FortiClient v4.0 MR3 Patch Release 5
for Windows Release Notes

FortiClient v4.0 MR3 Patch Release 5 Release Notes

September 25, 2012

04-435-181737-20120925

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
2012-09-25	Initial release.

Introduction

This document provides a summary of new features, support information, and known issues in FortiClient v4.0 MR3 Patch Release 5, build 0472.

Licensing

Licensing of FortiClient is controlled by FortiOS v4.0 MR3. All FortiGate models include ten free FortiClient connections. As of FortiOS v4.0 MR3 Patch Release 4, IPsec and SSL connections do not count towards this limit. For additional connections, a FortiClient license must be purchased with your FortiGate contract, as the license is enforced by the FortiGate unit. A FortiClient license can be purchased and added to your FortiGate contract at any time. See the FortiClient for Windows Licensing Guide for details.

As of FortiOS v4.0 MR3 Patch Release 4, IPsec and SSL-VPN connections do not count towards the FortiClient Connection License on the FortiGate device. Endpoint Control (NAC) connections are still counted.

Supported operating systems

FortiClient v4.0 MR3 Patch Release 5 supports the following operating systems:

- Microsoft Windows 7 SP1 (32-bit and 64-bit)
- Microsoft Windows Vista SP2 (32-bit and 64-bit)
- Microsoft Windows XP SP3 (32-bit)

Minimum system requirements

FortiClient v4.0 MR3 Patch Release 5 has the following minimum system requirements:

- Microsoft Internet Explorer 8.0 or later
- Windows compatible computer with Pentium processor or equivalent
- Compatible operating system and minimum RAM
  - Microsoft Windows 7 (512 MB)
  - Microsoft Windows Vista (512 MB)
  - Microsoft Windows XP (256 MB)
- 600 MB free hard drive space
- Native Microsoft TCP/IP communication protocol
- Native Microsoft PPP dialer for dial-up connections
- Wireless adapter for wireless network connections
- Adobe Acrobat Reader for documentation
- MSI installer 3.0 or later

Tools

FortiClient includes various utility tools and files to help with installations. The following tools and files are available in the FortiClient Tools zip file, which can be downloaded from the Fortinet Customer Service & Support site:

- FortiClientRepackagingToolGUI.exe /FortiClientRepackagingTool.exe

  An installer repackaging tool that is used to create customized MSI files.
- FCInstallerLight.exe

  This utility is not intended for end users. It is used in conjunction with the Endpoint Control feature in FortiOS v4.0 MR3. Endpoint Control will redirect all users detected as not running FortiClient to a dedicated portal. From this portal, the user can download FCInstallerLight.exe, which will then subsequently download the full FortiClient installation from the FDS servers.
- FCRemove.exe

  FCRemove.exe is a clean-up tool for use only if the *Add/Remove Programs* feature in Windows fails to remove FortiClient completely.
- ReinstallNIC.exe

  A utility to uninstall and reinstall the Windows NIC driver if the user is having problems with DHCP acquisition after FortiClient is installed (Windows 7 or higher ONLY).
- FortiClientVPNEditor.exe

  A utility for creating VPN tunnel configuration files and exporting the previous FortiClient configurations to FortiClient v4.0 MR3 format.

Language support

FortiClient v4.0 MR3 Patch Release 5 is localized for the following languages:

	Graphical User Interface	Documentation
English	Yes	Yes
French	Yes	No
German	Yes	No
Japanese	Yes	No
Portuguese (Brazil)	Yes	No
Spanish (Spain)	Yes	No
Slovak	Yes	No
Czech	Yes	No

Special Notices

General

Any IPsec VPN connections created from the FortiClient v4.0 MR3 Patch Release 5 Graphical User Interface (GUI) are supported by FortiOS v4.0 MR3 or later. To create a compatible tunnel configuration on the FortiGate, go to *VPN* > *IPsec* > *Auto Key (IKE)* > *Create FortiClient VPN*. See Appendix A for details.

VPN tunnel created on the FortiGate using the *Create FortiClient VPN* button can only be used with FortiClient v4.0 MR3 or later, and is not supported for older FortiClient versions.

Reconnect after resuming from Windows Sleep/Hibernate/Standby

Any active VPN connection will be disconnected when Windows enters Sleep, Hibernate, or Standby mode, user will have to reconnect after Windows resumes.

Saving login information

Due to security reasons FortiClient does not save the passwords of the VPN connections, it will only save the usernames.

Start VPN before logging on to Windows

Use the *Start VPN before logging on to Windows* setting in conjunction with X.509 Certificate Authentication, the certificates must be in the local certificate store.

Installation

The FortiClient v4.0 MR3 Patch Release 5 installation package is available in two different formats: an executable installation file, and a zipped MSI installation file. See the FortiClient Deployment Guide on creating custom MSI installation packages.

FortiClient v4.0 MR3 Patch Release 5 supports direct upgrade from FortiClient Connect v4.0 MR3, FortiClient v4.0 MR3 Patch Release 1, and Patch Release 3.

Uninstall any previous versions of FortiClient v4.0 MR2, or any versions of FortiClient Lite v4.0 MR3 before installing FortiClient v4.0 MR3 Patch Release 5.

Resolved Issues

The resolved issues table below does not list every bug that has been corrected with this release. For inquires about a particular bug, please contact Customer Service & Support.

Table 1 outlines resolved issues.

Table 1: Resolved issues

Bug ID	Description
155832	FortiClient should not send 2nd IKE request while 1st request is still in-progress.
156472	Cannot count FortiClient v4.0 MR3 Patch Release 3 SSL-VPN connections.
156524	GUI error on Spanish (Spain) PCs.
156945	Non-admin user cannot connect VPN from VPN connections screen.
157254	Japanese translations needed for GUI.
158275	Web Filter log message even if module is not installed.
158495	Add IKE localid type auto detection to differentiate ID_FQDN and ID_USER_FQDN.
165690	Cannot add connection due to script error.
168448	Do not prompt misleading server-cert-warning-window if ServerCert=0.
175333	Enabling *Protect Config Changes* greys out *Connect* button.
176644	XAuth password saved by VPN Editor is not used during IPsec connection attempt.
176645	Blue screen when the wireless network is enabled.

Known Issues

The known issues table below does not list every bug that has been identified with this release. For inquires about a particular bug or to report a new bug, please contact Customer Service & Support.

Table 2 outlines known issues.

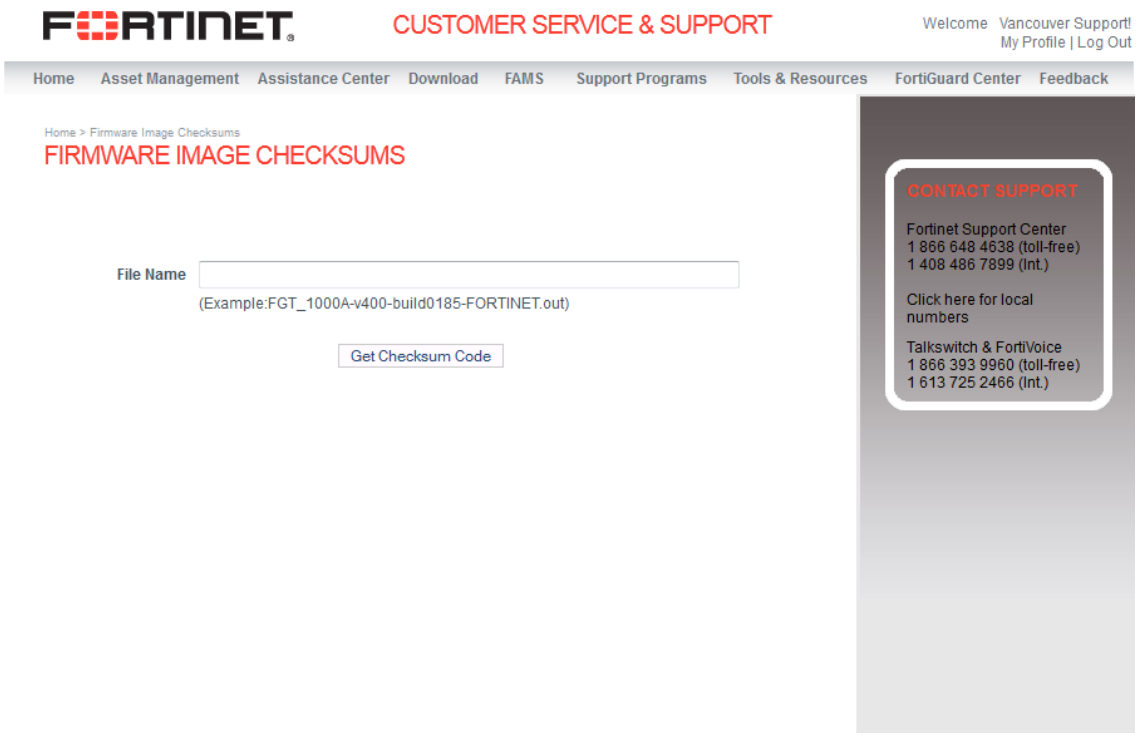
Table 2: Known issues

Bug ID	Description
149754	FortiClient Connect cannot connect via IPsec VPN using *System Store X509 Certificate*.
154627	WAN Optimization sometimes can make file transfer over CIFS slower.
154912	WAN Optimization does not work properly.
173894	WAN Optimization over IPsec sometimes does not work.
179956	Compatibility issue when using VPN Editor to import a v4.0 MR2 VPN to a v4.0 MR3 FortiClient.

Image Checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support website located at https://support.fortinet.com. After logging in, click on *Download* > *Firmware Image Checksum*, enter the image file, including the extension, and select *Get Checksum Code*.

Figure 1: Customer Service & Support image checksum tool



Appendix A: IPsec VPN Configuration

IPsec VPN configuration instruction for FortiOS v4.0 MR3

Described below are the steps to configure an interface mode IPsec VPN on FortiOS v4.0 MR3.

1. On the FortiGate (running v4.0 MR3) go to *VPN* > *IPSec* > *Auto Key (IKE)*.
2. Select the *Create FortiClient VPN* button on the right navigation pane.
3. Complete the FortiClient VPN tunnel configuration details on the page and select *OK*.
4. Verify that a Phase1 and Phase2 has been created for the VPN.
5. Configure the appropriate firewall policies under *Policy* > *Policy* for VPN traffic.

IPsec VPN configuration instruction for FortiClient v4.0 MR3 Patch Release 5

Described below are the steps to configure an interface mode IPsec VPN on FortiClient v4.0 MR3 Patch Release 5.

1. Open the FortiClient console and navigate to *IPsec VPN* main page.
2. Select the '+' icon on the bottom-left corner to add a new connection.
3. Complete the following information on the *Add Connection* page.
   - Connection Name
   - Remote Gateway
   - Authentication Method
   - XAuth
4. Select *OK.*
5. Select the VPN connection from the list and select *Connect* to establish the IPsec tunnel.

IPsec VPN configuration instruction for FortiOS v4.0 MR2

Described below are the steps to configure an interface mode IPsec VPN on FortiOS v4.0 MR2.

1. Create an address name for internal subnet if it does not exist. (optional)
2. Create an user group for FortiClient users on *User* > *User Group*.
3. Go to *VPN* > *IPsec* > *Auto Key* > *Create Phase1* and complete the following information:
   - Name (i.e. mydialup-phase1)
   - Remote Gateway (i.e. Dialup User)
   - Local Interface (i.e wan1)
   - Mode: Aggressive
   - Authentication Method
   - Enable IPsec Interface Mode option
   - XAUTH: Enable as server
   - User Group: <select the FortiClient user group>

4. Select *OK*.
5. Go to *VPN* > *IPsec* > *Auto Key* > *Create Phase2* and complete the following information:
   - • Name (i.e. mydialup-phase2)
   - • Phase1: select the phase1 VPN created before (i.e. mydialup-phase1)
6. Select *OK*.
7. From the FortiGate Command Line Interface, enter the following commands:

```
config vpn ipsec phase1-interface
edit <phase1 name>
set mode-cfg enable
set ipv4-start-ip <start ip address>
set ipv4-end-ip <end ip address>
set ipv4-netmask <network mask>
set ipv4-split-include <address group> (optional setting)
set ipv4-dns-server1 <server ip> (optional setting)
end
```

8. Configure appropriate firewall policies on *Firewall* > *Policy* for VPN traffic.

End of Release Notes