How to deploy commercial wildcard certificates to Zimbra 8

23.02.25

Pegasi Knowledge
https://ghost.pegasi.fi/wiki/

Table of Contents

How to deploy commercial wildcard certificates to Zimbra 8

Update 30.09.2019: Verified this is working with Comodo EssentialSSL. Please double check you have “AddTrust External CA Root” certificate in your chain as it may be missing in the bundle you receive from your SSL operator.

Today I did this and I thought I'd write it down in case someone is doing the same. You can skip the straight to Files you need for Zimbra if you already have your certificate.

Make a private key

If you are doing this for the first time you can do a new dedicated private key for wildcard cert to a secure location.

```
openssl genrsa -des3 -out <private key file name>.key 2048
```

Also it is necessary to make a non password version of the key to use with Zimbra

```
openssl rsa -in <private key file name> -out <new key file name to use with zimbra>
```

So you use the new key file without passphrase with Zimbra. Otherwise you need to supply a passphrase with every Zimbra restart and reboot.

Do a certificate signing request

In the location of the private key you made above do a certificate signing request

```
openssl req -new -key <you new private key file name>.key -out <csr file name>.csr
```

- Country Name: Use the two-letter code without punctuation for country, for example: FI, US or UK.
- State or Province: Spell out the state or province completely. For example: California, not CA
- Locality or City: The Locality field is the city or town where the organization is headquartered spelled in full. For example: Helsinki, London or New York
- Company: If the company or department has an &, @, or any other symbol using the shift key in its name, the symbol must be spelled out or omitted, in order to enroll.
    - Example: XY & Z Corporation would be XYZ Corporation or XY and Z Corporation.
    - Organizational Unit: This field is optional; but can be used to help identify certificates registered to an organization. The Organizational Unit (OU) field is the name of the department or organization unit making the request. To skip the OU field, press Enter on the keyboard.

    - Common Name: Here you write the wildcard domain name. For example *.pegasi.fi or *.company.com for your company.

Submit the certificate signing request

Use certificate issuer service to submit your request and see that you are requesting a wildcard certificate. After a while you will receive a signed certificate to your email.

Get CA chain files from Comodo

First we need both root and issuer CA certificates from Comodo. Download these files from the bottom of the page:

- comodorsaaddtrustca.crt (1.91 KB)
- addtrustexternalcaroot.crt (1.49 KB)
- comodorsadomainvalidationsecureserverca.crt (2.13 KB)

Get CA chain files from RapidSSL

First we need both root and issuer CA certificates from following locations:

- Geotrust
- Rapidssl

Be aware that these certificates are made on SHA2 using SHA1 root which is the current recommendation for safe certificates. If you have something else than what RapidSSL recommends then look up different CA chain. You can use check the issuer from your wildcard certificate (openssl x509 -in cert.crt -noout -text) and see if subject is matching in the CA files - all the way to the Geotrust.

Get CA chain files from other issuers

If you are using another certificate issuer you can easily lookup the CA certificates you need by command

```
openssl x509 <your new wildcard certificate file> -noout -text | less
```

And look for issuer certificate path such as

- Issuer: C=US, O=GeoTrust Inc., CN=RapidSSL SHA256 CA - G3

where first you need to locate RapidSSL CA certificate whose subject is “CN=RapidSSL SHA256 CA - G3”. Then you do the same to the issuer's CA certificate and follow the chain as needed.

Assemble certificate chain

Cat up the CA certificates into a single file:

```
cat <rapidssl_ca> <geotrust_ca> > rapidssl_geotrust_ca_chain.crt
```

or with Comodo EssentialSSL

```
cat addtrustexternalcaroot.crt comodorsaaddtrustca.crt
comodorsadomainvalidationsecureserverca.crt >
essentialssl_comodo_ca_chain.crt
```

Files you need for Zimbra

- Your private key you used to get the wildcard cert
- Certificate you got from issuer (RapidSSL for example)
- Issuer CA certificate (see below)
- Root CA certificate, if there is one (see below)

Check files with zmcertmgr

See that Zimbra is happy with the cert configuration

```
/opt/zimbra/bin/zmcertmgr verifycrt comm <private key file> <your new crt
file> <rapidssl geotrust chain file>
```

Backup previous certificates

It is best to backup the whole directory

```
cp -a /opt/zimbra/ssl/zimbra/commercial
/opt/zimbra/ssl/zimbra/commercial.backup
```

Copy over and install certificate files

```
cp <private key file> /opt/zimbra/ssl/zimbra/commercial/commercial.key
```

If you are using Zimbra version 8.7 or later do following as zimbra user (otherwise as root):

```
/opt/zimbra/bin/zmcertmgr deploycrt comm <your new cert file> <rapidssl
```

```
geotrust chain file>
```

Restart Zimbra

Do a restart to start using your new certificate.

```
zmcontrol restart
```