High Performance Network Security

FortiClient (Windows) - Release Notes

VERSION 5.4.4

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

December 11, 2017

FortiClient (Windows) 5.4.4 Release Notes

04-544-440205-20171211

TABLE OF CONTENTS

Change Log

Date	Change Description
2017-07-20	Initial release.
2017-08-18	Updated to add a special notice about Vulnerability Scan support.
2017-11-23	Added *Change in SSL VPN default* to *Special Notices*.
2017-12-11	Removed support for Windows XP.

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (Windows) 5.4.4 build 0890.

- Introduction
- Special Notices
- 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.

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.

When using the ten (10) free licenses for FortiClient in managed mode, support is provided on the Fortinet Forums (forum.fortinet.com). Phone support is not provided when using the free licenses. Phone support is provided for paid licenses.

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

Change in SSL VPN default

Starting with FortiClient 5.4.4, TLS is the default used for SSL VPN when establishing a tunnel connection with FortiGate. Previously with FortiClient 5.4.0 to 5.4.3, DTLS was the default. After you upgrade to FortiClient 5.4.4, you can configure DTLS to be the default by setting the following XML element in the FortiClient configuration file: `<prefer_dtls_tunnel>1<prefer_dtls_tunnel>`

When `<prefer_dtls_tunnel>` is set to `0`, FortiClient uses TLS, even if `dtls-tunnel` is enabled on FortiGate.

When `<prefer_dtls_tunnel>` is set to `1`, FortiClient uses DTLS, if it is enabled on the FortiGate and tunnel establishment is successful. If `dtls-tunnel` is disabled on FortiGate, or tunnel establishment is not successful, TLS is used.

SSL VPN cannot connect after upgrade to FortiOS to 5.4.x

After upgrading FortiOS to 5.4.x from 5.2 or earlier, problems might occur with FortiClient (Windows) when connecting with SSL VPN to FortiGate. Connection in FortiClient can become stuck at 40%, and display the following error message:

Unable to establish the VPN connection. The VPN server may be unreachable. (-5)

The error can be caused by changed default settings for encryption on FortiOS 5.4.

Workaround:

1. On the FortiClient (Windows) workstation, go to *Internet Explorer* > *Options* > *Advanced*.
2. Change the TLS settings to match those settings on FortiGate.
   For example, if *TLS 1.1* and *TLS 1.2* are enabled on FortiGate, enable them in Internet Explorer too.

Cooperative Security Fabric upgrade

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

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

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.x 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.

Installation Information

Firmware images and tools

When installing FortiClient version 5.4.4, 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 are available from the Fortinet Support site:

- FortiClientSetup_5.4.4.0890.exe
  Standard installer for Microsoft Windows (32-bit).
- FortiClientSetup_5.4.4.0890.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_5.4.4.0890_x64.exe
  Standard installer for Microsoft Windows (64-bit).
- FortiClientSetup_5.4.4.0890_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_5.4.4.0890.zip
  A zip package containing miscellaneous tools, including the FortiClient Configurator tool and VPN Automation files.

When creating a custom FortiClient 5.4.4 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 5.4.4 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 or later 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 5.4.4: Introduction on page 5, Special Notices on page 7, and Product Integration and Support on page 12.

Downgrading to previous versions

Downgrading FortiClient version 5.4.4 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 5.4.4 support

The following table lists version 5.4.4 product integration and support information.

FortiClient 5.4.4 support information

Desktop Operating Systems	• 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)
Server Operating Systems	• Microsoft Windows Server 2008 R2 • Microsoft Windows Server 2012, 2012 R2 • Microsoft Windows Server 2016 FortiClient 5.4.4 does not support Windows Server Core.
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 and later
FortiAuthenticator	• 4.2.0 • 4.1.0 and later • 3.3.0 and later • 3.2.0 and later • 3.1.0 and later • 3.0.0 and later

FortiClient EMS	• 1.2.0 and later • 1.0.0 and later FortiClient 5.4.1 enhancements to the Vulnerability Scan feature require FortiClient EMS 1.0.1 and later.
FortiManager	• 5.4.1 and later
FortiOS	• 5.4.1 and later Some FortiClient features are dependent on specific FortiOS versions. Only IPsec VPN and SSL VPN are supported with the following FortiOS versions: • FortiOS 5.6.0 and later • FortiOS 5.4.0 • FortiOS 5.2.0 and later
FortiSandbox	• 2.4.0 and later • 2.3.0 and later • 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.

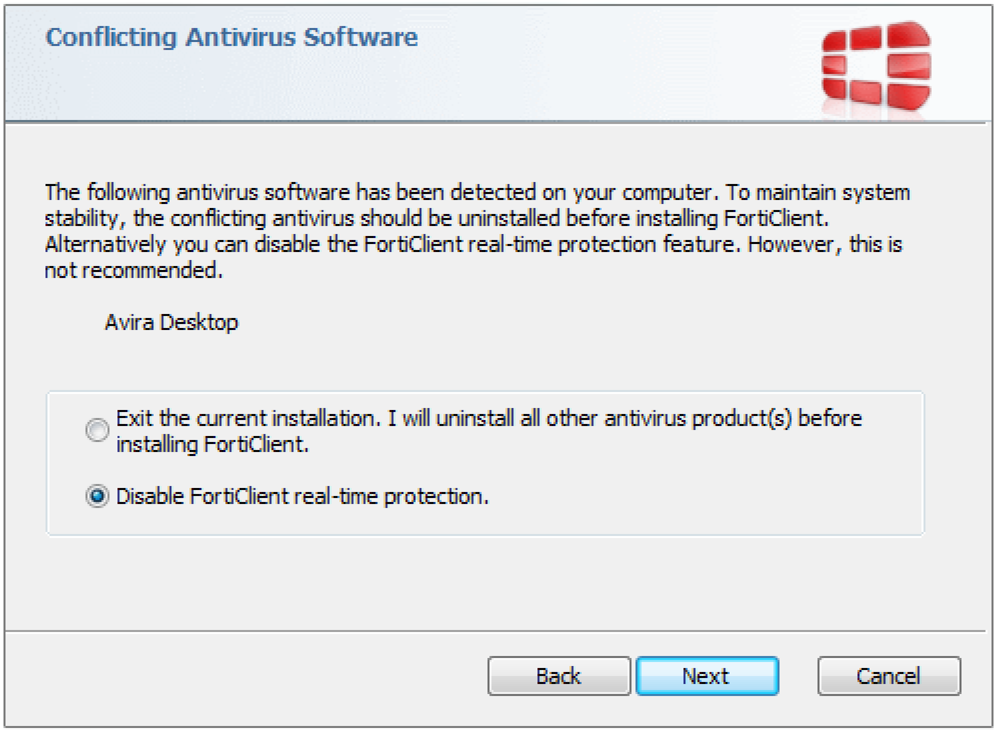
If the client workstation is configured to a regional language setting that is not supported by FortiClient, it defaults to English.

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



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 5.4.4. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
0379372	FortiClient 5.4 causes PC crash on Windows 8.1 Enterprise x64
0389712	User unable to establish SSL VPN connection (Windows 10 Build 1607)
0399409	FortiClient 5.4.2 does not install split tunneling routes
0401461	IPsec password issues
0402357	FortiClient upgrade causes reboot pop-up loop
0404824	Application is blocked as Riskware, even when Riskware detection is off
0405204	SSL exclusive routing doesn't work properly
0406356	Fresh install of FortiClient on Windows 10, message center shows 3 *Both FCT and Windows AV are disabled*
0406548	Problem with Numara TrackIT application when Web Filter is enabled on FortiClient
0408258	Backup config has `use_legacy_ssl_adapter=1`
0409622	Warn when SSL VPN cipher options do not match
0409809	FortiClient local privilege escalation with VPN before logon and untrusted certificate
0410237	FortiClient has unreliable behaviour while submitting the file to FortiSandbox
0410361	Malicious website violation list inconsistent between Windows and Mac
0411339	FortiClient conflict with PostgesSQL client Software / Vision Agent
0412343	SSL VPN performance testing
0412815	Should not allow FortiClient to be shut down if it's in registered status
0413078	Missing language-transforms file in `FortiClientSetup_5.4.3.0870_x64.zip`
0414854	Folders with commas fail to be added properly when config restored or pushed by EMS to FortiClient

Bug ID	Description
0415515	Should not show *FTM-Push* after unset `ftm-push`
0415712	B742: SSL VPN hostcheck was not working on Windows 7 32-bit PC when process runs on SYSTEM account
0416352	B870 : FortiClient doesn't connect to Telemetry gateway IP after registration
0416845	SSL VPN -> Bytes sent is not correct
0417061	FortiClient Console crashes when registered to EMS 1.2
0417286	Diagnostic Tool is missing Windows Update log on Windows 10
0417306	FortiClient 5.4.3 End User Avatar crashes on Windows 7 x86
0418095	SSL VPN: when FortiGate does not set DNS server, DNS will fail at the client side when using the new driver
0421901	SSL VPN V6 ->should reset IP address
0422163	Incorrect Compliance Result flag for third-party AV check
0423244	FortiProxy takes high CPU usage with all related features disabled
0423829	With FortiClient installed, cannot access mail.yahoo.com
0424511	Single Sign On Mobility Agent does not allow multiple FAC server entries
0434289	FortiClient b870 with trendmicro AV cause HTTP websites to fail to load on Windows 10
0435507	FortiClient GUI console displaying incorrect number of threats detected
0438057	FortiClient should protect itself from not getting into a non-responsive state
0438295	`fcconfig` crash
0438796	`fmon.exe` still running in the endpoint when EMS profile disabled Antivirus feature
0438799	Remove internal installer commands from installer help dialog
0438823	Click *OK* on *Permission Denied* should reset connection status while making SSL VPN connection
0438889	VPN V6 doesn't work properly
0439113	SSL VPN ->Should use new driver by default

Bug ID	Description
0439644	SSL V6 duplicate IP address
0440037	IPS engine categorized many application as storage backup
0440037	IPS engine categorized many application as storage backup
0440485	FortiClient console does not perform an integrity test
0440708	SSL VPN certificate warning pops up three times
0440721	Failed to uncheck the *Topline* checkbox for third-paty application patch
0441005	FortiClient console and FortiTray issues
0441394	FortiClient cannot reconnect to FortiGate after the FortiClient is quarantined and disconnected from FortiGate

Known Issues

The following issues have been identified in FortiClient (Windows) 5.4.4. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Bug ID	Description
0389865	FortiClient does not check the revocation status of SubCA
0399256	IPsec tunnel before Windows logon - certificate read from Smartcard with PIN
0403544	VPN IPsec auto-connect does not work on FortiClient 5.4.2 and Windows 7 (32-bit)
0405196	When users log in to their PC, the endpoint shows out of sync for a few minutes
0405303	Unable to use IPSec VPN with Client/PC PKI Certificate
0409656	FortiClient removed default route of LTE card after connecting to IPsec VPN
0410841	Only legacy VPN before logon works on Windows 8.1 and Windows Server 2012R2
0434983	Fortiproxy process crashed randomly
0437697	[Profiles][Sandbox] Sandbox setting issues between EMS 1.2.0 and FortiClient 5.4.3
0438876	User could still copy and upload downloaded network files when RTP was using FortiSandbox signature contained the file
0439534	BSOD on Windows 7 64-bit
0440034	FortiClient firewall detail page failed to show all firewall rules
0440185	b0870: FortiClient loses saved VPN password with weak connection
0440589	Cannot go back to FortiClient dashboard from setting by clicking dashboard in menu
0441216	`FortiESNAC` crashed
0441409	FortiClient Sandbox *Scan USB* and *Scan mapped network drive* stayed disabled when EMS profile enabled them **Workaround**: In the EMS (1.2.0 or newer), open the assigned endpoint profile for editing, and select the Advanced XML configuration tab. Click *Edit*; click *Test*, and then save the configuration. No need to change anything in the advanced configuration before saving it.
0441429	Reboot prompt triggered when an EICAR sample is quarantined on network

Bug ID	Description
0441440	Product name did not change on rebranding
0441447	FortiClient Application Firewall blocking network service caused no profile update from EMS
0441575	Invalid file path when Sandbox sample is detected
0441674	`fortifws.exe` process crashed

High Performance Network Security

Copyright© 2017 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.