



How to Connect Ignition's UA Client to TOP Server

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

Contents

INTRODUCTION 3

Overview3

Intended Audience3

Required Software.....3

CONFIGURING OPC UA IN TOP SERVER 4

CONFIGURING IGNITION 11

Connection Configuration11

Testing Connection Error! Bookmark not defined.

TROUBLESHOOTING ERROR! BOOKMARK NOT DEFINED.

CONCLUSION 18

Summary18

Contact Us.....18

Introduction

Overview

The purpose of this guide is to demonstrate how to make a basic OPCUA connection to the TOP Server from Inductive Automation's Ignition SCADA. This document will cover how to enable and configure the OPC UA interface in TOP Server, and then how to connect Ignition's OPC UA Client connector to that OPC UA endpoint. The information provided here is in no way a substitute for the Ignition documentation provided by Inductive Automation, nor for the TOP Server helpfile. For comprehensive information on the settings described in this guide please reference the appropriate help file.

Intended Audience

This guide is intended for Ignition users who are new to TOP Server. The document makes the assumption that the user has some familiarity with Ignition and has configured a TOP Server project (for assistance read [Introduction to TOP Server](#)).

Required Software

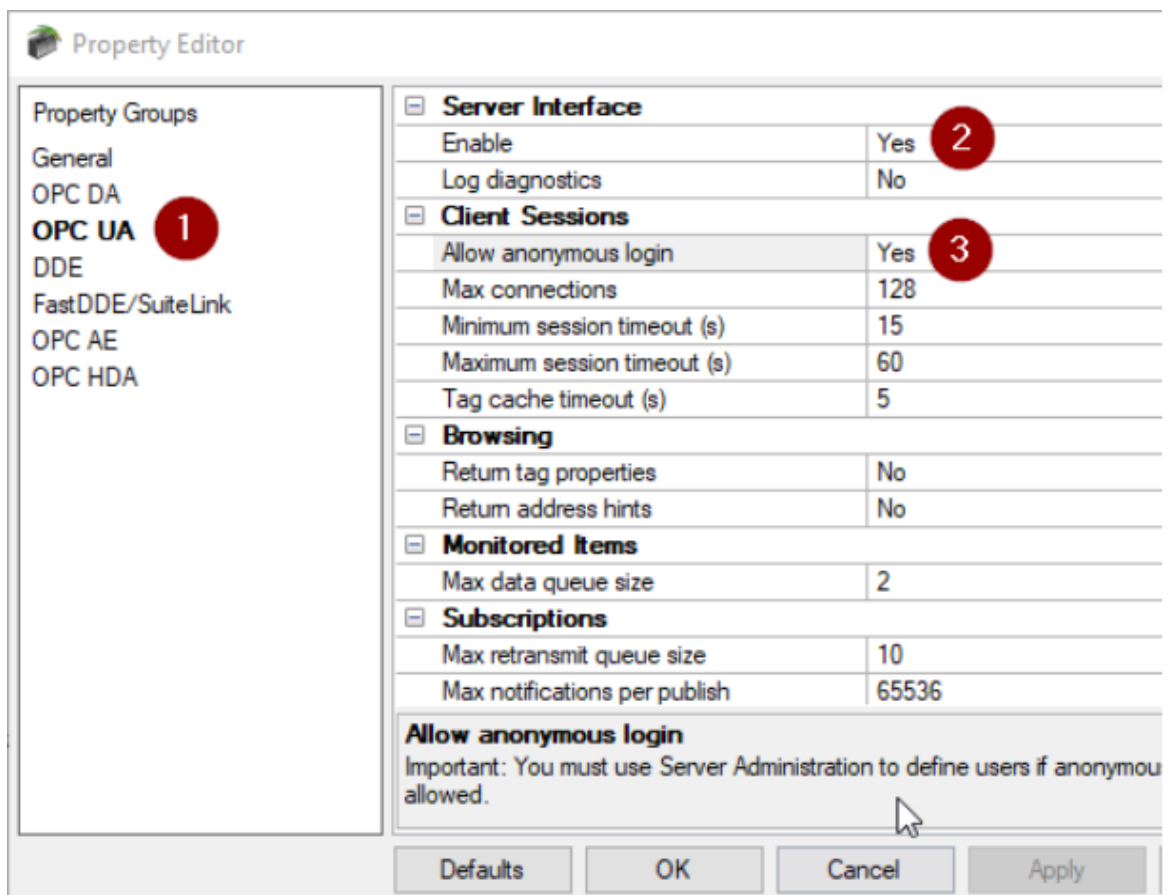
- Later TOP Server v5.x or above. If TOP Server is not already installed, the free two-hour demonstration version can be downloaded at <https://www.softwaretoolbox.com/topserverv6>. This version is fully functional but limited to two hours of runtime at a time. This demo timer is can be restarted for an additional 2 hours.
- Ignition



Configuring OPC UA in TOP Server

To connect any OPC UA client to the TOP Server, the OPC UA Server interface must be enabled, and the OPC UA Endpoint must be configured.

1. Open the TOP Server project properties. Within the OPC UA tab (1) verify that the OPC UA Interface is enabled (2), and whether the interface support anonymous user authentication (3). If the *Allow anonymous login* setting is set to No, all OPC UA Clients that connect to the TOP Server must provide a username and password in order to connect. (This username and password can be found in the TOP Server User manager – accessible through the Administrative settings icon in the system tray) Press apply and okay.



Property Editor

Property Groups

- General
- OPC DA
- OPC UA (1)**
- DDE
- FastDDE/SuiteLink
- OPC AE
- OPC HDA

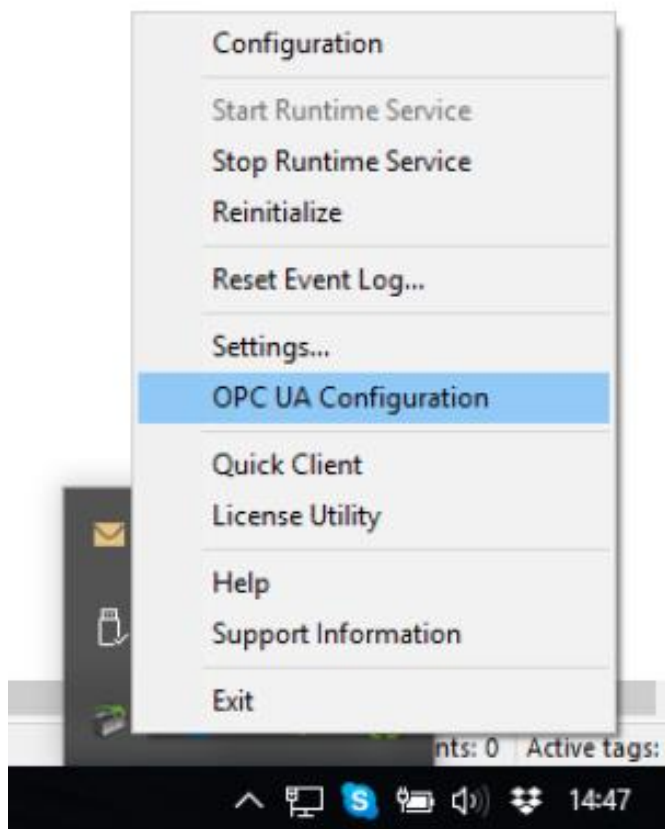
Server Interface	
Enable	Yes (2)
Log diagnostics	No
Client Sessions	
Allow anonymous login	Yes (3)
Max connections	128
Minimum session timeout (s)	15
Maximum session timeout (s)	60
Tag cache timeout (s)	5
Browsing	
Return tag properties	No
Return address hints	No
Monitored Items	
Max data queue size	2
Subscriptions	
Max retransmit queue size	10
Max notifications per publish	65536

Allow anonymous login
Important: You must use Server Administration to define users if anonymous allowed.

Defaults OK Cancel Apply



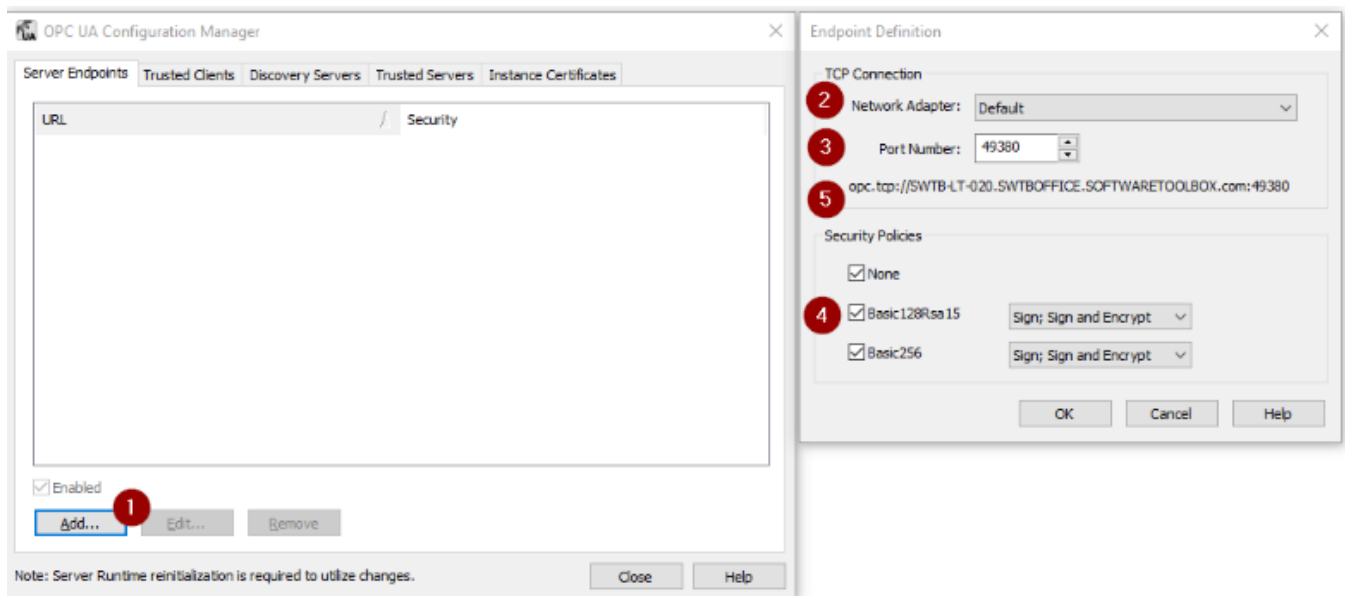
2. Launch the TOP Server's OPC UA Configuration utility. This can be launched by right clicking on the TOP Server Administrative Icon in the system tray, or by searching the start menu for "OPC UA Configuration".



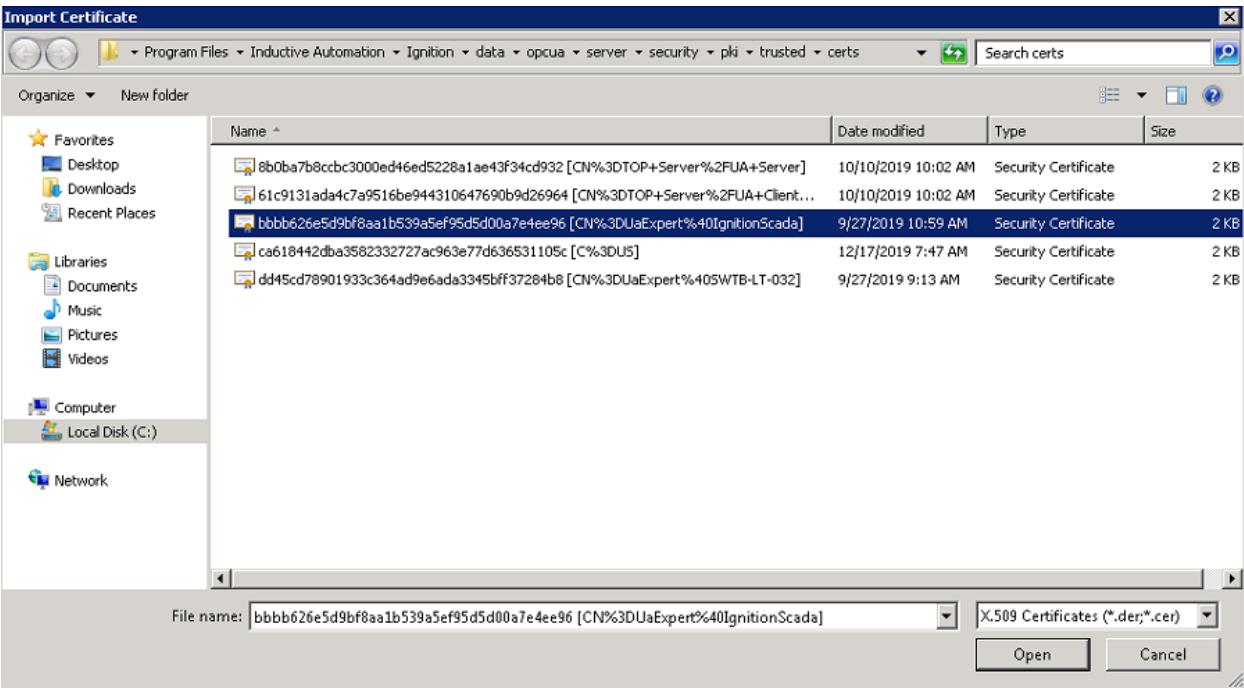
3. On the Server Endpoints tab: Add a new endpoint (1) and specify the appropriate network adapter (2) and desired port (3) on which the endpoint should be created. The supported security policies can also be configured here;
 - a. None – No endpoint authentication, message signing, or encryption will be used
 - b. Basic128Rsa15Sign – Both endpoints will authenticate the connection using certificate exchange. Signing will occur using the algorithms provided in the Basic128Rsa15 security suite.
 - c. Basic128Rsa15 Sign and Encrypt–Both endpoints will authenticate the connection using certificate exchange, and any messages exchanged over this connection will be encrypted. Signing and encryption will occur using the algorithms provided in the Basic128Rsa15 security suite.
 - d. Basic256 Sign –Both endpoints will authenticate the connection using certificate exchange. Signing will occur using the algorithms provided in the Basic256 security suite.
 - e. Basic256 Sign and Encrypt–Both endpoints will authenticate the connection using certificate exchange, and any messages exchanged over this connection will be encrypted. Signing and encryption will occur using the algorithms provided in the Basic256 security suite. Note which security policies the endpoint supports, and which policy the UA Client should use to connect.



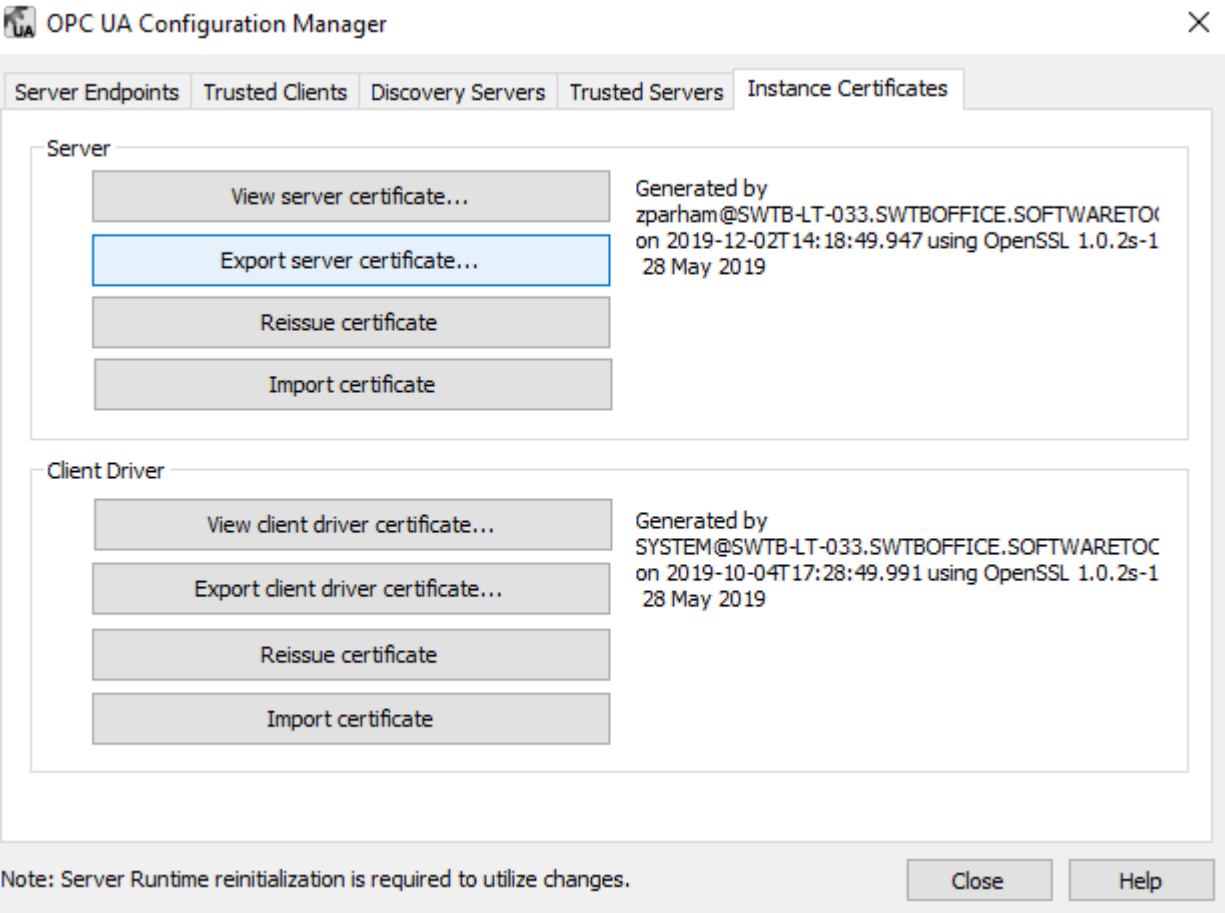
4. Make a note of the OPC UA Server endpoint (5) – this uri will be needed when connecting OPC UA Clients to the TOP Server



5. If using security on the UA endpoint, navigate to the Trusted Clients tab in the OPC UA Configuration Manager. Use the Import Button to import Ignition's OPC UA Certificate into the trusted clients certificate store. We will cover where to find this certificate in the Ignition section later in this document.

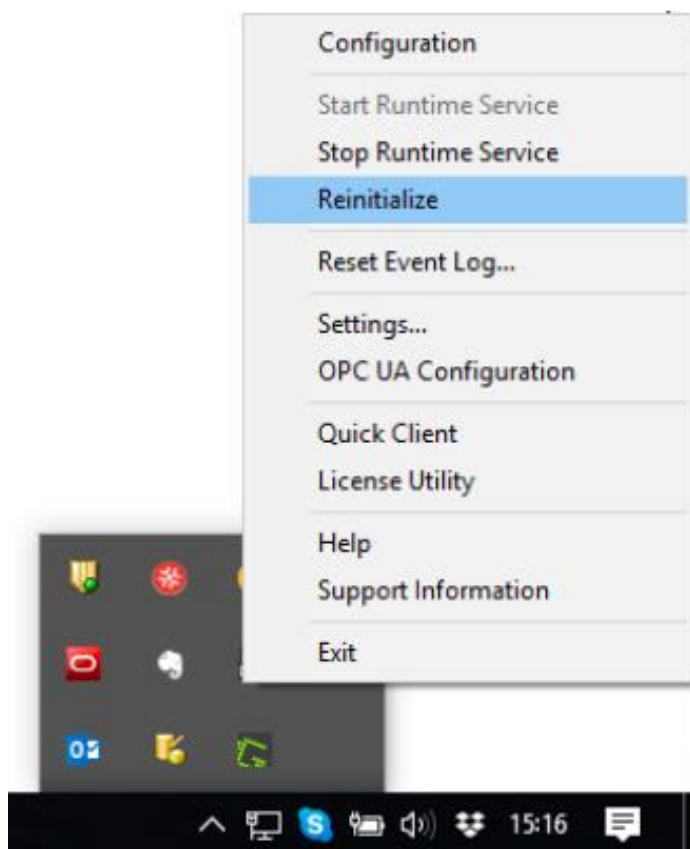


6. If using endpoint security on the OPC UA endpoint, export the TOP Server's OPC UA Server certificate while here. Importing this into Ignition will be covered later in the document.



7. Re-initialize the server. Either by opening the TOP Server configuration and navigating to Runtime > Reinitialize, or by selecting Reinitialize after right-clicking the Administrative

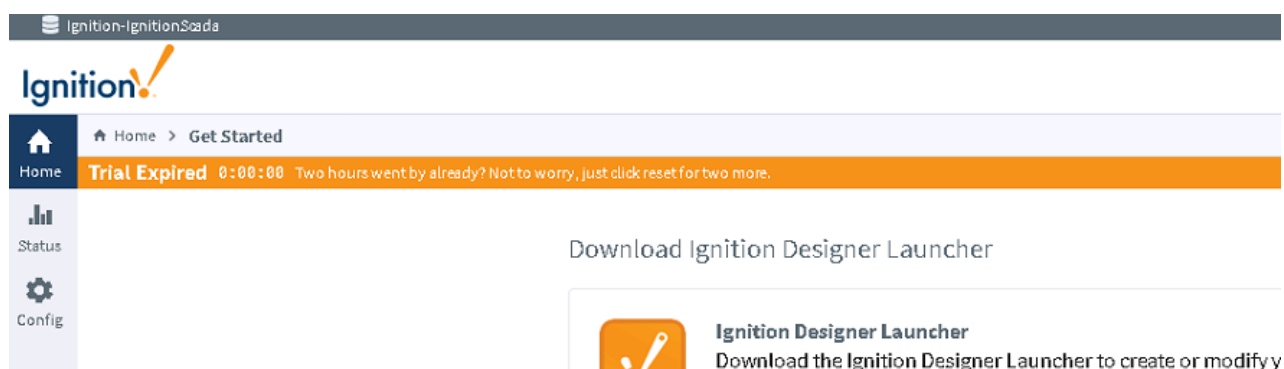
icon in the system tray. Changes to the OPC UA endpoints will not take effect until after this re-initialization is complete.



Configuring Ignition

Connection Configuration

1. Open a browser and navigate to the Ignition configuration gateway (<http://localhost:8088> by default). Log in using an Ignition account with configuration permissions. On the left side of the page, click the gear icon labeled Config.



2. Select "connect to a 3rd party OPC server" under Connections.

Configuration

From the Configure section you can set up all connections, projects, and settings
Here are some common actions to get you started.

PLATFORM

- Update System Name
- Configure Redundancy
- Install or Upgrade a Module
- Create New Project
- Activate a License
- Download Gateway Backup

NETWORKING

- Change Web Server Settings
- Enable SSL for the Gateway Network
- Create an SMTP Profile
- Manage incoming/outgoing Gateway Network connections

SECURITY

- Create a new user
- Assign a user a new role
- View the logs of an audit profile
- Define a Security Zone
- Set access levels on a Security Policy

CONNECTIONS

- Create a new database connection
- Connect to a 3rd party OPC server
- Create a new device connection

SYSTEMS

- Create an alarm journal profile
- Manage schedules and holidays
- Create a new alarm notification profile
- Test an alarm notification pipeline
- Add users to an on-call roster

DATA ACQUISITION

- Define a new realtime tag provider
- Manage tag historians
- Quickly read or write tags in a device

3. Choose "Create new OPC Connection"

Name	Type	Description	Read Only	Status	
Ignition OPC UA Server	OPC UA	A "loopback" connection to the Ignition OPC UA server running on this gateway.	false	Disabled	More edit

→ [Create new OPC Connection...](#)

Note: For details about a connection's status, see the [OPC Connection Status](#) page.

4. Choose OPC UA, then click Next

☒ **OPC UA**
 Connect to a device or server that supports OPC UA.

☐ **OPC-DA COM Connection**
 Provides access to legacy COM-based OPC-DA servers. Supports OPC-DA versions 2 and 3.

Next >

5. Skip to advanced configuration.

Endpoint Discovery

Endpoint URL

Example: opc.tcp://192.168.111.51:62541/discovery

→ Skip to Advanced Configuration

Next: Choose Server

6. Enter the discovery URL and server endpoint URL created in steps 4-5 of the TOP Server configuration. Choose the security mode and policy. Ensure this aligns with what was configured in the OPC UA Configuration, then click next.

Editing Endpoint Settings for OPC Connection

Main	
Discovery URL	<input type="text" value="opc.tcp://localhost:49380/discovery"/>
Endpoint URL	<input type="text" value="opc.tcp://127.0.0.1:49380"/>
Security Mode	<input type="text" value="None"/>
Security Policy	<input type="text" value="None"/>

Cancel

Next

7. Enter a relevant name and description. This will be shown in Ignition’s list of OPC UA connections. Click “create new OPC Connection.”

Main	
Name	TOP Server/UA@SWTB-LT-033.SWTBOI
Description	TOP Server
Enabled	<input checked="" type="checkbox"/> (default: true)
Read Only	<input type="checkbox"/> If selected, the connection to this OPC server will be read-only; all calls to write will fail. (default: false)

Authentication	
Username	
Change Password?	<input type="checkbox"/> Check this box to change the existing password.
Password	
Password	Re-type password for verification.

☐ Show advanced properties

Save Changes



8. If using OPC UA Security, the connection may initially appear as Faulted. This is expected because TOP Server is – by default – denying access to the Ignition OPC-UA Client, and the Ignition UA Client certificate must first be trusted.

✓ Successfully updated OPC Connection "TOP Server/UA@SWTB-LT-033.SWTBOFFICE.SOFTWARETOOLBOX.com"

Name	Type	Description	Read Only	Status	
Ignition OPC UA Server	OPC UA	A "loopback" connection to the Ignition OPC UA server running on this gateway.	false	Connected	More ▼ edit
SWToolbox	OPC-DA COM Connection		false	Connected	delete edit
TOP Server/UA@SWTB-LT-033.SWTBOFFICE.SOFTWARETOOLBOX.com	OPC UA	TOP Server	false	Connected	More ▼ edit

→ [Create new OPC Connection...](#)

Note: For details about a connection's status, see the [OPC Connection Status](#) page.

Return to the TOP Server OPC UA Configuration manager, and on the Trusted Clients tab, click on Ignition OPC-UA Client certificate. Click the Trust button to install/trust the Ignition Client certificate. The Ignition OPC Server Connections page will now show the Status of the TOP Server to be Connected.

Troubleshooting the OPC UA Connection from Ignition

1. The Ignition OPC UA Connection page shows the status of all OPC UA Server connections.
If the TOP Server connection is listed as disabled or faulted make sure that any configuration changes have been saved and are running.
2. If the connection is still showing that it is Faulted, open the OPC Connection Status page and click on the Faulted status.

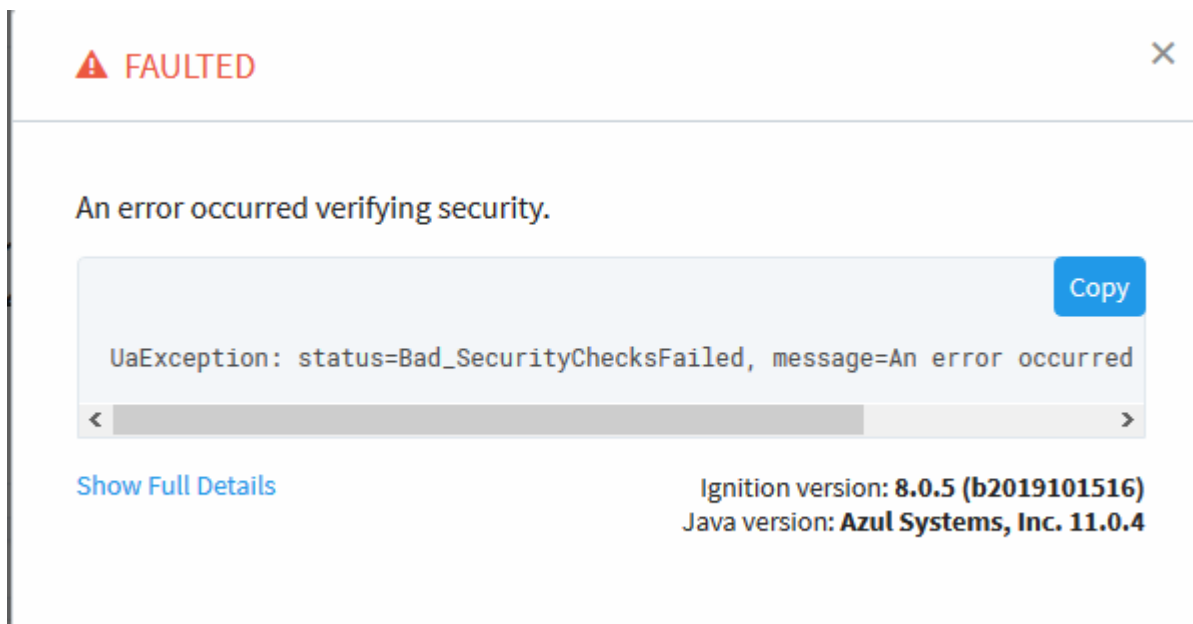
Connected Servers

2 / 3

Filter

Name ▾	Type	Uptime	Status	
TOP Server/UA@SWTB-LT-033.SWTBOFFICE.SOFTWARETOOLBOX.com	OPC UA	Unknown	▲ FAULTED	Subscriptions
SWToolbox	OPC-DA COM Connection	13 days	✓ CONNECTED	
Ignition OPC UA Server	OPC UA	an hour	✓ CONNECTED	Subscriptions

3. This will show the specific error code and associated explanation that can be used for further connection troubleshooting.



Information regarding OPC UA error codes can be found here:

http://support.softwaretoolbox.com/app/answers/detail/a_id/3718/

For certificate issues, please reference the [TOP Server OPC UA Certificate Exchange help file](#).

It is recommended to use the UnifiedAutomation UAExpert as a free and versatile OPC UA test client, that can be used to troubleshoot OPC UA connection issues.



Conclusion

Summary

This guide has demonstrated the basic steps for configuring an OPC UA connection from TOP Server to Ignition.

To evaluate what TOP Server can offer in terms of robust, reliable device data acquisition, download a free two hour demonstration of TOP Server at <https://www.softwaretoolbox.com/topserverv6>. This demonstration version is fully functional, only requiring a restart at the end of the two-hour demonstration period.

For further questions the Software Toolbox Support Team is available to help:

Contact Us

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

