BUSINESS GUIDE: SECURING
MICROSOFT EXCHANGE 2010 WITH
SYMANTEC™ SSL CERTIFICATES

Symantec Business Guide

Securing Microsoft Exchange 2010 with Symantec™ SSL Certificates

Best Practices for Securing Your Email Server with SSL Certificates and Subject Alternative Names

Securing Microsoft Exchange 2010 with Symantec™ SSL Certificates

Best Practices for Securing Your Email Server with SSL Certificates
and Subject Alternative Names

CONTENTS

Introduction: SSL is a Must-Have for Secure Communications

There are many reasons why now is the right time to make the move to Microsoft Exchange Server 2010, including a host of administration and security improvements. However, as with Exchange Server 2007, Exchange Server 2010 requires SSL certificates to ensure the security of all connections to the email server. This guide from Symantec™ will help you take the guesswork out of implementing SSL for Exchange 2010, making it easier than ever to get the SSL certificate you need for a successful and secure Exchange implementation, and to take advantage of powerful capabilities such as Subject Alternative Names (SANs).

How SSL Secures Exchange 2010 Communications

While most people know that SSL secures e-commerce transactions, SSL is also a cornerstone for securing many communication technologies, including email, instant messaging (IM), and voice-over-IP (VOIP). SSL is used to both authenticate your Exchange server and service as legitimately yours, and to trigger an encrypted session each time a user connects to your Exchange environment. When you request an SSL certificate, a third-party, such as Symantec, verifies your organization's information and issues a unique certificate to you, incorporating that information. This is known as the authentication process.

Secure Sockets Layer (SSL) technology protects your online transactions and helps increase trust in your website in three essential ways:

1. An SSL certificate enables **encryption** of sensitive information during online transactions.
2. Each SSL certificate is a unique **credential** identifying the certificate owner.
3. A Certificate Authority **authenticates** the indentity of the certificate owner before it is issued.

Once your server has been authenticated, a secure SSL connection is established, and encrypted data can be shared between the email or Web client and your Exchange server, ensuring the confidentiality and integrity of all communications.

Choosing the Right Type of SSL Certificates for Exchange 2010

There are three types of SSL certificates you can use to secure your Exchange infrastructure: self-signed that you create yourself; Windows Public Key Infrastructure (PKI) certificates; and certificates from trusted independent Certificate Authorities (CA) (sometimes referred to as Public Certificates). Microsoft recommends that you use an SSL certificate from a trusted, independent third-party CA before putting a new email server into production. If you use a certificate from a well-established CA, you can avoid the hassles of installing your own root certificate on every client that will access your Exchange server. (Your help desk will thank you for this, since they will be fielding configuration requests every time a new mobile or browser client tries to connect). Additionally, be aware that the Outlook Anywhere protocol will not work with a self-signed SSL certificate.

Naming Your Exchange Servers

Before you purchase and install your SSL certificates, you must identify the fully qualified domain name (FQDN, sometimes referred to as the URL) for your server, and add this name to the Trusted Server list in Active Directory. Your FQDN would look something like this:

mail.yourserver.com

You will need more than a single FQDN for your server. Your server will likely be responsible for multiple services, and you will need to identify every possible domain name that may be used by another server or client when pointing to your Exchange server. There are a few instances where you must use the FQDN as the common name – such as when you secure an Edge Transport server that performs simple mail transfer protocol SSL (SMTPS) over the Internet. In this case, you must use the same FQDN as is published in that server's "A" record on the public Internet DNS server. If using the FQDN is not possible or not desired, many administrators use the shorter domain name form of the FQDN for their common names.

Here is a sample set of common names that might be associated with a single Exchange server:

mail.yourserver.com
owa.yourserver.com
autodiscover.yourserver.com
outlook.yourserver.com

You will need to secure and authenticate each of your common names with SSL because any device needing to point to your server will need to use exactly these same names. Many IT professionals have dealt with problem scenarios where their Exchange implementation wasn't working due to misunderstandings about the server common name. Creating a solid naming schema for your Exchange 2010 environment will help you to avoid many major problems down the road.

Using FQDN Common Names

Keeping your Exchange 2010 common names in FQDN format is a good idea, but be aware that there are a few limitations. Common names can be no longer than 64 characters, and if your FQDN naming schema runs long, you will not be able to fit your full FQDN into the common name standard. Common names support Unicode, whereas an FQDN is limited to a subset of ASCII characters. That said, if you can use your FQDN as your common name, it may make your ultimate configuration easier.

Simplifying Security with Subject Alternative Names

Each of your common names needs to be authenticated by SSL, but it would be unnecessarily cumbersome and costly if you actually had to purchase and install a separate SSL certificate for each of your common names. Don't worry – there is a much easier method.

The solution to securing multiple common names for a single server, such as is necessary for an Exchange server, is getting a certificate with multiple SANs (subject alternative names). The SAN field extension in an SSL certificate has been part of the SSL certificate standard for more than a decade. This SAN-enabled certificate works just like a regular SSL certificate in nearly every way. It offers the same level of encryption and authentication; the only difference is that it protects multiple common names with a single SSL certificate. The SAN field extension is very flexible and works with virtually all browsers and mobile devices. By using the

SAN field extension, you can use a single certificate to protect different domains, IP addresses, server names and of course, Exchange 2010 domain names.

Purchasing Your SSL Certificates: Choosing the Right Certificate Authority

Once you have all your SAN names mapped out, you are ready to purchase your SSL certificate. Selecting a reliable and credible SSL provider is of the utmost importance. As the leading CA. Symantec sets the standard for online security and trust.

Browser root ubiquity is an important requirement when deciding on a CA for your SSL certificates. Many CAs claim to offer "99 percent browser ubiquity," but this claim does not mean that every certificate will activate without triggering a security warning in a browser. Newer or smaller CAs may not have had their roots included in the root store for some browsers. This is especially an issue for older browsers. Symantec SSL does not have this issue. Virtually every browser manufacturer adds Symantec SSL roots to their root store when new versions of that browser are released.

Managing Multiple Certificates

Managing enrollment, issuance, and renewals of certificates one-by-one is tedious and time-consuming, but an enterprise-class solution can make things simpler by centralizing management, purchasing, and backup of all SSL certificates.

Symantec offers different levels of control, depending on your organizational needs. With Symantec Trust Center Enterprise Account, you can pre-approve domain, organizational and contact information to streamline issuance. With Symantec Managed PKI for SSL, you get the same functionality, plus Symantec authenticates the primary administrator who pre-purchases Symantec™ SSL Certificates for instant issuance. Administrators can be assigned organizations, roles and privileges to manage security, account configuration, or certificates.

SAN SSL Certificates for Unified Communications

A SAN SSL certificate, sometimes referred to as a Unified Communications Certificate (UC Certificate or just UCC), is not typically issued as a separate specialized product. Ideally, you should be able to select the SSL certificate with the level of authentication and encryption that you need and then specify the additional names you need to secure with that certificate.

Buying a SAN certificate is easy, but it is important to know how many SANs you will need for that certificate prior to your purchase. With some CAs, you can edit your existing SANs if you ever need to change a name. If you do edit your SANs, you will need to revoke and reissue your certificate and reinstall it in order for those changes to be realized by your server.

Not all SSL providers allow you to revoke and reissue their certificates for free so make sure you choose a brand that does this. Some CAs offer only one type of SAN certificate, but with Symantec, you can add SANs to Symantec Secure Site, Symantec Secure Site Pro, Symantec Secure Site with EV, or Symantec Secure Site Pro with EV. You'll pay the original certificate price plus a fee for each additional SAN.

Using the New Microsoft Exchange Certificate Wizard

Setting up domain names for your Exchange Server 2010 is potentially simpler than ever with the new Exchange Certificate wizard. Its new graphical user interface acts as an alternative to the Exchange Power Shell. The Exchange Configuration option will set up a standard server configuration to be used when ordering an SSL certificate.

This is a convenient option, but double-check the default configuration options against your actual deployment – you don't want to order the wrong SANs for your SSL certificate because your naming is not the same as the default Exchange configuration.

SANs vs. Wildcard Certificates

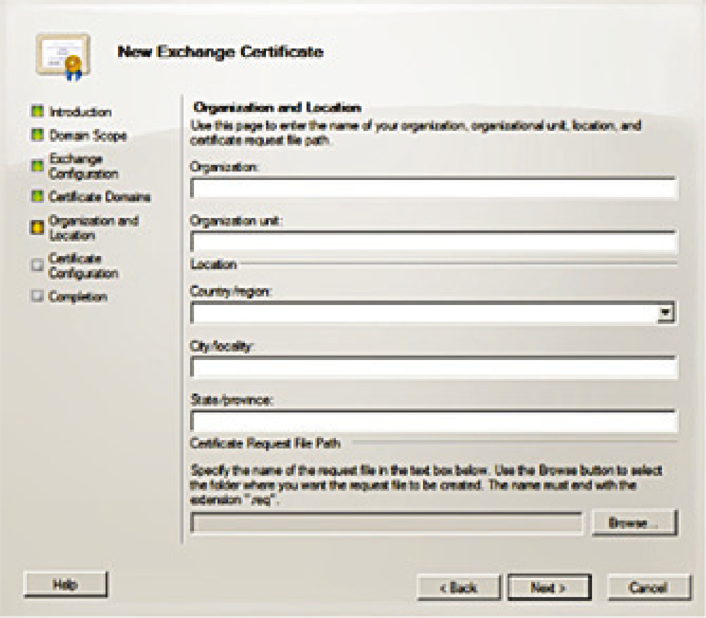
Wildcard certificates are different than SAN certificates. Wildcard certificates can protect an unlimited number of subdomains.

For instance, a wildcard certificate for "*.yourserver.com" secures sub-domains such as info. yours- erver.com and shop. yourserver.com. However, wildcards are also limited because they must share the same domain and the same number of levels, and you cannot secure the Exchange 2010 autodiscover ser- vice with a wildcard SSL certificate.

Generating a CSR with the Exchange Certificate Wizard

To enroll for your SSL certificate, you will need to generate a certificate signing request (CSR). Fortunately, Exchange 2010 comes with a certificate wizard that simplifies this process. Here are seven easy steps you can follow to generate your own CSR:

1. Open the Exchange Management Console by going to Start > Programs > Microsoft Exchange 2010 > Exchange Management Console. Select “Manage Databases” for your server.
2. Select “Server Configuration” in the left menu, and then “New Exchange Certificate” from the Actions pane on the right. When prompted for a friendly name, enter a name by which you can easily remember and identify this certificate. This name is used for identification only and does not form part of the CSR.
3. Under Domain Scope, you can check the box if you will be generating the CSR for a wildcard. Otherwise, just select next.
4. In the Exchange Configuration menu, Select the services that will be secured, and Enter the names through which you connect to those services, when prompted. If you selected a wildcard, skip this step. At the next screen, you will be able to review a list of the names that Exchange 2010 suggests you include in your certificate request.
5. On the Organization and Location page, your “Organization” should be the full legal name of your company as officially registered, and your “Organization Unit” is your department within the organization responsible for SSL. If you do not have a state/province, enter the city/locality information.



New Exchange Certificate

Organization and Location

Use this page to enter the name of your organization, organizational unit, location, and certificate request file path.

Specify the name of the request file in the text box below. Use the Browse button to select the folder where you want the request file to be created. The name must end with the extension ".req".

6. Click Browse to save the CSR to your computer as a .req file, then click Save, then Next, then New, and then Finish.

You will now be able to open the CSR with a text editor such as Notepad. Copy everything from the first dash (-) of the BEGIN line right through to the last dash of the END line. Paste it into the online order form.

NOTE: Exchange 2010 uses an RSA key length of 1024-bits by default, but we strongly recommend the use of a 2048-bit key. If you are creating a CSR for an Extended Validation Certificate or a certificate with a validity period beyond December 31, 2013, you must select a 2048-bit key length.

Installing Your SSL Certificate

Once you have purchased your Symantec SSL Certificate, you will receive an email that contains encoded data between the header and footer that look like the following. This is your SSL certificate.

```
-----BEGIN CERTIFICATE-----
[encoded data]
-----END CERTIFICATE-----
```

Use Notepad or another plain-text editor to create a file with the certificate content in the email. Make sure there are five (5) dashes to either side of the BEGIN CERTIFICATE and END CERTIFICATE and that no white space, extra line breaks or additional characters have been inadvertently added. Save the file with the extension of .txt or .p7b. Then, follow these six easy steps to install your Symantec SSL Certificate:

1. Start the Exchange Management Console: Start > Programs > Microsoft Exchange 2010 > Exchange Management Console.
2. Select “Manage Databases” for your server, and then select “Server configuration.” Select the certificate from the center menu (listed by its Friendly Name), and then select “Complete Pending Request” from the “Actions” pane.
3. Browse to the certificate file, then select Open > Complete.
4. Press the F5 key to refresh the certificate and verify that it now says “False” under “Self Signed”. If it still shows “True”, the wrong certificate may have been selected or the request may have been generated on a different server To resolve this issue, create a new CSR on this Exchange server and have the certificate reissued by your CA.
5. To enable the certificate, go back to the Exchange Management Console and click the link to “Assign Services to Certificate”. Select the server from the list provided, then click Next.
6. Select the services for which the certificate must be enabled, then click Next > Assign > Finish.

Your Symantec SSL Certificate should now be installed and enabled for use with your Exchange 2010 server.

Note On Base64 Encoding

Occasionally, Exchange 2010 will show an error message stating that “The source data is corrupted or not properly Base64 encoded.” Typically you can ignore that error even though it occurs, the certificate often still installs correctly.

Get Started with Your SSL Certificate

SSL brings trust to the Internet. Billions of times each day, and Symantec is here to help companies and consumers all over the world to engage in trusted communications and commerce. When your company protects the confidentiality and integrity of sensitive information with SSL certificates from Symantec, your business benefits and so does your reputation. Here are a few of the reasons why you should use Symantec SSL Certificates to protect your Microsoft Exchange 2010 environment:

- Free 24/7 technical support in multiple languages, including chat, email and phone support, along with an online knowledge base
- Scalable management with a single, Web-based portal that helps to reduce the cost and complexity of managing SSL certificates across your organization
- Express renewal and auto-pay renewal service to completely automate the renewal process so you don't have to generate a new CSR or reinstall your certificate for up to six years
- A robust PKI infrastructure that includes military-grade data centers and disaster recovery sites for unsurpassed customer data protection, availability and peace of mind
- Rigorous authentication practices, audited annually by KPMG, that lead the industry to establish an online business' credibility
- Cutting-edge technology made possible by Symantec's continuous investments in research and infrastructure to stay well ahead of evolving security risks

Learn More about SAN Certificates

Subject alternative name (SAN) is an optional feature used for Unified Communications (UC) to secure Microsoft Exchange 2007 Server, Office Communications Server 2007 or Mobile Device Manager as well as server names, intranet and local names. This capability is offered with any Symantec SSL Certificate so you can choose the certificate that fits your business. With Symantec SAN Certificates, you can secure up to twenty-four additional domain names by adding them to the SAN field during enrollment.

To learn more, visit http://go.symantec.com/ssl-certificates.

More Information

Visit our website

http://go.symantec.com/ssl-certificates

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