# SSL Certificates

## Self-issued Apache SSL certificate

```
# openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout domain.key -
out domain.crt
# mv domain.* /etc/ssl/private
```

Modify or create the config file for the virtual host in /etc/apache2/sites-available:

```
<VirtualHost *:443>
DocumentRoot /var/www/website
ServerName www.domain.com
SSLEngine on
SSLCertificateFile /home/user/ssl/domain.crt
SSLCertificateKeyFile /home/user/ssl/domain.key
# add the certificate chain file if using a class 3 certificate only
SSLCertificateChainFile /home/user/ssl/chain.crt
</VirtualHost>
```

Note that Windows 8 phones cannot establish SSL connections via Webdav through self-issued certificates.

## CAcert SSL certificates

CAcert is aimed at providing SSL certificates to the community with no or little charges. The following instruction is taken from Creating a Simple Apache Certificate

### Creating a Simple Apache Certificate

First of all go to the mod_ssl documentation for basic mod_ssl configuration. I will not go into mod_ssl, I'll just try to show you a way to get and install a CAcert certificate.

If you just want a certificate for a single site Apache server this is probably the simplest way to get a CAcert signed certificate. For the more complicated cases please have a look at ApacheServer and VhostsApache.

Once Apache is running with mod_ssl you'll have to register the domain component of your webserver (that is “example.org” for the server “www.example.org”) with your CAcert account. To do this go to CAcert homepage, log in, click “Domains → Add” and follow the instructions there. If your Domain is shown as “verified” on “Domains → Show” you can continue and generate a certificate for your server.

Generate a certificate signing request (CSR) using the following commands:

```
openssl genrsa -out domain.key 4096
openssl req -new -key domain.key -out domain.csr
```

While openssl script is running, fill the questions with appropiate answers

```
|| '''OpenSSL question''' || '''Sample Answer''' || '''Remarks''' ||
|| Country Name (2 letter code) [DE]: || AU ||<#ff8080> will be stripped
later ||
|| State or Province Name (full name) [Some-State]: || NSW, AU ||<#ff8080>
will be stripped later ||
|| Locality Name (eg, city) []: || Sydney ||<#ff8080> will be stripped later
||
|| Organization Name (eg, company) [Internet Widgits Pty Ltd]: || @home
||<#ff8080> will be stripped later ||
|| Organizational Unit Name (eg, section) []: || ||<#ff8080> will be
stripped later ||
|| Common Name (e.g. server FQDN or YOUR name) []: ||
testserver3.mydomain.tld ||<#00FF00> will be extracted and checked later ||
|| Email Address []: || mycacertaccount.primary.email ||<#00FF00> will be
extracted and checked later ||
||<-3> Please enter the following 'extra' attributes ||
||<-3> to be sent with your certificate request ||
|| A challenge password []: || || ||
|| An optional company name []: || || ||
```

Go to CACert, log in, and select “Server certificates → New”. If a Class 3 certificate is available for you I'd advise you to select a Class 3 certificate, which is a more secure subset of the Class 1 certificate.

Use Copy/Paste to input your CSR (the content of 'domain.csr' in the above example) into the big editor box. Be sure to include the header and footer lines and check that after the paste operation the request has not been truncated.

Click on “Send” and your certificate will be generated. That is, if you did not make a mistake. If you made one, read the error message, try to understand what it wants to say to you and try again while skipping the mistake. ;)

Use Copy/Paste with your favourite editor to save the certificate to a file (let's call the file domain.crt).

Move the private key and the certificate to a convenient location, for example directory *ssl* in your home.

If using a Class 3 certificate as proposed you'll need the certificate chain file. This is just the Class 3 root certificate and the Class 1 root certificate in PEM format concatenated. Do it yourself or download it here.

Store the certificate chain file in the *ssl* directory and let's call it cacert.chain for future reference.

Now all that remains to be done is to correctly configure Apache's mod_ssl. To use the certificate set the following directives in your SSL-configuration:

Modify or create the config file for the virtual host in /etc/apache2/sites-available:

```
<VirtualHost *:443>
DocumentRoot /var/www/website
ServerName www.domain.com
SSLEngine on
SSLCertificateFile /home/user/ssl/domain.crt
SSLCertificateKeyFile /home/user/ssl/domain.key
# add the certificate chain file if using a class 3 certificate only
#SSLCertificateChainFile /home/user/ssl/chain.crt
</VirtualHost>
```

This is it. Restart your Apache and see if it works! Click the SSL Certificate Checker to check whether the certificate is properly installed.

#### Renewing an existing certificate

To renew the certificate of an existing Apache configuration, you need to renew the certificate through the CAcert web interface, and then replace the existing certificate (in this example, `/home/user/ssl/domain.crt`) with the new certificate provided.

#### Note on Class 3 certificates

- if you install a Class 3 certificate, you need to install the certificate chain file on the server
- if you install a Class 1 certificate, you **must not** install the certificate chain file, otherwise the chain is broken and some apps refuse to connect to the server
- Internet Explorer still connect to the server, even if the chain is broken as described above
- Verify the chain with the SSL Certificate Checker

## Adding the root certificate to the client

#### Windows 7 Desktop

1. Visit http://www.cacert.org/index.php?id=3 and run the Windows installer package. This will install the root and intermediate certificates for Windows, Internet Explorer, Chrome, Safari, but not for Firefox.
2. Open Firefox and visit http://wiki.cacert.org. The “This Connection is Untrusted” error page shows up. This confirms that CAcert.org's certificate is not a trusted root CA certificate in Firefox.
3. Visit http://www.cacert.org/index.php?id=3 again under Firefox and install the certificates manually as explained below.
4. Click “Root Certificate (PEM Format)” link (Class 1). The “Download Certificate” dialog box shows up.
5. Check “Trust this CA to identify web sites” option and click “OK”. CAcert.org's root certificate is installed in Firefox now.
6. Click “Intermediate Certificate (PEM Format)” link (Class 3). The “Download Certificate” dialog box shows up.
7. Check “Trust this CA to identify web sites” option and click “OK”. CAcert.org's intermediate certificate is installed in Firefox now.

8. Close Firefox and run it again to visit http://wiki.cacert.org. The CAcert Wiki shows up properly now.

#### Windows 8 Phone

1. Download the original PEM certificates (root/class 1 and intermediate/class 3) from http://www.cacert.org/index.php?id=3.
2. Convert the format with this SSL Converter from PEM to DER/Binary.
3. Rename the file extension .der to .cer, and email it to the phone.
4. Open the email attachment on the phone to install the certificate.

#### iPad

1. Download the original PEM certificates (root/class 1 and intermediate/class 3) from http://www.cacert.org/index.php?id=3.
2. Email the certificates to the iPad and open the email attachment to install the certificate.
3. Alternatively, follow Adding CA Cert root and personal certificates to your iPhone, iPod or iPad
4. Note that CAcert is not a trusted authority as per 12th, so some apps on the iPad refuse to connect.

### Other resources

- CAcert
- SSL Certificate Checker
- SSL Converter
- Apache Server Client Certificate Authentication
- Creating SSL certificates with CAcert.org and OpenSSL
- Creating a Simple Apache Certificate (original article)
- Adding CA Cert root and personal certificates to your iPhone, iPod or iPad

## Comodo SSL certificates

### Install a free certificate (3 month validity)

Go to Comodo and follow the instructions to issue a free certificate which is valid for 3 months. The steps are equivalent to the guide below to install a PositiveSSL certificate.

### Install a PositiveSSL certificate

1. Purchase the certificate at Namecheap for $4.95 per year, when purchased for 5 years
2. Generate a certificate signing request (CSR) using the following commands:

```
openssl genrsa -out domain.key 2048
openssl req -new -key domain.key -out domain.csr
```

3. Copy your domain.crt file where your domain.key file is found (/home/user/ssl in the example below)
4. Create the chain file like so (the sequence of files is important) and copy it to the same location:

```
cat COMODORSADomainValidationSecureServerCA.crt COMODORSAAddTrustCA.crt
AddTrustExternalCARoot.crt > chain.crt
```

5. Modify or create the config file for the virtual host in /etc/apache2/sites-available:

```
<VirtualHost *:443>
DocumentRoot /var/www/website
ServerName www.domain.com
SSLEngine on
SSLCertificateFile /home/user/ssl/domain.crt
SSLCertificateKeyFile /home/user/ssl/domain.key
SSLCertificateChainFile /home/user/ssl/chain.crt
</VirtualHost>
```

6. Restart apache. Done.

## SSL not working

Make sure to issue the following command to activate mod_ssl for apache:

```
# a2enmod ssl
```