

Setting up OCSP for Apache server

Question

How do I set up an OCSP for server based on Apache?

Answer

Enable OCSP Stapling on Apache:

1. First check that Apache HTTPD Server 2.3.3 or above is installed by running one of the following commands:

```
apache2 -v  
httpd -v
```

Versions lower than 2.3.3 do not support OCSP stapling, so you should update Apache before proceeding with the rest of this tutorial.

2. Check whether OCSP stapling is already enabled or not:

Use openssl command:

```
openssl s_client -connect login.live.com:443 -tls1 -tlsextdebug -status
```

- Scroll down to "OCSP response:"
- If OCSP is enabled, the "OCSP Stapling" is

```
OCSP Response Status: successful (0x0)
```

- If OCSP is not enabled, you won't see any OCSP Response Data:

```
OCSP response: no response sent
```

If it is not enabled, you won't see any OCSP Response Data.

3. If Step 2 revealed no evidence that OCSP is enabled on your server, it is first worth checking that Apache can actually connect to our OCSP servers. Our OCSP servers are at the following locations:

DNS HOSTNAME(S)	Destination IP	Port
OCSP.ComodoCA.com OCSP.usertrust.com	178.255.83.1 or 2a02:1788:2fd::b2ff:5301	Tcp/80

To check connectivity, use the following telnet command:

```
telnet OCSP.ComodoCA.com 80
```

If the test is successful the reply will state 'Connected to [OCSP.ComodoCA.com](https://ocsp.comodo.com)' for at least one of the 'Destination IP' addresses in the table above.

If the test is unsuccessful the replies will state 'Network Unreachable' and/or 'Connection Timed Out'. Please make the required network changes to allow your Apache server to connect to our OCSP servers. Once complete, we advise you to re-run the test in step 2 to establish whether OCSP stapling is already enabled.

4. To enable OCSP stapling you need to edit the virtual host configuration file for your site using the editor of your choice (example editors include nano or vi):

```
nano /etc/apache2/sites-available/your-domain.com-ssl.conf
```

Make the following changes:

- Add the following lines inside the <VirtualHost> tags:

```
SSLUseStapling on
SSLStaplingResponderTimeout 5
SSLStaplingReturnResponderErrors off
```

- Add a line inside the tags which points to a trusted certificate chain file. This must contain the intermediate & root certificates in order:

```
SSLCACertificateFile /etc/apache2/ssl/full_chain.pem
```

- Add the following line outside the <VirtualHost> tags:

```
SSLStaplingCache shmcb:/var/run/ocsp\(128000\)
```

Use the example below as a reference configuration:

```
SSLStaplingCache shmcb: /var/run/ocsp(128000)
```

```
<VirtualHost *:443>
    ServerAdmin admin@your-domain.com
    ServerName your-domain.com
    DocumentRoot /var/www

    SSLEngine on
    SSLUseStapling on

    SSLStaplingResponderTimeout 5
    SSLStaplingReturnResponderErrors off

    SSLCertificateFile /etc/apache2/ssl/your-domain.com/your\_certificate.crt
    SSLCertificateKeyFile /etc/apache2/ssl/your-domain.com/your.key

    SSLCACertificateFile /etc/apache2/ssl/full_chain.pem
</VirtualHost>
</IfModule>
```

5. Test your configuration is OK:

```
apachectl -t
```

6. Restart Apache if OK:

```
service apache2 reload
```

7. Verify OCSP Stapling is working by repeating Step 2.

Revision #2

Created 2026-08-07 14:53:05 UTC by Sarath

Updated 2026-08-07 16:02:03 UTC by Sarath