CLOUDFLARE

PRODUCT BRIEF

Advanced Certificate Manager

Secure your application with Transport Layer Security (TLS) while reducing your certificate lifecycle management overhead.

Secure your web applications with TLS while reducing your team's workload

Advanced Certificate Manager automatically administers certificates, allowing flexibility for complex TLS requirements

TLS is the backbone of privacy and data security on the Internet, allowing your end users to browse the Internet privately without exposing their credit card information or other sensitive data. **Advanced Certificate Manager** can help your organization secure your web apps with TLS by:

- Delegating TLS certificates issuance, management, and renewal to Cloudflare. Automatic management means improved team productivity.
- Strengthening your security posture with automatic encryption for all new domains you create, customizable for your organizational and regulatory needs.

Which solution is right for you?	
Universal SSL certificates are ideal if you:	**Advanced or custom certificates are ideal if you:**
• Require a free SSL/TLS solution to reduce certificate lifecycle management overhead • Have only one level of subdomain • Need a one-size-fits-all solution	• Want full TLS coverage for all your hostnames • Have specific requirements for what hostnames need to be on the SSL/TLS certificates • Prefer to use a shorter validity period than the default 90 days • Have a preferred certificate authority you'd like to use • Want to set custom cipher suites

Streamline certificate management

Cloudflare automatically issues and renews TLS certs on your behalf, reducing overhead.

Customize your TLS deployment

Customize hostnames on the cert, adjust the validity period, select your own certificate authority (CA) and cipher suites, bring your own certs, and more.

Ensure compliance

Stay up to date with industry, regulatory, and organizational compliance requirements with the latest in cryptography.

Key features of Advanced Certificate Manager

Let Cloudflare automatically issue a certificate for every new domain you create

As your organization grows, it's very likely you will need new hostnames and new web properties, such as new product lines or localized versions of your websites. Automatic issuance with each new hostname means no security or privacy gaps for your newly created domains. Launching a new website is hard work—let Cloudflare take care of TLS for you.

Encrypt more than one level of subdomain

As you create more subdomains on your website, Cloudflare will always issue a certificate on your behalf —and renew them when their validity periods are up.

Choose your preferred certificate authority (CA)

Some organizations may prefer to choose a particular CA to work with. Advanced Certificate Manager allows you to choose which CA will issue your certificates. See the current list of CAs we work with.

You can generate a Certificate Signing Request (CSR) to get a custom certificate from the CA of your choice while Cloudflare maintains control of the private key. The private key associated with the CSR will be generated by Cloudflare and will never leave our network.

Customize the certificate validity period

While certs typically have a standard validity period of 90 days, Advanced Certificate Manager allows you to set shorter periods to ensure stronger security and reduce the blast radius in the event of a breach.

Accept requests only from your preferred TLS versions

Previous versions of TLS, such as TLS 1.1 or 1.2, may see slower connections and worse security than TLS 1.3. You can choose to set a minimum TLS version from which to accept requests. For example, if you set a minimum version of TLS 1.2, your website will accept connections from clients using TLS 1.2 and 1.3.

Control cipher suites used for TLS

With Advanced Certificate Manager, you can restrict connections between Cloudflare and clients—such as your visitor's browser—to only allow connections from specific cipher suites.

You may want to do this to follow specific industry recommendations, to disable weak or outdated cipher suites, or to comply with regulations or organizational requirements.

"Advanced Certificate Manager has simplified the way we manage certificates across our many domains, while still allowing us to meet our strict security requirements. The ability to manage cipher suites, as well as auto-renewal within our parameters, creates for an available and secure environment."

Colin Henderson
Director of Engineering, OneTrust

OneTrust

