QuickStart Guide

About FortiClient

FortiClient Endpoint Security is a unified security agent for Windows computers that integrates personal firewall, VPN, antivirus, anti-spyware, anti-spam, and web content filtering into a single software package. FortiClient has a sophisticated, user-friendly interface that allows for quickly setting up protection for your computer.

VPN allows secure access to enterprise applications from remote locations

WAN Optimization works with FortiGate units to accelerate network access

Antivirus protects you from malicious software

Firewall blocks outsiders from hacking into your computer

Web Filtering blocks malicious websites and enforces parental controls

Anti-spam detects, quarantines, and blocks spam messages and malicious attachments

App Detection works with FortiGate units to monitor and control which applications can run on an endpoint computer

		Porticilent Console				
	General	FORTICUE	inn.		77000	
	Chalma	🟦 General	General: Status		0	
	Status	Status	FortiClient Version: 4.0.29.118	Serial No.	FCT100000078232	
	Connection	Connection Update	100	Expiry Date	November-13-89	
	Update	Backup/Restore	No active connection			
	Backup/Restore	Log View Log Settings	Antivirus			
	Log View	Help & Support	Enable real-time protection Virus Signatures Version: 10.762 AntiVirus Engin	Enable startup list mor e: 4.0.9	itoring	
	Log Settings		Spyware Signatures Version: 1.211 Ant/Spyware Er	ngine: 1.0.8		
	Help & Support	WAN Optimization	Last scan August-26-091:57:06 PM			
		IntiVirus	Automatic update: scheduled at 13:49 every day			
V	VPN	🧱 Firewall	Last successful update: August-26-09 1:57:03 PM			
	WAN Optimization	Sy WebFilter				
J		🚳 AntiSpam				
۲	Anti∀irus	Kar App Detection				
× 1)	Firowall		Show FattClient console when I lagon into Windows			
ST AL	T II C W CII	ANNA STATE			Lock Settings	
T	WebFilter		Copyright © 2003-2009, Forlinet Inc. www.forlinet.cc			
SPAM	AntiSpam					
-	App Detection					

Installing FortiClient

FortiClient is installed interactively on the computer using the Installation Wizard. To install FortiClient on your Windows computer, run the *.exe or *.msi file after downloading it from the Fortinet website.

After the dowload completes, double-click on the installer file to run it.

- 1. In the FortiClient Setup screen, select the **FortiClient SSL VPN** check box to install it.
- 2. At the Welcome screen, click **Next**. It is recommended that you close all running applications before proceeding with the installation.
- At the Choose Installation Type screen, select the Free Edition or the Premium Edition. If you are installing the Premium Edition, enter the license key the field provided. Click Next.
- 4. At the End-User License Agreement screen, select the "I accept the terms of the License Agreement" check box and click Next.
- 5. In the Choose Setup Type screen, select one of the following:
 - **Complete** All features of FortiClient are installed.
 - VPN and Firewall Installs only VPN and Firewall features.
 - Custom Choose the features to install and file location. Recommended for advanced users.
- 6. Click **Install** to begin the installation. During installation, your network connections may be temporarily disconnected.
- 7. At the Completed page, click Finish.
- 8. When the installation is complete, the **FortiClient Configuration Wizard** opens. Use the wizard to schedule, update, and start an antivirus scan.

Anti-Virus Scan

To run a quick scan

- 1. Go to **AntiVirus > Scan** and click **Quick Scan**. The Antivirus Scanning window opens, displaying the scanning process and results.
- 2. The Infected file list displays the names of any infected files. Right-click on entries and choose from the following actions: delete the file, quarantine the file, submit virus to Fortinet, or submit as false positive to Fortinet.

To update anti-virus definitions

- 1. Go to **General > Update**.
- 2. Click Update Now.

Under Update Status, you can view the update process and results. A status of "No update available" means that your antivirus definitions and antivirus engine are running the latest version.



Use this server to update:				UID: 2860874
Component	Version	Expiry Date	Last Update	Update Status
AntiVirus Signatures	10.756	13/11/2009		
AntiVirus Extended Signat	10.420	13/11/2009		
AntiVirus Engine	4.0.9	13/11/2009		
AntiSpyware Signatures	1.210	13/11/2009		
AntiSpyware Engine	1.0.8	13/11/2009		
AntiSpam Engine	1.1.8	13/11/2009	26/08/2009 1:32:39 PM	No data/engine upd
Daily at 13:	49	*	🔘 Every 4 🚔 hour(s)	
when a new version of Forti	Client is ava	ilable:		
Download and install the	e new versio	n without notifica	tion.	
Download the new vers	ion and noti	iv me before insta	lina	
🔿 Matifu ma bafara daumla	adina or ina	talling the new ve	reion	
O Rolly the before downle	during of into	carring the new ve	raiden.	

VPN

To create an SSL VPN connection

- 1. Go to **VPN > Connections**.
- 2. Click Advanced and select Add.
- 3. In the New Connection window, enter the Connection Name.
- 4. Select the SSL VPN type.
- 5. Enter the IP address or the fully qualified domain name (FQDN) of the remote gateway.
- 6. Enter the Username and Password for the remote gateway.
- 7. Click **OK**.

To create a manual IPSEC connection

- 1. Go to VPN > Connections
- 2. Click Advanced and select Add.
- 3. In the New Connection window, enter enter the Connection Name.
- 4. Select the Automatic IPSEC VPN type.
- 5. For **Policy Server**, enter the IP address or FQDN of the FortiGate gateway.
- 6. Click **OK**.

To create an automatic IPSEC connection

- 1. Go to VPN > Connections.
- 2. Click Advanced and select Add.
- 3. In the New Connection window, enter the Connection Name.
- 4. Select the Manual IPSEC VPN type.
- 5. Enter the IP address or the fully qualified domain name (FQDN) of the remote gateway.
- 6. Enter the IP address and netmask of the network behind the FortiGate unit.
- 7. Select the Authentication Method.
- 8. Enter the Preshared Key.
- 9. Click OK.

Firewall Protection

To select a firewall mode

By default, FortiClient firewall runs in Normal mode to protect your system. Go to **Firewall** > **Status** to select a firewall mode (protection level):

- Deny all Blocks all the incoming and outgoing traffic.
- Normal You can select from the three protection profiles:
 - Basic home use Allows all outgoing traffic and denies all incoming traffic. Select this profile if your PC is a standalone home computer and not connected to other networks or PCs.
 - Basic business Allows all outgoing traffic, allows all incoming traffic from the trusted zone, and denies all incoming traffic from the public zone.
 - Custom profile The Custom profile allows you to configure the application level permissions, network zone permissions, and advanced firewall filtering rules. This is the default profile.
- Pass all No firewall protection.

To customize security settings

For the public and trusted zones, you can use the default high, medium, or low level security settings. Go to **Firewall > Network** to customize the security levels.

- High By default, incoming connections are allowed only if there are listening ports for these connections.
- **Medium** By default, most connections are allowed unless you customize the settings. Note that the default medium security level settings for public and trusted zones are different:
 - · For public zone, the incoming ICMP and NetBIOS packets are blocked.
 - · For trusted zone, these packets are allowed.
 - · Low Packet level rule is disabled and application level control is on.
- Low Packet level rule is disabled and application level control is on.



E C RTINET

Firewall: St

Firewall Mode

O Deny all

Normal

Pass al

5 hours

Inbound traffic (packets)

Blocked network packets

V Disable taskbar notification for blocked network traffic

V Current connections

Network statistics

Profile

Basic home use

Default profile. Firewall can be fully customized.

Basic busines:

5 minutes

Custom profile

Outbound traffic (packets)

Blocked application requests

View Connections

100

© Copyright 2009 Fortinet Incorporated. All rights reserved. Products mentioned in this document are trademarks or registered trademarks of their respective holders. Regulatory Compliance FCC Class B Part 15 CSA/CUS

4 Jun 2009



Visit these links for more information and documentation for your Fortinet product:

Technical Documentation - http://docs.forticare.com Training Services - http://campus.training.fortinet.com Fortinet Technical Support - http://support.fortinet.com Fortinet Knowledge Center - http://kb.forticare.com