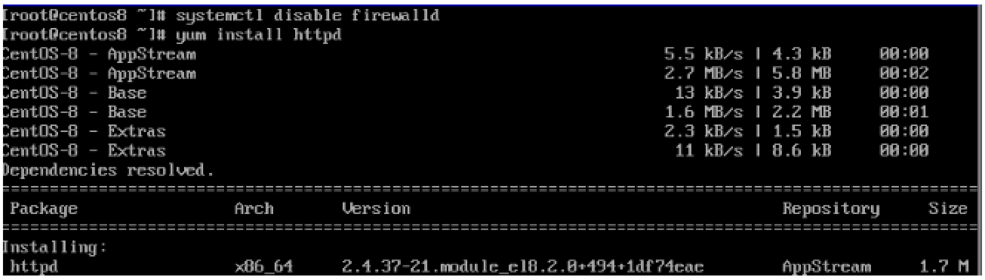
Report on VPN (Task 3)

Name: Aravindh JAWAHAR

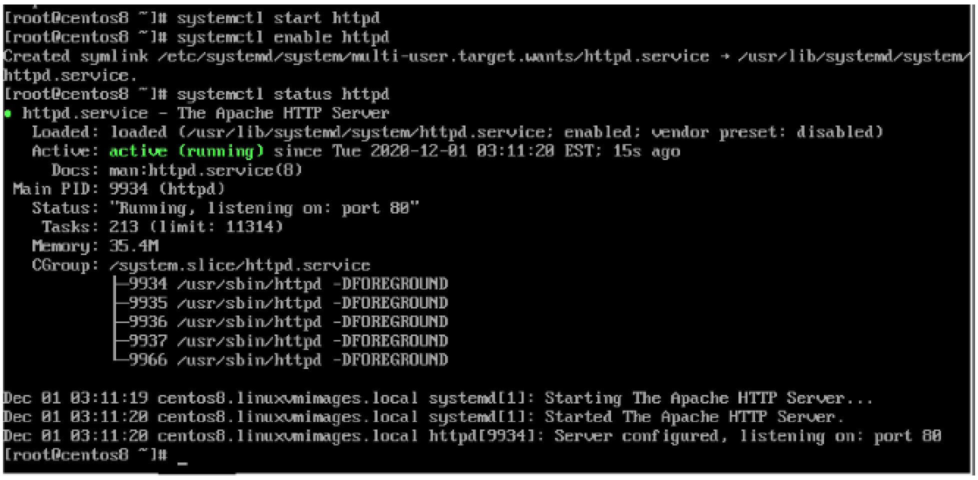
In this lab, we will create a PKI. We will see how to create a root CA and a client certificate. In this lab, we will need a CentOS 8 VM with internet that can be accessed from your computer web browser

Apache server has been installed using the yum install httpd command



```
[root@centos8 ~]# systemctl disable firewalld
[root@centos8 ~]# yum install httpd
CentOS-8 - AppStream                                          5.5 kB/s | 4.3 kB     00:00
CentOS-8 - AppStream                                          2.7 MB/s | 5.8 MB     00:02
CentOS-8 - Base                                                13 kB/s | 3.9 kB     00:00
CentOS-8 - Base                                               1.6 MB/s | 2.2 MB     00:01
CentOS-8 - Extras                                             2.3 kB/s | 1.5 kB     00:00
CentOS-8 - Extras                                              11 kB/s | 8.6 kB     00:00
Dependencies resolved.
==================================================================================================
 Package                Arch       Version                                Repository      Size
==================================================================================================
Installing:
 httpd                  x86_64     2.4.37-21.module_el8.2.0+494+1df74eac        AppStream     1.7 M
```

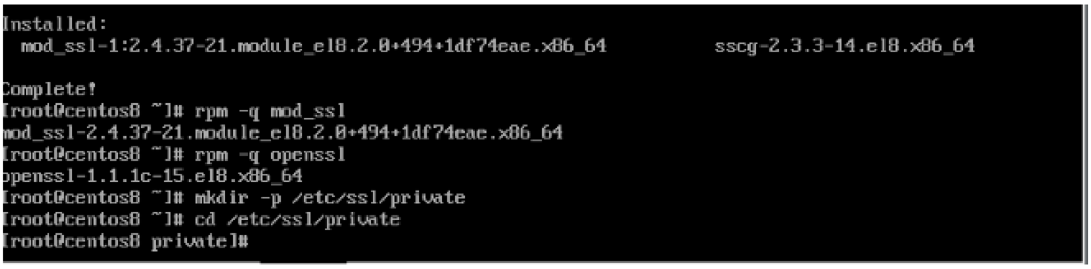
HTTPD service has been started to use the apache server on the external host using its physical IP address of the server with HTTP format without encryption. And the service should be enabled to achieve the usage of httpd on the browser without any load failure.



```
[root@centos8 ~]# systemctl start httpd
[root@centos8 ~]# systemctl enable httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/
httpd.service.
[root@centos8 ~]# systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor preset: disabled)
   Active: active (running) since Tue 2020-12-01 03:11:20 EST; 15s ago
     Docs: man:httpd.service(8)
 Main PID: 9934 (httpd)
   Status: "Running, listening on: port 80"
    Tasks: 213 (limit: 11314)
   Memory: 35.4M
   CGroup: /system.slice/httpd.service
           ├─9934 /usr/sbin/httpd -DFOREGROUND
           ├─9935 /usr/sbin/httpd -DFOREGROUND
           ├─9936 /usr/sbin/httpd -DFOREGROUND
           ├─9937 /usr/sbin/httpd -DFOREGROUND
           └─9966 /usr/sbin/httpd -DFOREGROUND

Dec 01 03:11:19 centos8.linuxvmimages.local systemd[1]: Starting The Apache HTTP Server...
Dec 01 03:11:20 centos8.linuxvmimages.local systemd[1]: Started The Apache HTTP Server.
Dec 01 03:11:20 centos8.linuxvmimages.local httpd[9934]: Server configured, listening on: port 80
[root@centos8 ~]# _
```

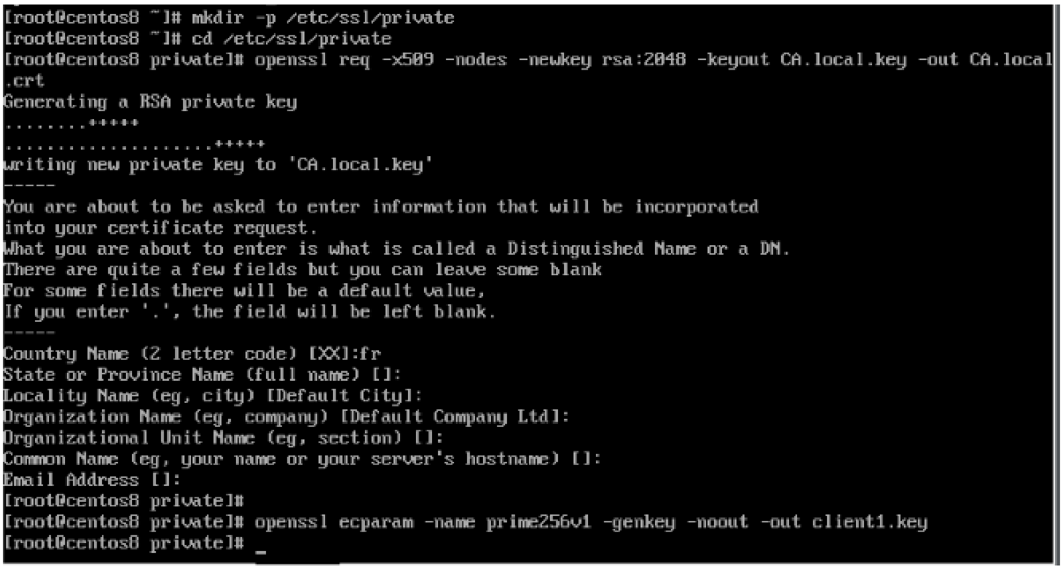
Now we are going to create https certificate for httpd server by installing SSL module using rpm command and we check the installation using the rpm command for both mod_ssl and openssl.



```
Installed:
  mod_ssl-1:2.4.37-21.module_el8.2.0+494+1df74eae.x86_64          sscg-2.3.3-14.el8.x86_64

Complete!
[root@centos8 ~]# rpm -q mod_ssl
mod_ssl-2.4.37-21.module_el8.2.0+494+1df74eac.x86_64
[root@centos8 ~]# rpm -q openssl
openssl-1.1.1c-15.el8.x86_64
[root@centos8 ~]# mkdir -p /etc/ssl/private
[root@centos8 ~]# cd /etc/ssl/private
[root@centos8 private]#
```

Now we create the directory for the Certificate authority (CA) . In the private directory we create certificate authority using the **OPENSSL** command along with **RSA** encryption with certificate and key for the encryption. The OpenSSL command will generate a 2048-bit RSA private key



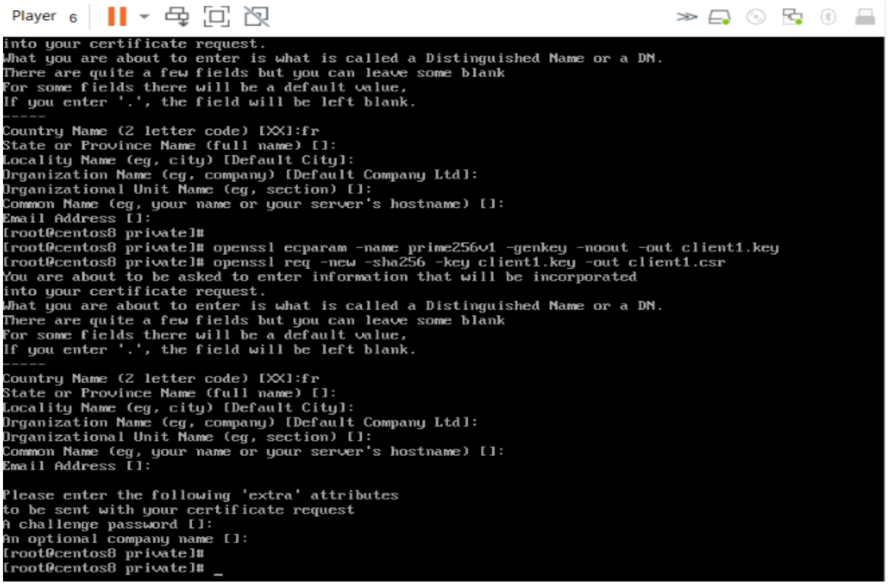
```
[root@centos8 ~]# mkdir -p /etc/ssl/private
[root@centos8 ~]# cd /etc/ssl/private
[root@centos8 private]# openssl req -x509 -nodes -newkey rsa:2048 -keyout CA.local.key -out CA.local
.crt
Generating a RSA private key
........+++++
....................+++++
writing new private key to 'CA.local.key'
-----
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) [XX]:fr
State or Province Name (full name) []:
Locality Name (eg, city) [Default City]:
Organization Name (eg, company) [Default Company Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:
Email Address []:
[root@centos8 private]#
[root@centos8 private]# openssl ecparam -name prime256v1 -genkey -noout -out client1.key
[root@centos8 private]# _
```

7 . using openssl command and ecparameters we generate key with the group name prime256v1 to client1.key file

8 . CSR stands for Certificate Signing Request. A **CSR contains** information such your organization's name, your domain name, and your location, and is filled out and submitted to a certificate authority

openssl req -new -sha256 -key client1.key -out client1.csr

The above command generates the new key called client1.key and generate the certificate signing request.



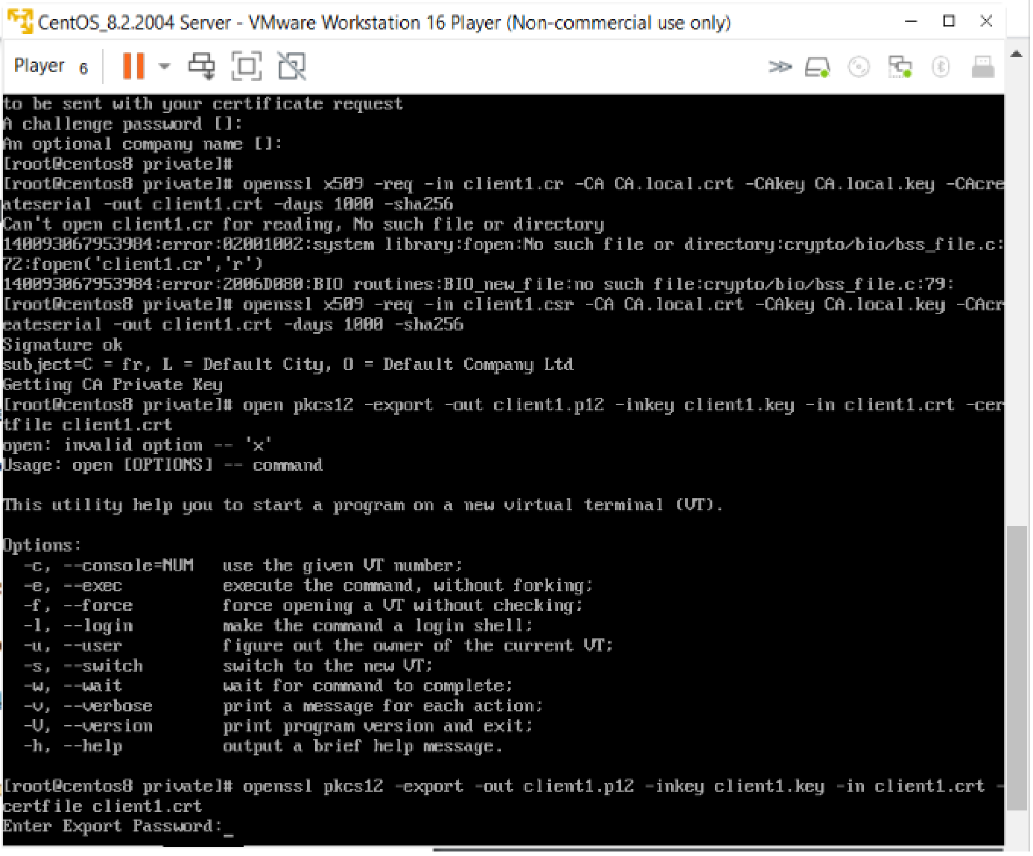
```
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:fr
State or Province Name (full name) []:
Locality Name (eg, city) [Default City]:
Organization Name (eg, company) [Default Company Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:
Email Address []:
[root@centos8 private]#
[root@centos8 private]# openssl ecparam -name prime256v1 -genkey -noout -out client1.key
[root@centos8 private]# openssl req -new -sha256 -key client1.key -out client1.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) [XX]:fr
State or Province Name (full name) []:
Locality Name (eg, city) [Default City]:
Organization Name (eg, company) [Default Company Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
[root@centos8 private]#
[root@centos8 private]# _
```

9 . The command

openssl x509 -req -in client1.csr -CA CA.local.crt -CAkey CA.local.key -CAcreateserial -out client1.crt -days 1000 -sha256

It ha the parameters that it required the client1.csr and then the local certificate key which will be valid for 1000 days under sha256 encryption method. And while exporting the password has been setup for the keys and certificates.


CentOS_8.2.2004 Server - VMware Workstation 16 Player (Non-commercial use only)
Player 6

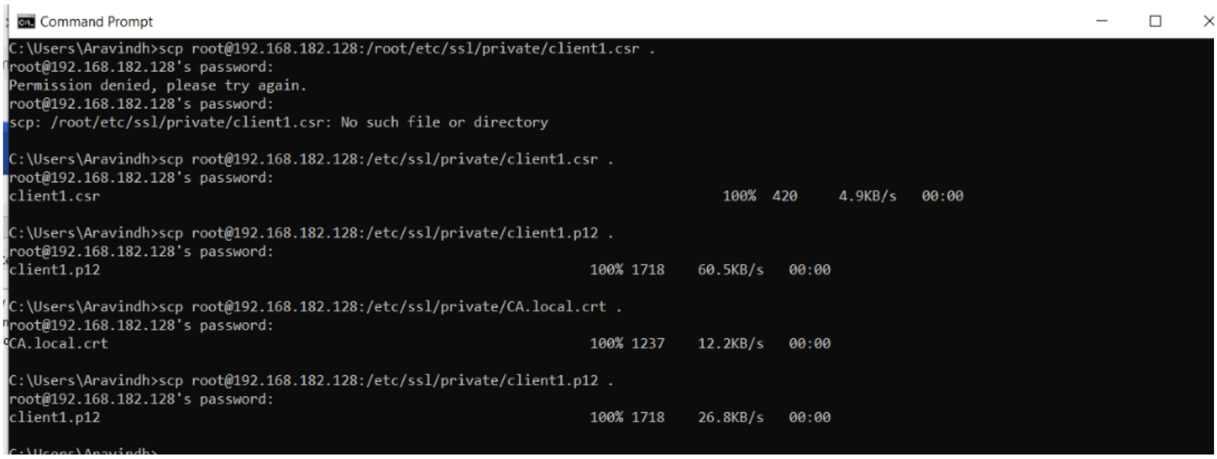
```
to be sent with your certificate request
A challenge password []:
An optional company name []:
[root@centos8 private]#
[root@centos8 private]# openssl x509 -req -in client1.cr -CA CA.local.crt -CAkey CA.local.key -CAcre
ateserial -out client1.crt -days 1000 -sha256
Can't open client1.cr for reading, No such file or directory
140093067953984:error:02001002:system library:fopen:No such file or directory:crypto/bio/bss_file.c:
72:fopen('client1.cr','r')
140093067953984:error:2006D080:BIO routines:BIO_new_file:no such file:crypto/bio/bss_file.c:79:
[root@centos8 private]# openssl x509 -req -in client1.csr -CA CA.local.crt -CAkey CA.local.key -CAcr
eateserial -out client1.crt -days 1000 -sha256
Signature ok
subject=C = fr, L = Default City, O = Default Company Ltd
Getting CA Private Key
[root@centos8 private]# open pkcs12 -export -out client1.p12 -inkey client1.key -in client1.crt -cer
tfile client1.crt
open: invalid option -- 'x'
Usage: open [OPTIONS] -- command

This utility help you to start a program on a new virtual terminal (VT).

Options:
  -c, --console=NUM   use the given VT number;
  -e, --exec          execute the command, without forking;
  -f, --force         force opening a VT without checking;
  -l, --login         make the command a login shell;
  -u, --user          figure out the owner of the current VT;
  -s, --switch        switch to the new VT;
  -w, --wait          wait for command to complete;
  -v, --verbose       print a message for each action;
  -V, --version       print program version and exit;
  -h, --help          output a brief help message.

[root@centos8 private]# openssl pkcs12 -export -out client1.p12 -inkey client1.key -in client1.crt -
certfile client1.crt
Enter Export Password:_
```

Now we copy the certificates from Linux VM to window using command prompt on host windows machine and downloaded to the location to import in the chrome



```
C:\Users\Aravindh>scp root@192.168.182.128:/root/etc/ssl/private/client1.csr .
root@192.168.182.128's password:
Permission denied, please try again.
root@192.168.182.128's password:
scp: /root/etc/ssl/private/client1.csr: No such file or directory

C:\Users\Aravindh>scp root@192.168.182.128:/etc/ssl/private/client1.csr .
root@192.168.182.128's password:
client1.csr                                                          100%  420     4.9KB/s   00:00

C:\Users\Aravindh>scp root@192.168.182.128:/etc/ssl/private/client1.p12 .
root@192.168.182.128's password:
client1.p12                                             100% 1718    60.5KB/s   00:00

C:\Users\Aravindh>scp root@192.168.182.128:/etc/ssl/private/CA.local.crt .
root@192.168.182.128's password:
CA.local.crt                                            100% 1237    12.2KB/s   00:00

C:\Users\Aravindh>scp root@192.168.182.128:/etc/ssl/private/client1.p12 .
root@192.168.182.128's password:
client1.p12                                             100% 1718    26.8KB/s   00:00

C:\Users\Aravindh>
```

12 . Go back to your web server and configure it for user authentication.

Add those lines in the https virtual host in /etc/httpd/conf.d/ssl.conf :

```
SSLOptions +StdEnvVars

SSLVerifyClient require

SSLCACertificateFile /etc/ssl/private/CA.local.crt
```

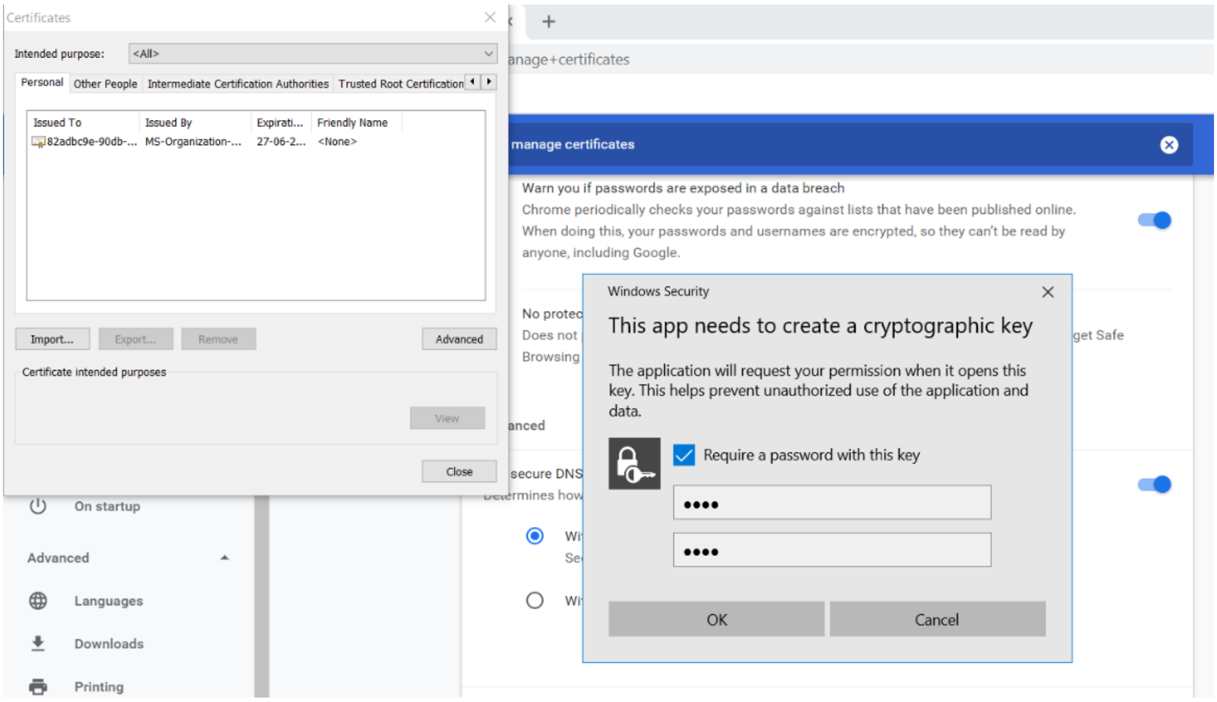
Now we configure the ssl.conf and opting to use our certificate for signing when used by the client to access the server in browser.

We set environment variables in SSLOption +StdEnvVars

Client verification is required and achieved by SSLVerifyClient require

Now we append the crt file or key to the ssl in order to make user sign with the corresponding generated certifiace.

Now we import the key and certificate in the chrome browser where the screenshots are below:



Certificates

Intended purpose: <All>

Issued To	Issued By	Expirati...	Friendly Name
82adbc9e-90db-...	MS-Organization-...	27-06-2...	<None>

manage certificates

Warn you if passwords are exposed in a data breach

Chrome periodically checks your passwords against lists that have been published online. When doing this, your passwords and usernames are encrypted, so they can't be read by anyone, including Google.

Windows Security

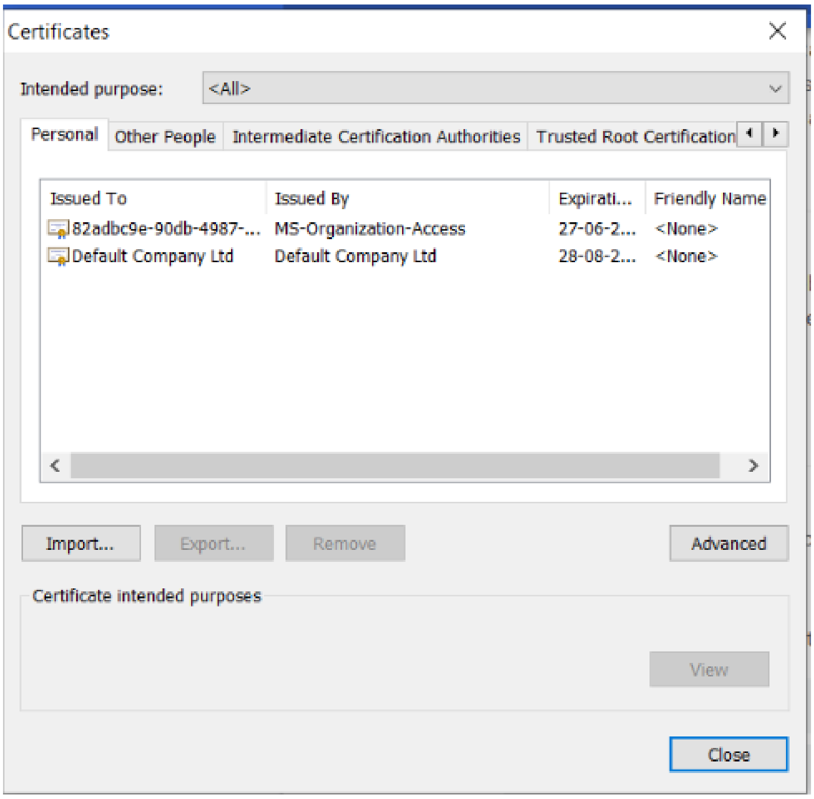
This app needs to create a cryptographic key

The application will request your permission when it opens this key. This helps prevent unauthorized use of the application and data.

☑ Require a password with this key

••••

••••



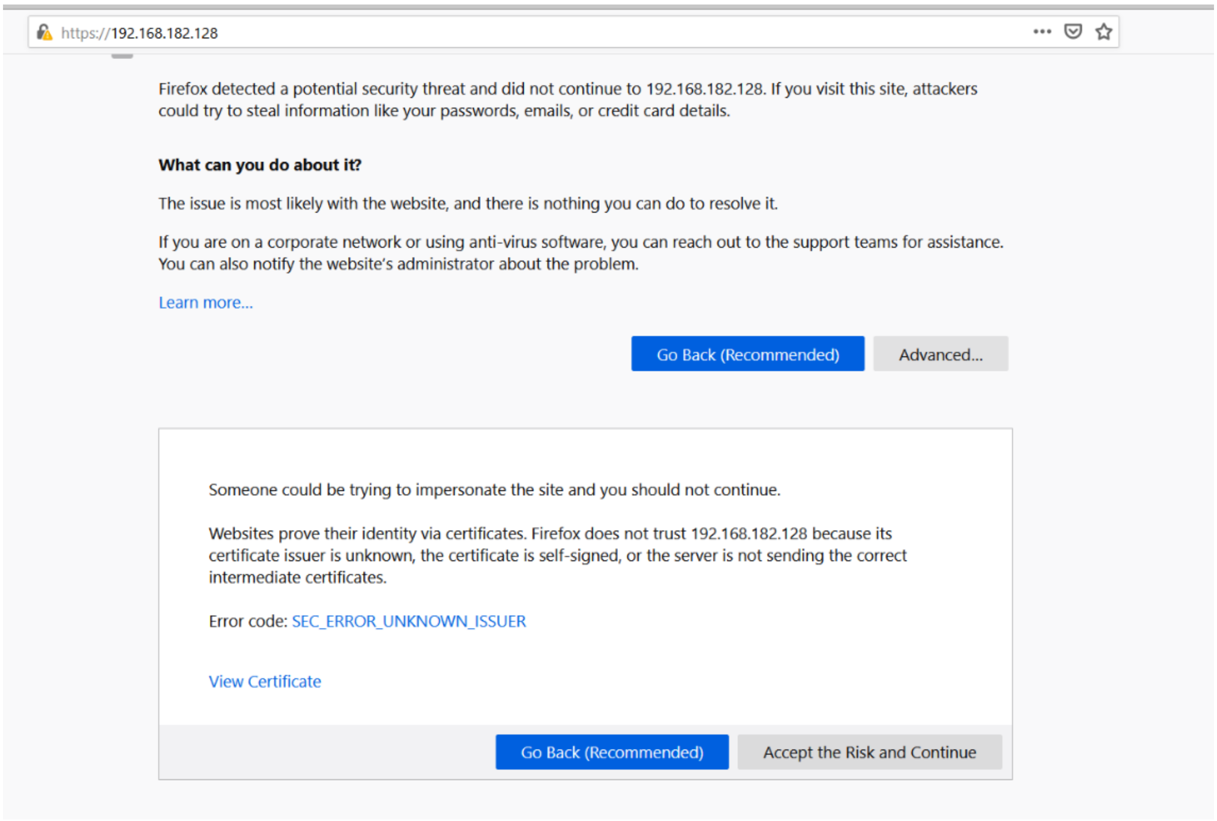
Certificates

Intended purpose: <All>

Issued To	Issued By	Expirati...	Friendly Name
82adbc9e-90db-4987-...	MS-Organization-Access	27-06-2...	<None>
Default Company Ltd	Default Company Ltd	28-08-2...	<None>

Personal
Other People
Intermediate Certification Authorities
Trusted Root Certification
Import...
Export...
Remove
Advanced
Certificate intended purposes
View
Close

14 . If we open in other browser than chrome in my case it will prompt for certificate signing request and you need to accept in order to open the server in the web browser.



https://192.168.182.128

Firefox detected a potential security threat and did not continue to 192.168.182.128. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

What can you do about it?

The issue is most likely with the website, and there is nothing you can do to resolve it.

If you are on a corporate network or using anti-virus software, you can reach out to the support teams for assistance. You can also notify the website's administrator about the problem.

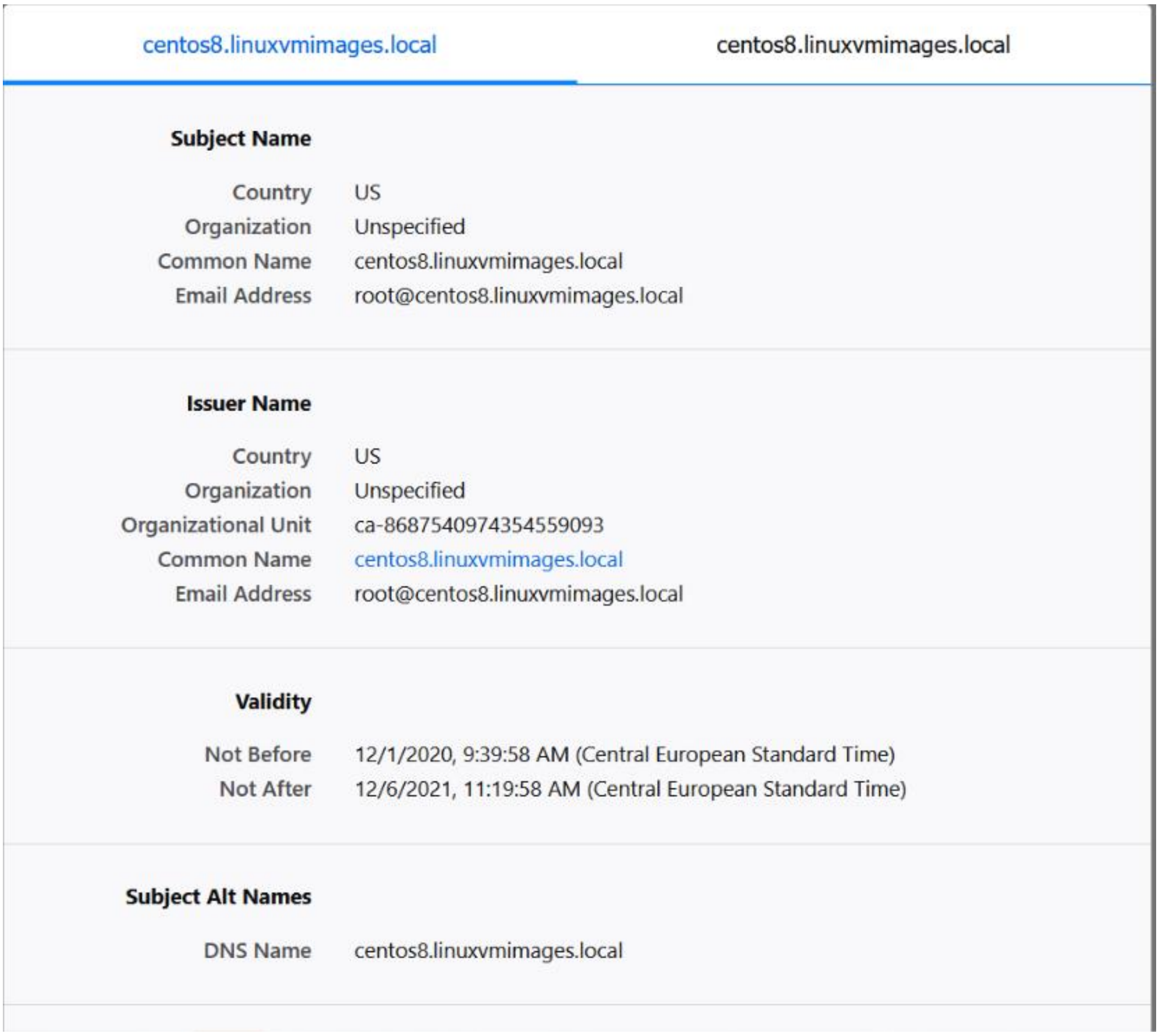
Learn more...

Someone could be trying to impersonate the site and you should not continue.

Websites prove their identity via certificates. Firefox does not trust 192.168.182.128 because its certificate issuer is unknown, the certificate is self-signed, or the server is not sending the correct intermediate certificates.

Error code: SEC_ERROR_UNKNOWN_ISSUER

View Certificate



centos8.linuxvmimages.local | centos8.linuxvmimages.local

Subject Name

Country	US
Organization	Unspecified
Common Name	centos8.linuxvmimages.local
Email Address	root@centos8.linuxvmimages.local

Issuer Name

Country	US
Organization	Unspecified
Organizational Unit	ca-8687540974354559093
Common Name	centos8.linuxvmimages.local
Email Address	root@centos8.linuxvmimages.local

Validity

Not Before	12/1/2020, 9:39:58 AM (Central European Standard Time)
Not After	12/6/2021, 11:19:58 AM (Central European Standard Time)

Subject Alt Names

DNS Name	centos8.linuxvmimages.local

15 . You fill out the appropriate forms add your public keys (they are just numbers) and send it/them to the certificate authority. (this is a **certificate Request**)The certificate authority does some checks (depends on authority), and sends you back the keys enclosed in a **certificate**.The certificate is **signed** by the **Issuing Certificate authority**, and this guarantees the keys.Now when someone wants your public keys, you send them the certificate, they **verify the signature** on the certificate, and if it verifies, then they can **trust your keys**.

16 . **Certificate**-based **authentication** is the use of a Digital **Certificate** to identify a user, machine, or device before granting access to a resource, network, application, etc. In the case of user **authentication**, it is often deployed in coordination with traditional methods such as username and password.