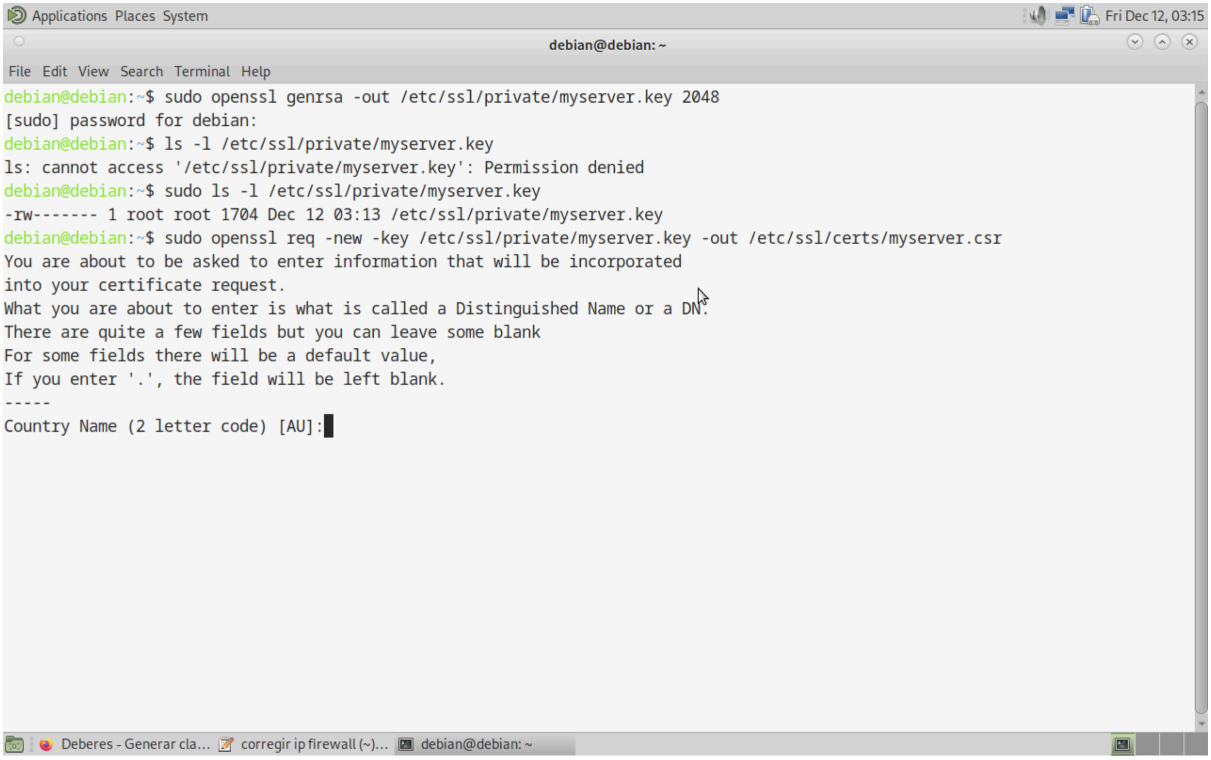
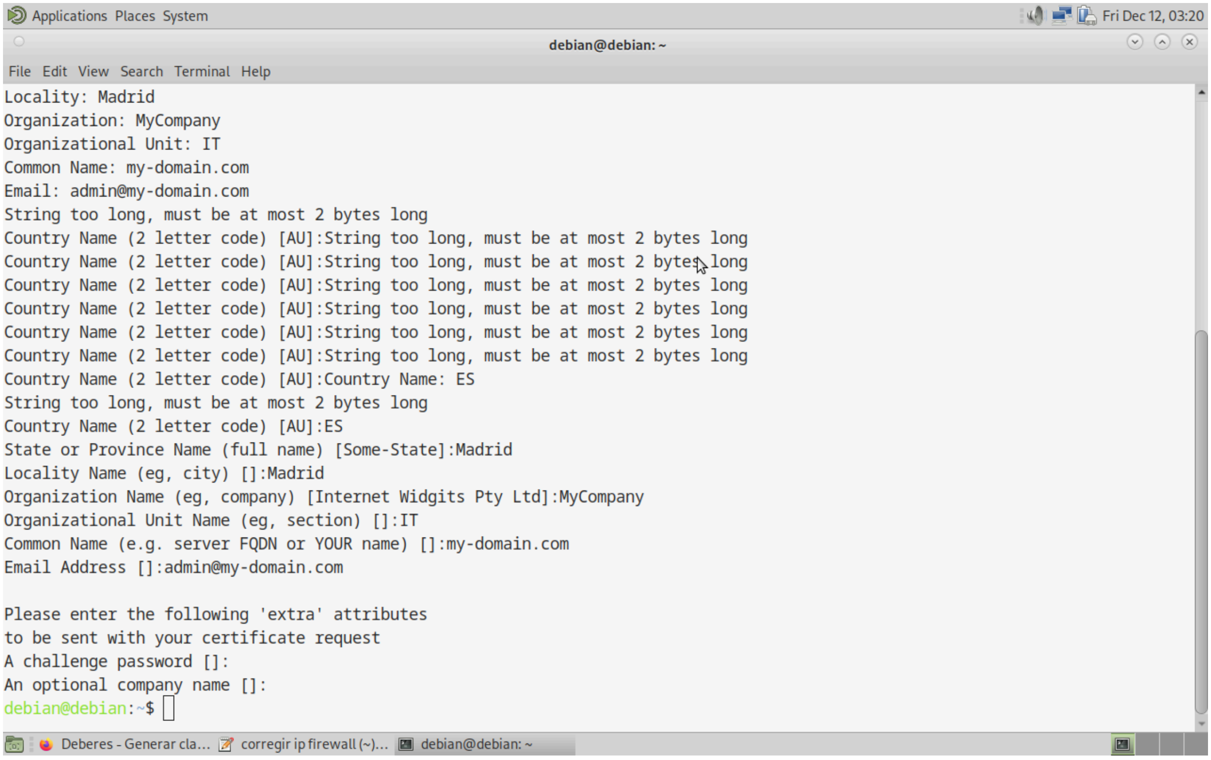
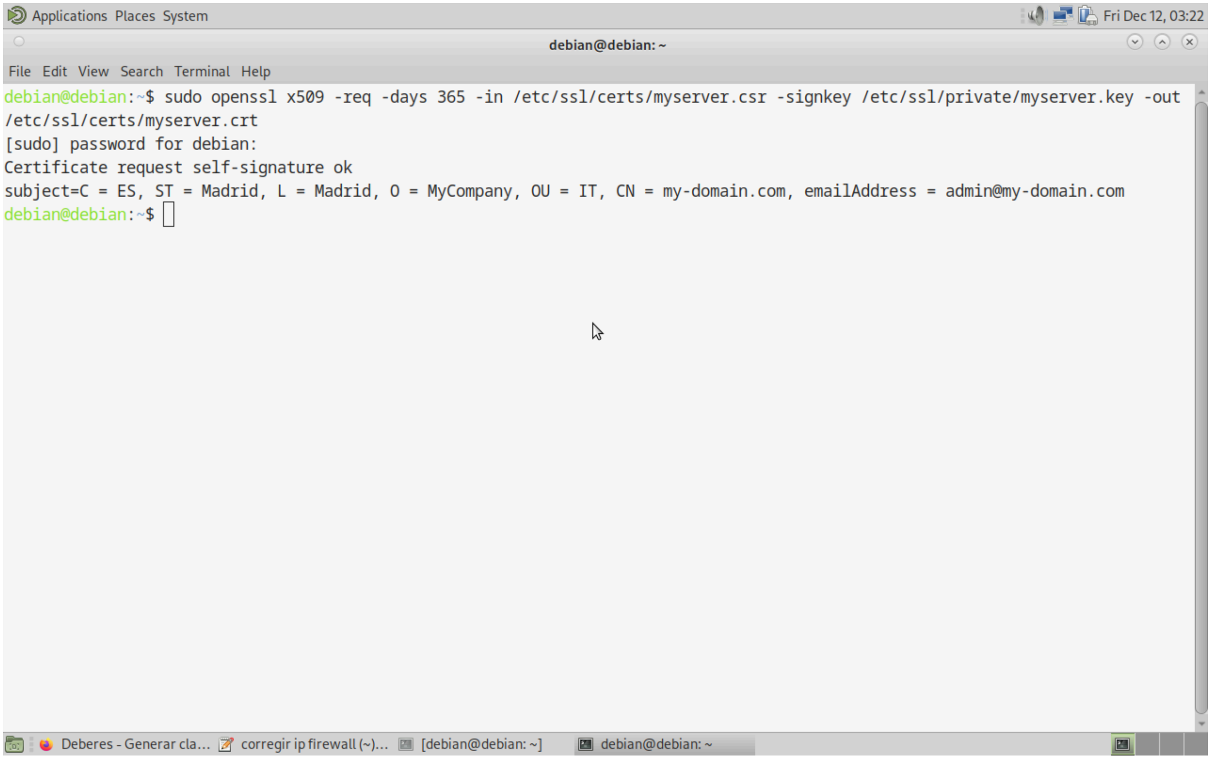

Applications Places System
Fri Dec 12, 03:15
debian@debian: ~
File Edit View Search Terminal Help
Deberes - Generar cla...
corregir ip firewall (~)...
debian@debian: ~

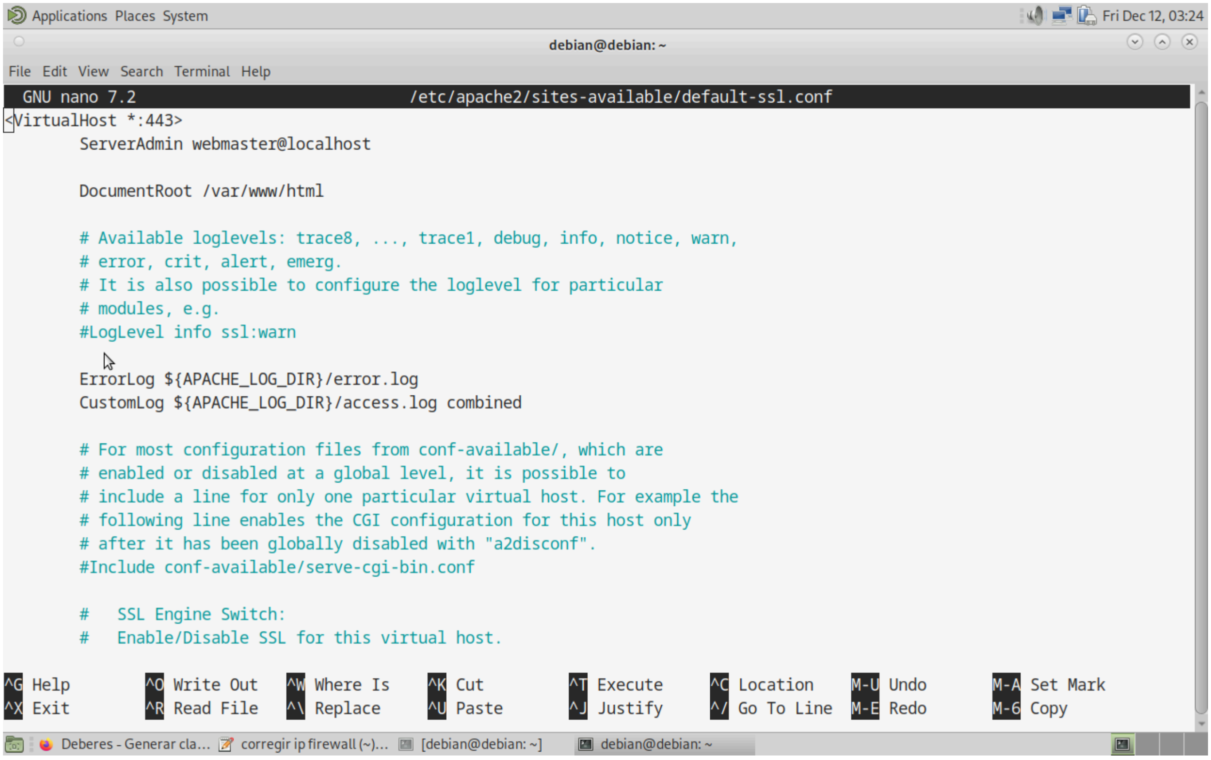
```
debian@debian:~$ sudo openssl genrsa -out /etc/ssl/private/myserver.key 2048
[sudo] password for debian:
debian@debian:~$ ls -l /etc/ssl/private/myserver.key
ls: cannot access '/etc/ssl/private/myserver.key': Permission denied
debian@debian:~$ sudo ls -l /etc/ssl/private/myserver.key
-rw------- 1 root root 1704 Dec 12 03:13 /etc/ssl/private/myserver.key
debian@debian:~$ sudo openssl req -new -key /etc/ssl/private/myserver.key -out /etc/ssl/certs/myserver.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
```


Applications Places System
Fri Dec 12, 03:20
debian@debian: ~
File Edit View Search Terminal Help
Deberes - Generar cla...
corregir ip firewall (~)...
debian@debian: ~

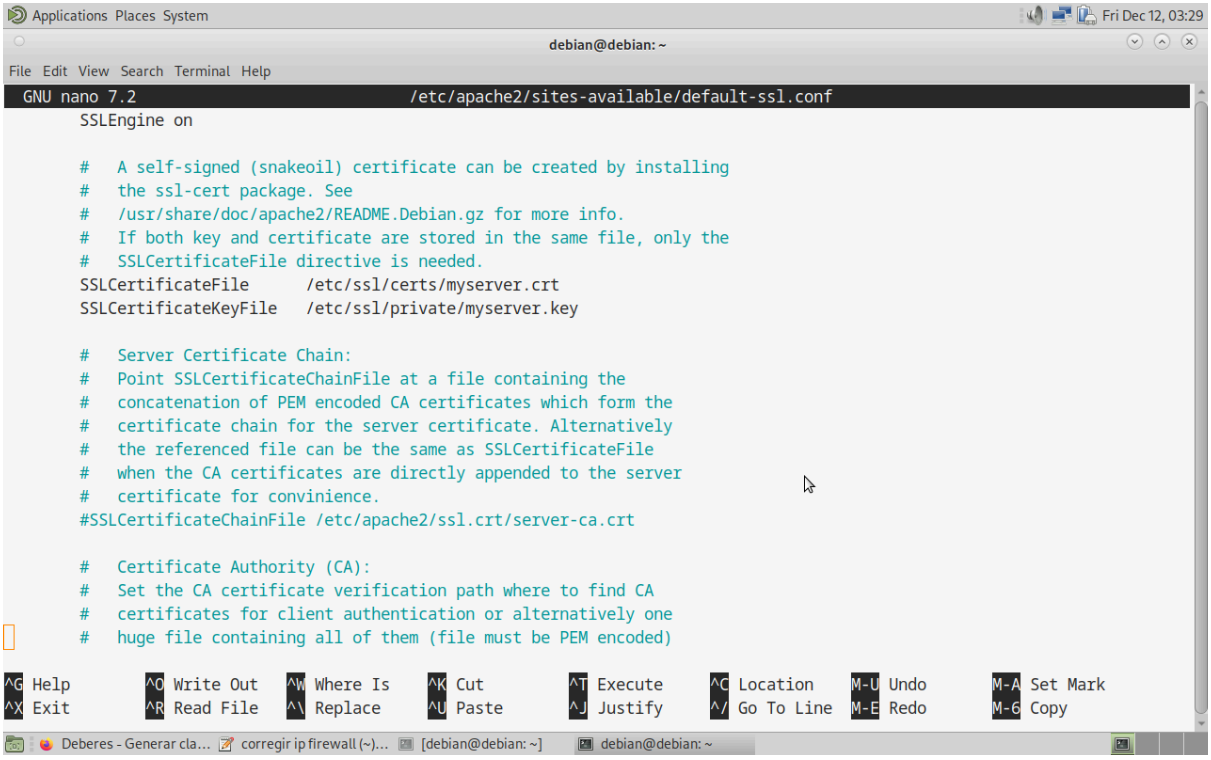
```
Locality: Madrid
Organization: MyCompany
Organizational Unit: IT
Common Name: my-domain.com
Email: admin@my-domain.com
String too long, must be at most 2 bytes long
Country Name (2 letter code) [AU]:String too long, must be at most 2 bytes long
Country Name (2 letter code) [AU]:String too long, must be at most 2 bytes long
Country Name (2 letter code) [AU]:String too long, must be at most 2 bytes long
Country Name (2 letter code) [AU]:String too long, must be at most 2 bytes long
Country Name (2 letter code) [AU]:String too long, must be at most 2 bytes long
Country Name (2 letter code) [AU]:String too long, must be at most 2 bytes long
Country Name (2 letter code) [AU]:Country Name: ES
String too long, must be at most 2 bytes long
Country Name (2 letter code) [AU]:ES
State or Province Name (full name) [Some-State]:Madrid
Locality Name (eg, city) []:Madrid
Organization Name (eg, company) [Internet Widgits Pty Ltd]:MyCompany
Organizational Unit Name (eg, section) []:IT
Common Name (e.g. server FQDN or YOUR name) []:my-domain.com
Email Address []:admin@my-domain.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
debian@debian:~$ 
```



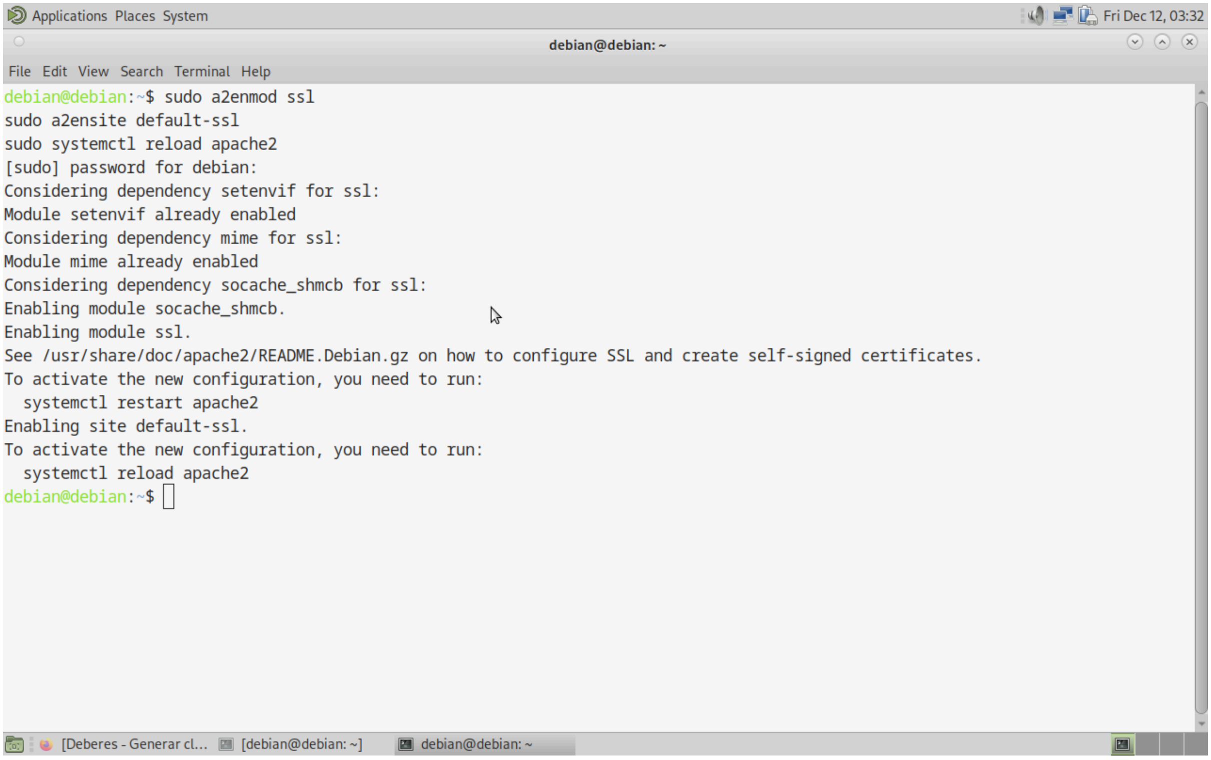
```
debian@debian:~$ sudo openssl x509 -req -days 365 -in /etc/ssl/certs/myserver.csr -signkey /etc/ssl/private/myserver.key -out
/etc/ssl/certs/myserver.crt
[sudo] password for debian:
Certificate request self-signature ok
subject=C = ES, ST = Madrid, L = Madrid, O = MyCompany, OU = IT, CN = my-domain.com, emailAddress = admin@my-domain.com
debian@debian:~$ 
```



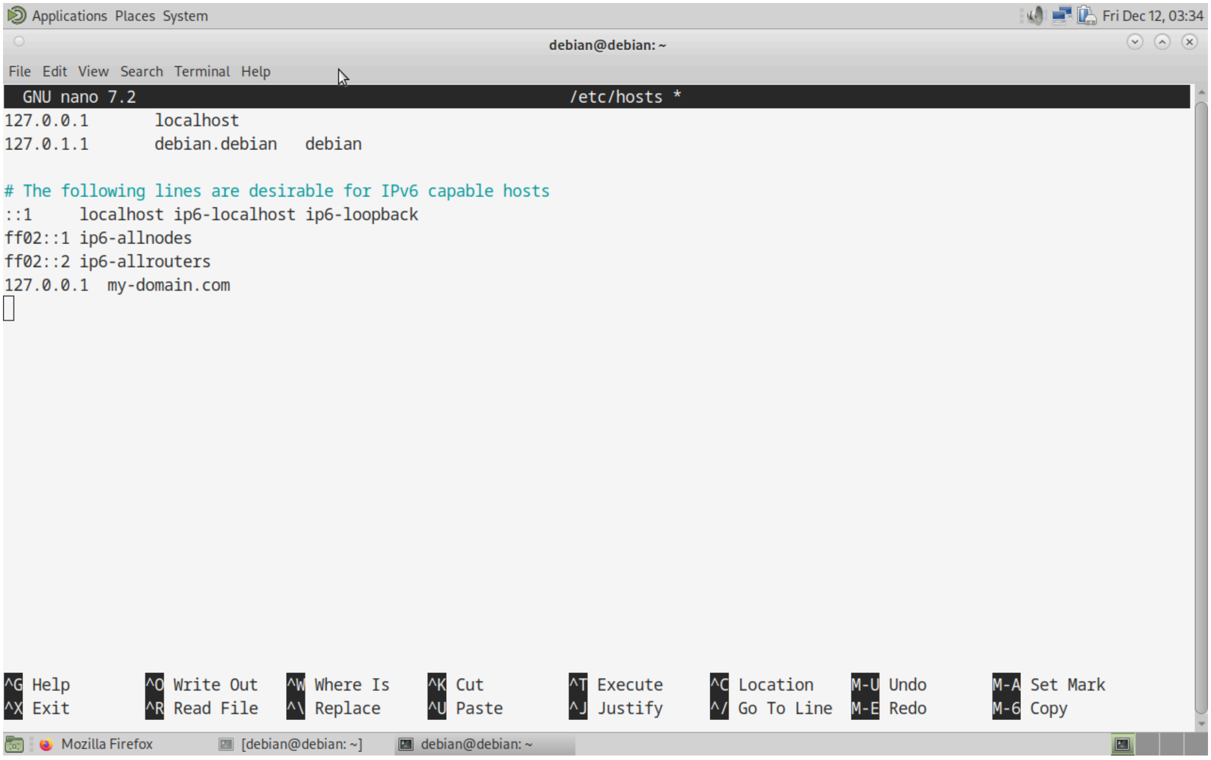
```
 GNU nano 7.2                     /etc/apache2/sites-available/default-ssl.conf
<VirtualHost *:443>
        ServerAdmin webmaster@localhost

        DocumentRoot /var/www/html

        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
        # error, crit, alert, emerg.
        # It is also possible to configure the loglevel for particular
        # modules, e.g.
        #LogLevel info ssl:warn

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

        # For most configuration files from conf-available/, which are
        # enabled or disabled at a global level, it is possible to
        # include a line for only one particular virtual host. For example the
        # following line enables the CGI configuration for this host only
        # after it has been globally disabled with "a2disconf".
        #Include conf-available/serve-cgi-bin.conf

        #   SSL Engine Switch:
        #   Enable/Disable SSL for this virtual host.
```


Applications Places System
Fri Dec 12, 03:29
debian@debian: ~
File Edit View Search Terminal Help

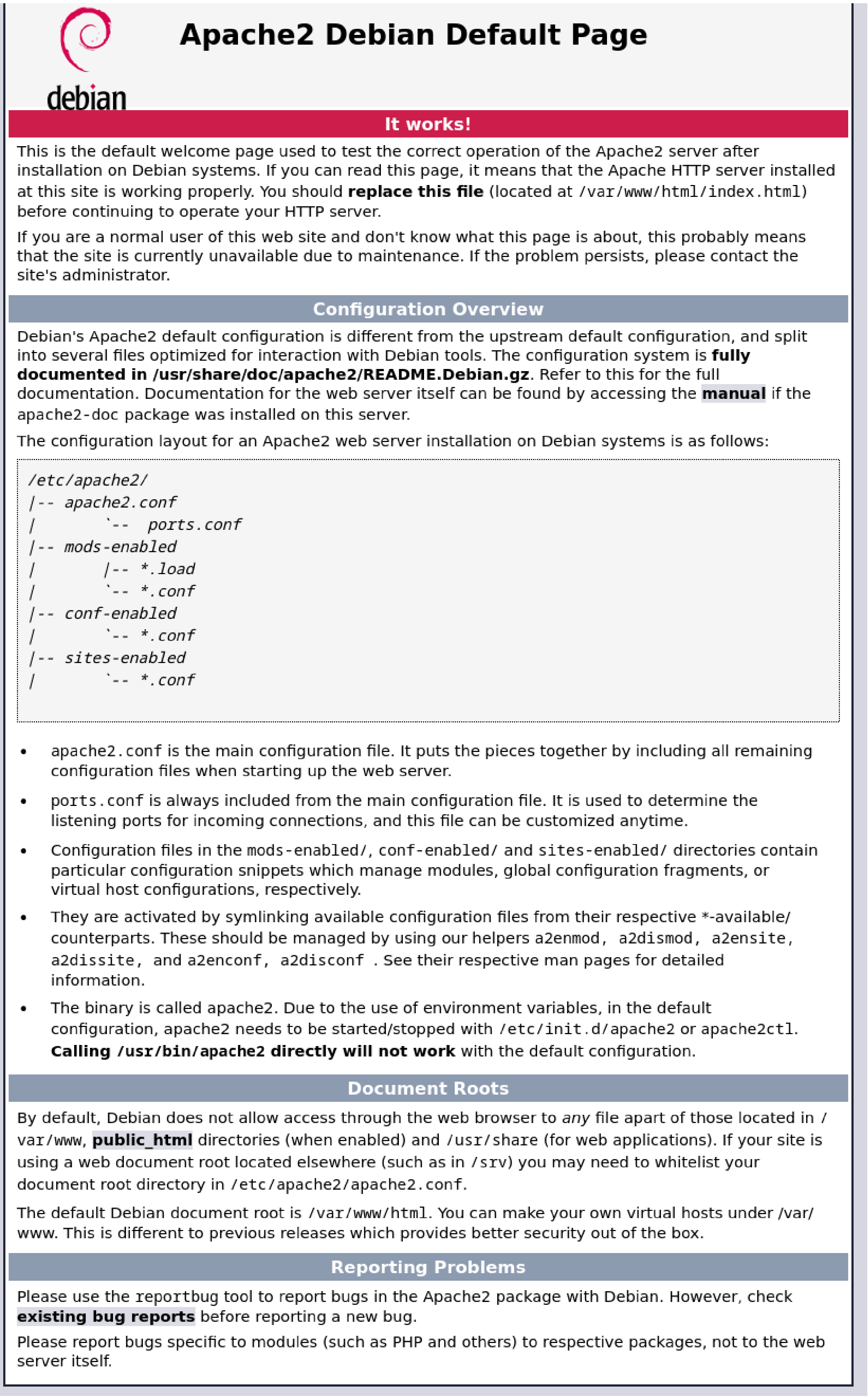
```
 GNU nano 7.2                    /etc/apache2/sites-available/default-ssl.conf
        SSLEngine on

        #   A self-signed (snakeoil) certificate can be created by installing
        #   the ssl-cert package. See
        #   /usr/share/doc/apache2/README.Debian.gz for more info.
        #   If both key and certificate are stored in the same file, only the
        #   SSLCertificateFile directive is needed.
        SSLCertificateFile      /etc/ssl/certs/myserver.crt
        SSLCertificateKeyFile   /etc/ssl/private/myserver.key

        #   Server Certificate Chain:
        #   Point SSLCertificateChainFile at a file containing the
        #   concatenation of PEM encoded CA certificates which form the
        #   certificate chain for the server certificate. Alternatively
        #   the referenced file can be the same as SSLCertificateFile
        #   when the CA certificates are directly appended to the server
        #   certificate for convinience.
        #SSLCertificateChainFile /etc/apache2/ssl.crt/server-ca.crt

        #   Certificate Authority (CA):
        #   Set the CA certificate verification path where to find CA
        #   certificates for client authentication or alternatively one
        #   huge file containing all of them (file must be PEM encoded)

^G Help      ^O Write Out  ^W Where Is   ^K Cut       ^T Execute   ^C Location   M-U Undo     M-A Set Mark
^X Exit      ^R Read File  ^\ Replace    ^U Paste     ^J Justify   ^/ Go To Line M-E Redo     M-6 Copy
```


Applications Places System
Fri Dec 12, 03:32
debian@debian: ~
File Edit View Search Terminal Help
[Deberes - Generar cl... [debian@debian: ~] debian@debian: ~

```
debian@debian:~$ sudo a2enmod ssl
sudo a2ensite default-ssl
sudo systemctl reload apache2
[sudo] password for debian:
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certificates.
To activate the new configuration, you need to run:
  systemctl restart apache2
Enabling site default-ssl.
To activate the new configuration, you need to run:
  systemctl reload apache2
debian@debian:~$ 
```


Applications Places System
Fri Dec 12, 03:34
debian@debian: ~
File Edit View Search Terminal Help
Mozilla Firefox [debian@debian: ~] debian@debian: ~

```
 GNU nano 7.2                                  /etc/hosts *
127.0.0.1       localhost
127.0.1.1       debian.debian   debian

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
127.0.0.1  my-domain.com

^G Help      ^O Write Out  ^W Where Is  ^K Cut       ^T Execute   ^C Location    M-U Undo   M-A Set Mark
^X Exit      ^R Read File  ^\ Replace   ^U Paste     ^J Justify   ^/ Go To Line  M-E Redo   M-6 Copy
```



Apache2 Debian Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the `mods-enabled/`, `conf-enabled/` and `sites-enabled/` directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
- They are activated by symlinking available configuration files from their respective *-available/ counterparts. These should be managed by using our helpers `a2enmod`, `a2dismod`, `a2ensite`, `a2dissite`, and `a2enconf`, `a2disconf` . See their respective man pages for detailed information.
- The binary is called apache2. Due to the use of environment variables, in the default configuration, apache2 needs to be started/stopped with `/etc/init.d/apache2` or `apache2ctl`. **Calling /usr/bin/apache2 directly will not work** with the default configuration.

Document Roots

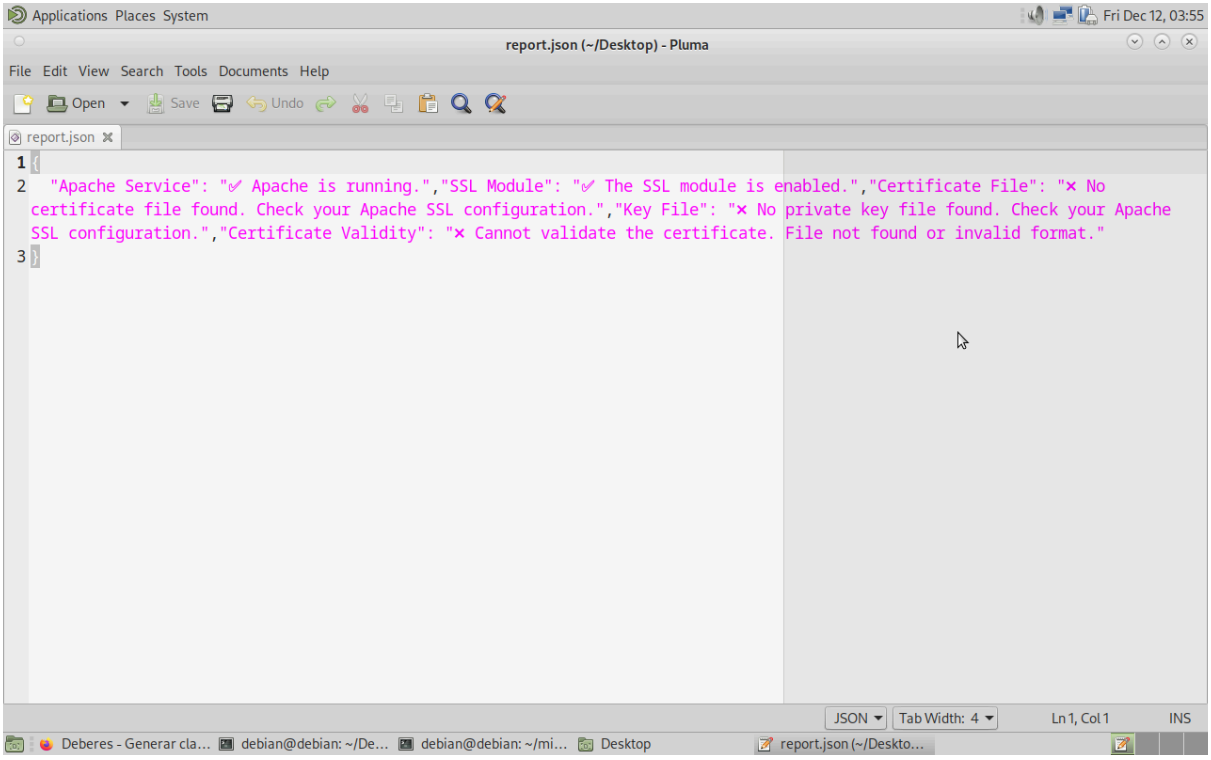
By default, Debian does not allow access through the web browser to *any* file apart of those located in `/var/www`, **public_html** directories (when enabled) and `/usr/share` (for web applications). If your site is using a web document root located elsewhere (such as in `/srv`) you may need to whitelist your document root directory in `/etc/apache2/apache2.conf`.

The default Debian document root is `/var/www/html`. You can make your own virtual hosts under /var/www. This is different to previous releases which provides better security out of the box.

Reporting Problems

Please use the `reportbug` tool to report bugs in the Apache2 package with Debian. However, check **existing bug reports** before reporting a new bug.

Please report bugs specific to modules (such as PHP and others) to respective packages, not to the web server itself.



```
{
  "Apache Service": "✓ Apache is running.","SSL Module": "✓ The SSL module is enabled.","Certificate File": "× No certificate file found. Check your Apache SSL configuration.","Key File": "× No private key file found. Check your Apache SSL configuration.","Certificate Validity": "× Cannot validate the certificate. File not found or invalid format."
}
```