# Symantec™ SSL Certificate Wildcard Option

**Datasheet: SSL Certificate Wildcard Option**

## Secure Multiple Subdomains with One Certificate

Symantec SSL Certificate Wildcard option provides encryption and authentication for multiple subdomains on a single server. As an example, *.qa.yourbusiness.com could be used to protect test1.qa.yourbusiness.com, test2.qa.yourbusiness.com, etc. Compared to purchasing and deploying individual certificates for each subdomain in use, Symantec SSL Certificate Wildcard option is a flexible and efficient way to extend SSL protection to multiple subdomains. And with Managed PKI for SSL, you can deploy Symantec Premium or Standard SSL Certificate with Wildcard and Subject Alternative Name (SAN) option on the same certificate.

There are several best practice deployments of Symantec SSL Certificate Wildcard option:

- **Secure multiple subdomains starting from several levels down from the top level domain, example, sublevel three or four.**
  This best practice deployment offers the convenience of securing multiple domains with one certificate while minimizing the risks of security breach at the top level domain cascading to all subdomains below that.
- **Secure multiple domains with domain names that are frequently changing**
  In some industries, enterprises have domains to meet seasonal or temporal requirements. Enterprises will be able to secure these domains easily with the wildcard option without incurring extensive time and labor in SSL certificate lifecycle management.
- **Secure large number of subdomains (extremely large SANs)**
  Some browsers have limits on the number of SANs that could be used to secure the system. Users may experience issues when they try to access the site. Under these circumstances, enterprises would have to use the wildcard option to secure the large number of subdomains.
- **Secure multiple different domains**
  Enterprises with multiple subsidiaries or different brands and identities may require protection on different domains, for example, *.qa.enterprise.yourbusiness.com and *.qa.enterprise.acquiredbusiness.com. A Symantec Premium or Standard SSL Certificate with Wildcard and SAN options provides the capability to streamline and secure these domains under one SSL certificate.
- **Secure the base subdomain**
  Enterprises with international organizations may require to protect the base subdomain, for example, *.qa.enterprise.yourbusiness.com and qa.enterprise.yourbusiness.com. Similarly, a Symantec Premium or Standard SSL Certificate with Wildcard and SAN options provides the capability to conveniently secure these domains under one SSL certificate.

### Key Benefits

- Lower administrative costs by managing less SSL certificates
- Simplify certificate installation and management by securing up to five subdomains with a single domain name
- Deploy SSL immediately to new or unprotected subdomains without delays in issuance, and provide valuable future-proofing
- Increase efficiency by securing base subdomain and different domains with one SSL certificate
- Fulfill administration needs of feature-rich environments that require secure client-server and server-server communications, beyond or behind the firewall
- Assure users and increase trust by demonstrating full authentication of the organization identified in the certificate
- Minimize compatibility issues with Symantec roots having nearly 100% root ubiquity in browsers and wide-reaching mobile browser support
- Facilitate quick responses with award-winning support for issue resolution
- Accommodate SSL wildcard requirements for web-based applications (Symantec O3, OpenSocial, etc.)

Symantec™

Norton™ SECURED
powered by VeriSign

The wildcard option is available on all Symantec SSL Certificates except for Symantec SSL Certificates with Extended Validation (EV). Symantec SSL Certificate with Wildcard option may not work on some older browsers, mobile and client-based applications. In these situations, Server-gated Cryptography (SGC) certificates could be used for maximum amount of coverage or compatibility.

Symantec SSL certificate with Wildcard is one of several options available for Enterprise to secure their website. Best practice deployments with other Symantec SSL certificate options include:

- EV SSL certificates to secure pages with login, passwords, Personally Identifiable Information (PII), and ecommerce fixtures such as shopping carts, checkout and payment. EV SSL certificates come with the strongest encryption available – up to 256 bit – to protect sensitive transactions and provide powerful visual cue of confidence to users via the green URL address bar. EV SSL certificates are available with Symantec Premium SSL Certificates or Symantec Secure Site Pro SSL Certificates.
- Subject Alternative Name (SAN) option to secure multiple top level domains such as www.symantec.com, www.symantec.co.uk. Enterprises can leverage the convenience of securing multiple domains on a single certificate while deploying strong encryption that comes with EV SSL certificates to secure mission-critical domains.

## Learn More

To learn more, contact a Symantec Sales Representative, call 650-426-5115, or send an email to SSL_EnterpriseSales_NA@symantec.com.

## More information

Visit our website

http://go.symantec.com/managed-pki-for-ssl

To speak with a Product Specialist in the U.S.

Call 1 (866) 893-6565 or 1 (650) 426-5112

To speak with a Product Specialist outside the U.S.

For specific country offices and contact numbers, please visit our website.

About Symantec

Symantec is a global leader in providing security, storage, and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

Symantec Corporation World Headquarters
350 Ellis Street
Mountain View, CA 94043 USA
1 (866) 893 6565
www.symantec.com

Symantec™

Norton™ SECURED
powered by VeriSign



UID: 135/11/12