



FortiClient Endpoint Security™

Version 4.0
Administration Guide

FortiClient Endpoint Security Administration Guide

Version 4.0

6 March 2009

04-403-86643-20090306

© Copyright 2009 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.

Regulatory compliance

FCC Class A Part 15 CSA/CUS



CAUTION: Risk of Explosion if Battery is replaced by an Incorrect Type.
Dispose of Used Batteries According to the Instructions.

Contents

Introduction	7
About FortiClient Endpoint Security	7
System requirements.....	7
Supported FortiGate models and FortiOS versions.....	8
Language Support.....	8
About this Guide	8
Documentation	8
Fortinet Tools and Documentation CD	9
Fortinet Knowledge Center	9
Comments on Fortinet technical documentation	9
Customer service and technical support.....	9
Installation	11
FortiClient software packages	11
Package types	11
Reduced size installers.....	12
Installation notes.....	12
Installing on Windows Vista SP1	12
Installing on servers.....	12
Installing from a drive created with subst.....	12
Changing the default firewall action	13
Installing FortiClient for central management.....	13
Configuring central management by specified FortiManager units.....	13
Configuring central management by discovered FortiManager units	14
Creating a network installer image.....	14
Installing FortiClient using Active Directory Server	15
Installing FortiClient as part of a cloned disk image	15
Installing FortiClient on cloned PCs	16
Installing FortiClient on Citrix Server for web filtering.....	16
Installer customization	17
Overview	17
Creating a customized installer using FCRepackager	17
Creating the sample installation.....	18
Performing additional customizations	18
Creating the custom MSI installation file.....	20
Customizing the FortiClient application for enterprise licensing	21
Deploying the customized FortiClient application	21
Transferring customizations to later versions of FortiClient.....	21

Customizing the installer using an MSI editor	21
Creating a FortiClient custom installation	22
Disabling VPN XAuth password saving	23
Enabling Remote Management with FortiManager	23
Locking Down the User Interface.....	25
Specifying install log file.....	25
Language transforms.....	25
Specifying multiple transforms on the command line	26
Setting a corporate security policy	27
Overview	27
User view of security policy	27
Configuring a corporate security policy	28
Licensing FortiClient PCs	29
Overview of licensing	29
Applying standard fixed licensing.....	29
Applying enterprise licensing.....	30
Configuring an enterprise license	30
Creating an enterprise client license key	31
Deploying the enterprise client license key.....	31
Creating a customized FortiClient installer	31
Enforcing use of FortiClient software	33
Overview	33
Configuring endpoint control on your FortiGate unit.....	33
Configuring Central Management by FGAMS	34
Setting required FortiClient version and installer download location	34
Configuring endpoint control in a FortiGate firewall policy.....	35
Uploading the FortiClient installer to your FortiGate unit.....	36
Configuring FortiGate VPNs for FortiClient PCs.....	37
Configuring the FortiGate settings - policy-based VPN	37
Configuring the FortiGate settings - route-based VPN	40
Configuring the FortiGate gateway as a policy server	41
Deploying FortiClient VPN	43
Overview	43
Creating configurations in FortiClient VPN	43
Importing VPN tunnel settings	44
Configuring VPN tunnel settings.....	44
Configuring certificates for FortiClient VPN	46
Exporting configurations to the FortiClient VPN installer	46

Using the FortiClient API.....	47
Overview	47
Controlling a VPN.....	47
Linking to the COM library	47
Retrieving a list of VPN connection names.....	48
Opening the VPN tunnel.....	48
Responding to XAuth requests.....	48
Monitoring the connection.....	49
Setting and monitoring a security policy.....	49
Setting a security policy	50
Reading a security policy.....	50
Monitoring policy compliance.....	50
Making the FortiClient application comply with the policy.....	51
API reference	52
Per-user web filtering	53
Overview of per-user web filtering	53
Using FortiClient for web filtering on a Windows network.....	53
Web filtering for remote users.....	53
Configuring FortiManager for FortiClient web filtering	54
Adding FortiClient PCs to the managed clients list.....	54
Defining web filter profiles.....	55
Configuring LDAP settings.....	55
Assigning web filter profiles to groups and users	55
Index	57

Introduction

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

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

About FortiClient Endpoint Security

FortiClient Endpoint 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 4.0 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
 - Microsoft Windows 7: 512 MB
- a compatible email application for the AntiSpam feature:
 - Microsoft Outlook 2000 or later
 - Microsoft Outlook Express 2000 or later
- a compatible email application for the AntiLeak feature:
 - Microsoft Outlook 2000 or later
- 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, 3.0 and 4.0.

Language Support

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

- English
- French
- 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 Endpoint 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.
- [Setting a corporate security policy](#) describes how you can require users to comply with a security policy to use VPN tunnels. The policy can require users to enable firewall, realtime antivirus protection, web filtering or antispam.
- [Licensing FortiClient PCs](#) describes how to manage enterprise licensing of FortiClient PCs, using either a volume license or a redistributable license.
- [Enforcing use of FortiClient](#) describes how to enforce use of FortiClient Endpoint Security using a FortiGate unit that can check hosts for the presence FortiClient Endpoint Security.
- [Configuring FortiGate VPNs for FortiClient PCs](#) describes how to configure VPNs on FortiGate units to work with the VPN client feature of FortiClient Endpoint Security.
- [Deploying FortiClient VPN](#) describes how to configure FortiClient VPN, a light VPN client that you can distribute to users who do not have FortiClient Endpoint Security.
- [Using the FortiClient API](#) describes the COM-based FortiClient API.
- [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

This manual, the *FortiClient Endpoint Security Administration Guide*, provides information about deploying the FortiClient application in your organization.

The [FortiClient Endpoint Security User Guide](#) and the FortiClient online help provide information and procedures for using and configuring the FortiClient software.

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 Endpoint Security 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](#)
- [Installation notes](#)
- [Changing the default firewall action](#)
- [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 cloned PCs](#)
- [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 Endpoint 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 13. 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 Endpoint 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 17.

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 33.

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

Installation notes

These notes describe special conditions that apply to specific types of installations.

Installing on Windows Vista SP1

Make sure that Windows is not installing updates while you install the FortiClient application. If Windows Update has run and it requested a reboot, be sure to reboot your computer before installing the FortiClient application.

Installing on servers

When installing FortiClient Endpoint 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.

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

Changing the default firewall action

By default, the FortiClient firewall allows unknown applications to access the network, or asks the user, depending on the selected firewall profile. (An unknown application is one that is not on the firewall applications list.) To make the FortiClient firewall always block unknown applications, add the `DEFAULTAPPLICATION=1` command line option when you run the FortiClient installer.

Installing FortiClient for central management

You can install the FortiClient Endpoint 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.

For information about centrally managing FortiClient PCs with FortiManager, see the FortiClient Manager chapter of the [FortiManager Administration Guide](#).

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:

FMGREENABLED=1	This enables FortiManager central management.
FMGREENABLEDISCOVER=1	This enables the FortiClient application to request central management.
FMGRTRUSTEDIPS=<FM_IP1>, <FM_IP2>,...	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. On each PC configured with the cloned hard disk image, the FortiClient application 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 cloned PCs

FortiClient 3.0 MR7 and later uses the PC hard drive serial number to create a FortiClient identifier for licensing and central management. Some manufacturers produce batches of PCs with identical hardware serial numbers. If you want to deploy FortiClient in an enterprise with such cloned PCs, you must specify an alternate method to create the FortiClient identifier when installing the application:

```
msiexec /i forticlient.msi USESWUID=1
```

or

```
FortiClientSetup /v"USESWUID=1"
```

The installer will generate a unique software identifier internally instead of using the PC hard drive serial number. You can combine the USESWUID option with other command line options as needed.

If you intend to make an image of the hard drive for deployment to other computers, you need to shut down FortiClient and use the RemoveFCTID tool to remove the FortiClient identifier. For more information, see [“Installing FortiClient as part of a cloned disk image” on page 15](#).

Installing FortiClient on Citrix Server for web filtering

You can install FortiClient Endpoint 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 Endpoint Security User Guide](#).

Installer customization

This chapter describes how to create a custom MSI package for FortiClient Endpoint 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 7](#). The computer should not already have the FortiClient application installed.

The ADMINMODE=1 option used in the following procedure enables you to make registry changes to your sample installation, which some customizations require. Also, this option permits modification of files in the FortiClient program directory, which normally only the FortiClient application can access. You should not use the ADMINMODE=1 option when you install of the FortiClient application onto your users' computers.

To perform the sample installation of the FortiClient software

- 1 Expand the FortiClient Endpoint 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 13](#). 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 18](#).

See the [FortiClient Endpoint Security User Guide](#) for information about configuring each of the FortiClient features.

Performing additional customizations

You can edit the registry to 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 DWORD value:
HKEY_LOCAL_MACHINE\Software\Fortinet\FortiClient\FA_UPDATE\FallbackToDefault
- 2 Set the 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.

Changing the certificate key size

The default VPN certificate key size in FortiClient v4.0 is 2048 bits. You can change the size.

To change the certificate key size

- 1 Using regedit or regedt32, edit the following key:
HKEY_LOCAL_MACHINE\Software\Fortinet\FortiClient\FA_CERT\key_size
- 2 Set the key value to one of: 1 (1024 bits), 15 (1536 bits), 2 (2048 bits), 3 (3072 bits) or 4 (4096 bits).

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 (for standard fixed license or volume license from FDS, not for enterprise license)	-k <license_key>
Lock down program for FortiManager. Specify the plain text password.	-L <lockdown_password>
Set random AV update time between specified hours. This is effective for FortiClient 3.0 MR5 or later. 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 AL AntiLeak Note: feature names are case-sensitive.
Shrink the .msi file by removing files for unused features. Valid only when used with -m option.	-z

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.

Customizing the installer language

You can further modify your customized installer with one of the language .mst files provided in the installer .zip file. This must be done as a separate step from the customizations described previously. The language files are:

- 1033.mst = US English (default)
- 1036.mst = French
- 1041.mst = Japanese
- 2052.mst = Simplified Chinese
- 1028.mst = Traditional Chinese

For example, to change your customized installer language to French, execute the following command in the folder where you expanded the installer .zip package:

```
FCRepackager -t 1036.mst -m transformed\FortiClient.msi
```

Customizing the FortiClient application for enterprise licensing

If you use enterprise licensing for your FortiClient PCs, your FortiClient installer needs specific additional customization. For more information, see [“Applying enterprise licensing” on page 30](#).

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 15](#).

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.

Transferring customizations to later versions of FortiClient

When a newer version of FortiClient Endpoint Security is released, your existing users can simply run the FortiClient installer and upgrade while keeping the customized settings. For new users, you will need to create a customized version of the new installer.

To customize the newer FortiClient installer, you do not need to repeat all of the customization steps described previously in this section. When you create your first customized FortiClient installer, you can also save your customizations to a transform (.mst) file. Simply run FCRepackager.exe again with no parameters. The output is a file named FortiClient.mst.

To modify the new FortiClient .msi installer with your saved customizations, use the following command:

```
FCRepackager -t FortiClient.mst -m FortiClient.msi
```

If the files are not in the current directory, you need to specify the path to them.



Note: An MSI installation package can upgrade an existing installation only if it has the same name as the original installation package. If necessary, rename the upgrade installation package to match the file name of the previous customized FortiClient installation package you provided to your users.

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 msixexec.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_4.0.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_4.0.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_4.0.mst. There is a space between TRANSFORMS=custom_4.0.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 or 4.0, 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 or 4.0 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 or 4.0, 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 address 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 address 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 FMGRTRUSTEDIPS=<FortiClientManager IP>
```
- Upgrade FortiClient


```
msiexec /i <folder of FortiClient.msi>\FortiClient.msi
  FMGRENABLED=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
  FMGRENABLED=1 FMGRIP=<FortiClientManager IP>
  FMGRENABLEDISCOVER=1
```
- Upgrade FortiClient on a PC which is behind a NAT device


```
msiexec /i <folder of FortiClient.msi>\FortiClient.msi
  FMGRENABLED=1 FMGRIP=<FortiClientManager IP> REINSTALL=ALL
  REINSTALLMODE=vomus FMGRENABLEDISCOVER=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 FMGRENABLED from 0 to 1.

- 3 Change the property FMGTRUSTEDIPS 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 subnets. You can specify a mixed list of addresses, ranges and subnets by separating each value with a comma.
- 4 Change the property FMGRENALEDISCOVER 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=custom4.0.mst; 2052.mst
```

Setting a corporate security policy

If your FortiClient PCs are centrally managed with FortiManager unit, you can set a security policy for VPN use.

This chapter contains the following sections:

- [Overview](#)
- [Configuring a corporate security policy](#)

Overview

You can set a security policy for your managed FortiClient PCs. Users cannot use a VPN connection unless the FortiClient settings comply with the policy. The security policy can require that any or all of the following features are enabled:

- Antivirus (real-time protection)
- Antispam
- Firewall (Normal mode)
- Web Filter

This provides security when users connect to your corporate network through a VPN.

User view of security policy

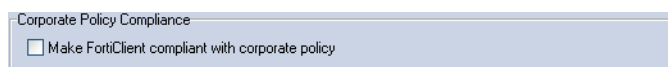
If a corporate security policy is set, the FortiClient Console General tab includes a Corporate Policy Compliance section that displays the compliance status of the FortiClient PC.

Figure 1: Corporate policy compliance status - in compliance



If the user disables any of the required features, the FortiClient PC is no longer in compliance with the policy. If a VPN tunnel is in use, it is disconnected. The Corporate Policy Compliance status changes to show the following.

Figure 2: Corporate policy compliance status - not in compliance



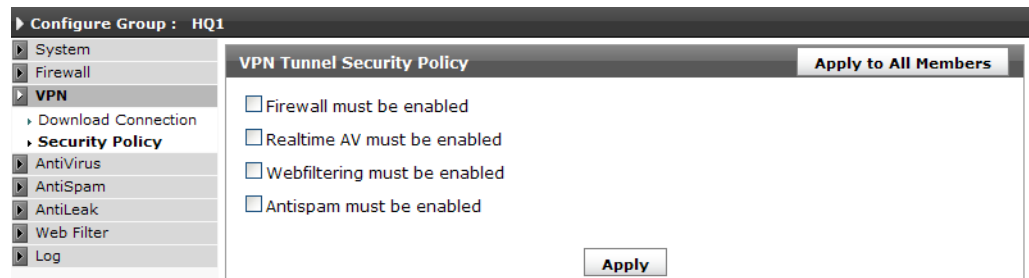
The user can bring FortiClient settings into compliance again by selecting the check box.

Configuring a corporate security policy

You configure your corporate security policy in the FortiClient Manager module of the FortiManager unit. It is simplest to apply security policies to client groups. If you have already created client groups, you can create security policies for those groups. If your FortiClient PCs are ungrouped, you can create a client group for the purpose of applying security policies.

To configure a security policy

- 1 In the FortiClient Manager, go to *Client/Group > Group*.
- 2 Select the client group that you want to configure.
- 3 From the FortiClient menu, select *VPN > Security Policy*.



- 4 Select any of the following policies that you want to enforce:
 - Firewall must be enabled
 - Realtime AV must be enabled
 - Webfiltering must be enabled
 - Antispam must be enabled
- 5 Select *Apply*.
- 6 Repeat steps 2 through 4 if you want to create security policies for other client groups.
- 7 Go to *Manage > Deploy Configuration*.
- 8 Select the client group(s) where you created security policies and then select *Deploy*.

When the updated configuration is deployed to the FortiClient PCs, their configuration settings are made compliant with the policy. On the FortiClient Console *General* tab, the *Corporate Policy Compliance* section shows the status message, "FortiClient is compliant with corporate policy."

Licensing FortiClient PCs

The FortiClient application's antivirus, antispam, and webfilter features require a license to continue receiving service after the initial evaluation period. This chapter describes how to license multiple FortiClient applications installed in an enterprise environment.

This chapter contains the following sections:

- [Overview of licensing](#)
- [Applying standard fixed licensing](#)
- [Applying enterprise licensing](#)

Overview of licensing

There are two modes of license management for your FortiClient PCs.

Standard Fixed License	The FortiClient application is licensed by means of a license key entered into the application. The license can be a single-user or a volume license. FortiManager does not manage this method of licensing, but it can distribute the license keys.
Enterprise License	The FortiManager unit controls licensing for FortiClient PCs. There are two types of enterprise licensing:
Volume	Instead of distributing a volume license key to your users, you install the license on your FortiManager unit. The license applies automatically to all of your managed FortiClient PCs that do not have a standard fixed license. The volume license has a seat limit which the FortiManager unit enforces.
Redistributable	You obtain a redistributable license from FortiCare and subdivide that license into client licenses for your users. You can set the expiry date and seat count for each client license. The expiry date of your client licenses cannot be later than that of the enterprise license. The total seat count limit of your client licenses can exceed the seat count limit of the enterprise license, but the total number of managed clients cannot. The FortiClient application must be specifically customized for use with redistributable licensing. You can include the client license key in the customized FortiClient installer or provide the license key to users to enter manually.

This chapter describes standard fixed and enterprise licensing. Procedures for configuring licensing on a FortiManager system are based on FortiManager version 4.0, but FortiManager version 3.0 MR7 procedures are very similar.

Applying standard fixed licensing

There are several ways to apply standard fixed licensing:

- Provide the license key to your users to enter into the FortiClient application.
- Create a customized FortiClient installer that includes the license key. Distribute the customized FortiClient installer to your users. The FCRepackager tool -k option enables embedding of a standard fixed license key. For more information, see [“Creating a customized installer using FCRepackager” on page 17](#).
- If you manage FortiClient PCs with a FortiManager unit, you can also manage their licenses. See [“To assign a standard fixed license with FortiManager”](#), next.

To assign a standard fixed license with FortiManager

- 1 Using FortiClient Manager, organize the managed FortiClient PCs into client groups where all members use the same license key.
For more information, see “Working with FortiClient groups” in the FortiClient chapter of the [FortiManager Administration Guide](#).
- 2 In the FortiClient Manager, go to *Manage > FortiClient Key* and select *Add* to add a license key to the FortiManager database.
- 3 In the *License Key* field, enter the license key.
- 4 Optionally, enter a description.
- 5 In the *Available Group(s)* list, select the client groups that use this license key and then select the green right arrow button to move the selected groups to the *Assigned Group(s)* list.
- 6 Select *OK*.
- 7 In the FortiClient *License Key Management* list, select the *Deploy to group* icon for the license key that you added. Select *OK* to confirm your request to deploy.

Applying enterprise licensing

To use enterprise licensing, you need to:

- 1 Obtain an Enterprise License from FortiCare and register it on your FortiManager unit. For more information, see [“Configuring an enterprise license” on page 30](#).
- 2 Create at least one enterprise client license for your FortiClient PCs. For more information, see [“Creating an enterprise client license key” on page 31](#).
- 3 Create a custom FortiClient installer that enables enterprise licensing. You can include the client license key in the installer or provide the client license key to users to apply after installation. For more information, see [“Creating a customized FortiClient installer” on page 31](#).
- 4 Deploy the customized FortiClient installer to your users.

Configuring an enterprise license

You need to register your enterprise license on your FortiManager unit.

To configure the enterprise license

- 1 In the FortiClient Manager, go to *Settings > Enterprise License*.
- 2 In the *License Mode* section, select *Enterprise License*.
- 3 In the *Enterprise License Key* field, enter the license key purchased from FortiCare.
- 4 Select *Download* to register the license. Information about the license displays below the *Enterprise License Key* field.
- 5 In the *Validation Type* section, select *Internal Validation*.
- 6 Select *Apply*.

Creating an enterprise client license key

After you register your enterprise license (see [“Configuring an enterprise license” on page 30](#)), you can create enterprise client licenses for your FortiClient PCs. For each client license, you can set the seat limit. The total number of seats licensed through enterprise client licenses cannot exceed the number of seats that the enterprise license permits.

To create enterprise client license keys

- 1 Go to *Setting > Enterprise License*.
You must have an enterprise license registered on the FortiManager unit. For more information, see [“Configuring an enterprise license” on page 30](#).
- 2 Select the *Enterprise Client License Management* link.
The list of enterprise client licenses is displayed.
- 3 Select *Add*.
The *New Client License* dialog opens, with an enterprise client license key value in place.
- 4 In the *Name* field, enter a name to identify the license.
- 5 In the *Seats Permitted* field, enter a number seats that is no larger than the maximum shown at the right.
- 6 In the *Expiry Date* field, enter a date that is no later than that of the enterprise license.
- 7 Optionally, enter a description.
- 8 Select *OK*.

Deploying the enterprise client license key

An enterprise client license key is effective only on FortiClient installations that are customized to accept an enterprise license instead of a standard fixed license.

You need to create a customized FortiClient installer using the FCRepackager tool, available in the FortiClient .zip installation package. Your customized installer can include the license key, or you can distribute the license key separately to your users.

Creating a customized FortiClient installer

To support enterprise licensing, you must make specific customizations of the installer.

- 1 Create a model FortiClient installation on a PC. For more information, see [“Installing FortiClient for central management” on page 13](#).
If you want to make other customizations in the FortiClient installer, you should make them first, following the procedures in the Customization chapter. See [“Creating a customized installer using FCRepackager” on page 17](#). Then, install the result of those customizations as your model installation.

2 Customize licensing by using the FCRepackager tool with the following command line options:

- -f <FortiManager_IP>, where <FortiManager_IP> is the IP address or fully qualified domain name of the FortiManager unit that will license the FortiClient PC,
- -a <license_model>, where <license_model> is 1 for enterprise client license with FortiManager validation or 2 for enterprise client license with external validation,
- -e <client license key>, where <client license key> is the enterprise client license key created on the FortiManager unit. You can omit this command line option if you prefer to distribute the license key in some other way,
- -m <installer_file>, where <installer_file> is the FortiClient .msi installer file you used to create the model installation.

For example, to customize the FortiClient installer at c:\FortiClient to receive licensing and validation from the FortiManager unit at 172.20.120.161, with client license key 116c2d1ae25f071cc53a013db36040836e, the command is (all on one line):

```
FCRepackager.exe -f 172.20.120.161 -a 1 -  
e 116c2d1ae25f071cc53a013db36040836e -m  
c:\FortiClient\forticlient.msi
```

The customized installer is created in a subdirectory called "transformed", c:\FortiClient\transformed, for example.

Distributing the customized FortiClient installer

You can distribute the customized FortiClient installer in various ways, such as:

- Put the installer on a file share. Users simply double-click the file to begin installation.
- On a Windows Advanced Server network, install the application on end users' computers remotely. For more information, see ["Installing FortiClient using Active Directory Server" on page 15](#).

Enforcing use of FortiClient software

This chapter describes how to enforce the use of FortiClient Endpoint Security software by using a FortiGate unit's Endpoint Control feature.

This chapter contains the following sections:

- [Overview](#)
- [Configuring endpoint control on your FortiGate unit](#)
- [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 Endpoint Security protects the PC on which it is installed.

FortiOS 4.0 Endpoint Control enforces the use of FortiClient End Point Security (Enterprise Edition) in your network. The compliance check ensures that the endpoint is running the most recent version of the FortiClient software and, optionally, checks that the antivirus signatures are up-to-date.

You enable endpoint control in a FortiGate firewall policy. When traffic attempts to pass through the firewall policy, the FortiGate unit runs compliance checks on the originating host on the source interface. Non-compliant endpoints are blocked. If web browsing, they receive a message telling them that they are non-compliant, or they are redirected to a web portal where they can download the FortiClient application installer.



Note: FortiOS 3.0 does not have Endpoint Control, but some FortiGate models support a similar *Check FortiClient is Installed and Running* firewall option. For information about this feature, refer to the 3.0 MR7 version of this [FortiClient Administration Guide](#) or to the 3.0MR7 version of the [FortiGate Administration Guide](#).

Configuring endpoint control on your FortiGate unit

Endpoint control requires that all hosts using the firewall policy have FortiClient Endpoint Security software installed. Make sure that all hosts affected by this policy are able to install this software. Currently, FortiClient Endpoint Security is available for Microsoft Windows 2000 and later only.

To set up endpoint control on your FortiGate unit, you need to

- Enable Central Management by the FortiGuard Analysis & Management Service (FGAMS). This is required if you will use FortiGuard Services to update FortiClient software or antivirus signatures. You do not need to enter account information. See [“Configuring Central Management by FGAMS” on page 34](#).
- Set the minimum required version of FortiClient and configure the source of FortiClient installer downloads for non-compliant endpoints. See [“Setting required FortiClient version and installer download location” on page 34](#).

- Enable endpoint control in the appropriate FortiGate firewall policies. See [“Configuring endpoint control in a FortiGate firewall policy” on page 35](#).



Note: You cannot enable *Endpoint Compliance Check* in firewall policies if the *Redirect HTTP Challenge to a Secure Channel (HTTPS)* option is enabled in *User > Options > Authentication*.

Optionally, you can configure software detection to monitor whether endpoints have specific applications installed. For more information, see the Endpoint control chapter of the [FortiGate Administration Guide](#).

Configuring Central Management by FGAMS

This setting is required if you want to obtain FortiClient software and antivirus updates from FortiGuard Services. No account is required because the central management service is not actually used.

To configure FGAMS central management

- 1 In your FortiGate unit's web-based manager, go to *System > Admin > Central Management*.
- 2 Select *Enable Central Management*.
- 3 Set *Type* to *FortiGuard Analysis & Management Service*.
- 4 Select *Apply*.

Setting required FortiClient version and installer download location

By default, FortiClient software is provided by FortiGuard Services and the latest version is the required version. In your FortiGate unit's web-based manager, go to *Endpoint Control > FortiClient* to view the current settings as well as the latest available versions of FortiClient software and antivirus signatures. There is a warning if FortiGuard service is not available.

To set the required FortiClient version and the download location

- 1 In your FortiGate unit's web-based manager, go to *Endpoint Control > FortiClient* and select the *Customize* link.
The *FortiClient Restriction Configuration* window opens.
- 2 In the *FortiClient Installer Download Location* section, select one of the following options:
 - *FortiGuard Distribution Network* — FortiGuard Services provides the FortiClient software.
 - *This FortiGate* — The FortiGate unit provides a FortiClient installer to download. Not all FortiGate models support storage of FortiClient software. For information about uploading a FortiClient installer to your FortiGate unit, see [“Uploading the FortiClient installer to your FortiGate unit” on page 36](#).
 - *Custom URL* — Specify a URL for a server from which users can download the FortiClient installer. You can use this option to provide a customized FortiClient installer even if your FortiGate unit cannot store FortiClient software.

You need to use either the *This FortiGate* or *Custom URL* option if you want to provide your users a customized version of the FortiClient application. This is required if a FortiManager unit will centrally manage FortiClient applications. For information about customizing the FortiClient application, see [“Installer customization” on page 17](#).

- 3 In the *Minimum FortiClient Version Required* section, select one of the following:
 - *Latest Available* — This is the default if the download location is FortiGuard.
 - FortiClient Enterprise Edition 4.n.n — This is available if the download location is *This FortiGate*. It shows the version of the software stored on the FortiGate unit.
 - *Specify* — If you select this option, enter a version number such as 4.0.2 in the box.
- 4 Select *OK*.

Configuring endpoint control in a FortiGate firewall policy

In a new or existing FortiGate firewall policy, the following options configure the Endpoint Compliance Check:

Figure 3: FortiGate Endpoint Compliance firewall policy options

- Enable Endpoint Compliance Check
 - Enforce FortiClient AV Up-to-date
 - Collect System Information from The Endpoints
 - Redirect Non-conforming Clients to Download Portal

Enable Endpoint Compliance Check	Check that the source hosts of this firewall policy have FortiClient Endpoint Security software installed. Note: Make sure that all of these hosts are capable of installing the software.
Enforce FortiClient AV Up-to-date	Check that the FortiClient Endpoint Security application has the antivirus (real-time protection) feature enabled and is using the latest version of the antivirus signatures available from FortiGuard Services.
Collect System Information from the Endpoints	Collect information about the host computer, its operating system and specific installed applications. This information is displayed in the FortiGate unit web-based manager under <i>Endpoint Control > Endpoints</i> . For more information, See the Endpoint Control chapter of the FortiGate Administration Guide .
Redirect Non-conforming Clients to Download Portal	Non-compliant users see a simple web page, hosted on the FortiGate unit, that explains why they are non-compliant. The page provides links to download a FortiClient application installer or updated antivirus signatures, as needed. If the redirect is not enabled, the non-compliant user simply has no network access.



Note: If the firewall policy involves a load balancing virtual IP, the endpoint compliance check is not performed.

To enable FortiClient checking in a firewall policy

- 1 In the FortiGate web-based manager, 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 *Enable Endpoint Compliance Check*.
- 4 If you want to enforce use of up-to-date antivirus signatures, enable *Enforce FortiClient AV Up-to-date*.
- 5 If you want to enable users to download FortiClient software, select *Redirect Non-conforming Clients to Download Portal*.
- 6 Select *OK*.

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

Uploading the FortiClient installer to your FortiGate unit

If you selected *This FortiGate* as the *FortiClient Installer Download Location*, you need to upload the FortiClient installer to the FortiGate unit.

The FortiClient installer file name must begin with “FortiClientSetup_”, followed by the version number, “4.0.2”, for example. You can upload either a .msi or .exe package.

To upload the FortiClient installer to the FortiGate unit

- 1 Place your installer file on a TFTP server that the FortiGate unit can access.
- 2 Connect to the FortiGate unit’s command line interface (CLI).
You can connect to the CLI through the FortiGate console, using SSH or Telnet (if enabled), or by using the CLI Console window that is part of the web-based manager.

- 3 Enter the following CLI command

```
execute restore forticlient tftp <filename> <server_ip>
```

where <filename> is, for example, `FortiClientSetup_4.0.2.msi`
and <server_ip> is the IP address of the TFTP server.

The TFTP server uploads the file to the FortiGate unit.

For more information about using the CLI, refer to the [FortiGate CLI Reference](#).

You can see the currently stored version of FortiClient software in the System Information section of the FortiGate unit dashboard. To view the dashboard, go to *System > Status*.

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 can be configured on FortiGate units running FortiOS 3.0 and 4.0. This type of VPN is simpler to configure, but FortiOS 3.0 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 Endpoint 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 and 4.0 only)

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

The following procedures are applicable to FortiGate version 4.0, 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 4.0 and 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 (4.0, 3.0)	Enter a descriptive name.
Gateway Name (2.80)	
Remote Gateway	Select <i>Dialup User</i> .
Local Interface (4.0, 3.0)	Select the interface through which clients connect to the FortiGate unit.
Mode	Select <i>Main (ID Protection)</i> .
Authentication Method	Select <i>Pre-shared Key</i> .

Pre-shared Key	Enter the pre-shared key. This must be the same pre-shared key provided to the FortiClient users.
Peer options	Select <i>Accept any peer ID</i> .

To configure phase 2 settings

- 1 FortiOS 4.0 and 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 (4.0, 3.0)	Enter a name for the VPN tunnel.
Tunnel Name (2.80)	
Phase 1 (4.0, 3.0)	Select the gateway name you entered in the Phase 1 configuration.
Remote Gateway (2.80)	
Concentrator (2.80)	Select <i>None</i> .
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 4.0 and 3.0)" on page 39.

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 38.

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 38.
Schedule	Always
Service	Any
Action	IPSEC (4.0, 3.0) Encrypt (2.80)
VPN Tunnel	Select the VPN tunnel you added in “To configure phase 2 settings” on page 38.
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 4.0 and 3.0)

- 1 Go to *System > DHCP > Service*.
- 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 <i>IPSEC</i> .
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 <i>Unlimited</i> 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 4.0 and 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 <i>Dialup User</i> .
Local Interface	Select the interface through which clients connect to the FortiGate unit.
Mode	Select <i>Main (ID Protection)</i> .
Authentication Method	Select <i>Pre-shared Key</i> .
Pre-shared Key	Enter the pre-shared key. This must be the same preshared key provided to the FortiClient users.
Peer option	Select <i>Accept any peer ID</i> .

- 3 Select *Advanced*.
- 4 Select *Enable IPsec Interface Mode*.
- 5 Select *OK*

To configure phase 2 settings

- 1 FortiOS 4.0 and 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.
Advanced	Select to configure the following optional setting.
DHCP-IPsec (4.0)	Select if you provide virtual IP addresses to clients using DHCP. For route-based VPNs, this option is effective only in FortiOS 4.0. For more information, see "To configure an IPsec DHCP server (FortiGate 4.0 and 3.0)" on page 39.

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 4.0 or 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 37 or “[Configuring the FortiGate settings - route-based VPN](#)” on page 40.
- 4 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.

Deploying FortiClient VPN

FortiClient VPN is a lightweight VPN client designed for enterprise deployment. Typically, it provides a connection to the corporate VPN for employees working from home or traveling. You preconfigure the VPN settings before providing the installer file to your users. The user needs only to start the application and select the Connect button.

The following topics are included in this section:

- [Overview](#)
- [Creating configurations in FortiClient VPN](#)
- [Exporting configurations to the FortiClient VPN installer](#)

Overview

Fortinet customers can obtain the FortiClient VPN package from the Fortinet Support web site at <http://support.fortinet.com>. The FortiClient VPN package contains:

- the FortiClient VPN installer file (32-bit and 64-bit) for several locales:

FortiClientVPN_4.0.2.nnnn_en-US.msi	32-bit English
FortiClientVPN_4.0.2.nnnn_x64_en-US.msi	64-bit English
FortiClientVPN_4.0.2.nnnn_fr-FR.msi	32-bit French
FortiClientVPN_4.0.2.nnnn_x64_fr-FR.msi	64-bit French
FortiClientVPN_4.0.2.nnnn_zh-CN.msi	32-bit Simplified Chinese
FortiClientVPN_4.0.2.nnnn_x64_zh-CN.msi	64-bit Simplified Chinese
FortiClientVPN_4.0.2.nnnn_zh-TW.msi	32-bit Traditional Chinese
FortiClientVPN_4.0.2.nnnn_x64_zh-TW.msi	64-bit Traditional Chinese

- a tools folder containing the configuration tool, FortiClientVPNEditor.

Users cannot install the FortiClient VPN application if they have FortiClient Endpoint Security installed. FortiClient Endpoint Security is an upgrade to FortiClient VPN.

The FortiClient VPN Editor can be installed on a computer that has FortiClient Endpoint Security installed. The editor automatically imports your VPN settings.

Creating configurations in FortiClient VPN

The FortiClient VPN Editor can configure or import configurations for VPN tunnels, certificates and revocation lists and then save them to one of the FortiClient VPN installer files or to a configuration file.

To start the FortiClient VPN editor

- 1 Expand the FortiClient VPN package into a folder.
- 2 Go to the tools subfolder.
- 3 Double-click FortiClientVPNEditor.exe.

To provide VPN tunnel definitions to your users, you will need to import or configure the VPN settings in the FortiClient VPN editor.

Importing VPN tunnel settings

If the computer you use to run the FortiClient VPN editor also has the FortiClient application installed on it, the FortiClient tunnel configurations are available in the FortiClient VPN editor. This is convenient if your FortiClient application has the same tunnel configuration that you want to provide to your users.

You can also import tunnel definitions into the FortiClient VPN editor from .vpl or .vpz export files, or from customized FortiClient installer files (.msi).



Note: The .vpz export file contains both the tunnel settings and any certificates the tunnel requires. If possible, import a .vpz file instead of a .vpl file for tunnels that use certificates.

To import VPN tunnel settings

- 1 In the FortiClient VPN editor, select the *Tunnels* tab.
- 2 Select *Import*.
- 3 In the *Open* dialog box, select one of the following file types:
 - a VPN policy package (.vpz)
 - a VPN policy files (.vpl)
 - a customized FortiClient installer file (.msi)
- 4 Select *Open*.

The imported tunnels are listed.

Configuring VPN tunnel settings

If you do not have a source from which to import VPN settings, you can configure a VPN tunnel just as you would in the FortiClient application. Both automatic configuration and manual configuration are supported. Automatic configuration is compatible with a FortiGate remote gateway configured as a VPN policy server. For more information, see the [FortiClient Endpoint Security User Guide](#).

To configure a VPN tunnel - automatic configuration

- 1 In the FortiClient VPN editor, select the *Tunnels* tab.
- 2 Select *New*.
- 3 In the *New Connection* dialog box, enter a connection name.
- 4 For *Configuration*, select *Automatic*.
- 5 For *Policy Server*, enter the IP address or FQDN of the FortiGate gateway.
- 6 Select *OK*.

To configure a VPN tunnel - basic configuration

- 1 In the FortiClient VPN editor, select the *Tunnels* tab.
- 2 Select *New*.
- 3 Enter the following information:

Connection Name	Enter a descriptive name for the connection.
Configuration	Select <i>Manual</i>
Remote Gateway	Enter the IP address or the fully qualified domain name (FQDN) of the remote gateway.

Remote Network	Enter the IP address and netmask of the network behind the FortiGate unit.
Authentication Method	Select <i>Pre-shared Key</i> or <i>X509 Certificate</i> .
Pre-shared Key	Enter the pre-shared key. This is available if <i>Authentication Method</i> is <i>Pre-shared Key</i> .
X509 Certificate	Select the X509 Certificate. The certificate must already be configured. See . This field is available if <i>Authentication Method</i> is <i>X509 Certificate</i> .

- 4 Select *Advanced* if you need to:
 - modify IKE or IPSec settings (see “Configuring IKE and IPSec policies” in the [FortiClient Endpoint Security User Guide](#))
 - configure the FortiClient VPN to use a virtual IP address
 - add the IP addresses of additional networks behind the remote gateway
 - configure Internet browsing over IPSec
 - configure extended authentication (XAUTH)

The *Advanced Settings* dialog box opens. This is the starting point for the rest of the procedures in this section.

To configure the virtual IP address

In the *Advanced Settings* dialog box, do the following:

- 1 Select *Acquire virtual IP address* and then select *Config*.
- 2 In the *Virtual IP Acquisition* dialog box, do one of the following:
 - Select *Dynamic Host Configuration Protocol (DHCP) over IPSec*.
 - Select *Manually Set* and enter the *IP address*, *Subnet Mask*, *DNS Server* and *WINS Server* addresses as required.
- 3 Select *OK*.

To add additional remote networks to a connection

In the *Advanced Settings* dialog box, do the following:

- 1 In the *Remote Network* section, select *Add*.
- 2 In the *Network Editor* dialog box, enter the *IP Address* and *Subnet mask* of the remote network and then select *OK*.
- 3 Repeat Steps 1 and 2 for each additional network that you want to add.
You can specify up to 16 remote networks.
- 4 Select *OK*.

To enable Internet browsing over IPSec

In the *Advanced Settings* dialog box, do the following:

- 1 In the *Remote Network* section, select *Add*.
- 2 Enter *0.0.0.0/0.0.0.0* and select *OK*.
- 3 Select *OK*.

To configure XAuth

In the *Advanced Settings* dialog box, do the following:

- 1 Select the *Config* button for *eXtended Authentication*.
- 2 In the *Extended Authentication* dialog box, select the maximum number of attempts the user can make to enter the correct user name and password.

Automatic XAUTH login is not available for the FortiClient VPN application.

- 3 Select *OK*.

Configuring certificates for FortiClient VPN

Configuring certificates is optional. Many VPN configurations do not use certificates.

If the computer you use to run the FortiClient VPN editor also has the FortiClient application installed on it, FortiClient certificates are available in the FortiClient VPN editor. You can also import certificates.

The FortiClient VPN Editor configures certificates in exactly the same way as the FortiClient application. Only the page names differ.

FortiClient VPN Editor page	FortiClient Endpoint Security page
Certificates	VPN > My Certificates
Certificate Authorities	VPN > CA Certificates
Revocation Lists	VPN > CRL

Refer to the “Managing digital certificates” section in the VPN chapter of the [FortiClient Endpoint Security User Guide](#) for detailed information about working with certificates.

Exporting configurations to the FortiClient VPN installer

When you have finished creating configurations in the FortiClient VPN Editor, you can easily export them to a FortiClient VPN installer. If you configured any certificates, these are also exported.

To export the tunnel configurations

- 1 On the *Tunnels* page, select the *Export* check box for each tunnel configuration that you want to export.
- 2 Select the *Export* button.
The *Save As* dialog box opens.
- 3 In the *Save as type* list, select *Installer Package File (*.msi)*.
- 4 Locate the FortiClient VPN installer file to update with VPN tunnel configurations.
- 5 Select *Save*.

You can also save configurations to a VPN policy file (.vpl) or policy package (.vpz) for distribution to FortiClient Endpoint Security users. The policy package is the preferred format because the file is password protected and it includes any certificates that the tunnel requires.

Using the FortiClient API

You can operate FortiClient VPNs using the COM-based FortiClient API.

This chapter contains the following sections:

- [Overview](#)
- [Controlling a VPN](#)
- [Setting and monitoring a security policy](#)
- [API reference](#)

Overview

The FortiClient COM library provides functionality to:

- Retrieve a list of the VPN tunnels configured in the FortiClient application.
- Start and stop any of the configured VPN tunnels.
- Send XAuth credentials.
- Set the security policy for the FortiClient VPN.
- Retrieve status information:
 - configured tunnel list
 - active tunnel name
 - connected or not
 - idle or not
 - remaining key life
 - current security policy
- Respond to FortiClient-related events:
 - VPN connect
 - VPN disconnect
 - VPN is idle
 - no longer in compliance with security policy
 - XAuth authentication requested

Controlling a VPN

This section uses example code snippets in Visual Basic to show how to operate a VPN tunnel programmatically.

Linking to the COM library

The COM library for FortiClient is `fccomintdll.dll`, located in the FortiClient installation directory, by default `c:\Program Files\Fortinet\FortiClient`. Using your development environment, create a reference to this library.

```
Begin FCCOMINTDLLLibCtl.VPN VPN1
```

This creates VPN1 as the FortiClient object.

Depending on your development environment, you might also need a type library file. You can find the file FCCOMIntDLL.tlb in the FortiClient .zip installation package.

Retrieving a list of VPN connection names

If needed, you can obtain a list of the VPN connections configured in the FortiClient application. The GetTunnelList function returns an array of the names.

```
tunnelList = VPN1.GetTunnelList
```

Typically, an application might put the tunnel names into a list from which the user chooses the required tunnel name. In this example, the list control List1 is populated with the tunnel names:

```
List1.Clear
For i = LBound(tunnelList) To UBound(tunnelList)
    List1.AddItem (tunnelList(i))
Next
```

Opening the VPN tunnel

Use the Connect method to establish the tunnel. The only parameter is the tunnel name, as configured in the FortiClient application. In this example, the tunnel name is "Office":

```
VPN1.Connect "Office"
```

Responding to XAuth requests

If the VPN peer requires you to supply XAuth credentials, you can easily provide for this by writing code that responds to the On XAuthRequest event. In this example, a small dialog box opens in which the user enters the user name and password.

```
Private Sub VPN1_OnXAuthRequest(ByVal bstrTunnelName As String)
    Dialog.Show 1

    outUserName = ""
    outPassword = ""
    outSavePassword = False

    If Not Dialog.Cancelled Then
        outUserName = Dialog.UserName
        outPassword = Dialog.Password
        outSavePassword = Dialog.SavePassword
    End If

    VPN1.SendXAuthResponse bstrTunnelName, outUserName,
        outPassword, outSavePassword
End Sub
```

Monitoring the connection

There are both function-based and event-based ways to monitor the VPN connection.

Events

The FortiClient API includes event calls for which you write appropriate code. Using events, you can provide live status information for users. This example shows how an application could respond to the OnConnect and OnDisconnect events by updating a user interface display. A checkbox, ConnectCheck, is selected when the VPN connects and cleared when the VPN disconnects.

```
Private Sub VPN1_OnConnect(ByVal bstrTunnelName As String)
    ConnectCheck.Value = 1
    textName = bstrTunnelName
End Sub

Private Sub VPN1_OnDisconnect(ByVal bstrTunnelName As String)
    ConnectCheck.Value = 0
    textName = bstrTunnelName
End Sub
```

There is also an OnIdle event.

Functions

At any time, you can programmatically determine which VPN connection is active using the GetActiveTunnel function, like this:

```
TunnelName = VPN1.GetActiveTunnel
```

The returned string is empty if no VPN tunnel is up.

The boolean function IsConnected returns True if the named connection is up, like this:

```
If IsConnected("Office") Then
    Rem perform functions requiring Office VPN
    ....
End If
```

There is also an IsIdle function.

Setting and monitoring a security policy

Starting with v3.0 MR7, the FortiClient application can enforce a security policy. Users cannot use a VPN connection unless the FortiClient settings comply with the policy. The security policy can require that any or all of the following features are enabled:

- Antivirus (real-time protection)
- Antispam
- Firewall (Normal mode)
- Web Filter

This is usually applied in an enterprise environment to provide security when users connect to the corporate network through a VPN. A FortiManager unit can deploy the security policy to FortiClient PCs.

The FortiClient API can also create a security policy. This section uses example code snippets in Visual Basic to show how to set and monitor a corporate security policy programmatically.

Setting a security policy

The SetPolicy method passes four boolean values, one for each feature: antivirus, antispam, firewall, and web filter. If the value is True, the policy requires that the feature is enabled. It is quite easy to create a check box for each of the boolean values and call SetPolicy in response to the user selecting a “Set Policy” button.

In this example, check boxes are named for the features (AVcheck for the antivirus check box, for example) and the “Set Policy” button is named SetSecPolicy.

```
Private Sub SetSecPolicy_Click()
    VPN1.SetPolicy AVcheck.Value, AScheck.Value, FWcheck.Value,
        WFcheck.Value
```

The FortiClient application receives the policy but does not change any settings. The FortiClient General tab and system tray menu show the option “Make compliant with corporate policy”.

If you want to programmatically make the FortiClient settings comply with the policy you set, you must use the MakeSystemPolicyCompliant method.

Reading a security policy

You can retrieve the security policy from the FortiClient application with the GetPolicy method. This returns four boolean values, one for each feature: antivirus, antispam, firewall, and web filter. If the value is True, the policy requires that the feature is enabled. If all four values are False, there is no security policy.

This example uses the returned boolean values to set check boxes named for the features (AVcheck for the antivirus check box, for example).

```
VPN1.GetPolicy a, b, c, d
AVcheck.Value = Int(a)
If b Then
    AScheck.Value = 1
Else
    AScheck.Value = 0
End If
If c Then
    FWcheck.Value = 1
Else
    FWcheck.Value = 0
End If
If d Then
    WFcheck.Value = 1
Else
    WFcheck.Value = 0
End If
```

The check boxes show the state of each feature in the policy. You could then make changes to the policy and set them using the SetPolicy method, as shown in [“Setting a security policy” on page 50](#).

Monitoring policy compliance

The FortiClient API includes event calls for which you write appropriate code. Using events, you can provide live status information for users. The OnOutOfCompliance event returns four boolean values, one for each feature. A value of True indicates that the feature is not in compliance with the policy.

This example shows how an application could respond to the OnOutOfCompliance event. A dialog box opens that lists the out-of-compliance features.

```
Private Sub VPN1_OnOutOfCompliance(ByVal bAV As Boolean, ByVal
    bAS As Boolean, ByVal bFW As Boolean, ByVal bWF As Boolean)

    OOCDialog.Show 1
    OOCDialog.Text = ""
    If bAV Then
        OOCDialog.Text = OOCDialog.Text + "Antivirus\n"
    End If
    If bAS Then
        OOCDialog.Text = OOCDialog.Text + "Antispam\n"
    End If
    If bFW Then
        OOCDialog.Text = OOCDialog.Text + "Firewall\n"
    End If
    If bWF Then
        OOCDialog.Text = OOCDialog.Text + "Web Filter"
    End If
End Sub
```

Making the FortiClient application comply with the policy

The FortiClient API includes a method that enables the features required by the security policy, bringing the application back into compliance. In this example, there is a “Make Compliant” button.

```
Private Sub MakeCompliantBtn_Click()
    VPN1.MakeSystemPolicyCompliant
End Sub
```

API reference

Table 2: Methods

Connect(bstrTunnelName As String)	Open the named VPN tunnel. This connection must already be configured in your FortiClient application.
Disconnect(bstrTunnelName As String)	Close the named VPN tunnel.
GetPolicy (pbAV As Boolean, pbAS As Boolean, pbFW As Boolean, pbWF As Boolean)	Retrieve security policy settings for Antivirus AntiSpam Firewall Web Filter True means feature must be enabled.
GetRemainingKeyLife (bstrTunnelName As String, pSecs As Long, pKBytes As Long)	Retrieve the remaining key life for the named connection. Whether keylife time (pSecs) or data (pKBytes) are significant depends on the detailed settings in the FortiClient application.
MakeSystemPolicyCompliant()	Apply the security policy defined by SetPolicy.
SendXAuthResponse (tunnelName As String, userName As String, password As String, savePassword As Boolean)	Send XAuth credentials for the named connection: User name Password True if password should be saved.
SetPolicy (bAV As Boolean, bAS As Boolean, bFW As Boolean, bWF As Boolean)	Set security policy settings for Antivirus AntiSpam Firewall Web Filter True means feature must be enabled.

Table 3: Functions

GetActiveTunnel() As String	Retrieve the name of the active connection.
GetTunnelList()	Retrieve the list of all connections configured in the FortiClient application.
IsConnected (bstrTunnelName As String) As Boolean	Return True if the named connection is up.
IsIdle(bstrTunnelName As String) As Boolean	Return True if the named connection is idle.

Table 4: Events

OnConnect(bstrTunnelName As String)	Connection established.
OnDisconnect(bstrTunnelName As String)	Connection disconnected.
OnIdle(bstrTunnelName As String)	Connection idle.
OnOutOfCompliance(bAV As Boolean, bAS As Boolean, bFW As Boolean, bWF As Boolean)	FortiClient has gone out of compliance with security policy. Arguments correspond to features. True indicates the feature is out of compliance with security policy.
OnXAuthRequest(bstrTunnelName As String)	The VPN peer on the named connection requests XAuth authentication.

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.



Note: The instructions in this chapter are based on FortiManager 4.0. There are minor changes in menu names since version 3.0. If you want to see per-user web filtering instructions for FortiManager 3.0, refer to the version 3.0 MR7 [FortiClient Administration Guide](#).

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 Endpoint 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 4.0 Endpoint 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 16.

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 13](#) 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 know the password configured on the FortiManager unit.

To set FortiClient Manager options

- 1 In the FortiClient Manager, go to *Settings > System > System 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.
If you want to apply lockdown to existing clients, select *Apply Lockdown Setting to All*.
- 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 new 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 > Client* and select *Search/Add New*.
- 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 *Global Configuration > 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 <i>Add</i> . To remove a URL, select it in the list and then select <i>Delete</i> .
Select category to block	Either select <i>Select All</i> or select individual categories to block. You can expand the categories to select specific sub-categories.
Select classification to block	Either select <i>Select All</i> 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 *Settings > LDAP Group/User > LDAP Settings* 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 *Settings > LDAP Group/User > LDAP Group/User*.
- 2 From the *LDAP Server* list, select the Windows AD domain controller.
- 3 Select *Synchronize*.
- 4 Expand domains as needed to show groups.
- 5 From the *Web Filter Profile* list, select the profile you want to assign.

- 6 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.
- 7 Repeat Step 4 through Step 6 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 > LDAP Group/User*.
- 2 From the *LDAP Server* list, select the Windows AD domain controller.
- 3 Select *Synchronize*.
- 4 Select *LDAP Users* at the top left of the page.
- 5 From the *Domain* list, select the required domain.
- 6 From the *Web Filter Profile* list, select the profile you want to assign.
- 7 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*.
- 8 Select *Assign Profile*.
For each selected user, the *Web Filter Profile* column lists the assigned profile.
- 9 Repeat Step 6 through Step 8 for each web filter profile you want to assign.

Index

A

- auto discovery
 - enabling, 24
- AV update schedule randomizing, 20

B

- block access unless firewall rule permits
 - installation option, 19

C

- central management
 - installing FortiClient for, 13
- cloned disk image
 - including FortiClient, 15
- cloned PC hardware
 - install with USESWUID option, 16
- code page, 8
- comments on Fortinet technical documentation, 9
- customer service, 9
- customization of FortiClient installer, 17
 - changing installer language, 20
 - deploying, 21
 - for enterprise licensing, 31
 - overview, 17
 - using FCRepackager, 17
 - using MSI editor, 21

D

- disable XAUTH password saving
 - installation option, 19
- disabling web filter rating by IP addresses
 - installation option, 19
- documentation, 8

F

- FCRepackager
 - using to create customized installer, 17
- FDS servers, fallback to public servers, 18
- FortiClient packages, 11
 - uploading to FortiGate unit, 36
- FortiClient PCs
 - adding to FortiManager database, 54
- FortiGate models
 - supported by FortiClient, 8
- FortiGate unit
 - configuring - policy-based VPN, 37
 - configuring - route-based VPN, 40
- FortiManager
 - adding FortiClient PCs, 54
 - configuring for FortiClient web filtering, 54
 - configuring web filter profiles, 55
 - FortiClient Manager options, 54

- Fortinet customer service, 9
- Fortinet Knowledge Center, 9
- FortiOS versions
 - supported by FortiClient, 8
- FortiTray
 - installation option to hide, 18

H

- hide FortiTray
 - installation option, 18

I

- installation options
 - block access unless firewall rule permits, 19
 - disable web filter rating by IP address, 19
 - disable XAUTH password saving, 19
 - hide FortiTray, 18
 - permit fallback to public FDS, 18
- installation packages, 11
- installing, 11
 - as part of a cloned disk image, 15
 - creating customized installer, 17
 - on cloned PC hardware, 16
 - setting to request FortiManager registration, 54
 - using Active Directory server, 15
- introduction, 7

L

- language support, 8
- LDAP
 - for Windows user and group information, 55
- license
 - creating a client license key, 31
 - enterprise license, 29
 - enterprise license, applying, 30
 - enterprise license, registering, 30
 - redistributable enterprise license, 29
 - standard fixed license, 29
 - standard fixed license, applying, 29
 - volume license, 29
- license key
 - specifying in FCRepackager customization, 20
 - specifying in MSI customization, 23
- lockdown
 - enabling in FCRepackager customization, 20
 - enabling in MSI customization, 24

M

- MSI installation file
 - creating, 20
 - shrinking, 20

P

- per-user web filtering
 - assigning profiles, 55
 - configuring FortiManager for, 54
 - overview, 53
 - remote users, 53
 - Windows network, 53
- policy server
 - configuring FortiGate unit as, 41

R

- remote management
 - enabling in MSI customization, 23
- RemoveFCTID.exe, 15
- removing identifier, 15

S

- sample installation
 - for customization, 18
- security policy
 - for FortiClient PCs, setting, 28
- software packages, FortiClient, 11
- system requirements, 7

T

- technical support, 9

U

- USESUID installation option, 16

V

- VPN XAUTH passwords
 - installation option to disable saving, 19
- VPN, policy-based
 - configuring on FortiGate unit, 37
- VPN, route-based
 - configuring on FortiGate unit, 40

W

- web filter
 - disabling rating of IP addresses, 19
- web filter profiles
 - assigning to groups and users, 55
 - defining in FortiClient Manager, 55
- web filtering
 - assigning profiles, 55
 - configuring FortiManager for, 54
 - on Citrix server, 53
 - on Windows Terminal server, 53
 - overview, 53
 - remote users, 53
 - Windows network, 53

X

- XAuth
 - disabling password saving, 23

FORTINET®

www.fortinet.com

FORTINET®

www.fortinet.com