FORTINET
High Performance Network Security

FortiClient (Windows) - Release Notes

VERSION 5.4.0

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

October 28, 2016

FortiClient (Windows) 5.4.0 Release Notes

04-540-290937-20161028

TABLE OF CONTENTS

Change Log

Date	Change Description
2015-10-09	Initial release.
2015-10-20	Added Conflicts with Cisco Systems VPN Client information to Special Notices.
2015-10-23	Added additional information to *Installing on Windows 7 and Windows XP* in Special Notices.
2015-11-26	Added SSL VPN on Windows 10 information to Special Notices.
2015-12-09	Added Using FortiClient VPN with other Third-Party VPN Clients to Special Notices.
2016-03-17	Added 301241, 232764, 309662, 303146, 298767 to Known Issues.
2016-04-07	Added support for DTLS to the VPN section of New Features.
2016-10-28	Added FortiClient May Generate Multicast Traffic special notice for 301241.

Introduction

This document provides a summary of enhancements, support information, and installation instruction for FortiClient (Windows) 5.4.0 build 0780.

- Introduction
- Special Notices
- What's New in FortiClient (Windows) 5.4.0
- Installation Information
- Product Integration and Support
- Resolved Issues
- Known Issues

Please review all sections prior to installing FortiClient.

Licensing

FortiClient offers two licensing modes:

- Standalone Mode
- Managed Mode

Standalone Mode

In standalone mode, FortiClient is not registered to a FortiGate or Enterprise Management Server (EMS). In this mode, FortiClient is free both for private individuals and commercial businesses to use. No license is required. All features and functions are activated.

Managed Mode

Companies with large installations of FortiClient usually need a means to manage their endpoints. This is accomplished by registering each FortiClient to a FortiGate, or to an EMS. In this mode, FortiClient licensing is applied to the FortiGate or EMS. No separate license is required on FortiClient itself.

Licensing on the FortiGate or EMS is based on the number of registered clients. FortiGate 30 series and higher models support ten (10) free managed FortiClient licenses. For additional managed clients, a FortiClient license subscription must be purchased. The maximum number of managed clients varies per device model.

FortiClient Licenses on the FortiGate

The following table shows client limits per FortiGate model series.

The ability to download the license file, pre-configure the client, create a custom installer, and rebrand are included.

FortiGate Series	FortiClient License Upgrade
FortiGate/FortiWiFi 30 to 90 series	200 clients
FortiGate 100 to 300 series	600 clients
FortiGate 500 & above FortiGate VM01 w/ FOS 5.4 & above	2000 clients
FortiGate 1000 series & above FortiGate VM04 w/ FOS 5.4 & above	2000 clients 8000 clients
FortiGate 3000 & above FortiGate VM08 w/ FOS 5.4 & above	2000 clients 8000 clients 20 000 clients

Each FortiGate offers 10 free licenses by default. FortiGate 1000 and 3000 series both may use the 2000 or 8000 client license.

In high availability (HA) configurations, all cluster members require an upgrade license key.

FortiClient Licenses on the EMS

A newly installed EMS offers 20,000 trial client licenses over a period of 60 days from the day of installation. After the trail period lapses, the number of client licenses will be 10, same as for a new FortiGate to which no FortiClient license has been applied.

A license may be applied to the EMS at any time during or after the trial period. Licenses are available in multiples of 100 seats, with a minimum of 100 seats.

Special Notices

FortiClient May Generate Multicast Traffic

The Application Firewall re-injects incoming IGMP packet back into the outgoing network. It should instead re-inject it into the incoming network (as that was the direction the traffic was headed).

Since IGMP uses IP layer broadcasts, re-transmission will cause it to be re-broadcasted. With at least two FortiClient endpoints in the network, each re-transmitting the packets received, a single original IGMP packet may be re-transmitted indefinitely.

Workaround: When registered to EMS or FortiGate, disable Application Firewall by using EMS or FortiGate. You should also disable *Block known communication channels used by attackers* by setting the `<candc_enabled>` XML element to `0`:

```
<firewall>
   ...
   <candc_enabled>0</candc_enabled>
   ...
</firewall>
```

SSL VPN on Windows 10

When a custom DNS server is configured for SSL VPN, sometimes Windows 10 DNS resolution is not correct after the SSL VPN is connected.

The following FortiClient XML configuration is recommended, so that FortiClient restarts Windows dnscache service when SSL is connected.

```
<sslvpn>
   <options>
      <dnscache_service_control>2</dnscache_service_control>
   </options>
</sslvpn>
```

Using FortiClient VPN with other Third-Party VPN Clients

It is not supported to run more than one VPN connection simultanously. If using any third-party VPN software (other than FortiClient), please disconnect FortiClient VPN first, before establishing connection with the other VPN software. To reconnect VPN using FortiClient, ensure to first disconnect any established VPN connection from a third-party VPN software.

Conflicts with Cisco Systems VPN Client

FortiClient VPN feature conflicts with Cisco Systems VPN Client 5.0.07.

When both Cisco VPN Client 5.0.07 and FortiClient VPN are installed on the same Windows computer, a BSoD is likely to occur if an IPsec VPN connection is established using FortiClient.

Cisco VPN Client 5.0.07 has reached end of support. It is suggested to use Cisco AnyConnect 3.1 or newer instead. This is actively maintained by Cisco Systems. With Cisco Anyconnect installed, a BSoD does not occur when using FortiClient to establish an IPsec VPN connection.

Please note that it is unknown what may occur if VPN connections are attempted using both Cisco Anyconnect and FortiClient VPN at the same time. This is not recommended. Consider disconnecting one VPN connection, before establishing a second one.

Change in FortiClient Endpoint Control Default Registration Port

FortiClient registers to the FortiGate using Endpoint Control (EC). In FortiClient 5.0 and 5.2, the default registration port is TCP port 8010. FortiOS 5.0 and 5.2 both listen on TCP port 8010.

Starting with FortiClient 5.4, EC registration will use port 8013 by default. To register to FortiOS 5.0 or 5.2, the user must specify port 8010 with the IP address, separated by a colon. For example, <ip_address>:8010.

FortiOS 5.4 will listen on port 8013. If registering from FortiClient 5.4 to FortiOS 5.4, the default ports will match. Specifying the port number with then IP address is then optional.

Installing on Windows 7, Windows XP, and Windows Server 2008 R2

FortiClient 5.4.0 files and drivers are digitally signed using SHA2 certificates. Microsoft Windows 7 and Windows XP are both known to have issues with the verification of SHA2 certificates. Ensure you have the update installed described in the *Affected Software* section of the Advisory for your operating system from the following link:

Availability of SHA-2 Code Signing Support for Windows 7 and Windows Server 2008 R2

What’s New in FortiClient (Windows) 5.4.0

AntiVirus

Advanced Persistent Threats

FortiClient 5.4.0 has enhanced capabilities for the detection of Advanced Persistent Threats (APT). There are two changes added in this respect:

- Botnet Command and Control Communications Detection
- FortiSandbox integration

Botnet Communication Detection

Botnets running on compromised systems usually generate outbound network traffic directed towards Command and Control (C&C) servers of their respective owners. The servers may provide updates for the botnet, or commands on actions to execute locally, or on other accessible, remote systems.

When the new botnet feature is enabled, FortiClient monitors and compare network traffic with a list of known Command and Control servers. Any such network traffic will be blocked.

FortiSandbox Integration

FortiSandbox offers the capabilities to analyse new, previously unknown and undetected virus samples in real-time. Files sent to it are scanned first, using similar Antivirus (AV) engine and signatures as available on the FortiOS and FortiClient. If the file is not detected, but is an executable file, it is run (sandboxed) in a Microsoft Windows virtual machine (VM) and monitored. The file is given a rating or score based on its activities and behaviour in the VM.

FortiClient integration with the FortiSandbox allows users to submit files to the FortiSandbox for automatic scanning. When configured, FortiClient will send supported files downloaded over the internet to FortiSandbox if they could not be detected by the local real-time scanning. Access to the downloaded file is blocked until scanning result is returned.

As FortiSandbox receives files for scanning from various sources, it collects and generates AV signatures for such samples. FortiClient periodically downloads the latest AV signatures from the FortiSandbox, and applies them locally to all real-time, as well as on-demand, AV scanning.

This feature requires FortiSandbox running version 2.1 or newer and is only available on FortiClient (Windows).

Enhanced Real-Time Protection Implementation

The Real-Time Protection (RTP) or on-access feature in FortiClient uses a tight integration with Microsoft Windows to monitor files locally or over a network file system as they are being downloaded, saved, run, copied, renamed, opened or written to. The FortiClient driver coupling with Windows has been re-written to use modern API's provided by Microsoft. All basic features remain the same, with a few minor differences in behaviour. Some noticeable performance enhancements could be observed in various use case scenarios.

Web Filtering

Web Browser Usage and Duration

If configured, FortiClient will record detailed information about the user's web browser activities, such as:

- A history of websites visited by the user (as shown in regular web browser history)
- An estimate of the duration or length of stay on the website

These logs are sent to FortiAnalyzer, if configured. With FortiAnalyzer 5.4.0 or newer, the FortiClient logs sent from various endpoints may be viewed in FortiView.

This feature requires FortiAnalyzer 5.4.0 or newer.

VPN

Authorized Machine Detection

For enterprises where new computers may be brought into the organisation by employees, FortiClient may be configured to check or identify the computer, before allowing it to establish IPsec VPN or SSL VPN connection to the FortiGate. The administrator may configure restrictions with one or more of the following:

- Registry check: Ensure a specific registry path contains a predetermined value.
- File check: Verify: the existence of a specific file at a specified location.
- Application check: Ensure that a specific application is installed and running.

The verification criteria can be configured using advanced FortiClient XML configurations on the FortiGate or the EMS.

This applies to FortiClient (Windows) only.

New SSL VPN Windows Driver

The FortiClient SSL VPN driver, `pppop.sys` was re-written to use the latest Microsoft Windows recommended CoNDIS WAN driver model. The new driver is selected when FortiClient is installed on Windows 7 or higher. The SSL VPN driver included in the previous versions of FortiClient will still be maintained.

New IPsec VPN Windows Driver

FortiClient IPsec VPN drivers have been updated to support Microsoft Windows NDIS 6.3 specification. The new drivers are compatible with Microsoft Windows 8.1 or higher.

Support for DTLS

FortiClient SSL VPN connections to FortiGate now support Datagram Transport Layer Security (DTLS) by using User Datagram Protocol (UDP) as the transport protocol. Previously FortiClient SSL VPN connections supported only Transport Control Protocol (TCP). You can now use FortiGate to configure SSL VPN connections that use DTLS. You cannot use FortiClient to configure SSL VPN connections that use DTLS. When FortiClient endpoints use a DTLS-enabled SSL VPN connection with FortiGate, and FortiGate communicates DTLS support, FortiClient uses DTLS via UDP. If DTLS fails, FortiClient will fall back to use TLS to establish an SSL VPN connection.

Endpoint Control

Integration with the New Enterprise Management Server

The Enterprise Management Server (EMS) is a new product from Fortinet for businesses to use to manage their computer endpoints. It runs on a Windows Server,so it does not require a physical Fortinet device. Administrators may use it to gain insight on the status of their endpoints. The EMS supports devices running Microsoft Windows, Mac OS X, Android and iOS.

FortiClient Endpoint Control protocol has been updated to seamlessly integrate with the EMS. Various changes were added to support EMS features, such as:

- Deployment of FortiClient to new (Microsoft Windows) devices
- Continuous monitoring of device status
- AV engine and signature update status reports
- AV scanning schedule. Requesting for AV scan
- Notifications about protection status

FortiGate Network Access Control with EMS Integration

When creating a FortiClient profile on EMS, the administrator can choose to configure the FortiClient to register to the same EMS or to a FortiGate. Changes in FortiClient 5.4.0 allow it to register to a FortiGate, while simultaneously, notifying the EMS of its registration status. The FortiClient EC registration to the FortiGate is required for Network Access Compliance (NAC). The administrator can configure the FortiGate to allow access to network resources only if the client is compliant with the appropriate interface EC profile.

This feature requires FortiOS 5.4.0 or newer.

Quarantine an Infected Endpoint from the FortiGate or EMS

A computer endpoint that is considered to be infected may be quarantined by the FortiGate or EMS (Enterprise Management Server) administrator. FortiClient needs to be registered and online, using Endpoint Control, to the said FortiGate or EMS.

Once quarantined, all network traffic to or from the infected endpoint will be blocked locally. This allows time for remediation actions to be taken on the endpoint, such as scan and clean the infected system, revert to a known clean system restore point or re-install the operating system.

The Administrator may un-quarantine the endpoint in the future from the same FortiGate or EMS.

This feature requires either FortiOS 5.4.0 or EMS 1.0.0.

Importing FortiGate CA Certificate after Endpoint Control Registration

When the FortiGate is configured to use SSL deep inspection, users visiting encrypted websites will usually receive an invalid certificate warning. The certificate signed by the FortiGate does not have a Certificate Authority (CA) at the endpoint to verify it. Users can manually import the FortiGate CA certificate to stop the error from being displayed. However, all users will have to do the same.

When registering Endpoint Control (EC) to a FortiGate, the FortiClient will receive the FortiGate's CA certificate and install it into the system store. If Firefox is installed on the endpoint, the FortiGate's CA certificate will also be installed into Firefox certificate store. Thus, the end user will no longer receive the invalid certificate error message when visiting encrypted websites.

The FortiGate CA certificates will be removed from the system store if FortiClient is uninstalled.

Enhancement to On-net/Off-net Configuration

The on-net feature requires the use of a FortiGate as the DHCP server. This is usually configured on the same FortiGate that the FortiClient will be registered. When the device on which FortiClient is running has an IP address from the FortiGate's DHCP server, it is on-net. For any other IP addresses, it is off- net.

There is a new way to configure the on-net feature. On the FortiGate, the DHCP server can be used, or several network subnets can be provided.

FortiClient will be on-net if:

- It is registered using EC to the FortiGate
- It belongs to one of the pre-configured on-net subnets, or
- It provides the DHCP for on-net properties.

Otherwise, it is off-net.

FortiClient GUI

AntiVirus Settings Page

With the introduction of botnet detection and the integration with FortiSandbox, the AV settings page on the FortiClient GUI has been updated to allow configuration of the new features. The AV settings page is accessible from the FortiClient dashboard. Select the AV tab on the left pane. Then click the settings icon on Real-Time Protection in the right pane.

The following may be selected on the AV settings page:

- File scanning (previously, Real-Time Protection or RTP)
- Scan unknown, supported files using FortiSandbox
- Malicious website detection
- Botnet detection (block known communication channels)

The use of FortiSandbox requires that file scanning is enabled.

FortClient Banner Design

If FortiClient is running in standalone mode and not registered to a FortiGate or EMS, a single banner at the bottom of the GUI is displayed. This is true for both the FortiClient full version, as well as the VPN only version. When registered to a FortiGate or EMS, the banner is hidden by default. Similarly, when created from a FortiClient Configurator, no banner is displayed by default.

Logging

Enhancement to FortiClient Logs

FortiClient will create a log entry to show just the URL visited by the user through a web browser. This is in addition to the network level logs generated by FortiClient.

Installation Information

Firmware images and tools

When installing FortiClient version 5.4.0, you can choose the setup type that best suits your needs. You can select one of the two options: Complete: All Endpoint Security and VPN components will be installed or VPN Only: only VPN components (IPsec and SSL) will be installed.

- FortiClientSetup_5.4.0.0780.exe

Standard installer for Microsoft Windows (32-bit).

- FortiClientSetup_5.4.0.0780.zip

A zip package containing FortiClient.msi and language transforms for Microsoft Windows (32-bit). Some properties of the MSI package can be customized with FortiClient Configurator tool.

- FortiClientSetup_5.4.0.0780_x64.exe

Standard installer for Microsoft Windows (64-bit).

- FortiClientSetup_5.4.0.0780_x64.zip

A zip package containing FortiClient.msi and language transforms for Microsoft Windows (64-bit). Some properties of the MSI package can be customized with FortiClient Configurator tool.

- FortiClientTools_5.4.0.0780.zip

A zip package containing miscellaneous tools including the FortiClient Configurator tool and VPN Automation files.

When creating a custom FortiClient 5.4.0 installer using the FortiClient Configurator tool, you can choose which features to install. You can enable or disable software updates, configure SSO, and rebrand FortiClient .

Upgrading from previous FortiClient versions

FortiClient version 5.4.0 supports upgrading from FortiClient 5.2.0 or later.

Please review the Introduction on page 6 and Product Integration and Support on page 17 chapters prior to installing FortiClient version 5.4.0.

Downgrading to previous versions

Downgrading FortiClient version 5.4.0 to previous FortiClient versions is not supported.

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal located at https://support.fortinet.com. After logging in, click on *Download > Firmware Image Checksums*, enter the image file name including the extension, and select *Get Checksum Code*.

Product Integration and Support

FortiClient 5.4.0 support

The following table lists version 5.4.0 product integration and support information.

FortiClient 5.4.0 support information

Desktop Operating Systems	• Microsoft Windows XP (32-bit) • Microsoft Windows 7 (32-bit and 64-bit) • Microsoft Windows 8, 8.1 (32-bit and 64-bit) • Microsoft Windows 10 (32-bit and 64-bit) FortiClient 5.4.0 does not support Microsoft Windows Vista (32-bit and 64-bit)
Server Operating Systems	• Microsoft Windows Server 2008 R2 • Microsoft Windows Server 2012, 2012 R2
Minimum System Requirements	• Microsoft Internet Explorer version 8 or later • Microsoft Windows compatible computer with Intel processor or equivalent • Compatible operating system and minimum 512MB RAM • 600MB free hard disk space • Native Microsoft TCP/IP communication protocol • Native Microsoft PPP dialer for dial-up connections • Ethernet network interface controller (NIC) for network connections • Wireless adapter for wireless network connections • Adobe Acrobat Reader for FortiClient documentation • Windows Installer MSI installer version 3.0 or later.
FortiAnalyzer	• 5.0.2 and later • 5.2.0 and later • 5.4.0
FortiAuthenticator	• 2.2.0 and later • 3.0.0 and later • 3.1.0 and later • 3.2.0 and later

FortiManager	• 5.0.2 and later • 5.2.0 and later • 5.4.0
FortiOS	• 5.0.0 and later • 5.2.0 and later • 5.4.0 Some FortiClient features are dependent on specific FortiOS versions.
FortiSandbox	• 2.1.0

Language support

The following table lists FortiClient language support information.

FortiClient language support

Language	Graphical User Interface	XML Configuration	Documentation
English	✔	✔	✔
Chinese (Simplified)	✔		
Chinese (Traditional)	✔		
French (France)	✔		
German	✔		
Japanese	✔		
Korean	✔		
Portuguese (Brazil)	✔		
Russian	✔		
Spanish (Spain)	✔		

The FortiClient language setting defaults to the regional language setting configured on the client workstation unless configured in the XML configuration file.

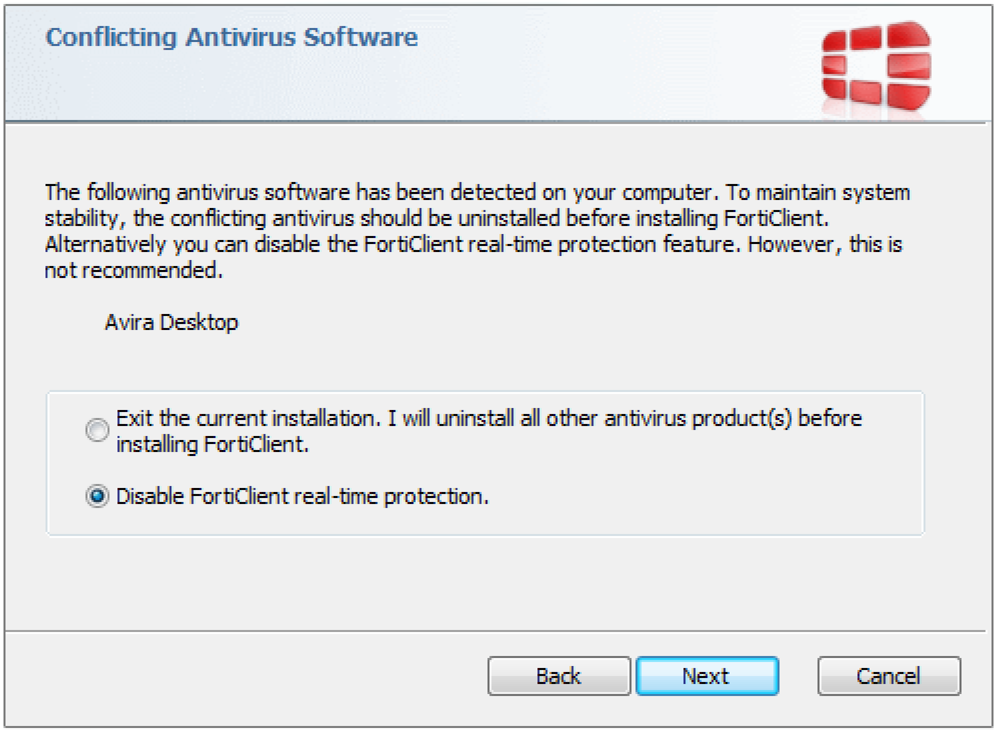
If the client workstation is configured to a regional language setting that is not supported by FortiClient , it defaults to English.

Conflicts with third party antivirus products

The antivirus feature in FortiClient is known to conflict with other similar products in the market. Consider removing other antivirus programs before installing FortiClient.

During a new installation of FortiClient, the installer will search for other registered third party software and, if any is found, warn users to uninstall them before proceeding with the installation. There is also an option to disable FortiClient Real Time Protection (RTP).

Conflicting Antivirus Software



Conflicting Antivirus Software

The following antivirus software has been detected on your computer. To maintain system stability, the conflicting antivirus should be uninstalled before installing FortiClient. Alternatively you can disable the FortiClient real-time protection feature. However, this is not recommended.

Avira Desktop

○ Exit the current installation. I will uninstall all other antivirus product(s) before installing FortiClient.

● Disable FortiClient real-time protection.

Conflicts with Cisco Systems VPN client

FortiClient VPN feature conflicts with Cisco Systems VPN Client 5.0.07. This Cisco Client has reached end of support. It is suggested to use Cisco AnyConnect 3.1 or newer instead. This is actively maintained by Cisco Systems and it does not have any conflicts with the FortiClient VPN feature.

Resolved Issues

The following issues have been fixed in version 5.4.0. To report any issues, please report them to the Beta Program Forums.

AntiVirus

Bug ID	Description
259518	`FortiClientVirusCleaner.exe` does not update the engine or definitions before scanning.
280302	`thunderbird pop3` inbox is quarantined when and email attachment contains a virus.

Endpoint Control

Bug ID	Description
288714	After logging out, the Workstation switched to the offline status.

VPN

Bug ID	Description
223787	Windows Server 2012 is unable to connect via SSL VPN.
265416	SSL VPN tunnel may inhibit FSSO clients by default.
268225	FortiClient 5.2.3 requires a smart card.
271244	FortiClient Windows does not accept `SSL VPN Realm Config`.
274075	SSLVPN routes are not always sent.
275233	Two-factor token code validation does not work with SSL VPN when *VPN before log on* feature is enabled.
275422	*IPsec VPN Auto-Connect* feature continuously pops up errors when connection is not available.
278114	Remove `autokey_keep_alive` from FortiClient Windows config
280427	FortiClient SSL VPN does not work with Firefox 38.0.1.
280449	Special characters cannot be used in IPsec Xauth.

Bug ID	Description
283587	`FortiSSLVPNclient.exe` should minimize to system tray after connecting.
288645	SSL custom DNS server does not have priority in Windows 10.
291874	Unable to connect to SSLVPN using FortiClient when FortiClient is behind a proxy server.
292000	FortiClient IPSec *Enable IPv4 Split tunnel* manually set information is automatically deleted when any change is applied.
286223	FortiClient slows down Network performance when the Application Firewall is enabled.

Other

Bug ID	Description
260643	FortiClient 5.0.9 does not recognize `wpad` file (proxy settings).
269474	Random Bluescreens occur when using FortiClient 5.2.2 or 5.2.3 side by side with Symantec endpoint protection.
272818	BSoD probably related to Symantec (teefer driver).
281556	Update OpenSSL libraries to version 1.0.2b.
284418	Configuration with `FCConfig.exe` is *Not Applied*.
284559	Update `sqlite` source code to `3.8.10.2`.
284836	Update OpenSSL library to v1.0.2d.
289473	Rebranded text.
289658	Cannot install when using `FortiClient 5.2.4 x64.exe` installer in 64bit Windows.

Known Issues

The following issues have been identified in FortiClient (Windows) 5.4.0. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Bug ID	Description
275020	FortiClient may display a certificate revocation warning in Internet Explorer 11.
290114	There may be a FortiProxy compatibility issue with the Trend AV web reputation module.
290418	Increase SSL VPN split tunnel buffer.

301241	FortiClient may generate multicast traffic.
	The Application Firewall re-injects incoming IGMP packet back into the outgoing network. It should instead re-inject it into the incoming network (as that was the direction the traffic was headed).
	Since IGMP uses IP layer broadcasts, re-transmission will cause it to be re-broadcasted. With at least two FortiClient endpoints in the network, each re-transmitting the packets received, a single original IGMP packet may be re-transmitted indefinitely.
	Workaround: When registered to EMS or FortiGate, disable Application Firewall by using EMS or FortiGate. You should also disable *Block known communication channels used by attackers*by setting the `<candc_enabled>` XML element to `0`:
	`<firewall>`
	`   ...`
	`   <candc_enabled>0</candc_enabled>`
	`   ...`
	`</firewall>`

232764	SSL VPN connection attempt may stop at 98% . Attempts to connect by SSL VPN stops at 98%. There are many varied reasons that this happens. The following are the two most common in recent reports. • It was caused by a Microsoft Windows OS issue on Windows 8.1 and 2012 R2. Installation of the following hotfix resolves it in this case: https://support.microsoft.com/en-us/kb/3046798 2. • On regular production Windows 10 OS, SSL VPN connection works correctly until after the first system reboot. Susequently, the first connection would still be successfull, but the next is likely to fail at 98%. **Workaround:** A reboot will again allow new SSL VPN connections to succeed.

Bug ID	Description
309662	SSL VPN connection attempt may cause BSoD on Windows 10 Insider Preview (build 14257 or newer).
303146	SSL VPN may conflict with other NDIS 6.1 VPN clients on Windows 10. FortiClient SSL VPN uses Microsoft Windows NDIS 6.1 https://msdn.microsoft.com/en-us/library/windows/hardware/ff556027. A number of other third-party applications that use the same protocol conflict with FortiClient SSL VPN. Here are known applications: • Pulse Secure (Junos Pulse Client) • Dell VPN (SonicWall VPN) With either of these installed, network traffic fails to go through the established VPN tunnel.
298767	FortiShield may cause BSoD following a post-installation reboot.

FORTINET®

High Performance Network Security