FortiClient for Mac OS v4.0 Patch Release 3

Release Notes

May 07, 2012

04-403-169934-20120507

Technical Documentation: http://docs.fortinet.com

Knowledge Base: http://kb.fortinet.com

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

Training Services: http://training.fortinet.com

Table of Contents

Change Log

Date	Change Description
2012-05-07	Initial Release

This document provides a summary of new features, installation instructions, resolved and known issues in FortiClient for Mac OS v4.0 Patch Release 3, build 0134.

FortiClient for Mac OS v4.0 Patch Release 3 contains bug fixes only; no new features were added in this release.

Technical documentation

The following documentation is available from the technical documentation website at http://docs.fortinet.com/fclient40.html

- QuickStart Guide for Mac OS
- FortiClient Licensing Guide for Mac OS

Articles and information on specific configuration issues are available at the knowledge base website at http://kb.fortinet.com

Licensing

Licensing of FortiClient for Mac OS is controlled by the FortiGate device (FortiOS v4.0 MR3 and later). FortiClient licenses can be purchased with your FortiGate support contract. FortiOS v4.0 MR3 Patch Release 4 and later does not require a license for VPN connections.

Supported operating systems

FortiClient for Mac OS v4.0 Patch Release 3 is supported by the following operating systems:

- Mac OS Lion (v10.7)
- Mac OS Snow Leopard (v10.6)

System requirements

FortiClient for Mac OS v4.0 Patch Release 3 has the following minimum system requirements:

- Intel processor
- 256MB of RAM
- 20MB of hard disk space
- TCP/IP communication protocol
- Ethernet NIC for network connections
- Wireless adapter for wireless network connections
- Abode Acrobat Reader for technical documentation

General information

Any IPsec VPN connections created from the FortiClient for Mac OS v4.0 Patch Release 3 Web-based Manager are only supported by FortiOS v4.0 MR3 and later. To create a compatible tunnel configuration on the FortiGate, go to *VPN* > *IPsec* > *Auto Key (IKE)* > *Create FortiClient VPN*.

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

Reconnect after resuming from Mac sleep/hibernate/standby

Any active VPN connection will be disconnected when Mac enters sleep/hibernate/standby mode; user will have to reconnect after Mac resumes.

Reconnect after IPsec phase 1 key expiration

Any active IPsec VPN connections will be terminated after the key life for the phase 1 proposal has expired; users will have to manually re-establish the connection. By default, the key life for phase 1 is 28800 seconds.

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)* page.
2. Select the *Create FortiClient VPN* button.
3. Fill the VPN tunnel configuration details on the page and click *OK*.
4. Verify that a phase1 and phase2 has been created for the VPN.
5. Configure appropriate firewall policies under *Firewall* > *Policy* page for VPN traffic.

IPsec VPN configuration instruction for FortiClient for Mac OS v4.0 Patch Release 3

Described below are the steps to configure an interface mode IPSec VPN on FortiClient for Mac OS v4.0 Patch Release 3:

1. Open the FortiClient console and navigate to IPSec VPN main page.
2. Click the + icon on the bottom-left corner to add a new connection.

3 Input the following information on the *Add Connection* page.

Connection Name

Remote Gateway

Authentication Method

XAuth

Select *OK*

4 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 doesn't exist yet. (optional)

2 Create an user group for FortiClient users on *User* > *User Group* page.

3 Navigate to *VPN* > *IPsec* > *Auto Key* > *Create Phase1* page and input 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>

Select *OK*

4 Navigate to *VPN* > *IPsec* > *Auto Key* > *Create Phase2* page and input the following information:

Name: (i.e. mydialup-phase2)

Phase1: select the phase1 VPN created before (i.e. mydialup-phase1)

Select *OK*

5 From the FortiGate CLI, 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
```

6 Configure appropriate firewall policies using *Firewall* > *Policy* page for VPN traffic.

Upgrade from FortiClient Connect v4.0.0 GA

Described below are the steps to upgrade from FortiClient Connect v4.0.0 GA to FortiClient v4.0 Patch Release 3:

1. Quit FortiClient Connect if it is running
2. Open *Finder* > *Applications*
3. Drag the 'FortiClient Connect' executable to Trash
4. Download the FortiClient v4.0 Patch Release 3 installer: FortiClient_4.0.3.134_macosx.dmg
5. Drag the FortiClient icon to the Applications folder

Upgrade from FortiClient v4.0 Patch Release 1/Patch Release 2

Described below are the steps to upgrade from FortiClient v4.0 Patch Release 1 or Patch Release 2:

1. From the FortiClient Web-based Manager select *FortiClient* > *Check for Updates*
2. Download the FortiClient v4.0 Patch Release 3 installer: FortiClient_4.0.3.134_macosx.dmg
3. Shutdown FortiClient
4. Drag the FortiClient icon to the Applications folder

Resolved Issues

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

Table 1: Resolved issues

Bug ID	Description
159369	Some authentication/encryption methods are not supported.
162906	RADIUS users cannot login in to SSL-VPN tunnel mode.
165034	The route is not removed after the VPN is disconnected.
168672	SSL-VPN tunnel gets disconnected after 30 seconds.
168759	SSL-VPN client does not check server certificate.

Known Issues

This section lists the known issues of this release, but is not a complete list. For inquires about a particular bug, please contact america_beta@fortinet.com.

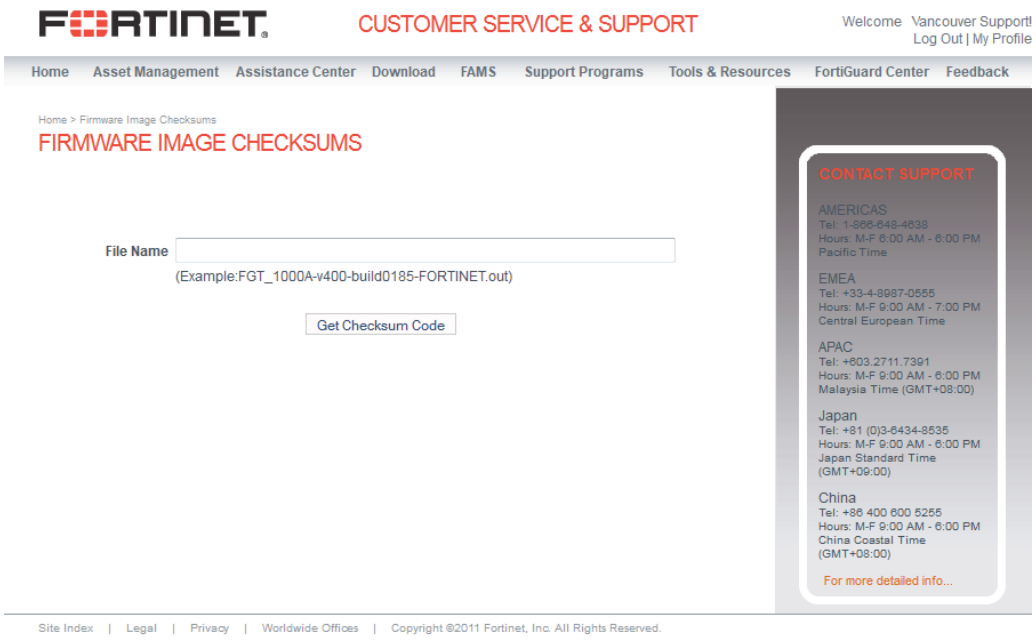
Table 2: Known issues

Bug ID	Description
144252	Error messages sometimes do not contain meaningful feedback.
147729	A warning message about *FCTUpgrader* may pop up after install. Workaround: Acknowledge the warning message.

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: Fortinet customer support image checksum tool



(End of Release Notes)