



**FortiClient Host Security
Version 3.0 MR6**

FORTINET®

www.fortinet.com

FortiClient Host Security Administration Guide
Version 3.0 MR6
29 January 2008
04-30006-0400-20080129

© Copyright 2008 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

Introduction	5
About FortiClient Host Security	5
System requirements	5
Supported FortiGate models and FortiOS versions	6
Language Support.....	6
About this Guide.....	6
Documentation.....	6
Fortinet Tools and Documentation CD	7
Fortinet Knowledge Center	7
Comments on Fortinet technical documentation	7
Customer service and technical support	7
Installation	9
FortiClient software packages.....	9
Package types.....	9
Reduced size installers	10
A note about installing on servers	10
A note about installing from a drive created with subst.....	10
Installing FortiClient for central management	11
Configuring central management by specified FortiManager units	11
Configuring central management by discovered FortiManager units	12
Creating a network installer image	12
Installing FortiClient using Active Directory Server.....	13
Installing FortiClient as part of a cloned disk image.....	13
Installing FortiClient on Citrix Server for web filtering	14
Installer customization	15
Overview.....	15
Creating a customized installer using FCRepackager.....	15
Creating the sample installation	16
Performing additional customizations	16
Creating the custom MSI installation file	18
Deploying the customized FortiClient application	18
Customizing the installer using an MSI editor.....	19
Creating a FortiClient custom installation.....	19
Disabling VPN XAuth password saving	21
Enabling Remote Management with FortiManager	21
Locking Down the User Interface	22
Specifying install log file	23
Language transforms	23
Specifying multiple transforms on the command line	23

Enforcing use of FortiClient.....	25
Overview.....	25
Configuring FortiClient checking.....	25
Configuring FortiClient checking on FortiGate units	25
Configuring FortiClient checking on FortiGate model 244B.....	26
Uploading the FortiClient installer to your FortiGate unit	27
Configuring FortiGate VPNs for FortiClient PCs	29
Configuring the FortiGate settings - policy-based VPN	29
Configuring the FortiGate settings - route-based VPN.....	32
Configuring the FortiGate gateway as a policy server	33
Per-user web filtering	35
Overview of per-user web filtering.....	35
Using FortiClient for web filtering on a Windows network	35
Web filtering for remote users.....	35
Configuring FortiManager for FortiClient web filtering	36
Adding FortiClient PCs to the managed clients list	36
Defining web filter profiles.....	37
Configuring LDAP settings.....	37
Assigning web filter profiles to groups and users.....	38
Index	39

Introduction

This chapter introduces you to FortiClient Host Security software and the following topics:

- [About FortiClient Host Security](#)
- [Documentation](#)
- [Customer service and technical support](#)

About FortiClient Host Security

FortiClient Host Security is a unified security agent for Windows computers that integrates personal firewall, IPSec VPN, antivirus, antispymware, antispam and web content filtering into a single software package.

With the FortiClient application, you can:

- create VPN connections to remote networks,
- scan your computer for viruses,
- configure real-time protection against viruses and unauthorized modification of the Windows registry,
- restrict access to your system and applications by setting up firewall policies.
- restrict Internet access according the rules you specify.
- filter incoming email on your Microsoft Outlook® and Microsoft Outlook® Express to collect spam automatically.
- use the remote management function provided by the FortiManager System.

System requirements

To install FortiClient 3.0 you need:

- A PC-compatible computer with Pentium processor or equivalent
- Compatible operating system and minimum RAM:
 - Microsoft Windows 2000: 128 MB
 - Microsoft Windows XP 32-bit and 64-bit: 256 MB
 - Microsoft Windows Server 2003 32-bit and 64-bit: 384 MB
 - Microsoft Windows Vista: 512 MB
- 100 MB hard disk space
- Native Microsoft TCP/IP communications protocol
- Native Microsoft PPP dialer for dial-up connections
- an Ethernet connection



Note: The FortiClient software installs a virtual network adapter.

Supported FortiGate models and FortiOS versions

The FortiClient software supports all FortiGate models running FortiOS version 2.36, 2.5, 2.8 and 3.0.

Language Support

The FortiClient Host Security user interface and documentation is localized for:

- English
- Simplified Chinese
- Japanese
- Korean
- Slovak

The FortiClient installation software detects which code page the computer is using and installs the matching language version. For any languages other than the above are detected, the English version of the software is installed.

About this Guide

This Administration Guide contains the following chapters:

- [Installation](#) describes several types of FortiClient installation beyond the simple end-user installations described in the *FortiClient Host Security User Guide*.
- [Installer customization](#) describes how to create a customized installation package to deploy to users in an organization. The customized installation can include enabling centralized management by a FortiManager server.
- [Enforcing use of FortiClient](#) describes how to enforce use of FortiClient Host Security using a FortiGate unit that can check hosts for the presence FortiClient Host Security.
- [Configuring FortiGate VPNs for FortiClient PCs](#) describes how to configure VPNs on FortiGate units to work with the VPN client feature of FortiClient Host Security.
- [Per-user web filtering](#) describes how to deploy the FortiClient application to perform web filtering customized for each user on a Microsoft Windows network. For larger deployments, a FortiManager system is used to manage web filter profiles.

Documentation

In addition to this *FortiClient Host Security User Guide*, the FortiClient online help provides information and procedures for using and configuring the FortiClient software.

For information about deploying the FortiClient application in your organization, see the [FortiClient Administration Guide](#).

Information about FortiGate Antivirus Firewalls is available from the FortiGate online help and the *FortiGate Administration Guide*.

Fortinet Tools and Documentation CD

All Fortinet documentation is available on the Fortinet Tools and Documentation CD shipped with your Fortinet product. (You do not receive this CD if you download the FortiClient application.) The documents on this CD are current at shipping time. For up-to-date versions of Fortinet documentation visit the Fortinet Technical Documentation web site at <http://docs.forticare.com>.

Fortinet Knowledge Center

Additional Fortinet technical documentation is available from the Fortinet Knowledge Center. The knowledge center contains troubleshooting and how-to articles, FAQs, technical notes, a glossary, and more. Visit the Fortinet Knowledge Center at <http://kc.forticare.com>.

Comments on Fortinet technical documentation

You can send information about errors or omissions in this document or any Fortinet technical documentation to techdoc@fortinet.com.

Customer service and technical support

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

Please visit the Fortinet Technical Support web site at <http://support.fortinet.com> to learn about the technical support services that Fortinet provides.

Installation

This chapter describes several types of FortiClient installation beyond the simple end-user installations described in the *FortiClient User Guide*. These installations can use the standard FortiClient installer packages provided by Fortinet or installers that you have customized. For information about customizing FortiClient installer packages, see the “[Installer customization](#)” chapter.

This chapter contains the following sections:

- [FortiClient software packages](#)
- [Installing FortiClient for central management](#)
- [Creating a network installer image](#)
- [Installing FortiClient using Active Directory Server](#)
- [Installing FortiClient as part of a cloned disk image](#)
- [Installing FortiClient on Citrix Server for web filtering](#)

FortiClient software packages

Fortinet provides several different installation packages for FortiClient software. Use the following information to choose the best package for your purpose.

Package types

The two main types of installation packages for FortiClient software are:

- a Windows executable (.exe) file
- a .zip file (compressed archive) containing a Microsoft Installer (MSI) package, language transform files and the FCRepackager tool

The 64-bit versions of these files have “_x64” in the name. If you are running 64-bit Windows, you must use a 64-bit installation package.

Windows executable (.exe) installer

The Windows executable (.exe) installer provides easy installation on a single computer by the end user. Any existing FortiClient 2.0 or 3.0 installation on the PC is upgraded. The *FortiClient Host Security User Guide* provides information about using these installers.

You cannot customize the .exe package prior to deployment, but you can use this package to install centrally-managed FortiClient applications. However, this is a more complicated procedure involving command-line options. See “[Installing FortiClient for central management](#)” on page 11. It might be simpler for your users if you create a customized installer from the .zip package.

MSI installer

The MSI installer in the .zip file package is customizable for a larger roll-out to many computers in an organization. This customization procedures in this chapter use the .zip file package exclusively. You can deploy the customized MSI installer to your users and they can install it following the simple instructions in the *FortiClient Host Security User Guide*. You can preconfigure all application settings, including the configuration for centralized management by a FortiManager system. For more information, see [“Installer customization” on page 15](#).

You can upgrade an existing FortiClient 2.0 or 3.0 installation by installing a newer version of the software. To upgrade using an MSI installer, you must use the following command line:

```
msiexec /i FortiClient.msi REINSTALL=ALL REINSTALLMODE=vomus
```

Reduced size installers

Reduced size versions of both the .exe and .zip installers are also available. These installers, with “_FG” in the name, contain a much smaller antivirus database. After installation, the FortiClient application obtains the entire database when it performs an antivirus update.

The reduced size installers are intended for upload to some FortiGate models that provide the FortiClient installer to users on a special web portal. This feature is part of a host check function that can check whether users have FortiClient software installed. Users who fail the check are redirected to the web portal. For more information, see [“Enforcing use of FortiClient” on page 25](#).

As with the full-size installers, only the MSI installer is customizable.

A note about installing on servers

When installing FortiClient Host Security on a server, follow the antivirus guidelines for other products installed on the server. You might need to exclude from antivirus scanning certain files and directories such as Exchange Server, SQL Server and other software with database back-ends.

A note about installing from a drive created with subst

Installing from an MSI package does not work if the MSI file is located on a drive created with the subst command. You can do any of the following:

- specify the real path to the file
- move the MSI file to a location where this is not an issue
- use the .exe installer instead, if possible

Installing FortiClient for central management

You can install the FortiClient Host Security application from a .zip or .exe package and configure it for central management. The installed FortiClient application can either accept management from a FortiManager unit at a specific IP address, or discover FortiManager units on its network.

Configuring central management by specified FortiManager units

Using installer command line options, you can specify the IP address of one or more FortiManager units that will control the FortiClient configuration.

The command-line options are as follows:

`FMGREENABLED=1` This enables FortiManager central management.
`FMGRIP=<FM_IP_Primary>` This specifies the primary (or only) FortiManager unit.

If there are multiple FortiManager units that could manage this FortiClient PC, add the following option.

`FMGRTRUSTEDIPS=<FM_IP1>,<FM_IP2>,...`

`<FM_IP1>,<FM_IP2>`, and so on can be individual IP addresses, IP address ranges or subnets. You can omit the FMGRIP option if the primary FortiManager unit IP address is included as a single IP address in the FMGRTRUSTEDIPS option.

Example command lines for the .exe package

For a FortiClient PC centrally managed by a FortiManager unit on IP address 172.16.100.5, the installation command line is:

```
FortiClientSetup /v"FMGREENABLED=1 FMGRIP=172.16.100.5"
```

For a FortiClient PC centrally managed by either a primary FortiManager unit on IP address 172.16.100.5 or a secondary FortiManager unit on 172.16.100.6, the installation command line is:

```
FortiClientSetup /v"FMGREENABLED=1 FMGRIP=172.16.100.5  
FMGRTRUSTEDIPS=172.16.100.5,172.16.100.6"
```

Note: You must enter the entire command on a single line.

Example command lines for the .zip package

Expand the .zip package into a folder before you execute these commands.

For a FortiClient PC centrally managed by a FortiManager unit on IP address 172.16.100.5, the installation command line is:

```
msiexec /i FortiClient.msi FMGREENABLED=1 FMGRIP=172.16.100.5
```

For a FortiClient PC centrally managed by either a primary FortiManager unit on IP address 172.16.100.5 or a secondary FortiManager unit on 172.16.100.6, the installation command line is:

```
msiexec /i FortiClient.msi FMGREENABLED=1 FMGRIP=172.16.100.5  
FMGRTRUSTEDIPS=172.16.100.5,172.16.100.6
```

Note: You must enter the entire command on a single line.

Configuring central management by discovered FortiManager units

Using installer command line options, you can enable discovery of FortiManager units and specify by IP address the FortiManager units from which the FortiClient application accepts central management.

The command-line options are as follows:

<code>FMGREENABLED=1</code>	This enables FortiManager central management.
<code>FMGREENABLEDISCOVER=1</code>	This enables the FortiClient application to request central management.
<code>FMGRTRUSTEDIPS=<FM_IP1>, <FM_IP2>, ...</code>	Specify individual IP addresses, IP address ranges or subnets from which the FortiClient application accepts central management.

Example command lines for the .exe package

For a FortiClient PC that accepts central management by any FortiManager unit on subnet 172.16.100.0/24, the installation command line is:

```
FortiClientSetup /v"FMGREENABLED=1 FMGREENABLEDISCOVER=1
FMGRTRUSTEDIPS=172.16.100.0/255.255.255.0"
```

Note: You must enter the entire command on a single line.

Example command lines for the .zip package

Expand the .zip package into a folder before you execute these commands.

For a FortiClient PC that accepts central management by any FortiManager unit on subnet 172.16.100.0/24, the installation command line is:

```
msiexec /i FortiClient.msi FMGREENABLED=1
FMGREENABLEDISCOVER=1
FMGRTRUSTEDIPS=172.16.100.0/255.255.255.0
```

Note: You must enter the entire command on a single line.

Creating a network installer image

You can place the FortiClient.msi file in a shared network folder from which users can install the FortiClient application. The FortiClient.msi file is a compressed archive containing all of the needed files. Creating an uncompressed set of installation files can improve installation speed, especially if the customized FortiClient application does not contain all features.

To create a network installer

- 1 Create or choose a shared network folder for the installation.
- 2 From the folder that contains the FortiClient.msi file, execute the following command:

```
msiexec /qb /a FortiClient.msi TARGETDIR=<location>
```

where <location> is the path to the shared network folder where you want to place the uncompressed installation files, for example `c:\fc_installer\`.

The shared network folder contains a FortiClient.msi file that is smaller than the original because the other files have been decompressed into a set of subfolders. To install the customized FortiClient application on their own PCs, users simply execute the FortiClient.msi file.

Installing FortiClient using Active Directory Server

You can customize the FortiClient installation and use the Active Directory Server to install different customized installations on different computers.

The following is a general description of how to deploy the FortiClient software to remote computers using Active Directory Server. For more details, see 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.

To deploy FortiClient using Active Directory Server

- 1 Put the FortiClient MSI installation file into a shared 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.

Installing FortiClient as part of a cloned disk image

If you configure PCs using a cloned hard disk image, you need to remove the unique identifier from the FortiClient application. You will encounter problems with FortiManager Server if you deploy multiple FortiClient applications with the same identifier.

This section describes how to include a custom FortiClient installation in a cloned hard disk image but remove its unique identifier. The FortiClient application on each cloned PC will generate its own unique identifier the first time the computer is started.

To include a FortiClient installation in a hard disk image

- 1 Using an MSI FortiClient installer, install and configure the FortiClient application to suit your requirements.
You can use a standard or a customized installation package.
- 2 Right-click the FortiClient icon in the system tray and select Shutdown FortiClient.
- 3 From the folder where you expanded the FortiClient .zip package, run RemoveFCTID.exe. The RemoveFCTID tool requires administrative rights.



Note: Do not make the RemoveFCTID tool part of a logon script.

- 4 Shut down the PC.



Note: Do not reboot the Windows operating system on the PC before you create the hard disk image. The FortiClient identifier is created before you log on.

- 5 Create the hard disk image and deploy it as needed.

Installing FortiClient on Citrix Server for web filtering

You can install FortiClient Host Security on Citrix Presentation Server 4.5 in a Windows Server 2003 or Windows Server 2008 Beta 3 environment.

You can use a standard or a customized installation package, but you must select the Custom installation option and make sure that you do not install the VPN feature. Citrix uses the Windows IPsec service, which the FortiClient VPN would disable.

After installing the FortiClient application, restart the Citrix server. This resolves the problem that the FortiClient installation can cause the Citrix console to lose communication with the server.

To implement per-user web filtering, you need to define web filter profiles for your users. For more information, see the [FortiClient 3.0 Host Security User Guide](#).

Installer customization

This chapter describes how to create a custom MSI package for FortiClient Host Security that you can deploy to your users. The customized installation can include the necessary configuration for central management by a FortiManager system.

This chapter contains the following sections:

- [Overview](#)
- [Creating a customized installer using FCRepackager](#)
- [Customizing the installer using an MSI editor](#)

Overview

This chapter describes two methods of producing a custom MSI installer: using FCRepackager and using the MSI editor. The FCRepackager tool is included in the FortiClient .zip file and is easier to use.

With both types of customized installation, you can:

- set which features are installed
- include the FortiClient license key
- enable or disable the installation wizard
- enable or disable update scheduling
- set update schedule randomly on install
- enable or disable upgrade of existing installation
- enable management by a FortiManager system and set the FortiClient Manager lockdown password

You can simply give your users the customized package to install. It works the same way as the standard installer provided by Fortinet. There are several other ways to distribute the customized installer, including a network installer image, Windows Active Directory server or the FortiClient host check feature on some FortiGate units. These are described in the [Installation](#) chapter.

Creating a customized installer using FCRepackager

Using the FCRepackager tool, you can create a custom installation package in a few steps:

- create a sample installation of FortiClient configured as you want the FortiClient application to be configured on your users' computers.
- create a custom installation package using either FCRepackager or an MSI editor. The FCRepackager application is easier to use.
- install the customized FortiClient application on your users' computers. With the proper administrative permissions, users can even do this themselves.

Creating the sample installation

You need to create a sample installation on a computer running one of the supported operating systems. See [“System requirements” on page 5](#). The computer should not already have the FortiClient application installed. The ADMINMODE=1 option in the procedure enables you to make customizations that require registry changes.

To perform the sample installation of the FortiClient software

- 1 Expand the FortiClient Host Security installer .zip package into a new folder.
- 2 From the folder where you expanded the .zip package, install the FortiClient application using one of following command lines:
 - if FortiClient applications will not be centrally managed,
`msiexec /i FortiClient.msi ADMINMODE=1`
 - if FortiClient applications will be centrally managed, follow the instructions in [“Installing FortiClient for central management” on page 11](#). Install from the .msi package and be sure to also add ADMINMODE=1 to the command line.

The FortiClient application wizard starts. Follow the wizard to install the features you require. Reboot the computer when the installer requests. When the computer restarts, the FortiClient installation wizard continues.

- 3 Continue configuring the application. The wizard Advanced Setup option covers security zones, proxy settings, update settings and AV scan settings. These can also be configured later.
- 4 Configure the sample installation as you want the FortiClient application to be configured on your user’s computers.
- 5 Optionally, perform additional customizations as described in [“Performing additional customizations” on page 16](#).

See the *FortiClient Host Security User Guide* for information about configuring each of the FortiClient features.

Performing additional customizations

By editing the registry, you can make additional customizations to your FortiClient installation.

Hiding the FortiTray

- 1 Using regedit or regedt32, edit the following key:
HKEY_LOCAL_MACHINE\Software\Fortinet\FortiClient\FA_FORTITRAY
- 2 Set the key value to 0.

Permitting fallback to public FDS servers

Managed FortiClient PCs receive push updates for antivirus definitions. Mobile users might not always be able to connect to the FortiManager unit. Optionally, you can configure FortiClient to use the default public FDS servers when necessary.

To permit fallback use of public FDS servers

- 1 Using regedit or regedt32, create the following key:
HKEY_LOCAL_MACHINE\Software\Fortinet\FortiClient\FA_UPDATE\FallbackToDefault
- 2 Set the key value to 1.

Disabling saving of VPN XAUTH passwords

This customization prevents users from saving their XAUTH passwords.

To disable saving of XAUTH passwords

- 1 Using regedit or regedt32, edit the following key:
HKEY_LOCAL_MACHINE\Software\Fortinet\FortiClient\FA_IKE\
- 2 Add the value DontRememberPassword as a DWORD under the key.
- 3 Set the value of DontRememberPassword to 1.

Disabling web filter rating of IP addresses

The FortiClient web filter requests ratings from the FortiGuard web filtering service for both the URL and the IP address. Optionally, you can disable the rating of IP addresses so that web sites are rated only by URL.

To disable rating of IP addresses

- 1 Using regedit or regedt32, edit the following key:
HKEY_LOCAL_MACHINE\Software\Fortinet\FortiClient\FA_WEBFILTER\
- 2 Add the value DontRateIP as a DWORD under the key.
- 3 Set the value of DontRateIP to 1.

Blocking all connections that have no firewall rule

By default, if there is no firewall rule for a particular network connection, the FortiClient application asks the user whether to allow the connection. For an enterprise deployment, you might prefer to block all connections except those that have a specific firewall rule to permit them.

To block all connections by default

- 1 Using regedit or regedt32, edit the following key:
HKEY_LOCAL_MACHINE\Software\Fortinet\FortiClient\FA_FCM\firewallbehavior
- 2 Set the key value to 0.

Creating the custom MSI installation file

With the sample application configured as you want for your users, you can create a custom MSI installer file for your customized FortiClient application.

- 1 Determine the command line options you need for your customized FortiClient installer from the following table.

Table 1: FCRepackager options

Specify license key	-k <license_key>
Lock down program for FortiManager. Specify the plain text password.	-L <lockdown_password>
Set random AV update time (MR5 or later) between specified hours. The sample installation must contain an update schedule.	-s <start_hour>-<end_hour>
Specify which features can be installed. The resulting .msi file cannot be used for upgrades, only for new installations. If the -i option is not specified, all features are available for installation.	-i <feature1>[,<feature2>] ... Features are: AV Antivirus VPN Virtual Private Network FW Firewall WF Web filter AS Antispam Note: feature names are case-sensitive.

Refer to the FCRepackager_Readme.txt file for more information about command line options.

- 2 In the folder where you expanded the installer .zip package, execute the following command line:

```
FCRepackager -m FortiClient.msi <options from step 1>
```

A new subdirectory is created, named transformed. It contains the new FortiClient.msi file.

Deploying the customized FortiClient application

You can distribute your new FortiClient.msi file to users. Users simply double-click the file to begin installation. On a Windows Advanced Server network, you can install the application on end users' computers remotely. See [“Installing FortiClient using Active Directory Server” on page 13](#).

VPN certificates are not included in the customized installer. You need to distribute these to your users separately and provide instructions or assistance to import them into each installed FortiClient application.

Customizing the installer using an MSI editor

Use an MSI editor to create a custom FortiClient installation package. Do not edit the MSI file directly. Create a transform file that contains the configuration changes you require. The transform file is applied to the original MSI file at run time by the msiexec.exe executable file. Creating a transform file takes a bit more time than editing the MSI file directly, however it will save you time in the long run as you can apply the same transform file to future FortiClient releases.



Caution: You must follow the editing rules described 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 were created specifically for modifying FortiClient installations:

- REGISTRY_MST_FWSettings
- REGISTRY_MST_AVSettings
- REGISTRY_MST_VPNSettings
- REGISTRY_MST_WEBFILTERSettings
- REGISTRY_MST_ANTISPAMSettings

If possible, avoid modifying any other components. FortiClient sub-features do not support “Advertised” installations.

The following rules **MUST** be followed:

- never delete a feature you do not need. If you do not need a feature, set the install level to 0.
- never delete a component you do not 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 component.
- never change the PRODUCTCODE.
- never change the UPGRADECODE.
- never add new features to the root of the feature tree. If you really need to add 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.

Creating a FortiClient custom installation

Use an MSI editor and the original FortiClient MSI installation file for the following procedure. These instructions assume you know how to:

- use an MSI editor
- use the command line msiexec commands
- roll out an MSI based installation to your network.



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

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. For example, custom_3.0.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_3.0.mst /L*v c:\log.txt
```

where <path to package> is the path to your package if not in the current directory.

There are no spaces in TRANSFORMS=custom_3.0.128.mst. There is a space between TRANSFORMS=custom_3.0.mst and /L*v c:\log.txt.

If there are any errors during installation, the log file is an invaluable source of information.

- 6 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.
- 7 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.
- 8 Roll out your custom FortiClient installation specifying the transform file.

Suppressing Features

To suppress FortiClient features from installing, create a transform which sets the Install Level of the feature to 0 (zero).

Adding a license key

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

```
msiexec /i FortiClient.msi ISX_LICENSE=1234567890abc
```

Note that the installation will not abort if you specify an invalid license key.

For more information on custom installs, see the Fortinet Knowledge Center at <http://kc.forticare.com/default.asp?id=1668>.

Disabling VPN XAuth password saving

With FortiClient 3.0, you can disable the ability for a user to save the VPN XAuth password using a registry setting in a custom installation.

To disable the VPN XAuth password saving

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

Enabling Remote Management with FortiManager

Network administrators can use FortiManager 3.0 to manage FortiClient installations across a network. This enables the administrator to apply a consistent FortiClient configuration for all users. Managed FortiClient PCs receive push updates for antivirus signatures.

To enable remote management using FortiManager 3.0, you must create a transform that changes the values of specific properties within the installer.

To enable remote management

- 1 Create a new, or edit an existing, MSI transform file.
- 2 Open the Property table and change the value of FMGRENABLED from 0 to 1.
- 3 Change the property FMGTRUSTEDIPS to the IP address(es) of the FortiManager(s) that FortiClient will accept commands from.

The addresses can be specified as individual IP address, IP address ranges, or subnets. You can specify a mixed list of addresses, ranges and subnets by separating each value with a comma. For example:

Property Name	Property Value	Meaning
TRUSTEDIPS	172.16.90.83	(trust a single ip only)
TRUSTEDIPS	172.18.2.0/255.255.255.0	(trust a subnet)
TRUSTEDIPS	172.16.3.1-172.16.3.50	(trust an ip range)
TRUSTEDIPS	172.16.90.83,172.18.2.0/255.255.255.0,172.16.3.1-172.16.3.50	(all the above)

- 4 Optionally, you can specify the IP address of your FortiManager device at installation time by setting the value of the property FMGRIP to the IP address of your FortiManager device. The address specified in FMGRIP is automatically trusted and does not need to be added to the FMGTRUSTEDIPS value.

Sample command lines

- Install FortiClient

```
msiexec /i <folder of FortiClient.msi>\FortiClient.msi
FMGRENABLED=1 FMGTRUSTEDIPS=<FortiClientManager IP>
```

- Upgrade FortiClient

```
msiexec /i <folder of FortiClient.msi>\FortiClient.msi
FMGREENABLED=1 FMGRTRUSTEDIPS=<FortiClientManager IP>
REINSTALL=ALL REINSTALLMODE=vomus
```

- Install FortiClient on a PC which is behind a NAT device

```
msiexec /i <folder of FortiClient.msi>\FortiClient.msi
FMGREENABLED=1 FMGRIP=<FortiClientManager IP>
FMGREENABLEDISCOVER=1
```

- Upgrade FortiClient on a PC which is behind a NAT device

```
msiexec /i <folder of FortiClient.msi>\FortiClient.msi
FMGREENABLED=1 FMGRIP=<FortiClientManager IP> REINSTALL=ALL
REINSTALLMODE=vomus FMGREENABLEDISCOVER=1
```

Using auto discovery

You can optionally enable a protocol that enables FortiClient to independently seek out a FortiManager once the FortiClient installation has completed. To enable this you must create a transform that changes the values of specific properties within the installer.

To enable FortiClient auto discovery

- 1 Create a new, or edit an existing, MSI transform file.
- 2 Open the Property table and change the value of FMGREENABLED from 0 to 1.
- 3 Change the property FMGRTRUSTEDIPS so that it specifies the IP address(es) of FortiManager(s) that FortiClient will accept commands from.

The addresses can be specified as individual IP addresses, IP address ranges, or sub nets. You can specify a mixed list of addresses, ranges and subnets by separating each value with a comma.

- 4 Change the property FMGREENABLEDISCOVER so that its value is 1.
- 5 Optionally, you can change the frequency of the search by changing the default values of the property FMGRDISCOVERINTERVAL. The value is expressed in milliseconds. The default is 30 seconds. It is unlikely that you should need to change this.
- 6 Optionally, you can also change the number of times that FortiClient will search for a FortiManager device by changing the default values of the property FMGRDISCOVERATTEMPTS. The default is 0, for never stop trying. It is unlikely that you should need to change this.

Locking Down the User Interface

Although the user interface is locked down to users who have limited accounts, users in the administrators group can change the FortiClient settings. You can also lock down the FortiClient UI presented to administrators.

If you have enabled Remote Management by following the section above, you can lock down FortiClient's UI using FortiManager. See the [FortiManager Administration Guide](#) for more information.

Alternatively you can force lock down for all users, including administrators, by creating a property in the MSI's Property table.

To lock the user interface for all users

- 1 Create a new, or edit an existing, MSI transform file.
- 2 Open the Property table and create a property called ADMINPWD.
- 3 Set its value to the MD5 of a pass phrase of your choice.

Specifying install log file

When installing using the MSI file, the install does not create the install log automatically. For an MSI installation to produce a log, add the following option to the command line:

```
/L*v <filepath>
```

For example:

```
msiexec /i FortiClient.msi /L*v c:\logfile.txt
```

Alternatively, you can install the appropriate logging active directory group policies.

Language transforms

The MST files that ship with the baseline FortiClient package are the English, Japanese and Simplified Chinese language transforms for the installer user interface:

- 1033.mst = US English
- 1041.mst = Japanese
- 2052.mst = Simplified Chinese
- 1028.mst = Traditional Chinese

Specifying multiple transforms on the command line

You can specify multiple transforms on the command line. Separate each transform with a semicolon. For example:

```
msiexec /i <path to package>FortiClient.msi  
TRANSFORMS=custom3.0.128.mst; 2052.mst
```


Enforcing use of FortiClient

This chapter describes how to enforce use of FortiClient Host Security using a FortiGate unit that can check hosts for the presence FortiClient Host Security.

This chapter contains the following sections:

- [Overview](#)
- [Configuring FortiClient checking](#)
- [Uploading the FortiClient installer to your FortiGate unit](#)

Overview

FortiGate units prevent viruses and other threats on the Internet from passing through the firewall to your private network. However, a computer, especially a portable computer, might become infected from media or unprotected connection to another network. This infection could spread on your internal network. FortiClient Host Security protects the PC on which it is installed.

Some FortiGate models, including 224B, 1000A and 3600A, can check that users have the FortiClient application running on their computers and deny network access to those who do not. Optionally, these FortiGate units can redirect denied users to an internal web portal from which they can download the FortiClient installation file.

Configuring FortiClient checking

FortiGate model 224B includes FortiClient checking as part of its network access control functionality. Other FortiGate models that provide FortiClient checking do so as a firewall policy option.

Configuring FortiClient checking on FortiGate units

Except for model 224B, FortiGate models that provide FortiClient checking do so as a firewall policy option. The firewall policy allows access to a particular network and when the user attempts to access that network, the FortiGate unit checks the status of FortiClient on the user's computer. You can configure FortiClient checking to deny access for several different reasons:

- FortiClient software is not installed
- FortiClient software is not licensed
- AV, Firewall or Web Filter functions are disabled
- the AV/IPS database is out-of-date

Optionally, you can redirected the denied user to a web portal from which the FortiClient installation file can be downloaded.

To enable FortiClient checking in a firewall policy

- 1 Go to **Firewall > Policy**.
- 2 Select the Edit icon for the firewall policy.
You can also perform the following steps as part of creating a new policy.
- 3 Select Check FortiClient is Installed and Running.
- 4 Under Restrict Access for, select the conditions that will cause the FortiGate unit to deny the user access.
- 5 If you want to enable users to download FortiClient software, select Redirect Restricted Users to FortiGate Download Portal.
- 6 Select OK.

For more information about creating firewall policies, see the Firewall chapter of the [FortiGate Administration Guide](#).

Configuring FortiClient checking on FortiGate model 244B

As part of its access control functionality, FortiGate model 244B can perform FortiClient checking of clients that connect to switch ports. There are two ways to apply FortiClient checking to specific switch ports:

- configure a strict access control policy based on a client profile that requires FortiClient checking
- configure a dynamic access control policy that quarantines a user for antivirus or IPS violations but releases the user from quarantine after a successful host check

The following procedures describe briefly how enable FortiClient checking on a FortiGate-244B unit. For more information, see “Configuring port quarantine” in the Switch chapter of the [FortiGate Administration Guide](#).

To configure the client profile

- 1 Go to **Switch > Port Quarantine > Client Profile**.
- 2 Select Create New or select the Edit icon for an existing client profile.
- 3 Select FortiClient AV Check and/or FortiClient Firewall Check as needed.
- 4 Optionally, select other client check options as needed.

To configure the access policy - strict policy

- 1 Go to **Switch > Port Quarantine > strict policy**.
- 2 Select Create New or select the Edit icon for an existing policy.
- 3 Select the client profile you defined in the preceding procedure.
- 4 From the Action list, select Quarantine.
- 5 In the Available Ports list, select each switch port to which this policy applies and then select the right-pointing arrow to move the port to the Member Ports list.
- 6 Select OK.

To configure the access policy - dynamic policy

- 1 Go to **Switch > Port Quarantine > Dynamic Policy**.
- 2 Select Create New or select the Edit icon for an existing policy.

- 3 Select the minimum level of IPS alert that will trigger quarantine.
- 4 Select Antivirus to trigger quarantine based on FortiGate virus detection.
- 5 In the Available Ports list, select each switch port to which this policy applies and then select the right-pointing arrow to move the port to the Member Ports list.
- 6 Select Portal.
- 7 Optionally, select Enable FortiClient Image Download to permit quarantined users to download the FortiClient installer.
- 8 Select Host Check and Auto-Recover.
- 9 From the Client Profile list, select the client profile you configured that requires FortiClient checking.

Uploading the FortiClient installer to your FortiGate unit

FortiGate models that support FortiClient download provide a convenient way to upload the FortiClient installer file using the System Status page in the web-based manager.

The file name must begin with “FortiClientSetup_”, followed by the version number, “3.0.525”, for example. On FortiGate units running FortiOS 3.0 MR5 or earlier, the remainder of the file name must be “_FG.exe”. It is not possible to upload an MSI installer package. In later versions of FortiOS, you can upload either an .msi or .exe package.

When you install the FortiClient application, you should perform an Antivirus update as soon as possible to obtain antivirus signatures.

To upload the FortiClient installer to the FortiGate unit

- 1 Connect your computer to the FortiGate unit's web-based manager.
Refer to the *Installation Guide* for your FortiGate unit for more information.
- 2 Go to **System > Status**.
- 3 In the System Information section, select Update on the FortiClient Version line.
- 4 Select Browse, navigate to the FortiClient installation file on the management computer and then select Open.
- 5 Select OK.

The FortiGate unit uploads the file.

Configuring FortiGate VPNs for FortiClient PCs

There are several ways to configure FortiGate units to accept VPN connections from FortiClient users.

- a policy-based VPN can be configured on FortiGate units running FortiOS 2.5 or later
- a route-based VPN (FortiOS 3.0 only) is simpler to configure, but it does not support DHCP over IPSec assignment of virtual addresses to FortiClient users

The procedures in this section cover basic setup of policy-based and route-based VPNs compatible with FortiClient Host Security. Only common preshared key and certificate authentication is shown here. For information about other types of authentication, see the *Authenticating FortiClient Dialup Clients Technical Note*.

Configuring the FortiGate settings - policy-based VPN

To configure the FortiGate unit to accept FortiClient VPN connections through a policy-based VPN, you need to:

- configure the FortiGate Phase 1 VPN settings
- configure the FortiGate Phase 2 VPN settings
- add the firewall policy
- optionally, configure an IPSec DHCP server so that clients can obtain virtual IP addresses by DHCP (FortiGate 3.0 only)

The default FortiGate phase 1 and 2 VPN settings match the default FortiClient VPN settings.

The following procedures are applicable to FortiGate version 3.0 and 2.80 gateways. Steps or fields specific to a particular version are marked accordingly. Procedures for FortiGate version 2.50 gateways are similar to version 2.80.

For detailed configuration information, see *FortiGate IPSec VPN Guide*.

To configure phase 1 settings

- 1 FortiGate 3.0: Go to **VPN > IPSEC > Auto Key** and select Create Phase 1.
FortiGate 2.80: Go to **VPN > IPSEC > Phase 1** and select Create New.
- 2 Enter the following information and select OK.

Name (3.0)	Enter a descriptive name.
Gateway Name (2.80)	
Remote Gateway	Select Dialup User.
Local Interface (3.0)	Select the interface through which clients connect to the FortiGate unit.
Mode	Select Main (ID Protection).

Authentication Method	Select Pre-shared Key.
Pre-shared Key	Enter the pre-shared key. This must be the same preshared key provided to the FortiClient users.
Peer option	Select Accept any peer ID.

To configure phase 2 settings

- 1 FortiOS 3.0: Go to **VPN > IPSec > Auto Key** and select Create Phase 2.
FortiOS 2.80: Go to **VPN > IPSec > Phase 2** and select Create New.
- 2 Enter the following information and select OK.

Name (3.0)	Enter a name for the VPN tunnel.
Tunnel Name (2.80)	
Phase 1 (3.0)	Select the gateway name you entered in the Phase 1 configuration.
Remote Gateway (2.80)	
Concentrator (2.80)	Select None.
Advanced	Select to configure the following optional setting.
DHCP-IPsec	Select if you provide virtual IP addresses to clients using DHCP. For more information, see “To configure an IPsec DHCP server (FortiGate 3.0)” on page 31 .

To add a source address

- 1 Go to **Firewall > Address**.
- 2 Select Create New.
- 3 Enter an address name.
- 4 Enter the individual address or the subnet address that you want the dialup users to access through the VPN.
- 5 Select OK.

To add a destination address

- 1 Go to **Firewall > Address**.
- 2 Select New.
- 3 Enter an address name.
- 4 Enter the subnet IP address from which remote FortiClient PCs are assigned virtual IP addresses.
- 5 Select OK.

To add a firewall policy

- 1 Go to **Firewall > Policy**.
- 2 Select Create New.
- 3 Enter the following information and select OK.

Source

Interface/Zone	Internal
Address Name	Select the address name you added in “To add a source address” on page 30 .

Destination

Interface/Zone External
Address Name If FortiClient PCs are not assigned virtual IP addresses, select All. Otherwise, select the address name you added in [“To add a destination address” on page 30.](#)

Schedule Always

Service Any

Action IPSEC (3.0)
 Encrypt (2.80)

VPN Tunnel Select the VPN tunnel you added in [“To configure phase 2 settings” on page 30.](#)

Allow Inbound Enable

Allow Outbound Enable

Inbound NAT Enable

Outbound NAT Disable

Protection Profile Optional

Log Traffic Optional

- 4 Move this policy above the Accept or Deny firewall policies in the policy list.

To configure an IPsec DHCP server (FortiGate 3.0)

- 1 Go to **System > Network > DHCP.**
- 2 Expand the interface that you selected as Local Interface in the Phase 1 configuration and select its Add DHCP Server icon.
- 3 Enter the following information and select OK.

Name Enter a name for the DHCP server.
Enable Select to enable the DHCP server.
Type Select IPSEC.
IP Range Enter the start and end for the range of IP addresses that this DHCP server assigns to DHCP clients.
Network Mask Enter the netmask that the DHCP server assigns to DHCP clients.
Default Gateway Enter the IP address of the default gateway that the DHCP server assigns to DHCP clients.
Domain Enter the domain that the DHCP server assigns to DHCP clients.
Lease Time Select Unlimited for an unlimited lease time or enter the interval in days, hours, and minutes after which a DHCP client must ask the DHCP server for new settings. The lease time can range from 5 minutes to 100 days.
Advanced Select to configure the following advanced options.
DNS Server 1 Enter the IP addresses of up to 3 DNS servers that the DHCP server assigns to DHCP clients.
DNS Server 2
DNS Server 3
WINS Server 1 Add the IP addresses of one or two WINS servers that the DHCP server assigns to DHCP clients.
WINS Server 2

Configuring the FortiGate settings - route-based VPN

To configure the FortiGate unit to accept FortiClient VPN connections through a route-based VPN, you need to:

- configure the FortiGate Phase 1 VPN settings
- configure the FortiGate Phase 2 VPN settings
- add the firewall policy

The default FortiGate VPN settings match the default FortiClient VPN settings.

The following procedures are applicable to FortiGate version 3.0 gateways. For detailed configuration information, see *FortiGate IPSec VPN Guide*.

To configure phase 1 settings

- 1 Go to **VPN > IPSEC > Auto Key** and select Create Phase 1.
- 2 Enter the following information.

Name	Enter a descriptive name.
Remote Gateway	Select Dialup User.
Local Interface	Select the interface through which clients connect to the FortiGate unit.
Mode	Select Main (ID Protection).
Authentication Method	Select Pre-shared Key.
Pre-shared Key	Enter the pre-shared key. This must be the same preshared key provided to the FortiClient users.
Peer option	Select Accept any peer ID.

- 3 Select Advanced.
- 4 Select Enable IPSec Interface Mode.
- 5 Select OK

To configure phase 2 settings

- 1 FortiOS 3.0: Go to **VPN > IPSEC > Auto Key** and select Create Phase 2.
- 2 Enter the following information and select OK.

Name	Enter a name for the VPN tunnel.
Phase 1	Select the gateway name you entered in the Phase 1 configuration.

To add a firewall policy

- 1 Go to **Firewall > Policy**.
- 2 Select Create New.
- 3 Enter the following information and select OK.

Source	
Interface/Zone	The Phase 1 configuration you created.
Address Name	All

Destination	
Interface/Zone	Internal
Address Name	All
Schedule	Always
Service	Any
Action	Accept
Protection Profile	Optional
Log Traffic	Optional

- 4 Move this policy above the Accept or Deny firewall policies in the policy list.

Configuring the FortiGate gateway as a policy server

You can configure a FortiGate version 3.0 gateway to work as a VPN policy server for FortiClient automatic configuration. When FortiClient users connect to the FortiGate gateway to download VPN policies, they are challenged for a user name and password. Configure the FortiGate unit as follows:

- 1 Create a user account for each FortiClient user.
- 2 Create a user group and add the FortiClient users to it.
For more information about creating users and groups, see the *FortiGate Administration Guide*.
- 3 Create a dialup VPN.
See [“Configuring the FortiGate settings - policy-based VPN”](#) on page 29.
- 4 Create a firewall policy for the dialup VPN. See [“To add a firewall policy”](#) on page 30.
- 5 Connect to the FortiGate unit CLI and configure VPN policy distribution as follows:

```
config vpn ipsec forticlient
  edit <policy_name>
    set phase2name <phase2_name>
    set usergroupname <group_name>
    set status enable
  end
```

<phase2_name> must be the name of the VPN phase 2 configuration.
<group_name> must be the name of the user group you created for FortiClient users.

Per-user web filtering

This chapter describes how to deploy the FortiClient application to perform web filtering customized for each user on a Microsoft Windows network. For larger deployments, a FortiManager system simplifies management of user web filter profiles.

This chapter contains the following sections:

- [Overview of per-user web filtering](#)
- [Configuring FortiManager for FortiClient web filtering](#)

Overview of per-user web filtering

FortiClient Host Security web filtering controls access to web sites based on FortiGuard Service web site rating categories and black/white URL lists. The web filter profile selects which FortiGuard categories the user is permitted to access. Additionally, URLs in the black list are always blocked and URLs in the white list are always permitted.

You select a web filter profile for each user or user group. Users with no assigned profile are assigned to a global profile. You can create as many profiles as you need, one per user if necessary.

You can define web filter profiles and users locally in the FortiClient application. This is most suitable for a PC with a limited number of users, or if you decide to assign occasional users to a default web filter profile. For information about configuring FortiClient web filtering, see the Web Filter chapter of the [FortiClient 3.0 Host Security User Guide](#).

If you have many FortiClient installations, you can manage their configurations with a FortiManager unit. This eliminates the need to configure all of the profiles and users on every FortiClient application you install.

Using FortiClient for web filtering on a Windows network

On a Microsoft Windows network, any user can log on at any PC. If you want to perform web filtering configurable to the group or user level, you can use a FortiManager unit to provide web filter profile information to each FortiClient application as needed.

Web filtering for remote users

You can install FortiClient on a Windows Terminal Server or a Citrix Presentation Server to provide web filtering for remote users on a Windows network. The user's PC does not need to have the FortiClient application installed. See ["Installing FortiClient on Citrix Server for web filtering"](#) on page 14.

Configuring FortiManager for FortiClient web filtering

To manage FortiClient web-filtering with a FortiManager unit, you need to:

- add each FortiClient PC as a managed client
- define the web filter profiles you will assign to users
- configure LDAP settings to obtain Windows group/user information
- assign web filter profiles to groups and users

Adding FortiClient PCs to the managed clients list

FortiClient Manager can search for FortiClient PCs on your network. FortiClient applications must be configured at installation with the IP addresses or subnets on which they accept remote management. See [“Installing FortiClient for central management” on page 11](#) for details.

Optionally, you can lock the FortiClient application settings so that users, even those with administrative privileges, cannot change the application’s settings unless they have the password configured on the FortiManager unit.

To set FortiClient Manager options

- 1 In the FortiClient Manager, go to **Setting > Global Setting**.
- 2 In the FortiClient Lockdown section, if you want to lock the configuration on the FortiClient PCs that you add, select Enable Lockdown and then enter a password.
- 3 In the Client Discovery section, check that the ports that connect to your network are enabled to listen for broadcast and unicast requests from FortiClient PCs.
- 4 To add FortiClient PCs directly to the Managed clients list, select Auto-populate managed client list. Otherwise, select Add to temporary client list.
- 5 Select Apply.

To search for FortiClient PCs

- 1 In the FortiClient Manager, go to **Client/Group > Search/Add Client**.
- 2 Do one of the following:
 - Select Lookup single client and enter the IP address of the FortiClient PC.
 - Select Scan attached networks, select the interface that connects to the network and enter the IP address and subnet mask of the network to scan.
- 3 Select Search.
- 4 If you selected the Add to temporary clients option (see [“To set FortiClient Manager options”](#)), discovered FortiClient PCs are listed in the Temporary Client list. Otherwise, discovered FortiClient PCs are added to the Managed Client list.

Configuring FortiClient installations to request registration

You can configure the FortiClient application to request management from a particular FortiManager unit. Depending on the FortiClient Manager settings, the FortiClient PC appears on the Temporary clients list or is added automatically to the Managed clients list.

Install the FortiClient application using the Microsoft Installer (the .msi file in the .zip package). Start the installer from the command line as follows to enable central management by a FortiManager server. Type the command on a single line.

```
msiexec /i FortiClient.msi FMGREENABLED=1 FMGRTRUSTEDIPS=<IP>
FMGREENABLEDISCOVER=1
```

<IP> is the address of the FortiManager unit

Defining web filter profiles

In the FortiClient Manager, go to **Setting > Web Filter Profile**. Select Create New. Enter the following information and select OK.

Name	Enter a name for the profile.
Comments	Optionally, enter descriptive information about the profile.
Bypass URLs	Bypass URLs are allowed even if they are in a blocked category.
Block URLs	Block URLs are always blocked. To add a URL, enter it in the field below the list and select Add. To remove a URL, select it in the list and then select Delete.
Select category to block	Either select Select All or select individual categories to block. You can expand the categories to select specific sub-categories.
Select classification to block	Either select Select All or select individual classifications to block.

Configuring LDAP settings

FortiClient Manager uses LDAP protocol to retrieve information about Windows AD users and groups from the domain controller.

Go to **Setting > LDAP Setting** and select Create New. Enter the following information and select OK.

Name	Enter a name for this LDAP server.
Server Name/IP	Enter the fully-qualified domain name or IP address of the Windows AD domain controller.
Server Port	Enter the port used to communicate with the LDAP server. The default is port 389. If needed, change the port to match the server.
BaseDN	Enter the Base Distinguished Name for the server. You can get this information from the server's administrator.
BindDN	Enter the Bind Distinguished Name for the server. You can get this information from the server's administrator.
Password	Enter the password required for logon to make queries.
Test Connection	Select this button to attempt a connection to the domain controller using the settings you have entered. The results of the connection test display below the button.

Assigning web filter profiles to groups and users

You can assign web filter profiles to Windows groups and users.

To assign web filter profiles to groups

- 1 In the FortiClient Manager, go to **Setting > LDAP Group/User**.
- 2 From the LDAP Server list, select the Windows AD domain controller.
- 3 Expand domains as needed to show groups.
- 4 From the Web Filter Profile list, select the profile you want to assign.
- 5 Select group(s) (each one has a check box) and then select Assign Profile.
For each selected group, the Web Filter Profile column lists the assigned profile.
- 6 Repeat Step 3 through Step 5 for each web filter profile you want to assign.

To assign web filter profiles to users

- 1 In the FortiClient Manager, go to **Setting > LDAP Group/User**.
- 2 From the LDAP Server list, select the Windows AD domain controller.
- 3 Select LDAP Users at the top left of the page.
- 4 From the Domain list, select the required domain.
- 5 From the Web Filter Profile list, select the profile you want to assign.
- 6 Select the user(s) you want to assign.
Optionally, to find a user, type the name in the User Name box at the top right of the page and select Go.
- 7 Select Assign Profile.
For each selected user, the Web Filter Profile column lists the assigned profile.
- 8 Repeat Step 5 through Step 7 for each web filter profile you want to assign.

Index

A

- auto discovery
 - enabling 22
- AV update schedule randomizing 18

B

- block access unless firewall rule permits
 - installation option 17

C

- central management
 - installing FortiClient for 11
- cloned disk image including FortiClient 13
- code page 6
- comments on Fortinet technical documentation 7
- customer service 7
- customization of FortiClient installer 15
 - deploying 18
 - overview 15
 - using FCRepackager 15
 - using MSI editor 19

D

- disable XAUTH password saving
 - installation option 17
- disabling web filter rating by IP addresses
 - installation option 17
- documentation 6

F

- FCRepackager
 - using to create customized installer 15
- FDS servers, fallback to public servers 16
- FortiClient check
 - configuring on FortiGate unit 25
- FortiClient packages 9
 - uploading to FortiGate unit 27
- FortiClient PCs
 - adding to FortiManager database 36
- FortiGate models
 - supported by FortiClient 6
- FortiGate unit
 - configuring - policy-based VPN 29
 - configuring - route-based VPN 32
- FortiManager
 - adding FortiClient PCs 36
 - configuring for FortiClient web filtering 36
 - configuring web filter profiles 37
 - FortiClient Manager options 36
- Fortinet customer service 7
- Fortinet Knowledge Center 7

- FortiOS versions
 - supported by FortiClient 6
- FortiTray
 - installation option to hide 16

H

- hide FortiTray
 - installation option 16

I

- installation options
 - block access unless firewall rule permits 17
 - disable web filter rating by IP address 17
 - disable XAUTH password saving 17
 - hide FortiTray 16
 - permit fallback to public FDS 16
- installation packages 9
- installing 9
 - creating customized installer 15
 - setting to request FortiManager registration 36
 - using Active Directory server 13
- introduction 5

L

- language support 6
- LDAP
 - for Windows user and group information 37
- license key
 - specifying in FCRepackager customization 18
 - specifying in MSI customization 20
- lockdown
 - enabling in FCRepackager customization 18
 - enabling in MSI customization 22

M

- MSI installation file
 - creating 18

P

- per-user web filtering
 - assigning profiles 38
 - configuring FortiManager for 36
 - overview 35
 - remote users 35
 - Windows network 35
- policy server
 - configuring FortiGate unit as 33

R

- remote management
 - enabling in MSI customization 21

RemoveFCTID.exe 13
removing identifier 13

S

sample installation
 for customization 16
software packages, FortiClient 9
system requirements 5

T

technical support 7

V

VPN XAUTH passwords
 installation option to disable saving 17
VPN, policy-based
 configuring on FortiGate unit 29
VPN, route-based
 configuring on FortiGate unit 32

W

web filter
 disabling rating of IP addresses 17
web filter profiles
 assigning to groups and users 38
 defining in FortiClient Manager 37
web filtering
 assigning profiles 38
 configuring FortiManager for 36
 on Citrix server 35
 on Windows Terminal server 35
 overview 35
 remote users 35
 Windows network 35

X

XAuth
 disabling password saving 21

FORTINET®

www.fortinet.com

FORTINET®

www.fortinet.com