FORTINET
High Performance Network Security

FortiClient (Windows) - Release Notes

VERSION 5.4.1

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

June 28, 2016

FortiClient (Windows) 5.4.1 Release Notes

04-541-357377-20160628

TABLE OF CONTENTS

Change Log **4**
Introduction **5**
Licensing 5
Standalone Mode 5
Managed Mode 5
Special Notices **7**
FortiClient upgrade on Windows XP 7
Cooperative Security Fabric Upgrade 7
Installing FortiClient on Windows 7 7
SSL VPN on Windows 10 8
Using FortiClient VPN with other Third-Party VPN Clients 8
Conflicts with Cisco Systems VPN Client 8
Change in FortiClient Endpoint Control Default Registration Port 8
What's New in FortiClient (Windows) 5.4.1 ..... **9**
FortiClient Telemetry 9
Vulnerability scan enhancements 9
Vulnerability auto-patching 9
Endpoint compliance 9
FortiSandbox support for removable media 9
Installation Information **10**
Firmware images and tools 10
Upgrading from previous FortiClient versions 10
Downgrading to previous versions 11
Firmware image checksums 11
Product Integration and Support **12**
FortiClient 5.4.1 support 12
Language support 13
Conflicts with third party antivirus products 14
Conflicts with Cisco Systems VPN client 14
Resolved Issues **15**
Known Issues **18**

Change Log

Date	Change Description
2016-06-24	Initial release.
2016-06-28	Added special notice about FortiClient upgrade on Windows XP

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (Windows) 5.4.1 build 0840.

- Introduction on page 5
- Special Notices on page 7
- What's New in FortiClient (Windows) 5.4.1 on page 9
- Installation Information on page 10
- Product Integration and Support on page 12
- Resolved Issues on page 15
- Known Issues on page 18

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.

Support for FortiClient in standalone mode is provided on the Fortinet Forums (forum.fortinet.com). Phone support is not provided.

Managed Mode

Companies with large installations of FortiClient usually need a means to manage their endpoints. EMS can be used to provision and centrally manage FortiClient endpoints, and FortiGate can be used with FortiClient endpoints for network security. Each FortiClient endpoint can register to a FortiGate or an EMS. In this mode, FortiClient licensing is applied to the FortiGate or EMS. No separate license is required on FortiClient itself.

FortiClient Licenses on the FortiGate

FortiGate 30 series and higher models include a FortiClient license for ten (10) free, connected FortiClient endpoints. For additional connected endpoints, you must purchase a FortiClient license subscription. Contact your Fortinet sales representative for information about FortiClient licenses.

FortiClient Licenses on the EMS

EMS includes a FortiClient license for ten (10) free, connected FortiClient endpoints for evaluation. For additional connected endpoints, you must purchase a FortiClient license subscription. Contact your Fortinet sales representative for information about FortiClient licenses.

Special Notices

FortiClient upgrade on Windows XP

FortiClient 5.4.1 supports Windows XP. However upgrade to FortiClient 5.4.1 is not supported on Windows XP. For existing endpoint users on Windows XP, you must uninstall the previous version of FortiClient, reboot Windows XP, and then install FortiClient 5.4.1.

Endpoint users on Windows XP may consider disabling FortiClient software updates. FortiClient will continue to receive engine and signature updates.

New installations of FortiClient 5.4.1 on Windows XP are supported.

Cooperative Security Fabric Upgrade

FortiOS 5.4.1 greatly increases the interoperability between other Fortinet products. This includes:

- FortiClient 5.4.1
- FortiClient EMS 1.0.1
- FortiAP 5.4.1
- FortiSwitch 3.4.2

The upgrade of the firmware for each product must be completed in a precise order so the network connectivity is maintained without the need of manual steps. Customers must read the following two documents prior to upgrading any product in their network:

- *Cooperative Security Fabric - Upgrade Guide*
  This document is available on the Fortinet Document Library on the FortiOS page (docs.fortinet.com/).
- *FortiOS 5.4.0 to 5.4.1 Upgrade Guide for Managed FortiSwitch Devices*,
  This document is available in the Customer Support Firmware Images download directory for FortiSwitch 3.4.2 (support.fortinet.com/).

Installing FortiClient on Windows 7

Files and drivers for FortiClient 5.4.0 and later are digitally signed using SHA2 certificates. Microsoft Windows 7 is known to have issues with the verification of SHA2 certificates. Ensure you have installed the update 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

During the installation process, FortiClient 5.4.1 checks whether the update for the operating system is installed on the endpoint. If the update is not installed, a dialog box is displayed that instructs you to install the required update. FortiClient 5.4.1 installation will not complete until the required update for the operating system is installed.

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 before establishing connection with the other VPN software. To reconnect VPN using FortiClient, ensure that you 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 and later will listen on port 8013. If registering from FortiClient 5.4 and later to FortiOS 5.4 and later, the default ports will match. Specifying the port number with then IP address is then optional.

What’s New in FortiClient (Windows) 5.4.1

This section identifies the new features and enhancements in FortiClient (Windows) 5.4.1. For more information, see the *FortiClient Administration Guide*.

FortiClient Telemetry

FortiClient can send endpoint telemetry data to FortiGate or FortiClient Enterprise Management Server. Telemetry data can include user identity and endpoint security context, such as vulnerability, security posture, OS details, interface, IP address, and MAC address.

Vulnerability scan enhancements

Vulnerability scan feature in FortiClient (Windows) can perform a full scan of the endpoint to find any OS, Microsoft Office, browser and third-party vulnerabilities. FortiClient (Windows) can then report the vulnerabilities to FortiAnalyzer and Central Management in FortiGate or FortiClient EMS.

If you are using FortiGate, FortiOS 5.4.1 is required.

If you are using FortiClient EMS, version 1.0.1 is required.

Vulnerability auto-patching

FortiClient (Windows) supports automatic patching of vulnerabilities where FortiClient will initiate and apply any updates required to resolve detected vulnerabilities and return endpoints to a secure state.

If you are using FortiGate, FortiOS 5.4.1 is required.

If you are using FortiClient EMS, version 1.0.1 is required.

Endpoint compliance

FortiClient can detect unauthorized and vulnerable endpoints. It helps enforce minimum compliance criteria and only allow network access to compliant endpoints.

If you are using FortiGate, FortiOS 5.4.1 is required.

FortiSandbox support for removable media

FortiClient (Windows) can now send files on removable media for on-demand FortiSandbox scanning.

Installation Information

Firmware images and tools

When installing FortiClient version 5.4.1, you can choose the setup type that best suits your needs. You can select one of the following options:

- Complete: All Endpoint Security and VPN components will be installed
- VPN Only: only VPN components (IPsec and SSL) will be installed.

The following files and tools are available:

FortiClient

- FortiClientSetup_5.4.1.0840.exe

Standard installer for Microsoft Windows (32-bit).

- FortiClientSetup_5.4.1.0840.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_5.4.1.0840_x64.exe

Standard installer for Microsoft Windows (64-bit).

- FortiClientSetup_5.4.1.0840_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_5.4.1.0840.zip

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

When creating a custom FortiClient 5.4.1 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 5.4.1 supports upgrading from FortiClient 5.2.0 or later.

When FortiClient endpoints are registered to FortiGate, you must upgrade endpoints to FortiClient 5.4.1 before you upgrade FortiGate to 5.4.1. See Cooperative Security Fabric Upgrade on page 7.

Please review the following sections prior to installing FortiClient version 5.4.1: Introduction on page 5, Special Notices on page 7, and Product Integration and Support on page 12.

Downgrading to previous versions

Downgrading FortiClient version 5.4.1 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 5.4.1 support

The following table lists version 5.4.1 product integration and support information.

FortiClient 5.4.1 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	• 5.4.1
FortiAuthenticator	• 4.1.0 • 4.0.0 and later • 3.3.0 and later • 3.2.0 and later • 3.1.0 and later • 3.0.0 and later

FortiClient EMS	• 1.0.0 and later FortiClient 5.4.1 enhancements to the Vulnerability Scan feature require FortiClient EMS 1.0.1.
FortiManager	• 5.4.1
FortiOS	• 5.4.1 Some FortiClient features are dependent on specific FortiOS versions.
FortiSandbox	• 2.2.0 and later • 2.1.0 and later

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

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 5.4.1. To report any issues, please report them to the Beta Program Forums.

AntiVirus

Bug ID	Description
366803	FortiClient deleting Outlook 2013 mail attachments
365532	FortiClient may break mail format on slow link
309157	FortiClient conflicts with Forefront TMG clients
305670	Unable to use Windows environment variables in folder or file exclusion list
300510	Scan removable media on insertion shall not launch scan of mapped network drive
295509	Unable to eject USB drive when AV is enabled

VPN

Bug ID	Description
290418	Increase SSL VPN split tunnel buffer.
309662	SSL VPN connection attempt may cause BSoD on Windows 10 Insider Preview (build 14257 or newer).
372313	FortiClient IPSec VPN PKI cannot connect from command line during SCCM deployment
365791	FortiClient SSL VPN DNS resolution problem
355181	Network loss when DHCP renewal process is triggered and SSL tunnel is up
368718	IPSec disconnect once FortiClient receives endpoint profile
292328	IPSec pre-shared VPN before Windows logon goes disconnect after logon
365039	FortiClient shows wrong status when disconnected and requires two authentication attempts to re-connect
369290	VPN disappear after receiving endpoint profile
364829	Validate IPSec VPN server subject name

Bug ID	Description
304679	VPN before Windows logon prompt for certificate when it shall not
357571	Cannot save username for SSL VPN when it contains "%"
301079	SSL VPN connection fails randomly with DNS round-robin record list
297133	Cannot access protected network on Windows 10 with IPSec over CDMA data card
298962	SSL VPN cross VDOM script execution for "on connect" script
302462	Store username and password for NTLM authentication without admin privilege

Web Filter

Bug ID	Description
365489	Web Filter not enable when FortiClient is off-net
368121	Fortiproxy interferes with Lync (Skype for business)
370670	Fortiproxy conflicts with Dynamsoft software
364312	Fortiproxy confilcts with Landesk application
356709	FortiClient is causing high delay for Microsoft Direct Access traffic

Application Firewall

Bug ID	Description
286223	FortiClient slows down network performance when application firewall enabled
356145	BSOD when Carbon Black is installed and application firewall enabled
300094	FortiClient blocks access to remote FortiGate via HTTPS

Other

Bug ID	Description
298767	FortiShield may cause BSoD following a post-installation reboot
301241	FortiClient may generate multicast traffic
368121	Fortishield conflicts with Lumension remote scan

Bug ID	Description
370372	Fortishield conflicts with WorkSite software
370055	VPN only installation shall not have Web Filter log
298767	BSOD after FortiClient installation
363610	Export logs for non-admin users
303118	Application dialer.exe could not receive information about the phone when FortiClient is installed
356709	OpenSSL Security Advisory [1 March 2016]
306485	Unable to register FortiClient when endpoint profile name has brackets
356506	Web browsing is slow when wanopt is enabled
310102	Adobe Acrobat considers that assistive device connected after installing FortiClient
307949	OpenSSL Security Advisory [28 January 2016]
310200	No system tray icon after upgrade
308464	FortiClient freeze on security prompt when connecting IPSec

Known Issues

The following issues have been identified in FortiClient (Windows) 5.4.1. 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.
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.
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.
373300	Citrix remote desktop UI latency when block malicious web sites is enabled
376833	Endpoint traffic is blocked for few seconds after FortiClient installer deployed
375898	No prompt informing user of unfixed critical or high vulnerabilities
373769	Sometimes vulnerability auto-patching does not work
291192	FortiClient cannot block Tor browser

Bug ID	Description
370402	Random IPSec disconnects
376372	Wrong state on Compliance tab in FortiClient Console
373170	VPN auto-connect when on-net does not behave properly
370011	FCAuth crashes when non-admin user tries to use system store certificate for IPSec
376825	The *Install Selected* button is inconsistent when there are no auto-updatable applications
376174	OnlineInstaller issue on PC without KB3033929
365833	IPSec does not support multiple DNS suffixes
375026	Diagnostic tool does not prompt user to run as administrator
377330	Fresh install or upgrade from FDS is not supported for Windows XP
377771	Upgrade 5.4.0 VPN only gets all functions installed

FORTINET®

High Performance Network Security

Copyright© 2016 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.