

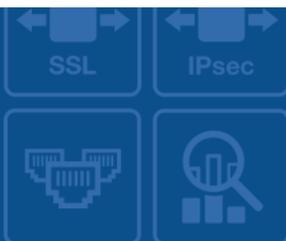


FORTINET[®]
High Performance Network Security



FortiClient (Windows) - Release Notes

VERSION 5.4.2



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



March 15, 2017

FortiClient (Windows) 5.4.2 Release Notes

04-542-393396-20170315

TABLE OF CONTENTS

Change Log	4
Introduction	5
Licensing	5
Standalone Mode	5
Managed Mode	5
Special Notices	7
SSL VPN cannot connect after upgrade to FortiOS to 5.4.x	7
FortiClient upgrade on Windows XP	7
Cooperative Security Fabric Upgrade	7
Installing FortiClient on Windows 7	8
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	9
What's New in FortiClient (Windows) 5.4.2	10
Installation Information	11
Firmware images and tools	11
Upgrading from previous FortiClient versions	11
Downgrading to previous versions	12
Firmware image checksums	12
Product Integration and Support	13
FortiClient 5.4.2 support	13
Language support	14
Conflicts with third party antivirus products	15
Conflicts with Cisco Systems VPN client	15
Resolved Issues	16
Known Issues	19

Change Log

Date	Change Description
2016-11-10	Initial release.
2016-11-17	Removed 389753 from Resolved Issues.
2016-11-21	Added 389240 and 390356 to Resolved Issues.
2016-12-08	Moved 295413 to Known Issues.
2016-12-12	Updated description of 390265.
2017-01-05	Added the following special notice: SSL VPN cannot connect after upgrade to FortiOS to 5.4.x on page 7.
2017-03-15	Changed FortiOS support from 5.4.1, 5.4.2 to 5.4.1 and later.

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (Windows) 5.4.2 build 0860.

- [Introduction](#)
- [Special Notices](#)
- [What's New in FortiClient \(Windows\) 5.4.2](#)
- [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.

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

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.

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 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 simultaneously. 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) 5.4.2

This section identifies the new features and enhancements in FortiClient (Windows) 5.4.2. For more information, see the *FortiClient Administration Guide*.

- FortiClient in standalone mode no longer includes a banner at the bottom of the console.

Installation Information

Firmware images and tools

When installing FortiClient version 5.4.2, 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_5.4.2.0860.exe
Standard installer for Microsoft Windows (32-bit).
- FortiClientSetup_5.4.2.0860.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_5.4.2.0860_x64.exe
Standard installer for Microsoft Windows (64-bit).
- FortiClientSetup_5.4.2.0860_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_5.4.2.0860.zip
A zip package containing miscellaneous tools, including the FortiClient Configurator tool and VPN Automation files.



When creating a custom FortiClient 5.4.2 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 5.4.2 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 5.4.2: [Introduction on page 5](#), [Special Notices on page 7](#), and [Product Integration and Support on page 13](#).

Downgrading to previous versions

Downgrading FortiClient version 5.4.2 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 5.4.2 support

The following table lists version 5.4.2 product integration and support information.

FortiClient 5.4.2 support information

Desktop Operating Systems	<ul style="list-style-type: none">• 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)
Server Operating Systems	<ul style="list-style-type: none">• Microsoft Windows Server 2008 R2• Microsoft Windows Server 2012, 2012 R2
Minimum System Requirements	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 5.4.2• 5.4.1
FortiAuthenticator	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none"> • 1.0.0 and later <p>FortiClient 5.4.1 enhancements to the Vulnerability Scan feature require FortiClient EMS 1.0.1 and later.</p>
FortiManager	<ul style="list-style-type: none"> • 5.4.2 • 5.4.1
FortiOS	<ul style="list-style-type: none"> • 5.4.1 and later <p>Some FortiClient features are dependent on specific FortiOS versions.</p>
FortiSandbox	<ul style="list-style-type: none"> • 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



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 5.4.2. For inquiries about a particular bug, please contact [Customer Service & Support](#).

Bug ID	Description
0373225	Improve VPN auto-connect user experience
0375898	There is no prompt informing user of unfixed critical or high vulnerabilities
0378644	Configuration update from EMS will restart scheduled AV scan
0378739	Application <code>eLeader.Business.SYS</code> is being crashed with FortiClient v5.4.1
0379641	FortiClient Configurator not populating XML directives correctly
0379665	On-demand scan goes on forever if update happens
0379922	FortiClient Configurator 5.4.1 removes configuration settings
0380130	Upgrade to 5.4.1 - No <i>VPN tunnel before logon</i> dialog box shown for Windows 10
0380607	Unable to renew the password with FortiClient 5.4.1
0382098	DNS issues with SSL VPN
0383032	Custom WF blocking page
0385662	FortiClient 5.4.1 crashes
0385889	Compliance status in GUI is misleading
0386272	Add Fail over support to FDN, if the configured proxy is not reachable
0386879	Change priorities for FortiClient registration
0387678	FortiClient with Okta 2FA - placing cursor in incorrect field for user response
0388377	FortiClient should send KA message immediately after receiving compliance rules or configuration
0389867	RTP settings break WF profile compliance
0390095	Sending Avatar image should be enabled by default
0390107	FortiClient IPSec set a random DNS server

Bug ID	Description
0390255	FortiTray crash
0390265	SSL VPN install issue: fortissl dialup connection shows <i>device missing</i>
0390548	FortiClient user Avatar agent crashed
0390739	Issues when enabling VPN before logon on Windows 10
0390740	RA certificate does not show on settings
0390807	Should not trigger non-compliance
0390907	Frequently show message <i>Configuration update was received from FortiGate</i>
0390968	FortiClient logs alert but not action taken
0391070	VPN auto-connect does not work
0391426	No <i>Fix All</i> button on compliance page
0392304	Lock/unlock doesn't work with special characters
0380668	When the network connection was up and down, FortiClient does not try to reconnect SSL VPN
0390067	Unusually high volume of <code>INIT</code> commands (for web filter) from FortiClient
0377789	Notification server gone after FDS or manual upgrade
0374791	Create manifest file for <i>FortiClient_Diagnostic_Tool.exe</i>
0304447	Auto-connect and always up

Common Vulnerabilities and Exposures

Bug ID	Description
389240	FortiClient (Windows) 5.4.2 is no longer vulnerable to the following CVE-References: <ul style="list-style-type: none">• 2016-2177• 2016-2178• 2016-2179• 2016-2181• 2016-2182• 2016-2183• 2016-6302• 2016-6303• 2016-6304• 2016-6305• 2016-6306• 2016-6307• 2016-6308 Visit https://fortiguard.com/psirt for more information.
390356	FortiClient (Windows) 5.4.2 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none">• 2016-6153 Visit https://fortiguard.com/psirt for more information.

Known Issues

The following issues have been identified in FortiClient (Windows) 5.4.2. For inquiries about a particular bug or to report a bug, please contact [Customer Service & Support](#).

Bug ID	Description
0291192	Application Firewall does not effectively block TOR browser methods
0303146	Windows 10 cannot pass traffic after connection to SSL VPN (conflict with Pulse Secure)
0374133	IPsec VPN works with x.509 certs, but not with Windows certificate store
0378018	FortiClient 5.4 - FortiTray not responding prevents auto-connect VPN
0378100	FortiClient causes .NET Framework error on Windows 7
0387850	Unable to move FortiClient from old EMS to new EMS
0388420	When enabling FortiClient AV, PC performance and application impacted
0389865	FortiClient does not check the revocation status of SubCA
0390034	FortiClient Crash and SSL VPN Hangs %98
0391546	FortiClient (Windows) causing One Solution RMS application to stop working and crash
0392477	GUI Settings page does not respond when clicking the <i>Cancel</i> button
0394982	IPsec VPN stayed in connection stage forever when switching users
0394241	FortiClient broadcast registration on IPsec VPN connection randomly failed
0393173	C&C Attack Communication with Botnet does not log in to FortiClient GUI
0392902	Different OTP challenge window for IPsec and SSLVPN
0392651	From FortiClient ver 5.4.1, 3G/4G users cannot log into internal SAP server
0391093	FortiTray causes slowness in Gmail\Chat in Chrome
0390813	When Application Firewall is enabled, network performance is impacted a lot
0295413	Windows 10: popup message says AV is not enabled, even if it is enabled



FORTINET

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.