



# FortiClient Endpoint Security

## Rebranding Tool Technical Note

Version 4.0 MR2



## ***FortiClient Endpoint Security***

Version 4.0 MR2

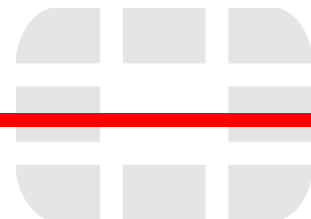
27 September 2010

04-420-130023-20100825

© Copyright 2010 Fortinet, Inc. All rights reserved. No part of this publication including text, examples, diagrams or illustrations may be reproduced, transmitted, or translated in any form or by any means, electronic, mechanical, manual, optical or otherwise, for any purpose, without prior written permission of Fortinet, Inc.

### **Trademarks**

Dynamic Threat Prevention System (DTPS), APSecure, FortiASIC, FortiBIOS, FortiBridge, FortiClient, FortiGate®, FortiGate Unified Threat Management System, FortiGuard®, FortiGuard-Antispam, FortiGuard-Antivirus, FortiGuard-Intrusion, FortiGuard-Web, FortiLog, FortiAnalyzer, FortiManager, Fortinet®, FortiOS, FortiPartner, FortiProtect, FortiReporter, FortiResponse, FortiShield, FortiVoIP, and FortiWiFi are trademarks of Fortinet, Inc. in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.



# Contents

<b>Introduction .....</b>	<b>3</b>
<b>About FortiClient.....</b>	<b>3</b>
<b>Registering your Fortinet product.....</b>	<b>3</b>
<b>Customer service &amp; technical support .....</b>	<b>3</b>
<b>Training .....</b>	<b>4</b>
<b>Documentation .....</b>	<b>4</b>
Fortinet Tools and Documentation CD .....	4
Fortinet Knowledge Base.....	4
Comments on Fortinet technical documentation .....	4
<b>Rebranding the FortiClient Application .....</b>	<b>5</b>
<b>Preparing to rebrand the FortiClient application .....</b>	<b>5</b>
<b>Installing the Rebranding Tool application .....</b>	<b>5</b>
<b>Customizing the application and installer .....</b>	<b>6</b>
Saving the rebranded msi file .....	9



# Introduction

This document describes how to rebrand the FortiClient application.

You must have a valid OEM agreement with Fortinet in order to create and deploy a rebranded version of FortiClient Endpoint Security.

This section contains the following topics:

- [About FortiClient](#)
- [Registering your Fortinet product](#)
- [Customer service & technical support](#)
- [Training](#)
- [Documentation](#)

## About FortiClient

FortiClient offers the full range of Fortinet threat protection to computers, even when being used on insecure public networks. This comprehensive, modular protection suite secures desktops against viruses, trojans, worms and more. The FortiClient product is a client-based software solution designed to be used in connection with our FortiGate appliances to provide security features like Endpoint Control and WAN Optimization for enterprise computers. The feature set includes VPN (IPSec and SSL), antivirus/antispymware, personal firewall, Web filtering, and antispam – each with separate modular installs to completely avoid any potential conflicts with other security software. Powered by FortiGuard security services, FortiClient has access to constantly-updated protection on a real-time basis against current and emerging threats.

## Registering your Fortinet product

Before you begin configuring and customizing features, take a moment to register your Fortinet product at the Fortinet Technical Support web site, <https://support.fortinet.com>. Many Fortinet customer services, such as firmware updates, technical support, and FortiGuard Antivirus and other FortiGuard services, require product registration.

For more information, see the Fortinet Knowledge Base article Registration Frequently Asked Questions.

## Customer service & technical support

Fortinet Technical Support provides services designed to make sure that you can install your Fortinet products quickly, configure them easily, and operate them reliably in your network.

To learn about the technical support services that Fortinet provides, visit the Fortinet Technical Support web site at <https://support.fortinet.com>.

You can dramatically improve the time that it takes to resolve your technical support ticket by providing your configuration file, a network diagram, and other specific information. For a list of required information, see the Fortinet Knowledge Base article Fortinet Technical Support Requirements.

## Training

Fortinet Training Services provides classes that orient you quickly to your new equipment, and certifications to verify your knowledge level. Fortinet provides a variety of training programs to serve the needs of our customers and partners world-wide.

To learn about the training services that Fortinet provides, visit the Fortinet Training Services web site at <http://campus.training.fortinet.com>, or email them at [training@fortinet.com](mailto:training@fortinet.com).

## Documentation

The Fortinet Technical Documentation web site, <http://docs.fortinet.com>, provides the most up-to-date versions of Fortinet publications, as well as additional technical documentation such as technical notes.

In addition to the Fortinet Technical Documentation web site, you can find Fortinet technical documentation on the Fortinet Tools and Documentation CD, and on the Fortinet Knowledge Base.

### Fortinet Tools and Documentation CD

Many Fortinet publications are available on the Fortinet Tools and Documentation CD shipped with your Fortinet product. The documents on this CD are current at shipping time. For current versions of Fortinet documentation, visit the Fortinet Technical Documentation web site, <http://docs.fortinet.com>.

### Fortinet Knowledge Base

The Fortinet Knowledge Base provides additional Fortinet technical documentation, such as troubleshooting and how-to-articles, examples, FAQs, technical notes, and more. Visit the Fortinet Knowledge Base at <http://kb.fortinet.com>.

### Comments on Fortinet technical documentation

Please send information about any errors or omissions in this technical document to [techdoc@fortinet.com](mailto:techdoc@fortinet.com).

# Rebranding the FortiClient Application

Using the FortiClient Rebranding Tool, you can create a rebranded end point security application and a rebranded application installer. Modifiable items include:

- Text strings such as company name, product name, copyright notice, and company website URL.
- Images such as company logo, splash screen, menu bar buttons and task bar icons.
- Installer resources such as the features installed with the application (antispam, firewall, antivirus, Web filter, etc.), license key, menu item names, and product names.

The tool modifies the .msi installation file that is distributed in the .zip archive version of the FortiClient application. A certificate and password are required to re-brand the client.

The FortiClient re-branding tool is not generally available for download. Please contact your Fortinet Sales representative at [sales@fortinet.com](mailto:sales@fortinet.com) for purchase inquiries.



**Note:** The Rebranding Tool does not support the stand-alone VPN Lite Clients: IPsec client and SSL VPN client. It can only be used with the full MSI installation file which includes the VPN module.

## Preparing to rebrand the FortiClient application

There are several resources that can be rebranded. The following items are examples of resources that are necessary to rebrand the FortiClient application:

**Table 1: A sample of resources to be rebranded.**

<b>Company name graphic</b>	A bitmap (.bmp) file containing the company name and/or logo. This appears in the top banner of the application.
<b>Splash screen graphic</b>	A bitmap (.bmp) file. This displays briefly when the application starts.
<b>Logo graphic</b>	A bitmap file 48 x 48 pixels containing the company logo.
<b>Top bar for dialogs graphics</b>	There are bitmaps for the left, middle and right portions of the banner. You need to replace the original banner that says "Fortinet".
<b>Text strings</b>	You need to replace Fortinet-related text strings with ones applicable to your company. For a string that you do not use, you can enter an empty string. Determine suitable text strings for company name, product name, copyright notice, company website, and the URL for license purchase.

## Installing the Rebranding Tool application

You can install the FortiClient Rebranding Tool anywhere on the computer that you intend to use for your rebranding project. The Rebranding Tool runs on both 32-bit and 64-bit versions of the Microsoft® Windows platforms.

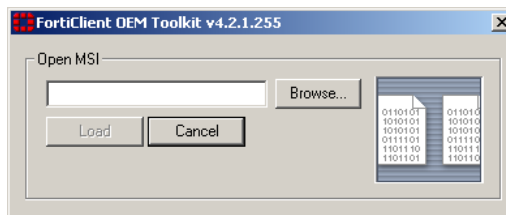


**CAUTION:** You have to use the Rebranding Tool that is from the same build as the FortiClient application that you want to rebrand.

### To install and start the Rebranding Tool

- 1 Extract the FortiClientRebrandingTool .zip file into a folder on your computer.
- 2 Double-click the FCRebrand.exe file to start the program. The FortiClient Rebranding Tool opens.

Figure 1: FortiClient Rebranding Tool application.



## Customizing the application and installer

The FortiClient Rebranding Tool allows you to change the look and feel of the application in the Application Resource tab. You can also change what features are installed (antispam, antivirus, Web filter, firewall, etc.) and other installation properties in the Installer Resources tab.

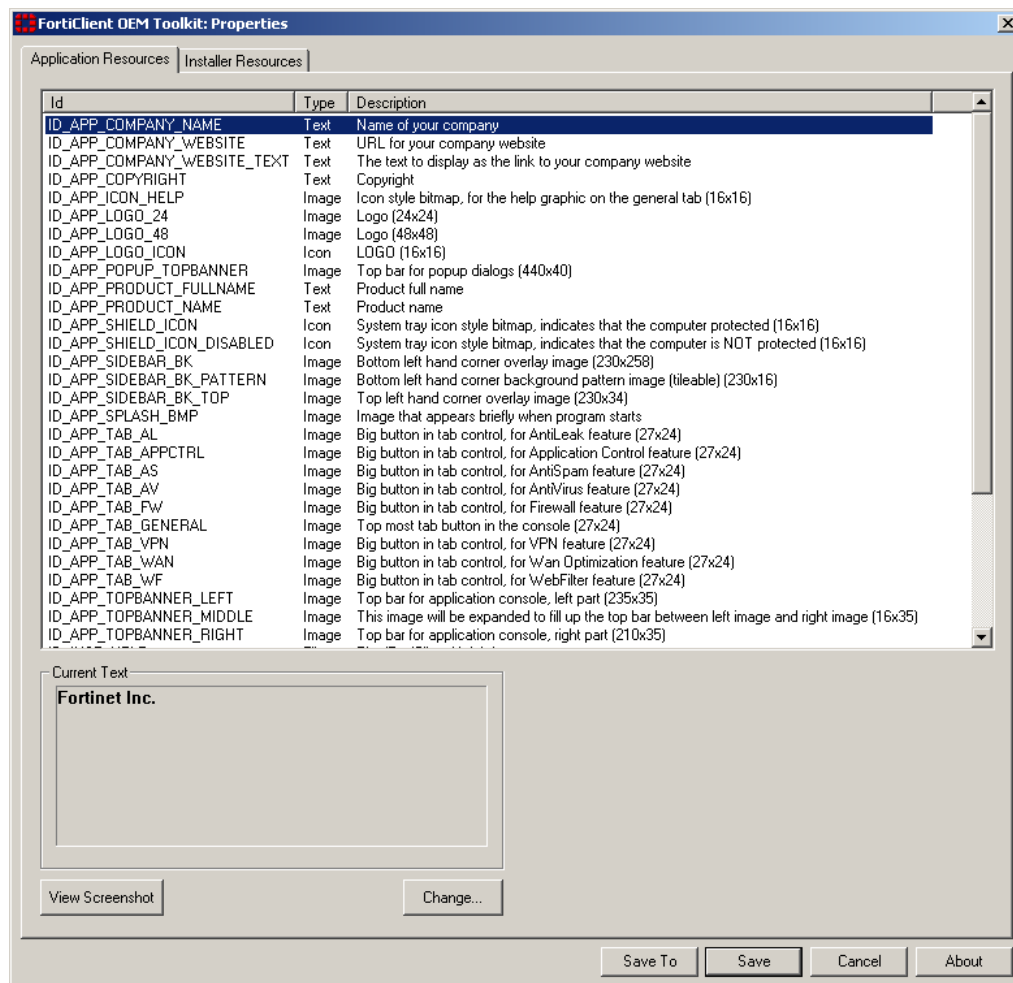
### To customize the FortiClient application and installer

- 1 Start the *FCRebrand.exe* application.
- 2 In the FortiClient OEM Toolkit window, click *Browse* and select the *FortiClient .msi* file that you want to rebrand. See [Figure 1](#).

3 Click *Load*.

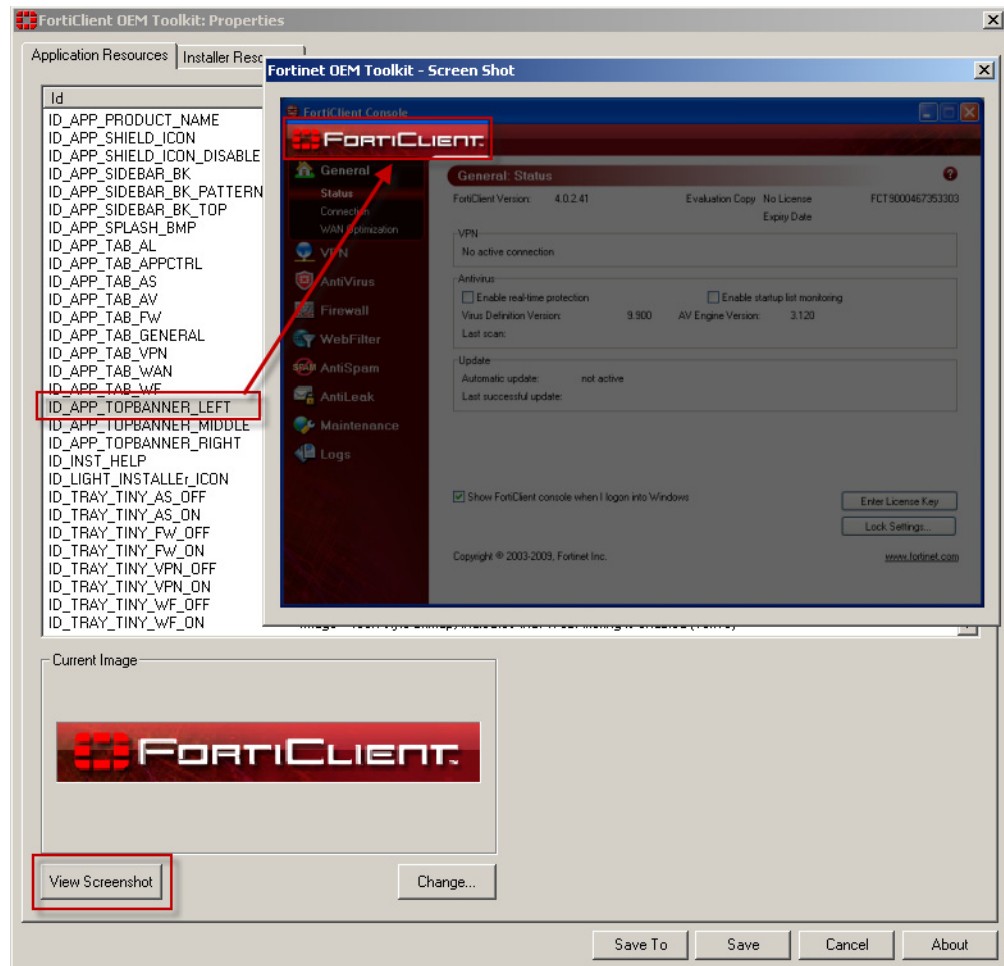
The FortiClient OEM Toolkit Properties window opens.

**Figure 2: FortiClient OEM Toolkit Properties.**



- 4 In the *Application Resources* tab, select the resource item that you want to customize.
- 5 The current resource displays in the bottom pane in the *Current* area. To see where the resource is in relation to the window, click *View Screenshot*.

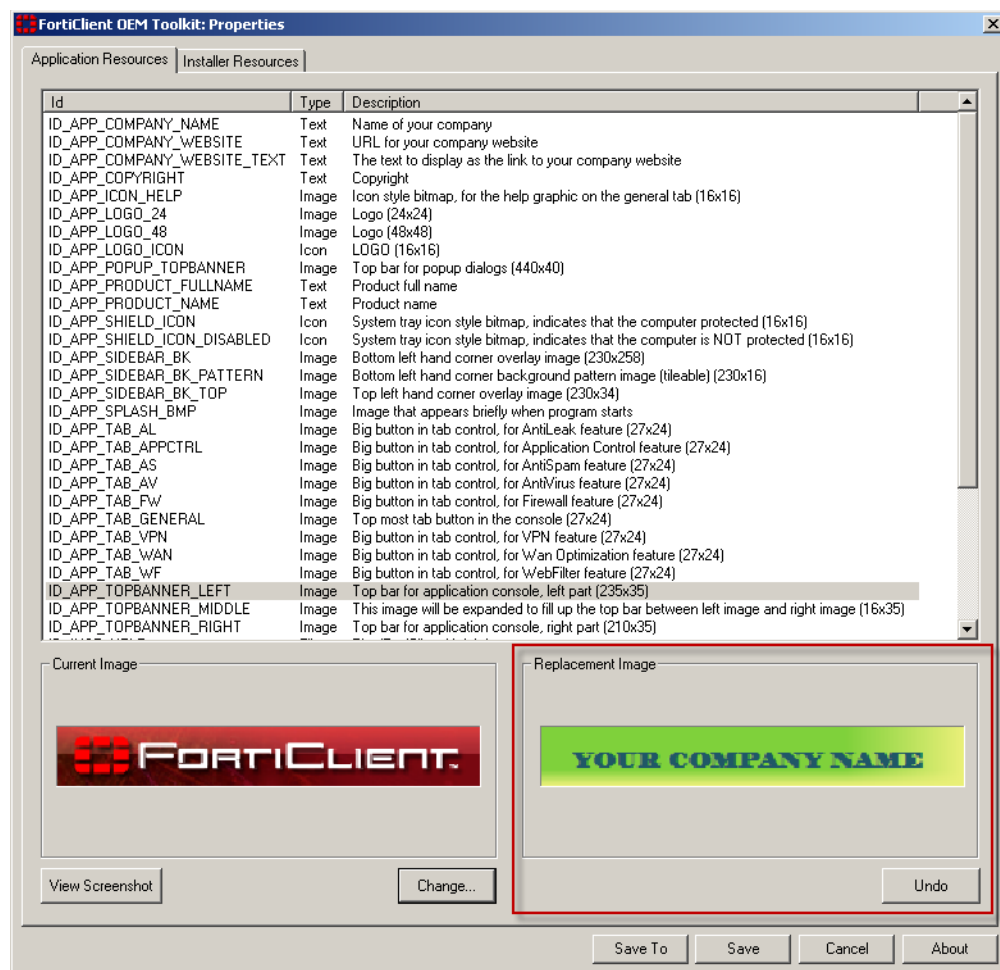
Figure 3: View of the resource location in the FortiClient application.



- 6 To change the resource, click *Change*.
- 7 Select the replacement item:
  - For text strings, enter the new text in the *Enter Text Resource* window and click **OK**.
  - For images or icons, browse to the replacement item in the *Open File* window and click *Open*.

The replacement item is shown.

Figure 4: Replacement image for an application resource.



- 8 If necessary, click *Undo* to restore the original resource item. You can undo any modifications until the modified .msi file is saved. Modifications cannot be undone after the .msi file has been saved.
- 9 Repeat the above steps for other resource items as needed.
- 10 Select the Installer Resources tab and repeat steps 5 through 7 for the installer resource items that you want to modify.
- 11 After you have modified the resources, you can save the msi file. Go to [Saving the rebranded msi file](#) for details.



**Note:** Note: You can rename the installer file, but you must also use this name for subsequent releases of your rebranded product. Microsoft Installer can only upgrade an application that was installed from an .msi file of the same name.

## Saving the rebranded msi file

After you have made the required changes using the FortiClient Rebranding Tool, you save the msi file in order to distribute it to your organization. You are required to have a certificate and password in order to save the rebranded msi file.

The certificate is a RSA 2048 bit certificate (stored as a Personal Information Exchange-PKCS #12 (\*.pfx)). You will need to provide the following information in order to receive a certificate and password from Fortinet:

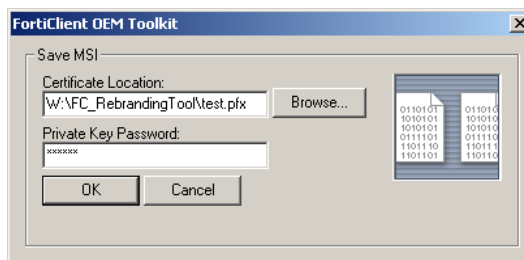
- Email
- Company
- Department
- City/State or Province/Country

If you do not have one, please contact your Fortinet Sales representative at [sales@fortinet.com](mailto:sales@fortinet.com).

#### To save the rebranded msi file

- 1 In the FortiClient OEM Toolkit properties window, do one of the following:
  - Click *Save* to save it with the same file name and location.
  - Click *Save To* to save it with a different file name and location.
- 2 If you selected *Save To*, click *Browse* to select the msi file location.
- 3 Click *Browse* and locate the certificate file (\*.pfx).
- 4 Enter the *Private Key Password* and click *OK*.

**Figure 5: Enter a certificate and password to save the msi file.**



- 5 After the file has been saved, click *OK* when the Done message appears. The FortiClient Rebranding tool automatically closes.



**FORTINET**®