HTTPS certificate

The question

A certificate needs an owner

HTTPS depends on a trusted, current certificate for the requested hostname. Renewal and live deployment both need attention.

01 Understand

02 Observe

03 Verify

A practical briefing for the people who own your domain.

HTTPS certificate

The mechanism

The client checks identity

It checks the certificate name, validity and chain against its trust store before establishing the authenticated connection.

01 Requested hostname

↓

02 Server certificate and chain

↓

03 Client trust and name checks

Trust is evaluated by the connecting client. The scanner records its own successful or unsuccessful authentication attempt.

HTTPS certificate

The evidence

Our result is one connection

> We test the submitted hostname using the scanner trust store. Revocation, future renewal and every edge endpoint are outside this check.

PUT THE OBSERVATION IN CONTEXT

Public signal

Service context

Operational validation

Use the finding to start an owned review.

HTTPS certificate

The handoff

Review renewal and deployment

Have your hosting owner confirm hostname coverage and the served chain. Assign alerts and verify renewal automation.

BRING THE RIGHT OWNERS TOGETHER

01 Web hosting or edge platform owner

02 Service operations

HTTPS certificate

Your checklist

Keep certificate evidence current

- ✓ List production hostnames
- ✓ Record the expiry
- ✓ Confirm the alert recipient
- ✓ Verify the live certificate

> Read the HTTPS certificate explainer.
>
> **/learn/certificate**