

# Installing EasyRSA

---

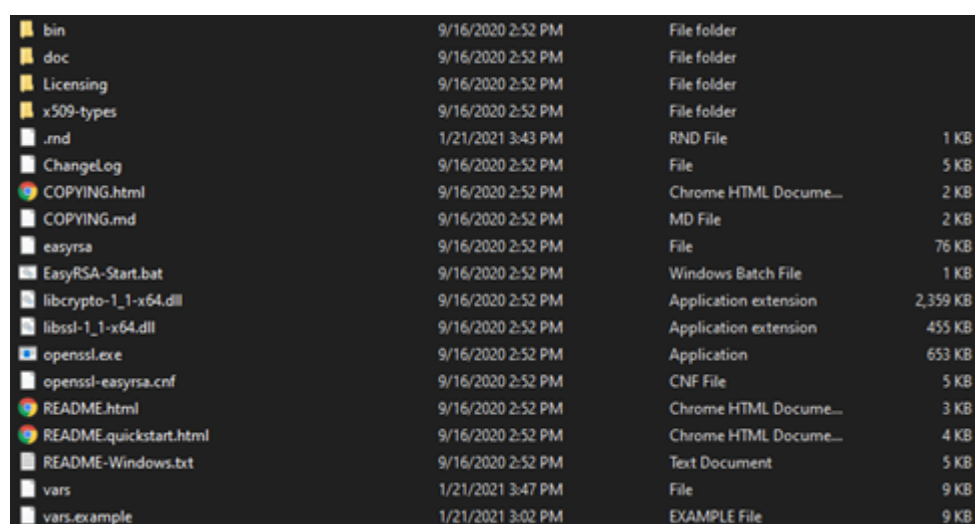
Package is available as a zip file.

<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.

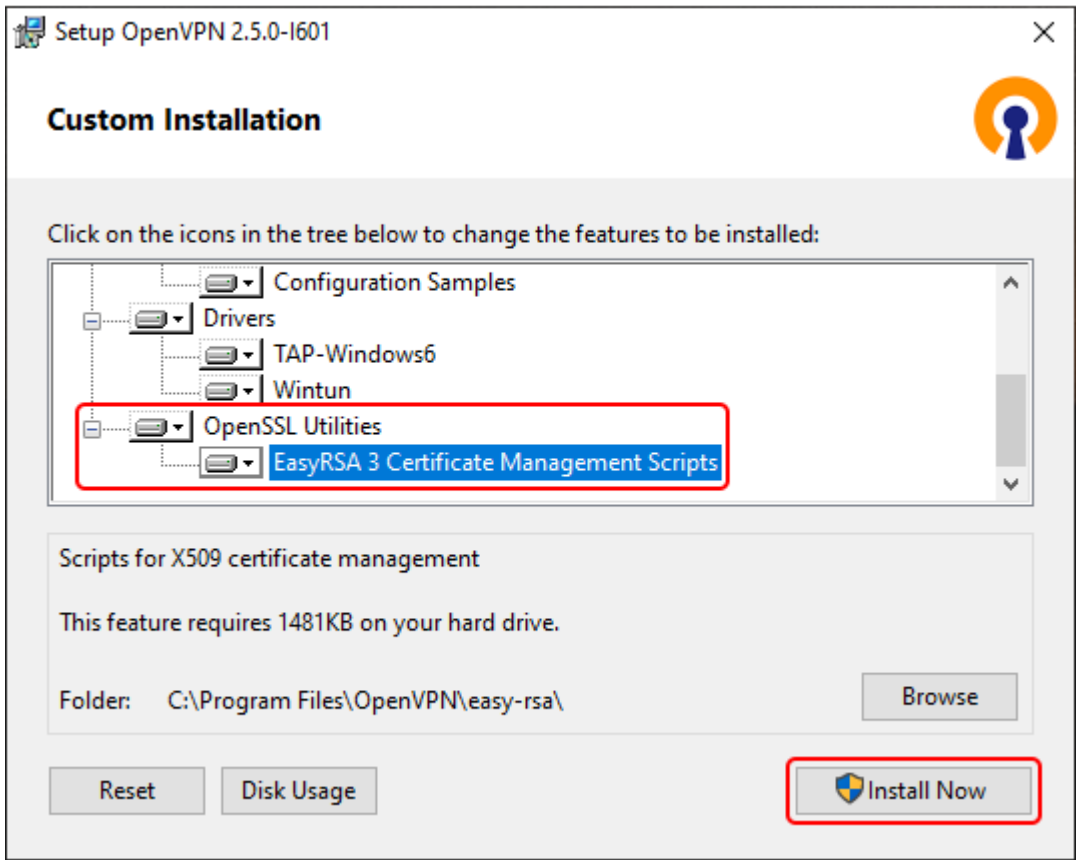
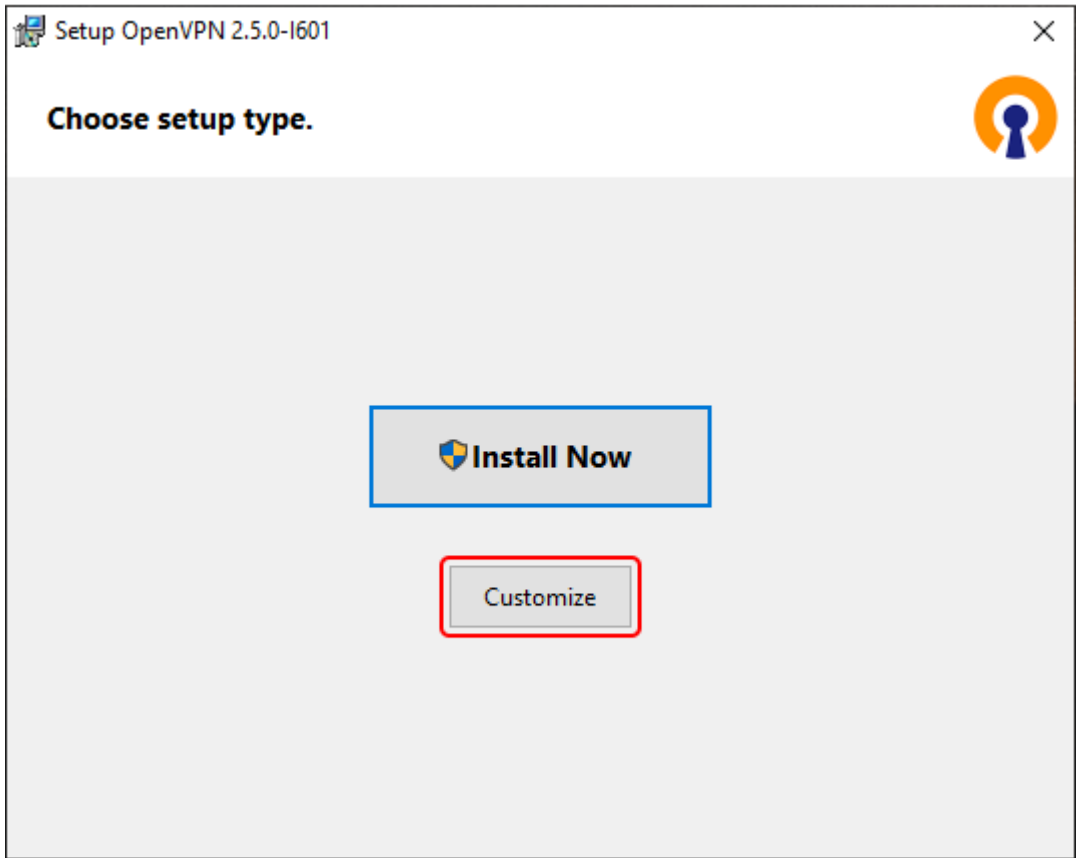
Same for certificates validity which is by default set to 825 days. Save your changes and close `vars`.

```
CAProgram Files\OpenVPN\easyrsa\ - Sublime Text (ADMIN / UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
vars
79 #
80 # This is used to adjust which elements are included in the Subject field
81 # as the DN ("Distinguished Name"). Note that in 'cn_only' mode the
82 # Organizational fields, listed further below, are not used.
83 #
84 # Choices are:
85 #   cn_only - Use just a commonName value.
86 #   org     - Use the "traditional" format:
87 #             Country/Province/City/Org/Org.Unit/email/commonName
88 #
89 #set_var EASYRSA_DN "cn_only"
90 #
91 # Organizational fields (used with "org" mode and ignored in "cn_only" mode).
92 # These are the default values for fields which will be placed in the
93 # certificate. Do not leave any of these fields blank, although interactively
94 # you may omit any specific field by typing the "." symbol (not valid for
95 # email).
96 #
97 # NOTE: The following characters are not supported
98 #       in these "Organizational fields" by Easy-RSA:
99 #       back-tick (`)
100 #
101 #set_var EASYRSA_REQ_COUNTRY  "US"
102 #set_var EASYRSA_REQ_PROVINCE "California"
103 #set_var EASYRSA_REQ_CITY    "San Francisco"
104 #set_var EASYRSA_REQ_ORG     "Copyleft Certificate Co"
105 #set_var EASYRSA_REQ_EMAIL   "me@example.net"
106 #set_var EASYRSA_REQ_OU      "My Organizational Unit"
107 #
108 # Preserve the Distinguished Name Field order
109 # of the certificate signing request
110 # *Only* effective in --dn-mode-org
111 #
112 #set_var EASYRSA_PRESERVE_DN  1
113 #
114 # Set no password mode - This will create the entire PKI without passwords.
115 # This can be better managed by choosing which entity private keys should be
116 # encrypted with the following command line options:
117 # Global option '--no-pass' or command option 'nopass'.
118 #
119 #set_var EASYRSA_NO_PASS      1
120 #
121 # Choose a size in bits for your keypairs. The recommended value is 2048.
122 # Using 2048-bit keys is considered more than sufficient for many years into
123 # the future. Larger key sizes will slow down TLS negotiation and make key/DN
124 # param generation take much longer. Values up to 4096 should be accepted by
125 # most software. Only used when the crypto alg is rsa, see below.
126 #
```

## 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':



## Step 1, initialize PKI and create CA

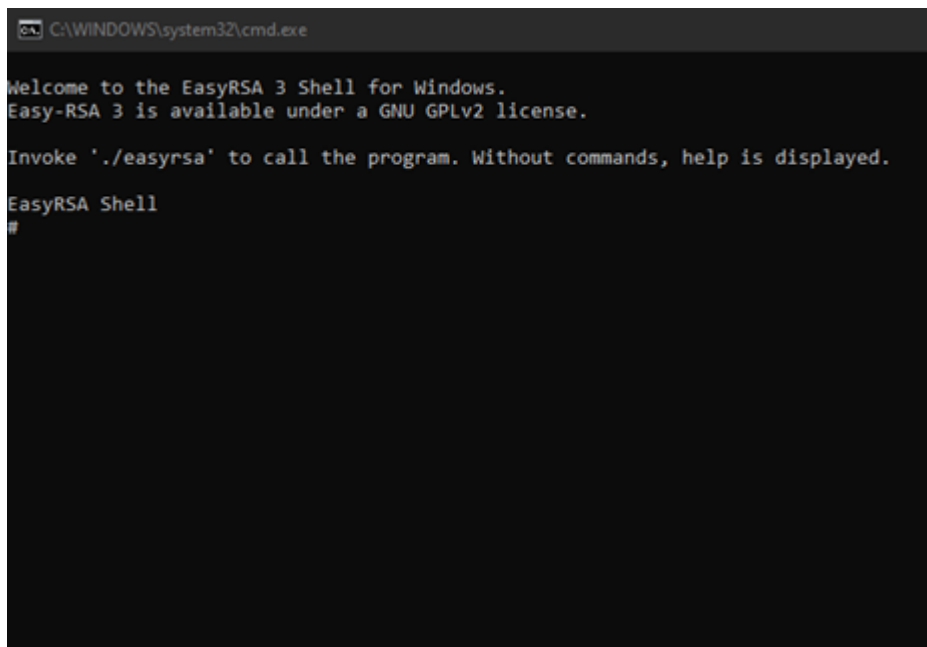
---

### Launch EasyRSA

---

Simply double-click on EasyRSA-Start.bat

A terminal window opens running EasyRSA shell.



```
C:\WINDOWS\system32\cmd.exe
Welcome to the EasyRSA 3 Shell for Windows.
Easy-RSA 3 is available under a GNU GPLv2 license.

Invoke './easysrsa' to call the program. Without commands, help is displayed.

EasyRSA Shell
#
```

## Step 1, initialize PKI and create CA

---

Use commands:

```
./easysrsa init-pki
```

```
./easysrsa 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:

```
./easymrsa 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:

```
./easymrsa 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:

```
./easymrsa 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.

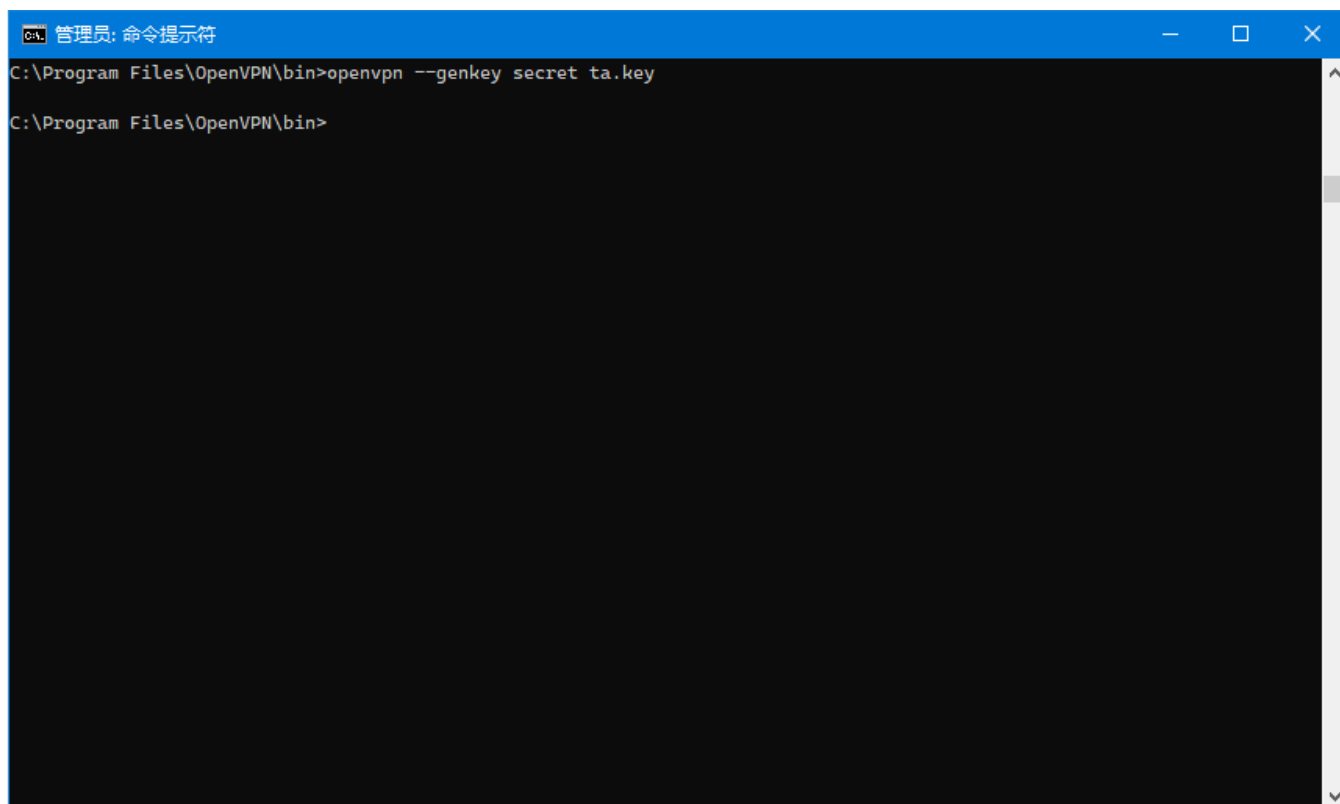
Result files are:

".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)



```
管理员: 命令提示符
C:\Program Files\OpenVPN\bin>openvpn --genkey secret ta.key
C:\Program Files\OpenVPN\bin>
```

```
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>
```