

08. IKEv2

Overview

IKEv2/IPsec is a standards-based VPN protocol with native support in most operating systems. PUQVPNC uses **strongSwan** as the IKEv2 implementation.

Key advantages:

- **No app required** — built into iOS, macOS, Windows, Android, Linux
- **MOBIKE support** — seamless switching between Wi-Fi and cellular without reconnection
- **Strong security** — certificate-based authentication with modern ciphers
- **Automatic reconnection** — reconnects transparently after network changes

IKEv2 is the best choice when you want **zero-install VPN** for end users — they can configure it using only the native OS settings.

“ **Requirement:** `strongswan` and `strongswan-pki` packages must be installed.

Global Settings

Navigate to **VPN Servers > IKEv2** to configure global IKEv2 settings.

PUQVPNC

Dashboard

Networks

Clients

VPN Servers

Diagnostics

Settings

About us

☀

🔗 Help

👤 admin (45.44.164.152)

🚪 Logout

IKEv2

Overview

Certificates

Advanced Settings

Networks

Online

Client Profiles

🛡️ Service Status

strongSwan

6.0.1-6+deb13u2

Starter

Running

PID: 3724658

Charon

Running

PID: 3724659

📜 Certificate Status

ROOT Certificate

Valid

certificate trusted, lifetimes valid

SERVER Certificate

Valid

certificate trusted, lifetimes valid

⚙️ Configuration

IKEv2 Enabled

YES

Server Domain

dev.puqvpncp.com

Server IP

77.87.125.201

Server IPv6

2a11:ff00::5

🔗 Online Connections

2

active connections

View all

IKEv2 global settings

Setting	Description
Enabled	Enable/disable IKEv2 globally
Ports	500 / 4500 UDP (standard IPsec ports)

Advanced Settings

PUQVPNCP

DashboardNetworks ▾Clients ▾VPN Servers ▾Diagnostics ▾Settings ▾About us

⚙️🔗 Help ▾👤 admin (45.44.164.152)🚪 Logout

IKEv2

✓

OverviewCertificatesAdvanced SettingsNetworksOnlineClient Profiles

25 ▾entries per page

Filter:

Name	Status	Username	AllowedIPs	Endpoint	Uptime	Bandwidth	Server	
client_1	Enable	user1	10.0.0.2	45.44.164.152	24 seconds ago	1M / 1M	IETS	
client_2	Enable	user2	10.0.0.3	45.44.164.152	34 seconds ago	3M / 3M	IETS	

Showing 1 to 2 of 2 entries

⏪

⏴

1

⏵

⏩

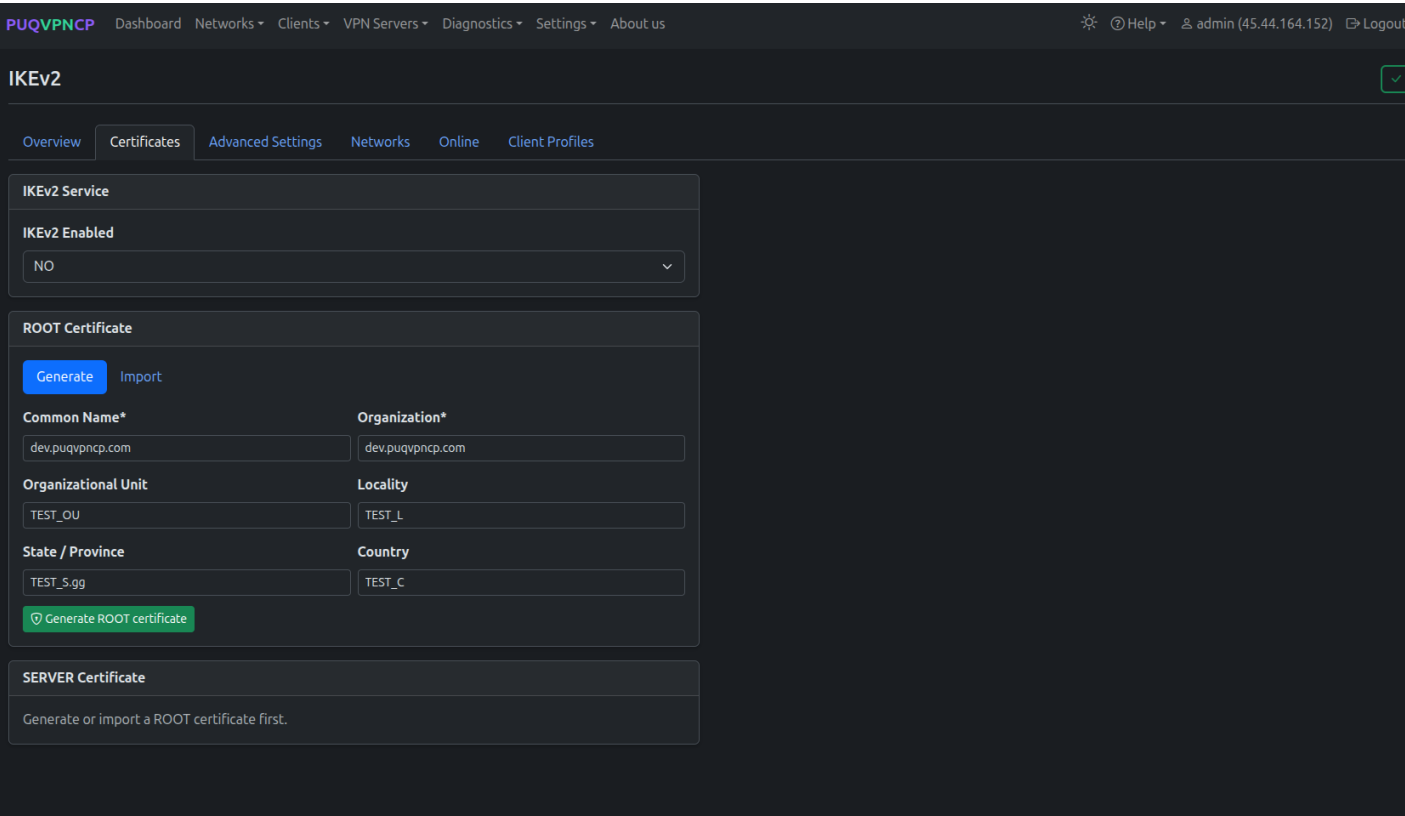
IKEv2 advanced settings

Setting	Description	Default
ESP	ESP encryption proposals	aes256gcm128-sha256
IKE	IKE encryption proposals	aes256-sha256-modp2048
IKE Lifetime (sec)	IKE SA lifetime	86400
Lifetime (sec)	Child SA lifetime	3600
DPD Delay	Dead Peer Detection interval	30
DPD Timeout	DPD timeout	150

Certificates

IKEv2 uses X.509 certificates for server authentication. PUQVPNCP manages the full PKI chain.

Root Certificate (CA)



IKEv2 Root CA certificate

The Root CA is created once and signs all server certificates. Clients must trust this CA.

Server Certificate

PUQVPNCP

Dashboard

Networks

Clients

VPN Servers

Diagnostics

Settings

About us

☀️ ⓘ Help

👤 admin (45.44.164.152)

🚪 Logout

IKEv2

✓

Overview

Certificates

Advanced Settings

Networks

Online

Client Profiles

IKEv2 Service

IKEv2 Enabled

NO

ROOT Certificate

Valid certificate trusted, lifetimes valid

Download CA cert

Download CA key

Delete

SERVER Certificate

Server Domain*

dev.puqvpncp.com

Server IP*

77.87.125.201

Server IPv6

2a11:ff00::5

Common Name*

dev.puqvpncp.com

Organization*

dev.softkeel.com

Organizational Unit

TEST_OU

Locality

TEST_L

State / Province

TEST_S

Country

TEST_S

Certificate Details

ROOT Certificate

subject: "CN=dev.puqvpncp.com, O=dev.puqvpncp.com, OU=TEST_OU, L=TEST_L, ST=TEST_S.eg, C=TEST_C"
issuer: "CN=dev.puqvpncp.com, O=dev.puqvpncp.com, OU=TEST_OU, L=TEST_L, ST=TEST_S.eg, C=TEST_C"
validity: not before Mar 10 19:43:24 2026, ok
not after Mar 07 19:43:24 2036, ok (expires in 3650 days)
serial: 45:43:8a:82:4b:20:69:fe
flags: CA CRLSign self-signed
subjkeyId: 54:8b:dd:43:53:73:c0:6a:00:f9:21:4d:14:6e:8b:07:de:2c:53:2a
pubkey: RSA 4096 bits
keyId: 26:16:78:81:1a:30:8a:4b:d0:1e:be:ab:34:7f:f5:32:2b:07:13:12
subjkey: 54:8b:dd:43:53:73:c0:6a:00:f9:21:4d:14:6e:8b:07:de:2c:53:2a

IKEv2 server certificate

The server certificate is signed by the Root CA and presented to clients during the IKE handshake.

“ **Important:** The server certificate's Subject Alternative Name (SAN) must match the VPN Domain or server IP.

Import Certificate

PUQVPNCP

DashboardNetworks ▾Clients ▾VPN Servers ▾Diagnostics ▾Settings ▾About us

☀️🔗 Help ▾👤 admin (45.44.164.152)🔑 Logout

OverviewCertificatesAdvanced SettingsNetworksOnlineClient Profiles

IKEv2 Service

IKEv2 Enabled

NO ▾

ROOT Certificate

Valid

certificate trusted, lifetimes valid

Download CA cert

Download CA key

Delete

SERVER Certificate

Server Domain*

dev.puqvpncp.com

Server IP*

77.87.125.201

Server IPv6

2a11:ff00::5

Common Name*

dev.puqvpncp.com

Organization*

dev.softkeel.com

Organizational Unit

TEST_OU

Locality

TEST_L

State / Province

TEST_S

Country

TEST_S

Generate SERVER certificate

Certificate Details

ROOT Certificate

subject: "CN=dev.puqvpncp.com, O=dev.puqvpncp.com, OU=TEST_OU, L=TEST_L, ST=TEST_S,gg, C=TEST_C"

issuer: "CN=dev.puqvpncp.com, O=dev.puqvpncp.com, OU=TEST_OU, L=TEST_L, ST=TEST_S,gg, C=TEST_C"

validity: not before Mar 10 19:43:24 2026, ok

not after Mar 07 19:43:24 2036, ok (expires in 3650 days)

serial: 45:43:8a:82:4b:20:69:fe

flags: CA CRLSign self-signed

subjKeyId: 54:8b:dd:43:53:73:c0:6a:00:f9:21:4d:14:6e:8b:07:de:2c:53:2a

pubkey: RSA 4096 bits

keyid: 36:16:78:81:1a:38:8a:4b:d0:1e:be:ab:34:7f:f5:32:2b:07:13:12

subjkey: 54:8b:dd:43:53:73:c0:6a:00:f9:21:4d:14:6e:8b:07:de:2c:53:2a

Import existing CA and server certificates

If you have existing certificates from another strongSwan installation, you can import them instead of generating new ones.

DNS

PUQVPNCP

Dashboard

Networks

Clients

VPN Servers

Diagnostics

Settings

About us

Help

admin (45.44.164.152)

Logout

IKEv2

Overview

Certificates

Advanced Settings

Networks

Online

Client Profiles

IKEv2 Service

IKEv2 Enabled

YES

ROOT Certificate

Valid

certificate trusted, lifetimes valid

Download CA cert

Download CA key

Delete

SERVER Certificate

Valid

certificate trusted, lifetimes valid

Delete SERVER certificate

Certificate Details

ROOT Certificate

subject: "CN=dev.puqvpncp.com, O=dev.puqvpncp.com, OU=TEST_OU, L=TEST_L, ST=TEST_S,gg, C=TEST_C" issuer: "CN=dev.puqvpncp.com, O=dev.puqvpncp.com, OU=TEST_OU, L=TEST_L, ST=TEST_S,gg, C=TEST_C" validity: not before Mar 10 19:43:24 2026, ok not after Mar 07 19:43:24 2036, ok (expires in 3649 days) serial: 45:43:8a:82:4b:20:69:fe flags: CA CRLSign self-signed subjkeyId: 54:8b:dd:43:53:73:c0:6a:00:f9:21:4d:14:6e:8b:07:de:2c:53:2a pubkey: RSA 4096 bits keyid: 36:16:78:81:1a:38:8a:4b:d0:1e:be:ab:34:7f:f5:32:2b:07:13:12 subjkey: 54:8b:dd:43:53:73:c0:6a:00:f9:21:4d:14:6e:8b:07:de:2c:53:2a

SERVER Certificate

subject: "CN=dev.puqvpncp.com, O=dev.softkeel.com, OU=TEST_OU, L=TEST_L, ST=TEST_S, C=TEST_S" issuer: "CN=dev.puqvpncp.com, O=dev.puqvpncp.com, OU=TEST_OU, L=TEST_L, ST=TEST_S,gg, C=TEST_C" validity: not before Mar 10 19:43:44 2026, ok not after Mar 09 19:43:44 2031, ok (expires in 1824 days) serial: 73:9c:2c:0c:f8:52:d9:f7 altNames: dev.puqvpncp.com, 77.87.125.201, 2a11:ff00::5 flags: serverAuth ikeIntermediate authkeyId: 54:8b:dd:43:53:73:c0:6a:00:f9:21:4d:14:6e:8b:07:de:2c:53:2a subjkeyId: 9d:28:fe:2d:84:54:7f:a8:11:75:74:42:85:ac:e4:63:6d:42:18:18 pubkey: RSA 4096 bits keyid: f4:27:73:5c:01:00:33:59:db:67:2b:24:c8:87:cd:70:9a:fc:2b:46 subjkey: 9d:28:fe:2d:84:54:7f:a8:11:75:74:42:85:ac:e4:63:6d:42:18:18

IKEv2 DNS configuration

Configure DNS servers pushed to IKEv2 clients.

Status

PUQVPNCP

Dashboard

Networks

Clients

VPN Servers

Diagnostics

Settings

About us

Help

admin (45.44.164.152)

Logout

IKEv2

Overview

Certificates

Advanced Settings

Networks

Online

Client Profiles

Restore defaults

config setup

Uniqueidsno

Strictrcpolicyno

charondebug

Charon debugging output log levels

dmn0 (audit)

ike0 (audit)

job0 (audit)

knl0 (audit)

asn0 (audit)

lib0 (audit)

tls0 (audit)

imc0 (audit)

pts0 (audit)

mgr0 (audit)

chd0 (audit)

cfg0 (audit)

net0 (audit)

enc0 (audit)

esp0 (audit)

tnc0 (audit)

imv0 (audit)

conn default

Authbypubkey

Closeactionnone

Compressno

Dpdactionclear

Dpddelay300

Dpddelay300

Dpddelay300

Dpddelay300

Inactivity86400

Espaes256-sha256,chacha20poly1305-sha512,aes256-sha1,aes256gcm16-ecp

Forceencapsyes

Fragmentationyes

Ikeaes256-sha1-modp1024,aes128-sha1-modp1024,chacha20poly1305-sha512

Ikelifetime86400

Installpolicyyes

Keyingtries5

Lifetime3600

Margintime600

IKEv2 service status

Shows the strongSwan daemon status, starter and charon PIDs, and current active SAs.

Online Users

PUQVPNCP

Dashboard

Networks

Clients

VPN Servers

Diagnostics

Settings

About us

Help

admin (45.44.164.152)

Logout

IKEv2

Overview

Certificates

Advanced Settings

Networks

Online

Client Profiles

25 entries per page

Filter:

Name	Clients	Network	Bandwidth
loadtest_net10	100	10.100.9.0/24	∞ / ∞
loadtest_net11	99	10.100.10.0/24	∞ / ∞
loadtest_net12	100	10.100.11.0/24	∞ / ∞
loadtest_net13	100	10.100.12.0/24	∞ / ∞
loadtest_net14	95	10.100.13.0/24	∞ / ∞
TETS	4	10.0.0.0/24	3M / 3M

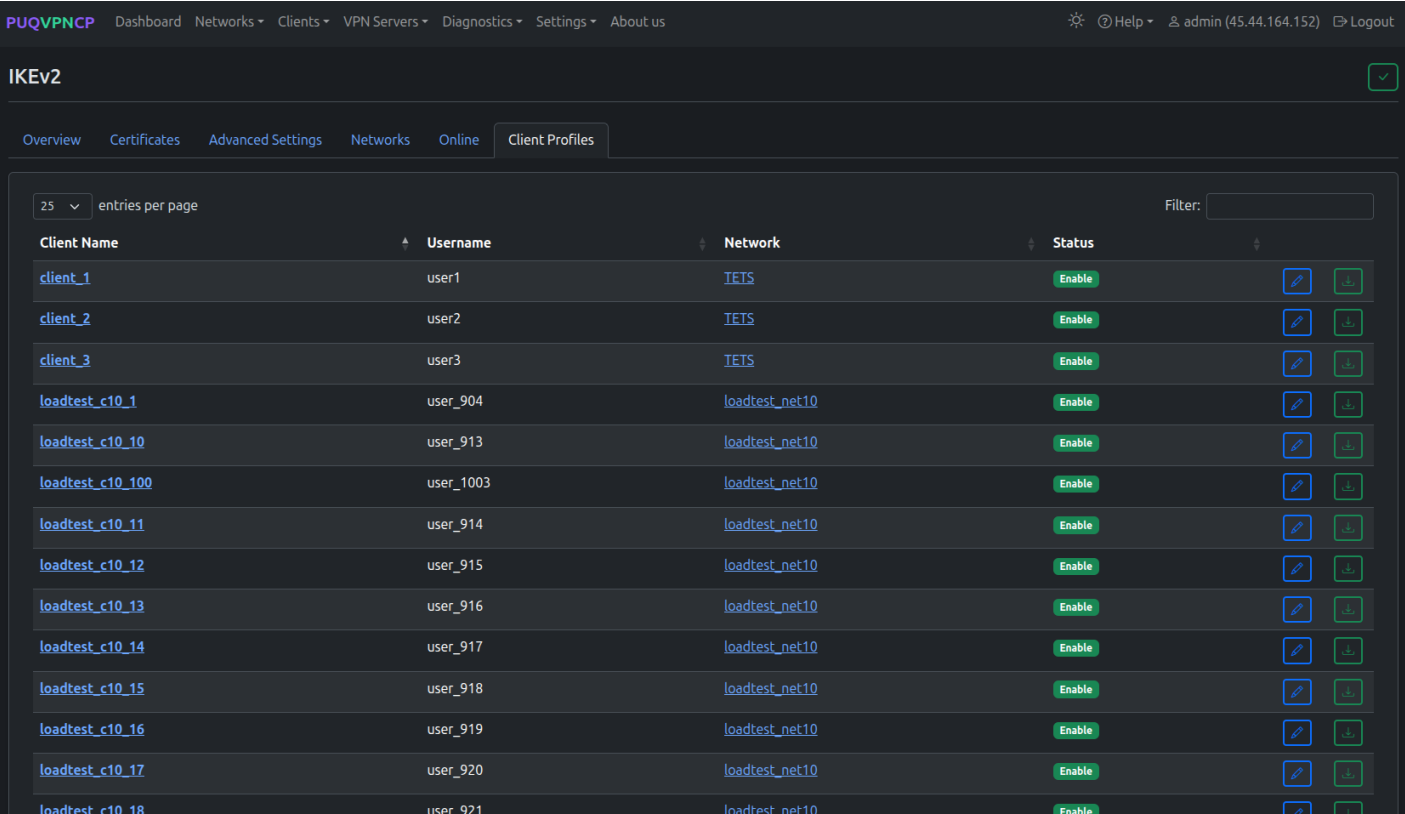
Showing 1 to 6 of 6 entries

IKEv2 online users

Lists all active IKEv2 security associations with:

- Client name and network
- Virtual IP assigned
- Remote (real) IP
- IKE and ESP proposals in use
- Connection duration

Client Profiles



IKEv2 client profiles — all clients across all networks

Lists all IKEv2 clients across all networks:

Column	Description
Client Name	Client name (link to client page)
Username	System user who owns this client
Network	Network this client belongs to
Status	Enable/Disable

Each client row has buttons to edit the client and download the `.sswan` configuration file.

Client Configuration

IKEv2 clients authenticate using **username/password** (EAP-MSCHAPv2) with server certificate validation.

Configuration by Platform

Platform	Method
----------	--------

iOS	Settings > VPN > Add Configuration > IKEv2. Or import <code>.mobileconfig</code> profile
macOS	System Preferences > Network > + > VPN > IKEv2
Windows	Settings > Network > VPN > Add VPN > IKEv2
Android	Settings > VPN > + > IKEv2/IPsec MSCHAPv2 (or use strongSwan app)
Linux	NetworkManager or <code>charon-cmd</code>

Required Client Settings

Field	Value
Server	Your VPN domain or IP
Remote ID	Same as server (domain or IP)
Authentication	Username (EAP)
Username / Password	From client's IKEv2 tab
CA Certificate	The Root CA certificate (download from panel)

“ **Tip:** Use **One-Time Links** to give users a downloadable `.sswan` profile that imports all settings automatically.

Per-Network Configuration

Each network can override the global IKEv2 settings:

- ESP and IKE proposals
- SA lifetimes
- DPD delay and timeout

See the IKEv2 tab in [Networks](#) for details.

Revision #39

Created 11 December 2022 06:27:23 by Ruslan

Updated 28 September 2026 23:33:16 by Ruslan