Installing EasyRSA

Package is available as a zip file.

https://github.com/OpenVPN/easy-rsa/releases

Version used for this document is 3.2.1

No standard installation procedure, simply unzip the file.

You should get such a directory:

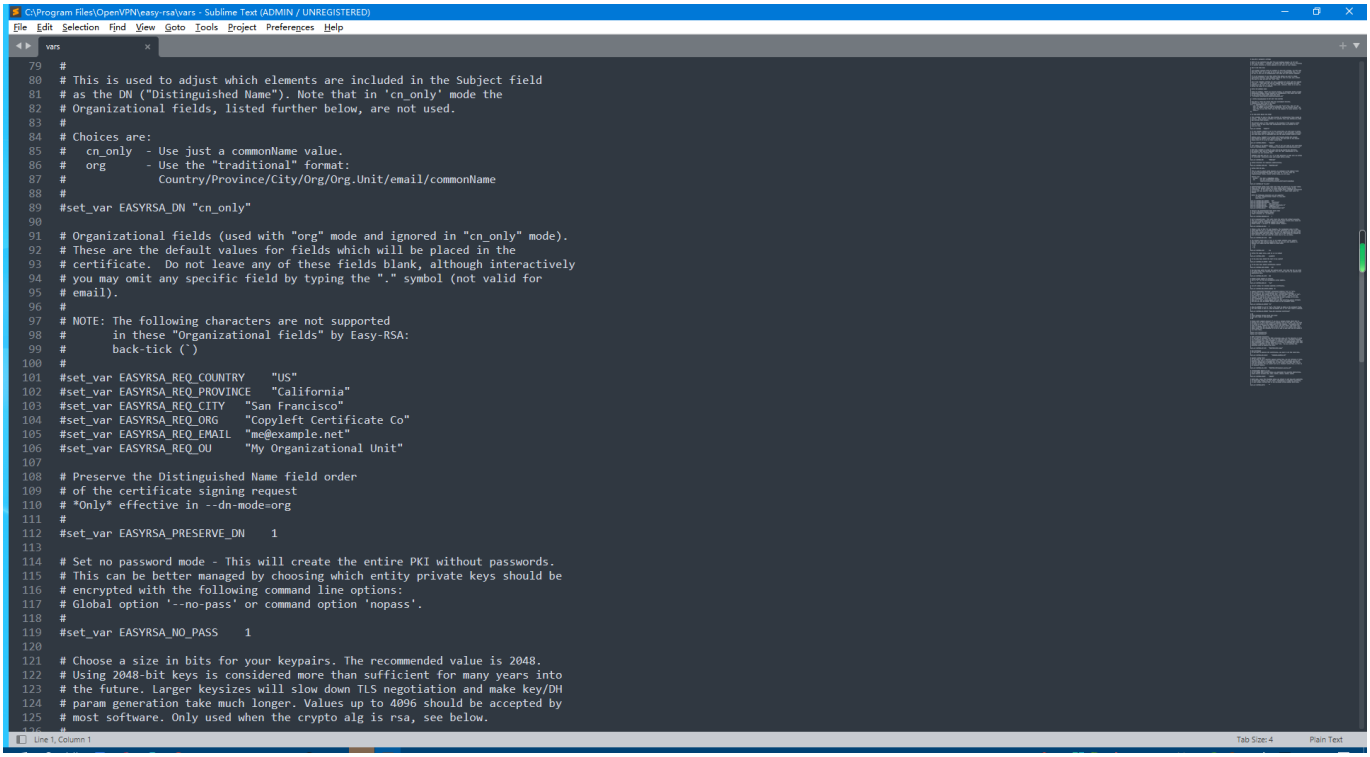
bin	9/16/2020 2:52 PM	File folder	
doc	9/16/2020 2:52 PM	File folder	
Licensing	9/16/2020 2:52 PM	File folder	
x509-types	9/16/2020 2:52 PM	File folder	
.rnd	1/21/2021 3:43 PM	RND File	1 KB
ChangeLog	9/16/2020 2:52 PM	File	5 KB
COPYING.html	9/16/2020 2:52 PM	Chrome HTML Docume...	2 KB
COPYING.md	9/16/2020 2:52 PM	MD File	2 KB
easyrsa	9/16/2020 2:52 PM	File	76 KB
EasyRSA-Start.bat	9/16/2020 2:52 PM	Windows Batch File	1 KB
libcrypto-1_1-x64.dll	9/16/2020 2:52 PM	Application extension	2,359 KB
libssl-1_1-x64.dll	9/16/2020 2:52 PM	Application extension	455 KB
openssl.exe	9/16/2020 2:52 PM	Application	653 KB
openssl-easyrsa.cnf	9/16/2020 2:52 PM	CNF File	5 KB
README.html	9/16/2020 2:52 PM	Chrome HTML Docume...	3 KB
README.quickstart.html	9/16/2020 2:52 PM	Chrome HTML Docume...	4 KB
README-Windows.txt	9/16/2020 2:52 PM	Text Document	5 KB
vars	1/21/2021 3:47 PM	File	9 KB
vars.example	1/21/2021 3:02 PM	EXAMPLE File	9 KB

This directory and all subdirectories should be archived in order to be able to create other certificates later if needed.

A copy of “vars.example” file can be edited and renamed “vars” if using default values is not desired.

For example, if you need to change validity of CA which is by default set to 10 years.

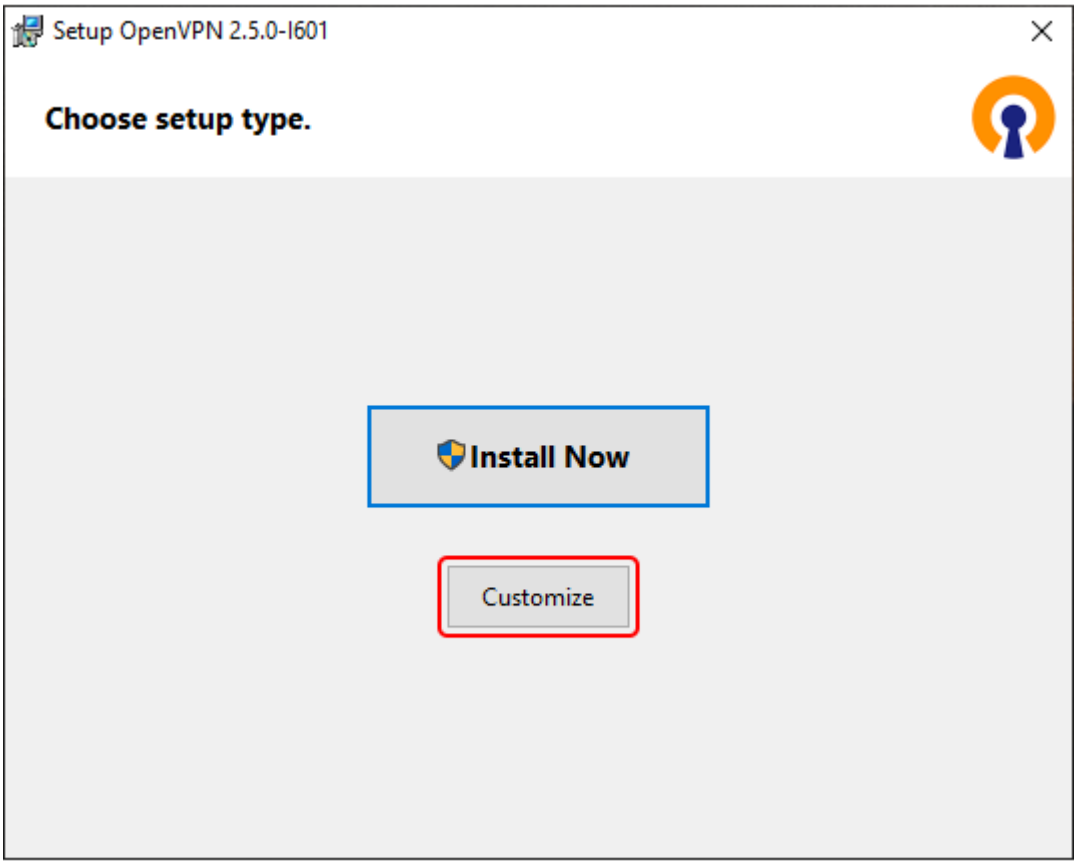
Same for certificates validity which is by default set to 825 days. Save your changes and close `vars`.

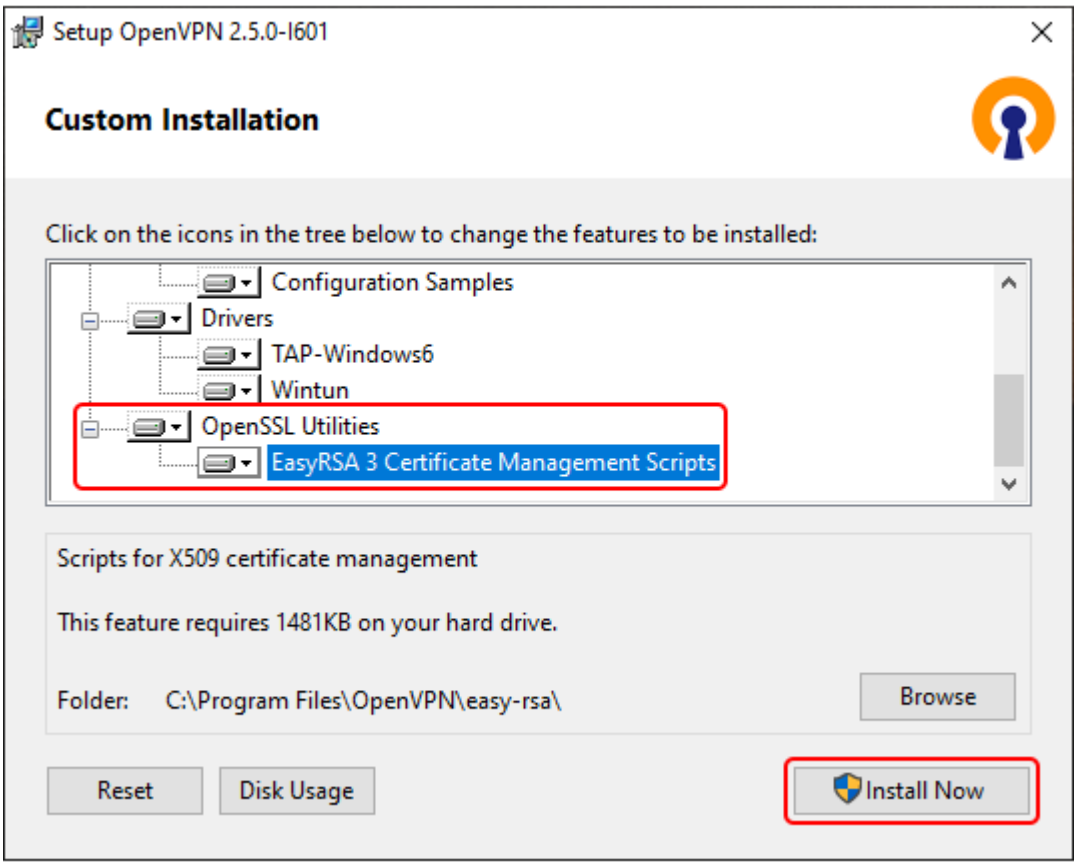


Or installing OpenVPN software

https://openvpn.net/community-downloads/

- Download an OpenVPN installer file from **here**.
  Run the downloaded file.
- Before starting the installation process, **click 'Customize'**:
- While in the 'Custom Installation' window, scroll down to **find OpenSSL Utilities → EasyRSA 3 Certificate Management Scripts**; make sure it is installed along with OpenVPN and **click 'Install Now'**:


Setup OpenVPN 2.5.0-I601
Choose setup type.
Install Now
Customize

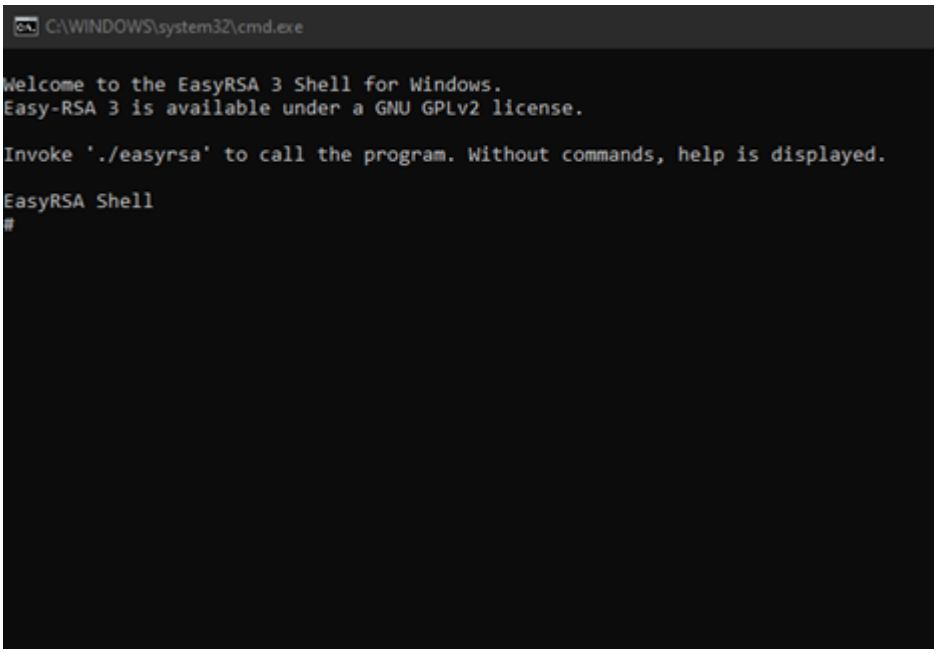

Setup OpenVPN 2.5.0-I601
Custom Installation
Click on the icons in the tree below to change the features to be installed:
Configuration Samples
Drivers
TAP-Windows6
Wintun
OpenSSL Utilities
EasyRSA 3 Certificate Management Scripts
Scripts for X509 certificate management
This feature requires 1481KB on your hard drive.
Folder: C:\Program Files\OpenVPN\easy-rsa\
Browse
Reset
Disk Usage
Install Now

Step 1, initialize PKI and create CA

Launch EasyRSA

Simply double-click on EasyRSA-Start.bat

A terminal window opens running EasyRSA shell.



Step 1, initialize PKI and create CA

Use commands:

```
./easyrsa init-pki
```

```
./easyrsa build-ca nopass
```

A “pki” subdirectory is then created, which contains among others the public certificate “ca.crt”.

The latter is used by the OpenVPN server and all clients.

PKI stands for Public Key Infrastructure.

You also have to give the name (common name or cn) of this certificate, used to authenticate the entity using this certificate.

Step 2, generate encryption key

Use command:

```
./easyrsa gen-dh
```

Be patient, it takes a while, as by default a 2048 bits key is generated.

The result file, “dh.pem” is located in “pki” folder.

It is used by the OpenVPN server.

Step 3, generate certificates for the OpenVPN server

Use command:

```
./easyrsa build-server-full <server-name> nopass
```

Replace `<SERVER_NAME>` with your server name. eg. `Server-01`
Option `nopass` can be used to disable password locking the key.

Result files are:

“server.crt” (public) in “issued” subfolder

“server.key” (private) in “private” subfolder

Step 4, generate certificates for each OpenVPN client

Use command for each openVPN client:

```
./easyrsa build-client-full <client-name> nopass
```

where is the authentication name (cn) for each clients

A password is required during this process in order to protect the use of the private key.

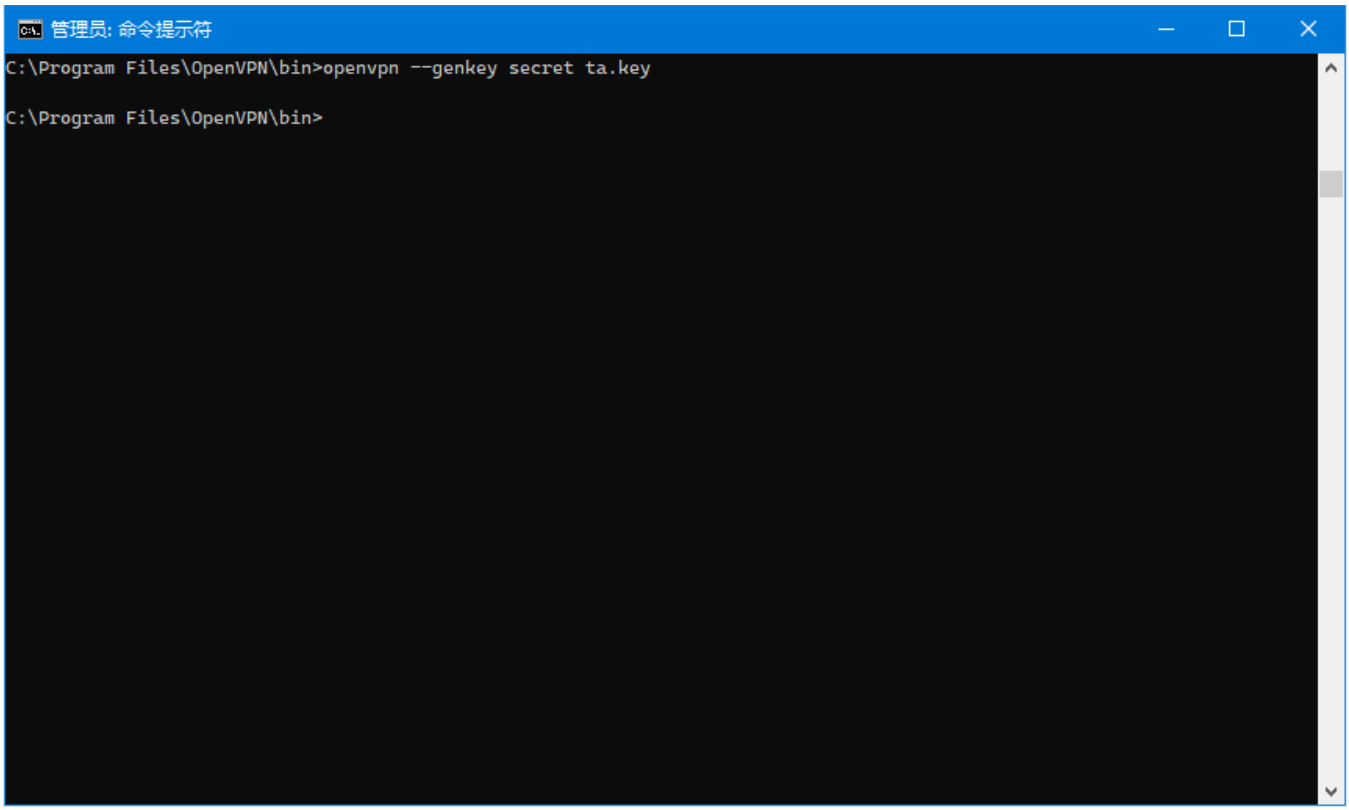
Result files are:

“.crt” (public) in “issued” subfolder

“.key” (private) in “private” subfolder

The password is the one used (PEM pass phrase) during corresponding certificate creation.

Step5,Generate a shared-secret key (Required when using tls-auth)



openvpn --genkey secret ta.key

In the server configuration

tls-auth ta.key 0

In the client configuration

tls-auth ta.key 1

client.ovpn

```
client
dev tun_c_ovpn
proto udp
remote 188.69.194.44 1194
resolv-retry infinite
keepalive 5 10
nobind
persist-key
persist-tun
verb 3
<ca>
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
</ca>
<cert>
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
</cert>
<key>
-----BEGIN PRIVATE KEY-----
-----END PRIVATE KEY-----
</key>
```