FortiClient - Administration Guide

Version 6.2.5

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

June 04, 2020
FortiClient 6.2.5 Administration Guide
04-625-546492-20200604

TABLE OF CONTENTS

Introduction

FortiClient is an all-in-one comprehensive endpoint security solution that extends the power of Fortinet's Advanced Threat Protection (ATP) to end user devices. As the endpoint is the ultimate destination for malware that is seeking credentials, network access, and sensitive information, ensuring that your endpoint security combines strong prevention with detection and mitigation is critical.

This document is written for FortiClient (Windows) 6.2.5. FortiClient (macOS) 6.2.5 does not support all features that this document describes.

FortiClient, FortiClient EMS, and FortiGate

FortiClient connects to EMS or EMS and FortiGate. You apply FortiClient licensing to EMS.

When you connect FortiClient only to EMS, EMS manages FortiClient. However, FortiClient cannot participate in the Fortinet Security Fabric.

When connected to EMS and a FortiGate, FortiClient integrates with the Security Fabric to provide endpoint awareness, compliance, and enforcement by sharing endpoint telemetry regardless of device location, such as corporate headquarters or a café. At its core, FortiClient automates prevention of known and unknown threats through its built-in host-based security stack and integration with FortiSandbox. FortiClient also provides secure remote access to corporate assets via VPN with native two-factor authentication coupled with single sign on (SSO).

FortiClient works cooperatively with the Security Fabric. This is done by extending it down to the endpoints to secure them via security profiles, by sharing endpoint telemetry to increase awareness of where systems, users, and data reside within an organization, and by enabling the implementation of proper segmentation to protect these endpoints.

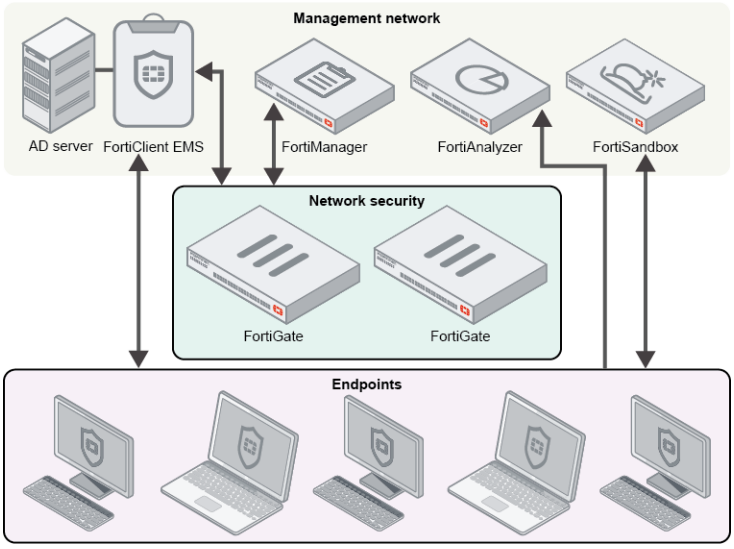
At regular intervals, FortiClient sends telemetry data to the nearest associated FortiGate. This visibility coupled with built-in controls from the FortiGate allows the security administrator to construct a policy to deny access to endpoints with known vulnerabilities or to quarantine compromised endpoints with a single click.

See Getting started with FortiClient on page 11.

Fortinet product support for FortiClient

The following Fortinet products work together to support FortiClient:

- FortiClient EMS
- FortiManager
- FortiGate
- FortiAnalyzer
- FortiSandbox



FortiClient EMS

FortiClient EMS runs on a Windows server. EMS can manage FortiClient endpoints by deploying FortiClient (Windows) and endpoint policies to endpoints, and the endpoints can connect FortiClient Telemetry to FortiGate and EMS. FortiClient endpoints connect to the FortiGate to participate in the Security Fabric. FortiClient endpoints connect to EMS to be managed in real time.

For information on EMS, see the *FortiClient EMS Administration Guide*.

FortiManager

FortiManager provides central FortiClient management for FortiGates that FortiManager manages. When endpoints are connected to managed FortiGates, you can use FortiManager to monitor endpoints from multiple FortiGates.

For information on FortiManager, see the *FortiManager Administration Guide*.

FortiGate

FortiGate provides network security. EMS defines compliance verification rules for connected endpoints and communicates the rules to endpoints and the FortiGate. The FortiGate uses the rules and endpoint information from EMS to dynamically adjust security policies. When using FortiManager, FortiGates communicate between endpoints, EMS, and FortiManager.

When FortiClient Telemetry is connected to the FortiGate, endpoints can participate in the Security Fabric.

For information on FortiGate, see the *FortiOS documentation*.

FortiAnalyzer

FortiAnalyzer can receive logs and software inventory reports from endpoints connected to FortiGate or EMS, and you can use FortiAnalyzer to analyze the logs and run reports. FortiAnalyzer receives logs and software inventory reports directly from FortiClient.

For information on FortiAnalyzer, see the *FortiAnalyzer Administration Guide*.

FortiSandbox

FortiSandbox offers capabilities to analyze new, previously unknown, and undetected virus samples in real time. Files sent to it are scanned first, using similar antivirus (AV) engine and signatures as are available on FortiOS and FortiClient. If the file is not detected but is an executable file, it is run in a Microsoft Windows virtual machine (VM) and monitored. The file is given a rating or score based on its activities and behavior in the VM.

As FortiSandbox receives files for scanning from various sources, it collects and generates AV signatures for such samples. FortiClient periodically downloads the latest AV signatures from FortiSandbox, and applies them locally to all realtime and on-demand AV scanning.

FortiClient supports connection to an on-premise FortiSandbox appliance or FortiSandbox Cloud. For more information, see the *FortiSandbox Administration Guide*.

Feature comparison of FortiClient free and paid versions

FortiClient is available as a free and paid version. The free version is available for Windows and macOS, while the paid version is available for Windows, macOS, and Linux. The following chart shows the modules available for each OS using the free or paid version of FortiClient:

Module	Free		Paid			
	Windows and Windows Server	macOS	Windows	Windows Server	macOS	Linux
Fabric Telemetry	No	No	Yes	Yes	Yes	Yes
Compliance	No	No	Yes	Yes	Yes	Yes
Sandbox Detection (including connection to FortiSandbox Cloud)	No	No	Yes	No	Yes	Yes
AntiVirus	No	No	Yes	Yes	Yes	Yes
Web Filter	No	No	Yes	No	Yes	No

Module	Free		Paid			
	Windows and Windows Server	macOS	Windows	Windows Server	macOS	Linux
Application Firewall	No	No	Yes	No	Yes	No
Remote Access	Only supports a limited version of the Remote Access feature. The following is supported: • IPsec and SSL VPN with user authentication • Certificate authentication • Two-factor authentication using FortiToken You can only download the free VPN client from FNDN or FortiClient.com. For details, see Standalone VPN client on page 76.		Yes	SSL VPN only	Yes	SSL VPN only
Vulnerability Scan	No	No	Yes	Yes	Yes	Yes
Central management	No	No	Yes	Yes	Yes	Yes
24x7 support	No	No	Yes	Yes	Yes	Yes

Getting started

This section describes how to get started with FortiClient. It also includes key concepts that administrators and endpoint users should be aware of when using FortiClient.

Getting started with FortiClient

In 6.2.5, you must use FortiClient with EMS. FortiClient must connect to EMS to activate its license and become provisioned by the endpoint profile that the administrator configured in EMS. You cannot use any FortiClient features (except for VPN, as described in Free three-day VPN access on page 66) until FortiClient is connected to EMS and licensed.

You can also use FortiClient with both EMS and FortiGate.

The setup process is as follows. The EMS administrator completes some actions, and the endpoint user completes others.

1. The administrator configures a FortiClient deployment package in EMS. The administrator specifies which modules to install in the deployment package.
2. The administrator prepares to deploy FortiClient from EMS. See Provisioning preparation on page 16.
3. The administrator deploys FortiClient on the endpoint from EMS. See Provisioning on page 23. FortiClient installs on the endpoint. For installation to be successful, the endpoint must be a computer or device on your network that has Internet access and is running a supported operating system.
   After FortiClient installs on the endpoint, it immediately connects to EMS to activate its license. The endpoint user may need to confirm the connection request to complete the Telemetry connection to EMS. FortiClient is now a managed endpoint. Once licensed, FortiClient becomes provisioned by the endpoint profile configured in EMS. The modules that the administrator included in the deployment package in step 1 become available for use.
   After the endpoint profile provisions FortiClient, it connects to the FortiGuard server to check for updates for the configured features.
   If configured, FortiClient also connects to the FortiGate. Once connected to the FortiGate, the endpoint is participating in the Security Fabric.
4. The administrator manages the endpoint using EMS.
5. If desired, the endpoint user can add a personal VPN configuration. See Configuring VPN connections on page 61.
6. The endpoint user can use the installed modules in FortiClient. Depending on what modules were installed, one, more, or all of the following tabs are available:
   - Fabric Telemetry
   - Malware Protection
   - Sandbox Detection
   - Web Filter
   - Application Firewall
   - Vulnerability Scan
   - Remote Access

FortiClient must maintain a Telemetry connection to EMS to maintain its licensed status. If FortiClient disconnects from EMS and does not reconnect within the given timeout, the endpoint loses its license and the endpoint user cannot use any FortiClient features until FortiClient reestablishes connection to EMS.

If FortiClient registers to EMS but later becomes offline (meaning it is still registered to but cannot reach EMS), all features function for 30 days. After 30 days, FortiClient becomes unregistered and all features are disabled.

EMS and endpoint profiles

In EMS, administrators can configure an endpoint profile. Administrators then include the profile in an endpoint policy, which is applied to groups of endpoints. The profile defines the configuration for FortiClient software on endpoints. Administrators can also use the endpoint profile to install and upgrade FortiClient on endpoints. The profile consists of the following sections:

- Deployment
- AntiVirus
- Sandbox
- Web Filter
- Firewall
- VPN
- Vulnerability Scan
- System Settings
- XML Configuration

When the endpoint receives the configuration information in the endpoint profile as part of an endpoint policy, FortiClient settings are automatically updated. FortiClient settings are locked and read-only when EMS provides the configuration in a profile.

For information on configuring endpoint profiles using EMS, see the *FortiClient EMS Administration Guide*.

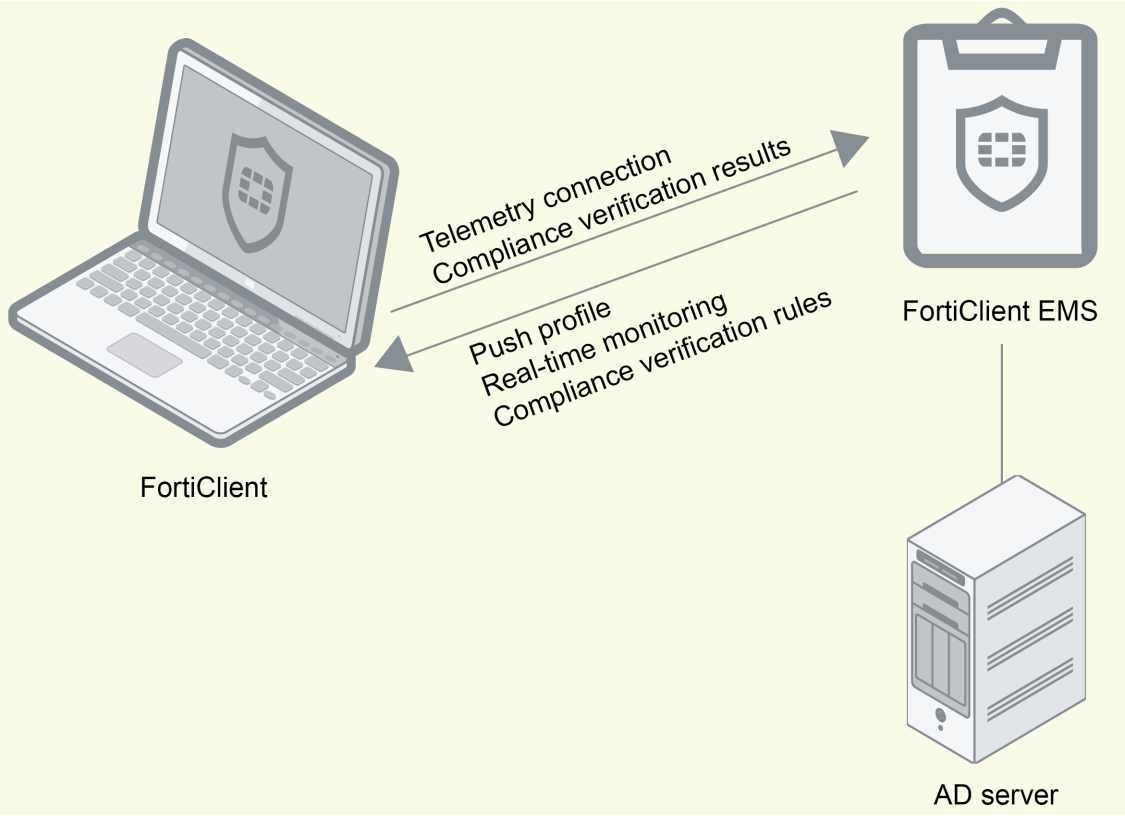
Telemetry connection options

FortiClient Telemetry can connect to EMS or FortiGate and EMS.

EMS manages FortiClient endpoints using the FortiClient Telemetry connection. Endpoints connect FortiClient Telemetry to FortiGate to participate in the Security Fabric. FortiGates do not manage endpoints.

EMS

In this scenario, EMS provides FortiClient endpoint provisioning. FortiClient connects Telemetry to EMS to receive configuration information in an endpoint profile as part of an endpoint policy from EMS. EMS also sends compliance verification rules to FortiClient and uses the results from FortiClient to dynamically group endpoints in EMS. Only EMS can control the connection between FortiClient and EMS. You must make any changes to the connection from EMS, not FortiClient. When FortiClient is connected to EMS, FortiClient settings are locked so the endpoint user cannot change any configuration. To disconnect FortiClient from EMS, the EMS administrator must deregister the endpoint in EMS.



See the *FortiClient Compliance Guide*.

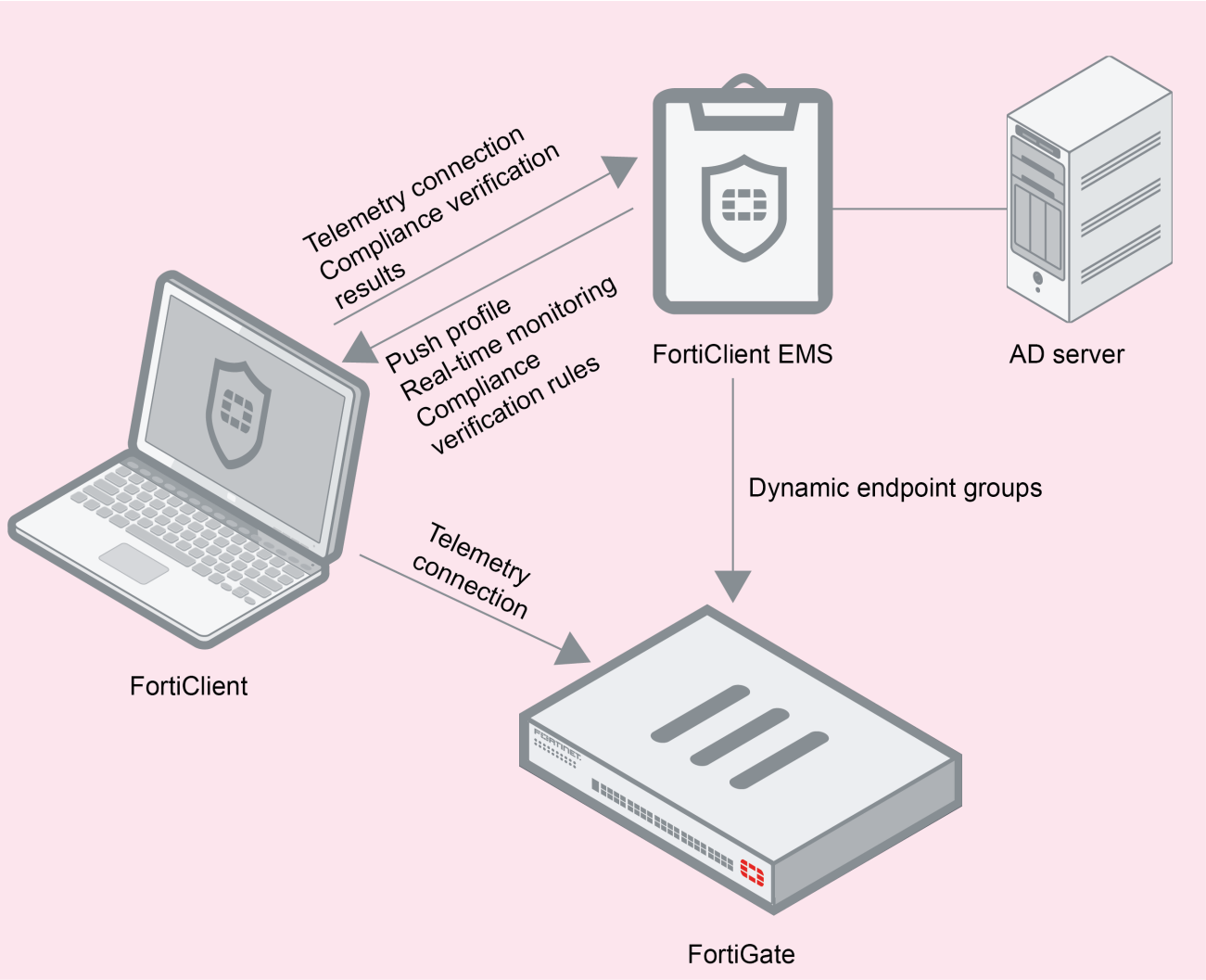
FortiGate and EMS

In this scenario, FortiClient Telemetry connects to EMS to receive a profile of configuration information as part of an endpoint policy and to FortiGate to participate in the Security Fabric. The FortiGate can also receive dynamic endpoint group lists from EMS and use them to build dynamic firewall policies. EMS sends group updates to FortiOS, and FortiOS uses the updates to adjust the policies based on those groups. This feature requires FortiOS 6.2.0 or a later version.

FortiGate does not provide configuration information for FortiClient and the endpoint. An administrator must configure FortiClient using an EMS endpoint profile.

Following is a summary of how the FortiClient Telemetry connection works in this scenario:

- FortiClient Telemetry connects to EMS.
- FortiClient receives a profile of configuration information from EMS as part of an endpoint policy.
- FortiClient Telemetry connects to the FortiGate using a Telemetry gateway list received from EMS. This allows the endpoint to participate in the Security Fabric.
- EMS sends compliance verification rules to the endpoint.
- FortiClient checks the endpoint using the provided compliance verification rules and sends the results to EMS.
- EMS receives the results form FortiClient and dynamically groups the endpoints according to the results.
- FortiOS pulls the dynamic endpoint group information from EMS. You can use this data to build dynamic firewall policies.
- EMS sends dynamic endpoint group updates to FortiOS. FortiOS uses the updates to adjust the policies based on those groups.



For details on configuring FortiOS to pull endpoint tags and their corresponding endpoint lists from EMS, see the *FortiClient EMS Administration Guide*.

Telemetry gateway IP lists

The Telemetry gateway IP list is a list of gateway IP addresses that FortiClient can use to connect Telemetry to FortiGate and/or EMS. After FortiClient installation completes on the endpoint, FortiClient automatically launches and uses the Telemetry gateway IP list to locate the FortiGate and/or EMS for Telemetry connection.

FortiClient EMS includes the option to create one or more Telemetry gateway IP lists. The list can include IP addresses for EMS servers and for FortiGates. Administrators can assign Telemetry gateway IP lists to domains and workgroups in EMS. Administrators can also update the assigned Telemetry gateway IP lists after FortiClient is installed, and the updated lists are pushed to endpoints. See the *FortiClient EMS Administration Guide*.

EMS and automatic upgrade of FortiClient

You can use EMS to create a FortiClient installer configured to automatically upgrade FortiClient on endpoints to the latest version.

After the FortiClient installer with automatic upgrade enabled is deployed to endpoints, FortiClient is automatically upgraded to the latest version when a new version of FortiClient is available via EMS. See the *FortiClient EMS Administration Guide*.

Provisioning preparation

Before provisioning FortiClient, administrators and endpoint users should understand the installation requirements and FortiClient setup types available for installation. Administrators should also be aware of the licensing requirements.

Installation requirements

The following table lists operating system support and the minimum system requirements:

Operating system support	Minimum system requirements
• Microsoft Windows 7 (32-bit and 64-bit) • Microsoft Windows 8.1 (32-bit and 64-bit) • Microsoft Windows 10 (32-bit and 64-bit) FortiClient 6.2.5 does not support Microsoft Windows XP, Microsoft Windows Vista, or Microsoft Windows 8.	• Microsoft Windows-compatible computer with Intel processor or equivalent. FortiClient does not support ARM-based processors. • Compatible operating system and minimum 512 MB RAM • 600 MB free hard disk space • Native Microsoft TCP/IP communication protocol • Native Microsoft PPP dialer for dialup connections • Ethernet NIC for network connections • Wireless adapter for wireless network connections • Adobe Acrobat Reader for viewing documentation • MSI installer 3.0 or later
Microsoft Windows Server 2008 R2 or newer	• Microsoft Windows-compatible computer with Intel processor or equivalent. FortiClient does not support ARM-based processors. • Compatible operating system and minimum 512 MB RAM • 600 MB free hard disk space • Native Microsoft TCP/IP communication protocol • Native Microsoft PPP dialer for dialup connections • Ethernet NIC for network connections • Wireless adapter for wireless network connections • Adobe Acrobat Reader for viewing documentation • MSI installer 3.0 or later

Operating system support	Minimum system requirements
• macOS Sierra (version 10.12) • macOS High Sierra (version 10.13) • macOS Mojave (version 10.14) • macOS Catalina (version 10.15)	• Apple Mac computer with Intel processor • 256 MB of RAM • 20 MB of hard disk drive (HDD) space • TCP/IP communication protocol • Ethernet NIC for network connections • Wireless adapter for wireless network connections

Linux distributions:
• Ubuntu 16.04 or newer
• Red Hat 7.4 or newer
• CentOS 7.4 or newer
with KDE or GNOME
	• Linux-compatible computer with Intel processor or equivalent
	• Compatible operating system and minimum 512 MB RAM
	• 600 MB free hard disk space
	• TCP/IP communication protocol
	• Ethernet NIC for network connections
	• Wireless adapter for wireless network connections
	If installing on Ubuntu 16.04 LTS, add the following line in `/etc/apt/sources.list`:
	`deb [arch=amd64] http://repo.fortinet.com/repo/ubuntu/ xenial multiverse`
	If installing on Ubuntu 18.04 LTS, add the following line in `/etc/apt/sources.list`:
	`deb [arch=amd64] http://repo.fortinet.com/repo/ubuntu/ bionic multiverse`

For Microsoft Windows Server, FortiClient supports the Vulnerability Scan, SSL VPN, and AV features, including obtaining a Sandbox signature package for AV scanning. To use SSL VPN on a Windows Server machine, you must enable your browser to accept cookies. Otherwise, tunnel connection fails.

Licensing

FortiClient requires a license. You apply FortiClient licensing to EMS. See the *FortiClient EMS Administration Guide* for details.

Contact your Fortinet sales representative for information about FortiClient licenses.

Required services and ports

You must ensure required port and services are enabled for use by FortiClient and its associated applications on your server. The required ports and services enable FortiClient to communicate with servers running associated applications.

Communication	Usage	Protocol	Port	Incoming/Outgoing	How to customize
FortiClient Telemetry	Endpoint management (EMS), participation in the Security Fabric (FortiGate)	TCP	8013	Outgoing	GUI
SYSLOG	Upload logs to syslog server	UDP	514	Outgoing	N/A
FortiSandbox	Send files to FortiSandbox for analysis	TCP	514	Outgoing	N/A
Remote access - SSL VPN	Establish VPN connection to the FortiGate	TCP	443 (default)	Outgoing	GUI
FortiAnalyzer/FortiManager	Upload logs to FortiAnalyzer or FortiManager	TCP	514	Outgoing	N/A
Remote access - IPsec VPN	Establish VPN connection to the FortiGate	UDP	IKE 500 ESP (IP 50) NAT-T 4500	Outgoing	N/A
FortiAuthenticator/FortiGate	SSO mobility agent, FortiClient SSO (FSSO)	TCP	8001 (default)	Outgoing	GUI
FortiGuard	URL rating	TCP	8888 (default)	Outgoing	Change to UDP via XML. See the *FortiClient XML Reference Guide*.
	AV/vulnerability signatures update	TCP	80	Outgoing	N/A
	Cloud-based behavior scan (CBBS)/applications that use cloud services	TCP	80	Outgoing	N/A

Communication	Usage	Protocol	Port	Incoming/Outgoing	How to customize
FortiManager	Use a FortiManager for FortiClient software and signature updates	TCP	80 (default)	Outgoing	GUI
SMTP/FortiGuard	Virus submission	TCP	25	Outgoing	N/A

For the list of required services and ports for EMS, see the *FortiClient EMS Administration Guide*.

FortiClient setup types and modules

When the administrator creates a FortiClient deployment package in EMS, they choose which setup type and modules to install:

- Security Fabric Agent
- Secure Access Architecture Components
- Advanced Persistent Threat (APT) Components
- Additional Security Features

The following table summarizes the impact of the options:

Setup type	Description	Impact on FortiClient
Security Fabric Agent	Enabled by default and installs components to support the Security Fabric available with FortiGate, including FortiClient Telemetry, vulnerability scanning, and vulnerability remediation.	Displays the following tabs: • *Fabric Telemetry* • *Vulnerability Scan*
Secure Access Architecture Components	Optional. Supports SSL and IPsec VPN access.	Displays the *Remote Access* tab.
Advanced Persistent Threat (APT) Components	Optional. Supports FortiSandbox and quarantine features.	Enables the *Sandbox Detection* tab to connect to FortiSandbox.
Additional Security Features	Optional. Supports AntiVirus, Web Filtering, Application Firewall, SSO mobility agent, and cloud-based malware outbreak detection. The administrator may select one, more, or all security features.	Displays the following tabs when all security features are selected: • *Malware Protection* • *Web Filter* • *Application Firewall* When *Single Sign On* is selected, FortiClient supports the SSO feature. When a security feature is not selected, the tab is hidden from view in FortiClient.

The administrator can use an EMS profile to disable installed components in FortiClient but cannot use an EMS profile to enable uninstalled components in FortiClient. See EMS and endpoint profiles on page 12.

For example, if the administrator creates the EMS installer with APT components selected, the *Sandbox Detection* tab is enabled in FortiClient. The administrator can use an EMS profile to disable *Sandbox Detection*. However, if the installer did not include APT components, the *Sandbox Detection* tab is disabled in FortiClient and the administrator cannot use an EMS profile to enable *Sandbox Detection*.

Firmware images and tools

Firmware images and tools are available for Windows, macOS, and Linux.

Microsoft Windows

The following files are available in the firmware image file folder:

File	Description
FortiClientTools_6.2.5.xxxx.zip	Zip package containing miscellaneous tools, including VPN automation files.
FortiClientSSOSetup_ 6.2.5.xxxx.zip	FSSO-only installer (32-bit).
FortiClientSSOSetup_ 6.2.5.xxxx_x64.zip	FSSO-only installer (64-bit).

The FortiClient 6.2.5 standard installer and zip package containing FortiClient.msi and language transforms are included with EMS 6.2.5.

The following tools and files are available in the FortiClientTools_6.2.xx.xxxx.zip file:

File	Description
FortiClientVirusCleaner	Virus cleaner.
SSLVPNcmdline	Command line SSL VPN client.
SupportUtils	Includes diagnostic, uninstallation, and reinstallation tools.
VPNAutomation	VPN automation tool.

The following files are available on FortiClient.com:

File	Description
FortiClientVPNSetup_ 6.2.5.xxxx.exe	Free VPN-only installer (32-bit).
FortiClientVPNSetup_ 6.2.5.xxxx_x64.exe	Free VPN-only installer (64-bit).

macOS

The following file is available in the firmware image file folder:

File	Description
FortiClientTools_6.2.5.xxx_macosx.tar	Includes utility tools and files to help with installation.

The following file is available on FortiClient.com:

File	Description
FortiClientVPNSetup_6.2.5.xxx_macosx.dmg	Free VPN-only installer.

The FortiClient 6.2.5 standard installer is included with EMS 6.2.5.

Linux

The following files are available in the firmware image file folder:

File	Description
forticlient_6.2.5.xxxx_amd64.deb	Standard installer package for Ubuntu.
forticlient_6.2.5.xxxx_x86_64.rpm	Standard installer package for Red Hat and CentOS.
forticlient_server_6.2.5.xxxx_amd64.deb	Headless (no GUI, CLI-only) installer for Ubuntu.
forticlient_server_6.2.5.xxxx_x86_64.rpm	Headless (no GUI, CLI-only) installer for Red Hat and CentOS.

Obtaining FortiClient installation files

The EMS administrator will provide a download link to the FortiClient installation files. Download the installation file for your OS from the provided link.

Provisioning

You can install FortiClient on a single computer using the installation wizard or deploy it to multiple Microsoft Windows systems using Microsoft Active Directory (AD).

FortiClient prevents uninstallation only for non-administrator users.

Installing FortiClient on computers

The following section describes how to install FortiClient on a computer running a Microsoft Windows, macOS, or Linux operating system.

Microsoft Windows

The following instructions guide you though the installation of FortiClient on a Microsoft Windows computer. For more information, see the *FortiClient (Windows) Release Notes*.

To check FortiClient's digital signature, right-click the installation file and select *Properties*. In this menu you can set file attributes, run the compatibility troubleshooter, view the digital signature and certificate, install the certificate, set file permissions, and view file details.

1. Double-click the FortiClient executable file. The *Setup Wizard* launches.
2. In the *Welcome to the FortiClient Setup Wizard* screen, perform the following actions:
   a. Click the *License Agreement* button, and read the license agreement. You have the option to print the EULA in this License Agreement screen. Click *Close* to return to the installation wizard.
   b. Select the *Yes, I have read and accept the license* checkbox.
3. Click *Next* to continue. The *Destination Folder* screen displays.
4. (Optional) Click *Change* to choose an alternate folder destination for installation.
5. Click *Next* to continue.
   FortiClient searches the target system for other installed AV software. If found, FortiClient displays the *Conflicting Antivirus Software* page. You can exit the current installation and uninstall the AV software, disable the conflicting software's AV feature, or continue with the installation with FortiClient realtime protection (RTP) disabled. FortiClient automatically disables RTP when one of the following is true:
   a. The OS is a server.
   b. Exchange Server is detected.
   c. SQL Server is detected.

A dialog displays during a new FortiClient installation and when upgrading from an older FortiClient version that does not have the AV feature installed.

It is recommended to uninstall conflicting AV software before installing FortiClient or enabling the AV RTP feature. Alternatively, you can disable the conflicting software's AV feature.

6. Click *Next*. The *Ready to install FortiClient* screen displays.
7. Complete the installation:
   a. Click *Install*.
   b. Click *Finish*. On a new FortiClient installation, you do not need to reboot your system. When upgrading the FortiClient version, you must restart your system for the configuration changes made to FortiClient to take effect. Select *Yes* to restart your system now or select *No* to manually restart later. FortiClient updates signatures and components from the FDN.
   c. FortiClient attempts to connect FortiClient Telemetry to EMS and the FortiGate.

If you have questions about connecting FortiClient Telemetry to the FortiGate, contact your network administrator.

   d. To launch FortiClient, double-click the desktop shortcut.

Microsoft Server

You can install FortiClient on a Microsoft Windows Server. You can use the regular FortiClient Windows image for Server installations.

Check the *FortiClient (Windows) 6.2.5 Release Notes* for supported Microsoft Windows Server versions.

Refer to the Microsoft knowledge base for caveats on installing AV software in a server environment. See the Microsoft Anti-Virus exclusion list.

macOS

The following instructions guide you though the installation of FortiClient on a macOS computer. For more information, see the *FortiClient (macOS) Release Notes*.

1. Double-click the FortiClient_6.2.5.xx_macosx .dmg installer file. The *FortiClient for macOS* dialog displays.
2. Double-click *Install*. The *Welcome to the FortiClient Installer* dialog displays.
3. (Optional) Click the lock icon in the upper-right corner to view certificate details and click *OK* to close the dialog.

4. Click *Continue*.
5. Read the Software License Agreement and click *Continue*. You have the option to print or save the Software Agreement in this window. You are prompted to *Agree* with the terms of the license agreement.
6. If you agree with the terms of the license agreement, click *Agree* to continue the installation.
7. Depending on your system, you may be prompted to enter your system password.
8. After the installation completes successfully, Click *Close* to exit the installer. FortiClient has been saved to the *Applications* folder.
9. Double-click the FortiClient icon to launch the application. The application loads to your desktop.

Additional steps may be required if using Web Filter or RTP with FortiClient (macOS). See the *FortiClient (macOS) Release Notes* for details.

Linux

The following instructions guide you though the installation of FortiClient on a Linux computer running Ubuntu, Red Hat, or CentOS. For more information, see the *FortiClient (Linux) Release Notes*.

Various CLI commands are available for FortiClient (Linux) 6.2.5. See FortiClient (Linux) CLI commands on page 92.

Installing FortiClient using a downloaded installation file

To installing on Red Hat or CentOS

1. Obtain a FortiClient Linux installation rpm file.
2. In a terminal window, run the following command:
   `$ sudo yum install <FortiClient installation rpm file> -y`
   `<FortiClient installation rpm file>` is the full path to the downloaded rpm file.

To install on Ubuntu

1. Obtain a FortiClient Linux installation deb file.
2. Install FortiClient using the following command:
   `$ sudo apt-get install <FortiClient installation deb file>`
   `<FortiClient installation deb file>` is the full path to the downloaded deb file.

Installation folder and running processes

The FortiClient installation folder is `/opt/forticlient`. In case there are issues or you need to report a bug, FortiClient logs are available in `/var/log/forticlient`.

Installing FortiClient on infected systems

The FortiClient installer always runs a quick AV scan on the target host system before proceeding with the complete installation. If the system is clean, installation proceeds as usual.

Any virus found during this step is quarantined before installation continues.

In case a virus on an infected system prevents downloading the new FortiClient package, use the following process:

1. Boot into “safe mode with networking”. This is required for the FortiClient installer to download the latest signature packages from the Fortinet Distribution Network.
2. Run the FortiClient installer.

This scans the entire file system. A log file is generated in the logs subdirectory. If a virus is found, it is quarantined. When complete, reboot into normal mode and run the FortiClient installer to complete the installation.

Windows does not allow FortiClient installation to complete in safe mode. An error message is generated. It is necessary to reboot into normal mode to complete the installation.

Installing FortiClient as part of cloned disk images

If you configure computers using a cloned hard disk image, you must remove the unique identifier from the FortiClient application. You will encounter problems with the FortiGate 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 computer configured with the cloned hard disk image, the FortiClient application generates its own unique identifier the first time the computer is started.

1. Install the FortiClient application.
2. Right-click the FortiClient icon in the system tray and select *Shutdown FortiClient*.
3. From the folder where you expanded the FortiClientTools.zip file, run RemoveFCTID.exe. The RemoveFCTID tool requires administrative rights.

Do not include the RemoveFCTID tool as part of a logon script.

4. Shut down the computer.

Do not reboot the Windows operating system on the computer 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 using the CLI

You can install FortiClient using the CLI. The following table summarizes the installation options available when using the CLI.

Option	Description
`/quiet`	Installation is in quiet mode and requires no user interaction.
`/passive`	Installation is in unattended mode, showing only the progress bar.
`/norestart`	Does not restart the machine after installation is complete.
`/promptrestart`	Prompts you to restart the machine if necessary.
`/forcerestart`	Always restarts the machine after installation.
`/uninstall`	Uninstalls FortiClient.
`/log <path to log file>`	Creates a log file in the specified directory with the specified name.

The following example installs FortiClient build 1131 in quiet mode, does not restart the machine after installation, and creates a log file with the name "example" in the c:\temp directory:

```
FortiClientSetup_6.2.5.1131_x64.exe /quiet /norestart /log c:\temp\example.log
```

Deploying FortiClient using Microsoft AD servers

There are multiple ways to deploy FortiClient MSI packages to endpoints including using AD servers. See Firmware images and tools on page 21.

The following instructions are based on Microsoft Windows Server 2008. If you are using a different version of Microsoft Server, your MMC or snap-in locations may be different.

Using Microsoft AD to deploy FortiClient

1. On your domain controller, create a distribution point.
2. Log into the server computer as an administrator.
3. Create a shared network folder where the FortiClient MSI installer file is distributed from.
4. Set file permissions on the share to allow access to the distribution package. Copy the FortiClient MSI installer package into this share folder.
5. Select *Start* > *Administrative Tools* > *Active Directory Users and Computers*.
6. After selecting your domain, right-click to select a new organizational unit (OU).
7. Move all the computers you want to distribute the FortiClient software to into the newly-created OU.

8. Create a group policy object (GPO), then create the FortiClient installer package:
   a. Select *Start* > *Administrative Tools* > *Group Policy Management*. The Group Policy Management MMC Snap-in opens. Select the OU you just created. Right-click it, *Select Create a GPO* in this domain, and link it here. Give the new GPO a name then select *OK*.
   b. Expand the GPO container and find the newly created GPO. Right-click the GPO and select *Edit*. The Group Policy Management Editor MMC Snap-in opens.
   c. Expand *Computer Configuration* > *Policies* > *Software Settings*. Right-click *Software Settings* and select *New* > *Package*.
   d. Select the path of your distribution point and FortiClient installer file and then select *Open*. Select *Assigned* and select *OK*. The package is then generated.
9. If you wish to expedite the installation process, on the server and client computers, force a GPO update.
10. The software is installed on the client computer's next reboot. You can also wait for the client computer to poll the domain controller for GPO changes and install the software then.

Using Microsoft AD to uninstall FortiClient

1. On your domain controller, select *Start* > *Administrative Tools* > *Group Policy Management*. The Group Policy Management MMC Snap-in opens. Expand the Group Policy Objects container and right-click the Group Policy Object you created to install FortiClient and select *Edit*. The *Group Policy Management Editor* opens.
2. Select *Computer Configuration* > *Policy* > *Software Settings* > *Software Installation*. You can now see the package used to install FortiClient.
3. Right-click the package and select *All Tasks* > *Remove*. Choose *Immediately* to uninstall the software from users and computers, or *Allow* users to continue to use the software but prevent new installations. Select *OK*. The package deletes.
4. If you wish to expedite the uninstall process on both the server and client computers, force a GPO update as shown in the previous section. The software is uninstalled on the client computer's next reboot. You can also wait for the client computer to poll the domain controller for GPO changes and uninstall the software then.

Uninstalling FortiClient

1. The EMS administrator deregisters the endpoint. See the *FortiClient EMS Administration Guide*.
2. In FortiClient, on the *Fabric Telemetry* tab, disconnect from EMS. The endpoint is no longer managed by EMS.
3. Go to *Settings*, then unlock the configuration.
4. In the Windows System Tray, right-click the FortiTray icon, then select *Shutdown FortiClient*.
5. Once FortiClient is shutdown, uninstall FortiClient using the Windows Add/Remove Programs application.

Upgrading FortiClient

For information about supported upgrade paths for FortiClient, see the *FortiClient and FortiClient EMS Upgrade Paths*.

An administrator will control FortiClient upgrades for you. See EMS and automatic upgrade of FortiClient on page 15.

When an administrator deploys a FortiClient upgrade from EMS to endpoints running a Windows operating system, an *Upgrade Schedule* dialog displays in advance on the endpoint to let endpoint users schedule the upgrade and mandatory endpoint reboot. If no FortiClient is installed on the endpoint, no reboot is required for the installation, and no *Upgrade Schedule* dialog displays. The endpoint user can postpone the reboot for a maximum of 24 hours. Before the mandatory reboot occurs, a FortiClient dialog displays with a 15 minute warning.

To upgrade FortiClient:

1. Go to *About*.
2. Beside the version, click *Update Available: <version number>*.

To upgrade FortiClient from FortiTray:

1. Select the Windows System Tray.
2. Right-click the *FortiTray* icon, and select *Update Available: <version number>*.

User details

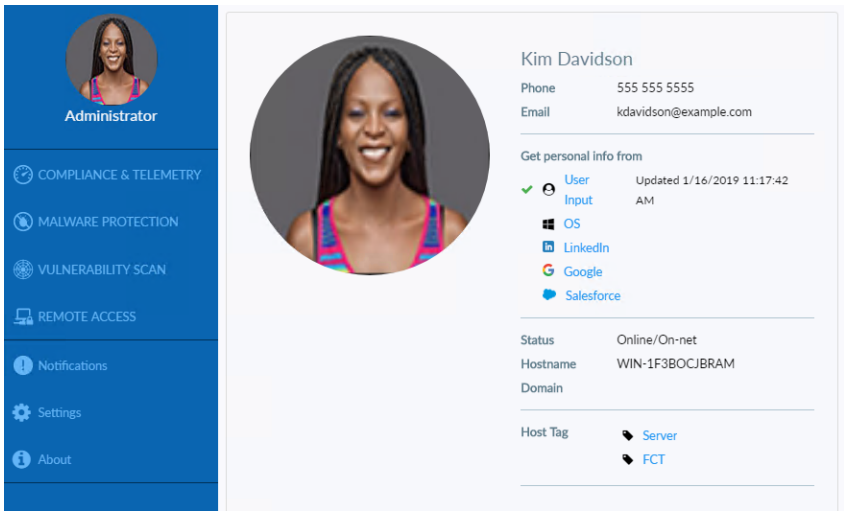
You can view and edit user details by clicking the user avatar in the upper left corner of FortiClient.

Viewing user details

When an administrator configures FortiClient to send logs to FortiAnalyzer or FortiManager, some user details are visible in FortiAnalyzer, FortiManager, and FortiOS. See Sending logs and software inventory reports to FortiAnalyzer or FortiManager on page 80.

Click the user avatar in the upper left corner of FortiClient to view the following information:

Full name	Displays the endpoint user's name if added by the endpoint user.
Phone	Displays the endpoint user's phone number if added by the endpoint user. See Retrieving user details from cloud applications on page 31 and Adding your phone number and email address manually on page 32.
Email	Displays the endpoint user's email address if added by the endpoint user. See Retrieving user details from cloud applications on page 31 and Adding your phone number and email address manually on page 32.
Get personal info from	Displays the source of the endpoint user's personal information and the last time the information was updated. The options are user-specified, from the OS, and from cloud applications: LinkedIn, Google, and Salesforce. You can click *User Input* to select an image or take a webcam photo to use as the user avatar. The endpoint user can provide information to FortiClient from an account for a cloud application, such as a Linkedin, Google, or Salesforce account. After the endpoint user logs into the account, FortiClient attempts to retrieve the following information when available: name, avatar, phone number, and email address. See Retrieving user details from cloud applications on page 31.
Status	Displays whether the endpoint is online or offline, on-net or off-net. See On-net/off-net status with EMS on page 36.
Hostname	Displays the hostname of the endpoint where FortiClient is installed.
Domain	Displays the name of the domain to which the endpoint is connected, if applicable.
Host Tag	Displays the tags that have been applied to the endpoint depending on the compliance verification rules configured in EMS. Host tags may or may not be visible depending on the EMS configuration.



Retrieving user details from cloud applications

You can direct FortiClient to retrieve information about you from one of the following cloud applications, if you have an account:

- LinkedIn
- Google
- Salesforce

FortiClient attempts to retrieve the following information after you log in:

- Username
- Phone number
- Email address
- Picture

FortiClient displays the retrieved information. The information is encrypted and only FortiClient can access it. FortiClient does not retrieve or save the password for your social media account.

Consider a situation where two users, User A and User B, use the same computer:

1. User A logs into the computer and provides their social media information in FortiClient.
2. FortiClient retrieves and displays User A's social media information while User A is logged in.
3. User A logs out of the computer.
4. User B logs into the computer.
5. FortiClient no longer displays User A's social media information. If User B previously provided their social media information, this automatically displays. Otherwise FortiClient displays the avatar for User B's OS account. If it was not previously provided, User B provides their social media information, which displays in FortiClient.
6. User B logs out and User A logs in. FortiClient displays User A's social media information.

If User A or B do not log out of their account and instead lock the screen or switch accounts, FortiClient may display either user's social media information to both users.

Although FortiClient can retrieve the endpoint user's username from cloud applications, the retrieved username does not display in FortiClient. Instead, the retrieved username is included in FortiClient logs with the phone number and email address. You can view log content in FortiOS, FortiAnalyzer, and FortiManager. See Sending logs and software inventory reports to FortiAnalyzer or FortiManager on page 80.

You can manually specify an avatar for FortiClient to use and edit the phone number and email address. See Specifying the user avatar manually on page 32 and Adding your phone number and email address manually on page 32.

1. Click the user avatar in the upper left corner of FortiClient.
2. Click one of the following links:
   - *Linkedin*
   - *Google*
   - *Salesforce*
3. A browser window opens. Log into your account.
4. Click *Allow* to grant FortiClient permission to use your information.

Adding your phone number and email address manually

Although FortiClient can retrieve information from a cloud application account, you can manually add or edit a phone number or email address in FortiClient.

The phone number can be a maximum of 30 characters and can include any of the following characters: *0123456789-+x*

To add a phone number and email address manually:

1. Click the user avatar in the upper left corner of FortiClient.
2. Click *Add Phone*, enter the phone number, and press *Enter*.
3. Click *Add Email*, enter the email address, and press *Enter*.

To edit a phone number or email address:

1. Click the user avatar in the upper left corner of FortiClient.
2. Click the phone number or email address, edit the information, and press *Enter*.

Specifying the user avatar manually

Although FortiClient can retrieve an avatar from Windows, an AD server, or a cloud application, you can add an avatar to FortiClient by taking a photo or uploading an avatar .

1. Click the user avatar in the upper left corner of FortiClient.
2. Under *Get personal info from*, click *User Input*.
3. Take a photo using the webcam, or select an existing image file.

Fabric Telemetry

The *Fabric Telemetry* tab displays whether FortiClient Telemetry is connected to EMS and FortiGate. You can use the *Fabric Telemetry* tab to manually connect FortiClient Telemetry to EMS and to disconnect FortiClient Telemetry from EMS.

FortiClient Telemetry

FortiClient can use a gateway IP address to connect FortiClient Telemetry to FortiGate or EMS. FortiClient only registers to a FortiGate if all of the following is true:

- FortiClient is registered to EMS.
- FortiClient has received a Telemetry gateway list from EMS.
- EMS has allocated a Fabric Agent license seat to the endpoint. A Fabric Agent license is required to register to the FortiGate.

If FortiClient becomes unregistered from EMS, it also becomes unregistered from the FortiGate.

For information about Telemetry gateway IP lists, see Telemetry gateway IP lists on page 15.

Telemetry data

When FortiClient Telemetry is connected to EMS or EMS and FortiGate, FortiClient collects the following data about the endpoint and its workload and sends it to EMS or EMS and FortiGate:

- Hardware information, such as MAC addresses
- Software information, such as the OS version on the endpoint
- Identification information, such as username, avatar, and hostname
- Vulnerability information that the vulnerability scanning module reports

When FortiClient Telemetry is connected to FortiGate, the Security Fabric uses the information to understand the endpoint and its workload to better protect it.

Connecting FortiClient Telemetry after installation

After FortiClient software installation completes on an endpoint, FortiClient automatically launches and connects Telemetry to the EMS server that created the installed deployment package.

To connect to an on-premise EMS:

1. When FortiClient locates EMS, the *Connecting FortiClient Telemetry* dialog displays. The following options are available:

Endpoint User	Displays the name of the endpoint user logged into the endpoint.
Logged into Domain	Displays the domain name if applicable.
Hostname	Displays the endpoint name.
Remember this Endpoint Management Server (EMS)	Select for FortiClient to remember the IP address of the EMS you are connecting Telemetry to. See Remembering gateway IP addresses on page 35.

2. Click *OK* to connect FortiClient Telemetry to the identified EMS.
After FortiClient Telemetry is connected to EMS, FortiClient receives an endpoint policy from EMS. A system tray bubble message displays once the download is complete. The endpoint policy may contain an endpoint profile of configuration information as well as a Telemetry gateway list. FortiClient uses the received gateway list to connect Telemetry to FortiGate. If there are multiple FortiGates configured in the list, FortiClient connects to the FortiGate in the list that is in the same subnet as the host system. If there are no FortiGates in the list that belong to the same subnet, FortiClient attempts to connect to the first reachable FortiGate in the list, starting from the top. FortiClient maintains the list order as configured in EMS.

You can also manually enter the EMS IP address on the *Fabric Telemetry* tab, in the *Register with Security Fabric* field. This displays the same *Connecting FortiClient Telemetry* dialog described above.

FortiClient uses the same process to connect Telemetry to EMS after the FortiClient endpoint reboots, rejoins the network, or encounters a network change.

To connect to EMS Cloud:

1. After initial installation, FortiClient should automatically register to FortiClient Cloud. If FortiClient did not automatically register to FortiClient Cloud enter the invitation code in the *Join FortiClient Cloud* field on the *Fabric Telemetry* tab in FortiClient. Your EMS administrator should have provided the code to you.
2. Click *Connect*. FortiClient is now managed by FortiClient Cloud.

Remembering gateway IP addresses

When you confirm Telemetry connection to EMS, you can instruct FortiClient to remember the EMS IP address. If a connection key is required, FortiClient remembers the connection key too. FortiClient can remember up to 20 IP addresses for EMS.

The remembered IP addresses display in the local gateway IP list. FortiClient can use the remembered gateway IP addresses to automatically connect to EMS.

See Forgetting gateway IP addresses on page 36.

1. In the *Connecting FortiClient Telemetry* dialog, select the *Remember this Endpoint Management Server (EMS)* checkbox.
2. Click *Accept*. FortiClient remembers the IP address and password, if applicable.

Forgetting gateway IP addresses

When you instruct FortiClient to forget an IP address for EMS, FortiClient Telemetry does not use the IP address to automatically connect to EMS when rejoining the network.

1. On the *Fabric Telemetry* tab, click the menu icon beside the *Disconnect* button.
2. In the *Remembered Gateway List*, click *Forget* beside the gateway IP addresses you no longer want FortiClient to remember.

Disconnecting FortiClient Telemetry

You must disconnect FortiClient Telemetry from EMS to connect to another EMS or to disable and uninstall FortiClient.

An EMS administrator may disconnect FortiClient for you. This is sometimes referred to as deregistering FortiClient. When an EMS administrator disconnects FortiClient Telemetry for you, the Telemetry gateway list is also removed from FortiClient.

1. On the *Fabric Telemetry* tab, click *Disconnect*. A confirmation dialog displays.
2. Click *Yes* to disconnect FortiClient Telemetry from EMS.

After you disconnect FortiClient Telemetry from EMS, FortiClient Telemetry automatically connects with EMS when you rejoin the network.

Compliance with EMS and FortiOS

In FortiClient 6.2.5, compliance depends on EMS and FortiOS. This feature is only available if using FortiClient 6.2.5 with EMS 6.2 or 6.4 and FortiOS 6.2 or 6.4.

The administrator can define compliance verification rules in EMS based on criteria such as certificates, the logged in domain, files present, OS versions, running processes, and registry keys. When a FortiClient endpoint registers to EMS, EMS dynamically groups the endpoint based on the compliance verification rules. FortiOS can receive the dynamic endpoint groups from EMS and use them to create dynamic firewall policies. The endpoint may be unable to access the network based on the compliance verification rules.

See the *FortiClient EMS Administration Guide*.

On-net/off-net status with EMS

Endpoints must connect FortiClient Telemetry to EMS and FortiGate for FortiClient to use an on-net, off-net, or offline status.

When FortiClient connects Telemetry to EMS, FortiClient determines whether the endpoint has an on-net or off-net status.

For more details on determining on-net/off-net status, see *Determining on-net/off-net status*.

EMS only

When FortiClient has connected Telemetry to EMS only, *DHCP onnet/offnet* and *On-Net Subnets* settings in EMS affect on-net/off-net status. See the *FortiClient EMS Administration Guide* for details on these settings.

The following table shows how various configurations determine the endpoint status when FortiClient Telemetry is connected to EMS:

DHCP onnet/offnet	On-net detection rules	Option 224 serial number	Resulting endpoint status
Disabled	Not configured	N/A	Endpoint is on-net when registered to EMS.
Enabled	Not configured	Not configured	Endpoint is off-net when registered to EMS.
Enabled	Not configured	Configured	On-net Since Option 224 is configured with a Fortinet device's serial number, EMS assumes FortiClient is on-net with that FortiGate.
N/A	Enabled, with subnet configured. Endpoint IP address is in the configured subnet.	N/A	On-net The endpoint is inside the on-net networks configured in the applied endpoint policy's on-net detection rules.
N/A	Enabled, with subnet configured. Endpoint IP address is not in the configured subnet.	N/A	Off-net The endpoint is outside the on-net networks configured in the applied endpoint policy's on-net detection rules.

An endpoint has an offline off-net status when it cannot connect FortiClient Telemetry to EMS and is outside any of the on-net networks.

An endpoint has an offline on-net status when it cannot connect FortiClient Telemetry to EMS but is inside one of the on-net networks, or if no on-net settings are configured within the assigned policy.

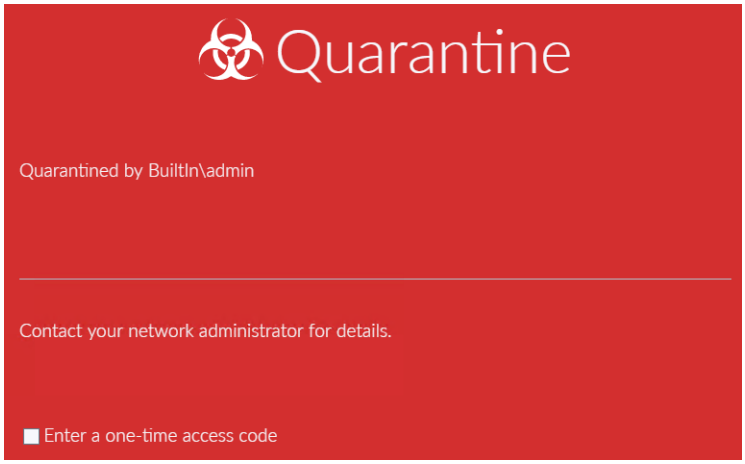
Logging to FortiAnalyzer

When FortiClient endpoints are on-net and logging to FortiAnalyzer is configured, FortiClient logs are sent to FortiAnalyzer. However, when FortiClient endpoints are off-net, and FortiAnalyzer is not reachable, FortiClient logs are held for the log retention period, and sent to FortiAnalyzer when FortiClient is on-net again. By default, FortiClient logs

are held for 90 days. You can control the log retention period by using the `<log_retention_days>` element in the XML configuration. See the *FortiClient XML Reference Guide*.

Quarantined endpoints

In certain situations, an administrator may quarantine an endpoint. When an endpoint is quarantined, the following page displays, and the endpoint user loses network access. Contact your system administrator for assistance.



If the EMS administrator customized the quarantine message, the message may display differently than the example above. In the following example, the EMS administrator has added a phone number to the message.

After the endpoint is quarantined, you can select the *Enter a one-time access code* checkbox and enter the code to access the FortiClient GUI. You can obtain the access code from the EMS administrator.

After using the code to access the FortiClient GUI, you can remove the endpoint from quarantine by clicking the *Unquarantine* button.

Malware Protection

The Malware Protection tab includes AntiVirus Protection, Cloud Based Malware Protection, AntiExploit, and Removable Media Access.

The *Malware Protection* tab displays in FortiClient when FortiClient is installed with *Additional Security Features* selected.

Antivirus

FortiClient includes an AV component to scan system files, executable files, removable media, dynamic-link library (DLL) files, and drivers. FortiClient also scans for and removes rootkits. In FortiClient, file-based malware, malicious websites, phishing, and spam URL protection are part of the AV component.

Updating the AV database

FortiClient informs you if the AV database is out of date. FortiClient automatically updates signatures. However, if you see the signatures are outdated, you can go to *About* to download updates from FortiGuard. See Viewing FortiClient engine and signature versions on page 43.

Scanning with AV on-demand

You can perform on-demand AV scanning. You can scan specific files or folders, and you can submit a file for analysis.

Scanning now

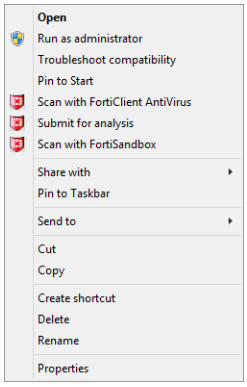
1. On the *Malware Protection* tab, go to *AntiVirus Protection*.
2. Beside the *Scan Now* button, use the dropdown list to select *Quick Scan*, *Full Scan*, *Custom Scan*, or *Removable media Scan*.

Quick Scan	Runs the rootkit detection engine to detect and remove rootkits. It looks for threats by scanning executable files, DLLs, and drivers that are currently running.
Full Scan	Runs the rootkit detection engine to detect and remove rootkits. It then looks for threats by performing a full system scan on all files, executable files, DLLs, and drivers.

Custom Scan	Runs the rootkit detection engine to detect and remove rootkits. It allows you to select a specific file folder on your local hard disk drive (HDD) to scan for threats.
Removable Media Scan	Runs the rootkit detection engine to detect and remove rootkits. It scans all connected removable media, such as USB drives.

Scanning files or folders

Right-click the file or folder and select *Scan with FortiClient AntiVirus* from the menu.



Submitting files to FortiGuard for analysis

You can send up to five files a day to FortiGuard for analysis.

You do not receive feedback for files submitted for analysis. The FortiGuard team can create signatures for any files that are submitted for analysis and determined to be malicious.

1. On your workstation, right-click a file or executable, and select *Submit for analysis* from the menu. A dialog displays that identifies the number of files submitted.
2. Confirm the location of the file that you want to submit, and click the *Submit* button.

Viewing AntiVirus scan results

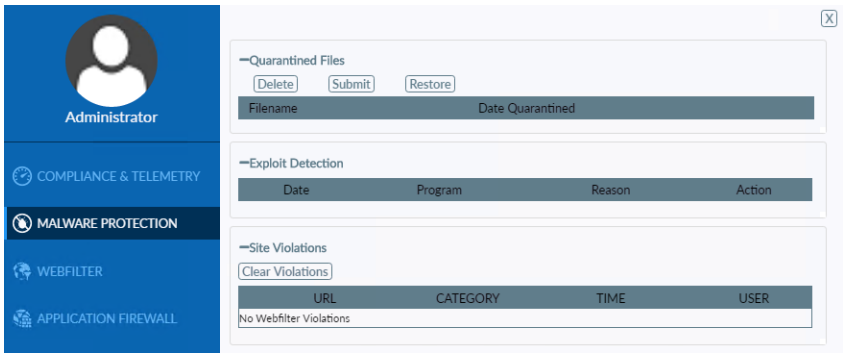
You can view quarantined threats, site violations, alerts, and RTP events.

For details on viewing quarantined threats, see Viewing quarantined files on page 47.

Viewing site violations

On the *Site Violations* page, you can view site violations and submit sites to be recategorized.

1. On the *Malware Protection* tab, click *X Threats Detected*.



Site Violations displays the following options:

URL	Website URL.
CATEGORY	Web filter category the site belongs to.
TIME	Date and time of the site violation.
USER	User who attempted to access the site.

2. Click *Close*.

Viewing alerts

When FortiClient AV detects a virus while attempting to download a file via a web browser, a warning displays.

Select *View recently detected virus(es)* to collapse the virus list. Right-click a file in the list to access the following context menu:

Delete	Delete a quarantined or restored file.
Quarantine	Quarantine a restored file.
Restore	Restore a quarantined file.
Submit Suspicious File	Submit a file to FortiGuard as a suspicious file.
Submit as False Positive	Submit a quarantined file to FortiGuard as a false positive.
Add to Exclusion List	Add a restored file to the exclusion list. Any files in the exclusion list are not scanned.
Open File Location	Open the file location on your workstation.

Depending on the settings received from EMS, virus alert dialog may or may not display when you attempt to download a virus in a web browser.

Viewing RTP events

When an AV RTP event has occurred, you can view these events in FortiClient.

1. From the *Malware Protection* tab, select *Threats Detected*.
2. Select *Real-time Protection events (x)*.
   The `realtime_scan.log` opens in the default viewer.
   Example log output:

```
Realtime scan result:
time: Wed Jan 9 09:52:18 2019, Realtime Protection Started, AV_ENGINE:6.00012 MDARE_
     ENGINE:2.00068 AV_SIG:1.00000 AV_EXT_SIG:1.00000 MDARE_SIG:1.00000
time: Wed Jan 9 09:52:42 2019, virus found: EICAR_TEST_FILE, action: Quarantined,
     C:\Users\Administrator\Downloads\5adfd0ce-278a-4697-8a97-624b307df63c.tmp
```

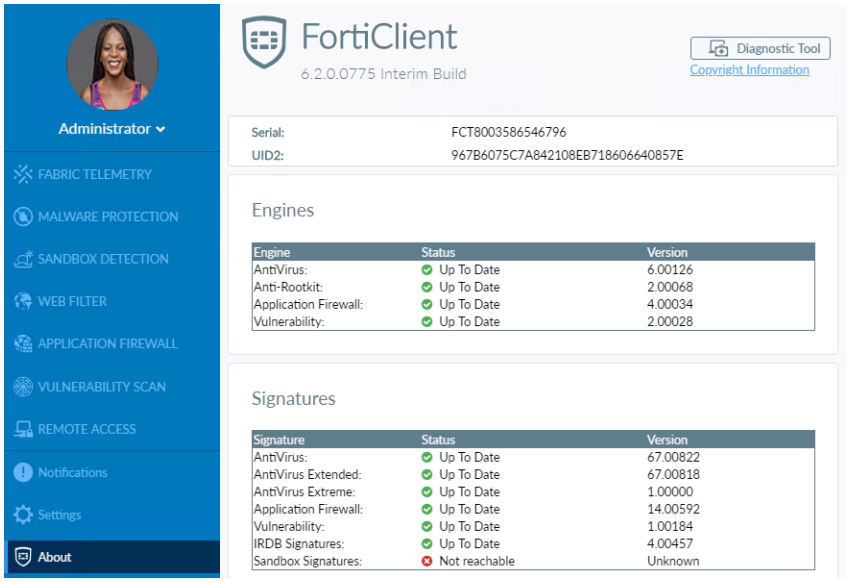
Viewing FortiClient engine and signature versions

You can view the current FortiClient version, engine, and signature information.

When EMS manages FortiClient, you can use a FortiManager or Micro-FortiGuard Server for FortiClient for FortiClient software and signature updates. When configuring the profile using EMS, select *Use FortiManager for client software/signature updates* to enable the feature, and enter your FortiManager's IP address. You can failover to FDN when FortiManager or Micro-FortiGuard Server for FortiClient is unavailable.

To view FortiClient engine and signature versions:

1. Go to *About*.



2. Hover the mouse over the *Status* field to see the date and time FortiClient last updated the selected item.
3. Click *Close*.

Cloud Based Malware Protection

The cloud-based malware protection feature helps protect endpoints from high risk file types from external sources such as the Internet or network drives by querying FortiGuard to determine whether files are malicious. The following describes the process for cloud-based malware protection:

1. A high risk file is downloaded or executed on the endpoint.
2. FortiClient generates a SHA1 checksum for the file.
3. FortiClient sends the checksum to FortiGuard (FQDN with port 8888) to determine if it is malicious against the FortiGuard checksum library.
4. If the checksum is found in the library, FortiGuard communicates to FortiClient that the file is deemed malware. By default, FortiClient quarantines the file.

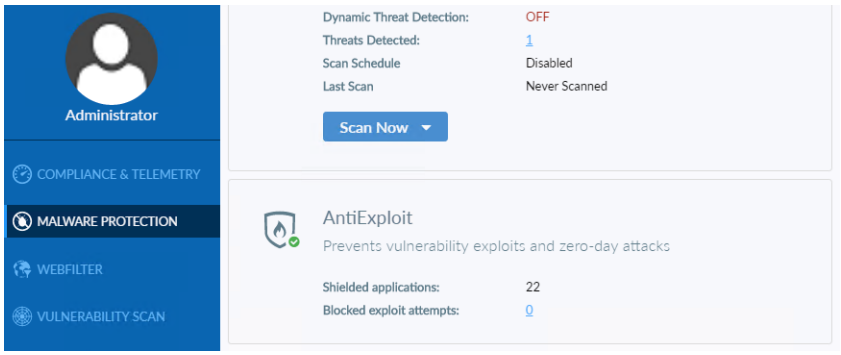
This feature only submits high risk file types such as .exe, .doc, .pdf, and .dll to FortiGuard. The list of high risk file types is the same as the list of file types submitted to Sandbox by default. See the *FortiClient EMS Administration Guide* for details.

For details on seeing quarantined files, see Viewing quarantined files on page 47.

AntiExploit

The anti-exploit detection feature helps protect vulnerable endpoints from unknown exploit attacks. FortiClient monitors the behavior of popular applications, such as web browsers (Internet Explorer, Chrome, Firefox, Opera), Java/Flash plugins, Microsoft Office applications, and PDF readers, against exploits that use zero-day or unpatched vulnerabilities to infect the endpoint. Once detected, the compromised application process is terminated. The anti-exploit detection feature also helps protect against memory-based attacks and drive-by download attacks. It also detects and blocks unknown and known exploit kits. It is a signature-less solution.

You can view the number and list of applications that FortiClient is protecting from evasive exploits. On the *Malware Protection* tab, under *AntiExploit*, the number of protected applications displays. You can view the list of application names on the *Malware Protection Settings* page.

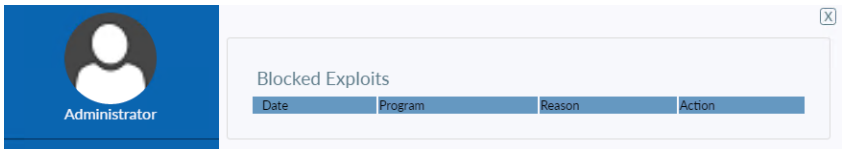


The anti-exploit detection feature is available only for FortiClient (Windows).

Viewing detected exploit attempts

You can view the exploit attempts FortiClient has blocked. See .

1. On the *Malware Protection* tab, click *Blocked exploit attempts*.
   In this page you can view the date and description of a blocked exploit attempt.



   This page displays the following information:

Date	Date of the detected exploit attempt.
Program	Program that attempted the detected exploit attempt.
Reason	Reason the detected exploit attempt was blocked.
Action	Action FortiClient took in response to the detected exploit attempt.

2. Click *Close*.

Viewing applications protected from exploits

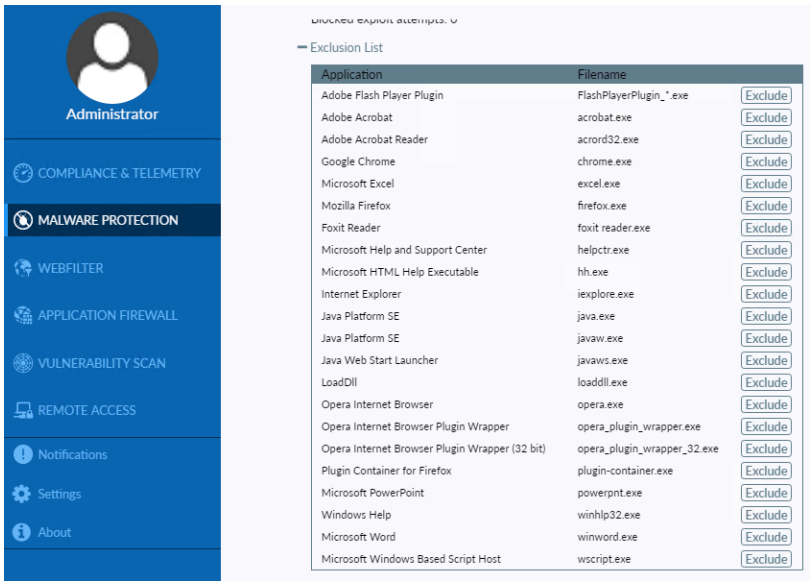
When you view the list of applications, you can use the following button names to determine which applications are protected from exploits:

- The applications with an *Exclude* button beside their names are protected from evasive exploits.
- The applications with an *Unexclude* button beside their names are not protected from evasive exploits. You can protect the application by clicking the *Unexclude* button. See .

See Viewing detected exploit attempts on page 45.

From the *Malware Protection* tab, click the *Settings* icon. Scroll to *AntiExploit* and expand the *Exclusion List*.

The list of protected applications displays.



Evaluating the anti-exploit detection feature

The anti-exploit detection feature blocks malicious content from exploiting vulnerabilities in applications. To test or verify this feature, you can use the Metasploit Framework module. This module requires Windows 7 x86, Firefox, and Adobe Flash Player.

Consider running the exploit with and without enabling the anti-exploit detection feature in FortiClient. FortiClient blocks such an exploit and displays a bubble message in FortiTray to notify the endpoint user.

In newer product versions, vendors resolve most publicly announced exploits. The FortiClient Vulnerability Scan feature can identify, report, and apply patches for supported applications. See Vulnerability Scan on page 55.

Removable media access

FortiClient controls access to removable media devices, such as USB drives. FortiClient can allow, block, or monitor access to removable media devices, as configured by the EMS administrator.

Quarantined files

Various features on the *Malware Protection* tab can quarantine files that pose a threat to the endpoint. This section describes viewing the quarantined files and the actions you can take with the quarantined files:

- Viewing quarantined files on page 47
- Submitting quarantined files for scanning on page 48

Viewing quarantined files

To view quarantined files:

1. On the *Malware Protection* tab, click *Threats Detected*. This option is available under *AntiVirus Protection* and *Cloud Based Malware Protection*. You can also click *Zero-Day* on the *Sandbox Detection* tab.
   You can view the original file location, virus name, and logs, and submit the suspicious file to FortiGuard. You cannot restore or delete the quarantined file.
   FortiClient organizes quarantined files into the following sections:
   - *Quarantined Files*: files that AntiVirus Protection has quarantined
   - *Cloud Protection Quarantined Files*: files that Cloud Based Malware Protection has quarantined
   - *Sandbox Quarantined Files*: files that Sandbox Detection has quarantined
2. The following information displays:

Filename	Names of the quarantined files.
Date Quarantined	Dates and time the files were quarantined.

3. Select a file from the list to view detailed information about the file and click *Details*.

Submit	Click submit for FortiGuard analysis.
Filename	Name of the quarantined file.
Original Location	Location of the file before scanning.
Date Quarantined	Date and time the file was quarantined.
Submitted	Displays *Not Submitted* when the selected file has not been submitted to FortiGuard for analysis by clicking the *Submit* button. Displays *Submitted* after clicking the *Submit* button.
Status	Status of the file, such as *Quarantined*.
Virus Name	Name of the detected virus.
Quarantined File Name	Name of the file after it was quarantined.
Log File Location	Location of the log file for the scan.
Quarantined By	FortiClient feature that quarantined the file.
Close	Click to close the details dialog.

4. Click *Close*.

FortiClient sends quarantined file information to EMS. If the EMS administrator whitelists the file (in the case of a false positive), EMS sends the whitelist information to FortiClient. After FortiClient receives the whitelist information, it releases the file from quarantine. See the *FortiClient EMS Administration Guide* for details.

Submitting quarantined files for scanning

To submit quarantined files to FortiSandbox for scanning:

1. On the *Malware Protection* tab, click *Threats Detected*. This option is available under *AntiVirus Protection* and *Cloud Based Malware Protection*. You can also click *Zero-Day* on the *Sandbox Detection* tab.
2. Select the file and click *Submit*.

Sandbox Detection

FortiClient supports integration with FortiSandbox, including on-premise FortiSandbox appliances and FortiSandbox Cloud. When configured, FortiSandbox automatically scans files downloaded on the endpoint or from removable media attached to the endpoint or mapped network drives. FortiClient also automatically scans files downloaded with an email client on the endpoint or from the Internet. In each case, if the file is not detected locally, and FortiSandbox integration is configured, FortiClient sends the file to the FortiSandbox for further analysis. Endpoint users can also manually submit files to FortiSandbox for scanning.

You can block access to files until FortiClient returns the FortiSandbox scanning result.

When scanning is complete, FortiClient can quarantine/deny access to infected files or alert and notify the endpoint user of infected files without quarantining the files. If FortiSandbox sends a verdict to FortiClient indicating that the file is malicious, FortiClient also sends the results to EMS.

As FortiSandbox receives files for scanning from various sources, it collects and generates AV signatures for such samples. FortiClient periodically downloads the latest AV signatures from FortiSandbox, and applies them locally to all realtime and on-demand AV scanning.

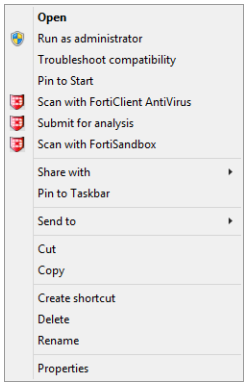
FortiClient can send a maximum of 300 files daily to FortiSandbox Cloud. If multiple files are submitted around the same time, FortiClient sends one file to FortiSandbox Cloud, waits until it receives the verdict for that file, then sends the next file to FortiSandbox Cloud.

If configured by the EMS administrator, FortiClient submits files with specified extensions to FortiSandbox. See the *FortiClient EMS Administration Guide* for details.

Scanning with FortiSandbox on-demand

You can send files to FortiSandbox for scanning on-demand when FortiSandbox is enabled and online.

Right-click a file and select *Scan with FortiSandbox* from the menu.



Viewing FortiSandbox scan results

Go to the *Sandbox Detection* tab. The following information displays:

Submitted	Displays the number of files submitted to FortiSandbox for scanning.
Zero-day	Displays the number of detected zero-day files. Click to view details about the files.
Clean	Displays the number of files determined clean after FortiSandbox scanning.
Pending	Displays the number of files waiting for FortiSandbox scanning.

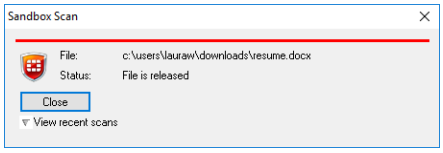
The *Zero-day File Details* section displays the name, status, and date and time quarantined for each zero-day file. Click a file to view the following information:

Original Location	Original location of the file on the local machine.
Submission Type	Whether the file was submitted to FortiGuard.
Virus Name	Name of the detected virus.
Quarantined File Name	Name of the quarantined file.

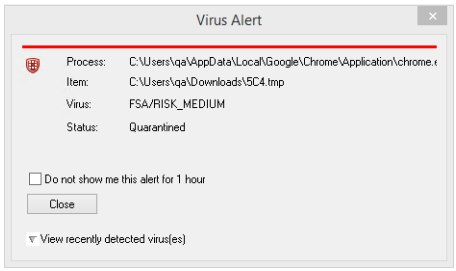
For details on viewing quarantined files, see Quarantined files on page 46.

Using the popup window

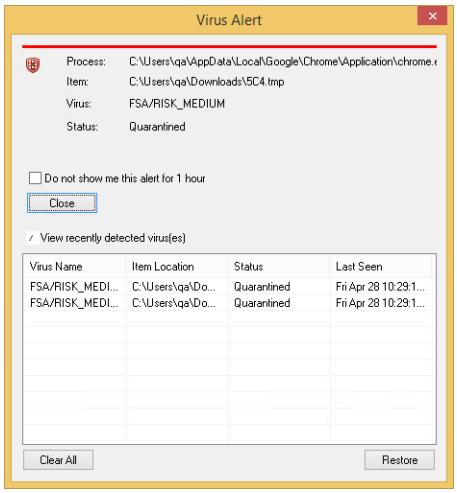
As FortiSandbox scans and releases files, a popup displays to inform you. You can view the recent scans by clicking the *View recent scans* option.



When FortiSandbox detects a virus and quarantines a file, the *Virus Alert* window displays.



You can use the *Virus Alert* window to view information about the recently scanned files by clicking the *View recently detected virus(es)* option.


Virus Alert
Process: C:\Users\qa\AppData\Local\Google\Chrome\Application\chrome.
Item: C:\Users\qa\Downloads\5C4.tmp
Virus: FSA/RISK_MEDIUM
Status: Quarantined
Do not show me this alert for 1 hour
Close
View recently detected virus(es)
Virus Name
Item Location
Status
Last Seen
FSA/RISK_MEDI...
C:\Users\qa\Do...
Quarantined
Fri Apr 28 10:29:1...
FSA/RISK_MEDI...
C:\Users\qa\Do...
Quarantined
Fri Apr 28 10:29:1...
Clear All
Restore

Web Filter

Web Filter allows you to block, allow, warn, and monitor web traffic based on URL category or custom URL filters. FortiGuard handles URL categorization. You can create a custom URL filter exclusion list that overrides the FortiGuard category.

If FortiClient is unable to contact FortiGuard, FortiClient blocks all web traffic by default. To configure FortiClient to allow web traffic when FortiGuard is unreachable, see the *FortiClient XML Reference Guide*.

Web browser plugin for HTTPS web filtering

The EMS administrator can enable a web browser plugin for HTTPS web filtering on the endpoint. This improves detection and enforcement of Web Filter rules on HTTPS sites. After this option is enabled, you must open the browser to approve installing the new plugin.

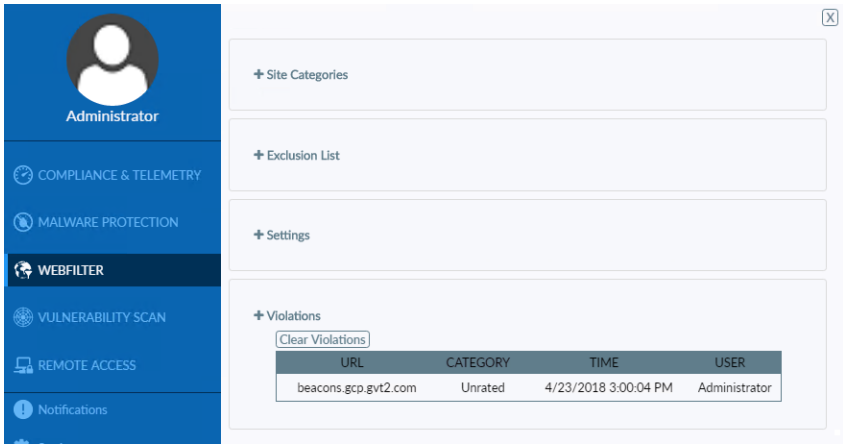
The web browser plugin is only supported for the Google Chrome browser on Windows platforms.

Viewing violations

You can view web filtering violations in FortiClient.

On the *Web Filter* tab, click the *Settings* icon.

Alternately, you can click *Sites Blocked (in last 7 days)*.

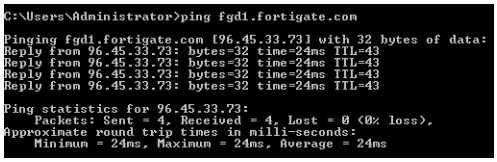


The following information displays under *Violations*.

URL	Website URL.
Category	Website subcategory.
Time	Date and time the website was accessed.
User	Name of the user generating the traffic. Hover the cursor over the column to view the complete entry in the popup bubble message.

Troubleshooting Web Filter

If Web Filter is not functioning as configured, this may be because FortiClient cannot contact FortiGuard. Open Command Prompt and run `ping fgd1.fortigate.com`. If FortiClient can contact FortiGuard, it should output the following:



If you have confirmed that FortiClient can contact FortiGuard but Web Filter still does not work as configured, ensure the necessary ports are open. FortiClient requires port 8888 or 53 to be open for FortiGuard URL rating. See Required services and ports on page 17.

Application Firewall

FortiClient can recognize the traffic generated by a large number of applications.

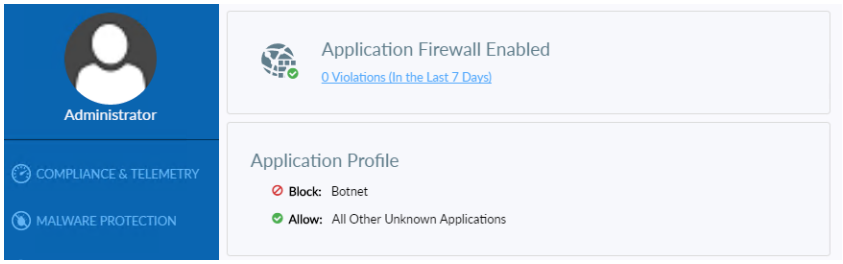
Viewing blocked applications

On the *Application Firewall* tab, click the *<number> Violations (In the Last 7 Days)* link.

A page of all blocked applications displays.

Viewing application firewall profiles

You can view the application firewall profile on the *Application Firewall* tab.



Vulnerability Scan

FortiClient includes a vulnerability scan component to check endpoints for known vulnerabilities. The vulnerability scan results can include:

- List of vulnerabilities detected
- How many detected vulnerabilities are rated as critical, high, medium, or low threats
- Links to more information, including links to the FortiGuard Center
- One-click link to install patches and resolve as many identified vulnerabilities as possible
- List of patches that require manual installation to resolve vulnerabilities

FortiClient can detect known vulnerabilities for many software. For the software list, see Vulnerability patches on page 88.

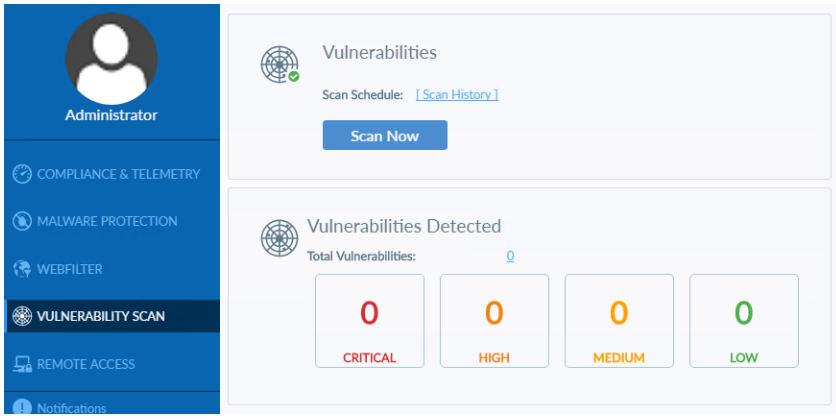
Vulnerability scan provides EMS with a list of all software installed on the endpoint, including vendor and version information. See the *FortiClient EMS Administration Guide*.

Scanning on-demand

You can scan on-demand. When the scan is complete, FortiClient displays a summary of vulnerabilities found on the endpoint. If any detected vulnerabilities require you to manually install remediation patches, the list of affected software also displays.

To scan on-demand:

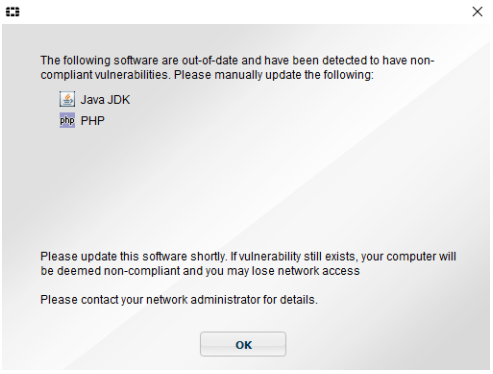
1. On the *Vulnerability Scan* tab, click the *Scan Now* button.



FortiClient scans the endpoint for known vulnerabilities, and a summary of vulnerabilities found on the system displays.

If any detected vulnerabilities require you to manually install remediation patches, a dialog displays that informs you what software should be updated. If you fail to update the identified software, you may lose access to the

network. If you lose access to the network, contact your system administrator for assistance. Following is an example of the dialog:



2. If applicable, read the list of software that requires manual installation of software patches, and click *OK*. See Manually fixing detected vulnerabilities on page 58.

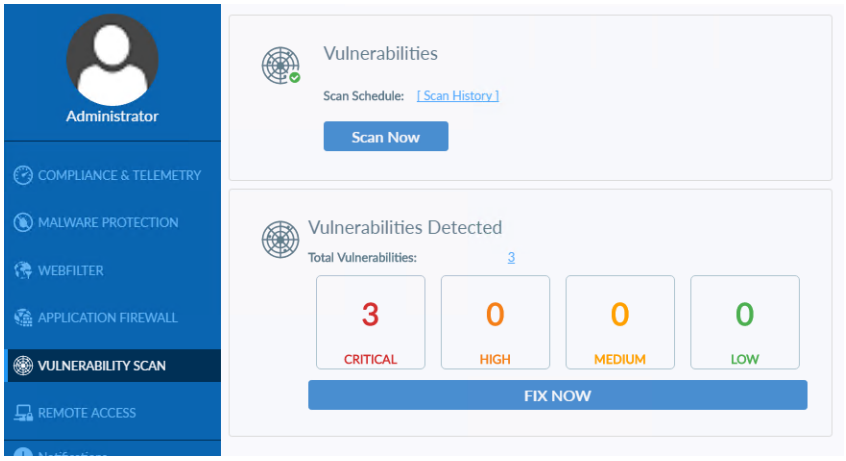
Automatically fixing detected vulnerabilities

The *Vulnerability Scan* tab identifies vulnerabilities on the endpoint that should be fixed by installing software patches. You can automatically install software patches by clicking the *Fix Now* link or review detected vulnerabilities before installing software patches.

Any software patches that cannot be automatically installed are listed on the *Vulnerability Scan* tab and you should manually download and install software patches for the vulnerable software.

You may be unable to automatically fix vulnerabilities. An administrator may have the vulnerabilities automatically fixed for you.

On the *Vulnerability Scan* tab, under *Vulnerabilities Detected*, click *Fix Now* to automatically install software patches to fix the detected vulnerabilities.

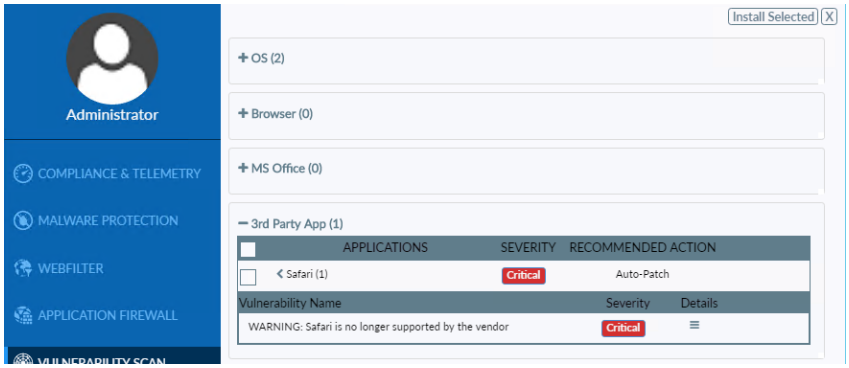


FortiClient installs the software patches. You may need to reboot the endpoint to complete installation.

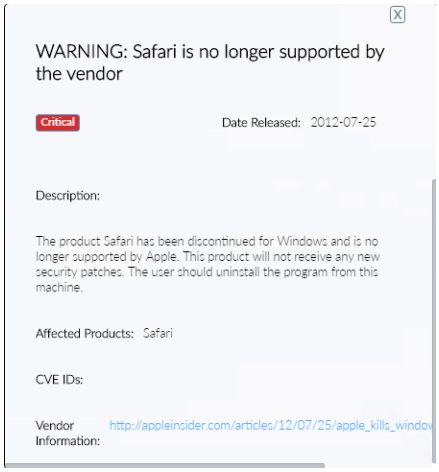
Reviewing detected vulnerabilities before fixing

To review detected vulnerabilities before fixing:

1. In the *Vulnerability Scan* tab, beside *Vulnerabilities Detected*, click the *<number>* link to review information about vulnerabilities before installing patches.
   A page of details displays.
2. Click each category with vulnerabilities to view its details. For example, click the *3rd Party App* category to view details about detected third party application vulnerabilities.



3. Expand the application to view its vulnerabilities.
4. Click the *Details* icon for each vulnerability to view its details and click *Close* to close the detailed view.



5. In each category, select the checkbox for the software for which you want to install patches.
   For example, in the *OS* category, expand *Operating System*, and select the checkbox beside the vulnerabilities for which you want to install patches.
   You may be unable to choose which patches to install, depending on your FortiClient configuration. You are also unable to select the checkbox for any software that requires manual installation of patches.
6. Click the *Install Selected* button to install patches.
   FortiClient installs the patches. You may need to reboot the endpoint to complete installation.

Manually fixing detected vulnerabilities

In some cases, FortiClient cannot automatically install software patches, and you must manually download and install software patches. After each scan, the *Vulnerability Scan* tab lists any software that requires you to manually download and install software patches. See also Scanning on-demand on page 55.

If a software vendor has ceased to provide patches for its software, the software is tagged as obsolete in the signatures used by the Vulnerability Scan feature, and you must uninstall the software to fix detected vulnerabilities. The obsolete tag is visible in the details. See Viewing details about vulnerabilities on page 58.

To manually fix detected vulnerabilities:

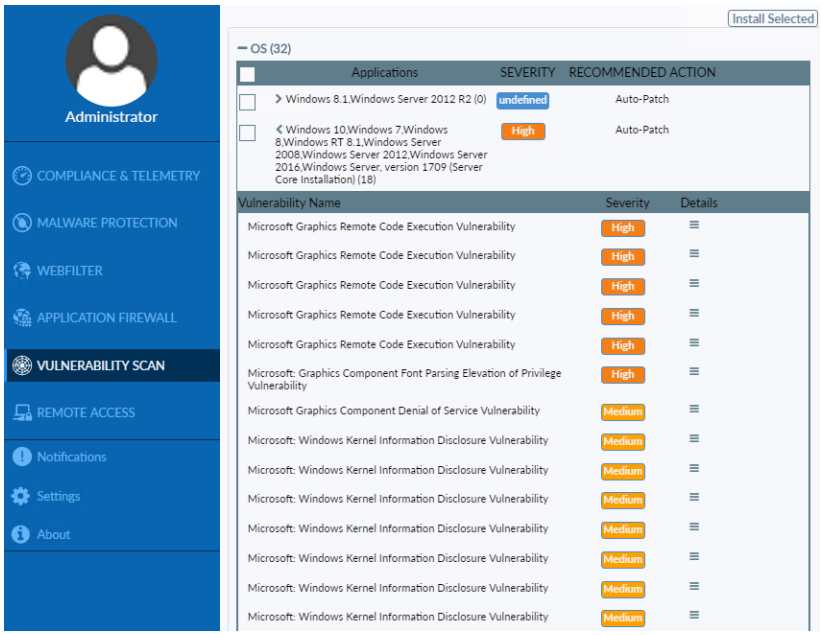
1. On the *Vulnerability Scan* tab, identify the software that requires manual fixing.
   Any software with detected vulnerabilities that requires you to manually download and install software patches is displayed in the *Vulnerabilities Detected* area.
2. Download the latest software patch for each software from the Internet, and install it on the endpoint.
3. After you install the software for all remaining vulnerabilities, go to the *Vulnerability Scan* tab, and click the *Scan Now* button to instruct FortiClient to confirm the vulnerabilities are fixed.
   If the manual fixes were successful, the *Vulnerability Scan* tab displays *Vulnerabilities Detected: None* after the scan completes.

Viewing details about vulnerabilities

To view details about vulnerabilities:

1. On the *Vulnerability Scan* tab, any software with detected vulnerabilities that requires you to manually download and install software patches displays in the *Vulnerabilities Detected* area.
2. View more details on all vulnerabilities by clicking the number of total vulnerabilities detected.
3. Expand the desired section. Vulnerabilities are divided into *OS, Browser, MS Office, 3rd Party App, Service, User Config*, and *Others*.

4. Expand the desired application. Click the *Details* icon beside the desired vulnerability.



If the detected vulnerability requires you to manually download and install a fix, it is communicated in the *Recommended Action* section. In addition, the following information may display: *The fix for the vulnerability must be manually installed from: <link>*.

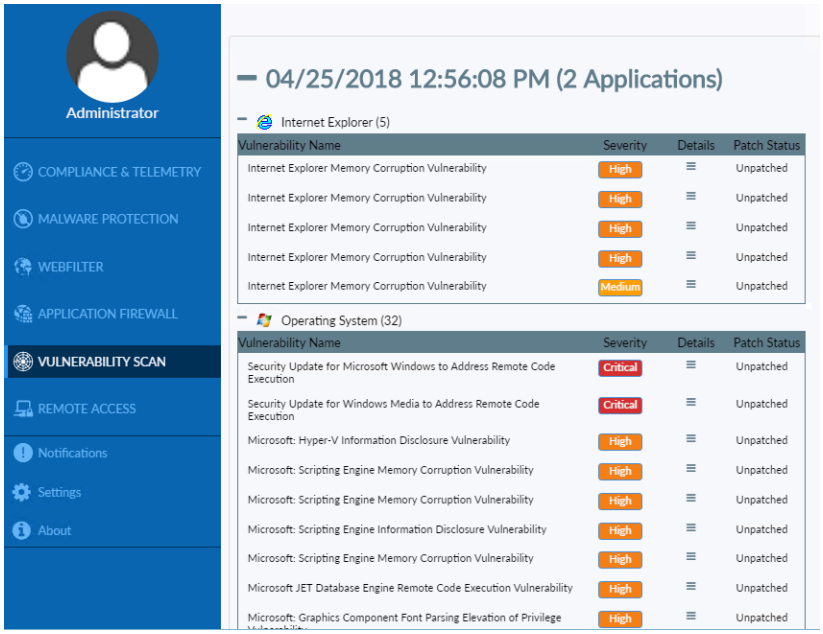
5. Click *Close*.

Viewing vulnerability scan history

You can view the history of the last seven vulnerability scans and patches. You can view the history to see what software was identified as vulnerable and whether patches for the vulnerabilities were installed.

To view vulnerability scan history:

1. In FortiClient, click the *Vulnerability Scan* tab.
2. Click *Scan History*. The vulnerability patch history displays by date. Click each date and software name to expand it and view details or contract it and hide details.



3. Click *Close* to return to the *Vulnerability Scan* tab.

Remote Access

FortiClient supports both IPsec and SSL VPN connections to your network for remote access. Administrators can use EMS to provision VPN configurations for FortiClient and endpoint users can configure new VPN connections using FortiClient.

When configuring and forming VPN connections, note that in FortiClient the user password is saved only for the user who entered it. It is not accessible in FortiClient to the device's other users. All other information is visible in FortiClient when other users are logged into the same device.

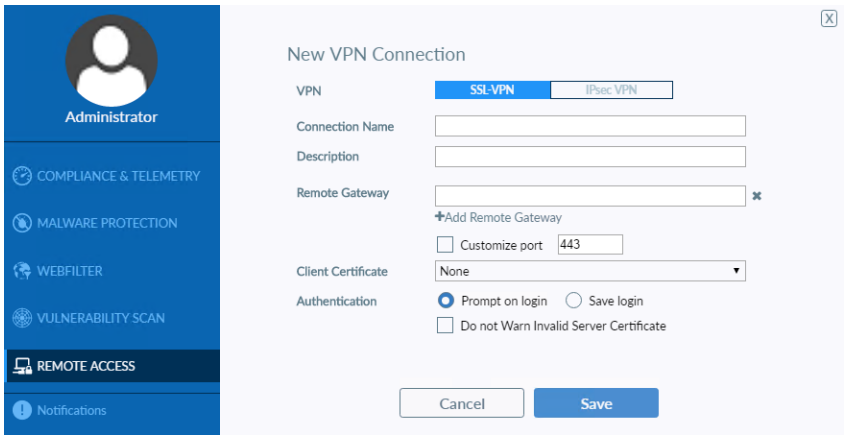
Configuring VPN connections

You can configure SSL and IPsec VPN connections using FortiClient.

Configuring an SSL VPN connection

To configure an SSL VPN connection:

1. On the *Remote Access* tab, click *Configure VPN*.



2. Select *SSL-VPN*, then configure the following settings:

Connection Name	Enter a name for the connection.
Description	(Optional) Enter a description for the connection.
Remote Gateway	Enter the remote gateway's IP address/hostname. You can configure multiple remote gateways by separating each entry with a semicolon. If one gateway is not available, the VPN connects to the next configured gateway.
Customize port	Change the port. The default port is 443.
Client Certificate	Select *Prompt on connect* or the certificate from the dropdown list.
Authentication	Select *Prompt on login* or *Save login*. The *Disable* option is available when *Prompt on connect* or a certificate is configured for *Client Certificate*.
Username	If you selected *Save login*, enter the username to save for the login.
Do not Warn Invalid Server Certificate	Select if you do not want to be warned if the server presents an invalid certificate.
+	Select the add icon to add a new connection.
-	Select a connection and then select the delete icon to delete a connection.

3. Click *Save* to save the VPN connection.

FortiClient supports split DNS tunneling for SSL VPN portals, which allows you to specify which domains the DNS server specified by the VPN resolves, while the DNS specified locally resolves all other domains. This requires configuring split DNS support in FortiOS.

If using FortiClient on a Windows Server 2016 machine, ensure that you disable IE Enhanced Security. Otherwise, SSL VPN may not function as configured.

Configuring an IPsec VPN connection

To configure an IPsec VPN connection:

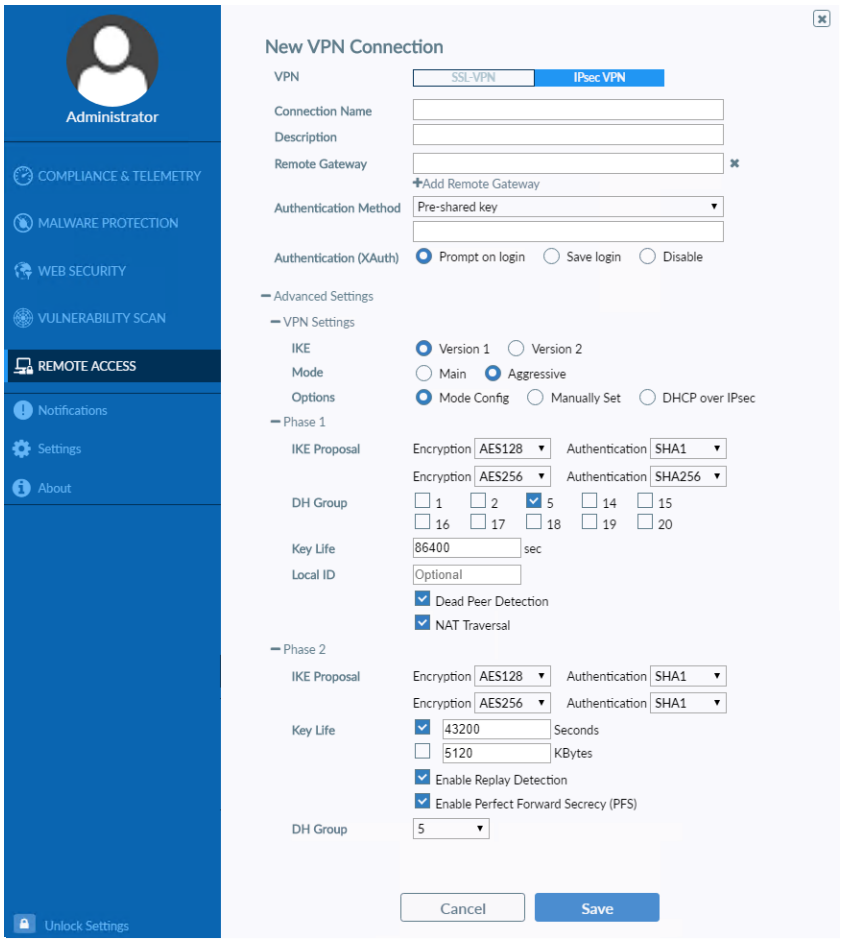
1. On the *Remote Access* tab, click *Configure VPN*.
2. Select *IPsec VPN*, then configure the following settings:

Connection Name	Enter a name for the connection.
Description	(Optional) Enter a description for the connection.
Remote Gateway	Enter the IP address/hostname of the remote gateway. You can configure multiple remote gateways. If one gateway is not available, the VPN connects to the next configured gateway.

Authentication Method	Select *X.509 Certificate* or *Pre-shared Key* in the dropdown list. When you select *x.509 Certificate*, select *Prompt on connect* or a certificate from the list.
Authentication (XAuth)	Select *Prompt on login*, *Save login*, or *Disable*. Available if IKE version 1 is selected.
Authentication (EAP)	Select *Prompt on login*, *Save login*, or *Disable*. Available if IKE version 2 is selected.
Username	If you selected *Save login*, enter the username to save for the login.
Advanced Settings	Configure VPN settings, phase 1, and phase 2 settings.
VPN Settings	
IKE	Select Version 1 or Version 2.
Mode	Available if IKE version 1 is selected. Select one of the following: • *Main*: Phase 1 parameters are exchanged in multiple rounds with encrypted authentication information. • *Aggressive*: Phase 1 parameters are exchanged in a single message with authentication information that is not encrypted. Although *Main* mode is more secure, you must select *Aggressive* mode if there is more than one dialup phase 1 configuration for the interface IP address, and the remote VPN peer or client is authenticated using an identifier (local ID).
Options	Select one of the following: • *Mode Config*: IKE Mode Config can configure host IP address, domain, DNS and WINS addresses. • *Manually Set*: Manual key configuration. If one of the VPN devices is manually keyed, the other VPN device must also be manually keyed with the identical authentication and encryption keys. Enter the DNS server IP address and the IP address and subnet values to assign. Select the checkbox to enable split tunneling. • *DHCP over IPsec*: DHCP over IPsec can assign an IP address, domain, DNS and WINS addresses. Select the checkbox to enable split tunneling.
Phase 1	Select the encryption and authentication algorithms used to generate keys for protecting negotiations and add encryption and authentication algorithms as required. You need to select a minimum of one and a maximum of two combinations. The remote peer or client must be configured to use at least one of the proposals that you define.
IKE Proposal	Select symmetric-key algorithms (encryption) and message digests (authentication) from the dropdown lists.

	DH Group	Select one or more Diffie-Hellman groups from DH group 1, 2, 5, 14, 15, 16, 17, 18, 19 and 20. At least one of the DH group settings on the remote peer or client must match one the selections on the FortiGate unit. Failure to match one or more DH groups results in failed negotiations.
	Key Life	Enter the time (in seconds) that must pass before the IKE encryption key expires. When the key expires, a new key is generated without interrupting service. The key life can be from 120 to 172,800 seconds.
	Local ID	Enter the local ID (optional). This local ID value must match the peer ID value given for the remote VPN peer's peer options.
	Dead Peer Detection	Select this checkbox to reestablish VPN tunnels on idle connections and clean up dead IKE peers if required.
	NAT Traversal	Select the checkbox if a NAT device exists between the client and the local FortiGate unit. The client and the local FortiGate unit must have the same NAT traversal setting (both selected or both cleared) to connect reliably.
Phase 2		Select the encryption and authentication algorithms that are proposed to the remote VPN peer. You can specify up to two proposals. To establish a VPN connection, at least one of the proposals you specify must match configuration on the remote peer.
	IKE Proposal	Select symmetric-key algorithms (encryption) and message digests (authentication) from the dropdown lists.
	Key Life	The *Key Life* setting sets a limit on the length of time that a phase 2 key can be used. The default units are seconds. Alternatively, you can set a limit on the number of kilobytes (KB) of processed data, or both. If you select both, the key expires when the time has passed or the number of KB have been processed. When the phase 2 key expires, a new key is generated without interrupting service.
	Enable Replay Detection	Replay detection enables the unit to check all IPsec packets to see if they have been received before. If any encrypted packets arrive out of order, the unit discards them.
	Enable Perfect Forward Secrecy (PFS)	Select the checkbox to enable perfect forward secrecy (PFS). PFS forces a new Diffie-Hellman exchange when the tunnel starts and whenever the phase 2 key life expires, causing a new key to be generated each time.
	DH Group	Select one Diffie-Hellman (DH) group (1, 2, 5, 14, 15, 16, 17, 18, 19 or 20). This must match the DH group the remote peer or dialup client uses.
+		Select the add icon to add a new connection.

-	Select a connection and then select the delete icon to delete a connection.



3. Click *Save* to save the VPN connection.

Connecting VPNs

You can connect VPN tunnels to FortiGate:

Connecting to SSL or IPsec VPN

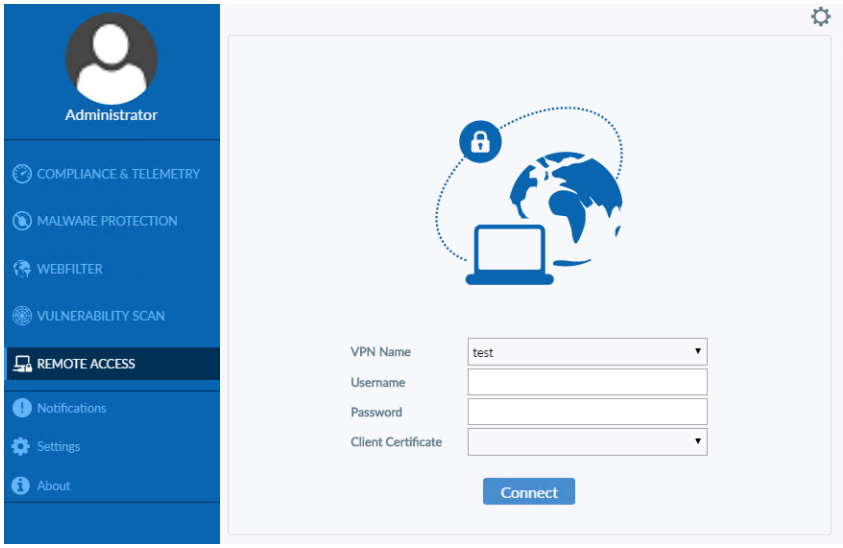
Depending on the FortiClient configuration, you may also have permission to edit an existing VPN connection and delete an existing VPN connection.

Internet Explorer's SSL and TLS settings should be the same as those on the FortiGate.

To connect to SSL or IPsec VPN:

1. On the *Remote Access* tab, select the VPN connection from the dropdown list.
   Optionally, you can right-click the FortiTray icon in the system tray and select a VPN configuration to connect.

   Provisioned VPN connections are listed under *Corporate VPNs*. Locally configured VPN connections are listed under *Personal VPNs*.

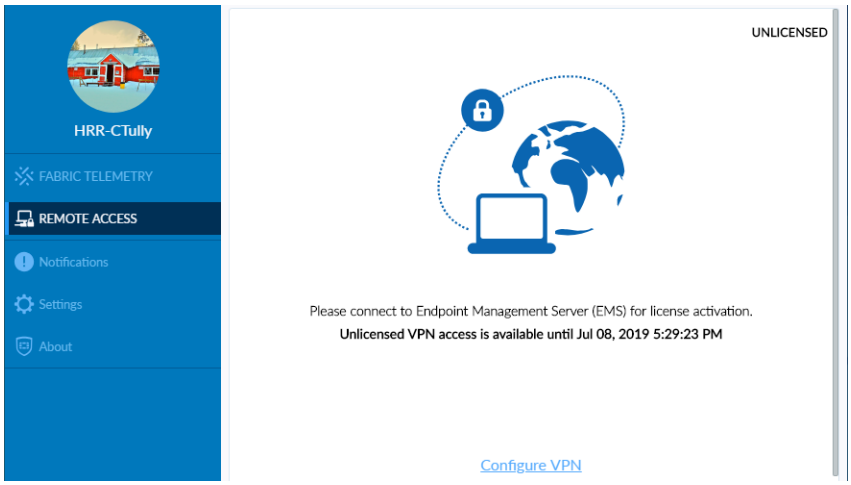


2. Enter your username and password.
3. If a certificate is required, select a certificate. If the VPN tunnel was configured to require a certificate, you must select a certificate. If no certificate is required, the option is hidden in FortiClient. Your administrator may have configured FortiClient to automatically locate a certificate for you.
4. Click the *Connect* button. Depending on the configuration received from EMS, you may also need to accept a disclaimer message to establish the connection.
   When connected, FortiClient displays the connection status, duration, and other relevant information. You can now browse your remote network. Click the *Disconnect* button when you are ready to terminate the VPN session.

Free three-day VPN access

For three days after initial FortiClient installation, you can configure and establish a VPN connection to a FortiGate, allowing the endpoint to reach an EMS behind a FortiGate. This is especially useful for remote users, as it allows them to connect to the corporate network to activate their FortiClient license.

The following shows the FortiClient GUI in this scenario. You can see that the user can access the VPN feature until July 8, 2019, meaning that they initially installed FortiClient three days earlier, on July 5, 2019. If the user does not use a VPN tunnel to activate their FortiClient license by 5:29 PM on July 8, as shown, FortiClient revokes the VPN access and all FortiClient features, including VPN, stop working.



Following successful registration to EMS, FortiClient receives a full license if available from EMS. EMS enables all FortiClient features configured on the assigned endpoint profile.

If FortiClient was registered to EMS and licensed for VPN, then becomes unregistered, the free three-day VPN access becomes available again.

If FortiClient goes offline after registering to EMS, FortiClient features remain enabled for 30 days. You can still establish a VPN connection to the FortiGate in this scenario.

Connecting VPN with FortiToken Mobile

VPN connections may require network authentication that uses a token from FortiToken Mobile, an application that runs on Android and iOS devices. For information about FortiToken Mobile, see the Fortinet Document Library.

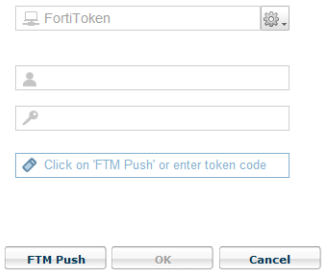
You can configure FortiGate to let you push a token from FortiToken Mobile to FortiGate to complete network authentication when connecting VPNs. When configured, you can select the push token option by clicking the *FTM Push* button in FortiClient. This notifies the FortiGate that you choose to use the push token option. Following this, you receive a notification of the authentication request on your device that has FortiToken Mobile installed. On your device, you can tap the notification and follow the instructions to allow or deny the authentication requests

If a push token is not configured, you must enter a token code from FortiToken Mobile into FortiClient when connecting VPNs.

You must have available the device with FortiToken Mobile installed to complete this procedure.

To connect VPN with FortiToken Mobile using push notifications:

1. On the *Remote Access* tab, select the VPN connection from the dropdown list.
2. Enter your username and password and click the *Connect* button. The *Click on 'FTM Push' or enter token code* box displays.



3. Click *FTM Push*. Your device with FortiToken Mobile installed receives a notification.
4. On your device with FortiToken Mobile installed, tap the notification and follow the instructions to allow the authentication request and complete network authentication without typing the token code. You can also deny the authentication request, or do nothing and let the notification request expire.

To connect VPN with FortiToken Mobile by typing token codes:

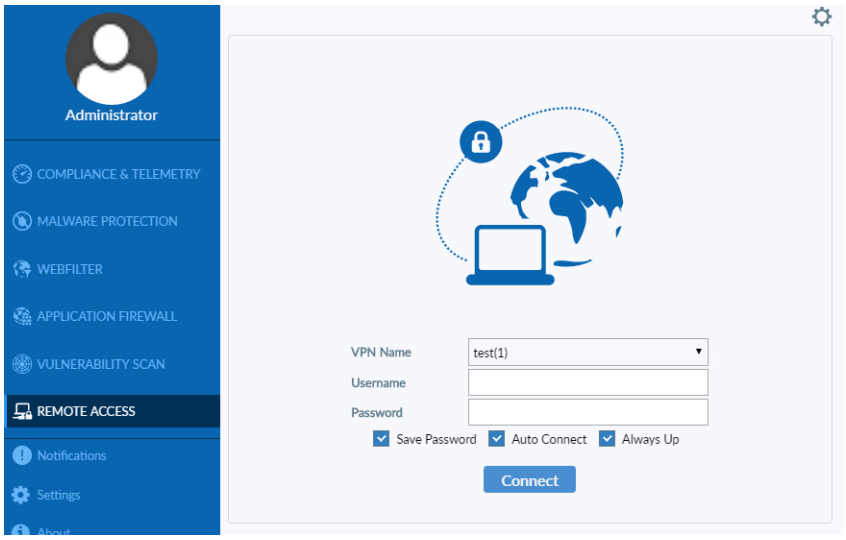
1. On the *Remote Access* tab, select the VPN connection from the dropdown list.
2. Enter your username and password and click the *Connect* button. The *Enter token code* box displays.
3. Enter the token code from FortiToken Mobile and click *OK* to complete network authentication.

Save password, auto connect, and always up

When an administrator uses EMS to configure a profile for FortiClient, the administrator can configure an IPsec or SSL VPN connection to FortiGate and enable the following features:

- *Save Password*: Allows the user to save the VPN connection password in FortiClient
- *Auto Connect*: When FortiClient is launched, the VPN connection automatically connects. Automatic connection to the VPN tunnel may fail if the endpoint boots up with a user profile set to automatic logon.
- *Always Up (Keep Alive)*: When selected, the VPN connection is always up, even when no data is being processed. If the connection fails, keep alive packets sent to the FortiGate sense when the VPN connection is available and reconnect VPN.

After FortiClient Telemetry connects to FortiGate when FortiGate and EMS are integrated, FortiClient receives a profile from EMS that contains IPsec and/or SSL VPN connections to FortiGate. The following example shows an SSL VPN connection named *test(1)*.



If the VPN connection fails, a popup displays to inform you about the connection failure while FortiClient continues trying to reconnect VPN in the background.

Depending on the VPN configuration, the popup may include a *Cancel* button. If you click the *Cancel* button, FortiClient stops trying to reconnect VPN.

Access to certificates in Windows Certificates Stores

On a Windows system, you can view certificates by using an MMC (Microsoft Management Console) snap-in called Certificates console. For more information, see the following Microsoft TechNet articles:

- *Add the Certificates Snap-in to an MMC*
- *Display Certificate Stores*

The Certificates console offers the following snap-in options:

- My user account
- Service account
- Computer account

You can select one or more snap-in options, which display in the Certificates console. FortiClient typically searches for certificates in one of the following accounts:

- User account – contains certificates for the logged on user
- Computer account – contains certificates for the local computer

If the certificate is in the local computer account, FortiClient can typically access the certificate. A certificate from the local computer account may be used to establish an IPsec VPN connection, regardless of whether the logged on user is an administrator or a non-administrator. For SSL VPN and IPsec VPN, the administrator needs to grant permission to users who are non-administrators to access the private key of the certificate. Otherwise, non-administrators cannot use the certificate in the computer account to establish SSL VPN connections. This restriction does not apply to any user with administrator level permission.

If the certificate is in the user account, FortiClient can access the certificate, if the user has already successfully logged in, and the same user imported the certificate. In all other scenarios, FortiClient may be unable to access the certificate.

The following table summarizes when FortiClient can (yes) and cannot (no) locate the certificate for users who are logged into the endpoint and connecting VPN tunnels:

Account	Connect VPN using FortiClient GUI or FortiTray	
	Logged in user with admin privilege	Logged in user with non-admin privilege
User account	Yes, certificate found, if the same administrator user imported the certificate	Yes, certificate found, if the same user imported the certificate
Computer account	Yes, certificate found	IPsec VPN: Yes, certificate found, if access permission granted to private key SSL VPN: Yes, certificate found, if access permission granted to private key
SmartCard	Yes, certificate found, if same user that was logged on at the time card was inserted	Yes, certificate found, if same user that was logged on at the time card was inserted

When a user imports a certificate into the user account, a different logged on user cannot access the same certificate.

A certificate on a smart card is imported into the user account of the logged on user. As a result, the same conditions apply as with the user account.

The following table summarizes when FortiClient can (yes) and cannot (no) locate the certificate before a user logs into the endpoint:

Account	Unknown user before logging into Windows
User account	No certificate found
Computer account	Yes certificate found
SmartCard	No certificate found

Advanced features (Windows)

When deploying a custom FortiClient XML configuration, use the advanced FortiClient profile options in EMS to ensure the FortiClient profile settings do not overwrite your custom XML settings. See the *FortiClient XML Reference Guide*.

Activating VPN before Windows logon

When using VPN before Windows logon, the user is offered a list of preconfigured VPN connections to select from on the Windows logon screen. This requires that the Windows logon screen is not bypassed. As such, if VPN before Windows logon is enabled, it is required to also select the *Users must enter a user name and password to use this computer* checkbox in the *User Accounts* dialog.

To activate VPN before Windows logon:

1. In FortiClient, create the VPN tunnels of interest or receive the VPN list of interest from FortiClient EMS.
2. Ensure that VPN is enabled before logon to the FortiClient *Settings* page.
3. On the Windows system, start an elevated command line prompt.
4. Enter `control passwords2` and press `Enter`. Alternatively, you can enter `netplwiz`.
5. Check the checkbox for *Users must enter a user name and password to use this computer*.
6. Click *OK* to save the setting.

Connecting VPNs before logging on (AD environments)

The VPN `<options>` tag holds global information controlling VPN states. The VPN connects first, then logs on to AD/domain.

```
<forticlient_configuration>
   <vpn>
      <ipsecvpn>
         <options>
            <show_vpn_before_logon>1</show_vpn_before_logon>
            <use_windows_credentials>1</use_windows_credentials>
         </options>
         <connections>
            <connection>
               <name>psk_90_1</name>
               <type>manual</type>
               <ike_settings>
                  <prompt_certificate>0</prompt_certificate>
                  <server>10.10.90.1;ipsecdemo.fortinet.com;172.17.61.143</server>
                  <redundantsortmethod>1</redundantsortmethod>
                  ...
               </ike_settings>
            </connection>
         </connections>
      </ipsecvpn>
   </vpn>
</forticlient_configuration>
```

This is a balanced but incomplete XML configuration fragment. It includes all closing tags but omits some important elements to complete the IPsec VPN configuration.

RedundantSortMethod = 1

This XML tag sets the IPsec VPN connection as ping-response-based. The VPN connects to the FortiGate which responds the fastest.

RedundantSortMethod = 0

By default, RedundantSortMethod =0 and the IPsec VPN connection is priority-based. Priority-based configurations try to connect to the FortiGate starting with the first in the list.

Creating redundant IPsec VPNs

To use VPN resiliency/redundancy, configure a list of VPN gateways, instead of just one:

```
<forticlient_configuration>
   <vpn>
      <ipsecvpn>
         <options>
            ...
         </options>
         <connections>
            <connection>
               <name>psk_90_1</name>
               <type>manual</type>
               <ike_settings>
                  <prompt_certificate>0</prompt_certificate>
                  <server>10.10.90.1;ipsecdemo.fortinet.com;172.17.61.143</server>
                  <redundantsortmethod>1</redundantsortmethod>
                  ...
               </ike_settings>
            </connection>
         </connections>
      </ipsecvpn>
   </vpn>
</forticlient_configuration>
```

This is a balanced but incomplete XML configuration fragment. It includes all closing tags, but omits some important elements to complete the IPsec VPN configuration.

RedundantSortMethod = 1

This XML tag sets the IPsec VPN connection as ping-response-based. The VPN connects to the FortiGate which responds the fastest.

RedundantSortMethod = 0

By default, RedundantSortMethod =0 and the IPsec VPN connection is priority-based. Priority-based configurations try to connect to the FortiGate starting with the first in the list.

Creating priority-based SSL VPN connections

SSL VPN supports priority-based configurations for redundancy.

```
<forticlient_configuration>
   <vpn>
      <sslvpn>
```

```
        <options>
           <enabled>1</enabled>
           ...
        </options>
        <connections>
           <connection>
              <name>ssl_90_1</name>
              <server>10.10.90.1;ssldemo.fortinet.com;172.17.61.143:443</server>
              ...
           </connection>
        </connections>
     </sslvpn>
  </vpn>
</forticlient_configuration>
```

This is a balanced but incomplete XML configuration fragment. It includes all closing tags, but omits some important elements to complete the SSL VPN configuration.

For SSL VPN, all FortiGates must use the same TCP port.

Advanced features (macOS)

When deploying a custom FortiClient XML configuration, use the advanced FortiClient profile options in EMS to ensure the FortiClient profile settings do not overwrite your custom XML settings. See the *FortiClient XML Reference Guide*.

Creating redundant IPsec VPNs

To use VPN resiliency/redundancy, configure a list of FortiGate or EMS IP/FQDN servers, instead of just one:

```
<forticlient_configuration>
  <vpn>
     <ipsecvpn>
        <options>
           ...
        </options>
        <connections>
           <connection>
              <name>psk_90_1</name>
              <type>manual</type>
              <ike_settings>
                 <prompt_certificate>0</prompt_certificate>
                 <server>10.10.90.1;ipsecdemo.fortinet.com;172.17.61.143</server>
                 <redundantsortmethod>1</redundantsortmethod>
                 ...
              </ike_settings>
           </connection>
        </connections>
     </ipsecvpn>
  </vpn>
</forticlient_configuration>
```

This is a balanced but incomplete XML configuration fragment. It includes all closing tags, but omits some important elements to complete the IPsec VPN configuration.

RedundantSortMethod = 1

This XML tag sets the IPsec VPN connection as ping-response-based. The VPN connects to the FortiGate or EMS which responds the fastest.

RedundantSortMethod = 0

By default, RedundantSortMethod =0 and the IPsec VPN connection is priority-based. Priority-based configurations tries to connect to the FortiGate or EMS starting with the first in the list.

```
            </connection>
         </connections>
      </sslvpn>
   </vpn>
</forticlient_configuration>
```

This is a balanced but incomplete XML configuration fragment. It includes all closing tags, but omits some important elements to complete the SSL VPN configuration.

For SSL VPN, all FortiGate or EMS units must use the same TCP port.

Creating priority-based SSL VPN connections

SSL VPN supports priority-based configurations for redundancy.

```
<forticlient_configuration>
   <vpn>
      <sslvpn>
         <options>
            <enabled>1</enabled>
            ...
         </options>
         <connections>
            <connection>
               <name>ssl_90_1</name>
               <server>10.10.90.1;ssldemo.fortinet.com;172.17.61.143:443</server>
               ...
            </connection>
         </connections>
      </sslvpn>
   </vpn>
</forticlient_configuration>
```

This is a balanced but incomplete XML configuration fragment. It includes all closing tags, but omits some important elements to complete the SSL VPN configuration.

For SSL VPN, all FortiGate or EMS must use the same TCP port.

VPN tunnel and script

This feature supports autorunning a user-defined script after connecting or disconnecting the configured VPN tunnel. The scripts are batch scripts in Windows and shell scripts in macOS. They are defined as part of a VPN tunnel configuration on EMS's XML format FortiClient profile. The profile is pushed down to FortiClient from EMS as part of an endpoint policy. When FortiClient's VPN tunnel is connected or disconnected, the respective script defined under that tunnel is executed.

Windows

Mapping a network drive after tunnel connection

The script maps a network drive and copies some files after the tunnel is connected.

```
<on_connect>
   <script>
      <os>windows</os>
      <script>
         <script>
            <![CDATA[ net use x: \\192.168.10.3\ftpshare /user:Ted Mosby md c:\test copy
                  x:\PDF\*.* c:\test ]]>
         </script>
      </script>
   </script>
</on_connect>
```

Deleting a network drive after tunnel disconnection

The script deletes the network drive after the tunnel is disconnected.

```
<on_disconnect>
   <script>
      <os>windows</os>
      <script>
         <script>
            <![CDATA[ net use x: /DELETE ]]>
         </script>
      </script>
   </script>
</on_disconnect>
```

macOS

Mapping a network drive after tunnel connection

The script maps a network drive and copies some files after the tunnel is connected.

```
<on_connect>
   <script>
      <os>mac</os>
```

```
      <script>
         /bin/mkdir /Volumes/installers
         /sbin/ping -c 4 192.168.1.147 > /Users/admin/Desktop/dropbox/p.txt
         /sbin/mount -t smbfs //kimberly:RigUpTown@ssldemo.fortinet.com/installers
               /Volumes/installers/ > /Users/admin/Desktop/dropbox/m.txt
         /bin/mkdir /Users/admin/Desktop/dropbox/dir
         /bin/cp /Volumes/installers/*.log /Users/admin/Desktop/dropbox/dir/.
      </script>
   </script>
</on_connect>
```

Deleting a network drive after tunnel disconnection

The script deletes the network drive after the tunnel is disconnected.

```
<on_disconnect>
   <script>
      <os>mac</os>
      <script>
         /sbin/umount /Volumes/installers
         /bin/rm -fr /Users/admin/Desktop/dropbox/*
      </script>
   </script>
</on_disconnect>
```

Standalone VPN client

Windows and macOS

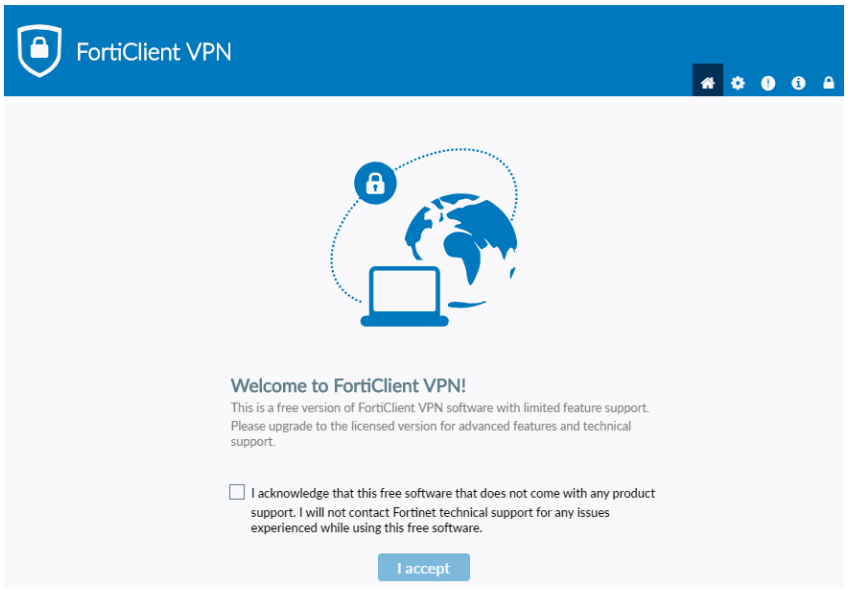
There is a VPN-only installer for Windows and macOS. You can also create a VPN-only installer using FortiClient EMS.

For FortiGate administrators, a free version of FortiClient VPN is available which supports basic IPsec and SSL VPN and does not require registration with EMS. This version does not include central management, technical support, or some advanced features.

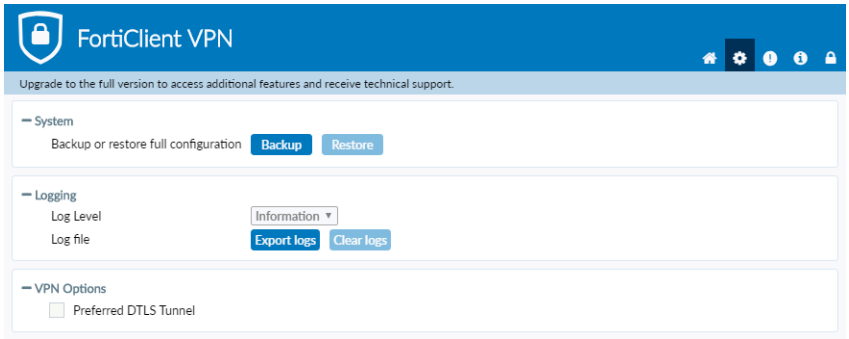
Full-featured FortiClient 6.2.5 requires registration to EMS. Each endpoint registered with EMS requires a license seat on EMS.

The FortiClient VPN installer differs from the installer for full-featured FortiClient. You can only download the free VPN client from FNDN or FortiClient.com.

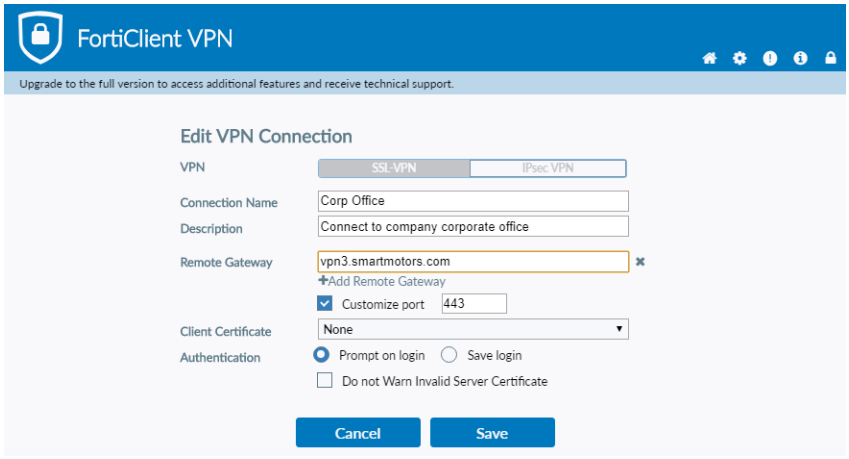
When the free VPN client is run for the first time, it displays a disclaimer. You cannot configure or create a VPN connection until you accept the disclaimer:



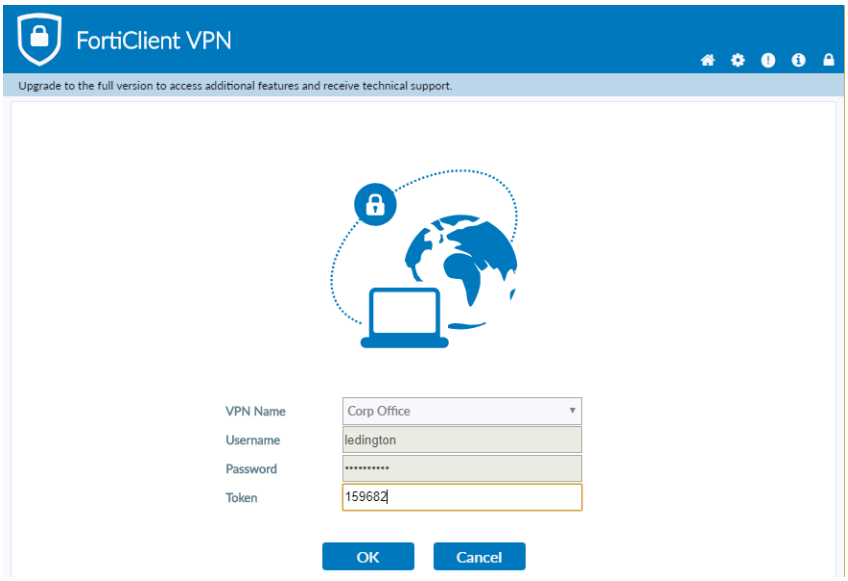
Only the VPN feature is available. You can access the *Settings*, *About*, and *Notifications* pages from a toolbar.



Configuring settings for a new VPN connection on the free VPN client resembles doing the same on a full FortiClient installation:



You can establish a VPN connection from the homepage:



Linux

An SSL VPN tunnel client standalone installer for Linux operating systems is available from FNDN. See the *FortiOS Release Notes*.

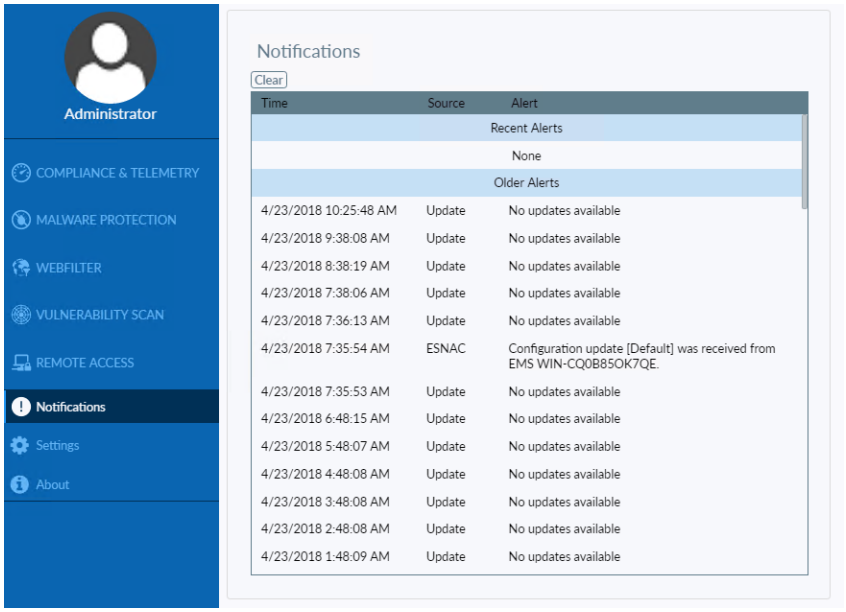
Notifications

Click the *Notifications* tab in FortiClient to view notifications.

Event notifications include:

- AV events, including scheduled scans and detected malware.
- Sandbox Detection events, including detected malware.
- Telemetry events, including configuration updates received from EMS.
- Web Filter events, including blocked website access attempts.
- System events, including signature and engine updates and software upgrades.

Click *Threat Detected* to view quarantined files, site violations, and RTP events.



Settings

This section describes the options on the *Settings* page. There are settings that EMS locks that you cannot change.

System

You can back up the FortiClient configuration to an XML file, and restore the FortiClient configuration from an XML file.

1. Go to *Settings*.
2. Expand the *System* section, then select *Backup* or *Restore* as needed.
   When performing a backup, you can select the file destination, password requirements, and add comments as needed.

Logging

Sending logs and software inventory reports to FortiAnalyzer or FortiManager

Sending logs and software inventory reports to FortiAnalyzer or FortiManager requires the following:

- FortiClient
- EMS
- FortiAnalyzer or FortiManager

When FortiClient connects Telemetry to EMS, the endpoint can upload logs and software inventory reports to FortiAnalyzer or FortiManager units on port 514 TCP.

Where you locate FortiClient logs and software inventory reports in FortiAnalyzer depends on where FortiClient Telemetry is connected:

- When FortiClient connects Telemetry to EMS, the FortiClient logs and software inventory reports display in the FortiClient ADOM in FortiAnalyzer. This scenario does not use FortiGate.
- When FortiClient connects Telemetry to FortiGate, the FortiClient logs and software inventory reports display in the FortiGate ADOM. Even if EMS is used with FortiGate to manage FortiClient endpoints, the FortiClient logs and software inventory reports still display in the FortiGate ADOM.

FortiClient collects information on regular software installed on the endpoint and sends the information to EMS and FortiAnalyzer. FortiClient sends the Software Inventory information when it first registers to EMS and when it first sends data to FortiAnalyzer. If software changes occur on the endpoint, such as installing new software, updating existing software, or removing existing software, FortiClient sends an updated inventory to EMS and FortiAnalyzer.

FortiClient Telemetry must connect to EMS for FortiClient to upload logs and software inventory reports to FortiAnalyzer or FortiManager.

Exporting the log file

To export the log file:

1. Go to *Settings*.
2. Expand the *Logging* section, and click *Export logs*.
3. Select a location for the log file, enter a name for the log file, and click *Save*.

VPN options

To configure VPN options:

1. Go to *Settings* and expand the *VPN Options* section.
2. Select *Enable VPN before logon* to allow selecting a VPN connection before logging into the system.
3. Select *Preferred DTLS Tunnel*. If enabled, FortiClient uses DTLS if it is enabled on the FortiGate and tunnel establishment is successful. If not enabled on the FortiGate or tunnel establishment is not successful, TLS is used. DTLS tunnel uses UDP instead of TCP and can increase throughput over VPN.
   When disabled, FortiClient uses TLS, even if DTLS is enabled on FortiGate.
4. Click *Save*.

Advanced options

To configure advanced options:

1. Go to *Settings*, and expand the *Advanced* section.
2. Configure the following settings, and click *OK*:

Default tab	Select the default tab to display when opening FortiClient.
Enable Single Sign-On mobility agent	Enable SSO.
Disable proxy (troubleshooting only)	Disable proxy when troubleshooting FortiClient.

FortiTray

When FortiClient is running on your system, you can select the FortiTray icon in the Windows system tray to perform various actions. The FortiTray icon is available in the system tray even when FortiClient is closed.

- Default menu options:
  - Open FortiClient
  - View *About* tab in FortiClient

  - Shut down FortiClient
- Dynamic menu options, depending on configuration:
  - Connect to a configured IPsec VPN or SSL VPN connection
  - Display the AV scan window (if a scheduled scan is currently running)
  - Display the Vulnerability scan window (if a vulnerability scan is running)

If you hover the cursor over the FortiTray icon, you receive various notifications including the FortiClient version, AV signature version, and AV engine version.

When EMS has locked the configuration, the option to shut down FortiClient from FortiTray is grayed out.

To establish a VPN connection from FortiTray:

1. Select the Windows System Tray.
2. Right-click the *FortiTray* icon, and select a VPN connection configuration.
3. Enter your username and password in the authentication window, and click *OK* to connect.

Diagnostic Tool

You can access the FortiClient Diagnostic Tool from FortiClient. Go to *About*.

On FortiClient (Windows), you can also access the Diagnostic Tool from the *Start* menu.

You can use the FortiClient Diagnostic Tool to generate a debug report, then provide the debug report to the FortiClient team to help with troubleshooting. For example, if you are working with customer support on a problem, you can generate a debug report and email the report to customer support to help with troubleshooting.

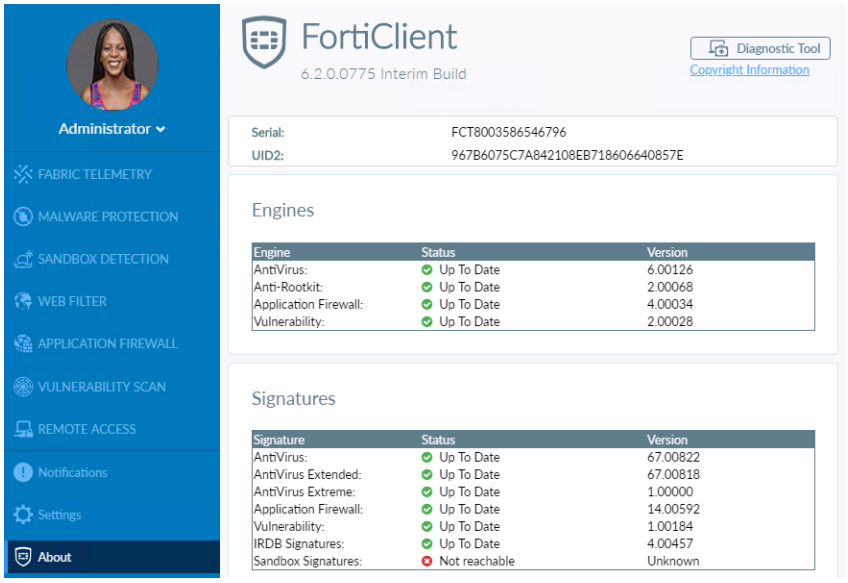
The FortiClient Diagnostic Tool does not record sensitive information. It contains information about the endpoint such as:

- Windows operating system version
- Windows software updates
- Names and versions of installed software
- Names and versions of installed drivers
- FortiClient configuration
- FortiClient logs

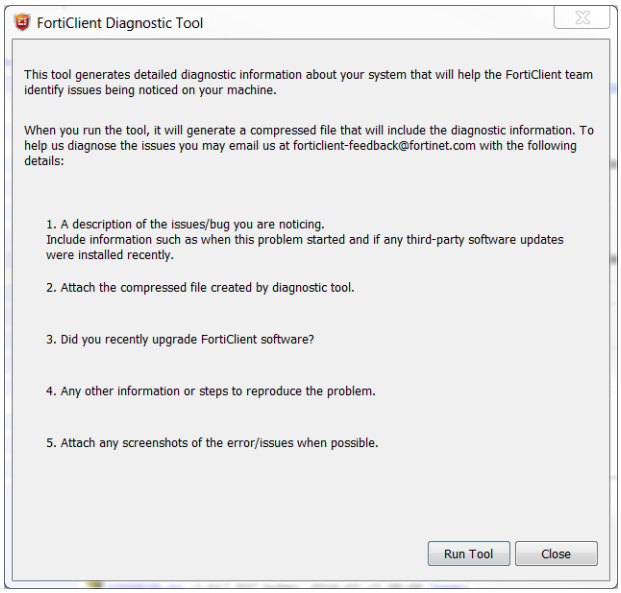
Before sending the package that the FortiClient Diagnostic Tool created to the FortiClient team, you can open and read the package.

To access the FortiClient Diagnostic Tool:

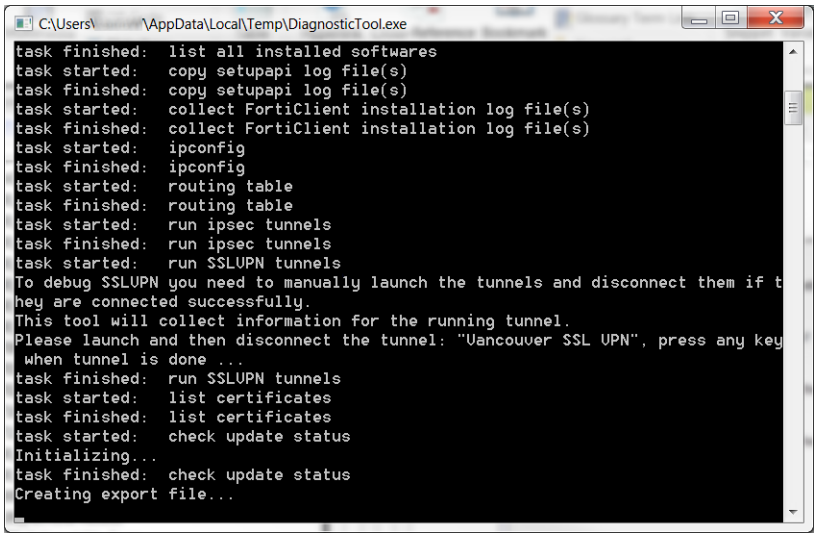
1. Go to *About*.



2. Click the *Diagnostic Tool* button in the top right corner. The FortiClient Diagnostic Tool dialog displays.



3. Click *Run Tool*. A window displays the provided status information.



4. (Optional) When prompted, launch and disconnect the VPN tunnels for which you want to collect information. The Diagnostic Tool creates a *Diagnostic_Result* file and displays it in a folder on the endpoint. The default folder location is *C:\Users <user name>\AppData\Local\Temp*.
5. Click *Close*.

Appendix A - FortiClient API

You can operate FortiClient VPNs using the COM-based FortiClient API. You can use the API only with IPsec VPN. The API does not currently support SSL VPN.

Overview

The FortiClient COM library provides functionality to:

- Retrieve a list of VPN tunnels configured in the FortiClient application.
- Start and stop any of the configured VPN tunnels.
- Send XAuth credentials.
- Retrieve status information:
  - Configured tunnel list
  - Active tunnel name
  - Connection status
  - Idleness status
  - Remaining key life
- Respond to FortiClient-related events:
  - VPN connect
  - VPN disconnect
  - VPN is idle
  - XAuth authentication requested

For more information, see the vpn_com_examples ZIP file located in the VPN utomation file folder in the FortiClientTools file.

API reference

The following tables provide API reference values:

`Disconnect(bstrTunnelName As String)`	Close the named VPN tunnel.
`GetPolicy pbAV As Boolean, pbAS As Boolean, pbFW As Boolean, pbWF As Boolean)`	Command was deprecated in FortiClient 5.0.
`GetRemainingKeyLife(bstrTunnelName As String, pSecs As Long, pKBytes As Long)`	Retrieve the remaining key life for the named connection. Whether key life time (pSecs) or data (pKBytes) are significant depends on the detailed settings in the FortiClient application.
`MakeSystemPolicyCompliant()`	Command was deprecated in FortiClient 5.0.

`SendXAuthResponse (tunnelName As String, userName As String, password As String, savePassword As Boolean)`	Send XAuth credentials for the named connection: • Username, password • True if password should be saved.
`SetPolicy (bAV As Boolean, bAS As Boolean, bFW As Boolean, bWF As Boolean)`	Command was deprecated in FortiClient 5.0.
`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.
`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)`	Command was deprecated in FortiClient 5.0.
`OnXAuthRequest(bstrTunnelName As String)`	The VPN peer on the named connection requests XAuth authentication.

Appendix B - FortiClient log messages

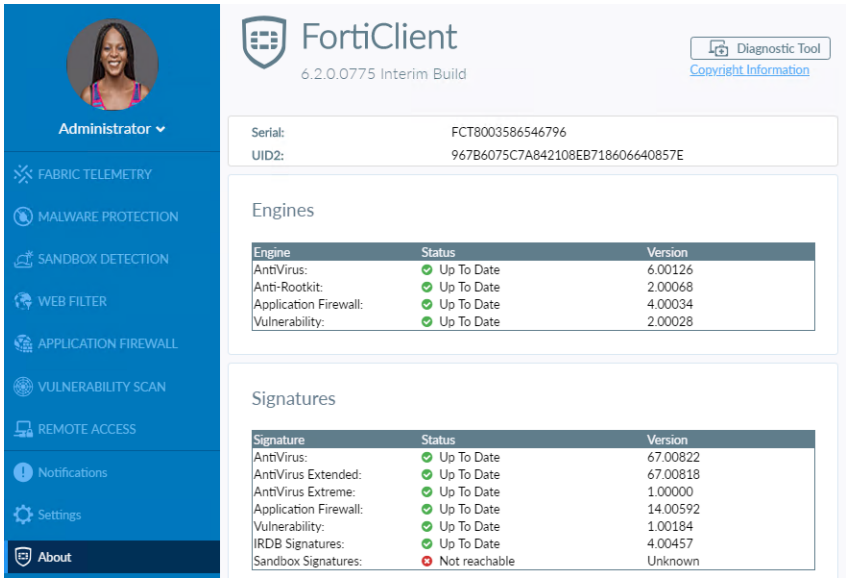
For a list of FortiClient log messages, see the FortiClient 6.2.5 Online Help. The table of log messages is too wide to fit into the page size of the *FortiClient 6.2.5 Administration Guide*.

Appendix C - Vulnerability patches

FortiClient checks many applications for vulnerabilities. FortiClient can automatically patch vulnerabilities from some applications, but not all applications. For some applications, you must manually patch vulnerabilities.

For the latest list of supported software, see the FortiGuard Center.

1. In FortiClient, go to *About* to check the Vulnerability signature version number. In the example, the version number is 1.00184.



2. Go to FortiGuard Labs > Learn More > Endpoint Vulnerability.
3. At the bottom of the page, click the desired Vulnerability signature version. The supported software is listed.

Appendix D - FortiClient processes

This section identifies the processes used by FortiClient (Windows) and FortiClient (macOS).

FortiClient (Windows) processes

The following table identifies the processes in Task Manager used by FortiClient (Windows):

Name	Description	Purpose
	FortiClient Virus Feedback Service	Used by AV and FortiClient to submit samples to FortiGuard
FCVbltScan.exe	FortiClient Vulnerability Scan Daemon	FortiClient Vulnerability Scan engine
FortiAvatar.exe	FortiClient User Avatar Agent	Used by FortiClient and FortiClient Telemetry to obtain avatar images for users
ipsec.exe	FortiClient IPsec VPN Service	Remote Access for IPsec VPN
FortiClient.exe	FortiClient Console	FortiClient GUI
FortiClient_Diagnostic_Tool.exe	FortiClient Diagnostic Tool	Diagnostic Tool
fcappdb.exe	FortiClient Application Database Service	Network Access Control (NAC) and AV
fcaptmon.exe	FortiClient Sandbox Agent	Sandbox Detection
FCDBLog.exe	FortiClient Logging Daemon	Logging
FCHelper64.exe	FortiClient System Helper	FortiClient ensures 32-bit processes can access 64-bit resources
fmon.exe	FortiClient Realtime AntiVirus Protection	AV

Name	Description	Purpose
fortiae.exe	FortiClient Anti-Exploit	Anti-Exploit engine
FortiESNAC.exe	FortiClient Network Access Control	FortiClient Telemetry
fortifws.exe	FortiClient Firewall Service	Application Firewall
FortiProxy.exe	FortiClient Proxy Service	AV and Web Filter
FortiScand.exe	FortiClient Scan Server	Offloading AV scanning to a separate process
FortiSettings.exe	FortiClient Settings Service	Used by FortiClient settings
FortiSSLVPNdaemon.exe	FortiClient SSLVPN daemon	Remote Access for SSL VPN
FortiTray.exe	FortiClient System Tray Controller	FortiTray
FortiUSBmon.exe	FortiClient USB monitor protection	Removable media access control.
FortiWF.exe	FortiClient Web Filter Service	Used by Web Filter
scheduler.exe	FortiClient Scheduler	Windows ensures FortiClient services are running when needed

FortiClient (macOS) processes

FortiClient (macOS) uses the following processes:

- The process for the FortiClient main GUI is located at `/Application/FortiClient.app/Contents/MacOS/FortiClient`
- The process for FortiTray controller is located at `/Application/FortiClient.app/Contents/Resources/runtime.helper/FortiClientAgent.app/MacOS/FortiClientAgent`
- The process for FortiClient upgrade GUI is located at `/Application/FortiClient.app/Contents/Resources/runtime.helper/FortiClientUpdate.app/Contents/MacOS/FortiClientUpdate`

The following table identifies the processes in the following location used by FortiClient (macOS):

`/Library/Application Support/Fortinet/FortiClient/bin`:

Name	Purpose
fctservctl	FortiClient Service Controller
epctrl	FortiClient endpoint control daemon
ftgdagent	Web Filter
fmon	AV scan main program
scanunit	AV scan scanner
vulscan	Vulnerability scan
fctappfw	Firewall service
fssoavgent_launchagent	FSSO agent
fssoavgent_launchdaemon	FSSO daemon
fctctld	VPN controller
sslvpnd	SSL VPN Daemon
racoon	IPsec VPN Service
racoonctl	IPsec VPN Controller
fctupdate	FortiClient update tool
fctupgrade	FortiClient upgrade tool

Appendix E - FortiClient (Linux) CLI commands

FortiClient (Linux) supports an installer targeted towards the headless version of Linux server. FortiClient (Linux) 6.2.5 for servers (forticlient_server_6.2.0.0xxx) offers a command line interface and is intended to be used with the CLI-only (headless) installation. The same set of CLI commands also work with a FortiClient (Linux) GUI installation.

The following summarizes the CLI commands available for FortiClient (Linux) 6.2.5:

Endpoint control

FortiClient 6.2.5 must establish a Telemetry connection to EMS to receive license information. FortiClient features are only enabled after connecting to EMS.

Usage

You can access endpoint control features through the `epctrl` CLI command. This command offers the end user the ability to connect or disconnect from EMS and check the connection status. You can access usage information by using the following commands:

```
jameslee@sunshine:~$ /opt/forticlient/epctrl -h
FortiClient Endpoint Control

Usage:
  /opt/forticlient/epctrl -r|--register <address> [-p|--port ]
  /opt/forticlient/epctrl -u|--unregister
  /opt/forticlient/epctrl -d|--details

Options:
  -h --help        Show the help screen
  -r --register    Register to an EMS address
  -p --port        EMS port
  -u --unregister  Unregister from the current EMS
  -d --details     Show telemetry details and status
```

Connecting to EMS

FortiClient can connect to EMS using the following commands. If EMS is listening on the default port, 8013, you do not need to specify the port number. If EMS is listening on another port, such as 8444, you must specify the port number with the EMS address. The example illustrates both use cases:

```
jameslee@sunshine:~$ /opt/forticlient/epctrl -r 172.17.60.251
Registering to EMS 172.17.60.251:8013.

jameslee@sunshine:~$ /opt/forticlient/epctrl -r 172.17.60.251 -p 8444
Registering to EMS 172.17.60.251:8444.
```

Endpoint control status

You can check FortiClient endpoint control status details with the `-d` argument. When FortiClient is connected to EMS only, the command output is as follows:

```
jameslee@sunshine:~$ /opt/forticlient/epctrl -d
====================================
FortiClient EMS Details
====================================
IP: 172.17.60.251:8013
Host: DESKTOP-ID2CVUA
SN: FCTEMS3764894213
Status: Connected
```

If FortiClient is connected to EMS and notifying FortiGate, the endpoint control status displays the serial numbers and hostnames of the EMS and FortiGates as follows:

```
jameslee@sunshine:~$ /opt/forticlient/epctrl -d

====================================
FortiClient EMS Details
====================================
IP: ems.fortinet.net:80
Host: DESKTOP-ID2CVUA
SN: FCTEMS3764894213
Status: Connected

====================================
FortiGate Details
====================================
IP: 172.17.60.40
Host: FGVM02TM18001119
SN: FGVM02TM18001119
Status: Connected
```

When FortiClient is not connected to EMS, the endpoint control status has no Telemetry data available as shown:

```
jameslee@sunshine:~$ /opt/forticlient/epctrl -d
No telemetry data available.
```

Disconnecting from EMS

FortiClient can disconnect from EMS only if the configuration received from EMS allows it. You can disconnect using the `-u` argument.

```
jameslee@sunshine:~$ /opt/forticlient/epctrl -u
Unregistering from EMS.
```

AV scanning

You may run an AV scan from the CLI on the entire file system or on a specified directory. You can only run an AV scan as the root user. After completing an AV scan, FortiClient prints the scan results and detailed log file locations. You can run the following command to run an AV scan, where `<dir>` is the directory to scan. You can perform a full scan by inputting `/` in place of `<dir>`.

```
sudo /opt/forticlient/fmon -s /opt/forticlient/vir_sig/ -o /opt/forticlient/ --unit /op-
t/forticlient -d <dir>
```

The following shows an AV scan performed on the `/var` directory:

```
jameslee@sunshine:/var$ sudo /opt/forticlient/fmon -s /opt/forticlient/vir_sig/ -o /op-
t/forticlient/ --unit /opt/forticlient -d /var
Signature dir : /opt/forticlient/vir_sig/
Log dir : /opt/forticlient/
Fmon on daemon mode.
Dest dir : /var
CPU number : 1
Server port : 40140
AV Engine path : /opt/forticlient/libav.so
AV Signature path : /opt/forticlient/vir_sig/vir_high:/opt/forticlient/vir_sig/vir_sandbox_sig
Load AV signature success.
<=== PID : 13821 Client Hello rc = 2185
Child : 13821 ready
===> Scan : /var/spool/anacron/cron.daily
===> Scan : /var/spool/anacron/cron.weekly
===> Scan : /var/spool/anacron/cron.monthly
===> Scan : /var/crash/_usr_bin_gedit.1001.crash
===> Scan : /var/crash/_opt_forticlient_fmon.1000.crash
===> Scan : /var/backups/apt.extended_states.1.gz
===> Scan : /var/backups/shadow.bak
===> Scan : /var/backups/dpkg.statoverride.2.gz
===> Scan : /var/backups/passwd.bak
===> Scan : /var/backups/dpkg.diversions.1.gz
===> Scan : /var/backups/apt.extended_states.0
===> Scan : /var/backups/dpkg.arch.2.gz
===> Scan : /var/backups/alternatives.tar.1.gz
===> Scan : /var/backups/dpkg.arch.0
===> Scan : /var/backups/dpkg.status.1.gz
===> Scan : /var/backups/dpkg.statoverride.0
===> Scan : /var/backups/dpkg.arch.1.gz
===> Scan : /var/backups/gshadow.bak
===> Scan : /var/backups/dpkg.diversions.2.gz
===> Scan : /var/backups/alternatives.tar.2.gz
.............................
.............................
 .............................
 -------------- scan_dispatch_worker finished -------------

Scan started at Mon Apr 22 14:43:45 2019

Found virus : EICAR_TEST_FILE
In file : /var/eicar.com
Action : Quarantine success
Quarantine file : /opt/forticlient/quarantine/eicar.com.1

--------------- Scan summary ----------------------
Total scan files : 10947
Found virus : 1
Worker crash : 0
Worker timeout : 0
-------------------------------------------------

Scan ended at Mon Apr 22 14:44:01 2019

Full results can be found in /opt/forticlient/Daemon - Mon Apr 22 14:43:45 2019.log
```

Vulnerability scanning

You can run a vulnerability scan from the CLI to check for vulnerable applications on the machine. You can only run a vulnerability scan as the root user. After completing a vulnerability scan, FortiClient prints the number of vulnerabilities present on the machine, their severity levels, and detailed log file locations. You can run a vulnerability scan by running the following command:

```
jameslee@sunshine:/home/jameslee$ sudo /opt/forticlient/vulscan -v /opt/forticlient/vcm_sig/ -
c -o /var/log/forticlient/vcm_log/
[INFo} Distribution name is Ubuntu
[INFO] Distribution version is 18.04.1 LTS (Bionic Beaver)
[INFO] LoadVulSig
[INFO] Decryption success!
[INFO] LoadFromDb
[INFO] Total sig : 13163
[INFO] Signature version=1.38
[INFO] Engine version=2.0.0.22
[INFO] Build install list
.............................
.............................
.............................
[INFO] Output directory: /var/log/forticlient/vcm_log/2019-04-18 18-45-42/
--------------- Scan summary ---------------------
Critical : 7
High : 2
Medium : 7
Low : 0
------------------------------------------------
```

You can patch existing vulnerabilities using FortiClient. FortiClient runs a vulnerability scan again after patching the vulnerabilities and prints the results. You can patch vulnerabilities as shown:

```
jameslee@sunshine:/home/jameslee$ sudo /opt/forticlient/vulscan -v /opt/forticlient/vcm_sig/ -
c -o /var/log/forticlient/vcm_log/ -p
[INFo} Distribution name is Ubuntu
[INFO] Distribution version is 18.04.1 LTS (Bionic Beaver)
[INFO] LoadVulSig
[INFO] Decryption success!
[INFO] LoadFromDb
[INFO] Total sig : 13163
[INFO] Signature version=1.38
[INFO] Engine version=2.0.0.22
[INFO] Build install list
...

Patching vid 55441
Hit:1 http://ca.archive.ubuntu.com/ubuntu bionic InRelease
Get:2 http://ca.archive.ubuntu.com/ubuntu bionic-updates InRelease [88.7 kB]
Get:3 http://security.ubuntu.com/ubuntu bionic-security InRelease [88.7 kB]
Get:4 http://ca.archive.ubuntu.com/ubuntu bionic-backports InRelease [74.6 kB]
Get:5 http://ca.archive.ubuntu.com/ubuntu bionic-updates/main amd64 DEP-11 Metadata [278 kB]
Get:6 http://security.ubuntu.com/ubuntu bionic-security/main amd64 DEP-11 Metadata [9,364 B]
Get:7 http://ca.archive.ubuntu.com/ubuntu bionic-updates/main DEP-11 48x48 Icons [66.7 kB]
Get:8 http://ca.archive.ubuntu.com/ubuntu bionic-updates/main DEP-11 64x64 Icons [123 kB]
Get:9 http://ca.archive.ubuntu.com/ubuntu bionic-updates/universe amd64 DEP-11 Metadata [222
kB]
Get:10 http://security.ubuntu.com/ubuntu bionic-security/main DEP-11 48x48 Icons [7,788 B]
Get:11 http://security.ubuntu.com/ubuntu bionic-security/universe amd64 DEP-11 Metadata [35.7
```

```
kB]
Get:12 http://ca.archive.ubuntu.com/ubuntu bionic-updates/universe DEP-11 48x48 Icons [194 kB]
Get:13 http://security.ubuntu.com/ubuntu bionic-security/universe DEP-11 48x48 Icons [16.4 kB]
Get:14 http://security.ubuntu.com/ubuntu bionic-security/universe DEP-11 64x64 Icons [92.2 kB]
Get:15 http://ca.archive.ubuntu.com/ubuntu bionic-updates/universe DEP-11 64x64 Icons [406 kB]
Get:16 http://ca.archive.ubuntu.com/ubuntu bionic-updates/multiverse amd64 DEP-11 Metadata
[2,468 B]
Get:17 http://security.ubuntu.com/ubuntu bionic-security/multiverse amd64 DEP-11 Metadata
[2,464 B]
Get:18 http://ca.archive.ubuntu.com/ubuntu bionic-backports/universe amd64 DEP-11 Metadata
[7,352 B]
Fetched 1,716 kB in 3s (591 kB/s)
Reading package lists... Done
[INFO] install command is: apt-get -y install --only-upgrade firefox
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
fonts-lyx
The following packages will be upgraded:
firefox
1 upgraded, 0 newly installed, 0 to remove and 315 not upgraded.
Need to get 0 B/48.1 MB of archives.
After this operation, 7,509 kB of additional disk space will be used.
 (Reading database ... 162206 files and directories currently installed.)
Preparing to unpack .../firefox_66.0.3+build1-0ubuntu0.18.04.1_amd64.deb ...
Unpacking firefox (66.0.3+build1-0ubuntu0.18.04.1) over (59.0.2+build1-0ubuntu1) ...
Processing triggers for mime-support (3.60ubuntu1) ...
Processing triggers for desktop-file-utils (0.23-1ubuntu3.18.04.1) ...
Setting up firefox (66.0.3+build1-0ubuntu0.18.04.1) ...
Installing new version of config file /etc/apparmor.d/usr.bin.firefox ...
Please restart all running instances of firefox, or you will experience problems.
Processing triggers for man-db (2.8.3-2) ...
Processing triggers for gnome-menus (3.13.3-11ubuntu1) ...
Processing triggers for hicolor-icon-theme (0.17-2) ...
[INFO] query command is: dpkg-query --show firefox
Package version found is 66.0.3+build1-0ubuntu0.18.04.1

Patching vid 55442
Hit:1 http://security.ubuntu.com/ubuntu bionic-security InRelease
Hit:2 http://ca.archive.ubuntu.com/ubuntu bionic InRelease
Hit:3 http://ca.archive.ubuntu.com/ubuntu bionic-updates InRelease
Hit:4 http://ca.archive.ubuntu.com/ubuntu bionic-backports InRelease
Reading package lists... Done
..............................
..............................
..............................
--------------- Scan summary ---------------------
Critical : 0
High : 0
Medium : 0
Low : 0
------------------------------------------------
```

FortiClient updates

You can run a FortiClient update task from the CLI once FortiClient has connected to EMS and is licensed. The update task downloads the latest FortiClient engine and signatures. You can only run an update task as the root user. Following are the command and its output:

```
root@sunshine:/home/jameslee# /opt/forticlient/update

***************Update starting**************
Sandbox test = 0
Sandbox host to test = (null)
log_level: 6
Enable custom fds server :80 failover port: 8000 failover to fdg: 1 allow sw update: 0
Updating FCTDATA: Update started forced update
[INFO] Engine version=2.0.0.22
[INFo} Distribution name is Ubuntu
[INFO] Distribution version is 18.04.1 LTS (Bionic Beaver)
[INFO] LoadVulSig [INFO] Decryption success!
[INFO] LoadFromDb [INFO] Total sig : 13163
[INFO] Signature version=1.38
Getting current FortiClient Components information
current av engine version: 6.2.126
av engine id: 06002000FVEN04100-00006.00126-9999999999
current av main sig full version: 67.1895
av main sig id: 06002000FVDB04000-00067.01895-9999999999
current av ext sig full version: 67.1892
...
...
user jameslee, type:7, session:0, pid:6913
user = jameslee
sandbox server not configured.
Updating FCTDATA: Update finished
[INFO] Engine version=2.0.0.22
[INFo} Distribution name is Ubuntu
[INFO] Distribution version is 18.04.1 LTS (Bionic Beaver)
[INFO] LoadVulSig
[INFO] Decryption success!
[INFO] LoadFromDb
[INFO] Total sig : 13163
[INFO] Signature version=1.38
Downloading done ret = 0
root@sunshine:/home/jameslee#
```

Existing signature details

You can check details of the existing FortiClient engine and signatures by running the update task with the `-d` argument:

```
jameslee@sunshine:/home/jameslee$ /opt/forticlient/update -d

====================================
 Engines
====================================
AntiVirus: 6.2.00126
Vulnerability: 2.00022
```

```
====================================
 Signatures
====================================
AntiVirus: 67.01895
AntiVirus Extended: 67.01892
Vulnerability: 1.00038
Sandbox: 3.00442
```

Update help

The update help option lists all options available for the update task. You can access this option as shown:

```
jameslee@sunshine:~$ /opt/forticlient/update -h
FortiClient Update

Usage:
/opt/forticlient/update
/opt/forticlient/update -d

Options:
-h Show the help screen
-d Show engine and signature versions
```

Change log

Date	Change Description
2020-02-27	Initial release.
2020-06-04	Updated Compliance with EMS and FortiOS on page 36.