unauthorized users from exchanging certificates in the future.



Add a Port

Use these settings to open a port through Windows Firewall. To find the port number and protocol, consult the documentation for the program or service you want to use.

Name: Remote Server Configuration

Port number: 32402

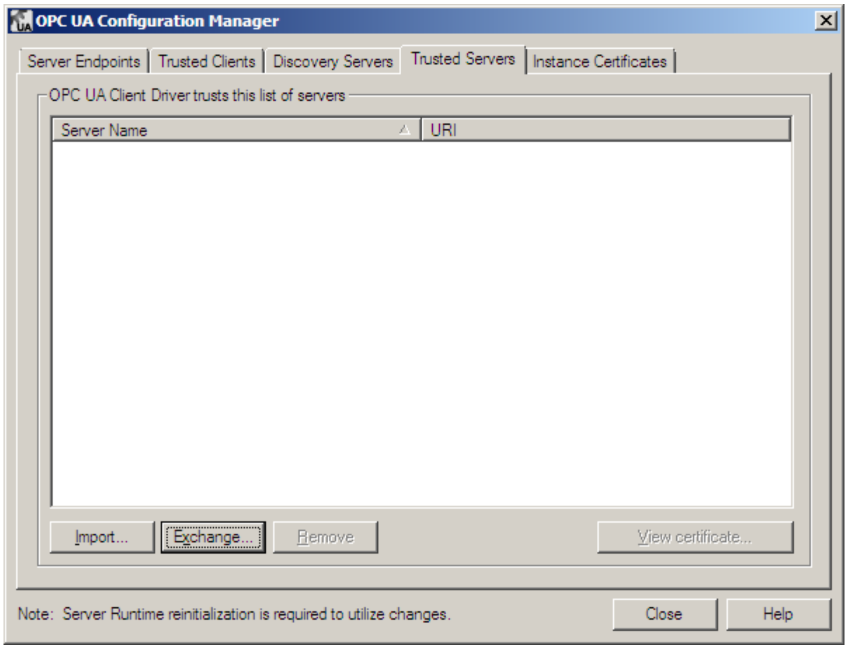
Protocol: ● TCP ○ UDP

What are the risks of opening a port?

4. Enable the exception in the windows firewall for **File and Printer Sharing**.

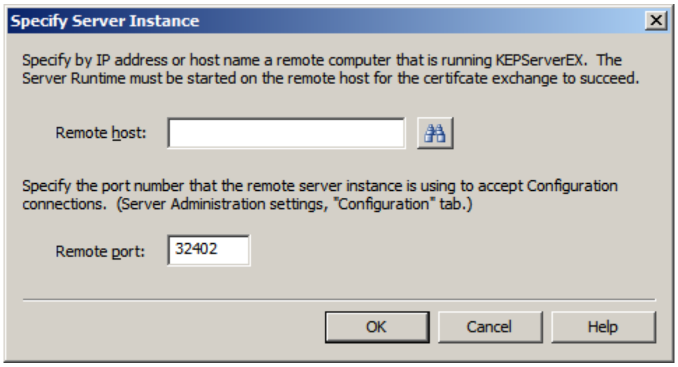
5. From the client computer, launch the **OPC UA Configuration Manager** by right-clicking on the **Administration** icon and selecting **OPC UA Configuration**.

6. Select the **Trusted Servers** tab.



Note: Server Runtime reinitialization is required to utilize changes.

7. Select **Exchange**.



Specify by IP address or host name a remote computer that is running KEPServerEX. The Server Runtime must be started on the remote host for the certifcate exchange to succeed.

Remote host:

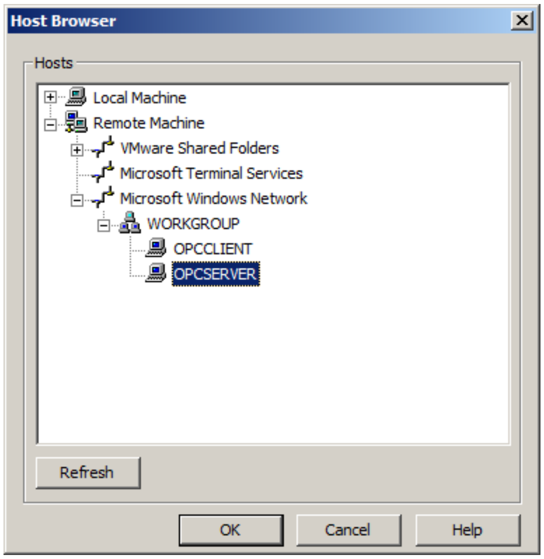
Specify the port number that the remote server instance is using to accept Configuration connections. (Server Administration settings, "Configuration" tab.)

Remote port: 32402

8. When the **Server Instance** dialog appears, click the **Browse** icon to the right of the **Remote host** field. Some newer operating systems will be required to have discovery and file sharing enabled.

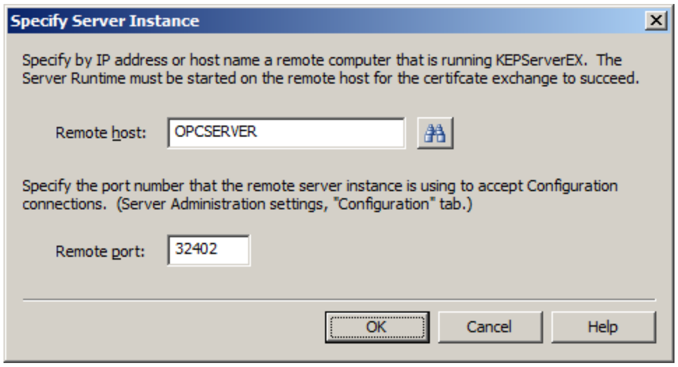
9. Browse to the server by navigating the tree.

10. Select the **computer name** and select **OK**.



Host Browser

11. Verify that the correct port is identified in the **Remote port** field. This value should be the same as what was viewed on the server computer when the exception was made to the firewall. This port is used for remote configuration of the server.



Specify Server Instance

Specify by IP address or host name a remote computer that is running KEPServerEX. The Server Runtime must be started on the remote host for the certifcate exchange to succeed.

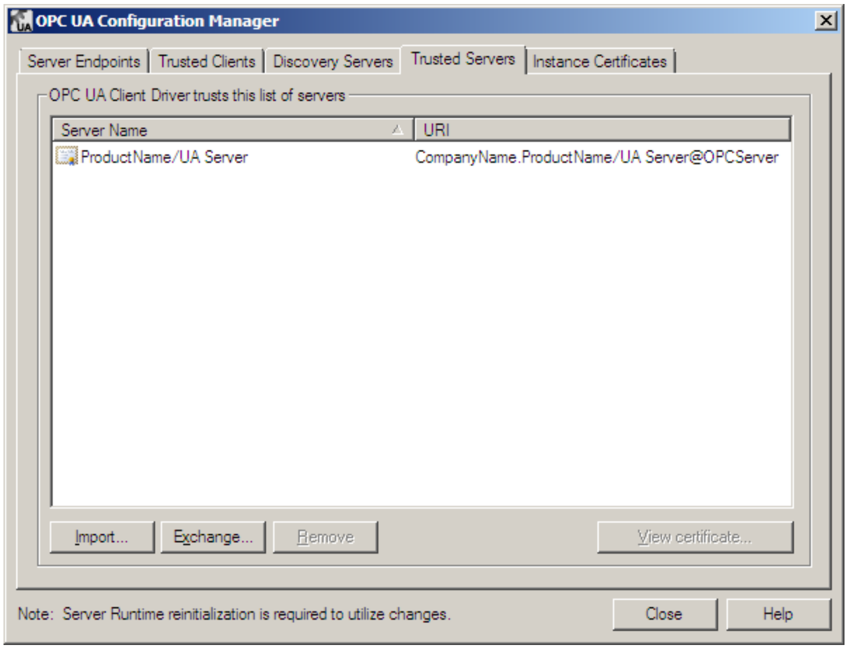
Remote host: OPCSERVER

Specify the port number that the remote server instance is using to accept Configuration connections. (Server Administration settings, "Configuration" tab.)

Remote port: 32402

12. Select **OK**.

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



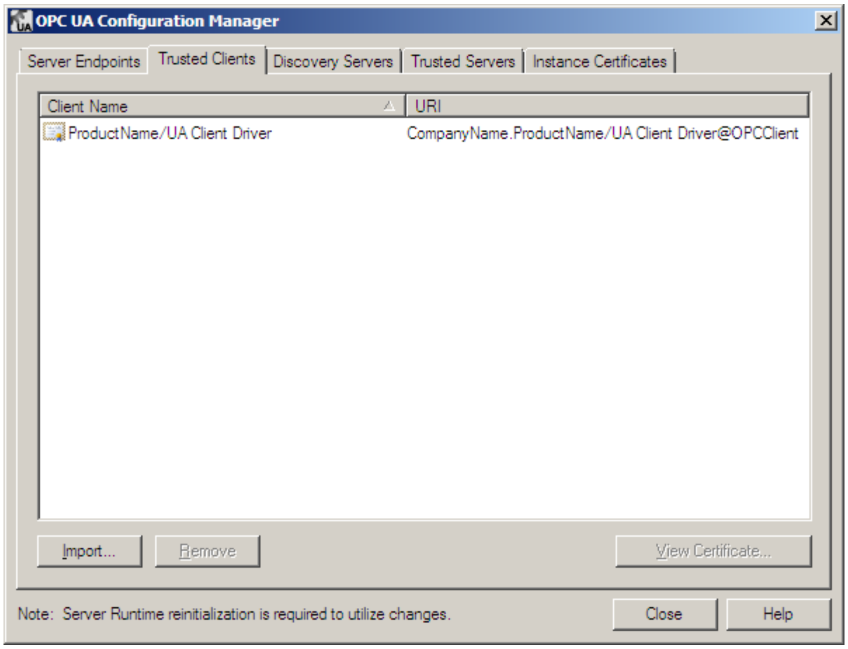
OPC UA Configuration Manager

OPC UA Client Driver trusts this list of servers

Server Name	URI
ProductName/UA Server	CompanyName.ProductName/UA Server@OPCServer

Note: Server Runtime reinitialization is required to utilize changes.

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



OPC UA Configuration Manager

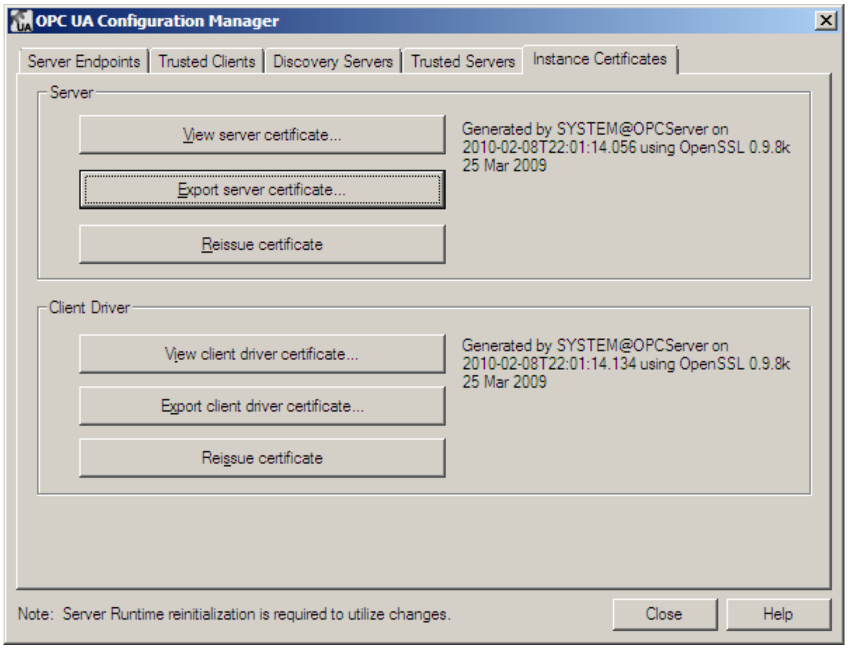
Client Name	URI
ProductName/UA Client Driver	CompanyName.ProductName/UA Client Driver@OPCClient

Note: Server Runtime reinitialization is required to utilize changes.

3.3 Manual

1. Launch the **OPC UA Configuration Manager** on the server computer by right-clicking on the **Administration** icon and selecting **OPC UA Configuration**.

2. Select the **Instance Certificate** tab.

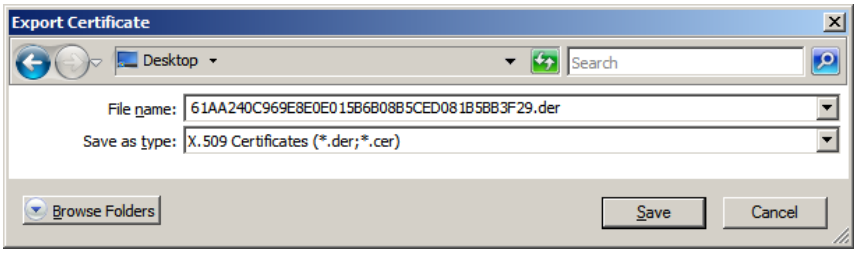

OPC UA Configuration Manager
Server Endpoints
Trusted Clients
Discovery Servers
Trusted Servers
Instance Certificates
Server
View server certificate...
Export server certificate...
Reissue certificate
Client Driver
View client driver certificate...
Export client driver certificate...
Reissue certificate
Close
Help

Generated by SYSTEM@OPCServer on 2010-02-08T22:01:14.056 using OpenSSL 0.9.8k 25 Mar 2009

Generated by SYSTEM@OPCServer on 2010-02-08T22:01:14.134 using OpenSSL 0.9.8k 25 Mar 2009

Note: Server Runtime reinitialization is required to utilize changes.

3. Under the **Server** group, select **Export server certificate**.
4. Select a location for the certificate file so that it can be easily located. The default file name is the thumbprint that identifies the certificate, but it may be changed to make managing the files easier.

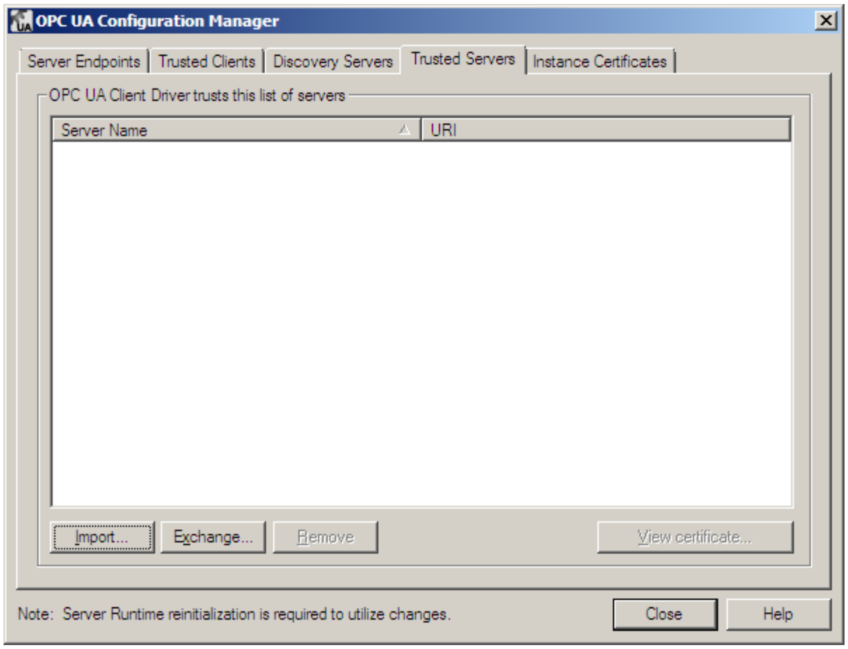


File name: 61AA240C969E8E0E015B6B08B5CED081B5BB3F29.der

Save as type: X.509 Certificates (*.der;*.cer)

5. Manually copy the server certificate file from the server computer and move it onto the client computer.
6. Launch the **OPC UA Configuration Manager** on the client computer.

7. Select the **Trusted Servers** tab.

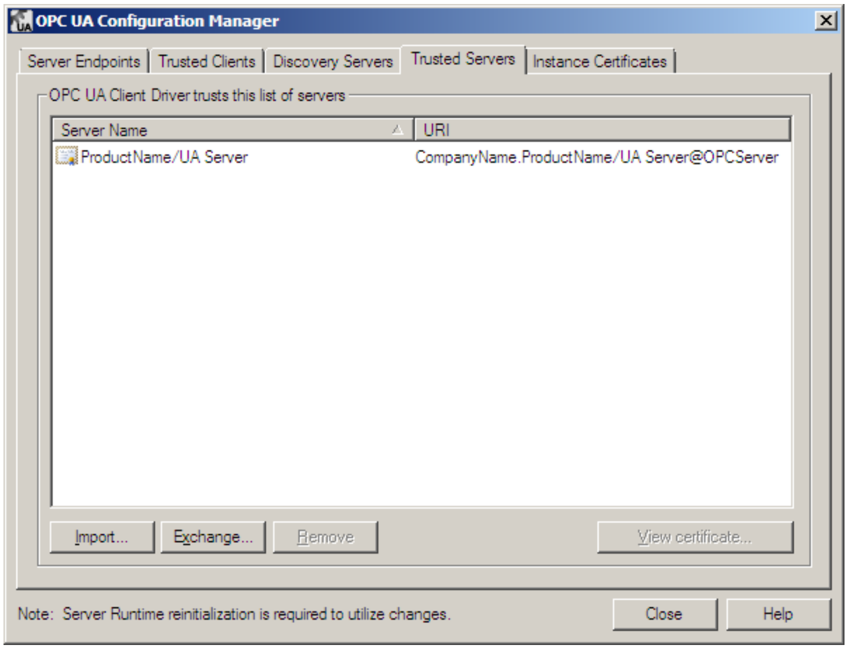


Note: Server Runtime reinitialization is required to utilize changes.

8. Select **Import** and locate the server certificate file.

9. Select **Open**.

10. The server certificate should appear in the **Trusted Servers** window and can be identified by the **URI**.

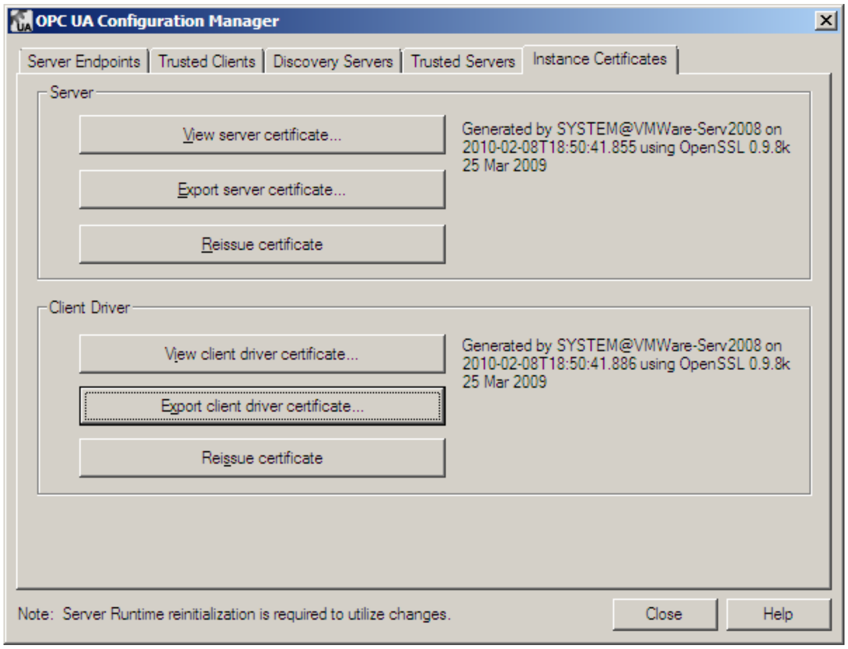


Server Name	URI
ProductName/UA Server	CompanyName.ProductName/UA Server@OPCServer

Note: Server Runtime reinitialization is required to utilize changes.

11. Select the **Instance Certificate** tab.

12. Under the **Client Driver** group, select **Export client driver certificate**.

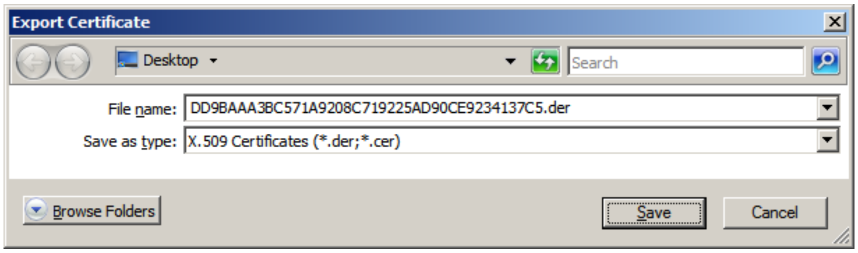

OPC UA Configuration Manager
Server Endpoints
Trusted Clients
Discovery Servers
Trusted Servers
Instance Certificates
Server
View server certificate...
Export server certificate...
Reissue certificate
Client Driver
View client driver certificate...
Export client driver certificate...
Reissue certificate
Close
Help

Generated by SYSTEM@VMWare-Serv2008 on 2010-02-08T18:50:41.855 using OpenSSL 0.9.8k 25 Mar 2009

Generated by SYSTEM@VMWare-Serv2008 on 2010-02-08T18:50:41.886 using OpenSSL 0.9.8k 25 Mar 2009

Note: Server Runtime reinitialization is required to utilize changes.

13. Select a location for the certificate file so that it can be easily located. Again, the file name can be changed if desired.



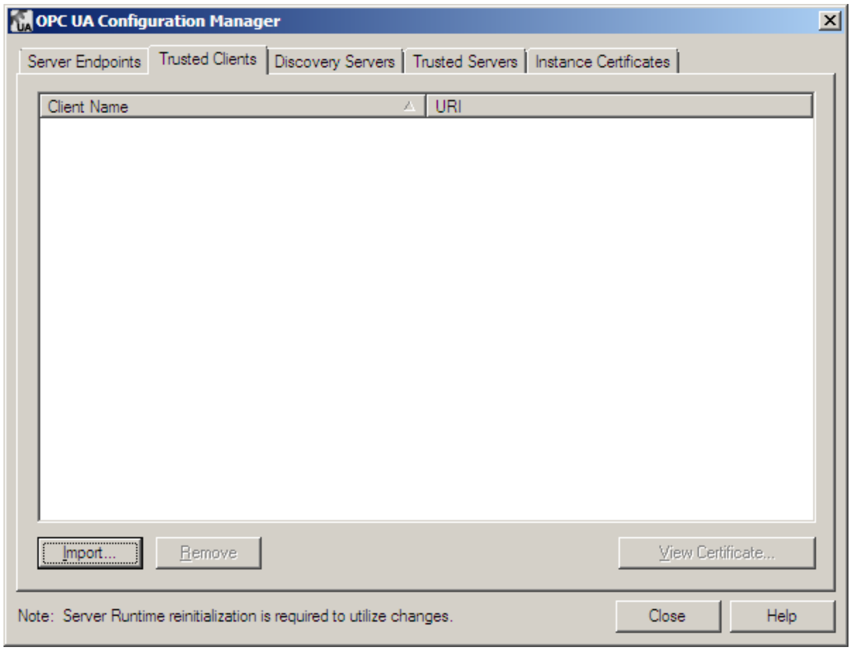
File name: DD9BAAA3BC571A9208C719225AD90CE9234137C5.der

Save as type: X.509 Certificates (*.der;*.cer)

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

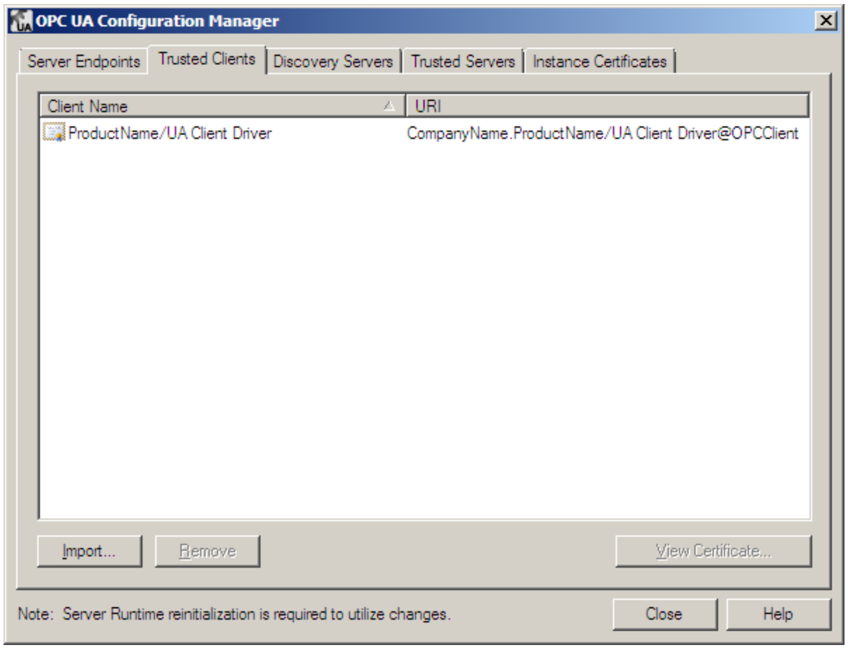
15. Launch the **OPC UA Configuration Manager** on the server computer.

16. Select the **Trusted Clients** tab.



Note: Server Runtime reinitialization is required to utilize changes.

17. Select **Import** and locate the client certificate file.
18. Select **Open**.
19. The client certificate should appear in the **Trusted Clients** window and can be identified by the **URI**.



Client Name	URI
ProductName/UA Client Driver	CompanyName.ProductName/UA Client Driver@OPCClient

Note: Server Runtime reinitialization is required to utilize changes.

4. Setting up the Server

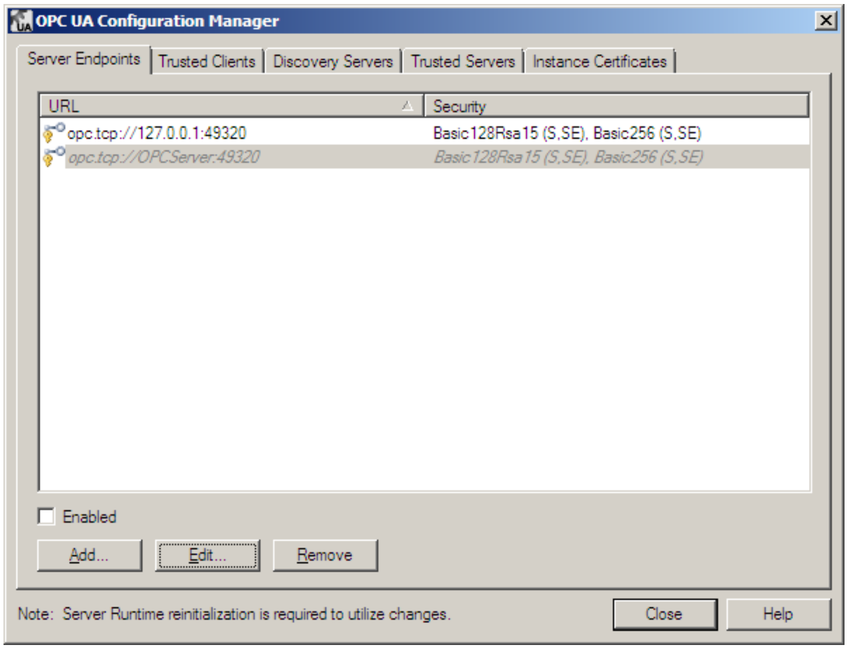
4.1 Endpoints

In order for an OPC UA client to connect to an OPC UA server, the client needs to 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. The server will, in turn, return all configured endpoints along with security requirements that are available to the client.

To simplify the process, the Discovery Endpoint and the Server Endpoint can be the same location as is the case for this server application.

During the install of the server application, an initial endpoint is created for local connections. Minor configuration changes are required to allow remote clients to discover and connect to the server. To become familiar with this configuration or to add and make changes to the existing endpoints, follow these steps:

1. Launch the **OPC UA Configuration Manager** by right-clicking on the **Administration** icon and selecting **OPC UA Configuration**.
2. Select the **Server Endpoints** tab.



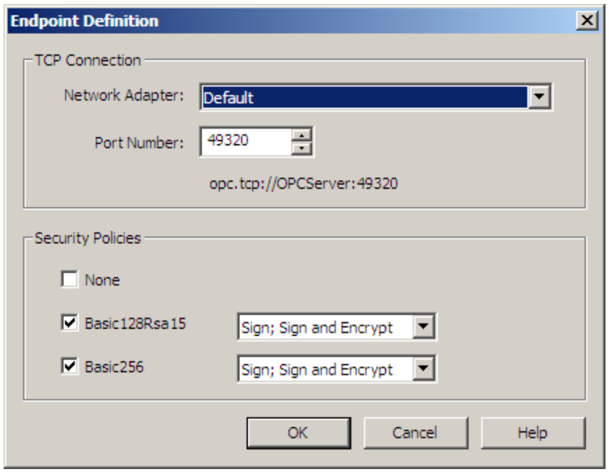
URL	Security
opc.tcp://127.0.0.1:49320	Basic128Rsa15 (S,SE), Basic256 (S,SE)
opc.tcp://OPCServer:49320	Basic128Rsa15 (S,SE), Basic256 (S,SE)

□ Enabled

Note: Server Runtime reinitialization is required to utilize changes.

3. Select the default endpoint that was created during the install for non-local connections.
4. Select **Edit**.
5. Make note of the port number so that it can be added to the firewall.

6. If necessary, modify the settings in the **Security Policies** group. Since these settings are for the server, this particular endpoint will allow all connections with the enabled policies. I.e. the default endpoint will only allow secure connections using signing and encryption. If security is not required, select **None** and you may also want to disable the security policies completely.



Endpoint Definition

TCP Connection

Network Adapter: Default

Port Number: 49320

opc.tcp://OPCServer:49320

Security Policies

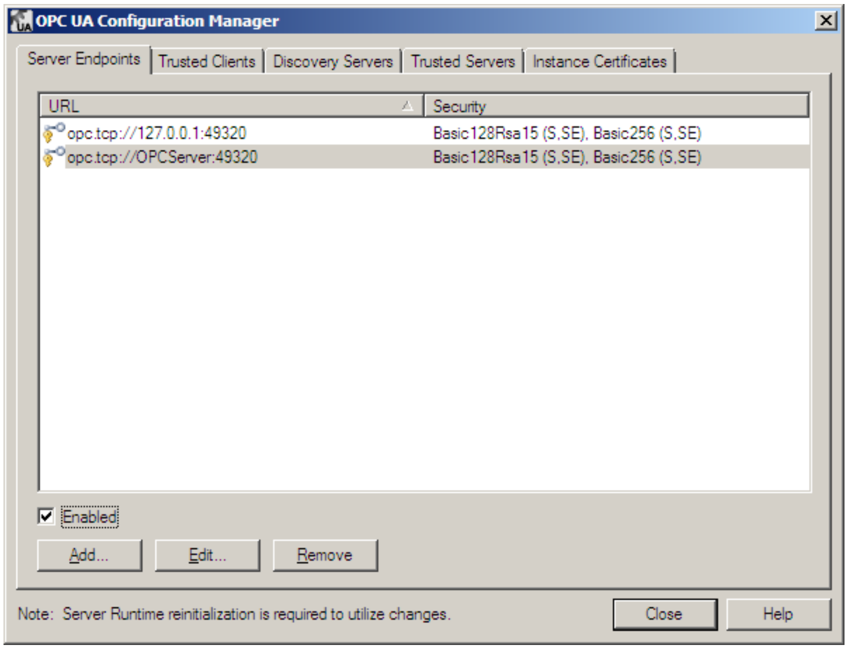
☐ None

☑ Basic128Rsa15 — Sign; Sign and Encrypt

☑ Basic256 — Sign; Sign and Encrypt

7. With the policies adjusted accordingly, select **OK**.

8. Enable the endpoint by selecting it in the list and checking the **Enable** box.



OPC UA Configuration Manager

URL	Security
opc.tcp://127.0.0.1:49320	Basic128Rsa15 (S,SE), Basic256 (S,SE)
opc.tcp://OPCServer:49320	Basic128Rsa15 (S,SE), Basic256 (S,SE)

☑ Enabled

Note: Server Runtime reinitialization is required to utilize changes.

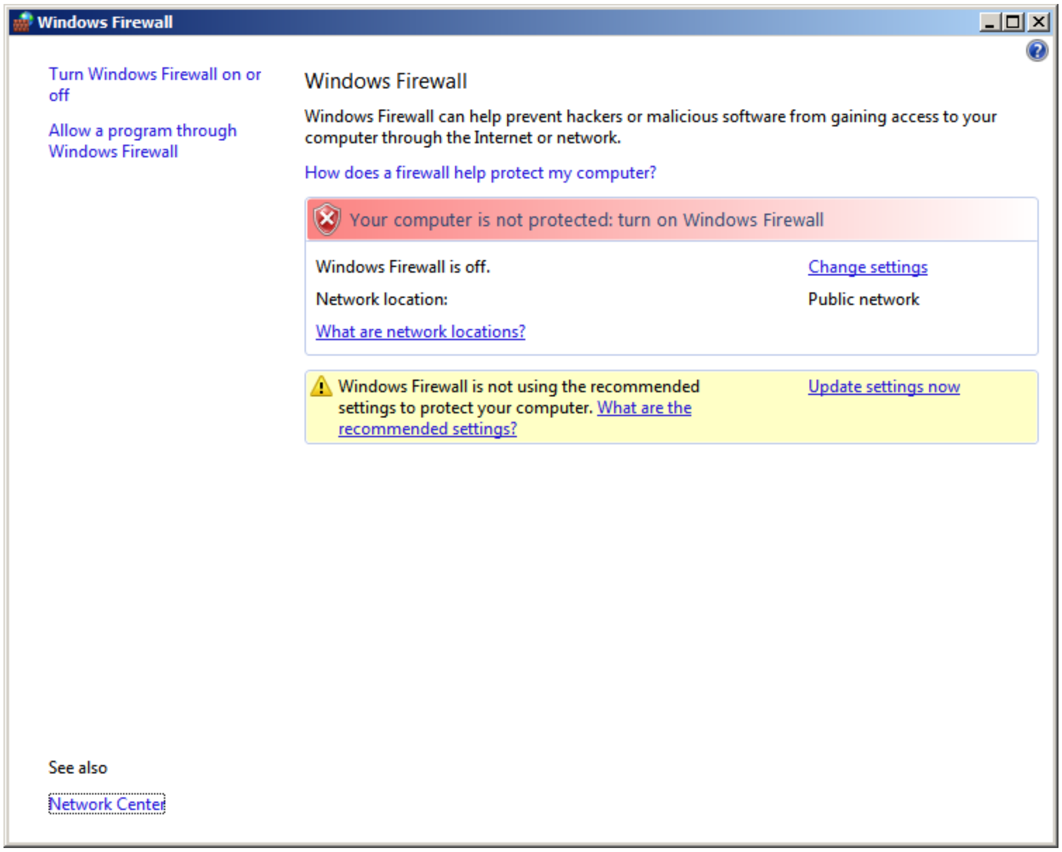
9. Apply the changes to the server Runtime by right-clicking on the **Administration** icon and selecting **Reinitialize** or if the server is not running, select **Start Runtime**.

4.2 Firewall

The purpose of a firewall is to drop incoming traffic that is not expected (unsolicited traffic) or traffic that does not correspond to the exceptions (excepted traffic) that are set within the firewall. Since OPC UA does not require callbacks, only the server computer needs to have the exception.

To add the exception, follow these steps on the server computer:

1. Launch the **Windows Firewall** by selecting **Start | Run** and then typing **firewall.cpl**.



Windows Firewall

Turn Windows Firewall on or off

Allow a program through Windows Firewall

Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or network.

How does a firewall help protect my computer?

Your computer is not protected: turn on Windows Firewall

Windows Firewall is off. Change settings

Network location: Public network

What are network locations?

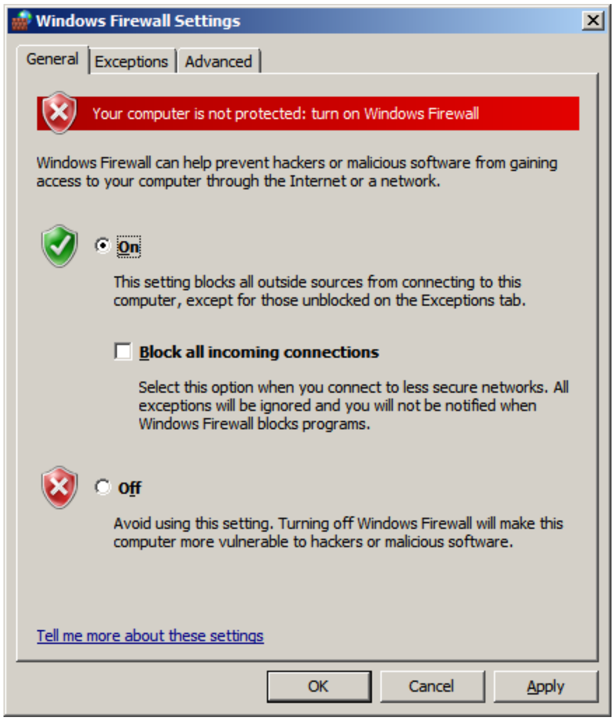
Windows Firewall is not using the recommended settings to protect your computer. What are the recommended settings? Update settings now

See also

Network Center

2. Windows Vista or Windows Server 2008 will not directly display the settings dialog. To view the dialog, select **Change Settings**.

3. Select the **General** tab.



Windows Firewall Settings

General | Exceptions | Advanced

Your computer is not protected: turn on Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.

● On

This setting blocks all outside sources from connecting to this computer, except for those unblocked on the Exceptions tab.

□ Block all incoming connections

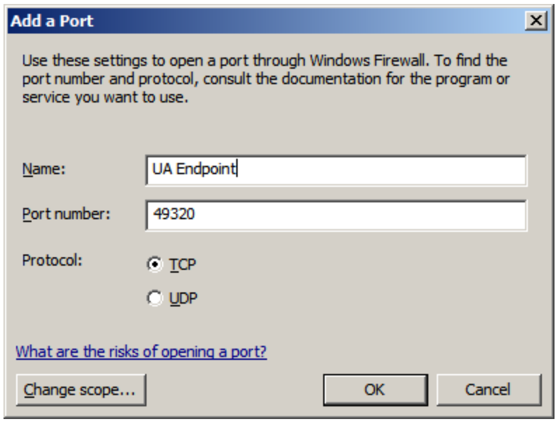
Select this option when you connect to less secure networks. All exceptions will be ignored and you will not be notified when Windows Firewall blocks programs.

○ Off

Avoid using this setting. Turning off Windows Firewall will make this computer more vulnerable to hackers or malicious software.

Tell me more about these settings

4. Verify that the firewall is enabled by choosing **On**.
5. Select the **Exceptions** tab.
6. Click **Add port**.
7. Enter **UA Endpoint** in the **Name** field.
8. Enter the port number that is assigned to the endpoint in the **Port number** field.
9. Verify that the correct **Protocol** is selected. The default is **TCP**.



Add a Port

Use these settings to open a port through Windows Firewall. To find the port number and protocol, consult the documentation for the program or service you want to use.

Name: UA Endpoint

Port number: 49320

Protocol: ● TCP ○ UDP

10. Click **OK**.
11. If multiple endpoints are assigned to the server, continue to add them now.
12. When done, click **OK** to close the settings dialog.

5.Setting up a Discovery Service (Optional)

Those who are familiar with Classic OPC are familiar with an application called OPCEnum. This application runs locally on the serving computer and exposes available Classic OPC servers to the remotely connecting client(s). A client simply needs to know the serving computer's location on the network.

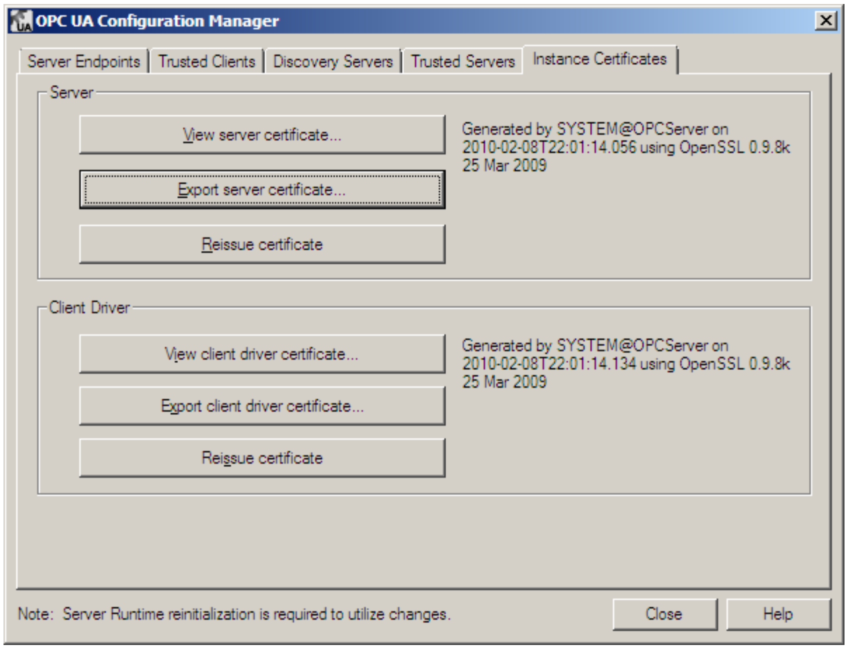
Unfortunately, OPC UA lost this luxury in exchange for its platform independence. However, to provide the same usability, a service was created that allows OPC UA servers to be discovered at a "well-know" location. This service, called the Local Discovery Service (LDS), is expected to be installed on every computer that is running an OPC UA server (the same way OPCEnum is installed alongside most Classic OPC servers). However, the development and implementation of the LDS is not as far along as OPC UA itself so the actual usage or the service will vary.

This server application does not provide a LDS, but can be register for discovery by exchanging certificates with one provided by the OPC Foundation.

5.1 Server

1. Launch the **OPC UA Configuration Manager** by right-clicking on the **Administration** icon and selecting **OPC UA Configuration**.

2. Select the **Instance Certificate** tab.


OPC UA Configuration Manager
Server Endpoints
Trusted Clients
Discovery Servers
Trusted Servers
Instance Certificates
Server
View server certificate...
Export server certificate...
Reissue certificate
Client Driver
View client driver certificate...
Export client driver certificate...
Reissue certificate
Close
Help

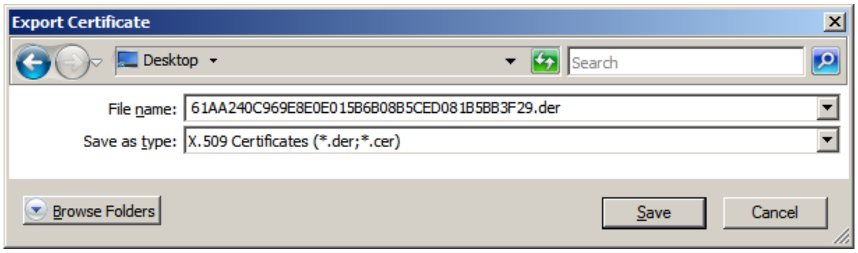
Generated by SYSTEM@OPCServer on 2010-02-08T22:01:14.056 using OpenSSL 0.9.8k 25 Mar 2009

Generated by SYSTEM@OPCServer on 2010-02-08T22:01:14.134 using OpenSSL 0.9.8k 25 Mar 2009

Note: Server Runtime reinitialization is required to utilize changes.

3. Under the **Server** group, select **Export server certificate**.

4. Select a location for the certificate file so that it can be easily located. The default file name is the thumbprint that identifies the certificate, but it may be changed to make managing the files easier.

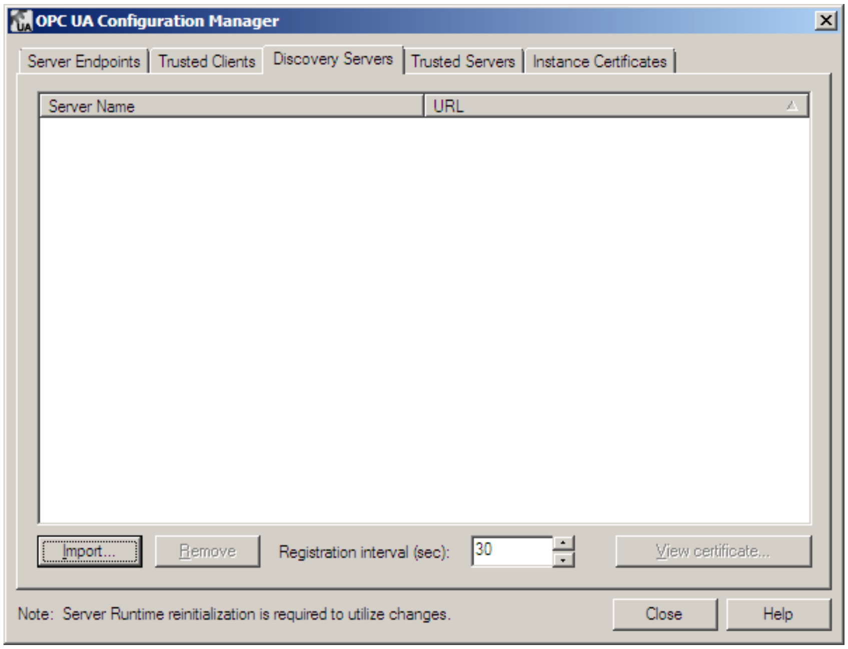


File name: 61AA240C969E8E0E015B6B08B5CED081B5BB3F29.der

Save as type: X.509 Certificates (*.der;*.cer)

5. If the Local Discovery Service is on another machine, manually copy the server certificate file from the server computer and move it onto the computer that is running the service.

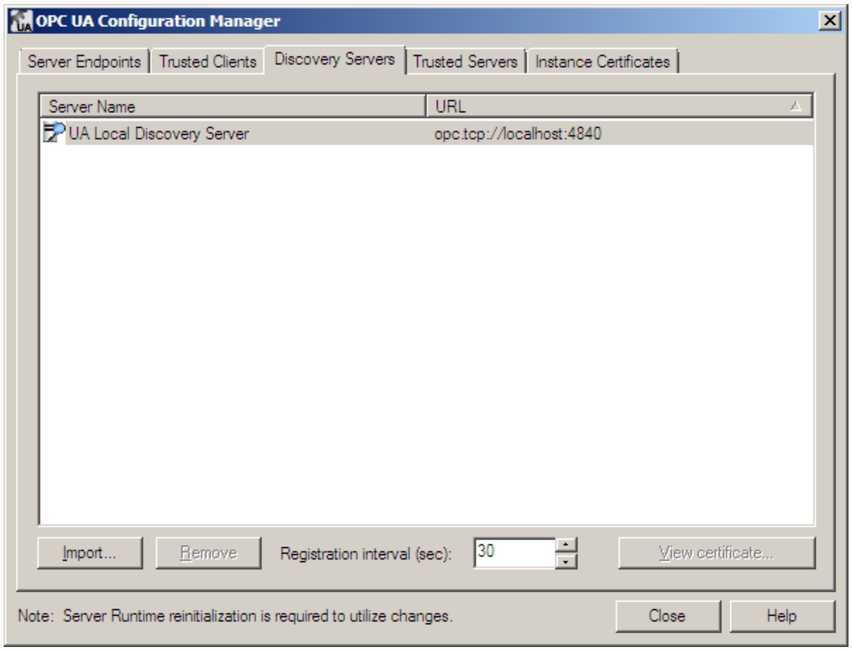
6. Select the **Discovery Servers** tab.



Registration interval (sec): 30

Note: Server Runtime reinitialization is required to utilize changes.

7. Select **Import** and locate the LDS certificate file.
8. Select **Open**.



Server Name	URL
UA Local Discovery Server	opc.tcp://localhost:4840

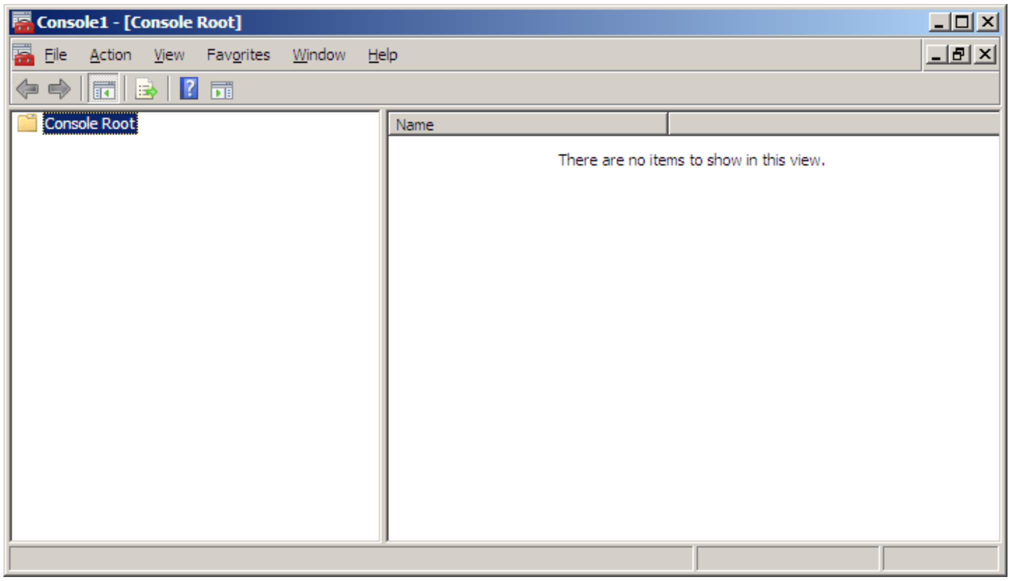
Registration interval (sec): 30

Note: Server Runtime reinitialization is required to utilize changes.

9. The LDS certificate should appear in the window. The **URL** defaults to localhost and must be changed if it resides on a remote computer.

5.2 OPC Foundation

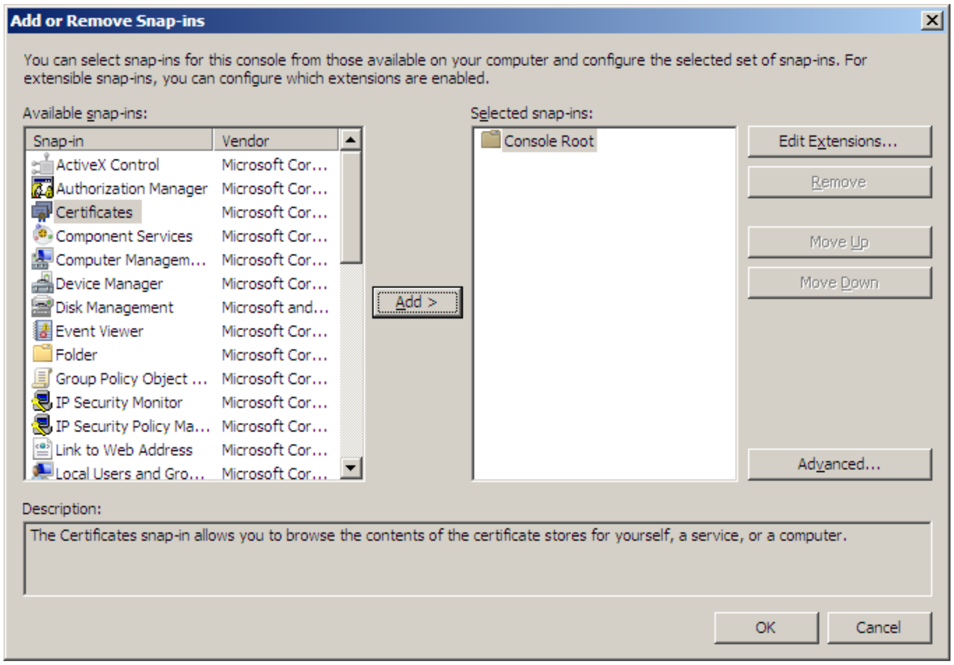
1. Launch the **Microsoft Management Console** by selecting **Start | Run** and then typing **mmc.exe**.



There are no items to show in this view.

2. Select **File | Add / Remove Snap-in**.

3. In the **Available snap-ins** window, select **Certificates**.



You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

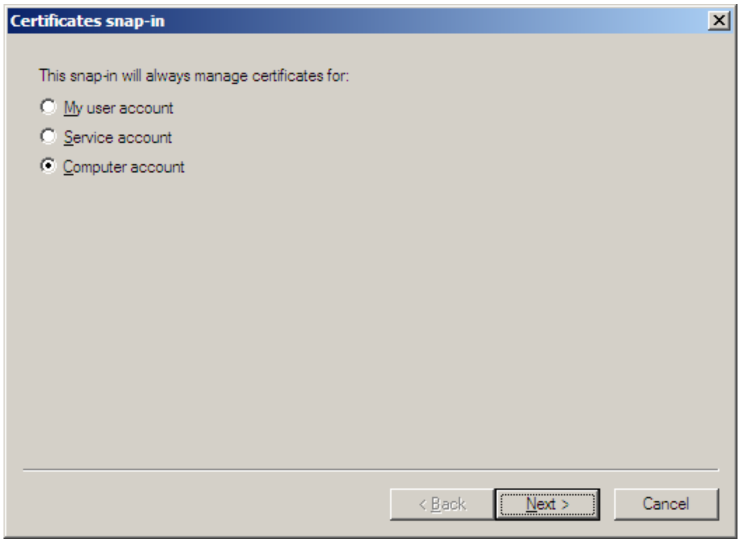
Snap-in	Vendor
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...
Group Policy Object ...	Microsoft Cor...
IP Security Monitor	Microsoft Cor...
IP Security Policy Ma...	Microsoft Cor...
Link to Web Address	Microsoft Cor...
Local Users and Gro...	Microsoft Cor...

Description:

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

4. Click **Add**.

5. Choose **Computer account** in the **Certificates snap-in** dialog.



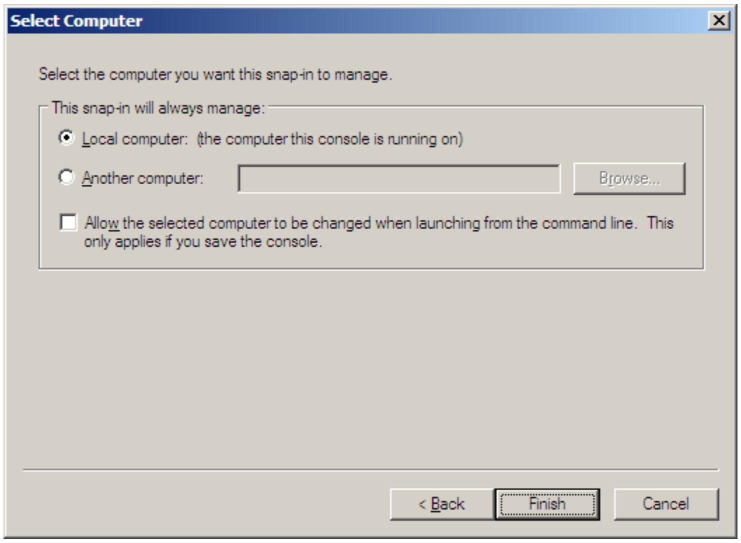
This snap-in will always manage certificates for:

○ My user account

○ Service account

● Computer account

6. Click **Next**.
7. Choose **Local computer** in the **Select Computer** dialog.



Select the computer you want this snap-in to manage.

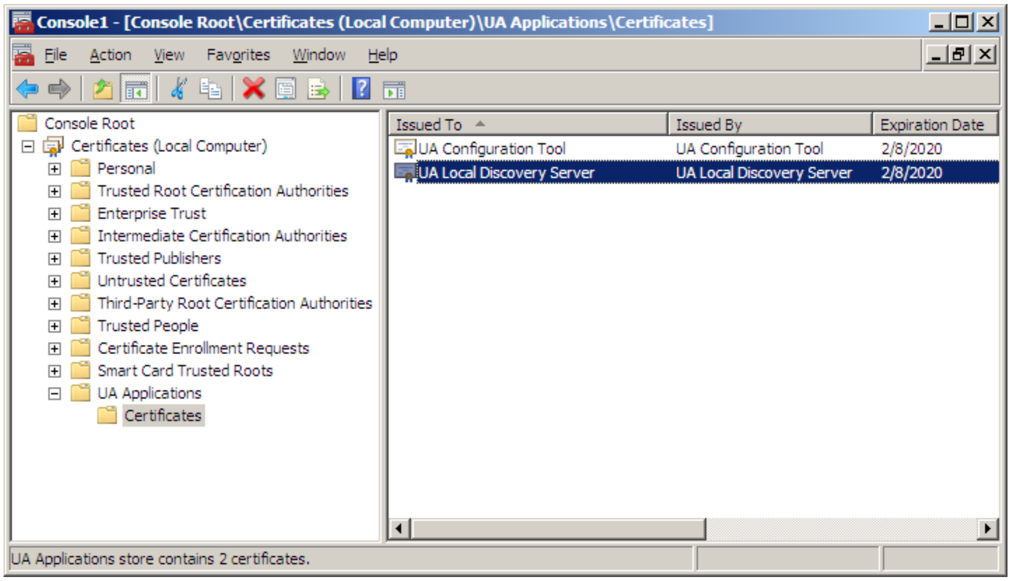
This snap-in will always manage:

● Local computer: (the computer this console is running on)

○ Another computer:

□ Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.

8. Click **Finish**.
9. Back in the **Add or Remove Snap-ins** dialog, click **OK** to apply the changes to the console.
10. Under the **Console Root** folder, expand **Certificates (Local Computer)**, **UA Applications**, **Certificates** and select **UA Local Discovery Server**.



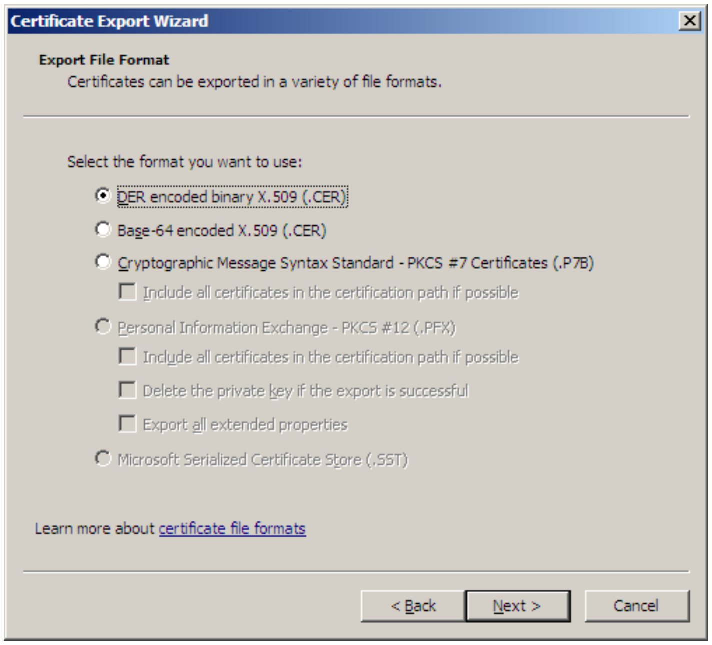
Console1 - [Console Root\Certificates (Local Computer)\UA Applications\Certificates]

- Console Root
  - Certificates (Local Computer)
    - Personal
    - Trusted Root Certification Authorities
    - Enterprise Trust
    - Intermediate Certification Authorities
    - Trusted Publishers
    - Untrusted Certificates
    - Third-Party Root Certification Authorities
    - Trusted People
    - Certificate Enrollment Requests
    - Smart Card Trusted Roots
    - UA Applications
      - Certificates

Issued To	Issued By	Expiration Date
UA Configuration Tool	UA Configuration Tool	2/8/2020
UA Local Discovery Server	UA Local Discovery Server	2/8/2020

UA Applications store contains 2 certificates.

11. Select **Action | All Tasks > Export.**
12. Select **Next** to begin the exportation process.
13. Choose **DER encoded binary X.509** for the file format.



Certificate Export Wizard

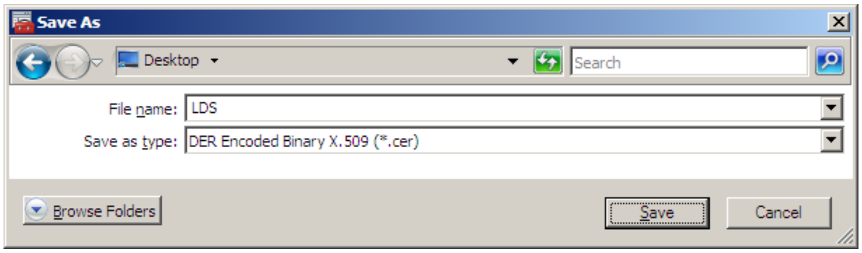
Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

● DER encoded binary X.509 (.CER)
○ Base-64 encoded X.509 (.CER)
○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
□ Include all certificates in the certification path if possible
○ Personal Information Exchange - PKCS #12 (.PFX)
□ Include all certificates in the certification path if possible
□ Delete the private key if the export is successful
□ Export all extended properties
○ Microsoft Serialized Certificate Store (.SST)

Learn more about certificate file formats

14. Click **Next**.
15. Supply a file name and a destination for the certificate.



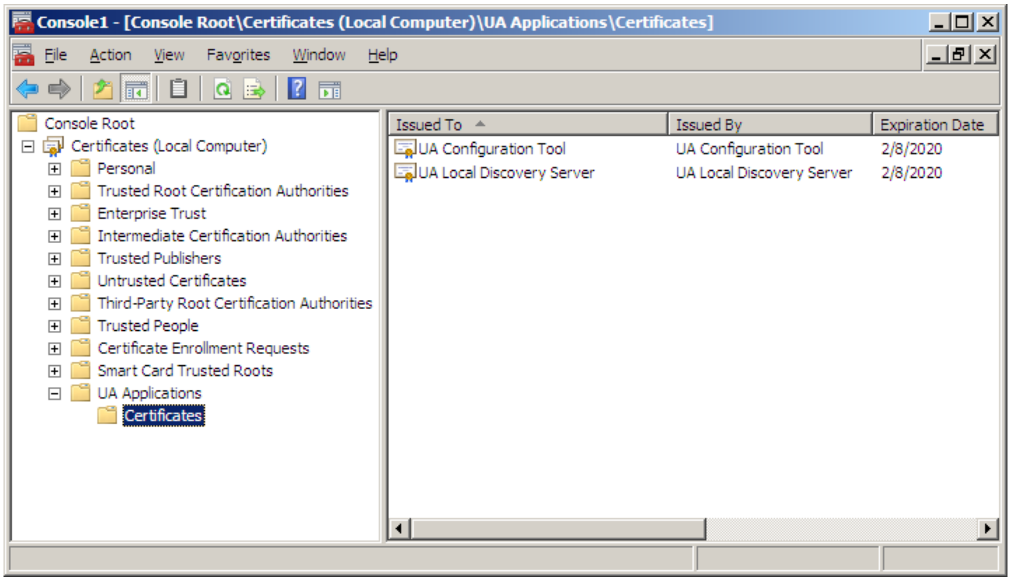
Save As

File name: LDS
Save as type: DER Encoded Binary X.509 (*.cer)

16. Click **Next**.

17. Review the summary and click **Finish**.

18. Under the **Console Root** folder, expand **Certificates (Local Computer)**, **UA Applications** and select, **Certificates**.

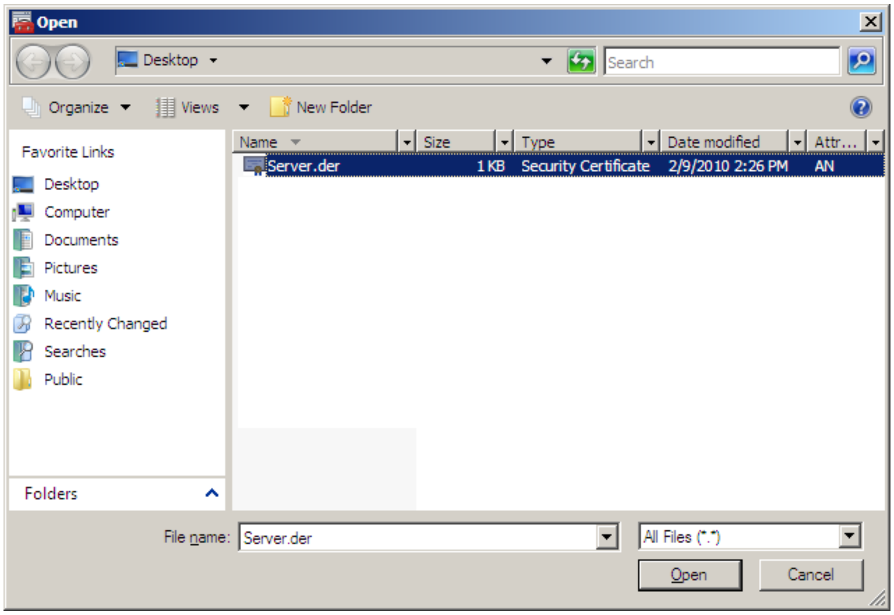

Console1 - [Console Root\Certificates (Local Computer)\UA Applications\Certificates]
File
Action
View
Favorites
Window
Help
Console Root
Certificates (Local Computer)
Personal
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Certificate Enrollment Requests
Smart Card Trusted Roots
UA Applications
Certificates

Issued To	Issued By	Expiration Date
UA Configuration Tool	UA Configuration Tool	2/8/2020
UA Local Discovery Server	UA Local Discovery Server	2/8/2020

19. Select **Action | All Tasks > Import.**

20. Click **Next** to begin the importation process.

21. Browse to the server certificate file that was previously exported from the OPC UA Configuration Manager.



Name	Size	Type	Date modified	Attr...
Server.der	1 KB	Security Certificate	2/9/2010 2:26 PM	AN

File name: Server.der

All Files (*.*)

22. Click **Open**.

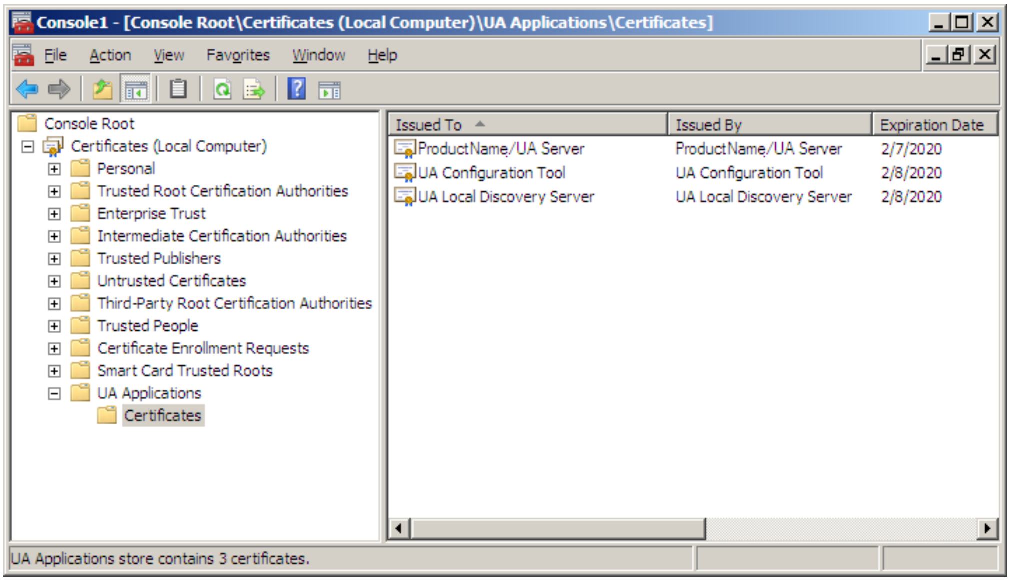
23. Click **Next**.

24. Choose **Place all certificates in the following store** on the **Certificate Store** page. Ensure that the **UA Applications** store is displayed as the destination.

25. Click **Next**.

26. Review the summary and click **Finish**.

27. The server's certificate will appear in the UA Applications store.



Console1 - [Console Root\Certificates (Local Computer)\UA Applications\Certificates]

- Console Root
  - Certificates (Local Computer)
    - Personal
    - Trusted Root Certification Authorities
    - Enterprise Trust
    - Intermediate Certification Authorities
    - Trusted Publishers
    - Untrusted Certificates
    - Third-Party Root Certification Authorities
    - Trusted People
    - Certificate Enrollment Requests
    - Smart Card Trusted Roots
    - UA Applications
      - Certificates

Issued To	Issued By	Expiration Date
ProductName/UA Server	ProductName/UA Server	2/7/2020
UA Configuration Tool	UA Configuration Tool	2/8/2020
UA Local Discovery Server	UA Local Discovery Server	2/8/2020

UA Applications store contains 3 certificates.

The discovery service is now configured.

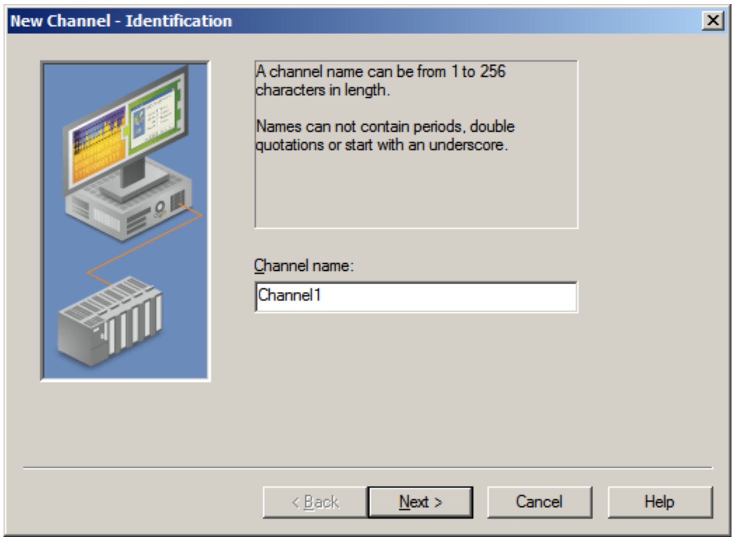
6. Setting up the Client

6.1 OPC UA Client Channel

The channel wizard is used to locate and identify the OPC UA server, configure session timeouts, and provide user information when applicable.

Add a UA Client channel by following these steps:

1. Launch the Configuration by right-clicking on the **Administration** icon and selecting **Configuration**.
2. Select **Edit | Devices > New Channel**.
3. On the **Identification** page, supply a name for the OPC UA client channel.



New Channel - Identification

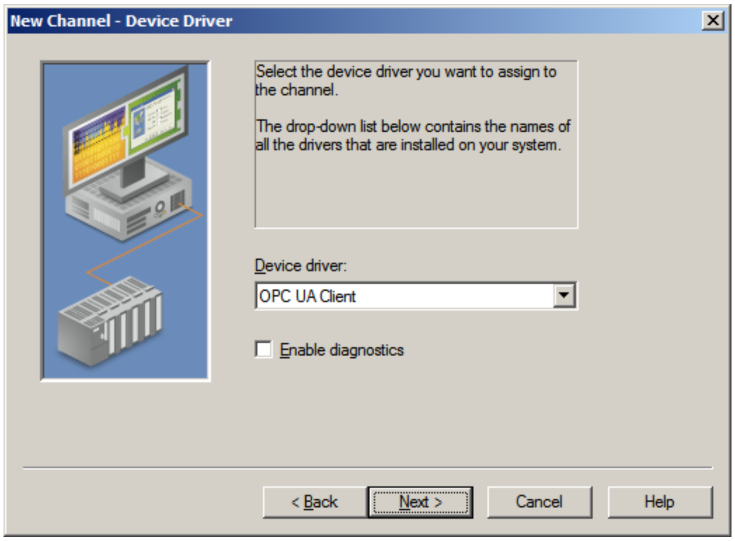
A channel name can be from 1 to 256 characters in length.

Names can not contain periods, double quotations or start with an underscore.

Channel name: Channel1

4. Click **Next**.

5. On the **Device Driver** page, select **OPC UA Client** in the **Device driver** list.



Select the device driver you want to assign to the channel.

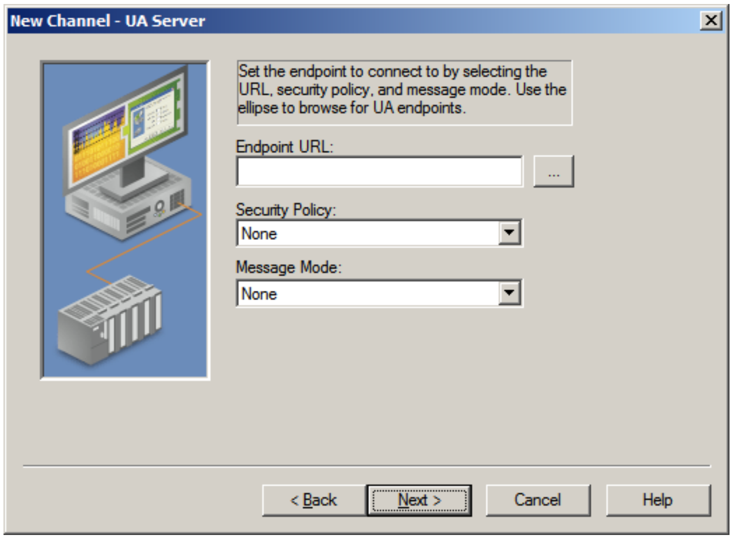
The drop-down list below contains the names of all the drivers that are installed on your system.

Device driver: OPC UA Client

☐ Enable diagnostics

6. Click **Next**.
7. Make no changes on the **Write Optimization** page.
8. Click **Next**.

9. On the **UA Server** page, the server's endpoint URL can be manually entered into the **Endpoint URL** field. The user can also choose to browse for the computer.



New Channel - UA Server

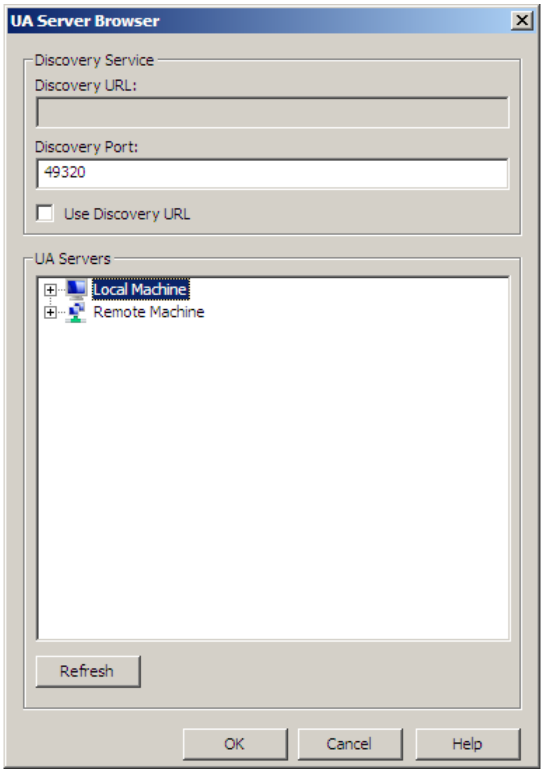
Set the endpoint to connect to by selecting the URL, security policy, and message mode. Use the ellipse to browse for UA endpoints.

Endpoint URL:

Security Policy: None

Message Mode: None

10. Click the **Browse** icon to the right of the **Endpoint URL** field.



UA Server Browser

Discovery Service

Discovery URL:

Discovery Port: 49320

☐ Use Discovery URL

UA Servers

⊞ Local Machine

⊞ Remote Machine

11. Begin with disabling the **Use Discovery URL** option. This option is disabled by default.

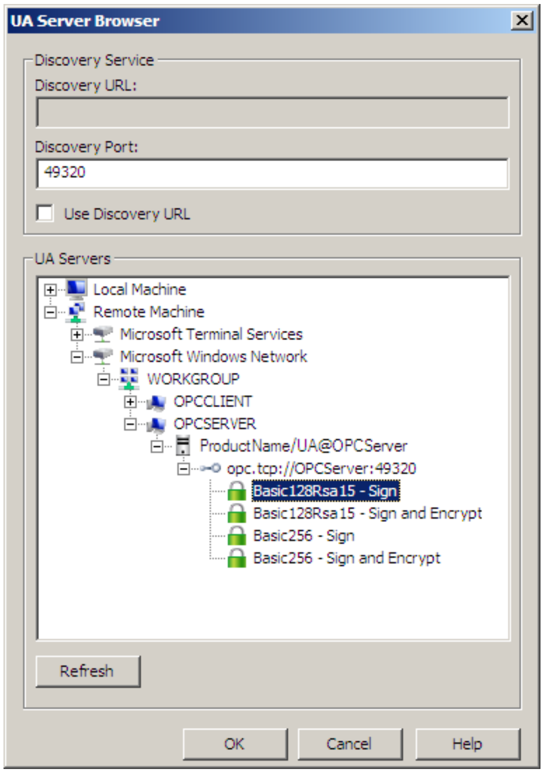
12. Enter the endpoint port number that was created on the server computer in the **Discover Port** field. The default port number should already be assigned and should agree with the default endpoint. Also, port 4840 will always be scanned by the browser so if a discovery server is being used, it is not necessary to enter the correct port number in this field.

13. If the port number was changed, click **Refresh**.

14. Navigate the **browse tree** to locate the server computer by its name. Endpoints that are assigned to localhost will only be found under the **Local Machine** branch.

15. Expand the computer and below it will be a list of available servers.

16. Expand the server(s) and select the correct endpoint.



Discovery URL:

Discovery Port: 49320

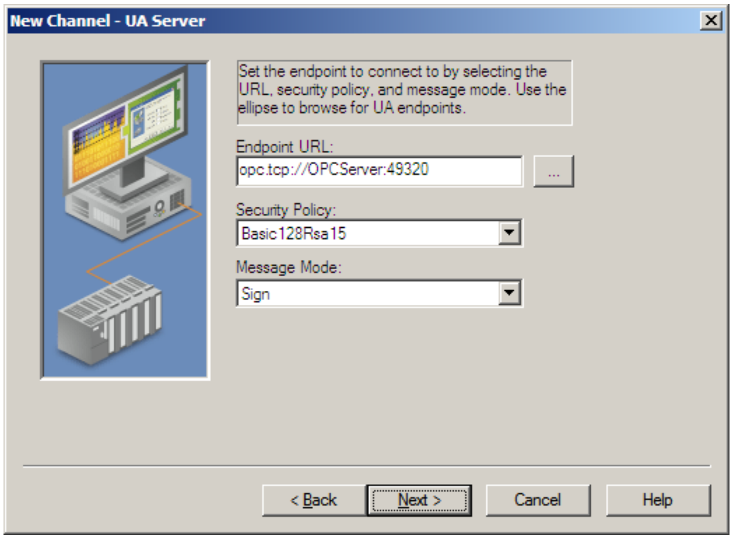
□ Use Discovery URL

- Local Machine
- Remote Machine
  - Microsoft Terminal Services
  - Microsoft Windows Network
    - WORKGROUP
      - OPCCLIENT
      - OPCSERVER
        - ProductName/UA@OPCServer
          - opc.tcp://OPCServer:49320
            - Basic128Rsa15 - Sign
            - Basic128Rsa15 - Sign and Encrypt
            - Basic256 - Sign
            - Basic256 - Sign and Encrypt

17. If you wish to continue to use this endpoint to discover OPC UA servers, enable the **Use Discovery URL** in the **Discovery** group at the top of the dialog. This is a global change that will affect all other UA client drivers when this dialog is used.

18. Click **OK**.

19. The endpoint information will appear in the **UA Server** page.



Set the endpoint to connect to by selecting the URL, security policy, and message mode. Use the ellipse to browse for UA endpoints.

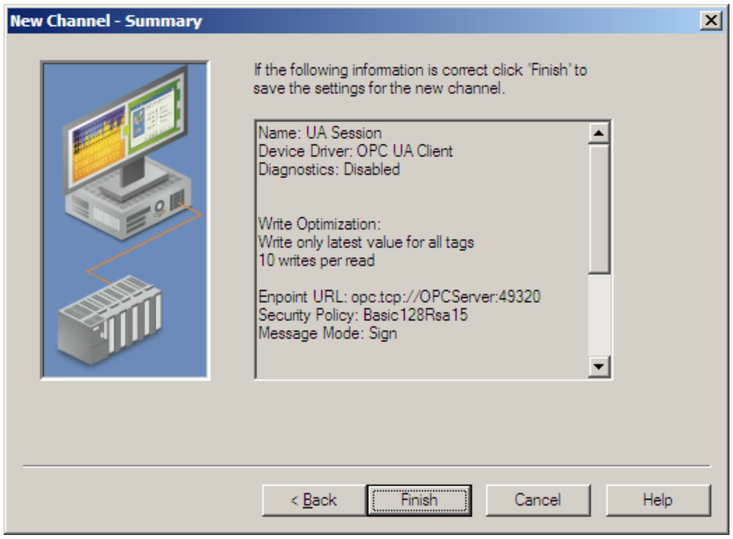
Endpoint URL: opc.tcp://OPCServer:49320

Security Policy: Basic128Rsa15

Message Mode: Sign

20. Click **Next.**

21. Use defaults on the **UA Session** page. These can be optimized later.
22. Click **Next**.
23. Keep the username and password blank on the **Authentication** page is not required.
24. Click **Next**.
25. View the **Summary** and click **Finish**.



If the following information is correct click 'Finish' to save the settings for the new channel.

Name: UA Session
Device Driver: OPC UA Client
Diagnostics: Disabled

Write Optimization:
Write only latest value for all tags
10 writes per read

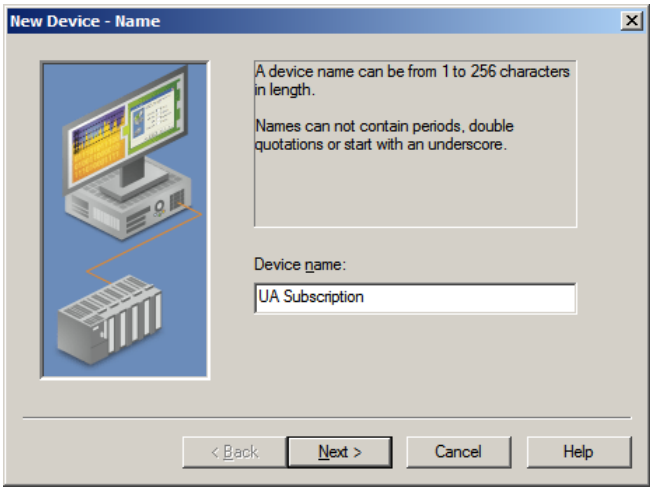
Enpoint URL: opc.tcp://OPCServer:49320
Security Policy: Basic128Rsa15
Message Mode: Sign

6.2 OPC UA Client Device

The device wizard will guide the user in setting up a subscription and will also provide 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.

Add a UA Client device by following these steps:

1. With the new channel selected, select **Edit | Devices > New Device**.
2. On the **Name** page, supply a name for the OPC UA client device.



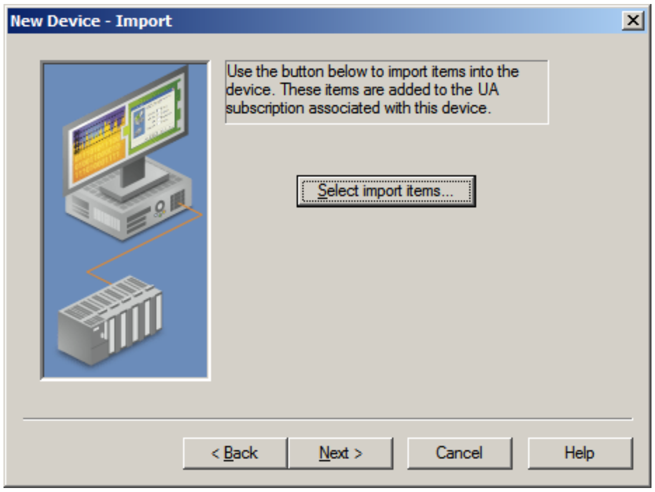
A device name can be from 1 to 256 characters in length.

Names can not contain periods, double quotations or start with an underscore.

Device name: UA Subscription

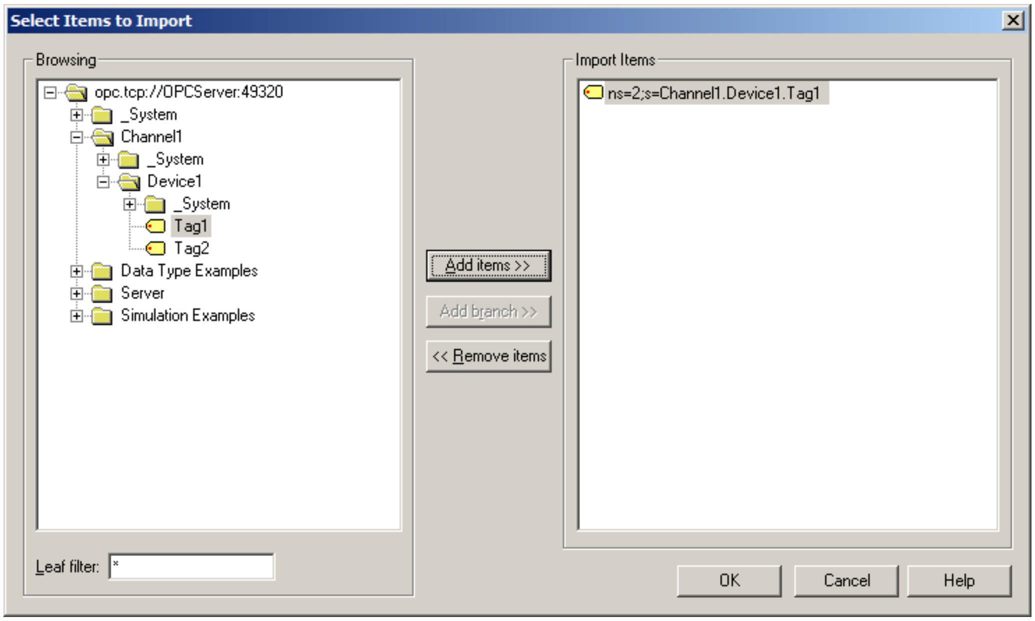
3. Click **Next**.
4. Use defaults on the **Subscription, Keep Alive, Priority and Timeout, Monitored Items, and Deadband** pages. These can be optimized later.

5. Click **Next** for each page.
6. On the **Import** page, click the **Select import items**.



Use the button below to import items into the device. These items are added to the UA subscription associated with this device.

7. The server's available items should appear in the **Browsing** window. If not, the security configuration is incorrect. See Trouble Shooting.
8. Select the desired items on the left and click **Add Items** or **Add Branch** to import them into the client.

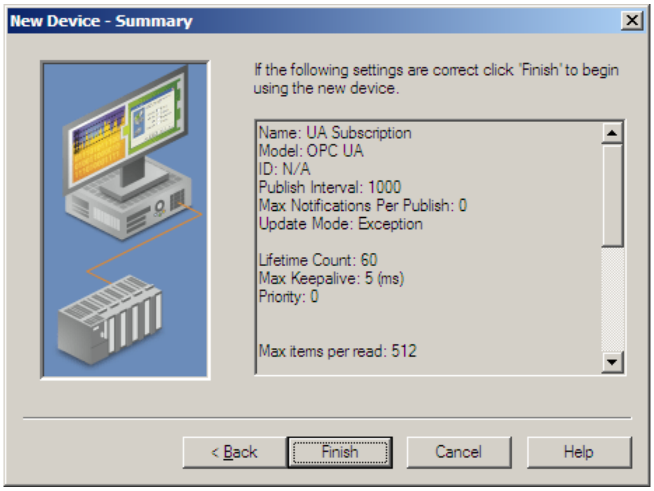


Import Items: ns=2;s=Channel1.Device1.Tag1

Leaf filter: *

9. When all the items are imported, click **OK**.
10. Click **Next** back on the **Import** page.

11. View the **Summary** and click **Finish**.



If the following settings are correct click 'Finish' to begin using the new device.

Name: UA Subscription
Model: OPC UA
ID: N/A
Publish Interval: 1000
Max Notifications Per Publish: 0
Update Mode: Exception

Lifetime Count: 60
Max Keepalive: 5 (ms)
Priority: 0

Max items per read: 512

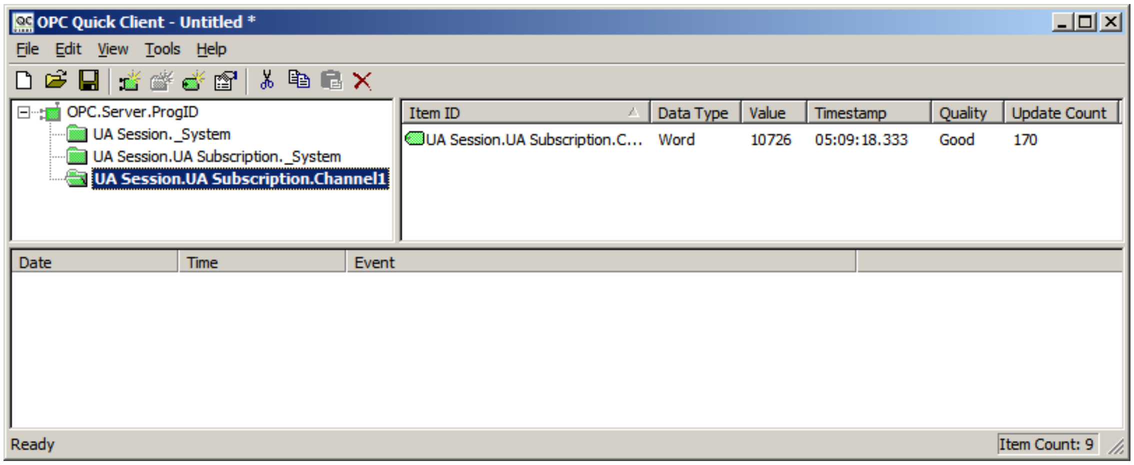
12. The imported items will populate under the device using the server's channel and device names as groups.

6.3 Verification

The items added in the OPC UA Client can now be browsed by an OPC DA client.

For easy verification, follow these steps:

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



OPC.Server.ProgID
UA Session._System
UA Session.UA Subscription._System
UA Session.UA Subscription.Channel1

Item ID	Data Type	Value	Timestamp	Quality	Update Count
UA Session.UA Subscription.C...	Word	10726	05:09:18.333	Good	170

Date	Time	Event

Ready

Item Count: 9

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

7. Summary

OPC Unified Architecture provides a means of exchanging data between an OPC server and an OPC client that aims to be platform independent, firewall friendly and secure. While UA is rather new to the OPC world, its current implementation in this application benefits users who are attempting to establish remote connections between a server and its clients. For more information about OPC UA, refer to the OPC Foundation at http://www.opcfoundation.org/.