



VPN Client

6.8.0

for Windows

Release Notes

Contents

- [About this release](#) on page 2
- [System requirements](#) on page 2
- [Build number and checksums](#) on page 2
- [Compatibility](#) on page 3
- [Enhancements](#) on page 3
- [Resolved issues](#) on page 4
- [Installation instructions](#) on page 4
- [Known issues](#) on page 4
- [Find product documentation](#) on page 5

About this release

This document contains important information about the current release. We strongly recommend that you read the entire document.

Forcepoint VPN Client is an end-user component for use with Forcepoint Next Generation Firewall (Forcepoint NGFW). The Forcepoint VPN Client provides a secure remote connection to your organization's network. Strong encryption prevents eavesdropping and modification of the traffic. The Forcepoint VPN Client provides easy and secure remote access to private networks where Forcepoint NGFW is used as a VPN gateway.

System requirements

The Forcepoint VPN Client is compatible with several Microsoft Windows operating systems and needs a specific software environment.

- Operating systems, 32-bit or 64-bit:
 - Windows 10
 - Windows 8.1
- Microsoft .NET Framework 4.5

Build number and checksums

The build number for Forcepoint VPN Client 6.8.0 is 6801.

Use the checksums to make sure that the installation files downloaded correctly.

- Forcepoint-VPN-Client-6.8.0.6801.exe

SHA256SUM:
3f11aa4001a701571ac6886eba41ff3a43a296f409343325bfe9ddd2f6cc8276

- Forcepoint-VPN-Client-x64.msi

SHA256SUM:
07a073bfc296bc20924099e69e727ee7057f65335ec464b9a7d4a84aba2ef42

- Forcepoint-VPN-Client-x86.msi

SHA256SUM:
463f2314a1df945c3f28470e26ab315b548ff2f12efb0d85fede5f618a4c2aa5

Compatibility

Forcepoint VPN Client is recommended for use with these Forcepoint NGFW component versions.

Component	Minimum compatible version	Recommended version
Forcepoint NGFW Security Management Center (SMC)	6.3.0	Latest 6.5.x maintenance version or higher
Forcepoint Next Generation Firewall (Forcepoint NGFW) in the Firewall/VPN role	6.3.0	Latest 6.5.x maintenance version or higher

Enhancements

This release of the product includes these enhancements.

Enhancements in Forcepoint VPN Client version 6.8.0

Enhancement	Description
Support for IKEv2 Message Fragmentation	Support for IKEv2 Message Fragmentation (RFC 7383) has been added to improve the performance of the VPN Client in networks that do not properly support IP fragmentation. This feature is automatically enabled when the VPN Client connects to NGFW Engine version 6.9 or higher.
SHA-256 support for certificate requests	The VPN Client now creates certificate requests using the SHA-256 message digest algorithm.
Improved event logging	The VPN Client now writes to the Windows event log when the status changes.

Resolved issues

These issues are resolved in this release of the product. For a list of issues fixed in a previous release, see the Release Notes for the specific release.

Description	Issue number
If you try to start the VPN Client from the Windows Start menu when the VPN Client is already running, the following message is shown: "VPN client is already running on this machine. Only one instance can be run at time."	VPN-184
If the VPN Client receives an encapsulated packet that is larger than it can handle, the VPN Client silently drops the connection.	VPN-417
In rare cases, the VPN Client might stop working during authentication.	VPN-426
The SSL VPN timeout might be shown incorrectly in the "Reauth. in" dialog box.	VPN-431
VPN Clients that have an IPsec connection to a VPN gateway might be disconnected when NGFW Engine nodes are rebooted.	VPN-476
The User Authentication dialog box for the VPN Client might not show the full server message.	VPN-477
When a VPN gateway has both IPsec and SSL VPN endpoints, failover to a backup gateway does not work. Only IPsec endpoints support backup gateways.	VPN-485
When an SSL VPN is used for the first connection to a VPN gateway, the user is prompted to verify the gateway certificate even though the gateway contact information .xml file is used in the installation.	VPN-486
Microsoft 365 applications might prevent VPN Client users from collecting diagnostics.	VPN-495

Installation instructions

Install Forcepoint VPN Client 6.8.0 as instructed in the *Forcepoint VPN Client Product Guide* and *Forcepoint VPN Client User Guide*.

Known issues

For a list of known issues in this product release, see Knowledge Base article [19131](#).

Known limitations

This release of the product includes these known limitations.

- Elliptic curve digital signature algorithm (ECDSA) certificates from Windows Certificate Stores cannot be used with IKEv1.

Find product documentation

On the Forcepoint support website, you can find information about a released product, including product documentation, technical articles, and more.

You can get additional information and support for your product on the Forcepoint support website at <https://support.forcepoint.com>. There, you can access product documentation, release notes, Knowledge Base articles, downloads, cases, and contact information.

You might need to log on to access the Forcepoint support website. If you do not yet have credentials, create a customer account. See <https://support.forcepoint.com/CreateAccount>.

Product documentation

Every Forcepoint product has a comprehensive set of documentation.

- *Forcepoint VPN Client Product Guide* for Windows
- *Forcepoint VPN Client User Guide* for Windows
- *Forcepoint Next Generation Firewall Product Guide*
- *Forcepoint Next Generation Firewall Installation Guide*

