securing microsoft exchange 2010

WITH THAWTE SSL CERTIFICATES

thawte®

strong ssl = 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 Microsoft Exchange Server 2007, Exchange 2010 requires SSL certificates to ensure the security of all connections to the email server. This guide from Thawte is designed to 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).

WHAT IS AN SSL CERTIFICATE?

An SSL certificate is a bit of code that provides security for online communications. When a web browser contacts your secured web site or application server, they use the SSL certificate to enable an encrypted connection. It's kind of like sealing a letter in an envelope before sending it through the mail. SSL certificates also inspire trust because each SSL certificate contains identification information. When you request an SSL certificate, a third party (such as Thawte) verifies your organization's information and issues a unique certificate to you incorporating that information. This is known as the *authentication process*.

CHOOSING THE RIGHT TYPE OF SSL CERTIFICATE 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 (sometimes referred to as Public Certificates). Microsoft recommends that you use an SSL certificate from a trusted, independent third-party certification authority (CA) before putting a new email server into production[1]. 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)[2]. Also be aware that the Outlook Anywhere protocol will not work with self-signed 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 or common name) 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 name that may be used by another server or client when pointing to your Exchange server. Keeping your Exchange 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.

1. Microsoft TechNet; Understanding Digital Certificates and SSL; http://technet.microsoft.com/en-us/library/dd351044.aspx

2. Patricio, Anderson; Managing Certificates in Exchange Server 2010; http://www.msexchange.org/articles_tutorials/exchange-server-2010/management-administration/managing-certificates-exchange-server-2010-part1.html [April 7, 2001]

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 environment will help you to avoid many major problems down the road.

FEWER HEADACHES 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 more – perfect for securing your Exchange server.

BEST PRACTICES FOR SANS

Use the "Certificate Principal Name" configured for your Outlook Anywhere connection in the Outlook profile as the Subject Name in your SSL certificate. Include the fully qualified Internet domain name (FQDN) for your server as a common name in your certificate. Also note that the autodiscover service (if you use it) must be listed as a SAN – autodiscover.yourserver.com. All the common names for the various services you use with your Exchange implementation must be listed in your SAN. The most typical services used are Outlook Web App (OWA), ActiveSync, and Outlook Anywhere. If you have deployed one or more Client Access Servers (CAS) you will also need to include all those FQDNs in your SAN list.

WILDCARD CERTIFICATES

Wildcard certificates are different than SAN certificates. Wildcard certificates can protect an unlimited number of subdomains. For instance, a wildcard certificate for *.yourdomain.com, secures sub-domains such as info.yourdomain.com and shop.yourdomain.com. However, wildcards are also limited because they must share the same domain and the same number of levels. In addition, you cannot secure the Exchange autodiscover service with a wildcard SSL certificate.

USING THE NEW EXCHANGE SERVER 2010 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 designed 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.

Purchasing Your SSL Certificate

Once you have all your SAN names mapped out, you are ready to move on to purchasing your SSL certificate. Buying SAN certificates is easy, It is important to know how many SANs you will need for that certificate before you purchase it. 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 reissue your certificate and reinstall it in order for those changes to be realized by your server. Not all SSL providers offer free unlimited reissues for their certificates so make sure you choose a brand that does this, such as Thawte.

Choose a reliable and credible SSL provider, you want one whose roots are ubiquitous, providing immediate support of the maximum number of browsers and servers. Making sure your CA's SSL roots are everywhere you need them to be is not something that you should be spending your valuable time on. If you have multiple certificates, you should probably consider purchasing an enterprise-class SSL certificate. These certificates typically come with robust management consoles that will help you track all your certificates in one place, help you avoid outages due to surprise expirations and may include robust reporting to help you forecast for future SSL certificate requirements.

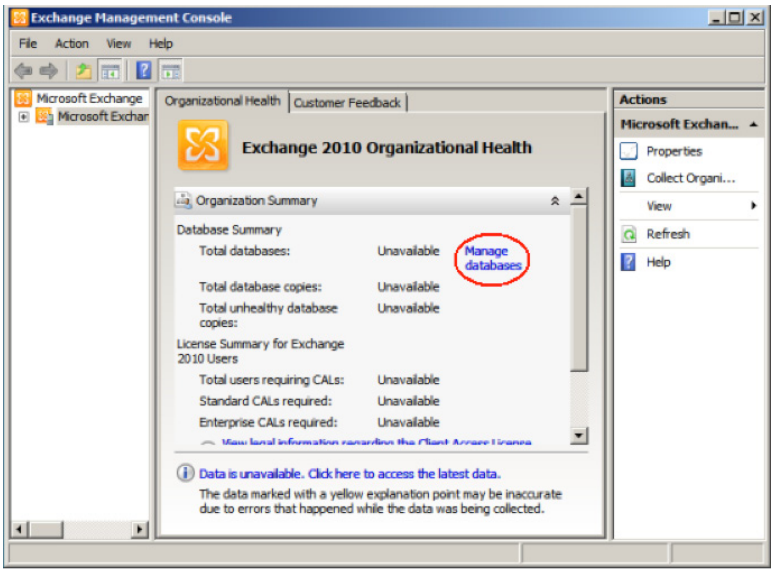
SAN SSL PURCHASE OPTIONS

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 that you need and then specify the additional names you need to secure with that certificate. Some CAs only offer one type of UC certificate, but with Thawte you do not have this limitation. You can add SANs to Thawte SGC SuperCerts, Thawte SSL Web Server certificates, or Thawte SSL Web Server certificates with EV. You'll end up paying the original certificate price plus a fee for enabling SANs to secure additional domain names.

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 six 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" as shown in the screenshot on the next page.

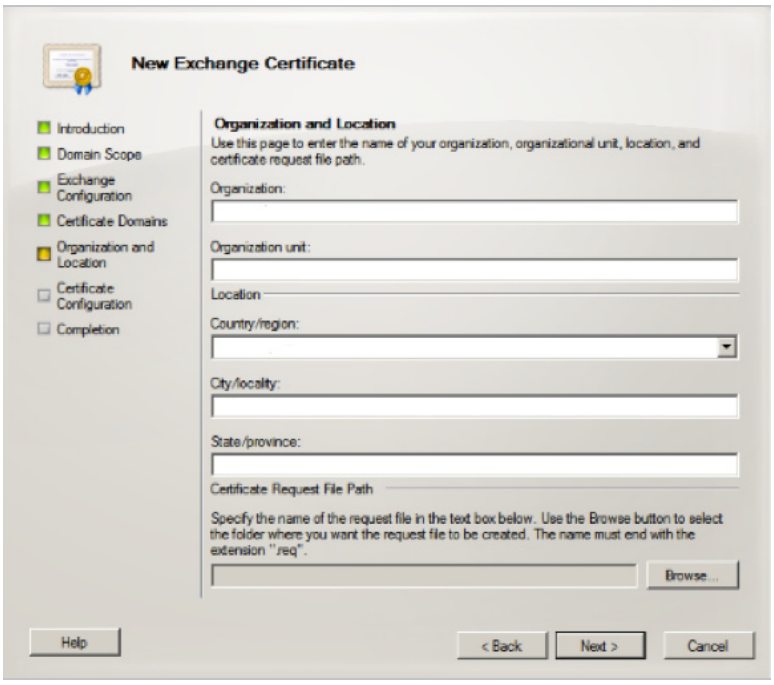


2. Select “Server Configuration” in the left menu, and then “New Exchange Certificate” from the actions menu on the right. When prompted for a friendly name, Enter a name by which you can easily remember and identify this certificate. This name is used for identification only and does not form part of 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.

5. 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. 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.



6. Click Browse to save the CSR as a .req file, then 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 Thawte strongly recommends 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 Thawte SSL Certificate

If you have purchased your SSL certificate from Thawte, you will receive an email that contains your SSL certificate. The email will contain encoded data between and header and footer that look like the text below. This is your SSL certificate.

-----BEGIN CERTIFICATE-----

[encoded data]

-----END CERTIFICATE-----

Use Notepad or another plaintext editor to create a file with the certificate content of 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 Thawte SSL certificate:

1. Start the Exchange Management Console: Start > Programs > Microsoft Exchange 2010 > Exchange Management Console.

2. Select “Manage Databases”, 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” menu.

3. Browse to the certificate file, then select Open > Complete

Note: 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.

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.

Congratulations! Your Thawte SSL certificate should now be installed and enabled for use with your Microsoft Exchange 2010 Server environment.

get started today with ssl

Thawte SSL Certificates for Exchange 2010

With Thawte as your online trust provider, customers will feel secure doing business with you over the internet. Expert multilingual support, robust authentication practices, and easy online management make Thawte the best value for SSL certificates and code signing certificates. Thawte SGC SuperCerts, Thawte SSL Web Server certificates and Thawte SSL Web Server certificates with EV can be enabled for SANs and are appropriate for use with Exchange 2010.

THAWTE SUBJECT ALTERNATIVE NAME (SAN) CERTIFICATES

Thawte Subject Alternative Name (SAN) certificates are powerful tools that you can use to secure multiple domain names, inexpensively and efficiently. These certificates, also known as Unified Communications certificates (UCC), are ideal for use with Microsoft Exchange 2010 and Microsoft Communications Server. To purchase a SAN certificate, simply purchase an SSL Web Server certificate, an SSL Web Server certificate with Extended Validation or an SGC SuperCert and add SANs during the enrollment purchase process. Unlike many CAs, Thawte does not limited you to one UCC option.

If you want a SAN certificate with server gated cryptography, you can get it. If you want a SAN certificate with Extended Validation, you can get it. If you want a SAN certificate with organization validation, you can get that, too. Thawte offers a flexible SAN certificate solution depending on your requirements.

THAWTE SGC SUPERCERTS

Thawte SGC Supercerts help keep online transactions secure by enabling every web site visitor to experience the strongest SSL encryption available to them. Most SSL certificates are capable of strong encryption (128-bit or higher), however, certain older browsers and operating systems cannot step-up to 128-bit encryption unless an SSL certificate with SGC technology is used. SGC SuperCerts include SGC, full organization authentication, the Thawte Trusted Site Seal, free reissues, and a 30-day money back guarantee.

THAWTE SSL WEB SERVER CERTIFICATES

Thawte SSL Web Server certificates secure confidential information exchanged online and confirm your site's identity to employees, business partners, and other users. When users click the Thawte® Trusted Site Seal or view certificate details, your organization name appears and shows that Thawte, a trusted certificate authority, has verified the site's identity. SSL Web Server Certificates include full organization authentication, the Thawte Trusted Site Seal, free reissues, and a 30-day money back guarantee.

THAWTE SSL WEB SERVER CERTIFICATES WITH EXTENDED VALIDATION (EV)

Thawte SSL Web Server certificates with Extended Validation (EV) enable the most visible security indicator: the green address bar in high-security browsers, assuring users that your site is secure and your identity has been authenticated to the industry's highest standard. When customers see the green address bar and the Thawte Trusted Site Seal, they gain the confidence to complete their transaction. Keep in mind that Extended Validation certificates can only be issued for FQDNs and not for internal names. SSL Web Server Certificates with EV include the Thawte Trusted Site Seal, free reissues, and a 30-day money back guarantee.