

OPC UA security: modes, certificates and trust lists

Do not leave an OPC UA connection at “it works”. Treat security mode, certificate trust and user authentication as separate decisions.

In short

- A connection can be encrypted and still be opened by an anonymous user, so security mode and user authentication must be checked separately.
- The “none” security mode is useful in a lab trial, but on a production network it leaves messages readable and modifiable.
- Adding a certificate to a trust list grants that application access, so certificates should not be accepted automatically without verifying their owner.

01 / Three separate decisions

In OPC UA, communication security (signing and encrypting the channel), application identity (certificates) and user authentication are different concepts. A connection can be encrypted and still be opened by an anonymous user. Give each its own checklist.

02 / Security mode

The security mode takes one of three values: none, sign only, sign and encrypt. “None” is useful in a lab trial, but on a production network it leaves messages readable and modifiable. Document that the security policy (algorithm suite) you use is supported by both server and client and that old, weak policies are disabled.

03 / Manage certificates

Every application instance carries a certificate. Adding a certificate to a trust list grants that application access. Do not auto-accept a certificate without verifying its owner. Track expiry dates; an expired certificate can become an unexpected data outage on a production line.

04 / A read account for AI work

Give the data science team a separate, read-only user and, if possible, a separate application certificate. A read account without write permission prevents a faulty model from changing a setting in the field. This guide is a suggested security practice and makes no certification or compliance claim.

Try it

List the endpoints on your own OPC UA server and tabulate each one’s security mode and accepted user token types.

References and online guide

[Open the online guide](#)

OPC Foundation: OPC UA

Proposed pilot steps do not claim field accuracy. Synthetic examples are not measurements from a production site.