Forcepoint

VPN Client

2.0.6

for macOS

Release Notes

Contents

About this release

This document contains important information about the current release of Forcepoint VPN Client for macOS. We strongly recommend that you read the entire document.

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

Note

Forcepoint VPN Client for macOS uses the SSL protocol only and by default uses port 443.

System requirements

Forcepoint VPN Client is compatible with macOS version 10.11 (El Capitan) and higher.

Build number and checksums

Forcepoint VPN Client 2.0.6 build number is 200429.

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

- VPNClient-2.0.6.200429.dmg

```
SHA1SUM:
97ae8bc747c8aee4343ed737a08d6da35b4bd778

SHA256SUM:
5d12014f31a306a24f1fe05e1baeba320876bf93e6c46ee97423c253ce3e66e5

SHA512SUM:
dd44ca07644973f64d740902f96b24b8
e47b4edb94b71e17c30eda363bd87d59
c219017f72b67f81756e2b1255158e2b
891c1448d02a4c0c6e206dbbdbf2f402
```

Compatibility

Forcepoint VPN Client for macOS is recommended to be used with the following Forcepoint NGFW component versions.

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

Enhancements

This release of the product includes these enhancements.

Enhancements in Forcepoint VPN Client 2.0.3 for macOS

Enhancement	Description
Redirection of DNS queries to an internal DNS server	It is now possible to configure all DNS queries to be directed through the VPN tunnel to an internal DNS server. For more information, see Knowledge Base article 17900.

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 the VPN Client receives an encapsulated packet that is larger than it can handle, the VPN Client silently drops the connection.	VPN-417
The SSL VPN timeout might be shown incorrectly in the "Reauth. in" dialog box.	VPN-431
When you use two-factor authentication and the challenge message includes characters that are not UTF-8 characters, the VPN Client stops working.	VPN-435
When you use two-factor authentication and the wrong password is entered in the first phase, the VPN Client does not request the password again. After a timeout, authentication fails.	VPN-436

Installation instructions

For information about installing or upgrading Forcepoint VPN Client, see the *Forcepoint VPN Client User Guide* for macOS.

Known issues

For a list of known issues in this product release, see Knowledge Base article 10234.

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 User Guide* for macOS
- *Forcepoint Next Generation Firewall Product Guide*
- *Forcepoint Next Generation Firewall Installation Guide*