IdenTrust™
part of HID Global

Applying for a TLS/SSL Certificate

During the application process, an applicant can choose the number of domain names to include in the IdenTrust TLS/SSL | Organization Identity | Organization Validated (OV), or IdenTrust TLS/SSL | Organization Identity | Extended Validated (EV) certificate. By default, the basic price of an IdenTrust TLS/SSL certificate allows up to two domains. Up to 48 more domains can be added to the certificate for an additional fee per added domain. Additional domain names may be included during the initial certificate application, or via the Certificate Management Center (CMC) after the TLS/SSL certificate issuance.

- Single Domain: A single domain TLS/SSL certificate establishes a secure connection between a browser and a server. With TLS/SSL certificates the communication is encrypted, assuring visitors that their information is secure and private. These certificates also authenticate an organization's identity. This is confirmed by the visual appearance of a padlock next to the web address in the browser.
- Multi-Domain: Also known as multi-SANs, these certificates are ideal to secure multiple names across different domains and sub-domains, and offer complete control over the Subject Alternative Name (SAN) field. A multi-domain certificate will allow you to secure domains such as: www.identrust.com, www.identrust1.com, www.identrust2.net, www.sales.identrust.com, and www.dev.identrust1.net.

To apply for a single or Multi-Domain IdenTrust TLS/SSL certificate, select BUY NOW on the TLS/SSL Certificate Types webpage and follow the certificate selection wizard options; in the certificate application page, type in the desired Fully Qualified Domain Name(s) (FQDN) or paste a Certificate Signed Request (CSR). The system automatically will determine the certificate type you have selected, as well as the appropriate pricing.

- Wildcard: IdenTrust TLS/SSL | Organization Identity | Organization Validated (OV), or IdenTrust TLS/SSL | Organization Identity | Extended Validated (EV) certificates can support TLS/SSL Wildcard usage. In order to issue a Wildcard certificate, IdenTrust will perform authentication processes to confirm that the requesting organization has full control of the entire domain namespace. A Wildcard certificate includes an asterisk that is correctly positioned in the FQDN and will cover all sub-domain names associated with that domain.

  *Wildcard TLS/SSL certificates are available under our Software-As-A-Service model only. Please contact Sales@IdenTrust.com for more information.

Additional Program Information

- ECA | Medium Assurance | TLS/SSL | Organization Validated (OV)
- IdenTrust TLS/SSL | Organization Identity | Extended Validated (EV)
- IdenTrust TLS/SSL | Organization Identity | Organization Validated (OV)
- FATCA Organization | Organization Identity | Software Storage

2022-05-17-apply-tls-ssl-sin-mul-wil