Validate

- DCV situations
  - Non-wildcard certificates
  - Wildcard certificates
  - Minimize downtime
  - Minimize customer effort
- Potential issues

import { Render } from "~/components";

When you create a custom hostname, choose one certificate validation method. The API accepts one `ssl.method` value: `http`, `txt`, or `email`.

DCV situations

Non-wildcard certificates

Wildcard certificates

- DCV Delegation (auto-issuance)
- Manual

Minimize downtime

If you want to minimize downtime, explore one of the following methods to issue and deploy the certificate before onboarding your customers:

- Delegated DCV: Place a one-time record at your authoritative DNS that allows Cloudflare to auto-renew all future certificate orders.
- TXT validation: Have your customers add a `TXT` record to their authoritative DNS.
- Manual HTTP validation: Add a `TXT` record at your origin.

Minimize customer effort

If you value simplicity and your customers can handle a few minutes of downtime, you can rely on Cloudflare automatic HTTP validation.

Automatic HTTP validation requires the hostname to point to your SaaS target before the CA can fetch the validation token. During that period, the hostname may route to Cloudflare before the certificate reaches `ssl.status: active`.

Potential issues

To avoid or solve potential issues, refer to our troubleshooting guide.

□□□ #2
□ □□□ □□□ 2026-11-01 00:27:03 UTC
□ □□□ □□□ 2026-11-01 00:27:05 UTC