

# Create a root certificate

[Order now](#) | [Download](#) | [FAQ](#)

If you already have a root certificate ready, use certificate import. More in the [certificate import instructions](#) section.

Go to menu item **VPN servers -> IKEv2**

The screenshot shows the PUQVPNCP web interface. The top navigation bar includes 'Dashboard', 'VPN servers', 'VPN accounts', 'Settings', and 'About us'. The 'VPN servers' menu is expanded, showing 'WireGuard' and 'IKEv2' (highlighted). The 'IKEv2' configuration page is displayed, featuring a 'Save' button and an 'Advanced settings' link. The 'IKEv2 Enabled' dropdown is set to 'NO'. The 'Starter' status is 'not running' and the 'Charon' status is 'not running'. The 'ROOT certificate' section shows 'Certificate not found' and a 'Common name\*' field with the value 'TEST\_CN'. The 'Organization\*' field has the value 'TEST\_O'. The 'Organizational Unit' field has the value 'TEST\_OU'. The 'Locality' field has the value 'TEST\_L'. The 'State or Province Name' field has the value 'TEST\_S'. The 'Country Name' field has the value 'TEST\_C'. A 'Generate ROOT certificate' button is highlighted. The 'SERVER certificate' section shows 'Certificate not found' and a 'Server Domain\*' field. The 'ROOT certificate' section also includes an 'Import ROOT certificate and key' button. The 'CaCert' and 'CaKey' sections are empty. The 'SERVER certificate info' section shows 'Certificate not found'.

You need to fill in the required fields such as:

- Common name
- Organization

Then click the button **Generate ROOT certificate**

After these steps, the **root certificate and private key** will be generated.  
Information about the certificate will be available in the same place.

PUQVPNCP

? HELP ?ruslan (79.184.3.204)Logout

Dashboard

VPN servers

VPN accounts

Settings

About us

IKEv2

SaveAdvanced settings

IKEv2 Enabled  
NO

Starter: **not running**

Charon: **not running**

ROOT certificate  
certificate trusted, lifetimes valid

Delete ROOT certificate

SERVER certificate  
Certificate failed

Server Domain\*  
dev.softkeel.com

Server IP\*  
77.87.125.200

Common name\*  
dev.softkeel.com

Organization\*  
dev.softkeel.com

Organizational Unit  
TEST\_OU

Locality  
TEST\_L

State or Province Name  
TEST\_S

Country Name  
TEST\_S

Generate SERVER certificate

Successfully

ROOT certificate certificate trusted, lifetimes valid

Download CA certificateDownload CA key

subject: "CN=TEST\_CN, O=TEST\_O, OU=TEST\_OU, L=TEST\_L, S=TEST\_S, C=TEST\_C"  
issuer: "CN=TEST\_CN, O=TEST\_O, OU=TEST\_OU, L=TEST\_L, S=TEST\_S, C=TEST\_C"  
validity: not before Dec 13 10:13:17 2022, ok  
not after Dec 10 10:13:17 2032, ok (expires in 3650 days)  
serial: 25:c6:13:87:bd:f4:93:00  
flags: CA CRLSign self-signed  
subjkeyId: 0f:1b:3c:bf:78:91:27:b7:f0:3b:2a:d9:d6:a4:e1:d2:cd:8f:4e:45  
pubkey: RSA 4096 bits  
keyid: e9:a8:b9:45:fa:ee:5c:48:2e:e7:e5:8e:fa:33:46:4c:cb:8c:20:f4  
subjkey: 0f:1b:3c:bf:78:91:27:b7:f0:3b:2a:d9:d6:a4:e1:d2:cd:8f:4e:45

SERVER certificate info Certificate failed

To download the root certificate and private key, you can use the buttons **Download CA certificate** and **Download CA key**

To remove the root certificate, use the **Delete ROOT certificate** button

Revision #6

Created 13 December 2022 09:07:08 by Ruslan

Updated 16 October 2023 08:58:16 by Yuliia Noha