OPC UA Security with OPC Data Client 5.3

A Guide for using OPC UA User Authentication

Software Toolbox
International Corporate
Headquarters, USA

148A East Charles Street
Matthews, NC 28105 USA
www.softwaretoolbox.com

TOLL FREE: 888-665-3678
GLOBAL: 704-849-2773
FAX: 704-849-6388

Table of Contents

Introduction

Purpose

The purpose of this document is to provide a guideline for users of the OPC Data Client library to manage the OPC UA User Authentication process with their OPC UA server. OPC UA offers the ability to allow user authentication between the client and server to ensure that only authorized users are allow to connect to the OPC server, read and write to tags, and make OPC server configuration changes. Successful use of this feature of OPC UA requires certain steps to be performed on the OPC UA client and server. Users may also optionally wish to use OPC UA security which allows encryption of communications using SSL certificates. We have a separate paper that covers this which may be found here: A Guide for Managing UA Certificates.

Intended Audience

This document is intended for current users of the UA component of Software Toolbox's OPC Data Client family of development products. The OPC Data Client is a client development toolkit for creating custom OPC UA clients to access information from an OPC UA server. The document assumes some familiarity with the OPC Data Client and its documentation including but not limited to the Concepts Document.

Introduction to OPC UA

The OPC Unified Architecture, also known as OPC-UA, is the latest open-standard architecture developed by the OPC Foundation to improve and expand interoperability standards in the Industrial Automation industry.

Why do we need a new architecture to begin with? OPC-UA was the result of several advancements and changes in the way data was commonly being accessed and exchanged. Some changes that lead to the need for a new architecture include:

- Microsoft's COM and DCOM (the basis for previous standards) were deprecated and are now considered legacy technologies

- Web services gained importance in data exchange between machines and for communications to factory floor devices

- Earlier specifications were decoupled and did not integrate well, e.g. items in a Data Access server could not communicate directly with items in an Alarms and Events server.

OPC-UA is designed for exchanging information in an object-oriented manner, rather than as isolated data points. This increases the accessibility of your plant floor data by letting you re-use information stored in a common object. OPC-UA also incorporates a service-oriented model, which increases interoperability with other platforms and improves security.

OPC-UA is not a replacement for existing OPC-DA standards. Because of the layered design of this architecture, it includes all the functionality of existing OPC-DA servers, but expands upon their functionality with a common interoperability layer. This interoperability layer unifies information exchange and provides a common interface for controlling processes.

What are the benefits of the new architecture? OPC-UA provides a way to connect clients and servers in a secure manner, without relying on Microsoft DCOM. This is a big advantage because it means that you are no longer saddled with the headaches associated with having to configure DCOM. This is because DCOM plays no role in data transport. OPC-UA can also allow users to make secure connections through firewalls and over VPN connections because it uses a single TCP/IP port number that is typically user configurable. In addition, it expands the ability to provide factory floor information to other business systems, as a result of the object-oriented model described above.

Introduction to OPC UA User Authentication

OPC UA allows configuration of user identities that consists of a username and password on the OPC UA Server. These user identities may have different permissions depending on how they are configured in the OPC server. Each OPC server may have different options for setting up user identities, so please consult your OPC server’s documentation for instructions on how to accomplish this.

When a client attempts to connect to a server that has configured user identities, it may need to specify a username and password in order to have access to the information in that server. If the information that the client provides matches with a user identity that is configured in the server, it will be granted the permissions associated with that user. If the client provides a username and password combination that does not exist in the server, the server will likely reject the client’s connection attempt depending on whether the OPC UA server has been configured to reject anonymous connections.

Aside from a simple string username and password, OPC UA allows for more complicated user identity mechanisms such as Kerberos user tokens or X.509 certificates. OPC Data Client supports this

functionality as well, but this topic will not be covered in this document because of the rarity of OPC servers that use these types of user identities. If your server does expect a user identity in the form of a Kerberos token or X.509 certificate, please contact us.

Note: This is **not** the same as exchanging SSL certificates in OPC UA. The certificate exchange process is separate and would need to be done in addition to specifying a user identity. The certificate exchange process is out of the scope of this document. If you are interested in learning more about this topic, please see our application note entitled A Guide for Managing UA Certificates.

User Authentication Process with OPC Data Client

This section will discuss how to specify a username and password with the OPC Data Client library. This will allow a client developed with the library to make a connection to OPC servers that require user authentication.

Specifying a User Identity with OPC Data Client

There are two relevant properties of the **EasyUAClient** object to use when wanting to provide a user identity to an OPC server.

- The **EasyUAClient.IsolatedParameters.Session.UserIdentity.UserNameTokenInfo.UserName** property can be assigned a string value that specifies the username to specify when connecting to the OPC server.
- The **EasyUAClient.IsolatedParameters.Session.UserIdentity.UserNameTokenInfo.Password** property must be assigned a string that contains the password associated with a particular username.

These two properties must be set before attempting to connect to the OPC server in order for the user identity to be provided to the OPC server. If a username or password that is provided does not match what the server is expecting, it could reject the connection and throw a **UAException**. It is highly recommended that you anticipate this in your code, and to handle any such errors gracefully by notifying the user of the problem.

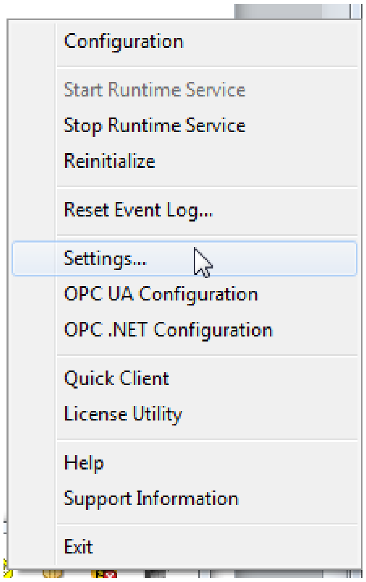
Software Toolbox support cannot directly support users of your custom application written with the OPC Data Client library if they were to contact us regarding user authentication issues. Provided you are on a support agreement, we will support you as the developer of the application. When there are support needs, the more accurate information you can provide, the better of a customer experience we can help you provide for your users. Proper exception handling is just one example of this.

Example of Using User Identities with TOP Server

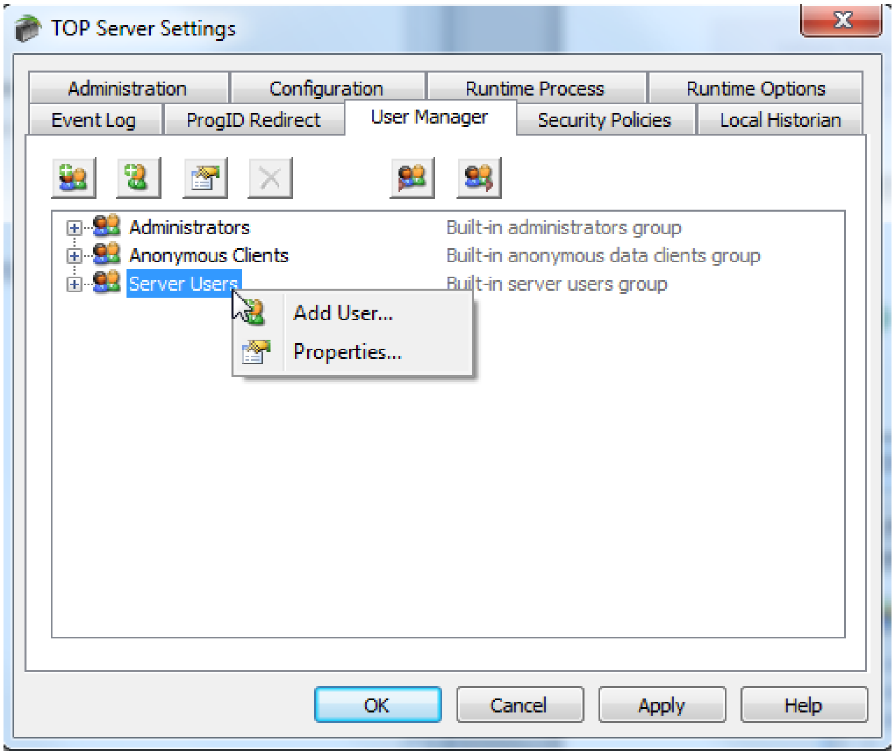
This section will walk through a simple example of setting up a user identity in TOP Server, and then using the OPC Data Client library to connect to the Top Server with that user's credentials.

Setting Up TOP Server User Identities

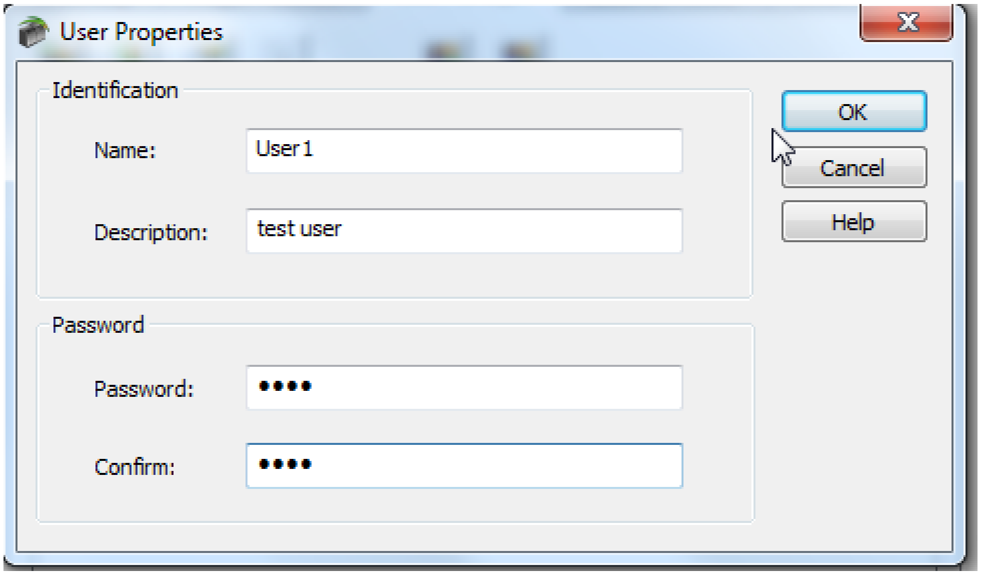
Open the TOP Server Settings by right clicking on the TOP Server Administration icon in the system tray as shown below.



When the TOP Server Settings menu opens, go to the User Manager tab, right click on the Server Users icon and choose Add User.



Enter a username and password into the appropriate fields. For the purposes of this, we will use" User1" as the username and "pass" as the password.



Name: User 1

Description: test user

Password: ••••

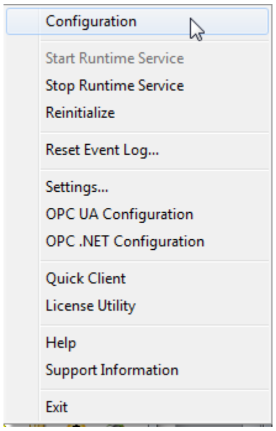
Confirm: ••••

You can continue to add more users as appropriate. Some OPC servers, including TOP Server, allow you to specific certain rights to each user. Configuration of those rights is outside the scope of this paper.

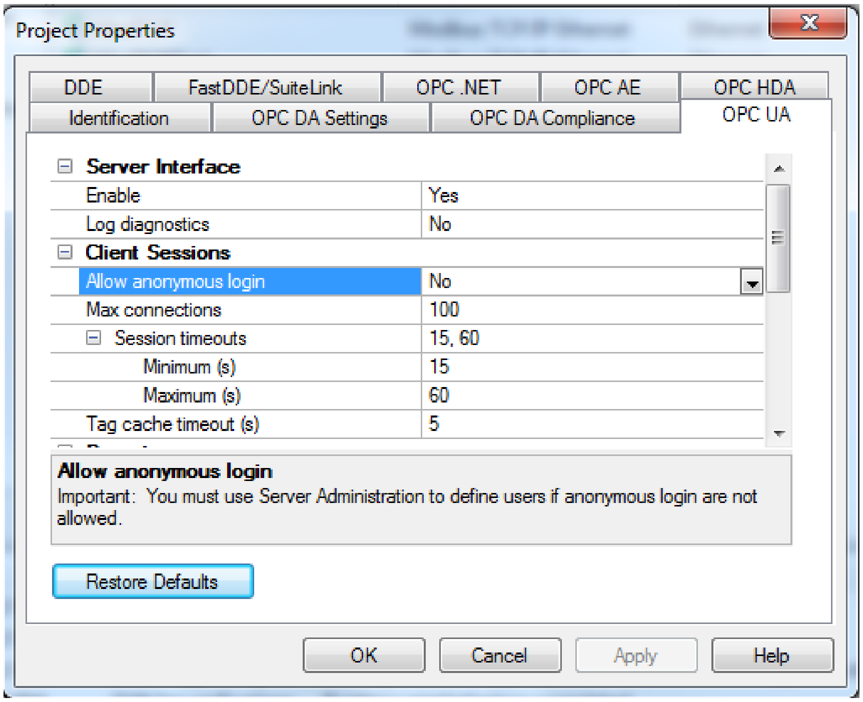
Consult your TOP Server documentation or your OPC UA server documentation for further details or contact us if you have questions about a Software Toolbox provided OPC UA server. When done, please close the TOP Server Settings menu.

Now it is necessary to tell TOP Server to not allow anonymous connections. If this step is skipped, anonymous users (users that do not specify a user identity) will be allowed to connect. The **default** behavior of TOP Server is to allow anonymous connections, so this step is **very** important.

Please open the TOP Server Configuration by right clicking on the TOP Server icon in the system tray and choosing Configuration.



Then, open the Project Properties window by going to “File | Project Properties”. Go to the OPC UA tab and make sure the “Allow Anonymous login” is set to “No”.



Server Interface	
Enable	Yes
Log diagnostics	No
Client Sessions	
Allow anonymous login	No
Max connections	100
Session timeouts	15, 60
Minimum (s)	15
Maximum (s)	60
Tag cache timeout (s)	5

Allow anonymous login
Important: You must use Server Administration to define users if anonymous login are not allowed.

Once this setting is changed, you must restart the TOP Server runtime service right clicking on the TOP Server icon in the system tray, choosing “Stop Runtime Service”, wait for the service to stop, and then choose “Start Runtime Service”.

This is the only configuration that is required to setup user identities in TOP Server.

Specifying the User Identity in OPC Data Client

Assuming that the user identity we configured above exists in TOP Server, only two lines of code in the OPC Data Client application are required:

EasyUAClient.IsolatedParameters.Session.UserIdentity.UserNameTokenInfo.UserName = “User1”

EasyUAClient.IsolatedParameters.Session.UserIdentity.UserNameTokenInfo.Password = “pass”

These two lines of code must be placed **before** any line of code that attempts to communicate with the TOP Server (such as reading, writing, subscribing, or browsing for tags). Once this is done, the OPC Data Client will include this user identity information in its requests to connect to TOP Server.

As mentioned earlier, it is recommended to have code in place that handles the situation where a server rejects the connection request because of a wrong username or password. In the event that the server

rejects a client connection, a **UAException** will be thrown that contains information related to the reason of the failure. We **strongly** recommend that there is code in place to handle this situation gracefully by notifying the user of the OPC Data Client application of the failure and logging in some fashion, the information related to the reason for the failure. This will aid the customer or your product support team, in troubleshooting any issues that occur in the field. Also, our support team will request that information if they are requested to help your team in supporting an issue. Plan for supportability from day 1 to insure a quality customer experience.

Contact Us

If you have any questions or are seeking further assistance, please contact us at:

Online Support:	http://support.softwaretoolbox.com
Email Support:	support@softwaretoolbox.com
Phone Support:	+1 (704) 849-2773
Fax:	+1 (704) 849- 6388
Mailing Address:	Software Toolbox, Inc. 148A East Charles Street, Matthews, NC 28105, USA