

[Directory](#) > [SSL/TLS](#) > [Edge certificates](#) > [Add CAA records](#)

Add CAA records

[Copy as Markdown](#) | [View as Markdown](#) | [Agent setup](#)

A Certificate Authority Authorization (CAA) DNS record specifies which certificate authorities (CAs) are allowed to issue certificates for a domain. This record reduces the chance of unauthorized certificate issuance and promotes standardization across your organization.

For additional security, set up [Certificate Transparency Monitoring](#) as well.

Note

For more technical details about CAA records, refer to the [introductory blog post](#).

Who should create CAA records?

You should [create CAA records](#) in Cloudflare if each of the following is true:

- You uploaded your own custom origin server certificate (not provisioned by Cloudflare).
- That certificate was issued by a CA (not self-signed).
- Your domain is on a [full setup](#) (not a [CNAME setup](#)).
- When adding new [Custom Hostname](#) and your customer has existing CAA records. In this case, ask your customer to remove the existing CAA records or add the missing CAA record.

CAA records added by Cloudflare

Cloudflare adds CAA records automatically in the following situations:

- When you have [Universal SSL](#) and add any CAA records to your zone.
- When you have [advanced certificates](#) and add any CAA records to your zone.

These records make sure Cloudflare can still issue Universal certificates on your behalf.

Subdomain zones caveat

CAA records are inherited. This means that, if you are using a [subdomain setup](#) - with `subdomain.example.com` on Cloudflare but `example.com` on a different DNS provider -, you should make sure that the parent domain (`example.com`) either has CAA records that allow [Cloudflare's partner CAs](#), or has no CAA records at all.

If Cloudflare has automatically added CAA records on your behalf, these records will not appear in the Cloudflare dashboard. However, if you run a command line query using `dig`, you can see any existing CAA records, including those added by Cloudflare (replacing `example.com` with your own domain on Cloudflare):

```
→ ~ dig example.com caa +short
```



```
# CAA records added by Google Trust Services
```

```
0 issue "pki.goog; cansignhttpexchanges=yes"
```

```
0 issuewild "pki.goog; cansignhttpexchanges=yes"
```

```
# CAA records added by Let's Encrypt
```

```
0 issue "letsencrypt.org"
```

```
0 issuewild "letsencrypt.org"
```

```
# CAA records added by SSL.com
```

```
0 issue "ssl.com"
```

```
0 issuewild "ssl.com"
```

```
# CAA records added by Sectigo
```

```
0 issue "sectigo.com"
```

```
0 issuewild "sectigo.com"
```

Note

This list is not exhaustive, and other CAs might be added or removed for operational reasons.

Create CAA records

Create a CAA record for each Certificate Authority (CA) that you plan to use for your domain.

Dashboard API

To add a CAA record in the dashboard,

1. In the Cloudflare dashboard, go to the **DNS Records** page.

Go to **Records** 

2. Select **Add record**.
3. For **Type**, select **CAA**.
4. For **Name**, type your domain.
5. Choose a **Tag**, which specifies the behavior associated with the record.
6. For **CA domain name**, enter the CA name.
7. Select **Save**.
8. Repeat for each CA associated with your domain.

Once you have finished creating all the records, you can review them in the list of records appearing under the DNS Records panel.

Certificate authorities and required CAA values

If you have CAA records on your domain, they must permit the certificate authority (CA) that Cloudflare uses. For the required CAA values for each CA Cloudflare may use, refer to [Certificate authorities](#).

CNAME chain CAA records [↗](#)

CAA records on a CNAME target also apply. If your hostname CNAMEs to a domain whose zone has restrictive CAA records, those records take precedence — even if your own domain has no CAA records.

Check CAA at all levels of your CNAME chain:

```
dig yourdomain.com CAA +short
dig cname-target.com CAA +short
```

WAS THIS HELPFUL?

 Yes

 No

[Previous](#)

[← Supported options](#)

[Next](#)

[Staging environment →](#)

Resources

[API](#)

[New to Cloudflare?](#)

[Directory](#)

[Sponsorships](#)

[Open Source](#)

Support

[Help Center](#)

[System Status](#)

[Compliance](#)

[GDPR](#)

Cloudflare Research

Company

[cloudflare.com](#)

[Our team](#)

[Careers](#)

Tools

[Cloudflare Radar](#)

[Cloudflare Labs](#)

[Speed Test](#)

[Is BGP Safe Yet?](#)

[Certificate Transparency](#)

Community

 [Community forum](#)

 [X](#)

 [Discord](#)

 [YouTube](#)

 [GitHub](#)

© 2026 Cloudflare, Inc. • [Privacy Policy](#) • [Terms of Use](#) • [Report Security Issues](#) • [Trademark](#)

•  [Cookie Settings](#)