

Limitations

 Copy as Markdown |  View as Markdown |  Agent setup

Universal SSL certificates present some limitations.

Proxy status

Cloudflare can only serve an SSL/TLS certificate for a DNS record when you set the record's [proxy status](#) to **Proxied**. If you do not do this, the origin server your record points to will be responsible for supporting SSL/TLS connections.

Hostname coverage

Full setup

When you rely only on Universal SSL in a full setup zone, coverage is limited to the root domain (for example, `example.com`) and first-level subdomains (for example, `www.example.com` or `blog.example.com`). Deeper subdomains — such as `dev.www.example.com` or `app3.dev.www.example.com` — are **not** covered and will not serve a valid certificate.

To enable SSL for deeper subdomains, you can:

- Purchase [Advanced Certificate Manager](#) — then turn on [Total TLS](#) for automatic certificate coverage of all proxied subdomains, or manually create advanced certificates for specific hostnames.
- Upload a [custom SSL certificate](#) that includes the required subdomains as Subject Alternative Names (SANs).

CNAME setup

On a [CNAME setup zone](#), each subdomain (regardless of level) has its own Universal SSL certificate and does not require additional features or purchases. As long as the subdomains are proxied to Cloudflare, a universal certificate [will be provisioned](#).

Certificate authority

For Universal SSL certificates, Cloudflare chooses the [certificate authority \(CA\)](#) used for your certificate.

Cloudflare can change the [certificate authority](#) without prior notification, and will not send any notification as the change happens.

If you want to choose the issuing certificate authority, [order an advanced certificate](#).

Validity period

For Universal certificates, Cloudflare controls the validity period. Refer to [validity periods and renewal](#) for details.

TLS settings

[Customizing cipher suites](#) is only available with [Advanced Certificate Manager](#) or within [Cloudflare for SaaS](#).

You can set up [minimum TLS version](#) at the zone level, but, for per-hostname settings, you must have [Advanced Certificate Manager](#).

Delegated DCV

Delegated DCV allows zones with [partial DNS setups](#) to delegate the DCV process to Cloudflare. DCV delegation will not work with Universal SSL certificates and requires the use of an [advanced certificate](#).

Spectrum

Universal SSL is not compatible with [Cloudflare Spectrum](#). If you are trying to use Spectrum, use either [an advanced certificate](#) or [a custom certificate](#).

Load balancing

Due to internal limitations, Universal SSL certificates do not cover [load balancing hostnames](#) by default. This behavior will be corrected in the future.

Browser support

For more on browser support, see [Browser compatibility](#).

SSL invalid brand check

Some domains are not eligible for Universal SSL if they contain words that conflict with trademarked domains.

To resolve this issue, you can:

- Purchase an [advanced certificate](#).
- Upload your own [custom certificate](#).

Certificate pinning

Cloudflare does not support HTTP public key pinning (HPKP) for universal, advanced, or custom hostname certificates. For details and recommended alternatives, refer to [Certificate pinning](#).

WAS THIS HELPFUL?

 Yes

 No

[Previous](#)
← Alerts

[Next](#)
Troubleshooting →

Resources

[API](#)
[New to Cloudflare?](#)
[Directory](#)
[Sponsorships](#)
[Open Source](#)
[Cloudflare Research](#)

Company

[cloudflare.com](#)
[Our team](#)
[Careers](#)

Community

 [Community forum](#)
 [X](#)
 [Discord](#)
 [YouTube](#)
 [GitHub](#)

Support

[Help Center](#)
[System Status](#)
[Compliance](#)
[GDPR](#)

Tools

[Cloudflare Radar](#)
[Cloudflare Labs](#)
[Speed Test](#)
[Is BGP Safe Yet?](#)
[Certificate Transparency](#)