



Administration Guide

FortiClient Host Security Version 3.0 MR5

FORTINET™

www.fortinet.com

FortiClient Host Security Administration Guide
Version 3.0 MR5
18 May 2007
04-30005-0400-20070518

© Copyright 2007 Fortinet, Inc. All rights reserved. No part of this publication including text, examples, diagrams or illustrations may be reproduced, transmitted, or translated in any form or by any means, electronic, mechanical, manual, optical or otherwise, for any purpose, without prior written permission of Fortinet, Inc.

Trademarks

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

Contents

Introduction	5
About FortiClient Host Security	5
System requirements	5
Supported FortiGate models and FortiOS versions	6
Language Support.....	6
About this Guide.....	6
Documentation.....	6
Fortinet documentation CD	6
Fortinet Knowledge Center	6
Comments on Fortinet technical documentation.....	7
Customer service and technical support	7
Installation	9
FortiClient software packages.....	9
Overview of installer customization	9
Creating a customized installer using FCRepackager.....	10
Creating the sample installation	10
Creating the custom MSI installation file	11
Deploying the customized FortiClient application	11
Customizing the installer using an MSI editor.....	12
Creating a FortiClient custom installation.....	12
Disabling VPN XAuth password saving	14
Enabling Remote Management with FortiManager	14
Locking Down the User Interface	15
Permitting fallback to public FDS servers	16
Specifying install log file	16
Language transforms	16
Specifying multiple transforms on the command line.....	16
Installing FortiClient using Active Directory Server.....	17
Installing FortiClient as part of a cloned disk image.....	17
Configuring FortiGate VPNs for FortiClient PCs.....	19
Configuring the FortiGate settings - policy-based VPN.....	19
Configuring the FortiGate settings - route-based VPN	22
Configuring the FortiGate gateway as a policy server.....	23
Index	25

Introduction

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

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

About FortiClient Host Security

The FortiClient Host Security software is a secure remote access client for Windows computers. It integrates IPSec VPN, antivirus, Windows registry monitoring, firewall, and web browsing control into a single software package.

With the FortiClient software, you can:

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

System requirements

To install FortiClient 3.0 you need:

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



Note: The FortiClient software installs a virtual network adapter.

Supported FortiGate models and FortiOS versions

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

Language Support

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

- English
- Simplified Chinese
- Japanese
- Korean

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 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.
- [Configuring FortiGate VPNs for FortiClient PCs](#) describes how to configure VPNs on FortiGate units to work with the VPN client feature of FortiClient Host Security.

Documentation

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

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

Fortinet documentation CD

All Fortinet documentation is available from the Fortinet documentation CD shipped with your Fortinet product. The documents on this CD are current at shipping time. For up-to-date versions of Fortinet documentation see the Fortinet Knowledge Center.

Fortinet Knowledge Center

The most recent Fortinet technical documentation is available from the Fortinet Knowledge Center. The knowledge center contains short how-to articles, FAQs, technical notes, product and feature guides, and much 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 how to create a custom MSI package for FortiClient Host Security that you can deploy to your users. The customized installation can include the necessary configuration for central management by a FortiManager system.

This chapter contains the following sections:

- [FortiClient software packages](#)
- [Overview of installer customization](#)
- [Creating a customized installer using FCRepackager](#)
- [Customizing the installer using an MSI editor](#)
- [Installing FortiClient using Active Directory Server](#)
- [Specifying install log file](#)

FortiClient software packages

Fortinet provides two installation packages for FortiClient software:

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

The Windows executable file provides easy installation on a single computer where the FortiClient application will not be managed by a FortiManager system. Nothing can be customized prior to installation. The *FortiClient Host Security User Guide* provides information about using this installer.

The MSI installer in the .zip file package is customizable for a larger roll-out to many computers in an organization. This procedures in this chapter use the .zip file package exclusively. You can deploy the customized MSI installer to your users and they can install it following the simple instructions in the *FortiClient Host Security User Guide*.

You can preconfigure all application settings, including the configuration for centralized management by a FortiManager system.

Overview of installer customization

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

Creating a customized installer using FCRepackager

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

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

Creating the sample installation

You need to create a sample installation on a computer running one of the supported operating systems. See [“System requirements” on page 5](#). The computer should not already have the FortiClient application installed.

To perform the sample installation of the FortiClient software

- 1 Expand the FortiClient Host Security installer .zip package into a new folder.
- 2 From the folder where you expanded the .zip package, install the FortiClient application using one of following command lines:
 - if FortiClient applications will not be centrally managed,


```
msiexec /i FortiClient.msi
```
 - if FortiClient applications will be centrally managed by FortiManager server


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

<IP> is an address or addresses that FortiClient trusts for remote management. It can be a single IP address like 10.16.90.83, a subnet like 10.18.2.0/255.255.255.0 or a range like 10.16.3.1-172.16.3.50.

You can enter multiple <IP> values separated by commas.

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. For more information, see “To configure the FortiClient software after the system reboot” in the Installation chapter of the *FortiClient Host Security User Guide*.
- 4 Configure the sample installation as you want the FortiClient application to be configured on your user's computers.

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

Creating the custom MSI installation file

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

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

Table 1: FCRepackager options

Specify license key	-k <license_key>
Lock down program for FortiManager. Specify the plain text password.	-L <lockdown_password>
Set random AV update time (MR5 or later) between specified hours. The sample installation must contain an update schedule.	-s <start_hour>-<end_hour>

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

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

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

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

Deploying the customized FortiClient application

You can distribute your new FortiClient.msi file to users. Users simply double-click the file to begin installation. On a Windows Advanced Server network, you can install the application on end users' computers remotely. See ["Installing FortiClient using Active Directory Server" on page 17](#).

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

Customizing the installer using an MSI editor

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



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

The following components were created specifically for modifying FortiClient installations:

- REGISTRY_MST_FWSettings
- REGISTRY_MST_AVSettings
- REGISTRY_MST_VPNSettings
- REGISTRY_MST_WEBFILTERSettings
- REGISTRY_MST_ANTISPAMSettings

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

The following rules MUST be followed:

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

Creating a FortiClient custom installation

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

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



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

To create and test a custom FortiClient installation

- 1 Make a copy of the FortiClient.msi file and rename the copy (i.e. "target.msi").
- 2 Open "target.msi" with an MSI editor and add your modifications to it.
- 3 Save the changes you made to the "target.msi" file and close the file.
- 4 With your MSI editor, make a transform file (*.mst)
 - The base package must be FortiClient.msi.
 - The target package must be target.msi.
 - Give the .mst file a suitable name. We suggest you include the version of FortiClient that was used to create the transform. For example, custom_3.0.mst.

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

```
msiexec /i <path to package>FortiClient.msi  
TRANSFORMS=custom_3.0.mst /L*v c:\log.txt
```

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

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

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

- 6 Test FortiClient to make sure the modifications you made are present and correct. If there are any mistakes, use your editor to make changes to the .mst file.
- 7 Test uninstalling the FortiClient software. It is critical that you do this before you roll out FortiClient to your network. The uninstall must complete without an error or rollback occurring.
- 8 Roll out your custom FortiClient installation specifying the transform file.

Suppressing Features

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

Adding a license key

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

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

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

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

Disabling VPN XAuth password saving

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

To disable the VPN XAuth password saving

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

Enabling Remote Management with FortiManager

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

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

To enable remote management

- 1 Create a new, or edit an existing, MSI transform file.
- 2 Open the Property table and change the value of FMGREENABLED 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	10.16.90.83	(trust a single ip only)
TRUSTEDIPS	10.18.2.0/255.255.255.0	(trust a subnet)
TRUSTEDIPS	10.16.3.1-172.16.3.50	(trust an ip range)
TRUSTEDIPS	10.16.90.83,172.18.2.0/255.255.255.0,172.16.3.1-10.16.3.50	(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
FMGREENABLED=1 FMGTRUSTEDIPS=<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 FMGRTRUSTEDIPS so that it specifies the IP address(es) of FortiManager(s) that FortiClient will accept commands from.

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

- 4 Change the property FMGRENABLEDISCOVER 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.

Permitting fallback to public FDS servers

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

To permit fallback use of public FDS servers

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

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 installers user interface:

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

Specifying multiple transforms on the command line

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

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

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

Installing FortiClient as part of a cloned disk image

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

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

To include a FortiClient installation in a hard disk image

- 1 Obtain the .zip file version of the FortiClient installer.
- 2 Install and configure the FortiClient application to suit your requirements.
See [“Creating the sample installation” on page 10](#).
- 3 Right-click the FortiClient icon in the system tray and select Shutdown FortiClient.
- 4 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.

- 5 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.

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

Configuring FortiGate VPNs for FortiClient PCs

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

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

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

Configuring the FortiGate settings - policy-based VPN

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

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

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

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

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

To configure phase 1 settings

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

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

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

To configure phase 2 settings

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

Name (3.0)	Enter a name for the VPN tunnel.
Tunnel Name (2.80)	
Phase 1 (3.0)	Select the gateway name you entered in the Phase 1 configuration.
Remote Gateway (2.80)	
Concentrator (2.80)	Select None.
Advanced	Select to configure the following optional setting.
DHCP-IPsec	Select if you provide virtual IP addresses to clients using DHCP. For more information, see "To configure an IPsec DHCP server (FortiGate 3.0)" on page 21.

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 20.

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 20.](#)

Schedule Always

Service Any

Action IPSEC (3.0)
 Encrypt (2.80)

VPN Tunnel Select the VPN tunnel you added in [“To configure phase 2 settings” on page 20.](#)

Allow Inbound Enable

Allow Outbound Enable

Inbound NAT Enable

Outbound NAT Disable

Protection Profile Optional

Log Traffic Optional

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

To configure an IPsec DHCP server (FortiGate 3.0)

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

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

Configuring the FortiGate settings - route-based VPN

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

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

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

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

To configure phase 1 settings

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

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

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

To configure phase 2 settings

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

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

To add a firewall policy

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

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

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

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

Configuring the FortiGate gateway as a policy server

You can configure a FortiGate version 3.0 gateway to work as a VPN policy server for FortiClient automatic configuration. When the FortiClient users connect to the FortiGate gateway to download the VPN policies, they are challenged for user names and passwords. 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 19.
- 4 Create a firewall policy for the dialup VPN. See [“To add a firewall policy”](#) on page 20.
- 5 Connect to the FortiGate unit CLI and configure VPN policy distribution as follows:

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

<phase2_name> must be the name of the VPN phase 2 configuration.

<group_name> must be the name of the user group your created for FortiClient users.

Index

A

- auto discovery
 - enabling 15
- AV update schedule randomizing 11

C

- cloned disk image including FortiClient 17
- code page 6
- comments on Fortinet technical documentation 7
- customer service 7
- customization
 - deploying 11
 - overview 9
 - using an MSI editor 12
 - using FCRepackager 10

D

- documentation 6

F

- FortiClient packages 9
- FortiGate models
 - supported by FortiClient 6
- FortiGate unit
 - configuring - policy-based VPN 19
 - configuring - route-based VPN 22
- Fortinet customer service 7
- FortiOS versions
 - supported by FortiClient 6

I

- install
 - using Active Directory server 17
- installation 9
- introduction 5

L

- language support 6
- license key
 - specifying in FCRepackager customization 11
 - specifying in MSI customization 13
- lockdown
 - enabling in FCRepackager customization 11
 - enabling in MSI customization 15

P

- policy server
 - configuring FortiGate unit as 23

R

- remote management
 - enabling in FCRepackager customization 10
 - enabling in MSI customization 14
- RemoveFCTID.exe 17
- removing identifier 17

S

- software packages, FortiClient 9
- system requirements 5

T

- technical support 7

V

- VPN, policy-based
 - configuring on FortiGate unit 19
- VPN, route-based
 - configuring on FortiGate unit 22

X

- XAuth
 - disabling password saving 14

FORTINET™

www.fortinet.com

FORTINET™

www.fortinet.com