Cloudflare Docs

SSL/TLS

Products > SSL/TLS > ... > Advanced certificates > Manage advanced certificates

# Manage advanced certificates

## Create a certificate

If you are using an existing Universal SSL certificate, Cloudflare will automatically replace this certificate once you finish ordering your advanced certificate.

Once you order a certificate, you can review the certificate's status in the dashboard at **SSL/TLS** > **Edge Certificates** or via the API with a GET request API.

**Dashboard** **API**

To create a new advanced certificate in the dashboard:

1. Log in to your Cloudflare account and select a domain.
2. Go to **SSL/TLS** > **Edge Certificates**.
3. Select **Order Advanced Certificate**.
4. If Cloudflare does not have your billing information, you will need to enter that information.
5. Enter the following information:
   - Certificate Authority
   - Certificate Hostnames
   - Validation method
   - Certificate Validity Period
6. Select **Save**.

> The available options for **Validation method** and **Certificate Validity Period** may vary depending on the certificate authority you choose and the hostnames that you include in your Advanced certificate order.

## Delete a certificate

**Dashboard** **API**

To delete an advanced certificate in the dashboard:

1. Log in to your Cloudflare account and select a domain.
2. Select **SSL/TLS** > **Edge Certificates**.
3. Select a certificate.
4. Select **Delete Certificate**.

## Restart validation

To restart validation for a certificate in a `validation_timed_out` status, send a PATCH request API to the API.

## Restrict cipher suites

Cipher suites are a combination of ciphers used to negotiate security settings during the SSL/TLS handshake (and therefore separate from the SSL/TLS protocol).
For more details, refer to Disable cipher suites.

## Perform domain control validation (DCV)

Before a certificate authority (CA) will issue a certificate for a domain, the requester must prove they have control over that domain. This process is known as domain control validation (DCV).

Normally, you only need to update DCV if you have your application on a partial setup (Cloudflare does not run your authoritative nameservers).

For more information about DCV, refer to DCV methods.

> Due to recent changes, HTTP DCV validation will soon not be allowed for wildcard certificates or certificates with multiple Subject Alternative Names (SANs). For more details and next steps, refer to Changes to HTTP DCV.

Cloudflare Dashboard · Community · Learning Center · Support Portal · Your Privacy Choices

Edit on GitHub · Updated 1 year ago