

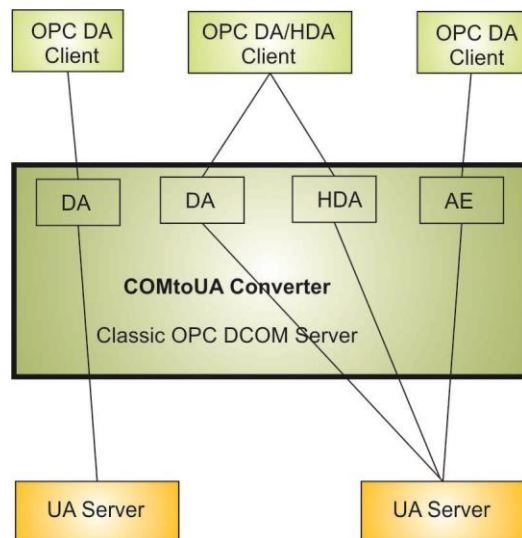
COMtoUA Converter Server User Manual

Copyright © 2013-2014 Advosol Inc.

Content	UA Server Access and Security Basics
	Setup
	Configuration
	COM Servers
	Certificate Management
	Trouble Shooting
	Tools
	License

Overview

COMtoUA is a Classic OPC DCOM server with the capability to act as multiple OPC DA, HDA and/or AE servers. Each server is configured to a UA server endpoint and enables Classic OPC clients to access OPC UA servers.



The **COMtoUA** converter makes OPC UA servers accessible from classic OPC client applications.

COMtoUA can be configured to serve as multiple OPC DA, HDA and/or AE servers.

Each of these pseudo servers are assigned to an endpoint of an OPC UA server.

Multiple pseudo servers can access the same UA server or endpoint, e.g. if the UA server supports the functionality of multiple Classic OPC specifications.

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.

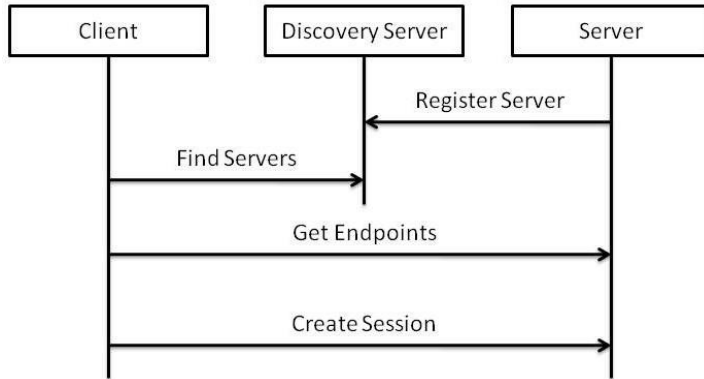
Or, the text content of the license file can be copied into the COMtoUA.NET4.exe.config application configuration file:

```
<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](#).

COMtoUA Setup

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

Steps after the COMtoUA converter server software is installed:

1. Run the **COMtoUAconfig** utility to:
 - Create the security certificate for the COMtoUA converter server UA client.
Either create a self-signed certificate or import a certificate purchased from a certificate authority. Edit the certificate permission settings to include the user account running COMtoUA.
 - Create the COM pseudo servers that can be accessed by Classic OPC client applications for the data exchange with OPC UA servers. The pseudo server configuration includes the selection of the UA server endpoint and security selections.
The UA servers should be running so that the endpoint information can be retrieved from the UA server.
 - Register COMtoUA with the configured pseudo servers with DCOM
2. Configure the DCOM and Firewall security settings for the COMtoUA configured pseudo servers for the proper access rights. The application name for the DCOM configuration is **Advosol COMtoUA Converter Server**. If the DCOM OPC clients are on the same machine as DCOMtoUA then the default DCOM settings are usually OK.
It's recommended to configure a particular user account for COMtoUA instead of the default "Launching User". The selection is in the Windows DCOMCnfg utility Identity tab.
3. Test the functionality of each configured COMtoUA pseudo server with the **OpcSecurityAnalyzer** or a test client of your choice.

The COMtoUA setup includes UA test applications:

- UA Simulation server and UA Discovery server
These servers can be used to create a test environment for the COMtoUA converter. The discovery server is not mandatory but can simplify the configuration process.
- UA test clients
These clients can be used to test the UA server access without going thru the COMtoUA converter.

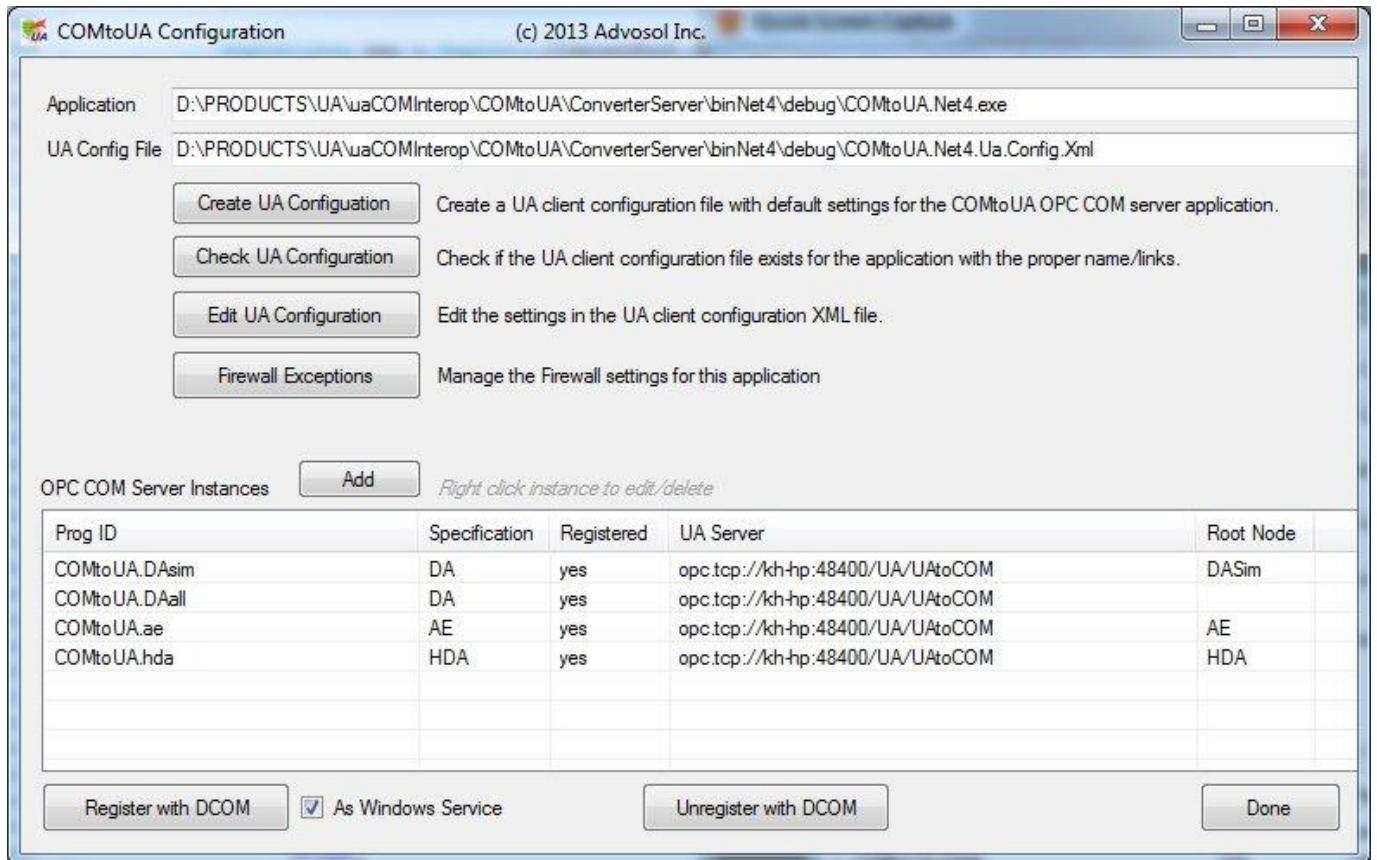
The UA test applications need to be configured with a certificate before they can be used. A suitable configuration tool is in the same directory as the UA application.

COMtoUA Configuration

The **COMtoUAconfig** utility is provided for creating and editing the COMtoUA configuration.

The configuration has two main parts:

- The pseudo servers with their DCOM registration details and the UA server endpoint selection
- The UA server communication configuration with the logging and certificates



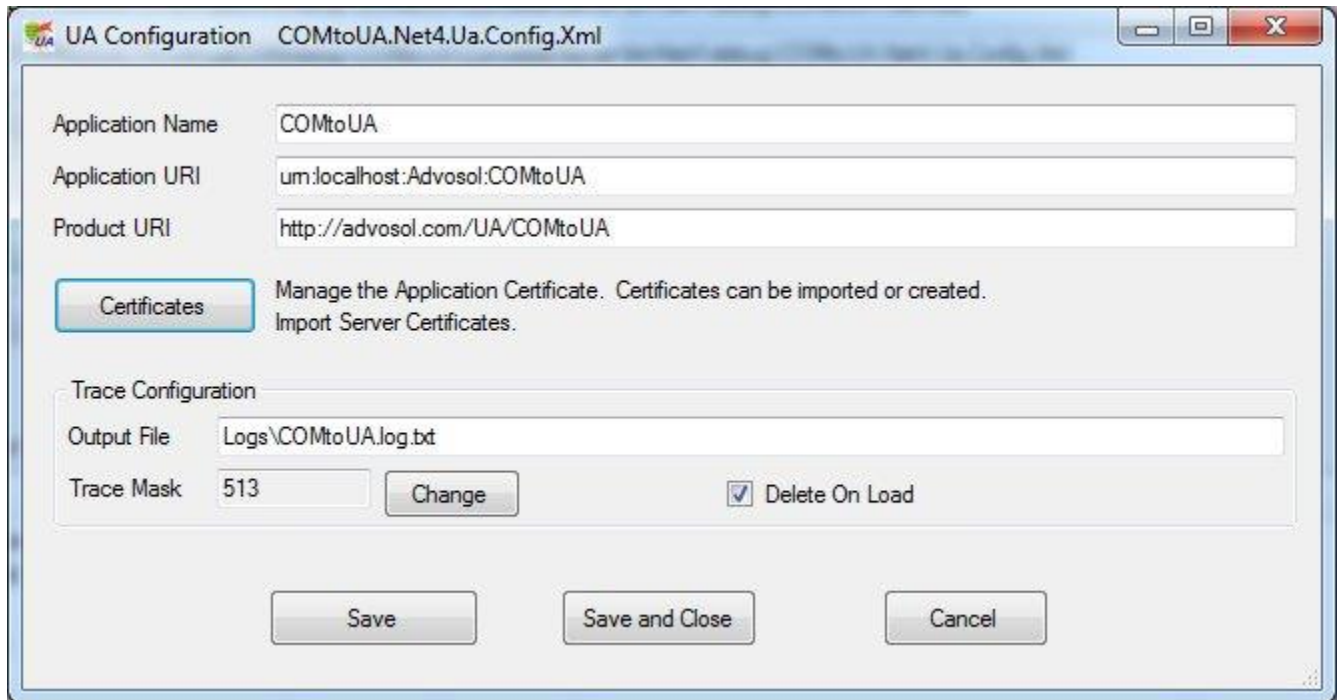
Click **Edit UA Configuration** to manage the security certificate and the logging level.

Select detailed logging levels with tracing only when necessary. The log file can quickly get big and performance is reduced.

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

COMtoUA can be registered to run as background process or as a Windows service.

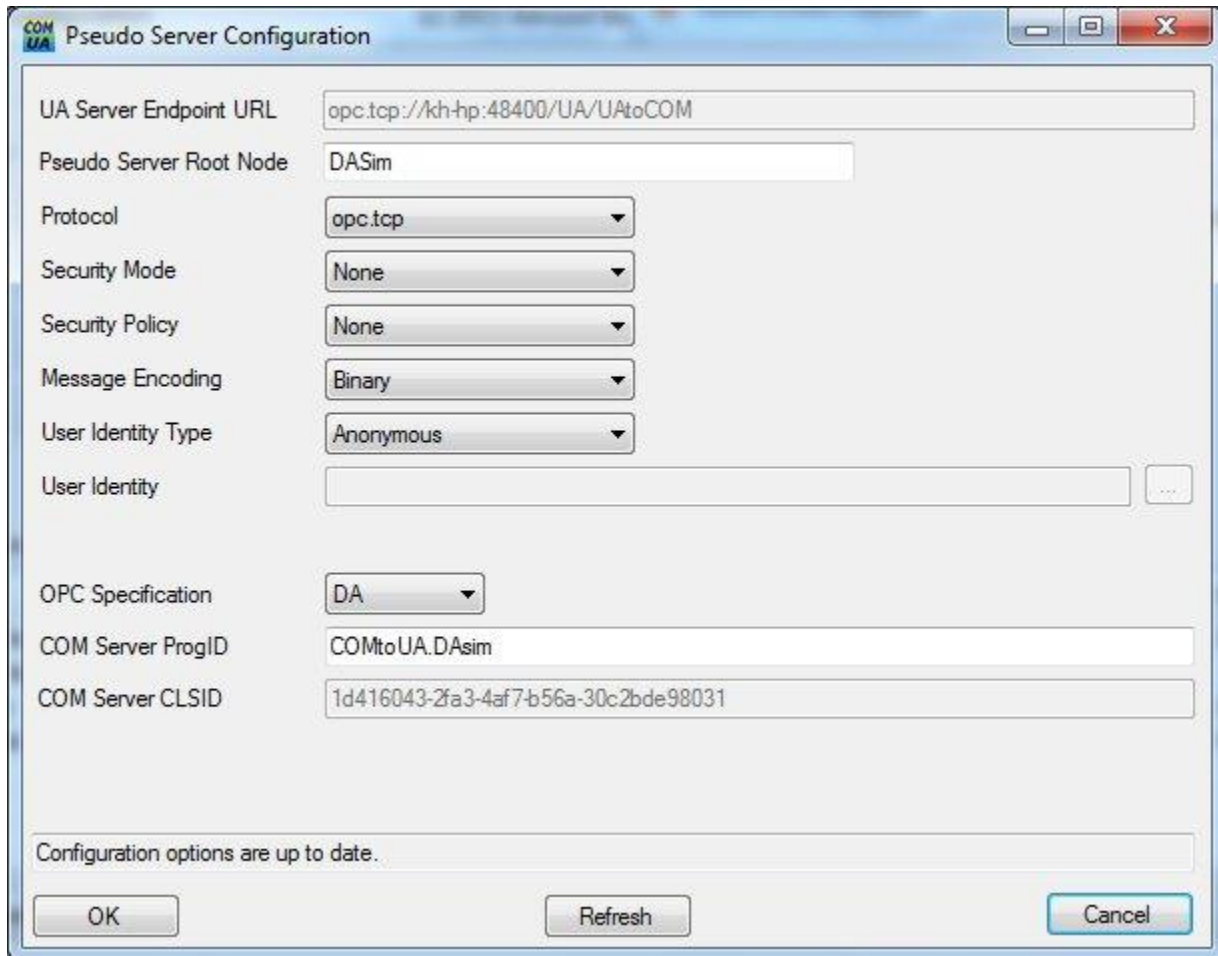
The UA configuration includes the application definitions and the certificate management. UA server endpoint selections are defined for each pseudo server.



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

Pseudo server Configuration

A pseudo server is an OPC DA, HDA or AE server that runs as part of the uaPLUS server. Each pseudo server is assigned to a UA server endpoint. The UA server must support the functionality corresponding to the type of the pseudo server. The pseudo servers can be mapped to the root of the UA server address space or to a particular node in the root by specifying the browse name of the node.



The screenshot shows a dialog box titled "Pseudo Server Configuration" with the following fields and values:

UA Server Endpoint URL	opc.tcp://kh-hp:48400/UA/UAtoCOM
Pseudo Server Root Node	DASim
Protocol	opc.tcp
Security Mode	None
Security Policy	None
Message Encoding	Binary
User Identity Type	Anonymous
User Identity	
OPC Specification	DA
COM Server ProgID	COMtoUA.DAsim
COM Server CLSID	1d416043-2fa3-4af7-b56a-30c2bde98031

Configuration options are up to date.

Buttons: OK, Refresh, Cancel

The UA server must be accessible for the configuration utility to collect the endpoint information from the UA server. The supported endpoints and communication options are read from the UA server and made available in the selection combo boxes.

The OPC Specification selection determines how the pseudo server is registered with DCOM.

The CLSID is auto created as a unique Guid.

Also the ProgID must be unique on the machine. COMtoUAconfig creates ProgID from the URL and other selections, making the created ProgID most likely unique. The user can accept this rather cryptic ProgID or change it to a preferred unique name.

Certificates and their Management

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

The configuration tools provided with COMtoUA 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 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.
- **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.
- **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.
- **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 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.

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 be exported into a DER file and imported by the partner application to ensure the both application find the certificate.

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 be 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. Test the access to the configured UA server with the provided UA Explorer Client.
3. Make sure that the OPC Core Components are installed. On 64bit machines the 64bit OPC Core Components need to be installed because client application may run in 64bit mode.
4. Test the access to the configured COMtoUA COM servers with the provided OpcSecurityAnalyzer utility. Browsing for DA2,HDA,AE server should list the COMtoUA configured server ProgIDs.
5. More detailed server access can be made with the provided OPC DA or OPC HDA or OPC AE test clients.
6. Run the provided Advosol UA Simulation server and change the COMtoUA configuration to a DA server for the uaPLUSsim UA server.

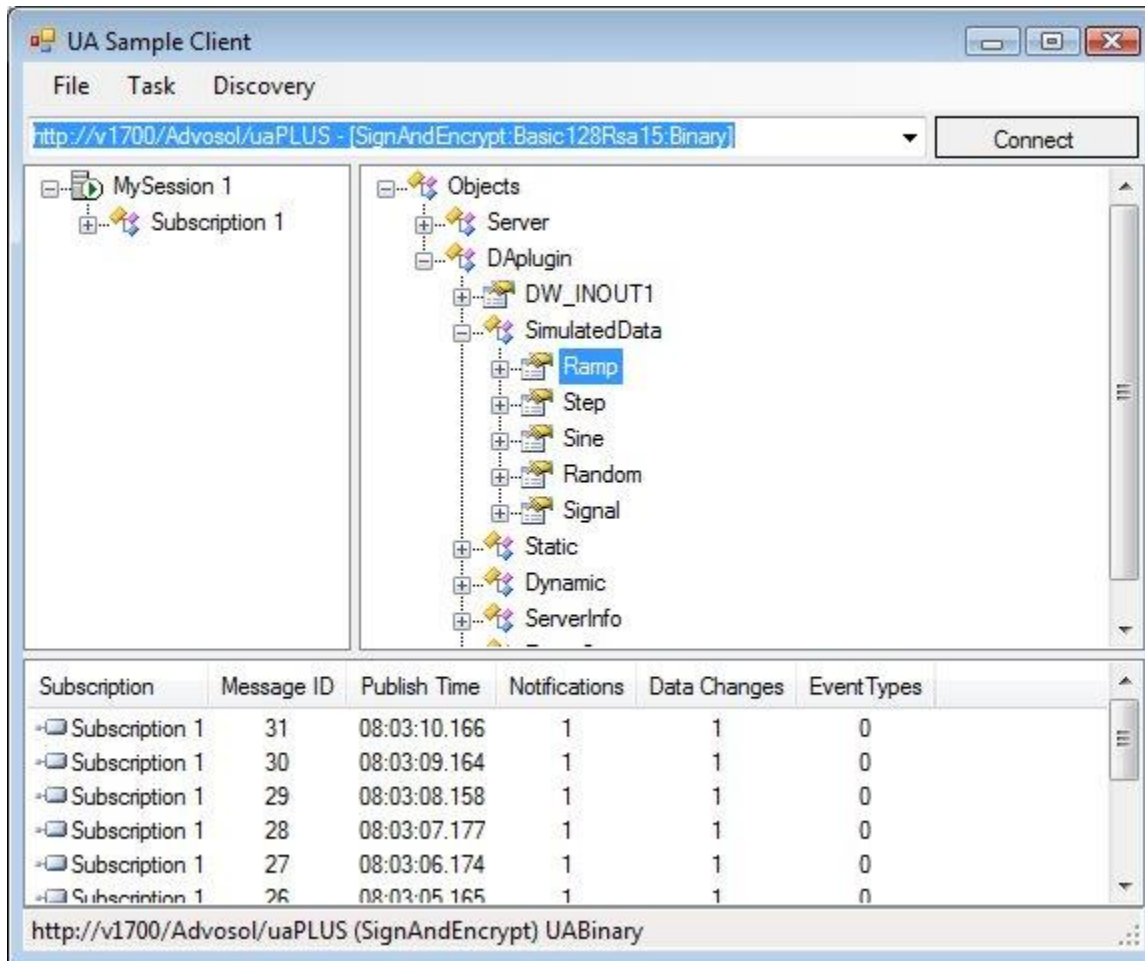
Tools

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

UA Explorer Client

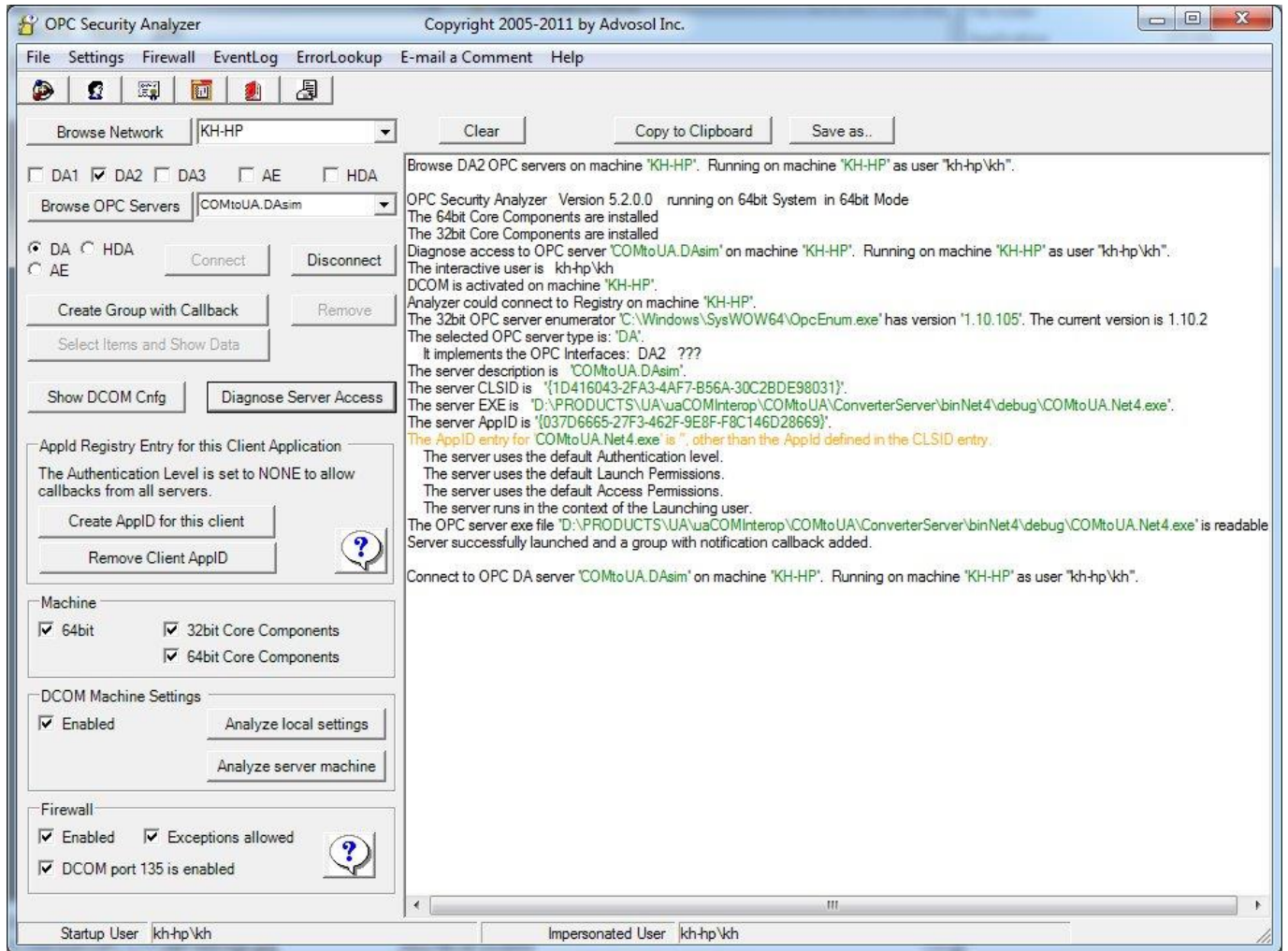
Use this UA client application to discover UA servers, test the access and explore the UA server.

Certificate may be to be exported/imported between the UA servers and the client before access is possible.



OPCSecurityAnalyzer

Use this application to check the DCOM configuration and the access to the COMtoUA configured COM servers.



UA Simulation Server

The UA simulation server can be used as a test environment.

The server can be run with a status window showing the current client activity.

The server must be configured for a certificate and the needed or preferred communication protocol options.

The **UAserverConfigHelper** utility is provided for the configuration.

Advosol uaPLUS Simulation Server

Endpoint URLs: `opc.tcp://kh-hp:62849/Advosol/uaSim` Show Info

Sessions

SessionId	Name	User	Last Contact
COM Client (kh-hp)	Anonymous	ns=3;i=501290240	12:28:11

Subscriptions

SubscriptionId	Publishing Interval	Item Count	Seq No
1	500	0	2
2	250	1	28

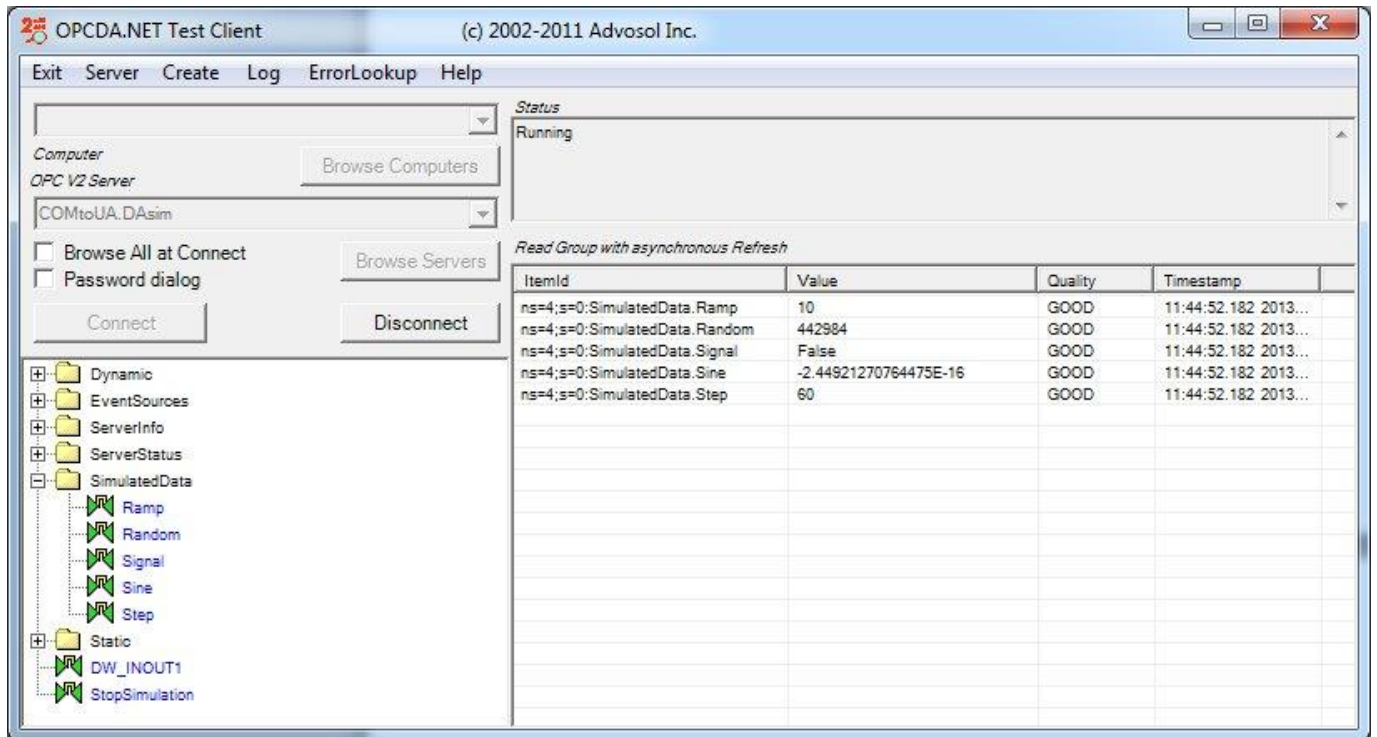
Status: Running 12:28:12

OPC DA Test Client

This Classic OPC DA V2 client application can be used to test the UA server access thru the COMtoUA converter. The server ProgID is one of the COMtoUA configured DA servers.

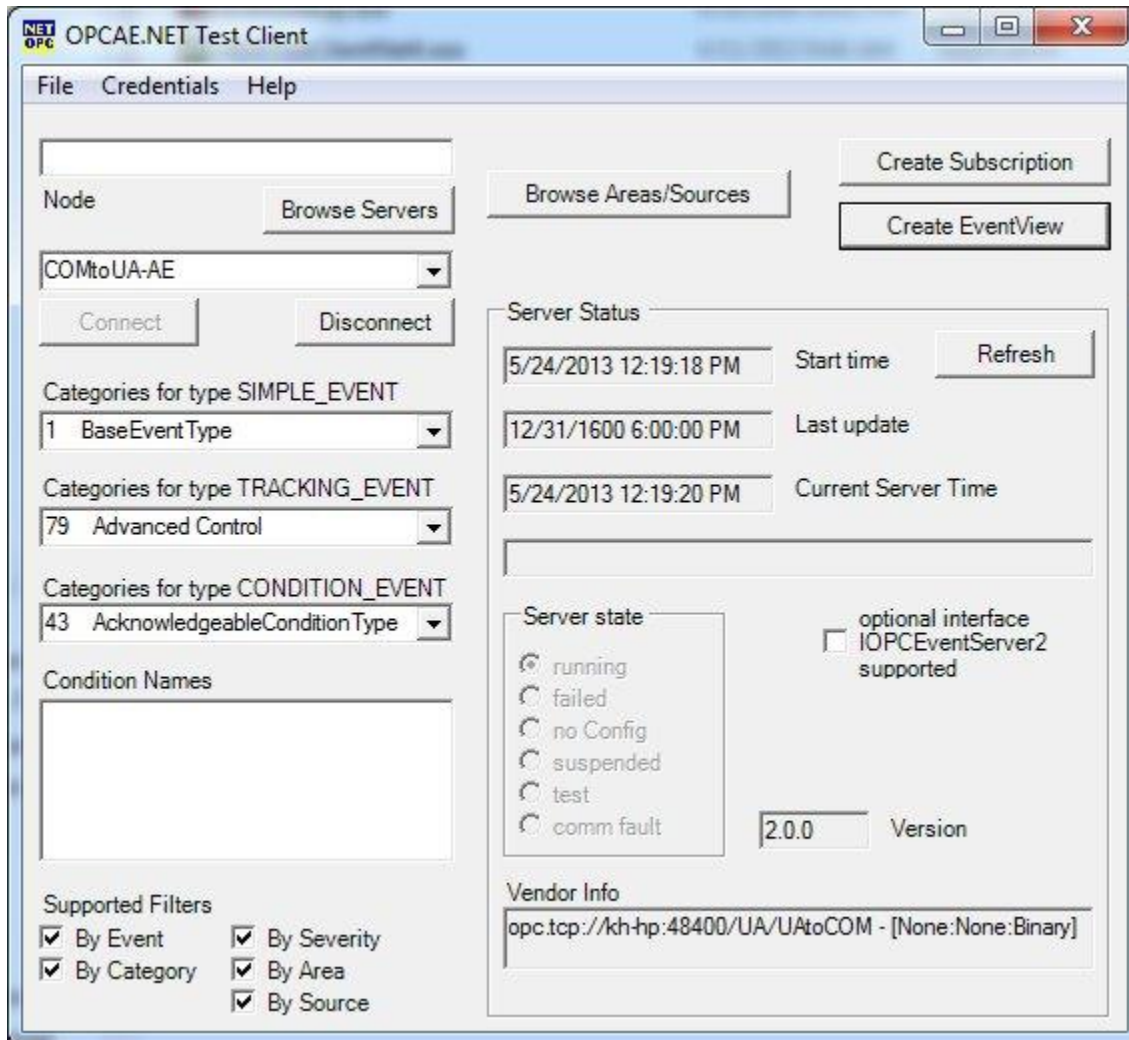
This client is built with the Advosol [OPCDA.NET-UA](#) client component and can access Classic OPC DA server and OPC UA servers. To find and access UA servers the application must first be configured for a certificate.

The **UAclientConfigHelper** utility is provided for the configuration.



OPC Alarm&Events Test Client

This Classic OPC AE client application can be used to test the UA server access thru the COMtoUA converter. The server ProgID is one of the COMtoUA configured AE servers.



OPC Historian Test Client

This Classic OPC HDA client application can be used to test the UA server access thru the COMtoUA converter. The server ProgID is one of the COMtoUA configured HDA servers.

