FortiClient (Windows) v5.2.1
Release Notes

FortiClient (Windows) v5.2.1 Release Notes

August 20, 2014

04-521-251127-20140820

Fortinet Document Library	docs.fortinet.com
Fortinet Video Library	video.fortinet.com
Customer Service & Support	support.fortinet.com
Training Services	training.fortinet.com
FortiGuard	fortiguard.com
Document Feedback	techdocs@fortinet.com

Table of Contents

Change Log

Date	Change Description
2014-08-20	Initial release.

Introduction

This document provides a summary of enhancements, support information, and installation instruction for FortiClient v5.2.1 build 0605. Please review all sections prior to installing FortiClient. For more information, see the FortiClient v5.2.1 Administration Guide available in the Fortinet Document Library.

This document includes the following sections:

- Introduction
- Installation Information
- Product Integration and Support
- Resolved Issues
- Known Issues
- Firmware Image Checksums

New features in FortiClient v5.2.1

The following is a list of new features in FortiClient v5.2.1

OpenSSL library

The OpenSSL library has been updated to the latest version 1.0.1i.

Logging to FortiManager/FortiAnalyzer

Uploading logs to FortiManager or FortiAnalyzer requires FortiClient to be registered to a FortiGate.

New features in FortiClient v5.2.0

The following is a list of new features in FortiClient v5.2.0.

Antivirus

Malware cleanup in safe mode

Malware that is already on a Microsoft Windows computer system that could not be removed in normal mode, may be removed by running FortiClient in safe mode. Only the FortiClient Antivirus feature is available in safe mode. Full or custom antivirus scans can be started while in safe mode. The resulting log files and any quarantined files, will be available both in safe mode, as well as after returning to normal mode.

The FortiClient installer always runs a quick antivirus scan on the target host system before proceeding with the installation. In case a virus on an infected system prevents downloading of the new FortiClient package, you can boot into safe mode, run the FortiClient installer to scan and quarantine the virus or malware, and then proceed with the installation.

Protection against security threats in URLs has moved to the Antivirus module

Malicious and Phishing URLs were previously configured and blocked as part of the Web Filtering feature. These are in the Security Risk category. This category has now been moved to become part of the Antivirus feature. When a custom FortiClient installation is created without the antivirus module, these threats are blocked by the Web Filtering feature.

View real-time protection events in the console

When an antivirus real-time protection event has occurred you can select to view these events in the FortiClient console. Select *AntiVirus* > *Threats Detected* and select *Real-time Protection events*. The `realtime_scan.log` will open in the default viewer.

Removable media scan

In FortiClient v5.2, you can select to perform an antivirus scan of all connected devices with removable storage. Select *AntiVirus* > *Scan Now* > *Removable media Scan* to scan these connected devices. When performing a *Full Scan*, removable storage is also scanned.

One-click button to enable antivirus

In the FortiClient console, you can enable the antivirus feature using a single button visible in the header. This is convenient in the event that you are on a tab other than the antivirus tab. The button is visible only when *Realtime Protection* is disabled.

Web Filtering

Manual URL filter list support

FortiClient now supports URL filters configured in the FortiOS security profile and applied to the FortiClient Profile.

Web Security

FortiClient Parental Control has been renamed Web Security. When FortiClient is registered to a FortiGate, Web Security is named Web Filter.

VPN

VPN over IPv6

VPN connections to the FortiGate can be established on a network that is configured with IPv6. New connections may be configured from the FortiClient console or through the XML configuration file. IPv6 is supported for IPsec and SSL VPN.

Note that FortiOS only supports VPN over IPv6 when both sides of the connection are using IPv6. A network with one end using IPv6 while the other end uses IPv4 is not supported.

Advanced VPN configuration in the FortiClient console

VPN configurations through the FortiClient console have been simplified since FortiClient v5.0. Only a few configuration entries were required and advanced configuration required use of the XML configuration file. In FortiClient v5.2, you can access IPsec VPN advanced settings in the FortiClient console. These advanced settings are useful when setting up connections to an IPsec VPN server other than a FortiGate.

Simplified FortiClient console for VPN only installations

FortiClient features may be customized in one of three ways:

- In the standard FortiClient installer,
- In the FortiClient Configurator tool,
- In the FortiGate FortiClient Profile, you can turn off and hide unused features.

When only the VPN feature is selected with any of these three methods, FortiClient will present a simplified console, with no tabs on the left-hand side.

VPN auto-connect based on DHCP off-net determination

VPN auto-connect ensures that FortiClient creates a VPN connection to the FortiGate when considered to be off-net. A site administrator, who has configured Endpoint Control on their FortiGate, may choose to enable VPN auto-connect in the Endpoint Control profile.

Computer endpoints or clients in the network should use the designated DHCP server for IP address assignments. The DHCP server sends a special tag within the protocol to identify if the client is on-net or off-net. The on-net status indicates that the endpoint is within the corporate network protected by the FortiGate.

When the client is off-net, FortiClient will automatically attempt to establish a VPN connection to the VPN server indicated in the FortiGate Endpoint Control configuration. When the client is on-net, no VPN connection is required.

This feature requires FortiOS v5.2.0 or later. The FortiGate must use a FortiClient v5.2 license.

VPN auto-connect improvements

VPN auto-connect/always-up regardless of how the VPN connection ended.

Application Firewall

Updated Application Firewall Engine

FortiClient now uses a common application firewall detection engine with FortiOS. This provides enhanced detection coverage. Signatures configured in the FortiGate security profile are available to FortiClient.

When the application being blocked is web-based, a message is displayed to the user in the web browser. For non-browser applications, a system tray notification is displayed. Notifications are disabled by default to reduce distractions to every day use of the system.

Endpoint Control

Improvements to the Endpoint Control page

The FortiGate *Endpoint Protection* > *FortiClient Profiles* page has been simplified.

VPN auto-connect based on DHCP off-net determination

See VPN auto-connect based on DHCP off-net determination.

Installation

Custom install - select features to include in the FortiClient install

The FortiClient Configurator can be used to create custom FortiClient MSI installers with various combinations. Some of the customization options available include:

- Select FortiClient features of interest
- Provide a custom XML configuration file
- Rebrand the FortiClient product

The customized executable installer generated may be used to install on all supported platforms manually. An MSI installer is also created for distribution using Active Directory or SCCM.

A FortiClient v5.2 license is required to use the FortiClient Configurator tool.

Client installer and Configurator updates (more granular installation options)

Select to install the complete feature set or VPN only in the regular client installer. When selecting to use the Configurator tool, you can install the complete feature set, a custom feature set, VPN only, or SSO only.

Client rebranding capabilities (via FortiClient Configurator)

You can edit various text and graphical UI elements using the rebranding option in the FortiClient Configurator tool.

Licensing

Licensing on the FortiGate 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.

The VPN on-net, off-net feature in Endpoint Control will be activated only when the FortiGate, to which FortiClient is registered, is running FortiOS v5.2 with a FortiClient v5.2 license.

Client limits

The following table shows client limits per FortiGate model series.

Table 1: FortiClient license upgrade

FortiGate Series	Free Registrations	FortiClient License Upgrade
FortiGate/FortiWiFi 30 to 90 series	10	1 year FortiClient license subscription for up to 200 clients
FortiGate 100 to 300 series	10	1 year FortiClient license subscription for up to 600 clients
FortiGate 500 to 800 series, FortiGate vM01, FortiGate VM02	10	1 year FortiClient license subscription for up to 2000 clients
FortiGate 1000 series, FortiGate VM04	10	1 year FortiClient license subscription for up to 8000 clients
FortiGate 3000 to 5000 series, FortiGate VM08	10	1 year FortiClient license subscription for up to 20 000 clients

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

For more information, go to www.forticlient.com.

Installation Information

Firmware images and tools

When installing FortiClient v5.2.1, 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_5.2.1.0605.exe

  Standard installer for Microsoft Windows (32-bit).
- FortiClientSetup_5.2.1.0605.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_5.2.1.0605_x64.exe

  Standard installer for Microsoft Windows (64-bit).
- FortiClientSetup_5.2.1.0605_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_5.2.1.0605.zip

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

When creating a custom FortiClient v5.2.1 installer using the FortiClient Configurator tool, you can choose which features to install. You can also select to enable or disable software updates, configure SSO, and rebrand FortiClient.

Upgrading from FortiClient v4.2 and later

FortiClient v5.2.1 supports manual upgrade from FortiClient v4.2 and later.

Please review the Introduction and Product Integration and Support chapters prior to installing FortiClient v5.2.1.

Downgrading to previous versions

Downgrading FortiClient v5.2.1 to previous FortiClient versions is not supported.

Product Integration and Support

FortiClient v5.2.1 support

The following table lists FortiClient v5.2.1 product integration and support information.

Table 2: FortiClient v5.2.1 support information

Desktop operating systems	• Microsoft Windows XP (32-bit) • Microsoft Windows Vista (32-bit and 64-bit) • Microsoft Windows 7 (32-bit and 64-bit) • Microsoft Windows 8 (32-bit and 64-bit) • Microsoft Windows 8.1 (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.
FortiOS versions	• 5.0.0 and later • 5.2.0 and later Some FortiClient features are dependent on specific FortiOS versions.
FortiAnalyzer versions	• 5.0.2 and later
FortiManager versions	• 5.0.2 and later
FortiAuthenticator versions	• 2.2.0 and later • 3.0.0
Web Browser	• Microsoft Internet Explorer version 8 or later

Language support

The following table lists FortiClient language support information.

Table 3: Language support

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

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

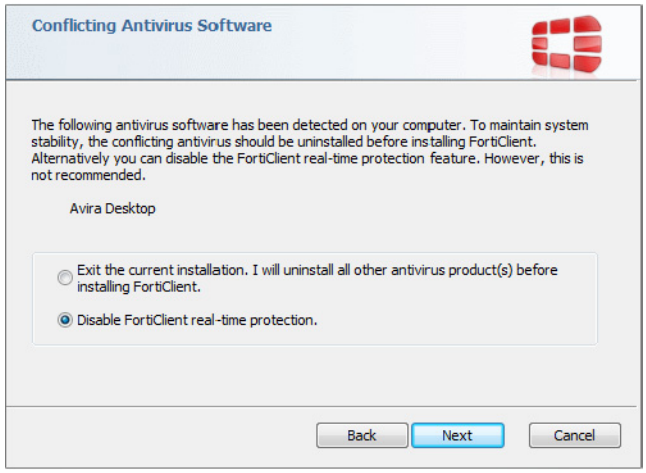
If the client workstation is configured to a regional language setting that is not supported by FortiClient, it defaults to English.

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 the option to disable FortiClient Real Time Protection (RTP).

Figure 1: 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 resolved issues table listed below does not list every bug that has been corrected with FortiClient v5.2.1 build 0605. For inquires about a particular bug, please contact Customer Service & Support.

Table 4: Resolved issues

Bug ID	Description
0239752	FortiClient conflicts with Cisco VPN.
0243805	FortiClient IPsec VPN negotiation window is displayed when logging into a workstation.
0245291	FortiClient configuration does not allow more than 53 web exclusions in the console.
0245380	FortiClient installer is missing the registry keys for fssoma.
0245443	Added an option to hide the desktop icon.
0246606	FortiClient custom MSI settings are not kept when installed by a user without admin rights.
0249261	Web Filter stays enabled when `disable_when_managed=1` and the client is on-net.

Known Issues

The known issues tables listed below do not list every bug that has been identified with FortiClient v5.2.1 build 0605. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Table 5: Known issues

Bug ID	Description
0241463	Provide support for DHCP over IPsec VPN while using IPv6.
0242217	Application Firewall cannot process IPv6 addresses.
0246479	IPsec VPN should support use of Elliptic Curve certificates.

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*.

Figure 2: Firmware image checksum tool