FortiClient (Windows) v5.0 Patch Release 7
Release Notes

FortiClient (Windows) v5.0 Patch Release 7 Release Notes

November 28, 2013

04-507-224699-20131128

Technical Documentation	docs.fortinet.com
Knowledge Base	kb.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
2013-11-28	Initial release.

Introduction

This document provides a summary of enhancements, support information, and installation instruction to upgrade your client to FortiClient (Windows) v5.0 Patch Release 7 build 0333. Please review all sections prior to upgrading. For more information, see the *FortiClient v5.0 Patch Release 7 Administration Guide* at http://docs.fortinet.com/fclnt.html.

This document includes the following sections:

Summary of enhancements

The following is a list of enhancements in FortiClient (Windows) v5.0:

FortiClient (Windows) v5.0 Patch Release 7

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

FortiClient (Windows) v5.0 Patch Release 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 (Windows) v5.0 Patch Release 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 (Windows) v5.0 Patch Release 4

- Assign endpoint control profiles based on Active Directory group
  Requires a FortiGate running FortiOS v5.0 Patch Release 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
  Requires a FortiGate running FortiOS v5.0 Patch Release 3 or later

- Removed Vulnerability Scan (VCM) and Application Firewall for standalone clients
  Requires a FortiGate running FortiOS v5.0 Patch Release 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 (Windows) v5.0 Patch Release 3

- Enhancements to FortiProxy
- Improved VPN usability with FortiToken

FortiClient (Windows) v5.0 Patch Release 2

- Customizable console for registered clients
- Endpoint control registration with redundant gateways (maximum 20)

  Enables roaming clients.
- Enhancement to the remembered FortiGates feature
- FortiClient uploads traffic, event, and vulnerability scan logs to FortiAnalyzer/FortiManager
  Requires a FortiAnalyzer/FortiManager running v5.0 Patch Release 2 or later and a FortiGate running FortiOS v5.0 Patch Release 2 or later.
- SSL VPN realm support (command line)
- Synchronize VPN elements; `save password`, `autoconnect`, and `always up`; with the FortiGate.
  Requires a FortiGate running FortiOS v5.0 Patch Release 2 or later.
- Web category filtering safe search support

  For popular search sites or portals including Google, Bing, Yahoo, and Yandex.

FortiClient (Windows) v5.0 Patch Release 1

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

FortiClient (Windows) v5.0.0

- 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/disable antivirus real-time protection.

  Manage/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 40C and higher models support ten (10) free managed FortiClient licenses. For additional managed clients, an upgraded 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.

Table 1: FortiClient license upgrade

FortiGate Series	Free registrations	FortiClient license upgrade SKU
FortiGate/FortiWiFi 30D, 40C series	10	No upgrade license.
FortiGate/FortiWiFi 60C, 60D, 80C, 90D series	10	200 client registrations FCC-C0102-LIC
FortiGate 100, 200, 300, 600, 800 series, VM01/VM01-XEN, VM02/VM02-XEN	10	2000 client registrations FCC-C0103-LIC
FortiGate 1000, 3000, 5000 series, VM04/VM04-XEN, VM08/VM08-XEN	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

- FortiClientOnlineInstaller_5.0.7.0333: Minimal installer for 32-bit and 64-bit Windows. This file downloads and installs the latest FortiClient file from the public FDS.
- FortiClientSetup_5.0.7.0333.exe: Standard installer for 32-bit Windows.
- FortiClientSetup_5.0.7.0333.zip: A zip package containing FortiClient.msi and language transforms for 32-bit Windows. Some properties of the MSI package can be customized with FortiClient Configurator tool.
- FortiClientSetup_5.0.7.0333_x64.exe: Standard installer for 64-bit Windows.
- FortiClientSetup_5.0.7.0333_x64.zip: A zip package containing FortiClient.msi and language transforms for 64-bit Windows. Some properties of the MSI package can be customized with FortiClient Configurator tool.
- FortiClientTools_5.0.7.0333.zip: A zip package containing miscellaneous tools including the FortiClient Configurator tool and VPN Automation files.

When upgrading on a 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 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.

Upgrading from FortiClient v5.0.0 or later

FortiClient (Windows) v5.0 Patch Release 7 supports direct upgrade from FortiClient v5.0.0 or later, along with the regular manual upgrade method.

Please review the Introduction, Product Integration and Support, and Known Issues chapters prior to upgrading. For more information on upgrading FortiClient, see the *FortiClient v5.0 Patch Release 7 Administration Guide* at http://docs.fortinet.com.

Upgrading from FortiClient Lite v4.0 MR3

FortiClient (Windows) v5.0 Patch Release 7 supports manual upgrade from FortiClient Lite v4.0 MR3 Patch Release 5.

Upgrading from FortiClient Connect v4.0 MR3

FortiClient (Windows) v5.0 Patch Release 7 supports manual upgrade from FortiClient Connect v4.0 MR3 Patch Release 5.

FortiClient (Windows) v5.0 Patch Release 7 does not support upgrading from older patch releases of FortiClient v4.0 MR3 (Patch Release 1 to 4).

Upgrading from FortiClient v4.0 MR2

FortiClient (Windows) v5.0 Patch Release 7 supports manual upgrade, upgrade through FortiGuard Distribution Servers (FDS), and upgrade through FortiManager v4.0 MR3 from FortiClient v4.0 MR2.

A successful software upgrade will convert and update all existing v4.0 MR2 configurations to FortiClient v5.0 Patch Release 7 formats. For information on exceptions, see “Known Issues” on page 16 before starting an upgrade.

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

Manual upgrade

FortiClient v4.0 MR2 may be upgraded to FortiClient v5.0 Patch Release 7 by running the FortiClient v5.0 Patch Release 7 installation file on the client computer. The installation file can be downloaded from the following sites:

- Fortinet Customer Service & Support: https://support.fortinet.com

  Requires a support account with a valid support contract.
- FortiClient homepage: www.forticlient.com

Upgrade through FDS

FortiClient v5.0 Patch Release 7 is available through FDS for existing FortiClient v4.0 MR2 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 v5.0 Patch Release 7. 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 v4.0 MR2 client computers that are managed by FortiManager may be upgraded to FortiClient v5.0 Patch Release 7 by pushing the update from the FortiManager.

FortiClient v5.0 Patch Release 7 does not support use of FortiManager for central management. FortiGate devices running FortiOS v5.0 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 v5.0 Patch Release 7 MSI installation package to FortiManager v4.0 MR3.

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 (Windows) v5.0 Patch Release 7 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 v5.0 Patch Release 7 Administration Guide*.

Downgrading to previous versions

FortiClient (Windows) v5.0 Patch Release 7 does not support downgrading to previous FortiClient versions.

Product Integration and Support

Operating system support

FortiClient (Windows) v5.0 Patch Release 7 supports the following operating systems:

- Microsoft Windows 8.1 (32-bit and 64-bit)
- Microsoft Windows 8 (32-bit and 64-bit)
- Microsoft Windows 7 (32-bit and 64-bit)
- Microsoft Windows Vista (32-bit and 64-bit)
- Microsoft Windows XP (32-bit)

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 NIC for network connections
- Wireless adapter for wireless network connections
- Adobe Acrobat Reader for user manual
- MSI installer 3.0 or later.

FortiOS support

FortiClient (Windows) v5.0 Patch Release 7 is supported by FortiOS v5.0.0 or later. Some FortiClient features are dependent on specific FortiOS versions. For more information, see Summary of enhancements.

FortiAnalyzer support

FortiClient (Windows) v5.0 Patch Release 7 is supported by FortiAnalyzer v5.0 Patch Release 2 or later for the logging feature. See the *FortiClient v5.0 Patch Release 7 Administration Guide* for more information.

FortiManager support

FortiClient (Windows) v5.0 Patch Release 7 is supported by FortiManager v5.0 Patch Release 2 or later for the logging and FDS update features. See the *FortiClient v5.0 Patch Release 7 Administration Guide* for more information.

FortiAuthenticator support

FortiClient (Windows) v5.0 Patch Release 7 is supported by FortiAuthenticator v2.0 MR2 or later and v3.0.0 for the FortiClient SSO Mobility Agent Service.

Web browser support

The FortiClient console is supported by Microsoft Internet Explorer version 8 or later.

Language support

The following table lists FortiClient language support information.

Table 2: Language support

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

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 (Windows) 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.

Resolved Issues

The resolved issues table listed below does not list every bug that has been corrected with FortiClient (Windows) v5.0 Patch Release 7 build 0333. The bug IDs are from Fortinet's internal bug tracking system. For inquires about a particular bug, please contact Customer Service & Support.

Table 3: Resolved issues

Bug ID	Description
0212567	Microsoft Outlook cannot connect when FortiClient is running.
0223886	Certificates containing non-ASCII characters is not used by FortiClient when connecting to SSL VPN.
0220726	IPsec over Huawei modem is not able to access resources via a VPN tunnel.
0221726	Web filtering works intermittently when the endpoint is offsite.
0218903	VPN access does not work when tethered via Blackberry phone.
0221449	FortiClient is affected by a Microsoft Windows 8.1 upgrade.
0225225	Microsoft Bing SafeSearch update.

Known Issues

The known issues table listed below does not list every bug that has been reported with FortiClient (Windows) v5.0 Patch Release 7 build 0333. The bug IDs are from Fortinet's internal bug tracking system. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Table 4: Known issues

Bug ID	Description
0181072	The FortiGate IP and port cannot be specified on the command line installer.
0188367	The welcome page should display a warning when installing FortiClient on a server platform. Installing FortiClient on server platforms is not supported.
0196405	SSL VPN tunnels are not imported when upgrading from FortiClient v4.0 MR2 Patch Release 8. Workaround: If the existing installation has only the SSL VPN standalone client, a manual upgrade will be successful. However, an upgrade pushed by FortiManager will result in a loss of any existing SSL tunnel configurations. These tunnel configurations cannot be transferred into FortiClient v5.0 Patch Release 7. Users in this scenario should manually save their existing SSL VPN tunnel configurations and recreate them in FortiClient v5.0 Patch Release 7.

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 including the extension, and select *Get Checksum Code*.

Figure 1: Firmware image checksum tool