FortiClient™ Connect Endpoint Security System

Release Notes
v4.0 MR3

04-430-141402-20110609

FORTINET

Table of Contents

Change Log

Date	Change Description
2011-06-08	Initial Release.
2011-06-09	Added the special notes section

Support will be provided to customers who have purchased a valid support contract. All registered customers with valid support contracts may enter their support tickets via the support site: https://support.fortinet.com

1 FortiClient Connect v4.0 MR3

This document provides a summary of the new features in FortiClient Connect v4.0 MR3 B0398 and provides information on installation instructions and known issues. The FortiClient Connect v4.0 MR3 is also known as v4.3.0.398.

1.1 What's New

The following is a brief list of the new features added in FortiClient Connect v4.0 MR3.

- Introduces New web UI design
- Simplified SSLVPN Feature
- Enhanced IPSec VPN Feature
- Redesigned Wan Optimization Feature
- Redesigned Application Detection Feature
- Supports Windows Certificate Store
- Introduces VPN HomePage View Option
- Repackaging Tool Support

1.2 Documentation

The following documentation is available from the Fortinet Technical documentation website at http://docs.fortinet.com

- FortiClient Connect Quickstart Guide
- FortiClient Connect Deployment Guide

Articles and information on specific issues are available from the Fortinet Knowledge Base at http://kb.fortinet.com

1.3 Language Support

FortiClient Connect v4.0 MR3 is localized for the following languages:

	GUI	Documentation
English	Yes	Yes
French	Yes	-
German	Yes	-
Japanese	Yes	-
Portuguese (Brazilian)	Yes	-
Spanish (Spain)	Yes	-
Slovak	Yes	-
Czech	Yes	-

1.4 Tools

FortiClient Connect 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 support site:

- FCRepackager.exe – The FortiClient repackager used to create customized MSI files.

- 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.

- VPNEditor\FortiClientVPNEditor.exe – It is for creating VPN tunnel configuration files and exporting the previous FortiClient configurations to FortiClient Connect 4.3 format.

1.5 Licensing

Licensing of FortiClient Connect is controlled by FortiOS 4.3.The user has to buy the FortiClient Connect license with FortiGate Support Contract, based on the number of simultaneous active VPN , NAC and WAN Optimization connections to the Fortigate.

1.6 Supported Operating System

The following operating systems are supported:

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

1.7 System Requirements

FortiClient Connect v4.0 MR3 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
- 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

2 Special Notices

2.1 General

IMPORTANT!

Web Browser Requirement

- Microsoft Internet Explorer 8.0 or later

2.2 Reconnect after resuming from Windows Sleep/Hibernate/Standby

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

2.3 Saving login information

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

3 Upgrade and Installation Information

This is a first release of the FortiClient Connect software, so upgrades from previous versions of FortiClient do not apply, but the user can use VPN Editor tool to export previous FortiClient configurations to 4.3 format for using it with FortiClient Connect v4.0 MR3.

Uninstall any previous version of FortiClient before installing FortiClient Connect v4.0 MR3.

The FortiClient Connect installation package is available in 2 different formats: an executable installation file and a zipped MSI installation file. For details on creating custom installations using MSI transforms, see the FortiClient Connect Deployment Guide.

4 Known Issues in FortiClient Connect v4.0 MR3

This section lists the known issues of this release, but is NOT a complete list.

Description: After the first failed IPSEC login attempt (due to wrong username/password), a login window reappears. If the correct username and password is not entered within 15 seconds the connection will fail.
Bug ID: 145872
Status: N/A
Workaround : To increase the period to more than 15 seconds , user can increase the dpd settings on the fortigate using the following commands.

```
config vpn ipsec phase1-interface
    edit <phase1 name>
        set dpd-retrycount <integer , default is 3>
        set dpd-retryinterval <seconds, default is 5>
    end
```

5 Appendix

5.1 How to Configure IPSec VPN

5.1.1 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.

Step 1: On the FortiGate (running v4.0 MR3) go to VPN > IPSec > Auto Key (IKE) page.
Step 2: Click on “Create FortiClient VPN” button.
Step 3: Fill the VPN tunnel configuration details on the page and click OK.
Step 4: Verify that a Phase1 and Phase2 has been created for the VPN.
Step 5: Configure appropriate firewall policies under Firewall > Policy page for VPN traffic.

5.1.2 IPSec VPN Configuration Instruction for FortiClient Connect v4.0 MR3

Described below are the steps to configure an interface mode IPSec VPN on FortiClient Connect v4.0 MR3.

Step 1: Open the FortiClient console and navigate to IPSec VPN main page.
Step 2: Click '+' icon on the bottom-left corner to add a new connection.
Step 3: Input the following information on the "Add Connection" page.

- Connection Name
- Remote Gateway
- Authentication Method
- XAuth
- Click OK

Step 4: Select the VPN connection from the list and click *Connect* to establish the IPSec tunnel.

5.1.3 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.

Step 1: Create an address name for internal subnet if it doesn’t exist yet. (optional)
Step 2: Create an user group for FortiClient users on User > User Group web UI page.
Step 3: Navigate to VPN > IPsec > Auto Key > Create Phase1 web UI 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*>
- Click OK

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

- Name (i.e. mydialup-phase2)
- Phase1: *select the phase1 VPN created before* (i.e. mydialup-phase1)
- Click OK

Step 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
- Click OK

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

(End of Release Notes.)