SSL FAQ

Which vendor should we buy our SSL certificate from?

Marketo does not recommend any single provider, but the following SSL Providers are commonly used:

- VeriSign
- Thawte
- Geotrust
- Comodo
- DigiCert
- GoDaddy
- Network Solutions
- RapidSSL

These certificates are recognized by most web browsers. Certain premium certificates will also show your name in the URL bar (usually in a green bar). These are more expensive and it will take more time to issue those, because the SSL vendor will do more background checks before issuing such a certificate.

What format does the certificate need to be?

When you download your certificate at the certificate vendor, please choose the PEM format, which is the standard format for Apache. If you are not able to get the certificate in the PEM format, please check with us: we may be able to convert it to the PEM format on our end.

Often, you will also need to include root or intermediate certificates. These are additional certificates to guarantee the main certificate is recognized in all browsers. Here are some examples:

- Godaddy: gd_bundle.crt
- Verisign: Symantec Secure Site Pro Intermediate CA Bundle

These are just examples: please check with your SSL vendor to include the correct files for your particular certificate.

How to generate the CSR?

Use the OpenSSL format to generate the CSR (http://www.openssl.org/). Normally, your IT department or web server administrator will know how to do this. They will provide you with 2 files:

- The CSR → provide this when you purchase the certificate
- The private key → provide this to Marketo, together with the certificate

If IT or the web team can't provide this to you, you can fairly easily generate the CSR yourself. First, install OpenSSL. If you are on Windows, download it here: http://slproweb.com/products/Win32OpenSSL.html. As of this writing, the current version is "Win32

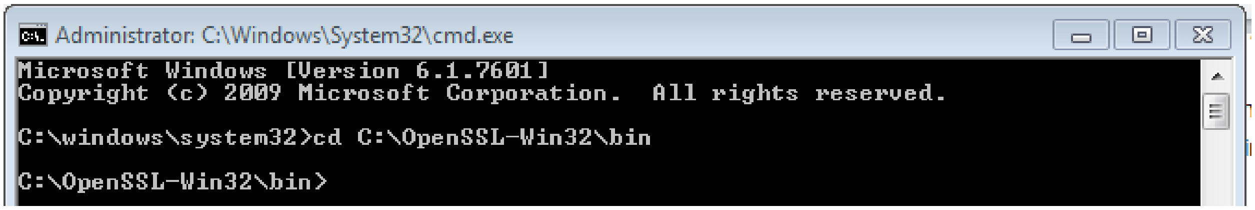
OpenSSL v1.0.1e Light" (which also works on 64-bit Windows). It installs into C:\OpenSSL-Win32 by default. Then go https://www.digicert.com/easy-csr/openssl.htm to generate the command line instructions that you'll need to generate the CSR. This is an example:

```
openssl req -new -newkey rsa:2048 -nodes -out pages_marketo_com.csr -keyout
pages_marketo_com.key -subj "/C=US/ST=California/L=San Mateo/O=Marketo
Inc./CN=pages.marketo.com"
```

Copy this to the clipboard. Then click on the Start menu, type "cmd" in the search box, right-click on the "cmd" program and select "Run as Administrator". Click "Yes" if there is a security warning. Type the following on the command line:

```
cd C:\OpenSSL-Win32\bin
```

Then press the "enter" key.

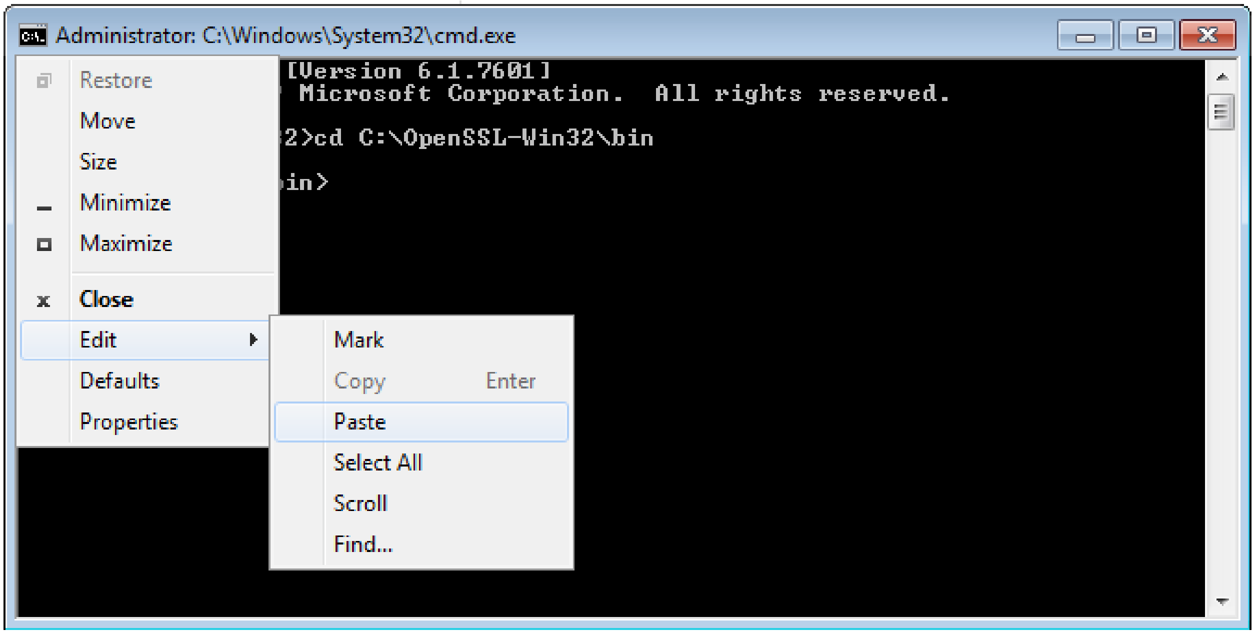


```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\windows\system32>cd C:\OpenSSL-Win32\bin

C:\OpenSSL-Win32\bin>
```

This brings you to the "bin" directory inside the OpenSSL directory. Then paste the code from the digicert website into the command window (click on the icon on the top left of the window to pull out the menu):

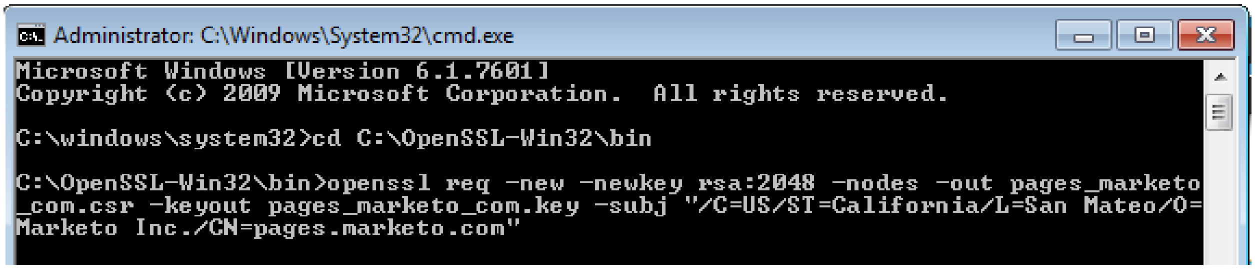


```
[Version 6.1.7601]
 Microsoft Corporation.  All rights reserved.

2>cd C:\OpenSSL-Win32\bin

in>
```

Last Updated: September 10th, 2013



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\windows\system32>cd C:\OpenSSL-Win32\bin

C:\OpenSSL-Win32\bin>openssl req -new -newkey rsa:2048 -nodes -out pages_marketo
_com.csr -keyout pages_marketo_com.key -subj "/C=US/ST=California/L=San Mateo/O=
Marketo Inc./CN=pages.marketo.com"
```

Then press the “enter” key and your CSR and private key will be saved in C:\OpenSSL-Win32\bin.

If you don’t want to install OpenSSL on your computer, you can use an online CSR Generator, for example: https://www.trustico.com/ssltools/create/csr-pem/create-a-new-csr-instantly.php. However, please realize that this exposes your private key to the operator of that website, meaning that they could theoretically purchase an SSL certificate that is registered in your name. Use this option as a last resort, and realize that Marketo does not assume responsibility for the security of private keys that are generated in this way.

Can I use a 1-year Certificate?

You can, but it will be more work on your end to download a new certificate every year, with a risk of the certificate expiring. We recommend using certificates that are valid at least 2 years, which is also usually cheaper per year.

Can we provide you with more than 1 certificate?

No, unfortunately this is not technically possible in our server architecture. If you need to secure multiple domains, please provide us with a wildcard certificate for multiple subdomains (*.company.com) or a SAN Certificate (also called UCC certificate). With a SAN certificate you can include multiple domains in a single certificate (they need to be full domains, wildcards can’t be used).

Do secure landing pages affect the CNAME for our branded tracking links?

No, the CNAME entry for branded tracking links remains unchanged.

Do I need always need a Private Key?

A private key is required for every certificate. With the private key you can generate the CSR (often, the private key is auto-generated when you generate the CSR). You will then purchase the certificate with the CSR, but we will still need to install the private key on the Marketo server, otherwise the certificate will not work.

Example private key:

```
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQDhBMDjqxbGdlkr
xGts6s0PhXTTYu3V6fFzTwrRWldN0GGAm1yfWDUjQssjVY0GYsIELh5SbBut6tWk
4vN9/DpfZjHhgvyLv/xNxKyzjDc2tBf3HlrY1hmbg0de6Xx/LBbMy0ZJAwuKbly+
0spnAyzb1diIV9VCxPglSJQ1v2C1/fKvSo/tXF11auvONLb2bWMm7I6Bd5NkDuTE
y2Fi98u4Qyyboh4C0rPgzyQLzmTqB99X9k1GIQtmsqg/CIa2ra02cb4I/ymrJ6q9
sjOvqLT8c3HDuArVoVW0XQUvrNDcpk8X8Yr2RgVxaCcnar04QPNveSSGqzRNWNS4
CL0arElVAgMBAAECggEAG8waiAV6qsmz+lQpcSsQafpylCqEdwiPa084ZuRiJJq5
cMnAh26+Ibz+mz7WTROmJB4OYOA6CyIXgmcG7WlbTK2zO8iSqjDtWi4Rp5yKtZdJ
3p1BW8gXIb718iOl3Y/0wRfbdumJY3B+xJQFrPQXdpDUTwOKtNTgUrrElF8v80tQ
b7sDQIrluxcLjE1z8NWDWiw89ajbP3DQ9EQ8OPzjs+Wz5BBkvaxftFYF7Mwsjbcj
K+CLwTooTdd8M54s6HLzppKtdXQ4w1WtPsZvQYCqWoHEVl2uHw6ZznlC/1RYAddZ
CKsTS5bVdlxG70KctXRoO+5HXdqyJ9GvuRm8xjboAQKBgQD8ZkieLws0EowRuCtE
u9e7YYCuAXd81on9k0QzMKvIaO2/FktxoCdTh+3VCOaqWeRxy5TiPqmLSDguvlic
KxTeAi+K9tIyQS5QZ64HQ/8QwNYkDrvgaTjZpihZ18dl8+CM3DP80qEH6iDEtVDr
4LARpa8/p6X91WzP3ib7mjVdBQKBgQDkOnrEWbIaBN6kWg18Zs6xZM1LsmjJY6bJ
sFojJ2Jg4cFzSH3bf3jdy4t7caMh9zsttLy/+BobsTRWv5mjgXuWvq7Ywi+Nb5at
rGntbzTnKwqe54Oc3dcAs4wmAyyFhyYMGTUVAvHbuEyHhQY2x1dHeCDPPQ7TOhO/
tCTbz8dsEQKBgFM+rO63F1vaTiY99s9ZoOJlWxqI007yN1rR6mlzwQR9TwR6JvHX
34CWUWO05tcChOzfN0CTaDnO3PDVyMXhE6XRVLrhgxweEVdliqlMzOBKqZYE4gQ2
0BBA1AgludcvYz0yF1doZMIGfz5BiunxFkELw0wcUAvzC0tXusW666S9AoGAVI21
3fi9GxaixZD3XhdYjDAkPt8iIzpgGGjVfCCjOfFpkiRRPHjFdqZqTpmTLopBynUj
WJu6UHgeQ+VILmNSPk72yCdpJqUo1b8Cn4yLtPklPinXgM5PUVszmQGkBPRFDEZq
fBZTNGvbLnoCC1le5IOE5EJis67YkjVTUnxwDYECgYEAwDhnnyL9LF25JJWvNm6I
H4IVdTxNn3XGWLrQgUfu1yJwdeU5Qas66bMlt4tcjUOoX5Dq5A0SaEXxgFTlvFg5
c7quYqJ3XkP/+ibONdnkcah2/Ji/0zTZ9WHAXi+afDuQytA1rTuK//AAwGhF2M74
v7LwazaYDE97ySYQERK4114=
-----END PRIVATE KEY-----
```

Why does it take about 3 weeks for Marketo to install the certificates?

To enable secure landing pages, we need to set up a dedicated landing page server for your organization. Non-secure landing pages are served from a shared web server, which is not suitable for secure pages.

Setting up a dedicated secure landing page server takes some time because there is a lot of back-end work involved, done by one of our network engineers: we will assign a new IP address for your new landing page server, install a new load balancer, reconfigure our internal DNS and install the certificate. We depend on external vendors for part of these tasks.

Checking & Changing the TTL

At least 1 day before the switch-over to the new secure landing pages, change the TTL of your CNAME to at most 300 seconds. In your DNS admin panel you can set the TTL. If you don’t have access to the DNS admin panel, you can use this website to look up the TTL of your CNAME:

http://mxtoolbox.com/DNSLookup.aspx?command=a

This will have to be at most 300 seconds, so that changes to the CNAME entry will propagate in 5 minutes, otherwise web browsers may have cached your old CNAME setting and still go to the old insecure landing pages for hours or days.

Will URLs to my existing non-secure Marketo Landing Pages continue to work?

Yes, your existing Marketo landing pages will be redirected to the secure pages. There are only few situations where you have to manually update the URL, specifically when you include a Marketo landing page on a secure website using an iframe: you will need to load the secure version of the landing page, otherwise the end user will get a security warning.

Converting Marketo Landing Pages to SSL does not affect any pages on your main (non-Marketo) website.

What do I need to do after go-live?

Do the following things:

- Re-approve all landing pages, which you can do in bulk by going to Design Studio, then clicking on “Landing Pages”. You can now multi-select pages and unapproved and approve again via the “Landing Page Actions” menu.
- It is also recommended to change all images, JavaScript files and other external links in landing pages to HTTPS, otherwise users may get an “Insecure Content on Secure Pages” error
- If you include a Marketo landing page on a secure website using an iframe, you will need to load the secure version of the landing page, otherwise the end user will get a security warning.
- If you use a Marketo Form on a Non-Marketo Page, you will need to update the Post URL to HTTPS.
- If you do a server-side post to a Marketo Form and you use your CNAME as the Post URL, you also need to change that to HTTPS

Will the Muchkin JavaScript API also be encrypted via SSL?

Yes, calls to the Munchkin JavaScript API automatically switch to SSL if the page on which the calls are made is SSL encrypted.