



FortiClient - Release Notes

VERSION 5.0.11

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



November 30, 2016

FortiClient 5.0.11 Release Notes

04-5011-397202 -20161130

TABLE OF CONTENTS

Change Log	4
Introduction	5
What's new in FortiClient version 5.0.....	5
Licensing.....	7
Client limits.....	8
Upgrade Information	9
Firmware images and tools.....	9
FIPS images and tools.....	9
Regular images and tools.....	9
Upgrading from FortiClient version 5.0.0 or later.....	10
Upgrading from FortiClient Lite version 4.3.....	10
Upgrading from FortiClient Connect version 4.3.....	10
Upgrading from FortiClient version 4.2.....	10
Manual upgrade.....	10
Upgrade through FDS.....	11
Upgrade through FortiManager.....	11
Downgrading to previous versions.....	12
Firmware image checksums.....	12
Product Integration and Support	13
FortiClient version 5.0.11 support.....	13
Language support.....	14
Conflicts with third party antivirus products.....	14
FIPS.....	15
Resolved Issues	16
Known Issues	17

Change Log

Date	Change Description
2016-11-30	Initial release.

Introduction

This document provides the following information for FortiClient version 5.0.11 build 0367:

- What's new in FortiClient version 5.0
- Licensing
- Upgrade Information
- Product Integration and Support
- Resolved Issues
- Known Issues

For more information, see the *FortiClient 5.0.11 Administration Guide* available in the [Fortinet Document Library](#).

What's new in FortiClient version 5.0

The following is a list of enhancements in FortiClient version 5.0:

FortiClient version 5.0.11

- There are no new features or enhancements in this release.

FortiClient version 5.0.10

- FortiClient can now run in Federal Information Processing Standard (FIPS) mode. It is certified to FIPS 140-2 Level 1 and Level 2. For reference, please see:
 - NIST Computer Security Publications
 - FIPS (Federal Information Processing Standards)
 - <http://csrc.nist.gov/publications/PubsFIPS.html>
- The OpenSSL library has been updated to the latest version 1.0.1k.

FortiClient version 5.0.9

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

FortiClient version 5.0.8

- There are no new features or enhancements in this release

FortiClient version 5.0.7

- Improved antivirus scanning performance
- Improvements to the Endpoint Control GUI

FortiClient version 5.0.6

- Improved usability of the repackager tool
- Repackaged clients can be upgraded
- Option to drop IPv6 traffic when an IPsec VPN connection is established. IPv4 traffic is sent through the tunnel or otherwise, depending on whether split tunnel is used.

FortiClient version 5.0.5

- Enhanced file copy performance
- Customized installation: Users may choose to install the entire FortiClient feature set or only the VPN features.
- Scan for viruses on the target system before installing FortiClient
- Enhanced GUI performance

FortiClient version 5.0.4

- Assign endpoint control profiles based on Active Directory group.
This feature requires a FortiGate running FortiOS version 5.0.3 or later.
On a system using Active Directory (AD) for user account verification, FortiClient will send the AD user name and group to the FortiGate during Endpoint Control (EC) registration. The FortiGate may be configured to select the correct EC profile by user or group.
- Display endpoint control profile details in registration dialog box.
This feature requires a FortiGate running FortiOS version 5.0.3 or later.
- Removed Vulnerability Scan (VCM) and Application Firewall for standalone clients.
This feature requires registration to a FortiGate running FortiOS version 5.0.2 or later.
FortiGate administrators may choose to display these two features (on FortiClient) for users registered to the FortiGate.
- Enhanced how the list and status of FortiGates are displayed for Endpoint Control registration

FortiClient version 5.0.3

- Enhancements to FortiProxy
- Improved VPN usability with FortiToken

FortiClient version 5.0.2

- Customizable console for registered clients
- Endpoint control registration with redundant gateways (maximum 20).
This feature enables roaming clients.
- Enhancement to the remembered FortiGates feature
- FortiClient uploads traffic, event, and vulnerability scan logs to FortiAnalyzer/FortiManager.
This feature requires a FortiAnalyzer/FortiManager running version 5.0.2 or later and a FortiGate running FortiOS version 5.0.2 or later.
- SSL VPN realm support (command line)
- Synchronize VPN elements; `save password`, `autoconnect`, and `always up`; with the FortiGate.
This feature requires a FortiGate running FortiOS version 5.0.2 or later.
- Web category filtering safe search support.
For popular search sites or portals including Google, Bing, Yahoo, and Yandex.

FortiClient version 5.0.1

- Endpoint Control registration over SSL VPN or IPsec VPN
- Remember multiple FortiGates for Endpoint Control registrations
- FortiClient console improvements

FortiClient version 5.0.0

- Antivirus and Antimalware
Protection against the latest virus, grayware (adware/riskware) threats.
Client antivirus is free, and auto updates every three hours.
- Application firewall
Block, allow, and monitor applications that send traffic to the network.
- Bring Your Own Device (BYOD)
- Diagnostic tool
- Enhancements to the FortiClient console
- Endpoint Management using FortiGate, including:
 - Automatic endpoint registration. User initiated endpoint registration.
 - Deploy VPN (IPsec/SSL) configuration.
 - Enable or disable antivirus real-time protection.
 - Manage and deploy web filtering and application firewall configuration.
- Localization support
- Parental Control/Web Filter
Block, allow, warn, and monitor web traffic based on category.
- Remote Access (IPsec and SSL VPN)
Secure Virtual Private Network access to your network.
Supports multiple gateways for a single tunnel.
- Rootkit detection and removal
- Single Sign-On Mobility agent support with FortiAuthenticator/FSSO collector agent
- Support automatic executing of a custom batch script via an IPsec VPN tunnel
- Support multiple (maximum 10) gateway IP/FQDN in a single IPsec VPN configuration
- Support XML configuration
- VPN from system tray
- VPN auto connect/always up
Supports the ability to automatically connect to a VPN tunnel without user interaction.
Supports the ability to configure the VPN to always be connected.
- Vulnerability scan
- Identify system and application vulnerabilities.

Licensing

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

Client limits

The following table shows client limits per FortiGate model series.

FortiClient license upgrade

FortiGate Series	Free registrations	FortiClient license upgrade SKU
FortiGate/FortiWiFi 30 to 40 series	10	No upgrade license.
FortiGate/FortiWiFi 60 to 90 series	10	200 client registrations FCC-C0102-LIC
FortiGate 100 to 800 series and VM01 to VM02	10	2000 client registrations FCC-C0103-LIC
FortiGate 1000 to 5000 series and VM04 to VM08	10	8000 client registrations FCC-C0105-LIC



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



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

Upgrade Information

Firmware images and tools

FortiClient images and tools are available for both FIPS and regular (non-FIPS) for both 32-bit and 64-bit environments.

FIPS images and tools

- FortiClientFIPSSetup_5.0.10.0367.exe: Standard FIPS installer for 32-bit Microsoft Windows.
- FortiClientFIPSSetup_5.0.10.0367.zip: A .zip package containing FIPS FortiClient.msi and language transforms for 32-bit Microsoft Windows. Some properties of the MSI package can be customized with the FortiClient Configurator tool.
- FortiClientFIPSSetup_5.0.10.0367_x64.exe: Standard FIPS installer for 64-bit Microsoft Windows.
- FortiClientFIPSSetup_5.0.10.0367_x64.zip: A .zip package containing FIPS FortiClient.msi and language transforms for 64-bit Microsoft Windows. Some properties of the MSI package can be customized with FortiClient Configurator tool.
- FortiClientFIPSTools_5.0.10.0367.zip: A .zip package containing miscellaneous tools including the FortiClient Configurator tool and VPN Automation files.

Regular images and tools

FortiClientOnlineInstaller_5.0.10.0367.exe: Minimal installer for 32-bit and 64-bit Microsoft Windows. This file downloads and installs the latest FortiClient file from the public FortiGuard Distribution Server (FDS).

FortiClientSetup_5.0.10.0367.exe: Standard installer for 32-bit Microsoft Windows.

FortiClientSetup_5.0.10.0367.zip: A .zip package containing FortiClient.msi and language transforms for 32-bit Microsoft Windows. Some properties of the MSI package can be customized with the FortiClient Configurator tool.

FortiClientSetup_5.0.10.0367_x64.exe: Standard installer for 64-bit Microsoft Windows.

FortiClientSetup_5.0.10.0367_x64.zip: A .zip package containing FortiClient.msi and language transforms for 64-bit Microsoft Windows. Some properties of the MSI package can be customized with FortiClient Configurator tool.

FortiClientTools_5.0.10.0367.zip: A .zip package containing miscellaneous tools including the FortiClient Configurator tool and VPN Automation files.



When upgrading on a Microsoft Windows XP system, a warning dialog box is displayed indicating that one of the files to be updated is currently in use. Please select the **Ignore** button to continue with the upgrade.

Users with newer Microsoft Windows OS versions will receive a different warning dialog box. It warns that a reboot will be required to complete the installation. Please click the **OK** button to continue with the installation.



An Endpoint License for FortiGate is required to use the FortiClient Configurator tool..

Upgrading from FortiClient version 5.0.0 or later

FortiClient version 5.0.11 supports direct upgrade from FortiClient version 5.0.0 or later, along with the regular manual upgrade method.



Please review the [Introduction on page 5](#), [Known Issues on page 17](#), [Product Integration and Support on page 13](#), and [Known Issues on page 17](#) chapters prior to upgrading. For more information on upgrading FortiClient, see the *FortiClient 5.0.11 Administration Guide* available in the [Fortinet Document Library](#).

Upgrading from FortiClient Lite version 4.3

FortiClient version 5.0.11 supports manual upgrade from FortiClient Lite version 4.3.5.

Upgrading from FortiClient Connect version 4.3

FortiClient version 5.0.11 supports manual upgrade from FortiClient Connect version 4.3.5.



FortiClient version 5.0.11 does not support upgrading from older patch releases of FortiClient version 4.3 (Patch Release 1 to 4).

Upgrading from FortiClient version 4.2

FortiClient version 5.0.11 supports manual upgrade, upgrade through FortiGuard Distribution Servers (FDS), and upgrade through FortiManager version 4.3 from FortiClient version 4.2.

A successful software upgrade will convert and update all existing version 4.2 configurations to FortiClient version 5.0.11 formats. For information on exceptions, see [Known Issues on page 17](#) before starting an upgrade.

An Internet connection is required for both manual and FDS software upgrades.

Manual upgrade

FortiClient version 4.2 may be upgraded to FortiClient version 5.0.11 by running the FortiClient version 5.0.11 installation file on the client computer. The installation file can be downloaded from the following sites:

- Fortinet Customer Service & Support: <https://support.fortinet.com>
- FortiClient homepage: www.forticlient.com

Upgrade through FDS

FortiClient version 5.0.11 is available through FDS for existing FortiClient version 4.2 users. Users will receive an update notification and they may choose to accept or reject the update.

If the user accepts the update, FortiClient will proceed to complete the installation of FortiClient version 5.0.11. If the update notice is rejected, the notification may be repeated at regular intervals.

Some users may have configured to *run updates automatically*. For such users, the upgrade will proceed without a prompt.

Upgrade through FortiManager

FortiClient version 4.2 client computers that are managed by FortiManager may be upgraded to FortiClient version 5.0.11 by pushing the update from the FortiManager.



FortiClient version 5.0.11 does not support use of FortiManager for central management. FortiGate devices running FortiOS 5.0 may be used for endpoint control.

After a successful upgrade, previously managed FortiClient systems will no longer be managed from FortiManager. The administrator should consider the impact of this on FortiClient distribution.

A software upgrade may be initiated by the administrator by manually uploading the FortiClient version 5.0.11 MSI installation package to FortiManager version 4.3.

The end-user receives a notification requesting permission to proceed with the upgrade. The manual package upload allows the administrator to configure the IP address of a FortiGate that will manage the clients upon completion of the upgrade.

Push update from FortiManager to managed FortiClient agents:

1. Obtain the FortiClient version 5.0.11 installation files from the Fortinet Customer Service & Support portal, <https://support.fortinet.com>. To download firmware images you require a support account with a valid support contract.
2. Configure the IP address of the FortiGate that will be used for managing the clients after the upgrade is completed.
3. Create a custom MSI installer file.
4. Configure *Endpoint Control* on your FortiGate device.
5. Upload the customized MSI installer file to FortiManager.
6. Distribute the MSI installer file to registered clients.
FortiClient will register to the FortiGate device after the update.
For more information on the *FortiClient Configurator tool*, see the *Custom FortiClient Installations* chapter in the *FortiClient 5.0.11 Administration Guide*.

Downgrading to previous versions

FortiClient version 5.0.11 does not support downgrading to previous FortiClient versions.

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, <https://support.fortinet.com>. To verify the integrity of the download, select the *Checksum* link next to the *HTTPS* download link. A dialog box will be displayed with the image file name and checksum code. Compare this checksum with the checksum of the firmware image.

Product Integration and Support

FortiClient version 5.0.11 support

The following table lists FortiClient version 5.0.11 product integration and support information:

Operating System	<ul style="list-style-type: none">• 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)
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 NIC for network connections• Wireless adapter for wireless network connections• Adobe Acrobat Reader for FortiClient documentation• MSI installer 3.0 or later.
FortiOS	<ul style="list-style-type: none">• 5.0.0 and later <p>Some FortiClient features are dependent on specific FortiOS versions.</p>
FortiAnalyzer	<ul style="list-style-type: none">• 5.0.2 and later• 5.2.0 and later
FortiManager	<ul style="list-style-type: none">• 5.0.2 and later• 5.2.0 and later
FortiAuthenticator	<ul style="list-style-type: none">• 2.2.0 and later• 3.0.0 and later• 3.1.0 and later• 3.2.0 and later
Web Browser	Microsoft Internet Explorer version 8 or later.

Language support

The following table lists FortiClient language support information.

Language support

Language	Graphical User Interface	XML Configuration	Documentation
English	✓	✓	✓
Chinese (Simplified)	✓	-	-
Chinese (Traditional)	✓	-	-
French (France)	✓	-	-
German	✓	-	-
Japanese	✓	-	-
Korean	✓	-	-
Portuguese (Brazil)	✓	-	-
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 the option to disable FortiClient Real Time Protection (RTP).

When upgrading from an older version of FortiClient which does not have the antivirus feature installed, a similar search is done.

FIPS

FortiClient version 5.0.11 supports running in FIPS mode. For each of the two architectures: 32-bit or 64-bit, there are two builds provided: regular non-FIPS and FIPS build.

The newly added FIPS build will only run in FIPS mode. This image has some slightly different implementations of FortiClient features. Here are some notable ones:

- a license key is required at the time of installation;
- only the VPN feature is installed;
- the Endpoint Control feature is, like all other non-VPN features, not installed;
- no software or signature updates are available from the FDS.

There are also a few strict restrictions to cryptography functions and resources. The following are some examples:

- MD5 and DES are both disabled
- digital certificate key length must be more than 1024 bits
- an external random number generator may be used for seeding random numbers.

Resolved Issues

The following issues have been fixed in FortiClient version 5.0.11. For inquiries about a particular bug, please contact [Fortinet Customer Service & Support](#).

Bug ID	Description
0275162	Uninstall Failed
0270263	FCT features all shown empty content after registered to FortiGate
0270396	Error if registered with user name as {888}

Known Issues

The following are known issues reported in FortiClient version 5.0.11. For inquiries about a particular bug or to report a bug, please contact [Fortinet Customer Service & Support](#).

Bug ID	Description
0397013	Windows server 2008r2 reported failure to log onto server after FortiClient enabled <i>VPN before logon</i>
0397008	Windows login page duplicated users after enabling <i>VPN before logon</i>
0396879	FCT restore with non-password file still showed password field
0396268	Empty WF Categories