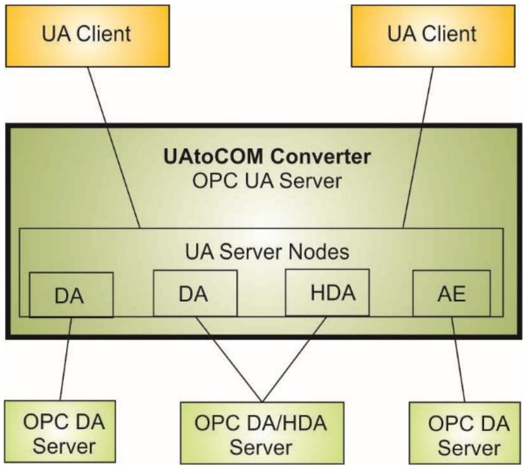
UAtoCOM Converter Server User Manual

Content

Overview

UAtoCOM is an OPC UA server with the capability to aggregate multiple OPC DA, HDA and/or AE servers. OPC UA clients can access Classic OPC DA, HDA, AE servers thru the UAtoCOM converter server.



The **UAtoCOM** converter makes Classic OPC servers accessible from OPC UA client applications.

UAtoCOM can be configured to handle multiple OPC DA, HDA and/or AE servers.

UAtoCOM can e.g. be used to access remote OPC servers. In combination with the Advosol COMtoUA converter server, Classic OPC clients can access remote OPC servers thru a secure UA communication link.

License

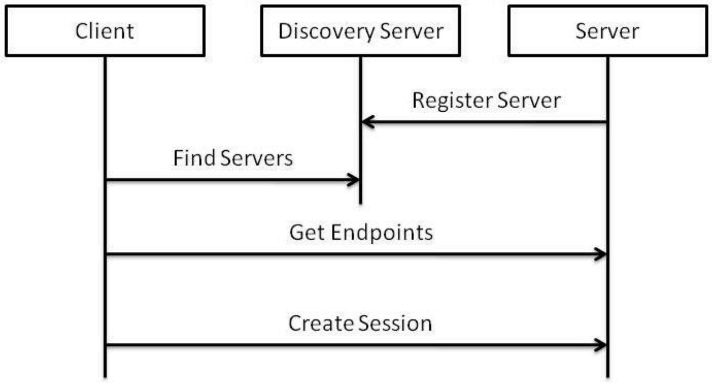
Without license the COMtoUA converter server works in evaluation mode and must only be used for evaluation purposes. In evaluation mode the server stops working after 30 minutes runtime and needs to be restarted to work again for 30 minutes.

The license file ***COMtoUA.vv.license*** (vv is the version number) must be copied into the directory with the COMtoUA.NET4.exe executable.
Or, the text content of the license file can be copied into the COMtoUA.NET4.exe.config application configuration file:

```
<AppSettings>
    <add key ="license" value="content from the license file"/>
```

UA Server Access and Security Basics

Client applications need to know the URL of the UA server endpoint. UA servers can be configured for multiple endpoints to support different communication protocols and security levels.
UA Discovery features simplify finding the available endpoint URLs. Each UA server has a Discover endpoint that can be accessed without security to get the endpoint details. UA servers register with UA discovery servers. Client can find the URL of the UA server Discover endpoint from the UA Discovery server.



The **UA security model** has two key elements: application certificates and secure channels. Application certificates are used to identify specific instances of UA applications and are no different from the ubiquitous SSL certificates which are used to provide security for Internet commerce applications. The difference is the UA security model is not limited to SSL as an implementation technology so UA uses a more general term.

Secure channels are logical connections between applications that are used ensure that the messages exchanged cannot be intercepted or altered during transmission. HTTPS and WS-Secure Conversation are examples of technologies that can be used to implement a UA secure channel.

UA application certificates are **X509 certificates** which rely on a secret (called a private key) only known to the legitimate holder of the certificate. A UA application can prove it knows the secret by creating digital signatures which can be verified with the public key contained in the certificate. These certificates can be issued by anyone but UA applications use the issuer to determine whether a certificate can be trusted. UA applications must never communicate with an application that they do not trust.

What this all means is a developer must always start by creating a certificate for their UA applications. Some UA applications, especially demo applications, create automatically self-signed application certificates. Unfortunately such a simplified handling works only with the client and server application on the same machine and both configured to use the same certificate store location.
For a certificate management that works in all situation please study the chapter Certificate Management.

UAtoCOM Setup

The UAtoCOM software is provided as an installer package.
Running the setup installs the software on the machine.

Steps after the UAtoCOM converter server software is installed:

1. Run the **UAtoCOMconfig** utility to:
   - Change the default UAtoCOM URLs and access policies to match the application requirements.
     Select the trace output options.

   - Create the security certificate for the UAtoCOM converter UA server.
     Either create a self-signed certificate or import a certificate purchased from a certificate authority.
     The certificate permission settings may have to be edited to include the user account running UAtoCOM.

   - Define the Classic OPC DA/HDA/AE servers that need to be accessible from UA clients.
     The DCOM configuration of the servers may have to be changed to allow access from the user account that is running UAtoCOM. This may be the Interactive account or e.g. SYSTEM if UAtoCOM is running as a Windows Service.

   - Optionally install UAtoCOM as a Windows Service.
     It's recommended to initially test the operation with UAtoCOM running as a process.

2. Start the UAtoCOM operation by executing UaToComNet4.exe

3. Test with a local UA test client
   The UAtoCOM distribution includes UA test clients:
   - UA Explorer Client   UaExplorerClient.Net4.exe
     Best suited to test the UA server access
   - Test clients for DA, HDA and AE functionality
     These clients can access UA servers and Classic OPC servers directly.

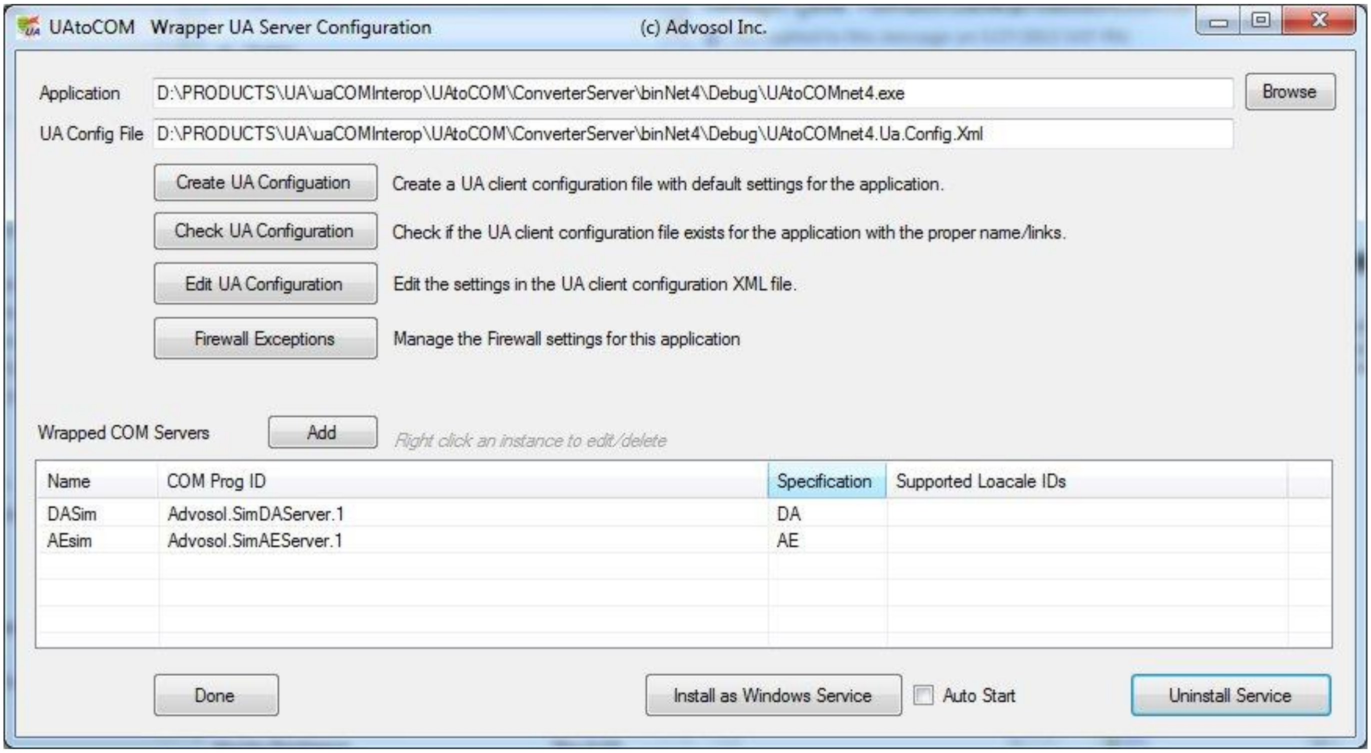
- OPCDATestClientUaNet4.exe	for Classic OPC DA functionality
- HDA-UATestClientNet4.exe	for Classic OPC HDA functionality
- AE-UATestClientNet4.exe	for Classic OPC AE functionality

The UA test applications need to be configured with a certificate before they can be used.
The UaClientConfigHelperNet4.exe utility is provided for this.

UAtoCOM Configuration

The ***UAtoCOMconfig*** utility is provided for creating and editing the UAtoCOM configuration.
The configuration has two main parts:

- The UA server endpoint configuration with the logging and certificates
- The wrapped COM servers



UAtoCOM Wrapper UA Server Configuration (c) Advosol Inc.

Application D:\PRODUCTS\UA\uaCOMInterop\UAtoCOM\ConverterServer\binNet4\Debug\UAtoCOMnet4.exe

UA Config File D:\PRODUCTS\UA\uaCOMInterop\UAtoCOM\ConverterServer\binNet4\Debug\UAtoCOMnet4.Ua.Config.Xml

Create UA Configuation — Create a UA client configuration file with default settings for the application.

Check UA Configuration — Check if the UA client configuration file exists for the application with the proper name/links.

Edit UA Configuration — Edit the settings in the UA client configuration XML file.

Firewall Exceptions — Manage the Firewall settings for this application

Wrapped COM Servers — Right click an instance to edit/delete

Name	COM Prog ID	Specification	Supported Loacale IDs
DASim	Advosol.SimDAServer.1	DA	
AEsim	Advosol.SimAEServer.1	AE	

□ Auto Start

Click ***Edit UA Configuration*** to manage the endpoints, the security certificate and the logging level .
Select detailed logging levels with tracing only when necessary. The log file can quickly get big and performance is reduced.

Right click a wrapped COM server instance to modify or delete the definition.

UAtoCOM can run

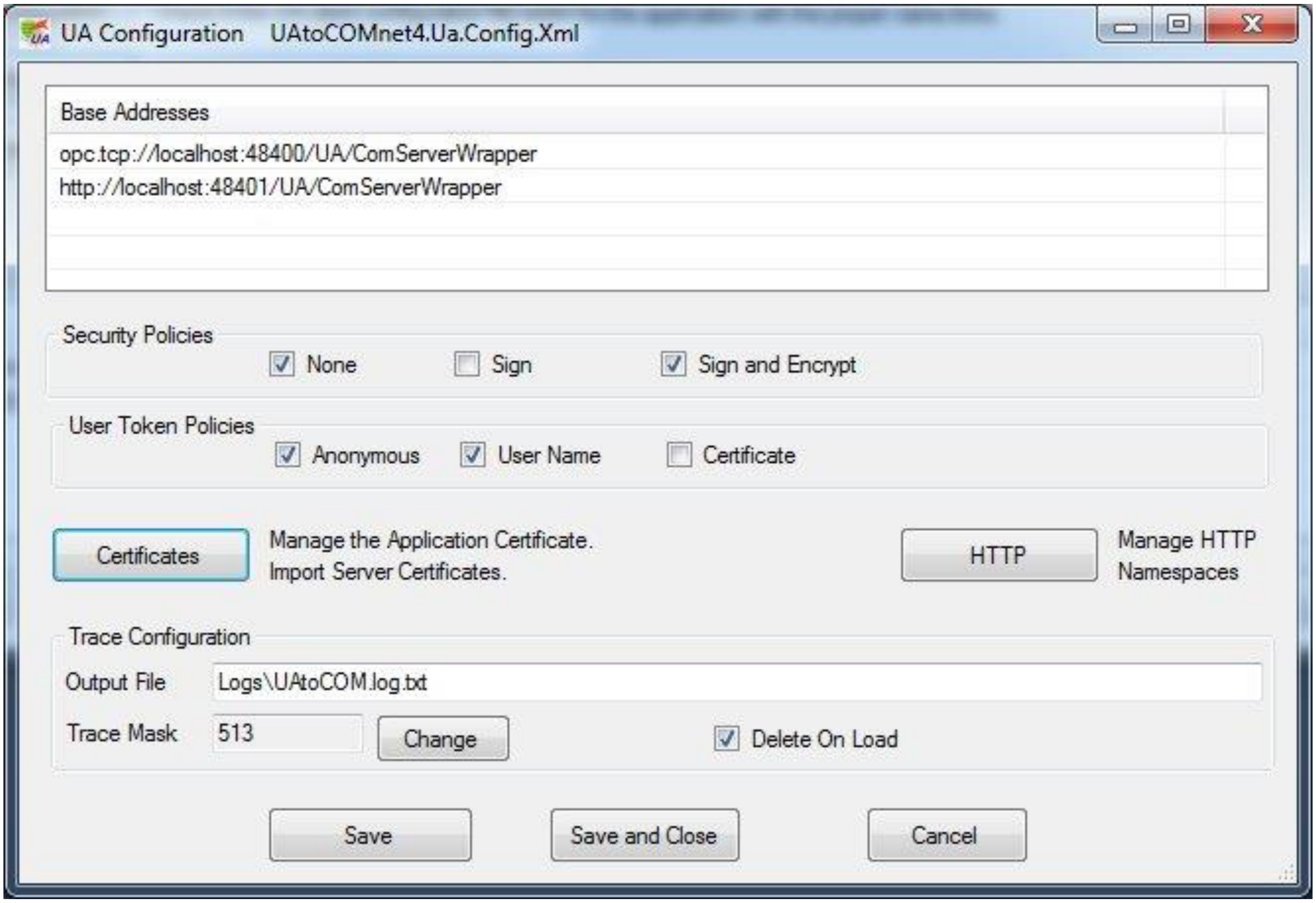
- as process with or without a visible status window
- as a Windows service.

The visibility of the status window is configured in the AppSettings section of the ***UAtoCOM.exe.config*** application configuration file:

```
<appSettings >
    <add key ="VisibleInTray" value="yes"/>
    <add key ="VisibleWindow" value="yes"/>
    <add key ="ShowStatusInfo" value="yes"/>
</appSettings>
```

UA Server Endpoints

The UAtoCOM UA server can be configured with endpoints for the desired communication protocols and security levels.



UA Configuration UAtoCOMnet4.Ua.Config.Xml

Base Addresses

opc.tcp://localhost:48400/UA/ComServerWrapper
http://localhost:48401/UA/ComServerWrapper

Security Policies: ☑ None □ Sign ☑ Sign and Encrypt

User Token Policies: ☑ Anonymous ☑ User Name □ Certificate

Manage the Application Certificate.
Import Server Certificates.

Manage HTTP Namespaces

Trace Configuration

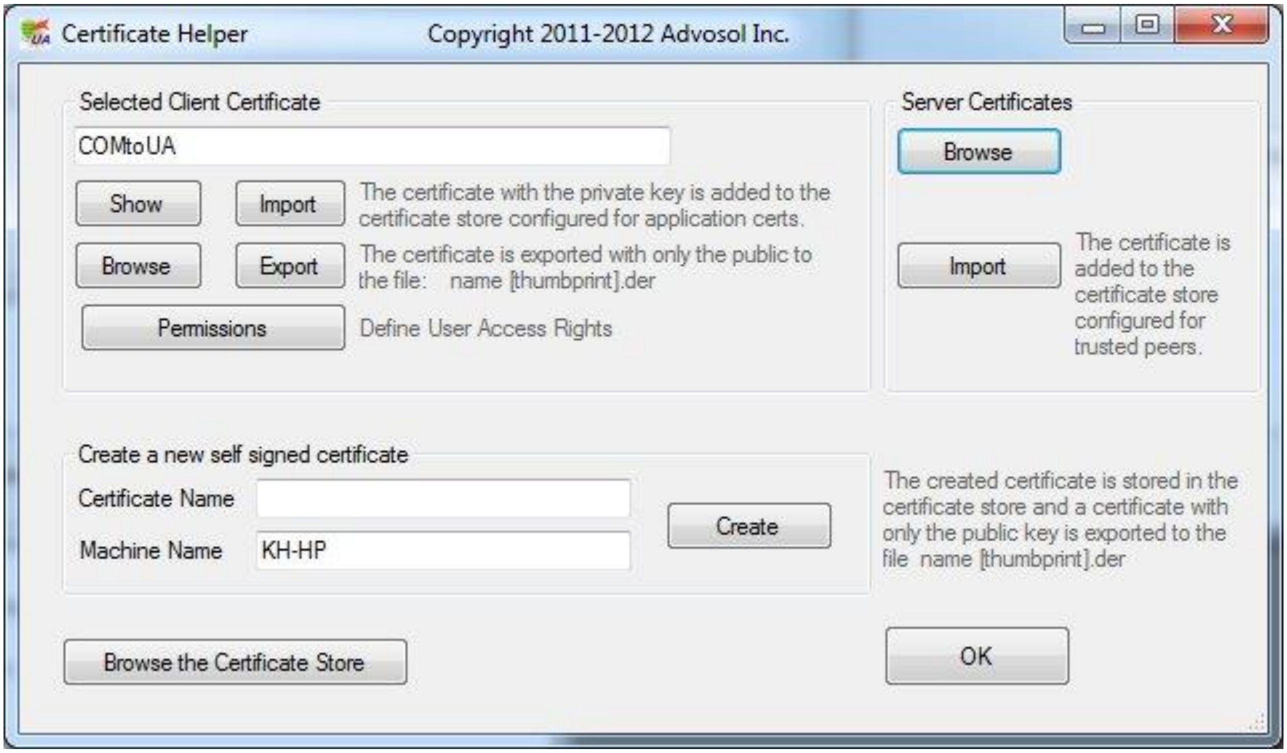
Output File: Logs\UAtoCOM.log.txt

Trace Mask: 513

☑ Delete On Load

To change a base address, select the text and then click the selected text to enable editing.

Right click a base address to delete it or add a new address.



Certificate Helper Copyright 2011-2012 Advosol Inc.

Selected Client Certificate: COMtoUA

The certificate with the private key is added to the certificate store configured for application certs.

The certificate is exported with only the public to the file: name [thumbprint].der

Define User Access Rights

Server Certificates

The certificate is added to the certificate store configured for trusted peers.

Create a new self signed certificate

Certificate Name:

Machine Name: KH-HP

The created certificate is stored in the certificate store and a certificate with only the public key is exported to the file name [thumbprint].der

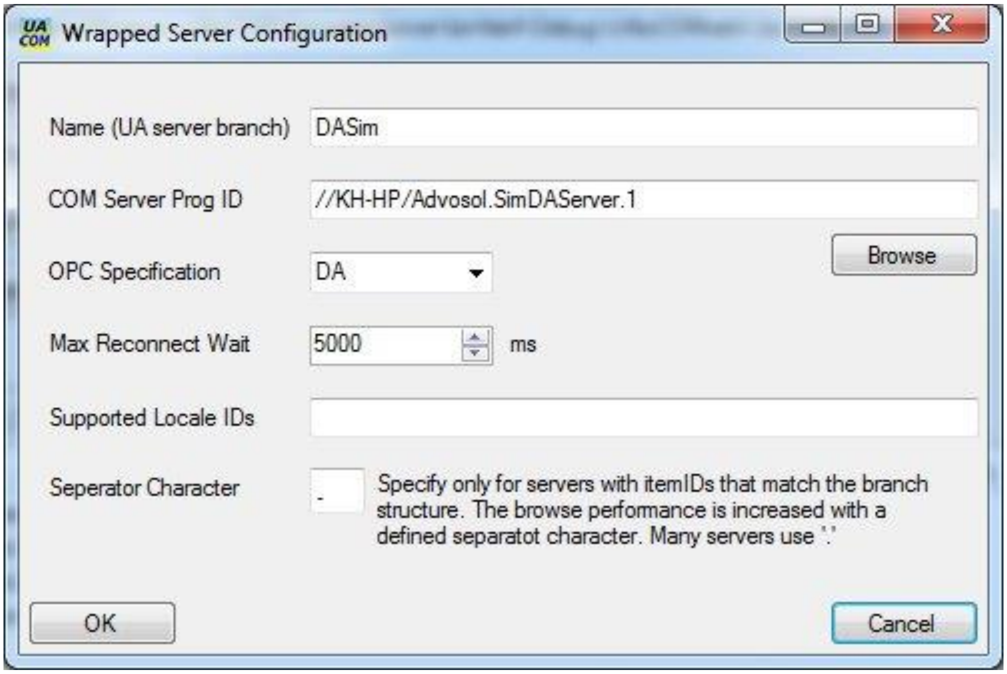
The user account running the UAtoCOM server must have Read for the certificate.
Use the ***Permissions*** dialog to manage the certificate access rights.

Username / Password Credentials

Username/password credentials are checked against existing Windows user accounts.
The client specified credentials are accepted if they match an existing Windows account.

This eliminate the need for username/password definitions in the application configuration file.
If needed an additional Windows account can be created for this use only.

Wrapped COM Server Configuration



Name (UA server branch): DASim

COM Server Prog ID: //KH-HP/Advosol.SimDAServer.1

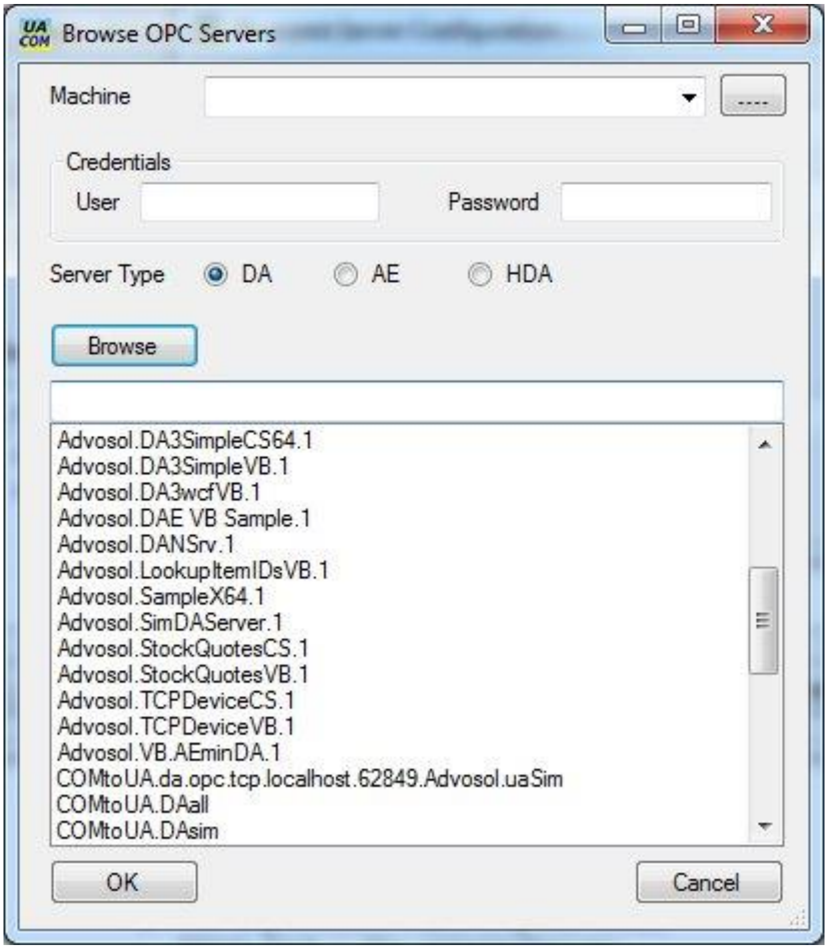
OPC Specification: DA

Max Reconnect Wait: 5000 ms

Supported Locale IDs:

Seperator Character: .

Specify only for servers with itemIDs that match the branch structure. The browse performance is increased with a defined separatot character. Many servers use '.'



Machine:

Credentials

User:

Password:

Server Type ● DA ○ AE ○ HDA

Advosol.DA3SimpleCS64.1
Advosol.DA3SimpleVB.1
Advosol.DA3wcfVB.1
Advosol.DAE VB Sample.1
Advosol.DANSrv.1
Advosol.LookupItemIDsVB.1
Advosol.SampleX64.1
Advosol.SimDAServer.1
Advosol.StockQuotesCS.1
Advosol.StockQuotesVB.1
Advosol.TCPDeviceCS.1
Advosol.TCPDeviceVB.1
Advosol.VB.AEminDA.1
COMtoUA.da.opc.tcp.localhost.62849.Advosol.uaSim
COMtoUA.DAall
COMtoUA.DAsim

Certificates and their Management

OPC UA uses X509 certificates for the authentication of UA server and client applications.

The configuration tools provided with UAtoCOM include features for the X509 certificate management.

Most difficulties with OPC UA applications are related to security certificates and a basic understanding of the certificate concept can help considerably.

Certificate Basics:

- Certificate Use
  Each UA application (server and client) needs a certificate created for this application. It identifies the application. The communication partner application imports the distributed certificate and uses it in the communication to ensure that it communicates with the application that issued the certificate.

- Domains
  Certificates are issued for a particular domain. In a LAN the domain is usually the network machine name or IP address. In remote access through firewalls the situation is not as simple. The domain the remote client uses is different and there may be multiple domains that point to the same machine.

- Certificate Creation
  X509 certificates can be created as self-signed certificates or they can be purchased from a certificate authority. For internal use self-signed certificates are usually sufficient.
  A certificate needs to be created for each UA application (server or client).
  Certificates are created with a private and a public key. For distribution to communication partner applications the certificate is exported with only the public key.

- Certificate Access Permissions
  Certificates in the Windows store and files in directories have access rights security settings. The default may not allow non-administrator users access. The user account running the UA application must have certificate read access rights. The Advosol configuration utilities have a Permissions setting feature.

- Certificate Store
  Certificates can be stored in the Windows Certificate Store or as files in any directory. The location is defined for each UA application in the application UA configuration XML file.
  The Advosol UA products are distributed with configuration settings for the Windows Certificate Store. The Advosol UA configuration tools are designed for the Windows Certificate Store.

The Advosol UA applications use the Windows Certificate Store. The application configuration utilities provide features for the creation and import/export of certificates.

UA products from other vendors may use different certificate locations. Even if these applications run on the same machine the certificates need to exported into a DER file and imported by the partner application to ensure the both application find the certificate.

Performance

OPC UA has an information model that is very different form Classic OPC DA and the specified interface methods are differently structured. The consequence is that the UAtoCOM converter has to make multiple Classic OPC server calls to gather all the information the needs to be returned in the UA method result.
The same is true for COMtoUA, the converter in the opposite direction. Converting in both directions causes a significant overhead, especially in browsing operations.

UAtoCOM implements sophisticated optimization and caching mechanisms to minimize server calls and optimize performance. OPC DA V3 methods are used if the OPC DA server supports these.

Separator Character Configuration Definition

OPC DA servers organize the items in a tree structure but the item ID used for read write access doesn't necessarily have to be the concatenated branch and item names. This freedom given by the OPC DA specification complicates browsing. The item ID has to be retrieved from the server for each browsed item.
For servers that use item IDs strictly according the tree structure, such as: b1.b2.b3.i1
the item IDs can instead be manipulated with string operations.
The item ID can be generated by appending the item name to the branch ID, or the ID of the branch can be obtained from the item ID by splitting off the item name.
Many servers use the period character '.' as the separator character between the concatenated branch and item names. However, the OPC DA specification allows other characters to be used.

For servers with few items browsing is quick, independent on how it has to be done. For servers with ten or hundred thousands of items browsing can become extremely slow if it involves multiple server calls for each item.

Specify the separator character in the UAtoCOM configuration if possible to improve browse performance.

Trouble Shooting

Most difficulties with OPC UA applications are related to security certificates.
See the above chapter Certificate Management for a basic description.

Certificates can be stored in the Windows Certificate Store or as files in any directory. The location is defined for each UA application in the application UA configuration XML file.
The Advosol UA products are distributed with configuration settings for the Windows Certificate Store.

UA products from other vendors may use different certificate locations. Even if these applications run on the same machine the certificates need to exported into a DER file and imported by the partner application to ensure the both application find the certificate.

Exporting/importing the certificates and using the default product configuration is usually safer and simpler than changing the configuration.

Certificate Access Permissions
Certificates in the Windows store and files in directories have access rights security settings. The default may not allow non-administrator users access. The user account running the UA application must have certificate read access rights. The Advosol configuration utilities have a Permissions setting feature.

Trouble Shooting Steps

1. Make sure that error logging is enable in the UA application configuration (TraceConfiguration element) and check the log file.

2. Make sure that the OPC Core Components are installed. On 64bit machines the 64bit OPC Core Components need to be installed because client applications my run in 64bit mode.

3. Test the access to the configured COM server with the provided OpcSecurityAnalyzer utility.
   More detailed server access can be made with the provided OPC DA or OPC HDA or OPC AE test clients.

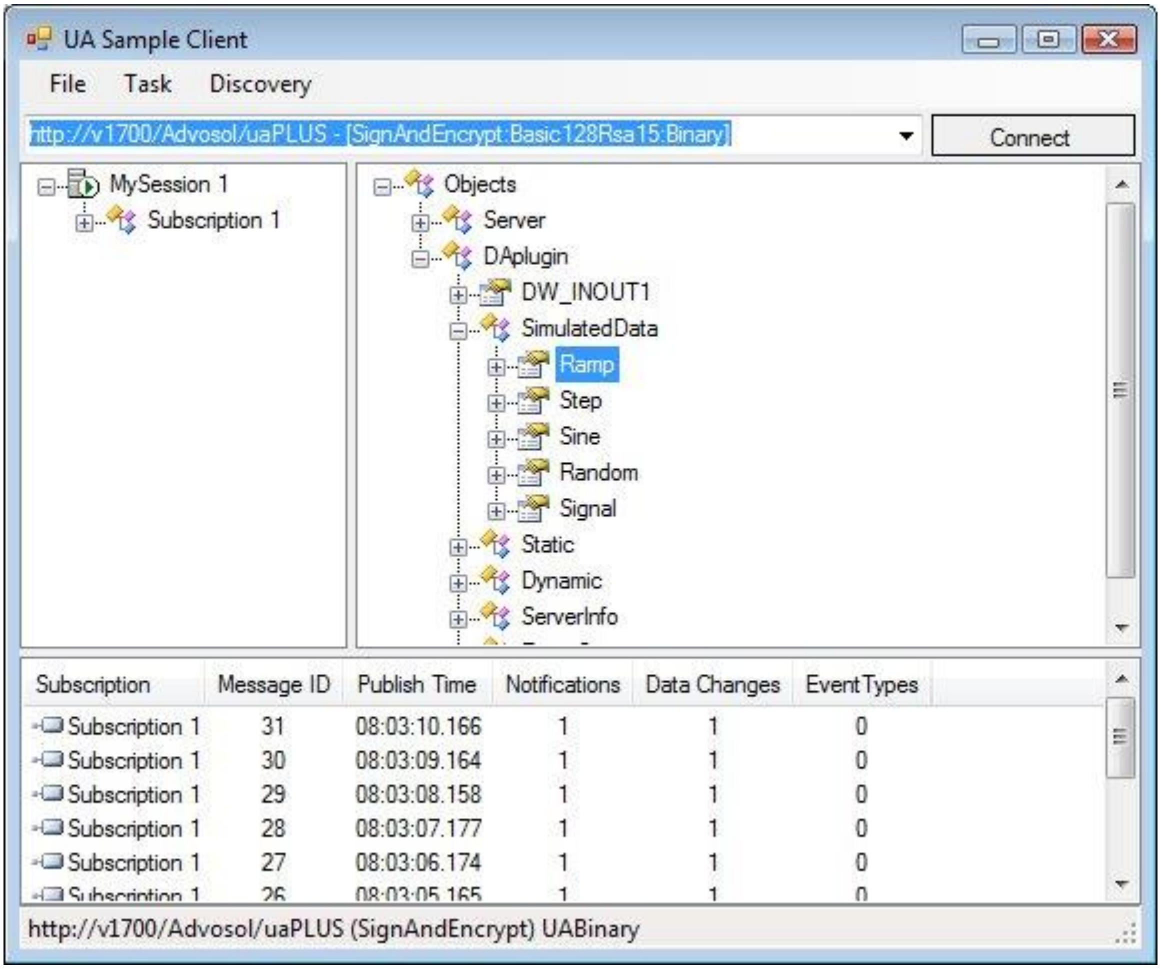
4. Test the access to the UAtoCOM UA server with the provided UA Explorer client or the DA-UA Test Client.
   Remember to configure the UA client (with the UaClientConfigHelper utility) with a certificate and export/import the server and client certificates if the client is not on the same machine as UAtoCOM.

5. The provided Advosol UA/AE Simulation server or the HDA demo server can be used as a test environment.
   Run the RegServer utility in the Tools\ComServers directories to register the server.

Tools

A set of test tools are included in the UAtoCOM distribution.

UA Explorer Client
Use this UA client application to discover UA servers, test the access and explore the UA server.
Certificate may be to be exported/imported between the UA servers and the client before access is possible.



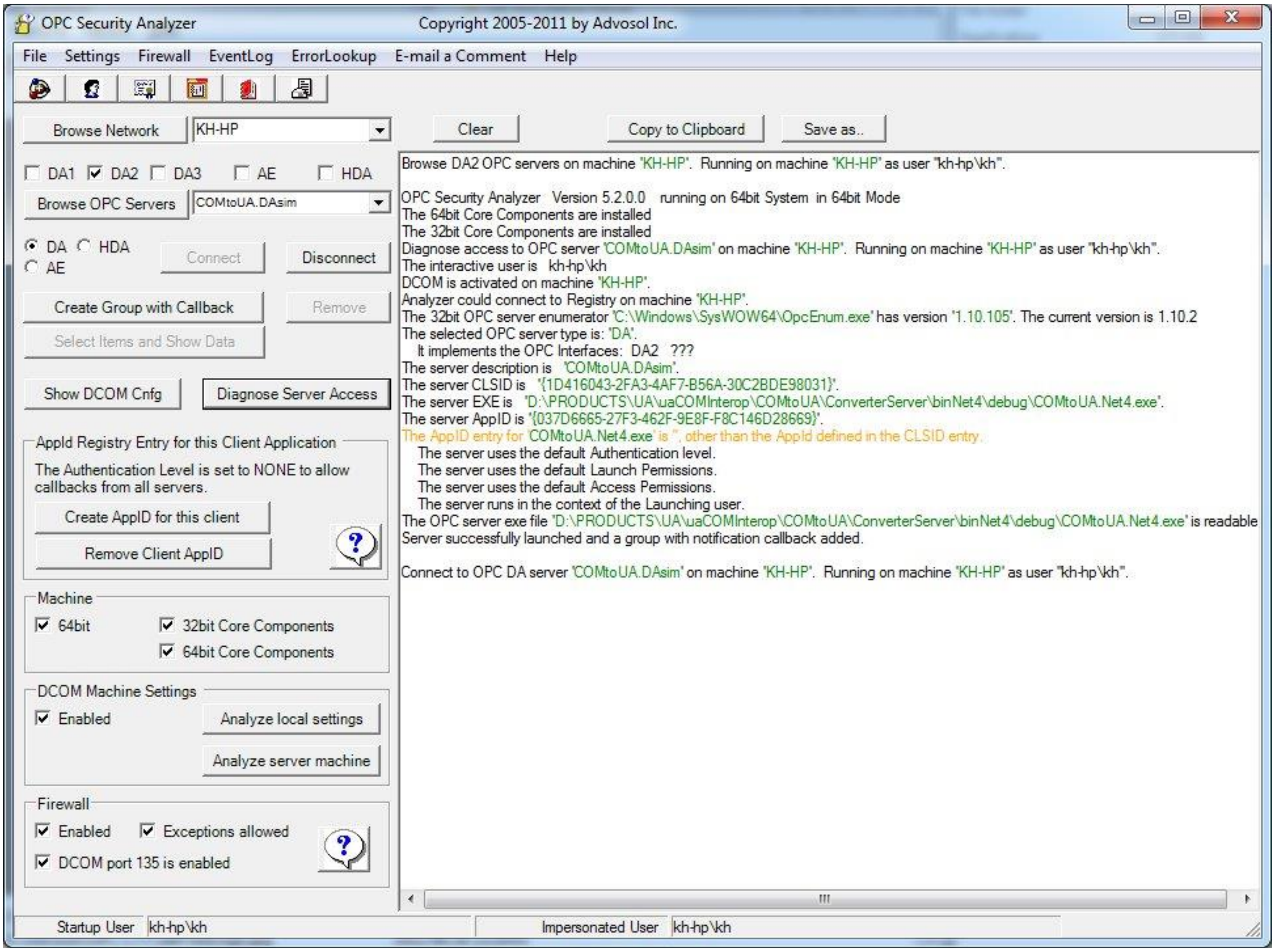
http://v1700/Advosol/uaPLUS - [SignAndEncrypt:Basic128Rsa15:Binary]

Subscription	Message ID	Publish Time	Notifications	Data Changes	EventTypes
Subscription 1	31	08:03:10.166	1	1	0
Subscription 1	30	08:03:09.164	1	1	0
Subscription 1	29	08:03:08.158	1	1	0
Subscription 1	28	08:03:07.177	1	1	0
Subscription 1	27	08:03:06.174	1	1	0
Subscription 1	26	08:03:05.165	1	1	0

http://v1700/Advosol/uaPLUS (SignAndEncrypt) UABinary

OPCSecurityAnalyzer

Use this application to check the DCOM configuration and the access to the Classic OPC servers to be accessed thru UAtoCOM.



KH-HP

□ DA1 ☑ DA2 □ DA3 □ AE □ HDA

COMtoUA.DAsim

● DA ○ HDA ○ AE

AppId Registry Entry for this Client Application

The Authentication Level is set to NONE to allow callbacks from all servers.

Machine

☑ 64bit ☑ 32bit Core Components ☑ 64bit Core Components

DCOM Machine Settings

☑ Enabled

Firewall

☑ Enabled ☑ Exceptions allowed ☑ DCOM port 135 is enabled

```
Browse DA2 OPC servers on machine 'KH-HP'.  Running on machine 'KH-HP' as user "kh-hp\kh".

OPC Security Analyzer   Version 5.2.0.0   running on 64bit System  in 64bit Mode
The 64bit Core Components are installed
The 32bit Core Components are installed
Diagnose access to OPC server 'COMtoUA.DAsim' on machine 'KH-HP'.  Running on machine 'KH-HP' as user "kh-hp\kh".
The interactive user is   kh-hp\kh
DCOM is activated on machine 'KH-HP'.
Analyzer could connect to Registry on machine 'KH-HP'.
The 32bit OPC server enumerator 'C:\Windows\SysWOW64\OpcEnum.exe' has version '1.10.105'. The current version is 1.10.2
The selected OPC server type is: 'DA'.
   It implements the OPC Interfaces:  DA2   ???
The server description is   'COMtoUA.DAsim'.
The server CLSID is   '{1D416043-2FA3-4AF7-B56A-30C2BDE98031}'.
The server EXE is   'D:\PRODUCTS\UA\uaCOMInterop\COMtoUA\ConverterServer\binNet4\debug\COMtoUA.Net4.exe'.
The server AppID is '{037D6665-27F3-462F-9E8F-F8C146D28669}'.
The AppID entry for 'COMtoUA.Net4.exe' is '', other than the AppId defined in the CLSID entry.
   The server uses the default Authentication level.
   The server uses the default Launch Permissions.
   The server uses the default Access Permissions.
   The server runs in the context of the Launching user.
The OPC server exe file 'D:\PRODUCTS\UA\uaCOMInterop\COMtoUA\ConverterServer\binNet4\debug\COMtoUA.Net4.exe' is readable
Server successfully launched and a group with notification callback added.

Connect to OPC DA server 'COMtoUA.DAsim' on machine 'KH-HP'.  Running on machine 'KH-HP' as user "kh-hp\kh".
```

Startup User kh-hp\kh   Impersonated User kh-hp\kh

Classic OPC Simulation Servers

The provided Classic OPC servers can be used as a test environment.

OPC DA/AE Simulation Server

The server is in the setup subdirectory   Tools\ComServers\DA-AE
Run the RegServer.exe utility in this directory to register the server with DCOM

The server is registered as
- *Advosol.SimDAServer.1*   (DA V2/V3)
- *Advosol.SimAEServer.1*   (AE)

OPC Historian Demo Server

The server is in the setup subdirectory   Tools\ComServers\HDA
Run the RegServer.exe utility in this directory to register the server with DCOM

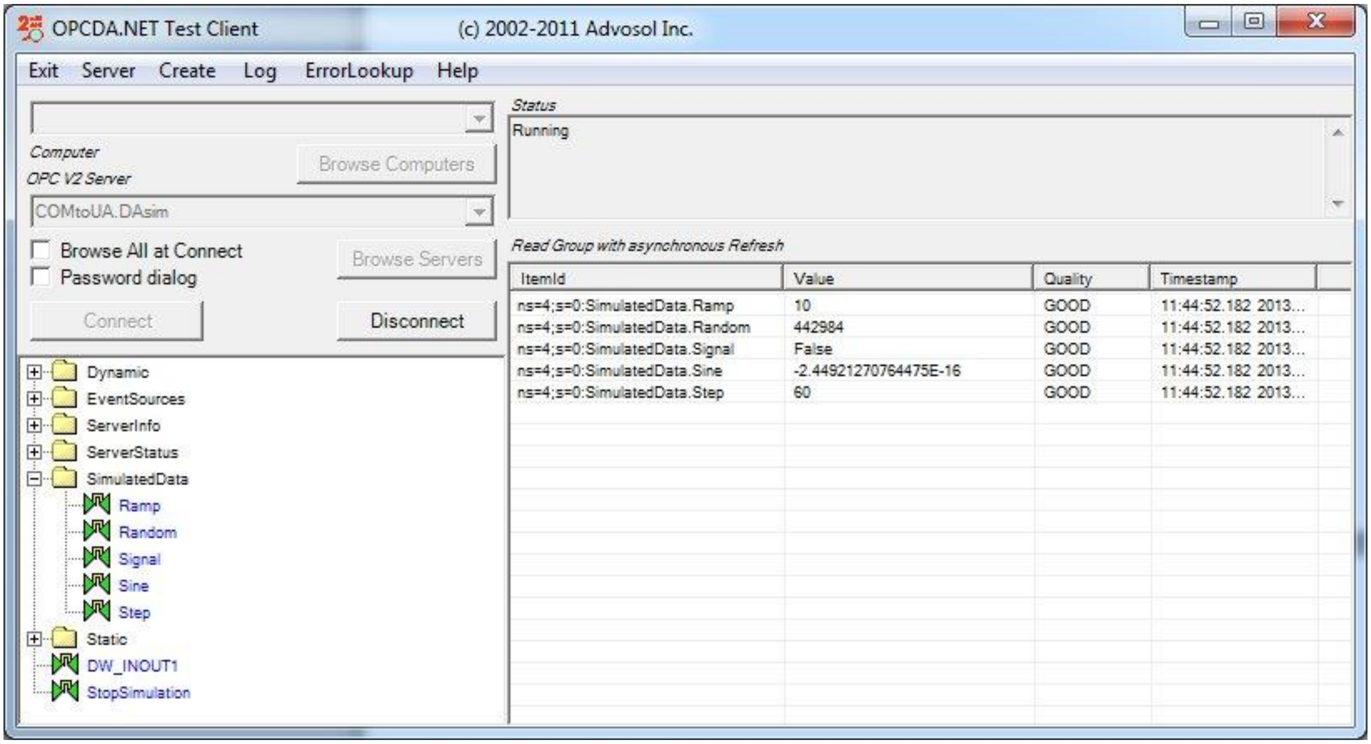
The server is registered as   *Advosol.HDA.Net4.Test.5*

OPC DA Test Client

This client is built with the Advosol OPCDA.NET-UA client component and can access Classic OPC DA servers and OPC UA servers. To find and access UA servers the application must first be configured for a certificate. The ***UAclientConfigHelper*** utility is provided for the configuration.

The client application can be used to:

- Access the DA functionality of UA servers
- Test the Classic OPC DA server access directly, without going thru the UAtoCOM converter server.



Computer

OPC V2 Server: COMtoUA.DAsim

□ Browse All at Connect

□ Password dialog

Status: Running

Read Group with asynchronous Refresh

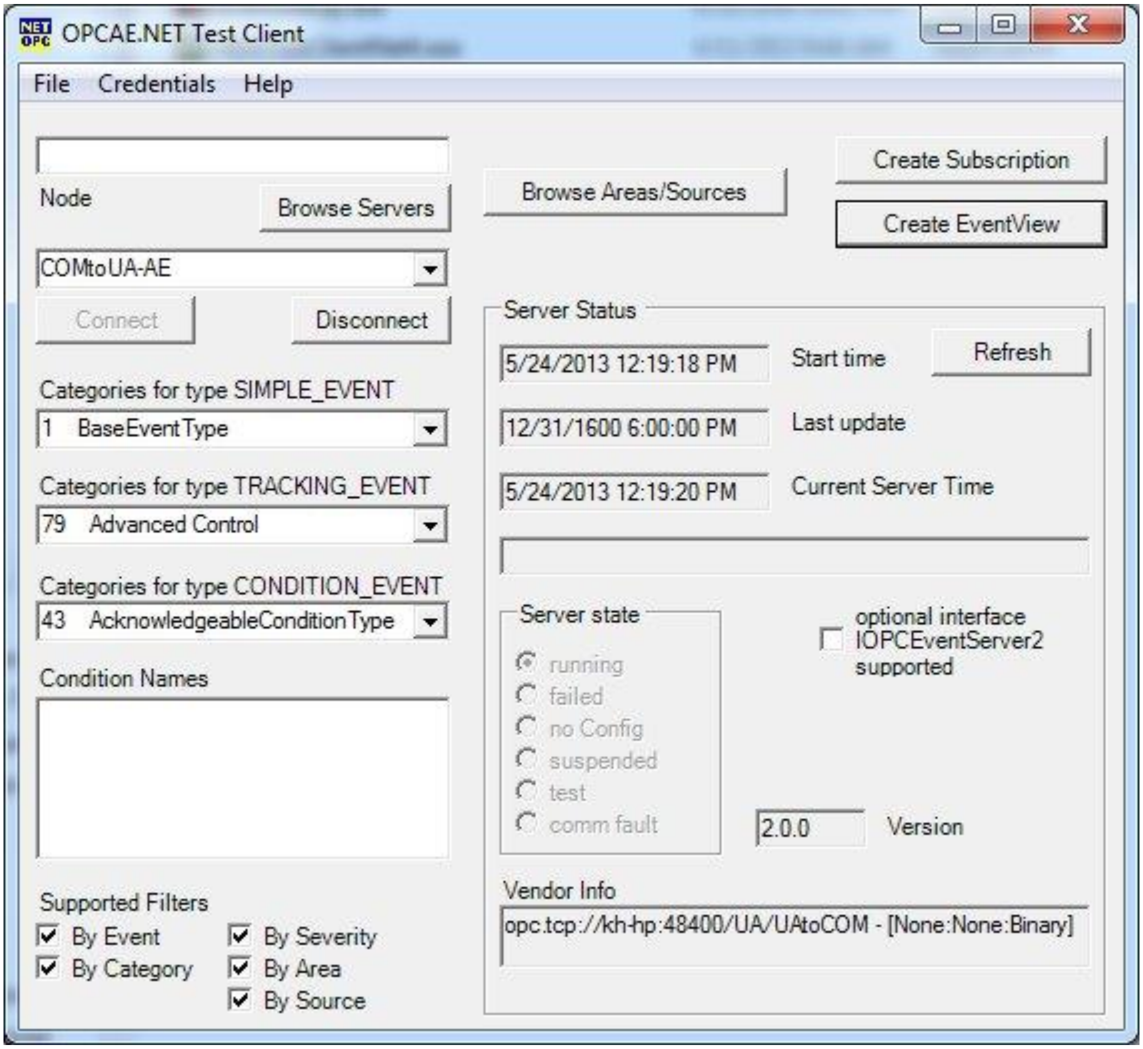
ItemId	Value	Quality	Timestamp
ns=4;s=0:SimulatedData.Ramp	10	GOOD	11:44:52.182 2013...
ns=4;s=0:SimulatedData.Random	442984	GOOD	11:44:52.182 2013...
ns=4;s=0:SimulatedData.Signal	False	GOOD	11:44:52.182 2013...
ns=4;s=0:SimulatedData.Sine	-2.44921270764475E-16	GOOD	11:44:52.182 2013...
ns=4;s=0:SimulatedData.Step	60	GOOD	11:44:52.182 2013...

OPC Alarm&Events Test Client

This client is built with the Advosol OPCAE.NET-UA client component and can access Classic OPC AE servers and OPC UA servers. To find and access UA servers the application must first be configured for a certificate.
The ***UAclientConfigHelper*** utility is provided for the configuration.

The client application can be used to:

- Access the DA functionality of UA servers
- Test the Classic OPC A&E server access directly, without going thru the UAtoCOM converter server.



Node:

COMtoUA-AE

Categories for type SIMPLE_EVENT: 1 BaseEventType

Categories for type TRACKING_EVENT: 79 Advanced Control

Categories for type CONDITION_EVENT: 43 AcknowledgeableConditionType

Condition Names:

Supported Filters

☑ By Event ☑ By Severity
☑ By Category ☑ By Area
☑ By Source

Server Status

5/24/2013 12:19:18 PM Start time

12/31/1600 6:00:00 PM Last update

5/24/2013 12:19:20 PM Current Server Time

Server state

● running
○ failed
○ no Config
○ suspended
○ test
○ comm fault

□ optional interface IOPCEventServer2 supported

2.0.0 Version

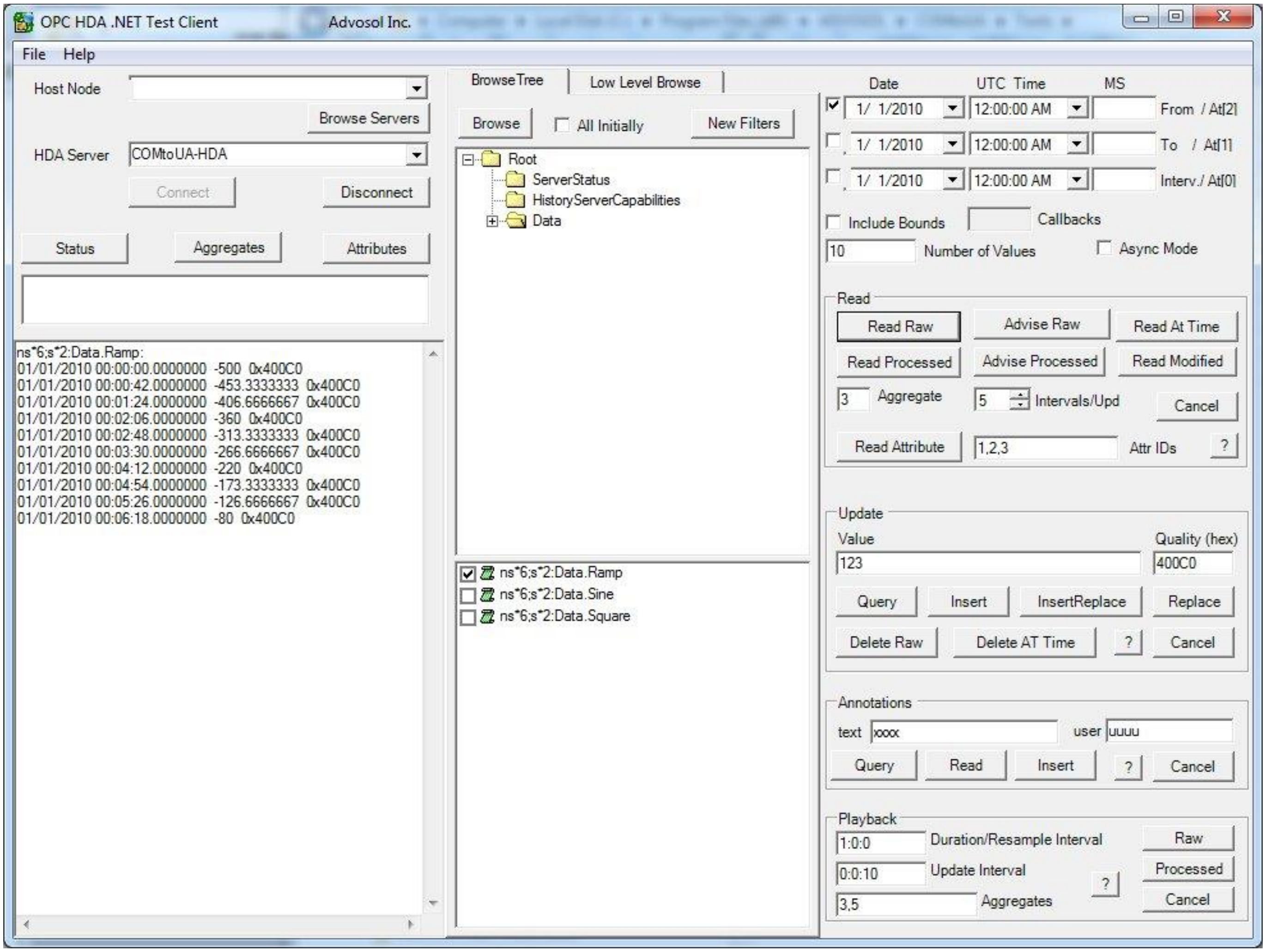
Vendor Info: opc.tcp://kh-hp:48400/UA/UAtoCOM - [None:None:Binary]

OPC Historian Test Client

This client is built with the Advosol OPCHDA.NET-UA client component and can access Classic OPC AE servers and OPC UA servers. To find and access UA servers the application must first be configured for a certificate. The ***UAclientConfigHelper*** utility is provided for the configuration.

The client application can be used to:

- Access the Historian functionality of UA servers
- Test the Classic OPC HDA server access directly, without going thru the UAtoCOM converter server.



HDA Server: COMtoUA-HDA

```
ns*6;s*2:Data.Ramp:
01/01/2010 00:00:00.0000000  -500  0x400C0
01/01/2010 00:00:42.0000000  -453.3333333  0x400C0
01/01/2010 00:01:24.0000000  -406.6666667  0x400C0
01/01/2010 00:02:06.0000000  -360  0x400C0
01/01/2010 00:02:48.0000000  -313.3333333  0x400C0
01/01/2010 00:03:30.0000000  -266.6666667  0x400C0
01/01/2010 00:04:12.0000000  -220  0x400C0
01/01/2010 00:04:54.0000000  -173.3333333  0x400C0
01/01/2010 00:05:26.0000000  -126.6666667  0x400C0
01/01/2010 00:06:18.0000000  -80  0x400C0
```

☑ ns*6;s*2:Data.Ramp
☐ ns*6;s*2:Data.Sine
☐ ns*6;s*2:Data.Square

☑ 1/ 1/2010 12:00:00 AM From / At[2]
☐ 1/ 1/2010 12:00:00 AM To / At[1]
☐ 1/ 1/2010 12:00:00 AM Interv./ At[0]

☐ Include Bounds
10 Number of Values
☐ Async Mode

3 Aggregate
5 Intervals/Upd
1,2,3 Attr IDs

Value: 123
Quality (hex): 400C0

text xxxx
user uuuu

1:0:0 Duration/Resample Interval
0:0:10 Update Interval
3,5 Aggregates