Client Export Utility   ❓

Server   Client   Client Specific Overrides   Wizards   Client Export

OpenVPN Server

Remote Access Server

OpenVPNTestServer UDP4:1194 ⌄

Client Connection Behavior

Host Name Resolution

Interface IP Address ⌄

Verify Server CN

Automatic - Use verify-x509-name where possible ⌄

Optionally verify the server certificate Common Name (CN) when the client connects.

Block Outside DNS

☐ Block access to DNS servers except across OpenVPN while connected, forcing clients to use only VPN DNS servers.

Requires Windows 10 and OpenVPN 2.3.9 or later. Only Windows 10 is prone to DNS leakage in this way, other clients will ignore the option as they are not affected.

Legacy Client

☐ Do not include OpenVPN 2.5 and later settings in the client configuration.

When using an older client (OpenVPN 2.4.x), check this option to prevent the exporter from placing known-incompatible settings into the client configuration.

Silent Installer

☐ Create Windows installer for unattended deploy.

Create a silent Windows installer for unattended deploy; installer must be run with elevated permissions. Since this installer is not signed, you may need special software to deploy it correctly.

Bind Mode

Do not bind to the local port ⌄

If OpenVPN client binds to the default OpenVPN port (1194), two clients may not run concurrently.

Certificate Export Options

PKCS#11 Certificate Storage

☐ Use PKCS#11 storage device (cryptographic token, HSM, smart card) instead of local files.

Microsoft Certificate Storage

☐ Use Microsoft Certificate Storage instead of local files.

Password Protect Certificate

☐ Use a password to protect the PKCS#12 file contents or key in Viscosity bundle.

PKCS#12 Encryption

High: AES-256 + SHA256 (pfSense Software, FreeBSD, Linux, Windows 10)   ⌄

Select the level of encryption to use when exporting a PKCS#12 archive. Encryption support varies by Operating System and program

Proxy Options

Use A Proxy

☐ Use proxy to communicate with the OpenVPN server.

Advanced

Additional configuration options

Enter any additional options to add to the OpenVPN client export configuration here, separated by a line break or semicolon.

EXAMPLE: remote-random;

[💾 Save as default]

Search ⊖

Search term

[Q Search] [↺ Clear]

Enter a search string or *nix regular expression to search.

OpenVPN Clients

User	Certificate Name	Export
CSVPNUser2	OpenVPNUser2-Cert	- Inline Configurations:

- Inline Configurations:
  - Most Clients
  - Android
  - OpenVPN Connect (iOS/Android)
- Bundled Configurations:
  - Archive
  - Config File Only
- Current Windows Installers (2.6.7-Ix001):
  - 64-bit
  - 32-bit
- Previous Windows Installers (2.5.9-Ix601):
  - 64-bit
  - 32-bit
- Legacy Windows Installers (2.4.12-Ix601):
  - 10/2016/2019
  - 7/8/8.1/2012r2
- Viscosity (Mac OS X and Windows):
  - Viscosity Bundle
  - Viscosity Inline Config

Only OpenVPN-compatible user certificates are shown

If a client is missing from the list it is likely due to a CA mismatch between the OpenVPN server instance and the client certificate, the client certificate does not exist on this firewall, or a user certificate is not associated with a user when local database authentication is enabled.

Clients using OpenSSL 3.0 may not work with older or weaker ciphers and hashes, such as SHA1, including when those were used to sign CA and certificate entries.

OpenVPN 2.4.8+ requires Windows 7 or later

Links to OpenVPN clients for various platforms:

OpenVPN Community Client - Binaries for Windows, Source for other platforms. Packaged above in the Windows Installers
OpenVPN For Android - Recommended client for Android
OpenVPN Connect: Android (Google Play) or iOS (App Store) - Recommended client for iOS
Viscosity - Recommended commercial client for Mac OS X and Windows
Tunnelblick - Free client for OS X
Using the Latest OpenVPN on Linux Distros - Install OpenVPN using the OpenVPN apt repositories to get the latest version, rather than one included with distributions.