Check device certificate validation

Exercise the device as a TLS client and record what happens when the server certificate is wrong.

Planning template only. No tests have been run and no results are asserted.

01 Plan the evaluation

1. Verify a valid connection first

Place FID in an authorized test link and exercise the device against its normal, valid server. Confirm that the intended transaction works and identify the hostname and connection you want to test.

2. Exercise invalid certificates

Select a target and a supported invalid-certificate case. Trigger a full, certificate-based TLS handshake and verify the intended test certificate was presented. Session resumption can omit certificate exchange; a new connection alone does not prove validation was exercised.

3. Review evidence, then rerun

Record the certificate identifier, handshake evidence, connection outcome, and any application-data evidence for each case. Preserve the device firmware and configuration, restore the valid baseline, and repeat after a fix.

Setup checklist

- A FID configuration with the certificate-validation workflow and compatible tool image; confirm the supplied release and scope in the quotation.
- An Ethernet-connected client, a reachable test destination, and a repeatable way to trigger the relevant TLS connections.
- A separate management connection. The 10 GbE Ubuntu appliance uses a third wired interface; WiFi management applies only to WiFi-enabled platforms.

Scope and limits

- This tests client certificate validation. It is not a claim to decrypt arbitrary traffic or defeat correctly enforced certificate pinning.
- Protocol, TLS behavior, target selection, and test-case coverage must be checked against the specific device. Results require engineering interpretation.
- FID can operate independently. Optional EtherShunt bypass is available only on 1 GbE links and is not hitless; 10 GbE FID does not inherit that bypass capability.

Offering: Documented FID workflow. Confirm the delivered configuration before testing.

Record the result

Check device certificate validation

Distinguish an explicit certificate rejection from a timeout, a failed connection for another reason, or a case the device never exercised. No observed application data is not, by itself, proof of correct certificate validation. Mark cases that were never exercised as Not run, and unexplained outcomes as Inconclusive.

Test owner

Date / run ID

Equipment / firmware / tool versions

Authorized scope and acceptance criteria (define before the test)

01 Valid-server control

The intended transaction succeeds before and after the test.

☐ Not run ☐ Pass ☐ Fail ☐ Inconclusive

Observed behavior / evidence reference:

02 Self-signed certificate

Whether the client rejects it or proceeds with application data.

☐ Not run ☐ Pass ☐ Fail ☐ Inconclusive

Observed behavior / evidence reference:

03 Wrong-hostname or expired certificate

The exercised case, connection outcome, and supporting evidence.

☐ Not run ☐ Pass ☐ Fail ☐ Inconclusive

Observed behavior / evidence reference:

Recovery, unresolved questions, and next action

Attach additional evidence as needed. Keep completed records in your approved storage; this worksheet does not submit any data.