# Types of SSL Certificates | SSL Certificate Types Explained

There are several types of different SSL certificates. While all provide the same level of TLS encryption, they serve different purposes and are used in different contexts.

Share



## SSL Certificate Types Learning Objectives

After reading this article you will be able to:

- Understand the different types of SSL (TLS) certificates
- Learn about the different SSL certificate validation levels

### Related Content


What is SSL?

What is an SSL Certificate?

SSL Handshake

Keyless SSL

How SSL Works


## What does an SSL certificate do?

An SSL certificate (more accurately called a TLS certificate), is necessary for a website to have HTTPS encryption. An SSL certificate contains the website's public key, the domain name it's issued for, the issuing certificate authority's digital signature, and other important information. It's used for authenticating an origin server's identity, which helps prevent on-path attacks, domain spoofing, and other methods attackers use to impersonate a website and trick users.

HTTPS creates an encrypted connection between a user's browser and the web server they are communicating with, protecting the communications from being intercepted. SSL certificates are necessary for establishing this encrypted connection (see What is an SSL certificate? to learn more).

## What are the different types of SSL certificates?

### Single Domain SSL Certificates

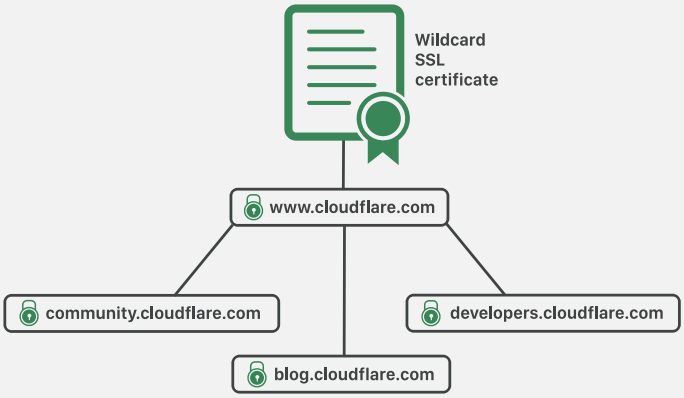
A single-domain SSL certificate applies to one domain and one domain only. It cannot be used to authenticate any other domain, not even subdomains of the domain it is issued for.

All pages on this domain are also secured with the certificate; for instance, if cloudflare.com has a single-domain certificate, then cloudflare.com/learning (the Learning Center main page) is also covered by that certificate.


### Wildcard SSL Certificates

Wildcard SSL certificates are for a single domain and all its subdomains. A subdomain is under the umbrella of the main domain. Usually subdomains will have an address that begins with something other than 'www.'

For example, www.cloudflare.com has a number of subdomains, including blog.cloudflare.com, support.cloudflare.com, and developers.cloudflare.com. Each is a subdomain under the main cloudflare.com domain.

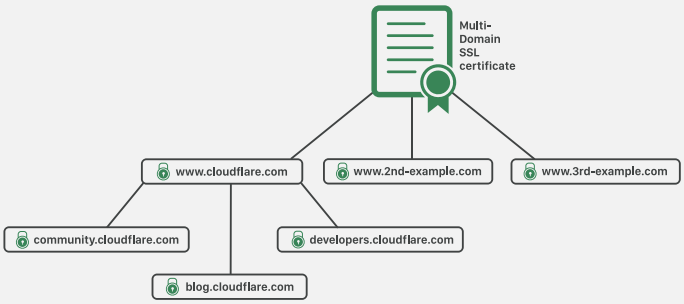



A single Wildcard SSL certificate can apply to all of these subdomains. Any subdomain will be listed in the

SSL certificate. Users can see a list of subdomains covered by a particular certificate by clicking on the padlock in the URL bar of their browser, then clicking on "Certificate" (in Chrome) to view the certificate's details.

### Multi-Domain SSL Certificates (MDC)

A multi-domain SSL certificate, or MDC, lists multiple distinct domains on one certificate. With an MDC, domains that are not subdomains of each other can share a certificate.




Cloudflare issues free SSL certificates to make it possible for anyone to turn on HTTPS encryption, and these certificates are MDCs. Dedicated and customized SSL certificates are available for purchase.

## What are SSL certificate validation levels?

A bank doesn't issue a loan to someone before performing a credit check. Similarly, before a certificate authority (CA) issues an SSL certificate to an organization, they have to validate the organization; it has to be proven that the organization actually owns and operates the domain. This is what's known as SSL certificate validation.

However, there are different levels of validation, ranging from bare minimum validation to thorough background investigations. An SSL certificate from any of these validation levels provides the same degree of TLS encryption; the only difference is how thoroughly the CA has authenticated the organization's identity.

### Domain Validation SSL Certificates

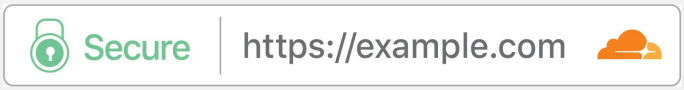
Domain Validation is the least-stringent level of validation. To obtain one of these SSL certificates, an organization only has to prove they control the domain. They can do this by altering the DNS record associated with the domain, or sometimes just by sending the CA an email. Often the process is automated.

This level of validation is the cheapest. It's a good option for blogs, portfolio sites, or for small businesses that are just looking to quickly launch HTTPS, especially if a business doesn't sell products via its website (e.g. a restaurant or coffee shop).

### Organization Validation SSL Certificates

Organization Validation involves a manual vetting process: The CA will contact the organization requesting the SSL certificate, and they may do some further investigating. Organization Validation SSL certificates will contain the organization's name and address, making them more trustworthy for users than Domain Validation certificates.

### Extended Validation SSL Certificates




Extended Validation involves a full background check of the organization. The CA will make sure that the organization exists and is legally registered as a business, that they actually are present at the address they list, and so on. This validation level takes the longest and costs the most, but Extended Validation SSL certificates are more trustworthy than other types of SSL certificates. Consequently, these certificates are necessary for a website's address to turn the browser URL bar green, the visual representation for users of a trustworthy TLS-encrypted site.

Large enterprises, financial institutions, and eCommerce stores should obtain Extended Validation certificates. This is especially crucial if a site or application handles sensitive customer data, such as passwords, credit card numbers, or names and addresses.

To learn more about how to get a free SSL certificate from Cloudflare, see our SSL page. Check if your website's SSL certificate is working properly.

Why Use HTTPS?
HTTP Security Gaps
Connection Not Private

About Encryption
What is Encryption?
Public Key Encryption
Asymmetric Encryption
Lava Lamp Encryption
Cryptographic Key
What is a Session Key?

SSL Glossary
What is Mixed Content?
SSL Handshake
What is an SSL Certificate?
SSL Certificate Types
Why Use TLS 1.3?
What is SNI?
What is Encrypted SNI?
What is Domain Spoofing?

Learning Center Navigation
Learning Center Home
DDoS Learning Center
CDN Learning Center
DNS Learning Center
Performance Learning Center
Security Learning Center
Serverless Learning Center
Bots Learning Center
Cloud Learning Center
Access Management Learning Center
Network Layer Learning Center
Privacy Learning Center
Video Streaming Learning Center