OPC Connectors

OPC DA Real-time values

This connector is used to get real time data from any available OPC server either on the local machine or across the network.

This connector can be used if the OPC server to connect does not have a specific connector available for it.

Prerequisites

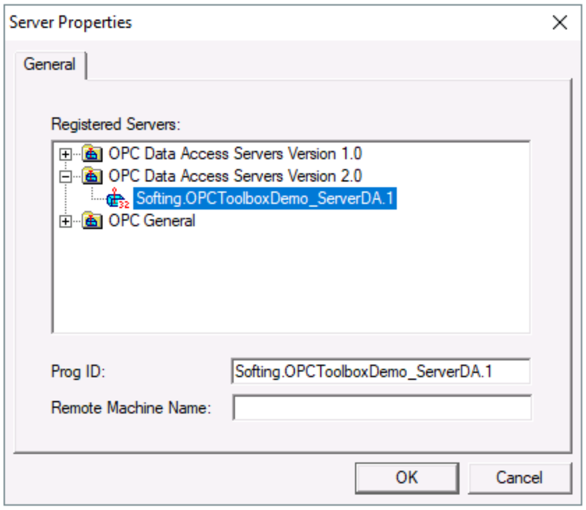
Verify Communication

Communication between the OPC server and an OPC client must be verified. Some OPC Server vendors like Kepware and Rockwell Automation provide OPC clients with their servers. These clients can be used to validate.

If an OPC client is not provided with the server, **XLReporter** provides an independent OPC client to verify connectivity and data retrieval from any OPC DA server. This client is found on **XLReporter's** product CD under **Tools, OPC, OPC_DA**. It can also be downloaded from www.SyTech.com.

To run, double-click **SampleClientDA.exe**.

To connect to an OPC server, select **Edit**, **New Server Connection** to open the **Server Properties** window.



Registered Servers:

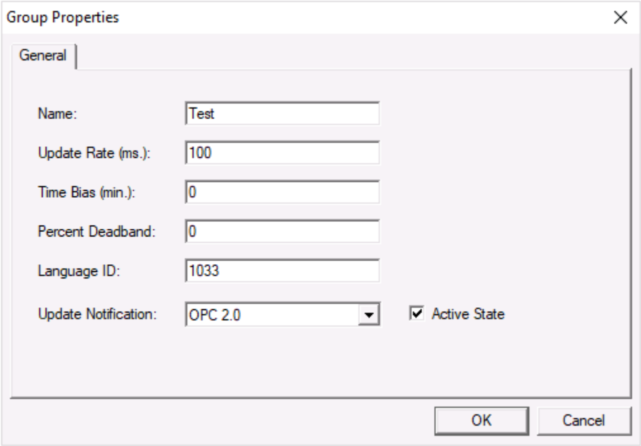
- OPC Data Access Servers Version 1.0
- OPC Data Access Servers Version 2.0
  - Softing.OPCToolboxDemo_ServerDA.1
- OPC General

Prog ID: Softing.OPCToolboxDemo_ServerDA.1

Remote Machine Name:

Expand the **OPC Data Access Servers Version 2.0**, select your OPC DA server and click **OK**.

From the **Edit** menu select **New Group**.



Name: Test

Update Rate (ms.): 100

Time Bias (min.): 0

Percent Deadband: 0

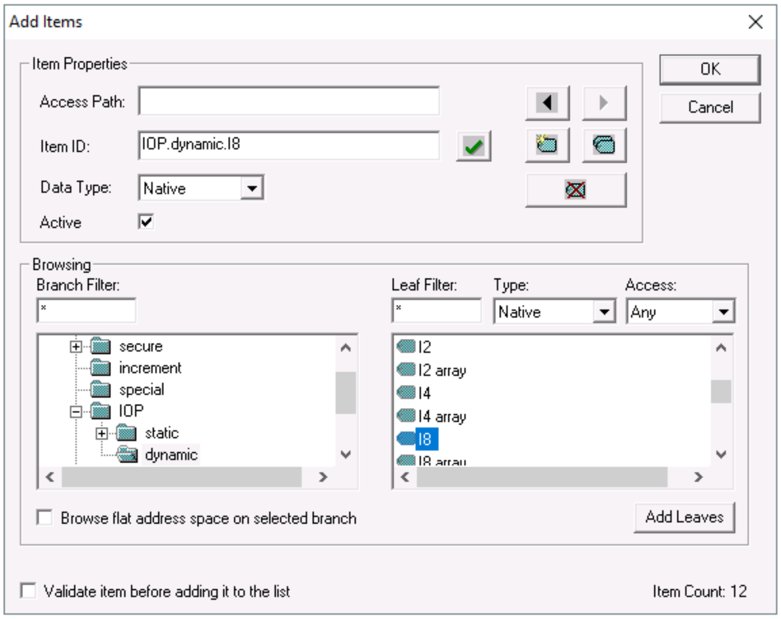
Language ID: 1033

Update Notification: OPC 2.0

☑ Active State

Specify **Name** and click **OK**.

Click on the group name created, and select **Edit**, **New Item**.



Access Path:

Item ID: IOP.dynamic.I8

Data Type: Native

Active ☑

Branch Filter: *

Leaf Filter: *

Type: Native

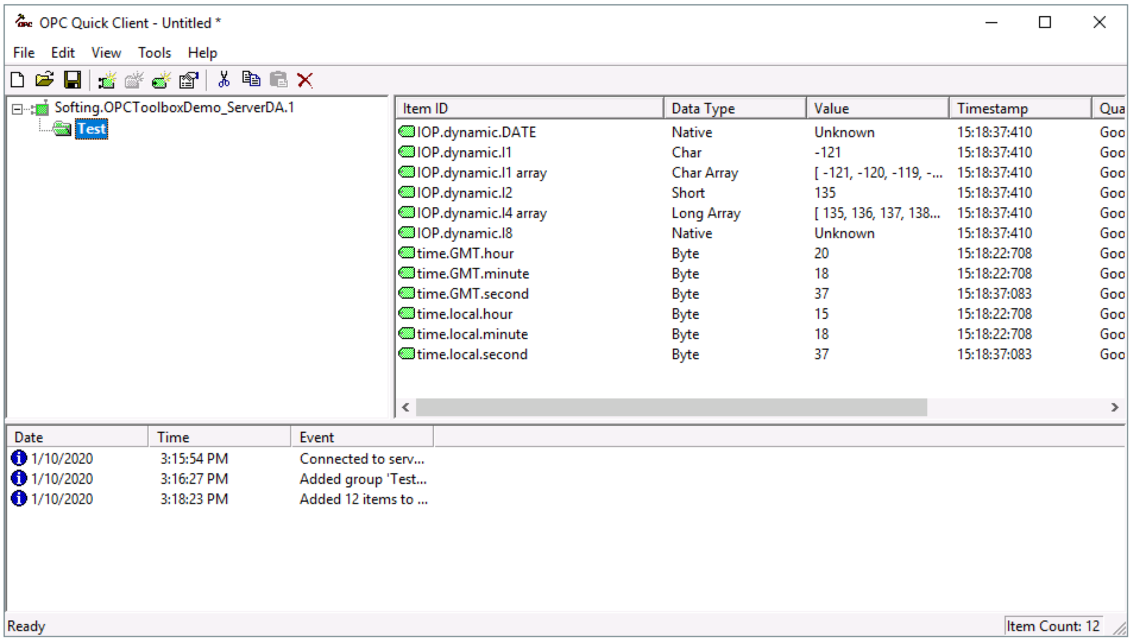
Access: Any

☐ Browse flat address space on selected branch

☐ Validate item before adding it to the list

Item Count: 12

This opens the **Add Items** window. In the browsing section drill into the tree and select Leaf items on the right. For each leaf you want to view data for, click the Add Leaves button. Click **OK** when you have selected the tags to read.


OPC Quick Client - Untitled *
File Edit View Tools Help
Softing.OPCToolboxDemo_ServerDA.1
Test

Item ID	Data Type	Value	Timestamp	Qua
IOP.dynamic.DATE	Native	Unknown	15:18:37:410	Goo
IOP.dynamic.I1	Char	-121	15:18:37:410	Goo
IOP.dynamic.I1 array	Char Array	[-121, -120, -119, -...	15:18:37:410	Goo
IOP.dynamic.I2	Short	135	15:18:37:410	Goo
IOP.dynamic.I4 array	Long Array	[135, 136, 137, 138...	15:18:37:410	Goo
IOP.dynamic.I8	Native	Unknown	15:18:37:410	Goo
time.GMT.hour	Byte	20	15:18:22:708	Goo
time.GMT.minute	Byte	18	15:18:22:708	Goo
time.GMT.second	Byte	37	15:18:37:083	Goo
time.local.hour	Byte	15	15:18:22:708	Goo
time.local.minute	Byte	18	15:18:22:708	Goo
time.local.second	Byte	37	15:18:37:083	Goo

Date	Time	Event
1/10/2020	3:15:54 PM	Connected to serv...
1/10/2020	3:16:27 PM	Added group 'Test...
1/10/2020	3:18:23 PM	Added 12 items to ...

Ready

Item Count: 12

All of the selected tags appear along with their real time values, type, quality, and timestamp.

If the client does not respond as described contact the OPC DA Server vendor technical support to troubleshoot and correct these issues.

Remote Communication

If **XLReporter** is not installed on the same machine as the OPC DA Server, the **XLReporter** machine must have the OPC Core Components installed.

To determine if the core components are installed verify the following file exists:

- C:\Windows\SysWow64\OPCEnum.exe (64-bit OS)
- C:\Windows\system32\OPCEnum.exe (32-bit OS)

If the components are not installed then they are provided in the XLReporter installation folder under *_repairtools\OPC*. Alternatively, these can be downloaded from www.opcfoundation.org.

Server Settings

In order to connect to an OPC DA server remotely both the machine where the server is running and the machine where the client is running must have matching Windows user accounts and the client must be logged in with a matching account.

In addition, on the machine with the OPC DA server, certain DCOM settings must be enabled. For details on what DCOM settings to enable, see OPC and DCOM: 5 Things You Need to Know.

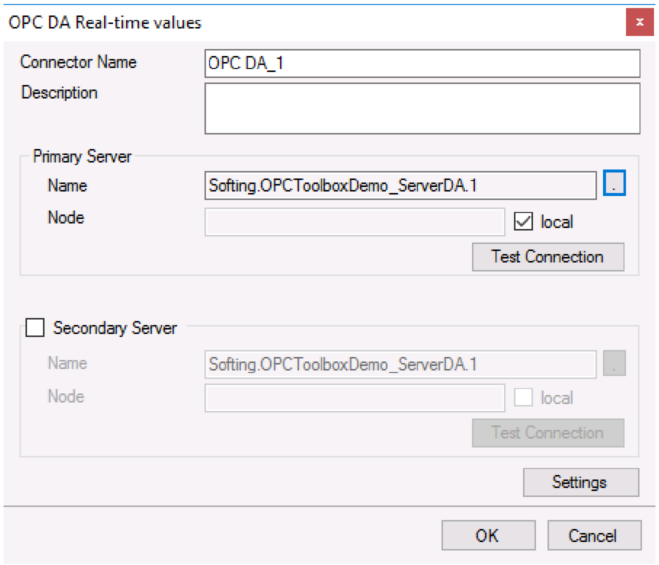
Windows Firewall

If the Windows Firewall is enabled on the machine where the OPC DA server is running TCP Port 135 must be opened in order for remote clients to connect.

Connector

To configure the connector to the OPC DA server, from the **Project Explorer** select **Data, Connectors**.

- Click **Add**
- Select **OPC, OPC DA Real-time values**
- Click **OK**



OPC DA Real-time values

Connector Name: OPC DA_1

Description:

Primary Server

Name: Softing.OPCToolboxDemo_ServerDA.1

Node: ☑ local

□ Secondary Server

Name: Softing.OPCToolboxDemo_ServerDA.1

Node: □ local

Primary Server

These settings define the **Name** and **Node** of the OPC DA server. A browse button is provided to browse for any available OPC DA server on the local machine or across the network.

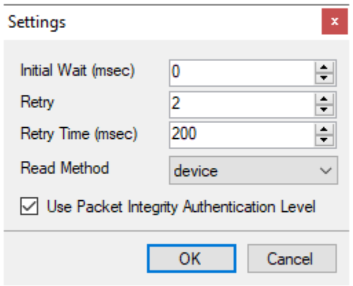
Use the **Test Connection** button to verify a connection to the server.

Secondary Server

These settings define the (optional) secondary OPC DA to connect to if a connection to the **Primary Server** fails.

Settings

The **Settings** button is used to update tuning parameters if there are issues retrieving data from this connector.



Settings

Initial Wait (msec): 0

Retry: 2

Retry Time (msec): 200

Read Method: device

☑ Use Packet Integrity Authentication Level

The **Initial Wait** setting is the amount of time (in milliseconds) the **Connector** waits after making a request and before retrieving data. This can be useful when communications do not respond immediately.

Retry determines how many attempts are made when bad values are returned. The default is 2 and it should typically not be changed. The **Retry Time** determines how the time in between retries.

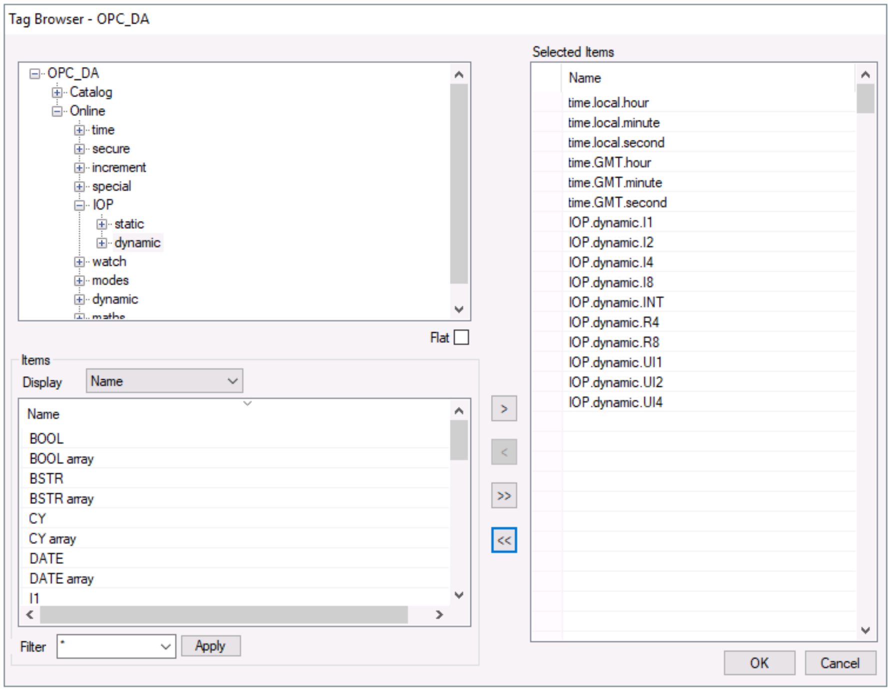
The **Read Method** setting determines how data is read from the server. By default, this is set to *device*. *Cache* is a faster way to read data but can cause bad quality data to be returned so only change this setting if good quality data is read.

If the **Use Pack Integrity Authentication Level** is checked, when a connection is made to a remote OPCDA server it uses the packet integrity authentication level. This must be set if the Microsoft DCOM hardening has been implemented on the system where the OPCDA server is installed.

Verify Data Communication

To verify communication to the OPC DA Server, open the **Project Explorer** and select the **Tools** tab. Launch the **System Check** application.

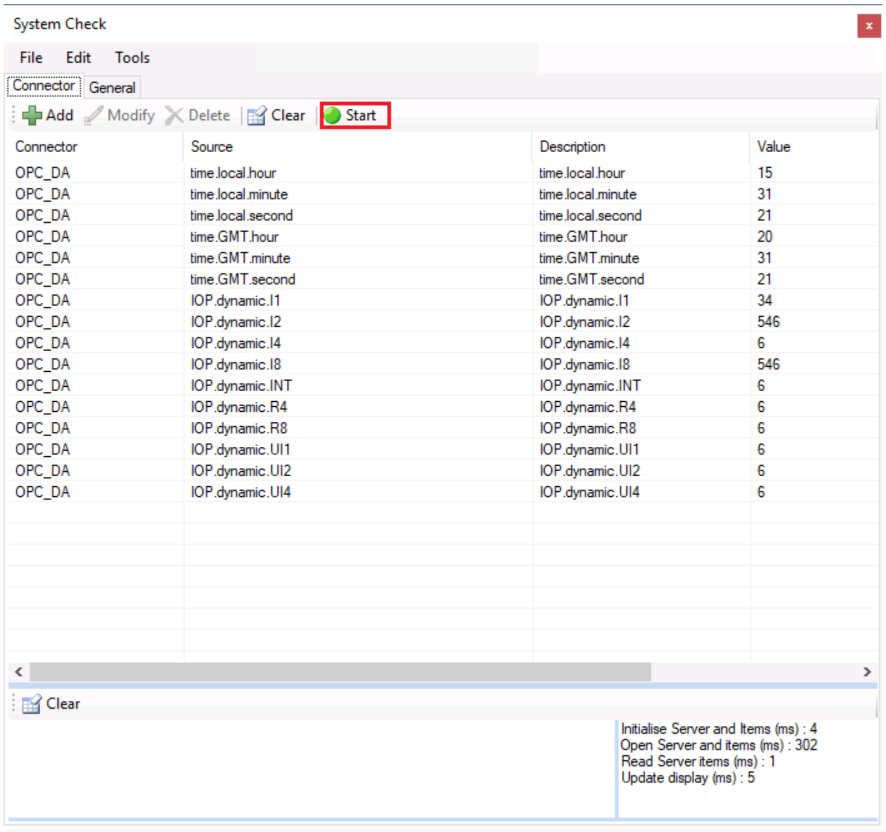
- Click **Add**
- Choose the OPC DA Server Connector from the dropdown list,
- Click the pushbutton ([…]) next to Items to open the Tag Browser window.
- Select one or more tags, click **OK**



Selected Items

Name
time.local.hour
time.local.minute
time.local.second
time.GMT.hour
time.GMT.minute
time.GMT.second
IOP.dynamic.I1
IOP.dynamic.I2
IOP.dynamic.I4
IOP.dynamic.I8
IOP.dynamic.INT
IOP.dynamic.R4
IOP.dynamic.R8
IOP.dynamic.UI1
IOP.dynamic.UI2
IOP.dynamic.UI4

- Click **Start** to verify the communication.



Connector	Source	Description	Value
OPC_DA	time.local.hour	time.local.hour	15
OPC_DA	time.local.minute	time.local.minute	31
OPC_DA	time.local.second	time.local.second	21
OPC_DA	time.GMT.hour	time.GMT.hour	20
OPC_DA	time.GMT.minute	time.GMT.minute	31
OPC_DA	time.GMT.second	time.GMT.second	21
OPC_DA	IOP.dynamic.I1	IOP.dynamic.I1	34
OPC_DA	IOP.dynamic.I2	IOP.dynamic.I2	546
OPC_DA	IOP.dynamic.I4	IOP.dynamic.I4	6
OPC_DA	IOP.dynamic.I8	IOP.dynamic.I8	546
OPC_DA	IOP.dynamic.INT	IOP.dynamic.INT	6
OPC_DA	IOP.dynamic.R4	IOP.dynamic.R4	6
OPC_DA	IOP.dynamic.R8	IOP.dynamic.R8	6
OPC_DA	IOP.dynamic.UI1	IOP.dynamic.UI1	6
OPC_DA	IOP.dynamic.UI2	IOP.dynamic.UI2	6
OPC_DA	IOP.dynamic.UI4	IOP.dynamic.UI4	6

```
Initialise Server and Items (ms) : 4
Open Server and items (ms) : 302
Read Server items (ms) : 1
Update display (ms) : 5
```

OPC UA Real-time values

This connector is used to get real time data from any available OPC UA server either on the local machine or across the network.

Prerequisites

Verify Communication

Communication between the OPC server and an OPC client must be verified. Some OPC Server vendors provide OPC clients with their servers. These clients can be used to validate.

If an OPC client is not provided with the server, you can download the UAExpert OPC UA client from Unified Automation to verify connectivity and data retrieval from the OPC UA server.

Remote Communication

If **XLReporter** is not installed on the same machine as the OPC UA Server, the **XLReporter** machine must have the OPC Core Components installed.

To determine if the core components are installed verify the following file exists:

- C:\Windows\SysWow64\OPCEnum.exe (64-bit OS)
- C:\Windows\system32\OPCEnum.exe (32-bit OS)

If the components are not installed then they are provided in the tools folder of the installation or from www.opcfoundation.org.

Windows Firewall

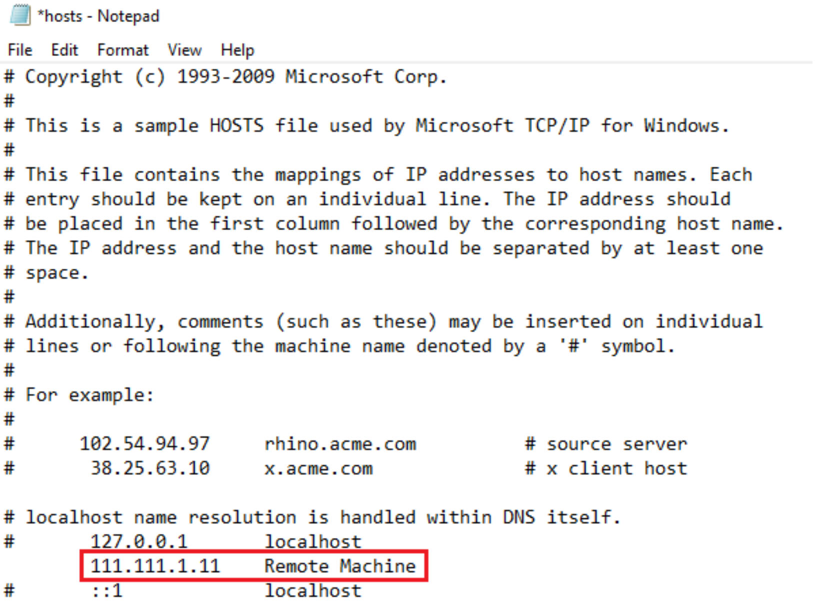
If the Windows Firewall is enabled on the machine where the OPC UA server is running the **Port** configured for the server must be opened in order for remote clients to connect.

OPC Server Certificate Constraints

If the OPC UA server does not contain or contains an incorrect or otherwise unusable IP address, the machine name can be used in its place when establishing the connections. However, if the machine name cannot be associated with a specific IP address, then administrator edits to the HOSTS file on the client machine may be necessary.

The HOSTS file can be found in C:\Windows\System32\drivers\etc. Right-click it and open it in Notepad.

Add an entry similar to the one in the red box below, where *111.111.1.11* is the IP address of the remote machine and *Remote Machine* is the name of that machine that appears in the OPC UA Server certificate.



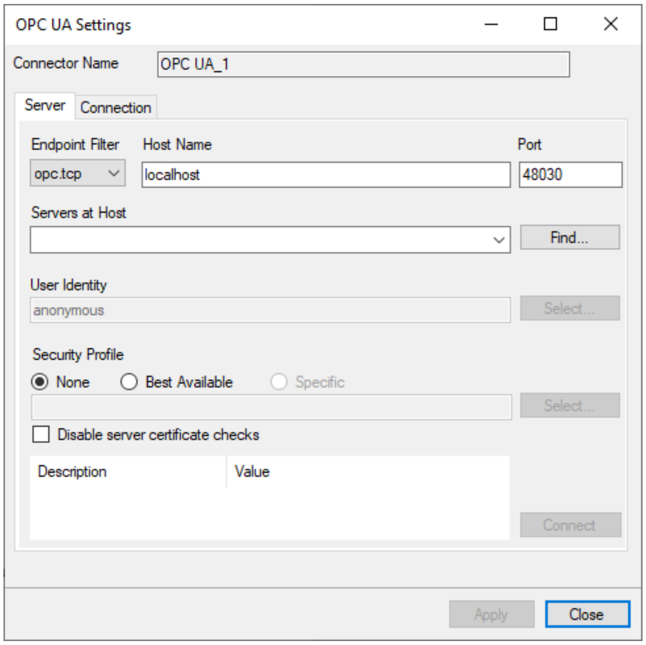
```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
        111.111.1.11    Remote Machine
#       ::1             localhost
```

If the file cannot be saved in this directory, save it to the Documents folder and then copy and overwrite the HOSTS file currently in this directory.

Connector

To configure the connector to the OPC UA server, from the **Project Explorer** select **Data, Connectors**.

- Click **Add**
- Select **OPC, OPC UA Real-time values**
- Click **OK**



Connector Name: OPC UA_1

Endpoint Filter: opc.tcp

Host Name: localhost

Port: 48030

Servers at Host:

User Identity: anonymous

Security Profile: ● None ○ Best Available ○ Specific

□ Disable server certificate checks

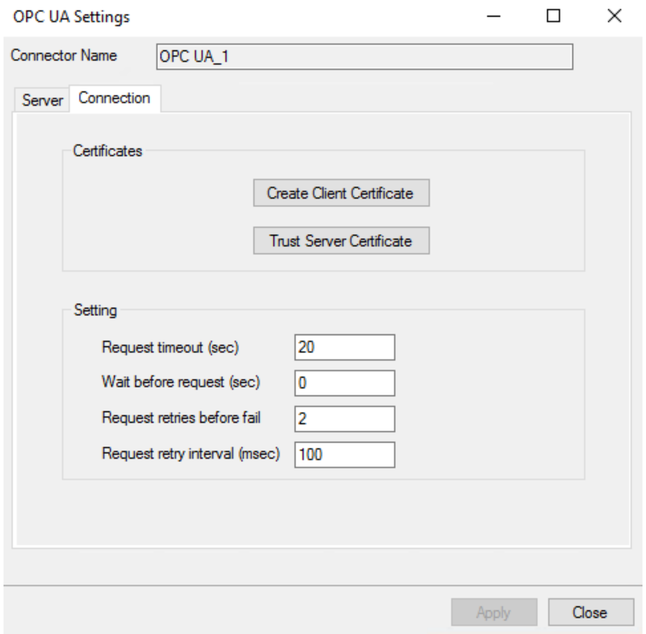
Description	Value

Under the **Server** tab, for **Host Name**, select or enter the name or IP address of the machine where the server is running. Enter the **Port** number as set up in the server.

For **Servers at Host**, click **Find**. Select the one you wish to connect to.

For **User Identity**, click **Select** to specify.

Select the **Connection** tab at the top. Under the **Connection** tab are **Certificates** options and general **Settings**.



Connector Name: OPC UA_1

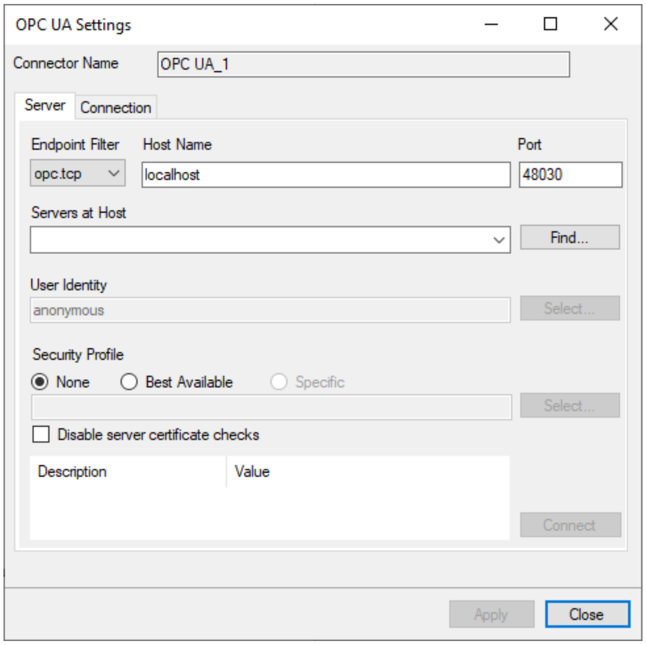
Request timeout (sec): 20

Wait before request (sec): 0

Request retries before fail: 2

Request retry interval (msec): 100

The Client Certificate is automatically created on installation. If required, to recreate the certificate select **Create Client Certificate**. For most OPC UA servers, the default settings will be sufficient, but if the server requires more advanced certificate settings you can specify them with the **Advanced** button.



Connector Name: OPC UA_1

Endpoint Filter: opc.tcp

Host Name: localhost

Port: 48030

Servers at Host:

User Identity: anonymous

● None ○ Best Available ○ Specific

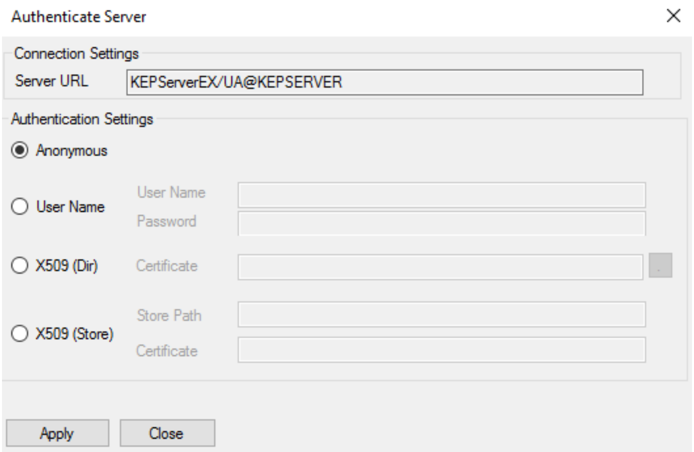
□ Disable server certificate checks

Navigate back to the **Server** tab of the connector. Set **Host Name** to the name or IP address of the server machine.

Typically information about the **Port** number to use can be found in the OPC UA server settings.

The **Servers at Host** dropdown displays all the available servers based on the **Host Name** and **Port**.

Click the **Select** button next to the **User Identity** field.



Authenticate Server

Connection Settings

Server URL: KEPServerEX/UA@KEPSERVER

Authentication Settings

● Anonymous

Depending on the security settings over the **Server**, select an appropriate **User Identity** and click **Apply**.

Select an appropriate **Security Profile** radio button. If **Specific** is chosen, click **Select** on the right to select a specific profile to use.

Click **Get Endpoints** to get the list of available endpoints, select the one that best fits the security settings configured for the server and click **OK**.

Click **Connect** to ensure connectivity. This may require an exchange of certificates between the client and the server. If prompted to exchange, click **Yes**. This action requires Windows administrator rights.

If the **Connect** fails, be sure that the client certificate is trusted by the server and then attempt to **Connect** again.

The **Disable server certificate checks** option can be used to bypass all the checks normally done against the certifcate passed back from the OPC UA server. This is typically used if settings like the *Domain* or *Application URI* do not match what is expected but you would like to proceed with connection. Use this setting with caution as it disables many security features.

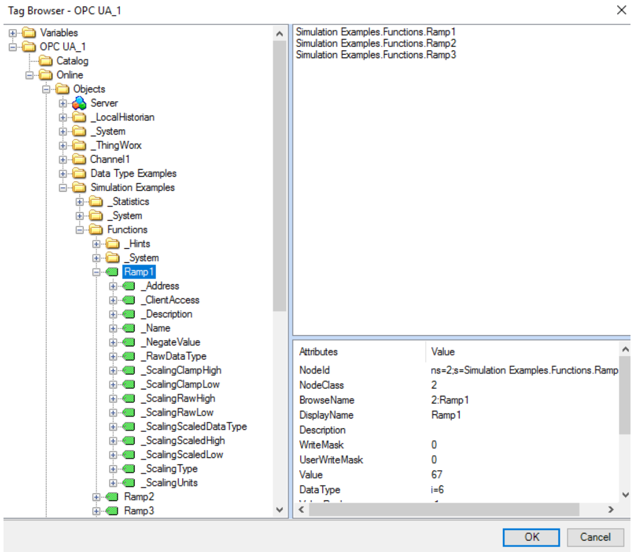
Trusted Clients

In some cases, the OPC UA server must be configured to trust the client certificate submitted in order to establish a connection. Refer to the documentation provided by the specific OPC UA Server for details.

Verify Data Communication

To verify communication to the OPC UA Server, open the **Project Explorer** and select the **Tools** tab. Launch the **System Check** application.

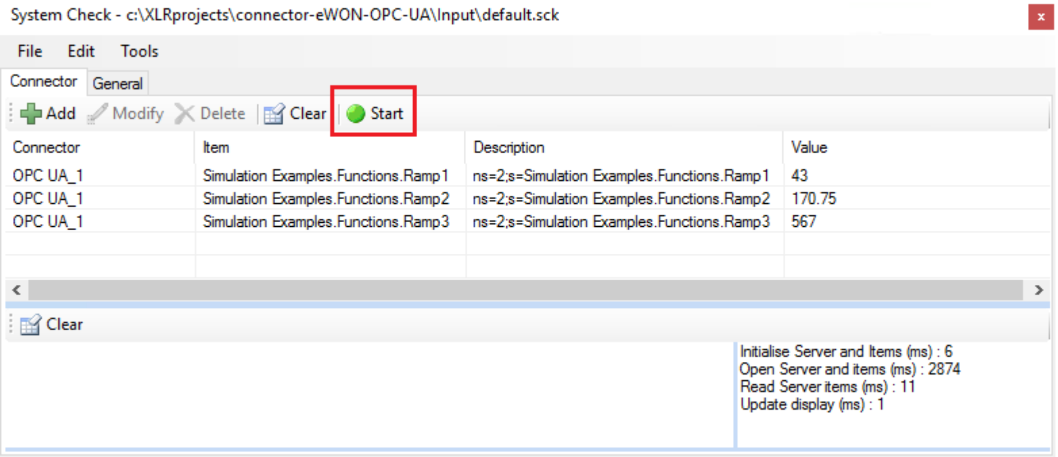
- Click **Add**
- Choose the OPC UA Server Connector from the dropdown list,
- Click the pushbutton ([…]) next to Items to open the Tag Browser window.
- Select one or more tags, click **OK**



Simulation Examples.Functions.Ramp1
Simulation Examples.Functions.Ramp2
Simulation Examples.Functions.Ramp3

Attributes	Value
NodeId	ns=2;s=Simulation Examples.Functions.Ramp
NodeClass	2
BrowseName	2:Ramp1
DisplayName	Ramp1
Description	
WriteMask	0
UserWriteMask	0
Value	67
DataType	i=6

- Click **Start** to verify the communication.


System Check - c:\XLRprojects\connector-eWON-OPC-UA\Input\default.sck
File
Edit
Tools
Connector
General
Add
Modify
Delete
Clear
Start
Clear

Connector	Item	Description	Value
OPC UA_1	Simulation Examples.Functions.Ramp1	ns=2;s=Simulation Examples.Functions.Ramp1	43
OPC UA_1	Simulation Examples.Functions.Ramp2	ns=2;s=Simulation Examples.Functions.Ramp2	170.75
OPC UA_1	Simulation Examples.Functions.Ramp3	ns=2;s=Simulation Examples.Functions.Ramp3	567

```
Initialise Server and Items (ms) : 6
Open Server and items (ms) : 2874
Read Server items (ms) : 11
Update display (ms) : 1
```

OPC HDA Historical values

This connector is used to get historical data from any available OPC HDA server either on the local machine or across the network.

This connector can be used if the OPC HDA server to connect does not have a specific connector available for it.

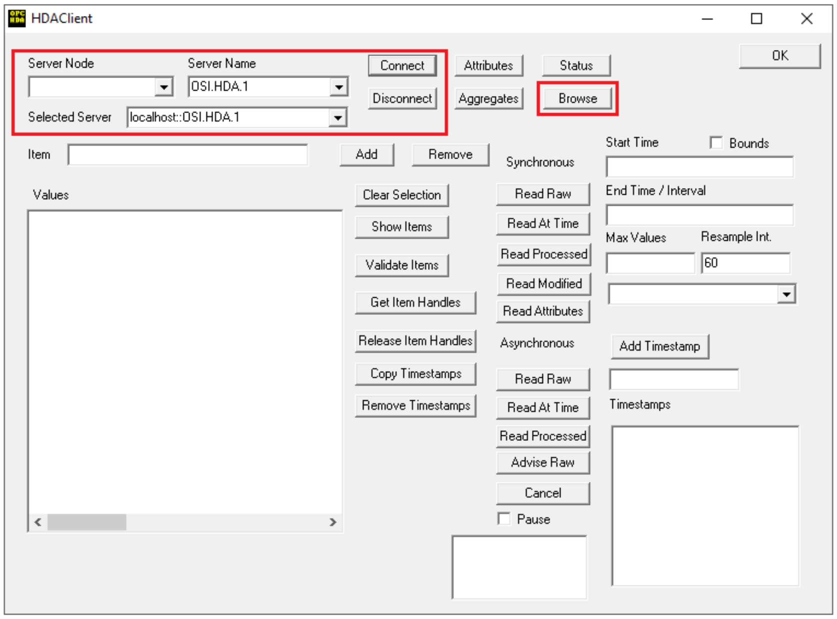
Prerequisites

Verify Communication

Communication between the OPC server and an OPC client must be verified. Some OPC Server vendors provide OPC HDA clients with their servers. These clients can be used to validate.

If an OPC HDA client is not provided with the server, **XLReporter** provides an independent OPC HDA client to verify connectivity and data retrieval from any OPC HDA server. This client is found on **XLReporter's** product CD under **Tools, OPC, OPC_HDA**. It can also be downloaded from www.SyTech.com.

To run, double-click **SampleClientHDA.exe**.



HDAClient

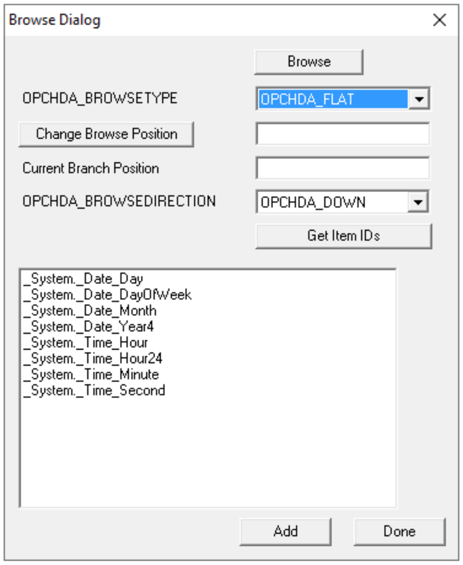
Server Name: OSI.HDA.1

Selected Server: localhost::OSI.HDA.1

Resample Int.: 60

To connect to an OPC HDA server select the **Server Name** from the dropdown list and click **Connect**.

Click **Browse** to open the **Browse Dialog** window.



Browse Dialog

OPCHDA_BROWSETYPE: OPCHDA_FLAT

Current Branch Position

OPCHDA_BROWSEDIRECTION: OPCHDA_DOWN

```
_System._Date_Day
_System._Date_DayOfWeek
_System._Date_Month
_System._Date_Year4
_System._Time_Hour
_System._Time_Hour24
_System._Time_Minute
_System._Time_Second
```

The easiest way to get a list of tags is to set **OPCHDA_BROWSETYPE** to *OPCHDA_FLAT*. Choose each tag to test by selecting it and clicking **Add**. When complete, click **Done** to return to the **HDA Client** window.

Click **Show Items** to display the selected tags in the left pane window. Click **Validate Items** then **Get Item Handles** to register these tags with the server.

Enter the **Start Time** and **End Time** . Note this is in UTC(Universal Time Clock) and click **Read Raw**. The raw values for each selected tag will appear on the left along with a timestamp and quality.

To read processed data, click **Aggregates**, select the appropriate aggregate (e.g., maximum, minimum, etc.). and click **Read Processed**. One minute calculations between the start and end time should appear for each selected tag.

If the client does not respond as described contact the OPC HDA Server vendor technical support to troubleshoot and correct these issues.

Remote Communication

If **XLReporter** is not installed on the same machine as the OPC HDA Server, the **XLReporter** machine must have the OPC Core Components installed.

To determine if the core components are installed verify the following file exists:

- C:\Windows\SysWow64\OPCEnum.exe (64-bit OS)
- C:\Windows\system32\OPCEnum.exe (32-bit OS)

If the components are not installed then they are provided in the tools folder of the installation or from www.opcfoundation.org.

Server Settings

In order to connect to an OPC HDA server remotely both the machine where the server is running and the machine where the client is running must have matching Windows user accounts and the client must be logged in with a matching account.

In addition, on the machine with the OPC HDA server, certain DCOM settings must be enabled. For details on what DCOM settings to enable, see OPC and DCOM 5 things you need to know.

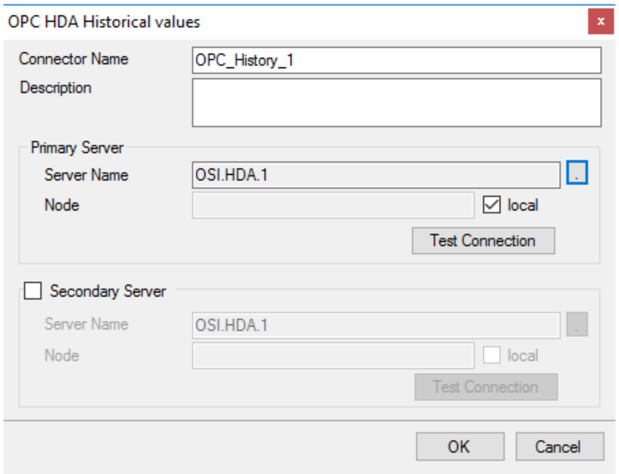
Windows Firewall

If the Windows Firewall is enabled on the machine where the OPC HDA server is running TCP Port 135 must be opened in order for remote clients to connect.

Connector

To configure the connector to the OPC HDA server, from the **Project Explorer** select **Data, Connectors**.

- Click **Add**
- Select **OPC, OPC HDA Historical values**
- Click **OK**



OPC HDA Historical values

Connector Name: OPC_History_1

Description:

Primary Server

Server Name: OSI.HDA.1

Node: ☑ local

☐ Secondary Server

Server Name: OSI.HDA.1

Node: ☐ local

Primary Server

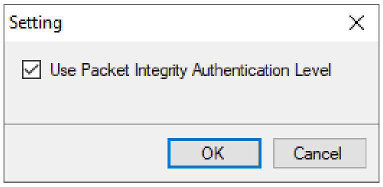
These settings define the **Name** and **Node** of the OPC HDA server. Use the browse button to browse the local or remote machine to select the OPC HDA server.

Use the **Test Connection** button to verify a connection to the server.

Secondary Server

These settings define the (optional) secondary historian to connect to if a connection to the **Primary Server** fails.

Settings



Setting

☑ Use Packet Integrity Authentication Level

If the **Use Pack Integrity Authentication Level** is checked, when a connection is made to a remote OPCHDA server it uses the packet integrity authentication level. This must be set if the Microsoft DCOM hardening has been implemented on the system where the OPCHDA server is installed.

Data Group

The following describes the historical data group settings specific to the **OPC HDA Historical Values** connector.

Group Types

The following group types are available:

Summary Values from Server

This group type retrieves summary calculations directly from the historian. Consult the historian documentation from the OPC HDA server vendor to see what calculations are supported.

Summary Values from XLReporter

This group type retrieves sampled values from the historian and performs calculations on those samples for reporting.

By default, summary values are calculated time weighted and values are propagated based on the last known value. However, to change this so that summary values are calculated strictly on the data returned check **use raw values**.

Raw Values

This group retrieves values logged to the historian between the start and end time specified.

Group Settings

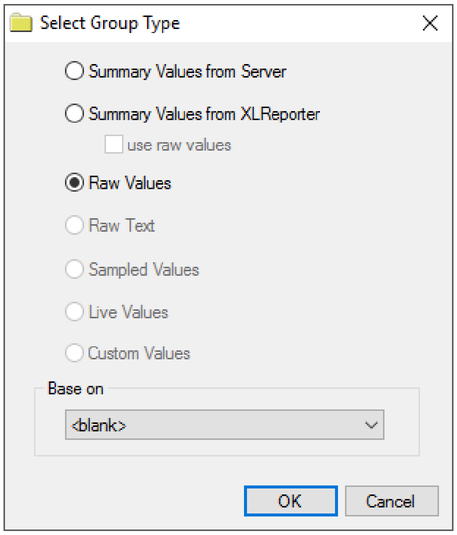
Setup Tab (Summary Values for XLReporter)

The **Retrieval** settings define how data is retrieved for the calculations selected for the group. The following settings are available:

- **Retrieval Mode**
  This setting defines how data is retrieved from the historian. Both *Sampled Values* and *Raw Values* are available where *Sampled Values* uses the *Interpolated* calculation. Note, if the OPC HDA server does not support the *Interpolated* calculation, do not use *Sampled Values*.
- **Rate**
  The interval (in seconds) that sampled values are retrieved from the historian.
- **Lead Time**
  The amount of time (in seconds) to retrieve data before the start time.

Verify Data Communication

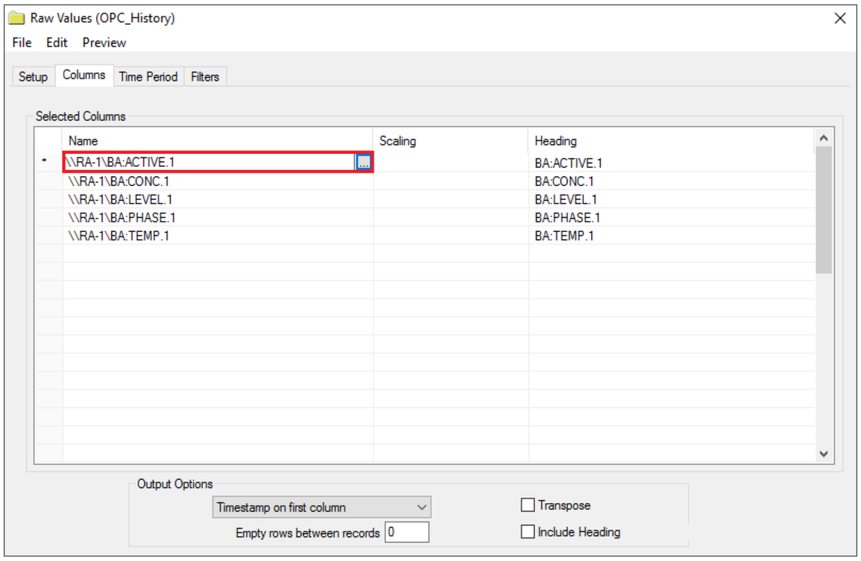
To verify communication with the OPC HDA Server, open the **Project Explorer** and select the **Tools** tab. Open **Connector Groups**. Select your OPC HDA Server connector and then select **Add**.



○ Summary Values from Server
○ Summary Values from XLReporter
□ use raw values
● Raw Values
○ Raw Text
○ Sampled Values
○ Live Values
○ Custom Values
Base on
<blank>

Set the Group Type to **Raw Values** and click **OK**.

On the **Columns** tab:



Name	Scaling	Heading
\\RA-1\BA:ACTIVE.1		BA:ACTIVE.1
\\RA-1\BA:CONC.1		BA:CONC.1
\\RA-1\BA:LEVEL.1		BA:LEVEL.1
\\RA-1\BA:PHASE.1		BA:PHASE.1
\\RA-1\BA:TEMP.1		BA:TEMP.1

Timestamp on first column

Empty rows between records 0

□ Transpose

□ Include Heading

- Select the first row under the **Name** column
- Click the browse pushbutton (…)
- In the Tag Browser expand **Online** and add **Items** from the lower left.
- Click **OK** to add these to the group.

To retrieve data, select **Preview**. In the **Preview** window, use the data picker to select a date and time with for which data has been logged. Click **Refresh** to view data. The first 60 records starting at the date and time specified should be displayed.

OPC UA HA Historical values

This connector is used to get historical data from any available OPC UA HA server either on the local machine or across the network.

Prerequisites

Verify Communication

Communication between the OPC server and an OPC client must be verified. Some OPC Server vendors provide OPC clients with their servers. These clients can be used to validate.

If an OPC client is not provided with the server, you can download the UAExpert OPC UA client from Unified Automation to verify connectivity and data retrieval from the OPC UA HA server.

To retrieve historical data with UA Expert, first identify a variable (tag) that has the **Historizing** attribute set *true*. Then, from the **Document** menu select **Add**. Set **Document Type** to *History Trend View* and click **Add**. The trend can display any variable added to the **Configuration** section.

Remote Communication

If **XLReporter** is not installed on the same machine as the OPC UA HA Server, the **XLReporter** machine must have the OPC Core Components installed.

To determine if the core components are installed verify the following file exists:

- C:\Windows\SysWow64\OPCEnum.exe (64-bit OS)
- C:\Windows\system32\OPCEnum.exe (32-bit OS)

If the components are not installed then they are provided in the tools folder of the installation or from www.opcfoundation.org.

Windows Firewall

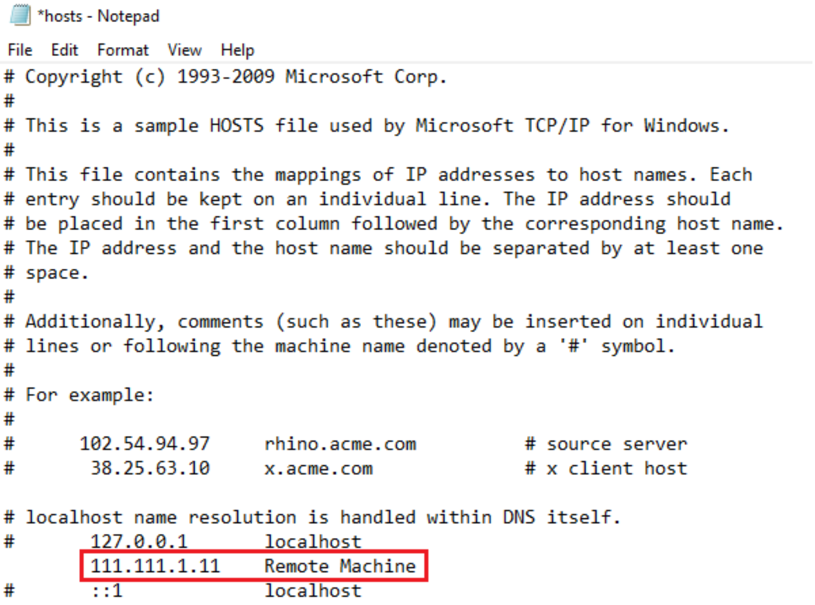
If the Windows Firewall is enabled on the machine where the OPC UA HA server is running the **Port** configured for the server must be opened in order for remote clients to connect.

OPC Server Certificate Constraints

If the OPC UA server does not contain or contains an incorrect or otherwise unusable IP address, the machine name can be used in its place when establishing the connections. However, if the machine name cannot be associated with a specific IP address, then administrator edits to the HOSTS file on the client machine may be necessary.

The HOSTS file can be found in C:\Windows\System32\drivers\etc. Right-click it and open it in Notepad.

Add an entry similar to the one in the red box below, where *111.111.1.11* is the IP address of the remote machine and Remote Machine is the name of that machine that appears in the OPC UA Server certificate.

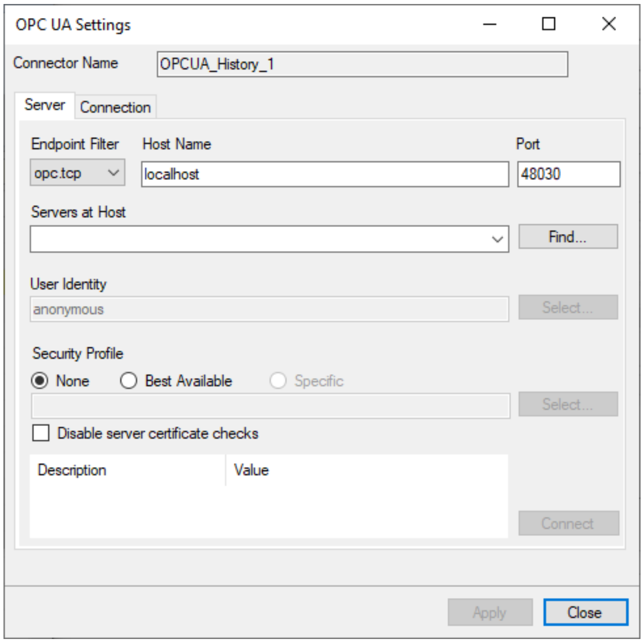


```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
        111.111.1.11    Remote Machine
#       ::1             localhost
```

If the file cannot be saved in this directory, save it to the Documents folder and then copy and overwrite the HOSTS file currently in this directory.

Connector

The connector defines the OPC UA HA server to connect to.



Connector Name: OPCUA_History_1

Endpoint Filter: opc.tcp

Host Name: localhost

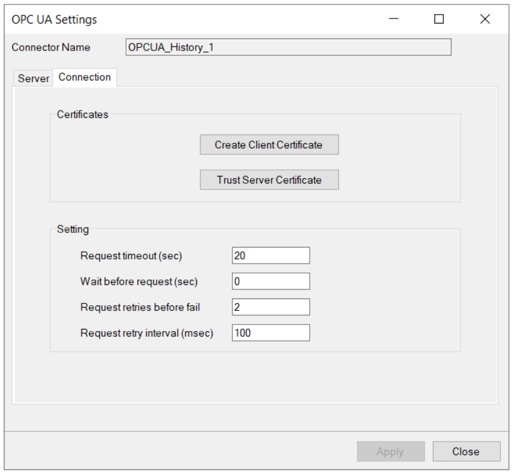
Port: 48030

User Identity: anonymous

Security Profile: ● None ○ Best Available ○ Specific

□ Disable server certificate checks

Enter the **Host Name** where the server resides and enter the **Port** number as set up in the server. The **Endpoint Filter** can be changed as necessary, however *opc.tcp* should be correct for most endpoints. **Server at Host** shows you all the available servers based on the settings. Select the one you wish to connect to. Select the **Connection** tab at the top.



OPC UA Settings

Connector Name: OPCUA_History_1

Server | Connection

Certificates

Setting

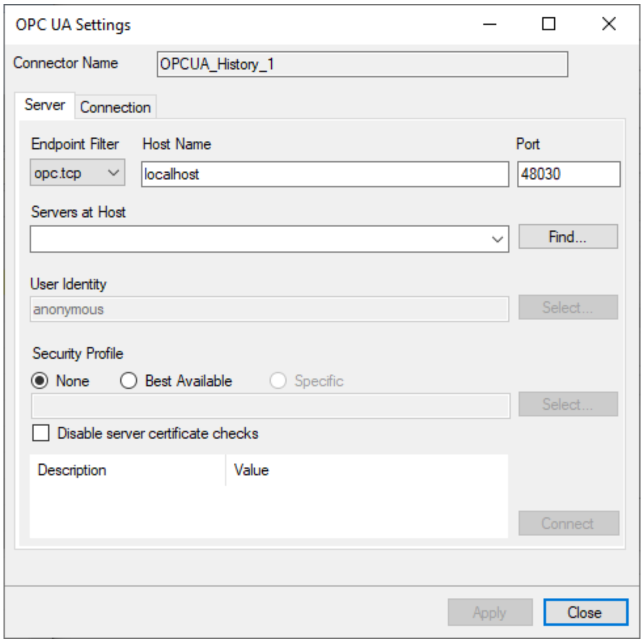
Request timeout (sec): 20

Wait before request (sec): 0

Request retries before fail: 2

Request retry interval (msec): 100

The Client Certificate is automatically created on installation. If required, to recreate the certificate select **Create Client Certificate**. For most OPC UA HA servers, the default settings will be sufficient, but if the server requires more advanced certificate settings you can specify them with the **Advanced** button. Click **Create** to creating the client certificate.



OPC UA Settings

Connector Name: OPCUA_History_1

Server | Connection

Endpoint Filter: opc.tcp

Host Name: localhost

Port: 48030

Servers at Host:

User Identity: anonymous

Security Profile: ● None ○ Best Available ○ Specific

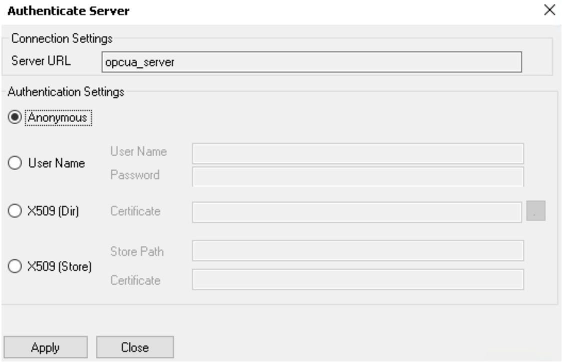
□ Disable server certificate checks

Description	Value

Navigate back to the **Server** tab of the connector. Set **Host Name** to the name or IP address of the server machine.

Typically information about the **Port** number to use can be found in the OPC UA HA server settings.

The **Servers at Host** dropdown displays all the available servers based on the **Host Name** and **Port**. Click the **Select** button next to the **User Identity** field.



Authenticate Server

Connection Settings

Server URL: opcua_server

Authentication Settings

● Anonymous

○ User Name — User Name: Password:

○ X509 (Dir) — Certificate:

○ X509 (Store) — Store Path: Certificate:

Depending on the security settings over the **Server**, select an appropriate **User Identity** and click **Apply**.

Select an appropriate **Security Profile** radio button. If **Specific** is chosen, click **Select** on the right to select a specific profile to use.

Click **Connect** to ensure connectivity. This may require an exchange of certificates between the client and the server. If prompted to exchange, click **Yes**. This action requires Windows administrator rights.

If the **Connect** fails, be sure that the client certificate is trusted by the server and then attempt to **Connect** again.

The **Disable server certificate checks** option can be used to bypass all the checks normally done against the certifcate passed back from the OPC UA server. This is typically used if settings like the *Domain* or *Application URI* do not match what is expected but you would like to proceed with connection. Use this setting with caution as it disables many security features.

Data Group

The following describes the historical data group settings specific to the **OPC UA HA Historical Values** connector.

Group Types

The following group types are available:

Summary Values from Server

This group type retrieves summary calculations directly from the historian.

Summary Values from XLReporter

This group type retrieves sampled values from the historian and performs calculations on those samples for reporting.

By default, summary values are calculated time weighted and values are propagated based on the last known value. However, to change this so that summary values are calculated strictly on the data returned check **use raw values**.

Raw Values

This group retrieves values logged to the historian between the start and end time specified.

Group Settings

Setup Tab (Summary Values for XLReporter)

The **Retrieval** settings define how data is retrieved for the calculations selected for the group. The following settings are available:

- **Retrieval Mode**
  This setting defines how data is retrieved from the historian. Both *Sampled Values* and *Raw Values* are available where *Sampled Values* uses the *Interpolated* calculation. Note, if the OPC UA HA server does not support the *Interpolated* calculation, do not use *Sampled Values*.
- **Rate**
  The interval (in seconds) that sampled values are retrieved from the historian.
- **Lead Time**
  The amount of time (in seconds) to retrieve data before the start time.

Server Calcuations

The following calculations are presented when a Summary Values from Server data group is configured. Please consult the documentation on your specific OPC UA HA server to see which calculations are supported.

- **Interpolated**
  The calculated value at the beginning of the interval based on data points before and after the timestamp.
- **Average**
  The time weighted average over the interval using interpolated bounding values.
- **Average 2**
  The time weighted average over the interval using simple bounding values.
- **Maximum**
  The maximum raw value in the interval.
- **Maximum 2**
  The maximum value in the interval including the simple bounding values.
- **Time of Maximum**
  The timestamp of the maximum raw value in the interval.
- **Time of Maximum 2**
  The timestamp of the maximum value in the interval including the simple bounding values.
- **Minimum**
  The minimum raw value in the interval.
- **Minimum 2**
  The minimum value in the interval including the simple bounding values.
- **Time of Minimum**
  The timestamp of the minimum raw value in the interval.
- **Time of Minimum 2**
  The timestamp of the minimum value in the interval including the simple bounding values.
- **Range**
  The difference between the maximum and minimum values in the interval.
- **Range 2**
  The difference between the maximum 2 and minimum 2 values in the interval.
- **Standard Deviation Sample**
  The standard deviation for the interval for a sample of the population (n-1)
- **Standard Deviation Population**
  The standard deviation for the interval for the entire population (n) including the simple bounding values.
- **Variance Sample**
  The variance for the interval as calculated by the standard deviation sample.
- **Variance Population**
  The variance for the interval as calculated by the standard deviation population.
- **Total**
  The total (time integral) for the interval including interpolated bounding values.
- **Total 2**
  The total (time integral) for the interval including simple bounding values.
- **Count**
  The number of raw values for the interval.
- **Average (raw)**
  The average value for the interval (sum of raw values divided by count of raw values).
- **Start Value**
  The first raw value for the interval.
- **End Value**
  The last raw value for the interval.
- **Delta Value**
  The difference between the start and end values of the interval.
- **Start Bound**
  The value at the beginning of the interval using simple bounding values.

- **End Bound**
  The value at the end of the interval using simple bounding values.
- **Delta Bounds**
  The difference between the start and end bound values of the interval.
- **Annotation Count**
  The number of annotations in the interval.
- **Duration Good**
  The total time in the interval during wich data is good quality.
- **Duration Bad**
  The total time in the interval during wich data is bad quality.
- **Percentage Good**
  The percentag of time in the interval (0-100) during wich data is good quality.
- **Percentage Bad**
  The percentag of time in the interval (0-100) during wich data is bad quality.
- **Worst Quality**
  The worst status code of data in the interval.
- **Worst Quality 2**
  The worst status code of data in the interval including simple bounding values.
- **Duration in State Zero**
  The time a boolean or numeric value was in a zero state during the inteval including simple bounding values.
- **Duration in State Non Zero**
  The time a boolean or numeric value was in a non zero state during the inteval including simple bounding values.
- **Number of Transactions**
  The number of changes between a zero and non zero state for a boolean or numeric value during the interval.

Bounding Values

- Intepolated Bounding Values
  Bounding values determined by a calculation using the nearest Good quality value.
- Simple Bounding Values
  Bounding values determined by a calculation using the nearest value regardless of quality.

Information in this document is subject to change without notice. SmartSights, LLC assumes no responsibility for any errors or omissions that may be in this document. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the prior written permission of SmartSights, LLC.