Securing Multiple Domains with SAN/UCC

How to Simplify Your Site Security and Save Money
Securing your site is now about more than simply protecting your current customers’ information—it’s about getting visitors to trust your site as soon as possible. That’s because consumers will soon have an easier way to tell how secure your site is before they even think about buying or logging in.

Many browsers are beginning to flag non-secure sites that accept credit cards or use passwords. This is just the first step in a series of changes that will eventually include additional negative visual indicators that will mark unencrypted websites so that they stand out to consumers. For example, in Google Chrome, the company will add the words “Not Secure” and an exclamation point icon next to the web address on any unencrypted site.

These changes make deploying the right kind of encryption and validation paramount for websites that want to stay secure and thrive. In this guide, you’ll learn how multiple domain certificates work, how to select the right multi-domain certificate for your needs and some typical situations where multiple domain certificates are ideal.

Securing Multiple Domains

As the backbone of website security, Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), both historically referred to as “SSL,” are a must. SSL is simple when you have only one domain name/URL for your site, but what if you have more than one domain directing to your site? Keeping those multiple domains securely encrypted can become overly complex, but it must be done. So how do you make it easier to manage without it costing you more?

Typically, one SSL/TLS certificate secures a single domain name or URL. But there are some common situations where having a certificate that allows you to secure multiple domains with one certificate is the best choice. There are two ways to secure multiple domains. The first is through SAN (Subject Alternative Name), also known as UCC (Unified Communications Certificates). SAN/UCC can secure totally different domains on one certificate. The second is through wildcard certificates. Wildcard secures unlimited subdomains. SAN/UCC can also be added to a wildcard certificate, further extending the certificate functionality.

Depending on your organization’s needs, a multiple domain certificate can save you considerable time and money compared to buying and managing many individual certificates for each domain name you own.

Benefits of Using SAN

- Lowers administrative and deployment costs by allowing up to 100 SANs with a single certificate in Symantec Managed PKI for SSL, up to 100 SANs in Symantec Trust Center Enterprise Account and up to 24 SANs in Symantec Trust Center.
- Reduces complexity in certificate installation and management by providing single-certificate support of any combination of domain names (even at different subdomain levels), local host names and internal IP addresses.
- Maximizes flexibility by securing web, SMTP, POP/IMAP and other unified communications (UC) servers, including Microsoft Exchange Server, Lync Server, Office Communications Server or Mobile Device Manager Environments.
- Fulfills administration needs of feature-rich environments that require secure client-server and server-server communications.
- Meets UC certificate compliance requirements for Microsoft Exchange and Communications Server.
- Reduces risk by using specific hostnames for SSL authentication.
- Increases value by incorporating the highest standards in SSL technology and issuance: a minimum of full organization authentication, up to 256-bit session encryption, nearly 100% root ubiquity in browsers and wide-reaching mobile browser support.
Do You Need a Multi-Domain Certificate?
SAN stands for Subject Alternative Name certificates and allows you to secure multiple domain names with a single SSL certificate. Regardless of how easy it is to obtain a single SSL/TLS certificate, securing multiple domains with multiple, single certificates can quickly become expensive and cumbersome.

SAN works well for businesses that operate multiple websites or multiple brands. For example, a clothing store, operating separate sites for each brand, perhaps one for women’s, men’s and children’s apparel, may hold multiple domains, one for each section of the business. In this case, all three clothing websites can be secured under one SAN without buying three separate SSL/TLS certificates.

Here are some additional common situations where multi-domain SAN certificates are often more practical and cost-effective:

- **Microsoft Exchange Server (Unified Communications):** Often referred to as Unified Communications (UC) certificates, SAN certificates were primarily designed to support real-time communications infrastructures. Our SAN certificates are recognized by Microsoft for compliance with UC usage and are perfect for securing multiple domains in Microsoft Exchange/Lync Server, Office Communications Server or Mobile Device Manager Environments.

- **Federating two or more Unified Communications platforms:** When a company uses more than one UC platform—for example, Google Apps and Microsoft Office Communications Server—those systems will need to be federated to allow employees to collaborate with their colleagues across platforms. This scenario is fairly common, and SSL/TLS certificates are necessary to validate cross UC platform server-to-server connections.

- **Multiple domain names:** Sometimes you may have multiple domain names that all point to one site; for instance you have one URL with your full company name and another with the acronym for your company. Perhaps you have different top-level domains for your company website like .com, .net or .org, or maybe your company is present in several different countries and you have country-specific URLs (.uk, .de, .au, etc.) all pointing to your main site. A multi-domain certificate lets you secure your main site as well as all the other domain names with one certificate.

How Does a Multi-Domain Certificate Work?
The multi-domain certificate is just like a regular SSL/TLS certificate in nearly every way. You can get domain, organization or extended validation, it offers the same level of encryption, and the encryption technology works the same way too.

The difference is the Subject Alternative Name (SAN) extension. With a multi-domain certificate, you can specify a list of domains to be protected by a single SSL/TLS certificate. Nearly every browser and mobile device understands how to use this functionality, so the encryption works across devices and browsers.

To see this process in action, click the padlock in your browser on an “https” page to examine the SSL/TLS certificate. In the details tab, the “Subject Alternative Names” field lists the multiple names for that certificate (see Figure 2).
Selecting the Right Multi-Domain Certificate

While SSL/TLS is standardized, there are differences between SSL/TLS providers and the certificates they offer. Here are some important criteria you should keep in mind when shopping for a multi-domain certificate:

- **Reputation:** Choose an SSL/TLS certificate from a reputable security company. This is especially important for e-commerce or B2B sites where customers and partners look at who supplies your SSL/TLS for a sense of confidence that you're protecting their sensitive information.

- **Convenience:** Find out how easy it is to add, change or delete domain names. Look for self-service features that let you maintain the certificate yourself so that you don't have to call the vendor or submit a service or support request for each change.

- **Number of domain names:** While it's important that the certificate you choose can support all the domains you need to secure, don't be misled into buying more than you need.

### Which Kind of Validation Is Best for You?

The other factor you'll want to consider before you select a multi-domain certificate is whether an extended validation (EV) certificate would be the best choice instead of an organization-validated certificate. If you will be securing publicly facing webpages, an EV certificate may be the way to go.

Multi-domain certificates with EV offer the most rigorous business verification process available. If your business depends on the web and collects user information, an EV certificate is the better choice. Make it even easier for customers to feel confident that your site is secure.

Securing Multiple Domains with Symantec Security Center

As a leading SSL/TLS provider with a strong, credible reputation for security, Symantec offers SSL/TLS certificates that are ideal for situations that call for a multi-domain SSL/TLS solution. Simply install the certificate on an unlimited number of servers, all at no additional cost.

Symantec multi-domain certificates are fully compatible with the latest UC platforms, making them an easy-to-use, cost-effective solution for any UC environment.

Symantec also allows you to add SANs to your extended validation certificates. SAN will help you send a clear message to visitors that your website is safe, making it a vital security component that can instill trust in your visitors.

### SAN/UCC can save you time and money compared to buying and managing individual certificates for each domain you own.

In addition, Symantec provides an online management portal that you can use to add, edit or delete SAN names and then reissue your certificate whenever you need to, a feature that simplifies and significantly reduces the burden of managing your UC security.

Look for self-service features that let you maintain the certificate.

Symantec Website Security.
Security Made Simpler
SAN makes it possible to secure multiple domain names, internal servers, and IP addresses with one SSL/TLS certificate. Multi-domain or UC certificates can be a cost-effective and time-saving alternative to individual SSL/TLS certificates.

Symantec certificates with additional SAN fields combine affordability, convenience, and reliability—everything you need to effectively secure multiple domain names, your Exchange environment, and other internal servers. Available in organization or extended validation, Symantec certificates give you the features and flexibility you need to manage all of your domain names at an affordable cost.

Why Symantec?

- **Reputation:** When you choose Symantec, your site displays the Norton Secured Seal—the most recognized trust mark on the web, giving visitors confidence in your business and your site. Symantec displays over 1 billion trust seals daily.

- **Trusted:** Symantec secures the world’s top companies, including more than 90 percent of the Fortune 500, and is a long-standing, reputable market leader.²

- **Encryption:** Symantec offers superior encryption that’s 64,000 times stronger than industry standard (RSA) certificates, with daily malware scans, vulnerability assessments, warranty protection, and SSL Assist Plus.³

- **Automation:** Symantec simplifies the process of managing your website’s security and certificates. No more spreadsheets, which are prone to error and could lead to security gaps.

- **Authentication:** Multi-layered security makes our certificate issuance and authentication processes the most rigorous in the industry.⁴

- **Protection:** Cloud WAF protects applications beyond the data center, without sacrificing performance, and our Code Signing Service is the only code signing service that protects and monitors your signing keys for malware.

- **Flexible:** Take advantage of flexible licensing options with a start anywhere/right for you approach.

- **Support:** We are present 24 hours a day, 7 days a week. Symantec continues to earn near-perfect scores for our customer service worldwide.⁴

- **Corporate responsibility:** Our Corporate Responsibility Team works to identify and refuse certificates to hate groups and other rogue organizations.

---

2. Internal customer analysis, October 2015 against Fortune 500 2015 list.
5. Based on Forbes Global 2000 list published in 2015 and internal customer analysis conducted in October 2015.
For global offices and contact numbers, please visit our website.

For product information in the U.S., call:
1-866-893-6565 or 1-520-477-3111

Symantec World Headquarters
350 Ellis Street
Mountain View, CA 94043 USA
1-866-893-6565
www.symantec.com/ssl

For product information in Asia Pacific, call:
Australia: +61 3 9674 5500
New Zealand: +64 9 9127 201
Singapore: +65 6622 1638
Hong Kong: +852 30 114 683

Symantec Website Security Solutions Pty Ltd
3/437 St Kilda Road, Melbourne, 3004
ABN: 88 088 021 603
www.symantec.com/en/aa/ssl-certificates

For product information in the Americas (Non-U.S.), call:
Mexico: 554 738 0448
Brazil: 800 038 0598

For product information in the U.K., call:
0800 032 2101 or +44 (0) 208 6000 740

Symantec (UK) Limited
350 Brook Drive
Green Park, Reading
Berkshire, RG2 6UH UK
www.symantec.co.uk/ssl

For product information in Europe, call:
+353 1 793 9053 or +41 (0) 26 429 7929
Germany: 0800 128 1000
France: 0800 90 43 51
Spain: 900 93 1298

Follow Us: