

Advantech SE Technical Share Document

Date	2019 / 09 / 17	Related Product	WebAccess/SCADA 8.4.1	
Category	■ FAQ □ SOP □ Driver Tech Note			
Abstract	How to use OPCUA to achieve SuperSCADA configuration			
Keyword	SuperSCADA, WebAccess/SCADA , OPC UA server			
Related OS	Win7, Windows Server 2008 / 2012 / 2016, Win10			
Revision History				
Date	Version	Author	Reviewer	Description
2019/09/17	V1.0	Kelvin Huang	Nick Liu	

■ Problem Description & Architecture:

This FAQ instructs user how to use OPCUA to achieve SuperSCADA configuration.

Structure:

Lower :WebAccess OPC UA Server (172.16.13.26) – LAN – **Upper**:OPC UA Client (172.16.12.185)

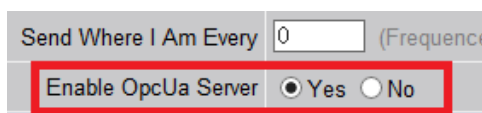
In this document, we are going to talk about how OPC UA Client modifies WebAccess OPC UA Server tag value(s). In order to control tag values, **Security Policy CAN NOT setup as "None"**. Also, **WebAccess user must have a password**. Besides, Upper WebAccess can get lower WebAccess's tag value

Software Required:

1. WebAccess OPC UA Server
2. OPC UA Client: Unified Automation UaExpert
3. OPC UA import tool

■ Brief Solution - Step by Step:

1. WebAccess allows its OPC UA Server start automatically after kernel starts. User has to enable "Enable OpcUa Server" in SCADA Node property.



In order to allow OPC UA Client to control device (modify tag value), SCADA Node runtime user must have a "password". Last, download whole WebAccess project.

e.g. admin user's password is "admin"

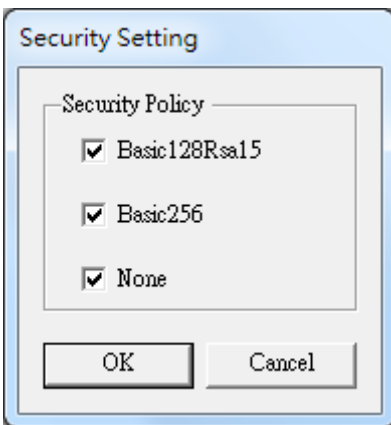


2. Creating a WebAccess project with number of tags, then download and start the kernel. Once the

kernel starts, OPC UA Server will start and display in the computer lower right corner.



3. Move mouse pointer above OPC UA Server icon, then click right button of mouse
Select "Security Setting"



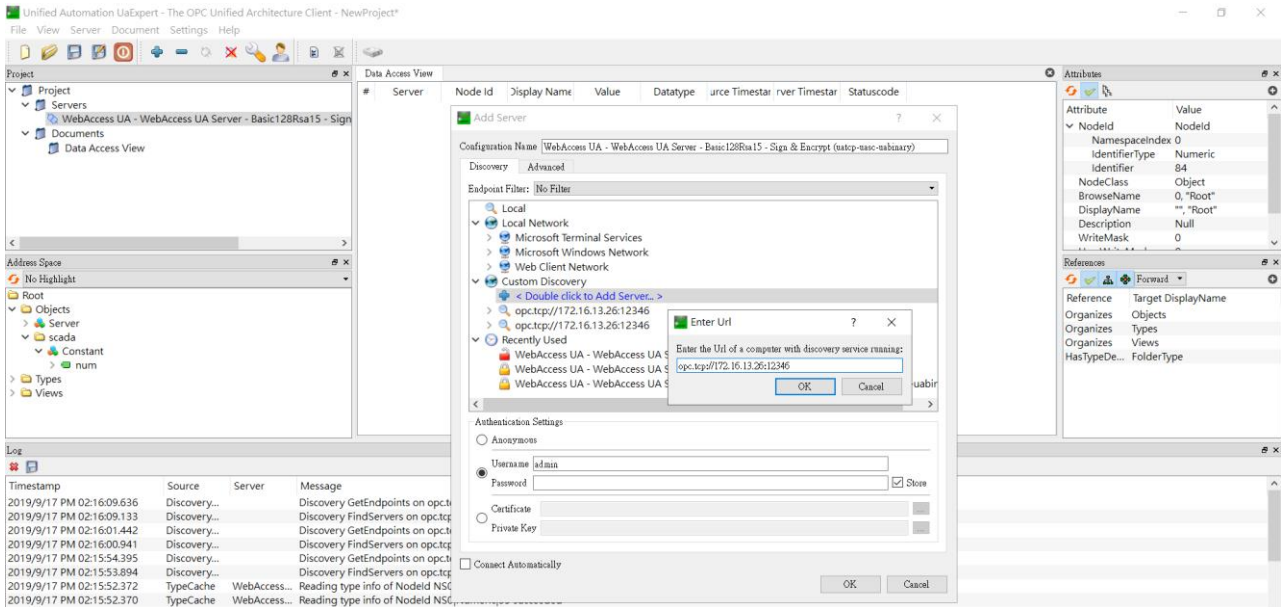
Once click "OK", OPC UA Server will automatically restart and then security configuratio will valid.

4. Run 3rd party UaExpert OPC UA Client

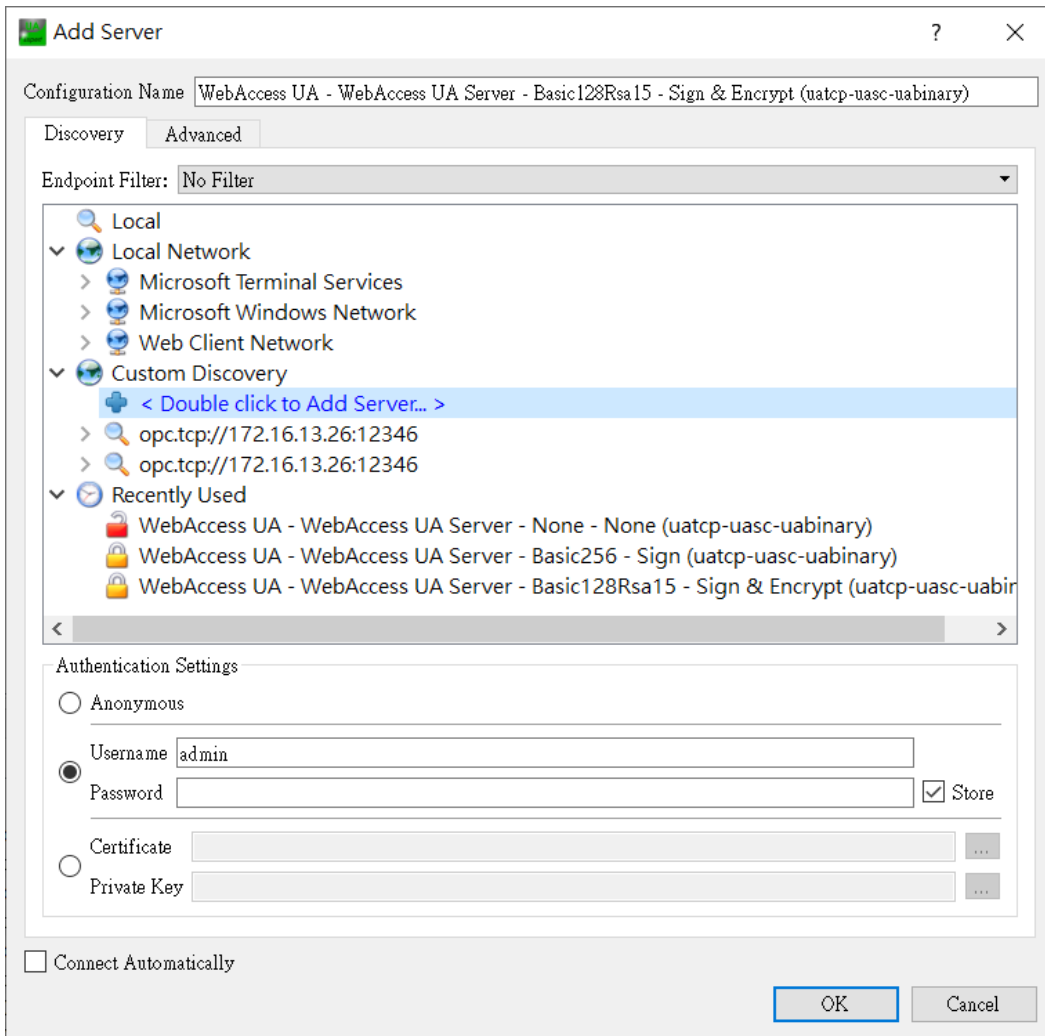


5. Click "Add Server" and WebAccess OPC UA Server will be detected automatically. User may also manually add OPC UA Server in "+ Double click to Add Server..." if necessary. Put checkmark in "Connect Automatically", then click "OK" button.

Note: by using "anonymous" in Authentication Settings, user won't be able to modify WebAccess tag value. It fails because incorrect WebAccess user name and password.



6. "opc.tcp://172.16.13.26:12346" will be added in Custom Discovery.

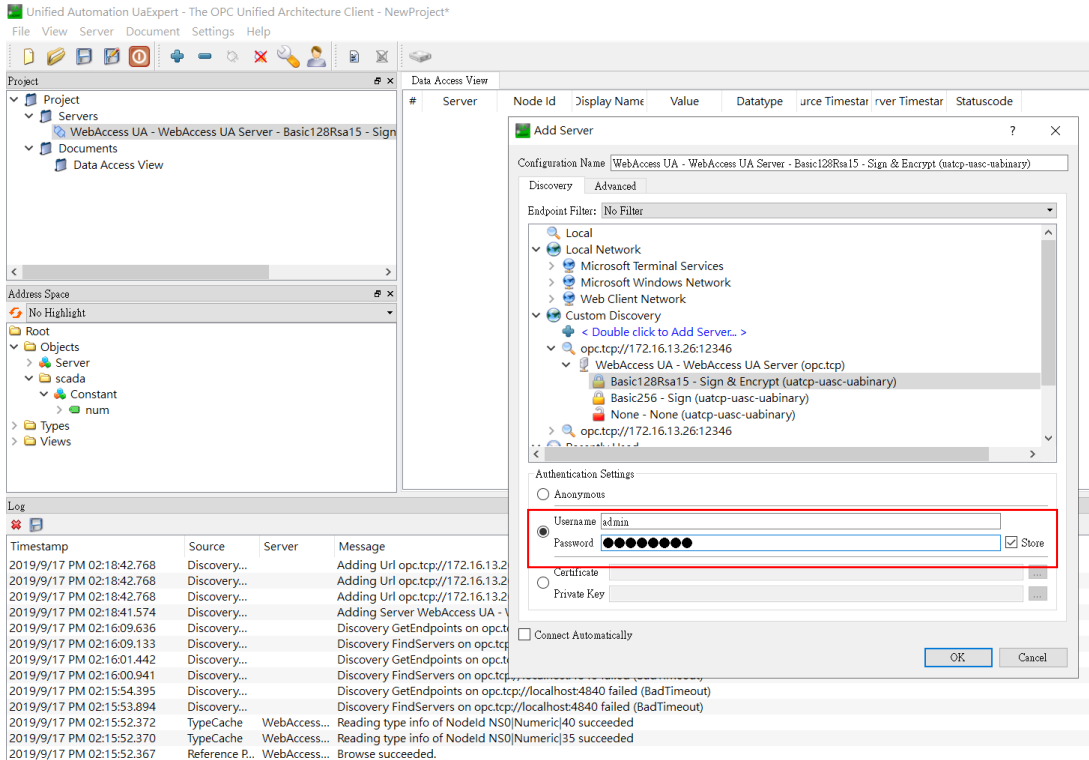


7. Click trigger icon to browse it.

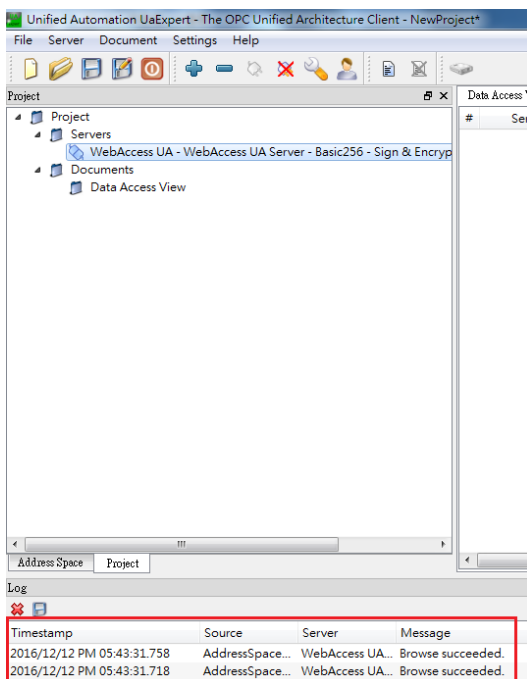
Enter User Name and Password

Note: check in “store” in order to enter Password

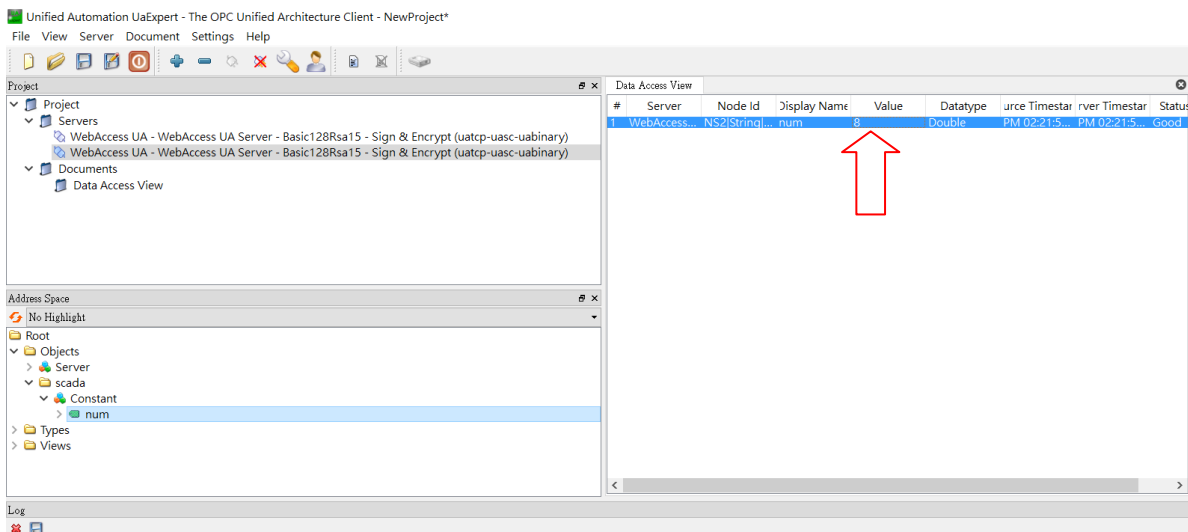
Select “Basic256 – Sign & Encrypt (uatcp-uasc-uabinary) and click “OK” button



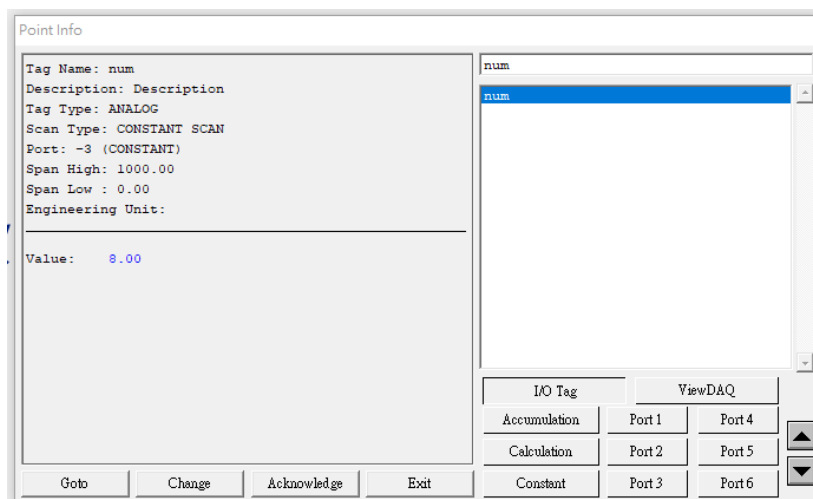
8. “Browse succeeded” in Unified Automation UaExport Log Area



9. Check “Address Space” and tag values will be able to monitor, double click to change tag value

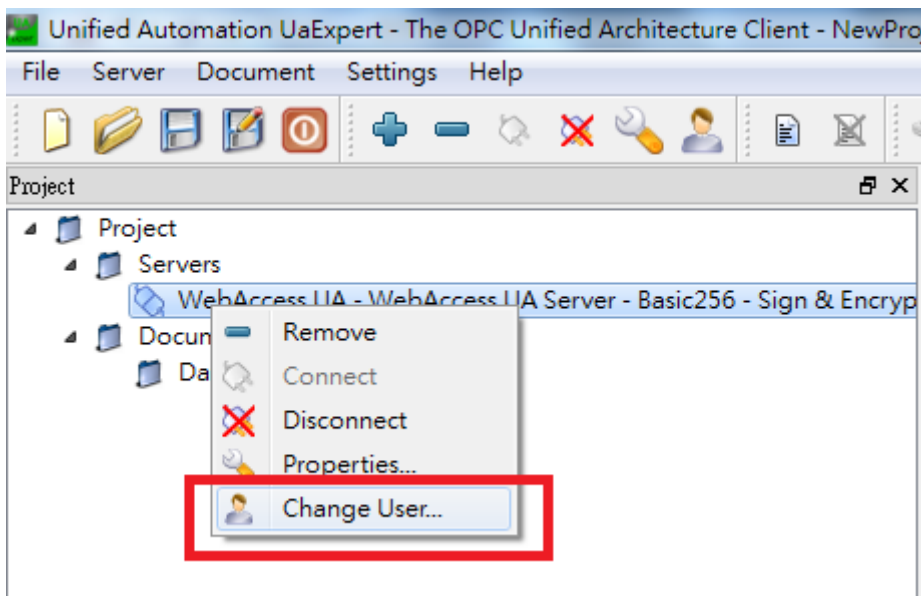


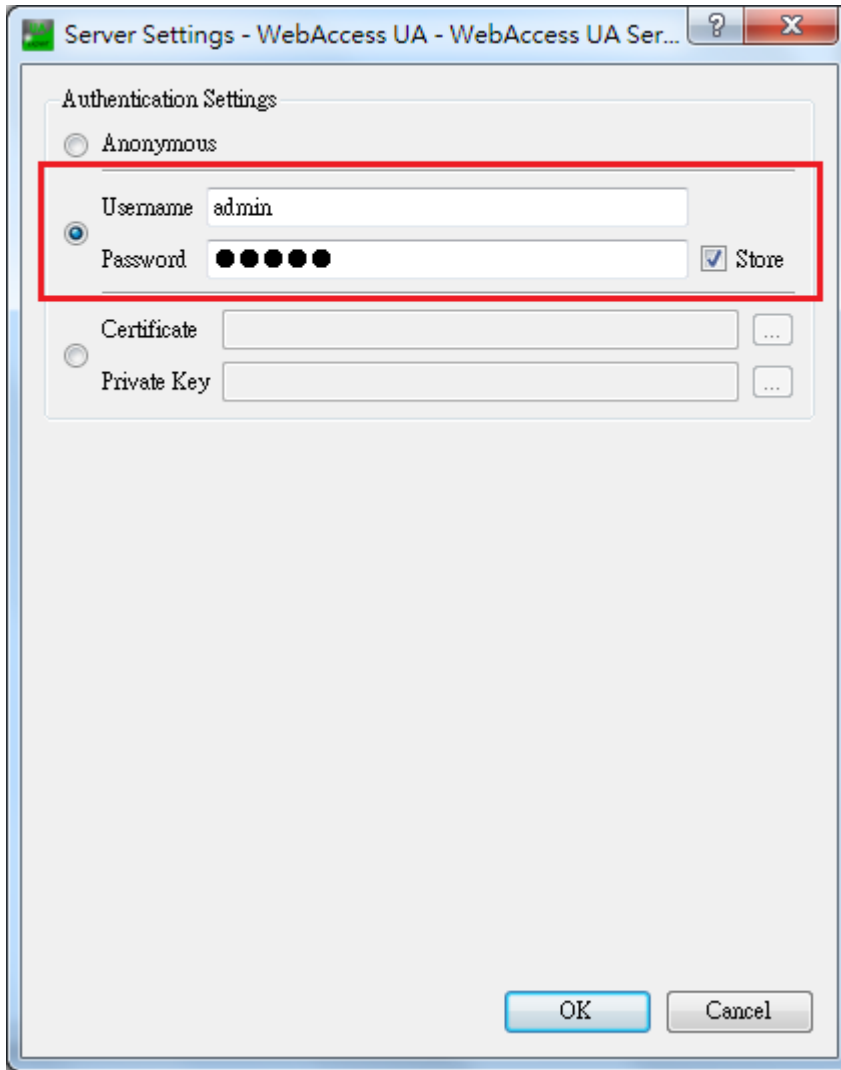
10. Then you will see lower WebAccess’s tag value was changed



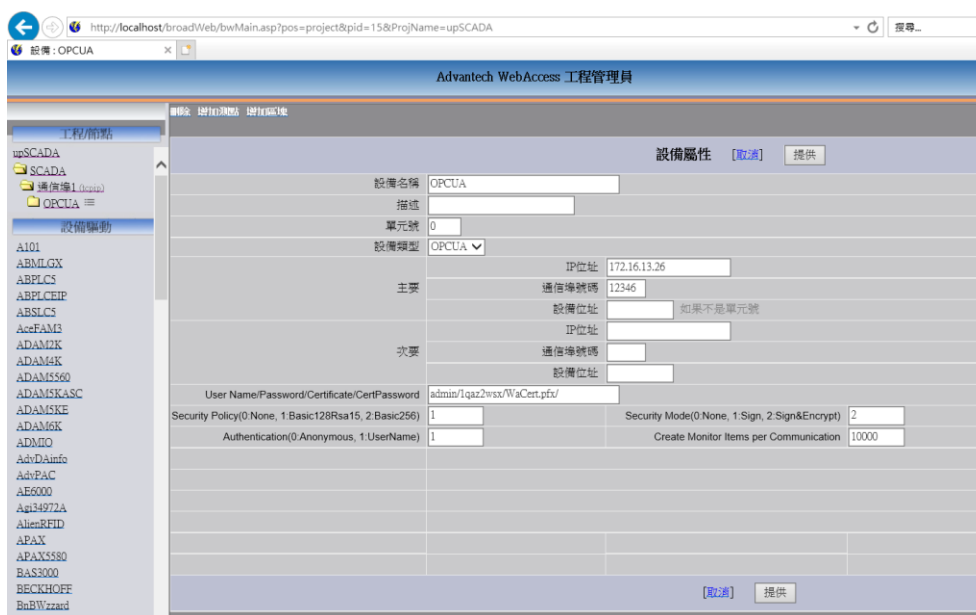
11. Note: check user & password

It can't change tag value, then check User Authorize





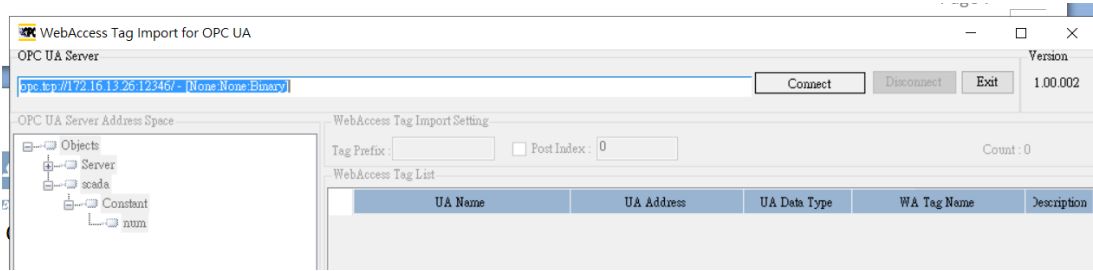
12. In upper WebAccess , create Project Node, SCADA Node, comport(tcpip) and device (OPCUA)



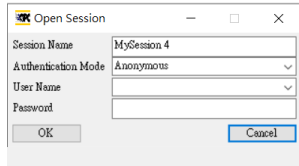
13. Opc.Ua.SampleClient.exe in C:\WebAccess\Node\tool\opcua_import_tool



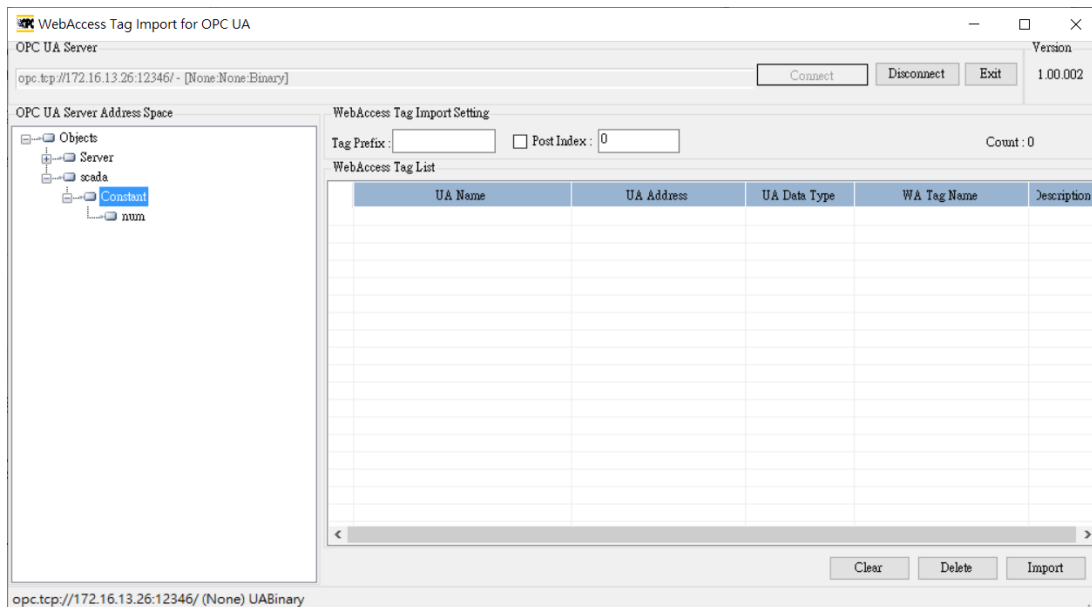
14. opc.tcp://172.16.13.26:12346/- [None:None:Binary],click connect



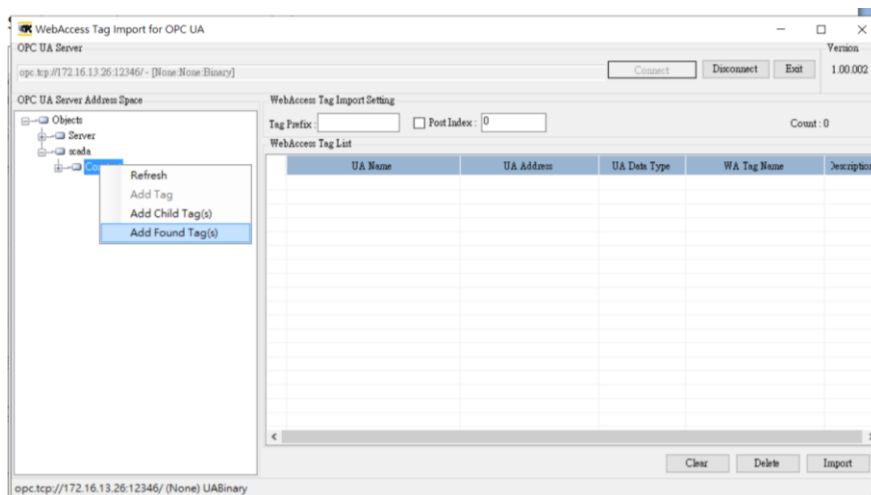
Click ok



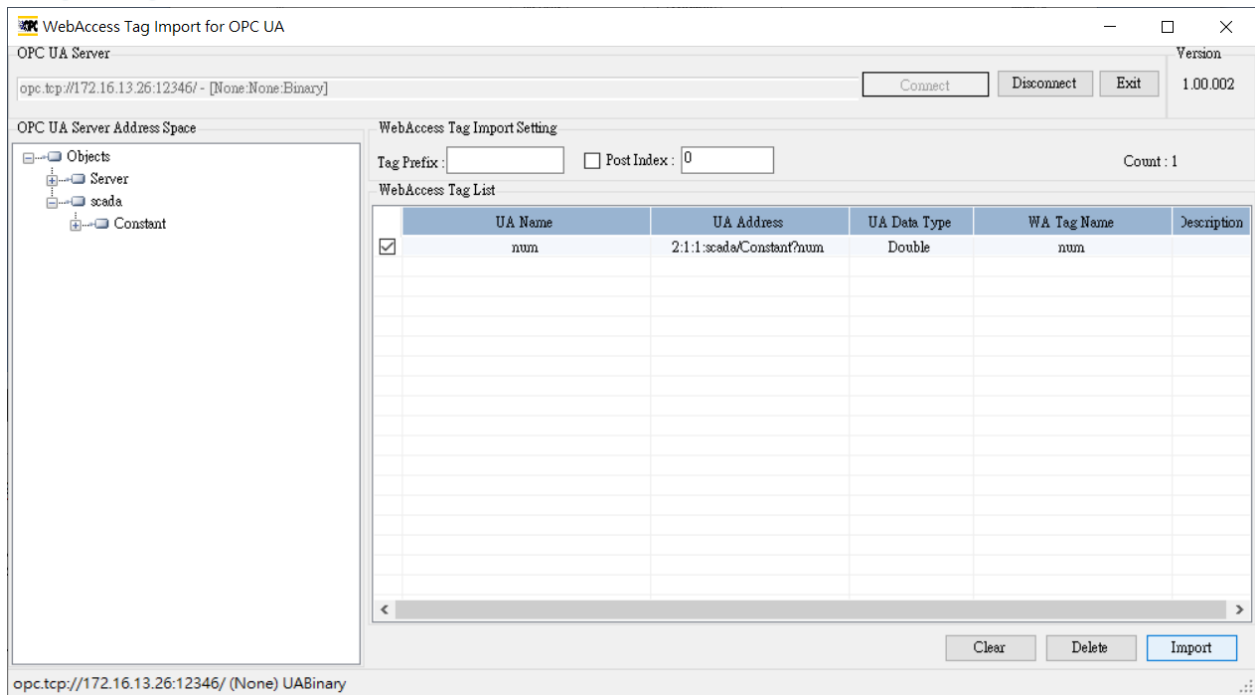
See lower WebAccess tag: num in below



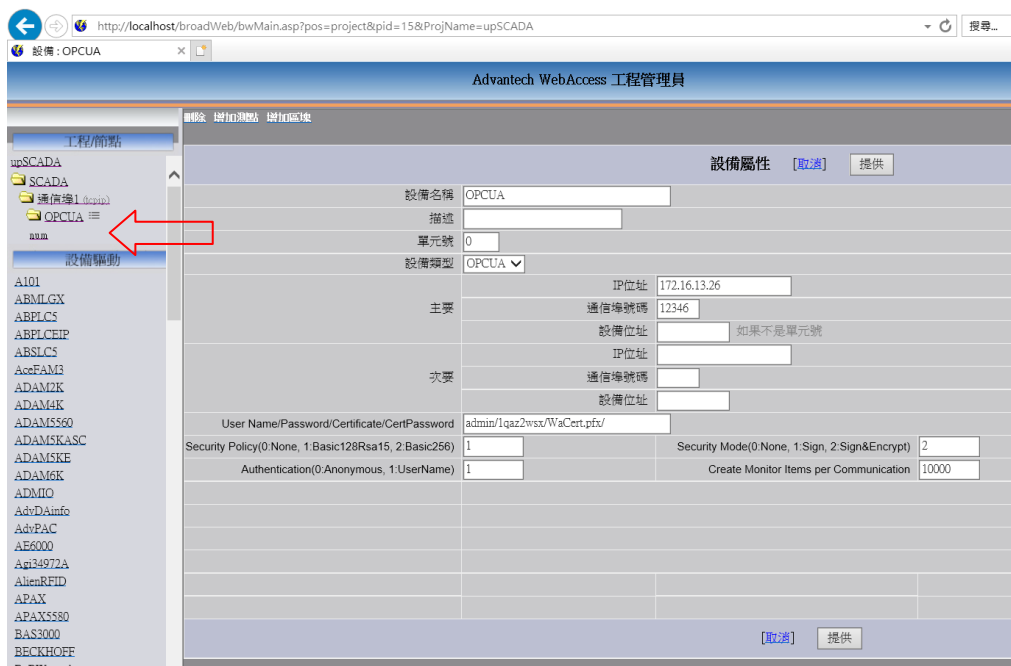
Add Found Tags



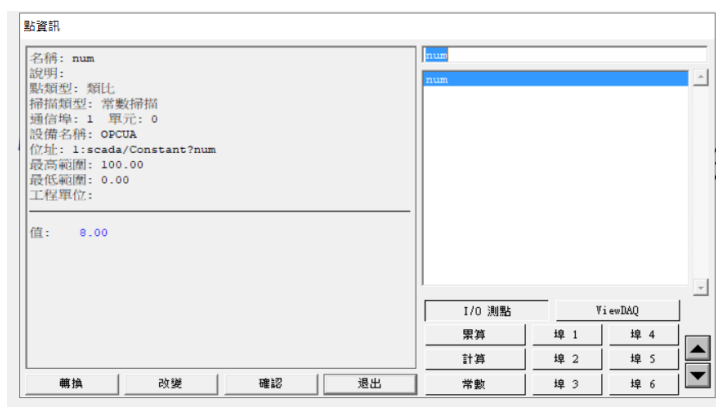
Click import tag to upper WebAccess



15. You will see lower WebAccess tag will be added to upper WebAccess

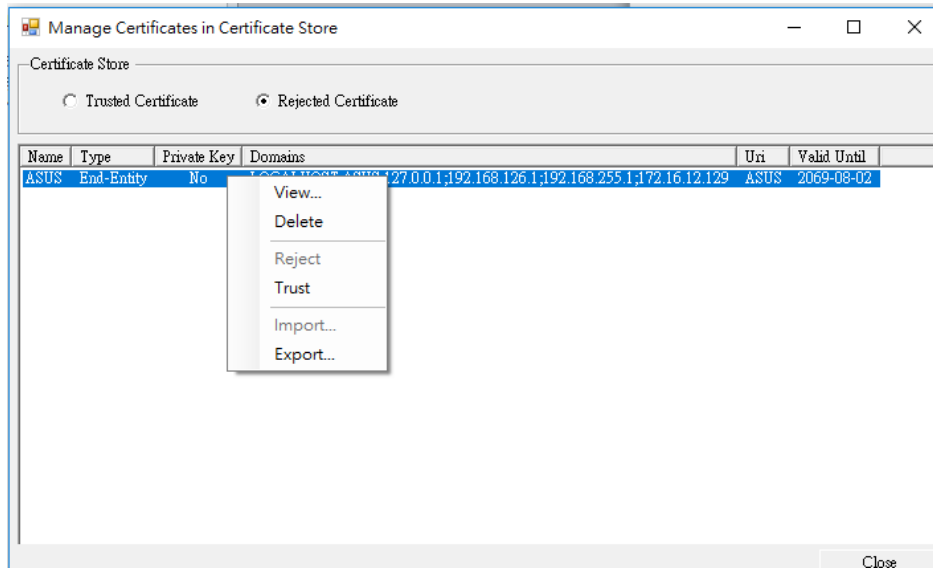


16. You will see lower WebAccess tage value will update to upper WebAccess



If upper WebAccess found value is * , please check if OPCUA server reject the upper device. If found

upper device was rejected, click **Trust**



■ **Pin Definition (in case of serial connection):**

■ **Reference:**