FortiClient™ Host Security Software

Release Notes
FortiClient v2.0 GA

June 29, 2005

Table of Contents

Release Notes FortiClient v2.0 GA

Trademarks
Products mentioned in this document are trademarks or registered trademarks of their respective holders.

Fortinet Technical Support Email Contacts:
amer_support@fortinet.com for the Americas
eu_support@fortinet.com for EMEA
apac_support@fortinet.com for Asia Pacific

1 FortiClient Host Security v2.0 GA

This document describes the new features of the FortiClient Host Security v2.0 GA release software and provides additional information on upgrading, installation, and custom installations using MSI transforms . FortiClient v2.0 GA adds support for the FortiGuard-Web Filtering service, simple firewall configuration profiles, an improved upgrade process and various GUI improvements.

FortiClient v2.0 GA is also known as v2.0.062.

1.1 Language Support

FortiClient Host Security v2.0 GA is localized for English and Simplified Chinese.

FortiClient Host Security v2.0 GA is tested on English, French, German, Spanish and Simplified Chinese OS versions only.

1.2 License

FortiClient v2.0 GA includes 30 days of free Antivirus updates and Web-Filtering support. A license key is required to enable the advanced VPN features and take FortiClient out of evaluation mode . The license key format has not changed . A valid FortiClient v1.0, v1.2 or 1.6 license key can be used with FortiClient v2.0 GA. Note that reinstalling FortiClient v2.0 GA will NOT give you another 30 days of free AV updates or Web-Filtering support.

If no license key is entered, the following features are enabled:

- Personal firewall
- VPN using DES encryption and MD5 or NULL authentication only
- 30-days of free AV updates
- 30-days of free Web-Filtering support

Access to ongoing AV updates and Web-Filtering support is controlled by the FortiGuard servers and requires purchasing an AV subscription.

Contact your local Fortinet sales engineer or license@fortinet.com to get a new license key.

1.3 System Requirements

FortiClient v2.0 GA has the following system requirements:

- PC-compatible computer with Pentium processor or equivalent
- Compatible operating systems and minimum RAM:
- Microsoft Windows 2000™ : 64 MB
- Microsoft Windows XP™ : 128 MB
- Microsoft Windows Server™ 2003 : 128 MB
- 30 MB hard disk space
- Native Microsoft TCP/IP communications protocol
- Native Microsoft PPP dialer for dial-up connections
- Ethernet for network connections
- Microsoft Internet Explorer™ 5.0 or later
- Adobe Acrobat™ Reader 4.0 or later for user manual

1.4 Supported Operating Systems

FortiClient v2.0 GA supports the following operating systems:

- Microsoft Windows 2000 Professional
- Microsoft Windows 2000 Server
- Microsoft Windows 2000 Advanced Server
- Microsoft Windows XP Home
- Microsoft Windows XP Professional
- Microsoft Windows Server 2003
- Microsoft Windows Small Business Server 2003

Notes: Microsoft Windows XP Service Pack 2 is supported in FortiClient v1.2 MR1 or later. Microsoft Windows Server 2003 SP1 is NOT supported by FortiClient 2.0 due to TCP/IP stack issues.

2 Upgrade Information

The FortiClient 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 Appendix A.

Important: FortiClient v2.0 GA includes an improved upgrade process. FortiClient v2.0 GA will automatically uninstall previous FortiClient versions 1.2 and 1.6 before installing v2.0 GA. The upgrade process will also delete any incompatible AV signature files as part of the automatic uninstall. The user can choose to keep any existing configuration data. This change in the upgrade process means that it is no longer necessary to manually uninstall versions 1.2 or 1.6 of FortiClient before installing v2.0 GA. If you are running FortiClient v1.0, it is still recommended that you manually uninstall FortiClient before installing v2.0 GA.

If you are upgrading from v1.2 GA or MR1 and want to keep your current configuration information, you may need to reconfigure the firewall application list immediately after upgrading (if you had been using the personal firewall component). The default policy setting for handling other inbound traffic from the public zone changed from DROP, in v1.2 GA and MR2, to ALLOW in v1.2 MR2 or later. You should review the firewall policies after upgrading. This is not an issue for new installations or clean upgrades where the configuration information was deleted during the uninstall.

The FortiClient v2.0 GA configuration wizard gives you the choice to perform a basic or advanced setup. If you choose the basic setup option, the wizard will prompt you for the update server settings. If you choose the advanced setup option , the wizard will prompt you for trusted and public zone Internet addresses, the proxy server settings and update server settings. All other configuration options are set to default by the wizard and can be modified once the installation is complete.

Note: The personal firewall is enabled and the security level set to Normal by default. After installing you may need to configure the firewall applications and network settings to allow your normal traffic patterns to resume with the firewall enabled. If you are installing on Windows XP, FortiClient will *disable* the XP firewall as part of the installation.

2.1 Exporting VPN policies for Backup Purposes

The FortiClient VPN policies can be exported for backup purposes or to transfer the policies to another computer.

To export a FortiClient v1.0 VPN configuration:

1. On the Windows Start menu, select Run.
2. Type "regedit" and press enter.
3. In the Registry Editor, open the Registry key:
   KEY_LOCAL_MACHINE\\SOFTWARE\\Fortinet\\FortiClient\\IPSec
4. On the Registry menu, select Export Registry File.
5. Save the file.

To export a FortiClient v1.2 or later VPN configuration:

1. On the FortiClient VPN Connections tab, select Export.
2. Save the .vpl file.

2.2 Upgrade Instructions

The FortiClient v2.0 GA installer allows you to choose which FortiClient components to install. You can choose from the VPN, AV, Personal Firewall and Web Filtering components. The management console, update and log components are always installed and are not displayed as selectable components.

To upgrade FortiClient v1.0 to v2.0 GA:

1. Backup the VPN policies (optional).
2. Manually uninstall FortiClient v1.0.
3. Copy the FortiClient v2.0 GA software to your computer.
4. Run the FortiClient self-extracting install file.

To upgrade FortiClient v1.2 or v1.6 to v2.0 GA:

1. Backup the VPN policies (optional).
2. Copy the FortiClient v2.0 GA software to your computer.
3. Run the FortiClient self-extracting install file.

2.3 Importing VPN Policies

To import a FortiClient v1.0 VPN configuration to FortiClient v2.0 GA:

1. Copy the Registry backup file you created in Section 2.4 to the computer with the FortiClient v.2.0 GA software installed.
2. Double click on the Registry backup file.
3. Restart the FortiClient Host Security software.

To import a FortiClient v1.2 or 1.6 VPN configuration to v2.0 GA:

1. Copy the .vpl file you created in Section 2.4 to the computer with the FortiClient v2.0 GA software installed.
2. In the FortiClient VPN Connections tab, select Import.
3. Select the .vpl file.
4. Select Open to import the configuration.

2.4 Remote/Silent Installations

FortiClient v1.2 MR2 or later supports group policy installation via a Microsoft Active Directory Server domain controller.

The following is a general description of how to deploy the FortiClient software to remote computers using Active Directory. For complete details, refer to the Active Directory manuals or online help. To complete this procedure, you must log on as a member of the Domain Administrators security group, the Enterprise Administrators security group, or the Group Policy Creator Owners security group.

1. Unzip the FortiClient MSI installation file to a share folder.
2. Open the Group Policy Object Editor.
3. Select Computer Configuration.
4. Select Software Settings.
5. Right-click Software Installation, select New, and then select Package.
6. Select the FortiClient MSI installation file and select Open.
7. In Deploy Software, select Assigned.

3 New Features and Enhancements

The following is a list of the new features supported in FortiClient v2.0 GA. Short descriptions are provided. For further details on the features and configuration instructions/samples, please refer to the FortiClient user manual and online help.

3.1 New Features Added in FortiClient v2.0 GA

3.1.1 FortiGuard-Web Filtering

FortiClient v2.0 GA adds support for FortiGuard-Web Filtering and is an optional installation component. FortiClient uses the same FortiGuard-Web Filtering servers as the FortiGate product. Web Filtering support must be purchased to be fully enabled, but 30 days of free Web Filtering support is included in the unlicensed version as a preview.

FortiGuard-Web Filtering provides 8 basic categories of URLs, which are broke down into sub-categories. The 8 basic URL categories are:

1. Potentially liable
2. Controversial
3. Potentially non-productive
4. Potentially bandwidth consuming
5. Potentially security violating
6. General interest
7. Business oriented
8. Others

FortiClient v2.0 GA includes three basic Web Filtering profiles that provide preset Web Filtering configurations. The available profiles are:

1. Default
2. Child
3. Adult

These profiles can be modified to create a custom configuration. The configuration can be password protected. If the password is left blank, password protection is disabled. In v2.0 GA, multiple Web Filtering configurations tied to the user are not supported – i.e. a single configuration is used for all users.

The user can also define specific URLs to be blocked (black listed) or allowed (white listed).

3.1.2 Simple Firewall Configuration Profiles

FortiClient v2.0 GA provide simple firewall configuration profiles to make it easy for non-technical users to ensure that their PC is properly protected from attacks. Three profiles are available:

1. Basic home use – Allows all outgoing connections and denies all incoming connections.
2. Basic business – Allows all outgoing connections and denies any incoming connections from the public zone.
3. Custom Profile – The default profile. The firewall can be fully customized.

If the Basic home use or Basic business profiles are selected, the applications and network tabs are hidden, since these settings are dictated by the profile.

3.1.3 Antivirus Features

FortiClient v2.0 GA adds support for scanning and cleaning NTFS Alternative Data Streams (ADS).

3.1.4 GUI Improvements

FortiClient v2.0 GA includes various GUI improvements, including:

1. Tabs for components that were not installed are no longer displayed.
2. Balloon notifications have been added for events such as blocked firewall traffic and expired AV or Web Filtering services.
3. The FortiClient serial number is displayed on the General tab to assist with support calls.
4. The FortiGuard UID is displayed on the Updates tab to assist with support calls related to the AV and Web Filtering services
5. The FortiClient AV engine and signature information is displayed in the Taskbar/System Tray when the mouse cursor is held over the FortiClient icon.
6. The application type is displayed in the log data based on the port number – i.e. 192.168.1.1:143 (imap)

3.2 New Features Added in FortiClient v1.6 GA

The following is a list of the new features supported in FortiClient v1.6 GA. Short descriptions are provided. For further details on the features and configuration instructions/samples, please refer to the FortiClient user manual and online help.

3.2.1 Antivirus Features

Virus code emulator
Description: The code emulator significantly improves polymorphic virus detection. The emulator is used to extract the virus body from morphed code and is also used as a generic extraction engine.

File repair engine
Description: Provides the ability to clean and repair infected files.

Optimized AV engine and improved Heuristic detection
Description: Provides major performance improvements when scanning for macro infected files and fine tunes the heuristic virus detection logic.

Heuristic detection of massively deployable worms through email
Description: Prevents the PC from distributing email worms by detecting if a process tries to send the same email to multiple recipients (over a designated threshold) or tries to send an email repeatedly. The process is terminated automatically or the user is asked whether they want to terminate the process.

Startup folder monitoring
Description: Adds the ability to monitor the Windows Startup folder and notify the user if a startup item is added. The user is asked whether they want to allow the startup item to be added.

Improved Microsoft Windows XP SP2 support
Description: FortiClient v1.6 supports the new network driver architecture which provides a more stable VPN connection and improved wireless NIC support.

3.2.2 Firewall Features

Common network attack blocking
Description: FortiClient now blocks common network attacks without using signatures. Not using signatures provides common network attack protection without impacting performance.

3.2.3 VPN Features

Tunnel establishment before user log on
Description: FortiClient can be configured to establish the VPN tunnel during boot/startup and before performing user authentication (Windows login). This option is set on the VPN connections page.

3.2.4 System and Administration Features

AV signature update through proxy
Description: Adds support for updating the AV signature file via a proxy. HTTP and Socks 4/5 are supported.

3.2.5 GUI Features

Multiple user and Windows Terminal Server support
Description: Support Windows XP user quick switch and Windows Terminal server. The FortiClient service and console displays popups and warnings to the appropriate desktop based on the current user.

4 Appendix A: FortiClient Custom Installations

4.1 General Guidelines

FortiClient v1.2 MR2 or later uses Microsoft Installer (MSI) technology. An MSI editor can be used to create a custom FortiClient installation package. The MSI file should not be edited directly. The recommended solution is to create a transform file that contains the configuration changes you need. The transform is applied to the original MSI file at runtime by msiexec. Creating a transform takes a bit more time than editing the MSI file directly, but it will save you time and trouble in the future since it should be possible to apply the same transform to future FortiClient releases.

Warning: You MUST follow the editing rules laid out in this section. Ignoring these rules may result in a custom installation that cannot be upgraded or patched by future releases of FortiClient.

The following components have been created specifically for modifying FortiClient installations. If possible, you should avoid modifying other components:

- REGISTRY_MST_FWSettings
- REGISTRY_MST_AVSettings
- REGISTRY_MST_VPNSettings

FortiClient sub-features do not support "Advertised" installations.

The following rules MUST be followed:

- **NEVER delete a feature you don't need.** If you don't need a feature, set the install level to 0
- **NEVER delete a component you don't need.**
- **NEVER move a component from one feature to another.**
- **NEVER modify the installation UI or installation execution order.**
- **NEVER rename ANY existing component or feature.**
- **NEVER change the component code of ANY existing feature.**
- **NEVER change the PRODUCTCODE.**
- **NEVER change the UPGRADECODE.**
- **NEVER add new features to the root of the feature tree.** If you *really* need to a a feature, add it as a sub-feature of an existing FortiClient feature. However, before you add a feature, question why you are adding a feature and what you are trying to accomplish.

4.2 How to create a FortiClient custom installation

You will need an MSI editor and the original FortiClient MSI installation file. These instructions assume that you know how to use an MSI editor, how to use the command line msiexec commands, and how to roll out an MSI based installation to your network.

Note: When you perform a silent or reduced UI installation, the MSI automatically disables the FortiClient Wizard from executing after rebooting the PC. You do not need to edit the MSI to disable the wizard.

To create and test a custom FortiClient installation:

1. Make a copy of the FortiClient.msi file and rename the copy (i.e. "target.msi").

2. Open "target.msi" with an MSI editor and add your modifications to it.

3. Save the changes you made to the "target.msi" file and close the file.

4. With your MSI editor, make a transform file (*.mst)
    - The base package must be “FortiClient.msi”
    - The target package must be “target.msi”
    - Give the mst file a suitable name. We suggest you include the version of FortiClient that was used to create the transform. i.e. “custom_16099.mst”

5. Test the installation by installing the baseline package with the transform onto a single PC. Use the following command:

    msiexec /i <path to package>FortiClient.msi TRANSFORMS=custom_16099.mst /L*v c:\log.txt

    - Substitute “<path to package>” with the path to your package (if it's not in the current dir)
    - There are no spaces in “TRANSFORMS=custom_16099.mst”
    - There is a space between “TRANSFORMS=custom_16099.mst” and “/L*v c:\log.txt”
    - If there are any errors during installation, the log file is an invaluable source of information.

7. Test FortiClient to make sure the modifications you made are present and correct. If there are any mistakes, use your editor to make changes to the mst file. Some editors allow you to load and edit the mst file directly.

8. Test uninstalling the FortiClient software. It is critical that you do this before you roll out FortiClient to your network. The uninstall must complete without an error or rollback occurring.

9. Roll out your custom FortiClient installation specifying the transform file.

4.3 Adding a license key

The MSI property ISX_LICENSE can be set to your license key. You can create and set this property in the property table, or you can specify it on the command line:

msiexec /i FortiClient.msi ISX_LICENSE=1234567890abc

Note that the installation will NOT abort if an invalid license is specified.

4.4 Disabling VPN XAuth password saving

The ability for a user to “save” the VPN XAuth password can now be disabled through a registry setting in a custom installation. To disable this feature:

1. Create a new, or edit an existing, MSI transform file.
2. Edit the LOCAL_MACHINE\Software\Fortinet\FortiClient\FA_IKE registry key.
3. Add the value DontRememberPassword under the key.
4. Set the value of DontRememberPassword to 1.

4.5 Language transforms

The MST files that ship with the baseline FortiClient package are the English and Simplified Chinese language transforms:

- 1033.mst = US English
- 2052.mst = Simplified Chinese

4.6 Specifying multiple transforms on the command line

Multiple transforms can be specified on the command line. Separate each transform with a semicolon:

msiexec /i <path to package>FortiClient.msi TRANSFORMS=custom1_6_099.mst; 2052.mst

5 Appendix B: Software Image MD5 Checksums

```
96d63bd6c78fbb995ba8601a05f44c3d *FortiClientSetup_2.0.062.exe
fd0aa2440309b4ee776aba70d47323dc *FortiClientSetup_2.0.062.zip
```

(End of Release Notes.)