FortiClient - Administration Guide

Version 6.0.0

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 COOKBOOK
https://cookbook.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: techdocs@fortinet.com

FORTINET®

July 9, 2018
FortiClient 6.0.0 Administration Guide
04-600-478344-20180709

TABLE OF CONTENTS

Change Log

Date	Change Description
2018-05-31	Initial release.
2018-06-18	Added note to FortiClient 6.0.0 on page 13.
2018-06-27	Updated Linux computer on page 36.
2018-07-09	Updated Quarantined endpoints on page 59.

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 your endpoint security combines strong prevention with detection and mitigation is critical.

This document is written for FortiClient (Windows) 6.0.0. Not all features described in this document are supported for FortiClient (OS X) 6.0.0 or FortiClient (Linux) 6.0.0.

FortiClient modes and features

FortiClient is available in standalone and managed modes.

Standalone mode

In standalone mode, FortiClient is not connected to FortiGate or EMS. In this mode, FortiClient is free for private individuals and commercial businesses to use; no license is required. See Getting started with standalone mode on page 15.

Support for FortiClient in standalone mode is provided on the Fortinet Forums. Phone support is not provided.

Managed mode

In managed mode, FortiClient is connected to EMS or FortiGate. Another option is to connect FortiClient to EMS and FortiGate. In managed mode, FortiClient licensing is applied to FortiGate or EMS. No separate license is required for FortiClient itself.

When connected only to EMS, FortiClient is managed by EMS. However, FortiClient cannot participate in network compliance or Fortinet Security Fabric.

When connected to FortiGate, FortiClient integrates with 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.

FortiClient works cooperatively with 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 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 managed mode on page 16.

Feature comparison of standalone and managed modes

The following table provides a feature comparison between standalone FortiClient (free version) and managed FortiClient (licensed version).

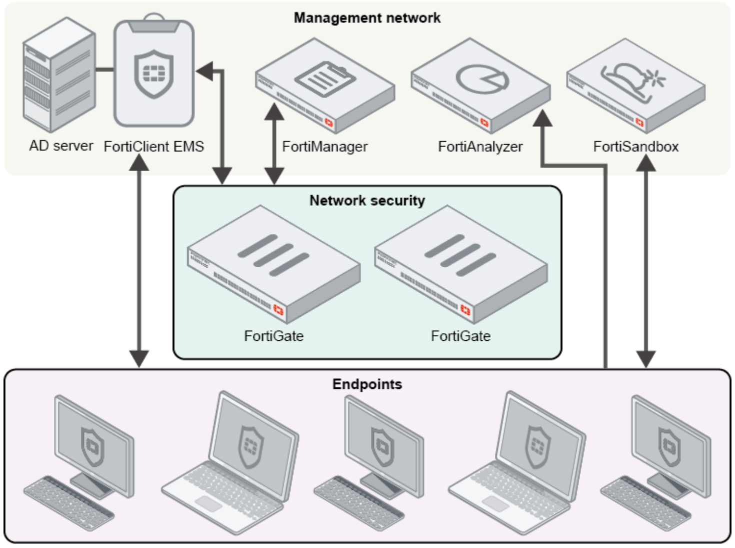
Both modes (free and licensed)	Only with managed mode (licensed)
Installation options • Security Fabric Agent: Telemetry, vulnerability scanning, vulnerability patching • Secure Remote Access: SSL and IPsec VPN components • Advanced Persistent Threat (APT): FortiSandbox detection and quarantine components • Additional Security Features: AntiVirus, Web Filtering, Single Sign On, Application Firewall. Select one, two, or all additional security features.	**Security Fabric and network access compliance** • Participation in Security Fabric • Compliance status • Define and enforce enterprise security policies when FortiClient used with FortiGate • On-net/off-net detection
Advanced Persistent Threat • Integration with FortiSandbox	**Central monitoring and management** • Centralized FortiClient monitoring with FortiGate or EMS • Centralized configuration provisioning and deployment when FortiClient used with EMS
AntiVirus • Realtime Antivirus protection • Antirootkit/antimalware • Grayware blocking (adware/riskware)	**Central logging** • Upload logs to FortiAnalyzer or FortiManager. FortiClient must connect to FortiGate or EMS to upload logs to FortiAnalyzer or FortiManager.
Web Filter • Web filtering • YouTube education filter	
Application control • Application Firewall • Block specific application traffic	
Remote access • SSL VPN	

Both modes (free and licensed)	Only with managed mode (licensed)
• IPsec VPN • Client certificate support • X.509 certificate support • Elliptical Curve certificate support • Two-factor authentication	
Vulnerability management • Vulnerability scanning • Links to FortiGuard with information on the impact and recommended actions • Automatic software patching for identifying vulnerabilities • List of software that requires manual installation of software patches	
Logging • VPN, Application Firewall, Antivirus, Web Filter, Update, and Vulnerability Scan logging • View logs locally	

Fortinet product support for FortiClient

The following Fortinet products work together to support FortiClient in managed mode:

- 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 profiles to endpoints, and the endpoints can connect FortiClient Telemetry to FortiGate or EMS. FortiClient endpoints connect to FortiGate to participate in Security Fabric or compliance enforcement. FortiClient endpoints connect to EMS to be managed in real time.

For information on EMS, see the *FortiClient EMS Administration Guide*, available in the Fortinet Document Library.

FortiManager

FortiManager provides central FortiClient management for FortiGate devices managed by FortiManager. In FortiManager, you can create one or more FortiClient profiles to assign to multiple FortiGate devices. You can also import FortiClient profiles from one FortiGate device and assign the FortiClient profile to other FortiGate devices. When endpoints are connected to managed FortiGate devices, you can use FortiManager to monitor endpoints from multiple FortiGate devices.

For information on FortiManager, see the *FortiManager Administration Guide*, available in the Fortinet Document Library.

FortiGate

FortiGate provides network security. FortiGate devices define compliance rules for NAC (network access control) for connected endpoints, and FortiClient communicates the compliance rules from FortiGate to endpoints. When FortiManager is used, FortiGate devices communicate between endpoints, EMS, and FortiManager.

When FortiClient Telemetry is connected to FortiGate, endpoints can participate in Security Fabric or compliance enforcement.

For information on FortiGate, see the *FortiOS Handbook*, available in the Fortinet Document Library.

FortiAnalyzer

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

For information on FortiAnalyzer, see the *FortiAnalyzer Administration Guide*, available in the Fortinet Document Library.

FortiSandbox

FortiSandbox offers the 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 the FortiSandbox, and applies them locally to all realtime and on-demand AV scanning.

For more information, see the *FortiSandbox Administration Guide*, available in the Fortinet Document Library.

This feature requires a FortiSandbox running version 2.1 or newer and is only available on FortiClient (Windows).

Feature comparison of FortiClient Windows, OS X, and Linux

FortiClient is available for Windows, OS X, and Linux. The following chart shows which modules are available for each OS.

Module	Windows	OS X	Linux
Fabric Telemetry	Yes	Yes	Yes
Compliance	Yes	Yes	Yes
Sandbox Detection	Yes	No	No
AntiVirus	Yes	Yes	Yes
Web Filter	Yes	Yes	No
Application Firewall	Yes	Yes	No
Remote Access	Yes	Yes	No
Vulnerability Scan	Yes	Yes	Yes
Central Management	Yes	Yes	Yes

What’s New in FortiClient 6.0

The following is a list of new features and enhancements in FortiClient 6.0.

- FortiClient 6.0.0 on page 13

FortiClient 6.0.0

The following is a list of new features in FortiClient version 6.0.0.

EMS quarantine file management

FortiClient 6.0 file quarantine functionality has been enhanced to support FortiClient EMS-based central quarantine management. This feature requires EMS 6.0.0.

User data security improvement

FortiClient user data security has been improved so user-specific saved information including the username, saved password, avatar, social ID and VPN information is not accessible to other users using the same device.

New FortiClient GUI

FortiClient 6.0.0 introduces a new UI that improves user experience and provides a refreshed look and feel. The new navigation bar provides up-to-date status information of all features while making them more accessible.

Improved FortiSandbox Detection techniques

Sandbox Detection has been enhanced in FortiClient 6.0 for better detection and interception of file transfers so files can be sent to FortiSandbox for behavior analysis.

Installed Software Inventory

FortiClient now sends all installed software application information to EMS so it can be displayed in the Software Inventory. This feature requires EMS 6.0.0.

Customize system quarantine message

FortiClient Console can now display a customized quarantine message. This feature requires EMS 6.0.0.

FortiClient installs and runs as a 64-bit process on 64-bit platforms

FortiClient 6.0.0 now supports 64-bit installation.

Linux support

FortiClient 6.0.0 introduces expanded platform coverage to include Linux support. FortiClient Linux 6.0.0 supports Fabric Agent, Vulnerability Detection, Anti-Malware and Sandbox Threat Intelligence (no file submission). FortiClient (Linux) can be centrally managed using FortiClient EMS. Note the FortiClient 6.0.0 Administration Guide is mainly written for FortiClient (Windows); not all features described are available for FortiClient (Linux).

Note FortiClient supports standalone SSL VPN for Linux with the standalone SSL VPN client. This feature is not part of FortiClient (Linux) 6.0.0. See Standalone SSL VPN client on page 115.

Getting Started

FortiClient can be used in standalone or managed mode. This section describes how to get started with each mode. It also includes key concepts that administrators and endpoint users should be aware of when using FortiClient in managed mode.

Getting started with standalone mode

In standalone mode, FortiClient software is installed to computers or devices that have Internet access and are running a supported operating system. After FortiClient is installed, FortiClient automatically connects to FortiGuard Center to protect the computer or device.

To get started with FortiClient in standalone mode:

1. Prepare to install FortiClient. See Provisioning Preparation on page 24.
   During installation, endpoint users choose which FortiClient modules to install. See FortiClient setup types and modules on page 28.
2. Install FortiClient on computers or devices with Internet access. See Provisioning on page 32.
3. Launch FortiClient.
   FortiClient connects to the Fortinet FortiGuard server to protect the computer.
4. Configure FortiClient settings. See Settings on page 116.
5. Configure the installed components.
   Depending on what FortiClient modules were installed, endpoint users can configure one, more, or all of the following modules:
   - Sandbox Detection on page 75
   - Antivirus on page 61
   - Web Filter on page 86
   - Remote Access on page 100
6. Use the installed modules using the tabs in FortiClient.
   Depending on what modules were installed, one, more, or all of the following tabs are available in FortiClient:
   - Malware Protection
   - Web Filter
   - Application Firewall
   - Vulnerability Scan on page 93
   - Remote Access

The *Compliance & Telemetry* tab is visible but not used in standalone mode.

Getting started with managed mode

In managed mode, FortiClient software is used with FortiGate or EMS. Another option is integrated mode where FortiGate and EMS are used together with FortiClient.

In managed mode, FortiClient software is installed to computers or devices on your network that have Internet access and are running a supported operating system. The computers or devices are referred to as endpoints. After FortiClient software is installed on endpoints, FortiClient performs the following actions:

- Automatically connects to FortiGuard Center to protect the endpoint
- Automatically attempts to connect FortiClient Telemetry to FortiGate or EMS

The endpoint user confirms the request to complete the FortiClient Telemetry connection to FortiGate or EMS.

Administrators can optionally configure a FortiClient Telemetry connection that requires no confirmation by the endpoint user. See Custom FortiClient installation files on page 31.

After FortiClient Telemetry is connected to FortiGate or EMS, FortiClient receives a profile from FortiGate and/or EMS, and the endpoint is managed.

To get started with FortiClient in managed mode:

1. (Administrators) Configure FortiGate and/or EMS to work with FortiClient.
   The following table identifies where to find information about configuring FortiGate and EMS.

FortiGate	See the *FortiOS Handbook - Security Profiles*.
EMS	See the *FortiClient EMS Administration Guide*.

2. (Administrators) Prepare to provision FortiClient. See Provisioning Preparation on page 24.
   Administrators can choose which FortiClient modules to install. See FortiClient setup types and modules on page 28.
3. (Administrators) Provision FortiClient on endpoints. See Provisioning on page 32.
   After FortiClient installs on endpoints, FortiClient Telemetry attempts connection to FortiGate or EMS. See FortiClient Telemetry on page 44.

   After FortiClient Telemetry connects to FortiGate or EMS, FortiClient receives a profile from FortiGate and/or EMS. The computer with FortiClient installed and FortiClient Telemetry connected is now a managed endpoint.
4. (Administrators) Manage endpoints using EMS. Administrators can also use FortiOS to monitor endpoints.
5. (Endpoint users) Configure the installed components using FortiClient.
   Depending on what FortiClient modules were installed, whether FortiGate compliance rules are used, and whether an EMS administrator has locked settings, endpoint users can configure none or some of the following modules:
   - Sandbox Detection
   - AntiVirus
   - Web Filter
   - Application Firewall
   - Remote Access
6. (Endpoint users) Use the installed modules in FortiClient.
   Depending on what modules were installed, one, more, or all of the following tabs are available in FortiClient:

- Compliance & Telemetry
- Malware Protection
- Web Filter
- Application Firewall
- Vulnerability Scan
- Remote Access

Managed mode concepts

This section introduces the following concepts related to administering FortiClient in managed mode:

- Terminology on page 17
- FortiGate and FortiClient profiles on page 18
- EMS and endpoint profiles on page 20
- Telemetry connection options on page 20
- Telemetry gateway IP lists on page 22
- EMS and automatic upgrade of FortiClient on page 23

In FortiOS, administrators configure a *FortiClient Profile*, and in EMS administrators configure an *endpoint profile*, and these profiles can be downloaded to FortiClient in managed mode. Unless referring specifically to a profile created by using FortiOS or EMS, this guide uses the term *profile* when referring to a FortiClient Profile or endpoint profile received by FortiClient.

Terminology

The following clarifies the terminology used in the following sections.

Term	Definition
Managed mode	FortiClient used with FortiGate or EMS.
Integrated mode	FortiClient used with FortiGate and EMS. In this scenario, FortiClient connects FortiClient Telemetry to FortiOS and EMS.
Fabric Telemetry connection	Connection between FortiClient and FortiOS when FortiClient is used with FortiGate.
Management Telemetry connection	Connection between FortiClient and EMS when FortiClient is used with EMS.

Term	Definition
Endpoint	Computer or device where FortiClient is installed. An endpoint has Internet access and is running a supported operating system.
Connect FortiClient Telemetry	Establish connection between FortiClient and FortiGate or FortiClient and EMS. This is also referred to as registering FortiClient to FortiGate/EMS.
Profile	XML configuration file provided from FortiGate or EMS to the endpoint when in managed or integrated mode. In FortiOS, administrators configure a *FortiClient Profile*. This profile defines compliance rules for endpoint access to the network through FortiGate. It also defines how FortiGate handles endpoints that fail to comply with compliance rules. In EMS, administrators configure an *endpoint profile*. This profile defines the configuration for FortiClient software on endpoints. Unless referring specifically to a profile created using FortiOS or EMS, this guide uses the term profile when referring to a FortiClient Profile or an endpoint profile received by FortiClient.

FortiGate and FortiClient profiles

In FortiOS, administrators can configure a FortiClient profile and apply the profile to endpoints. The profile achieves the following goals:

- Defines compliance rules for endpoint access to the network through FortiGate
- Defines the non-compliance action for FortiGate—that is, how FortiGate handles endpoints that fail to comply with compliance rules

Compliance rules

FortiGate compliance rules define what configuration FortiClient software and the endpoint must have for the endpoint to maintain access to the network through FortiGate.

FortiOS 6.0.0 and later versions use one of the following two methods to determine endpoint compliance. The FortiOS configuration determines which method is used. FortiOS versions prior to 6.0.0 only use the second method below to determine endpoint compliance. In both cases, FortiClient must be installed on the endpoint.

1. An endpoint is considered compliant if FortiClient is managed by the EMS server authorized in FortiOS.
2. An endpoint is considered compliant if it complies with the specific compliance rules configured in FortiOS. The following list shows a sample of the compliance rules administrators can enable or disable in a FortiClient profile using the FortiOS GUI:
    - Telemetry data
    - Endpoint Vulnerability Scan on client
    - System compliance:
        - Minimum FortiClient version
        - What log types FortiClient will send to FortiAnalyzer

- What applications/processes are running on client. May include requirements for specific signatures.

  Configuring compliance rules for running applications requires using the FortiOS CLI to set the following fields: `application-check-rule`, `process-name`, and `app-sha256-signature`. The `app-sha256-signature` field is optional. See the *FortiOS CLI Reference*.

- Security posture check:
  - Realtime protection
  - Third party Antivirus on Windows
  - Web filter
  - Application firewall

Administrators can also define additional compliance rules using the FortiOS CLI.

Although the compliance rules define what configuration FortiClient software and the endpoint must have, the FortiClient profile from FortiGate does not include any configuration information. The endpoint user or administrator is responsible for configuring FortiClient to adhere to the compliance rules. An administrator can use EMS to configure FortiClient.

Non-compliance action

In addition to compliance rules, the FortiClient profile also defines how FortiGate handles non-compliant endpoints. FortiGate can block and quarantine endpoints, or FortiGate can warn endpoints about the non-compliance but allow network access. Administrators set the rules and non-compliance action using FortiOS, and FortiGate enforces the rules.

FortiOS 5.6.0 and later versions allow FortiGate to enforce compliance rules for FortiClient endpoints.

FortiClient displays compliant and non-compliant status and information about how endpoint users can return non-compliant endpoints to a compliant state. The administrator or endpoint user is responsible for reading the information in FortiClient and updating FortiClient software on the endpoint to adhere to the compliance rules. Endpoint users can edit settings in FortiClient not controlled by the compliance rules or EMS.

Compliance rules configured using the CLI

When using FortiOS to create FortiClient profiles, administrators can configure some rules only by using the FortiOS CLI. Administrators must use the CLI to configure the following options:

- Allowed operating system for endpoints
- Registry entries for endpoints
- File in the file system on endpoints

See the *FortiOS CLI Reference*.

EMS and endpoint profiles

In EMS, administrators can configure an endpoint profile and apply the profile to 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, 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*, available in the Fortinet Document Library.

Telemetry connection options

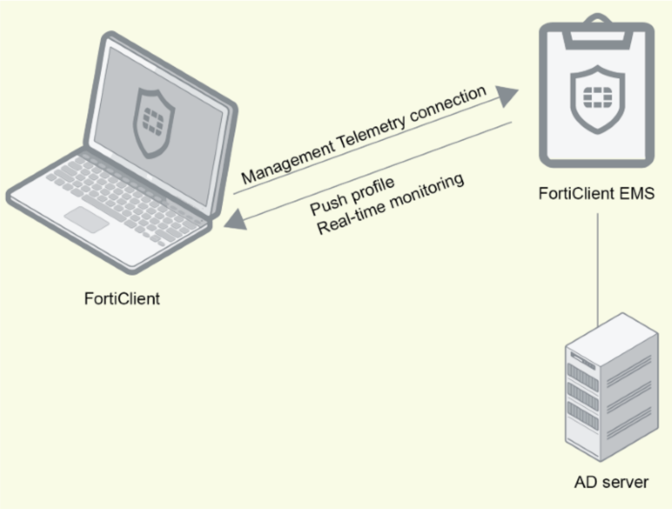
FortiClient Telemetry can connect to the following products:

- EMS on page 20
- FortiGate on page 21
- FortiGate and EMS integration on page 21

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

EMS

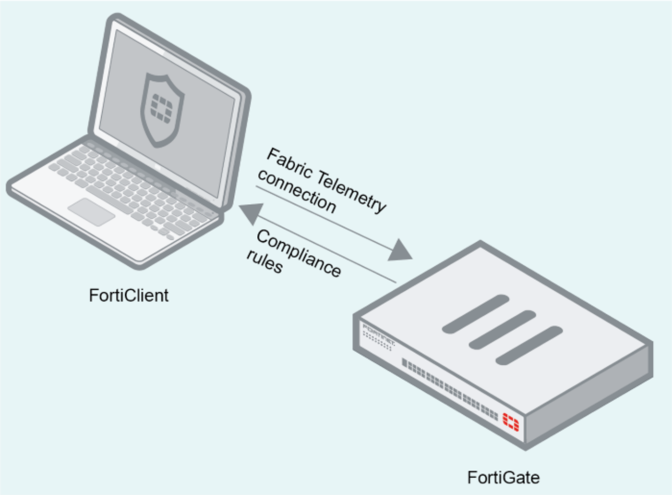
In this scenario, EMS provides FortiClient endpoint provisioning. FortiClient connects Telemetry to EMS to receive configuration information in an endpoint profile from EMS. Note this scenario does not support compliance; it is only for central management of endpoints. Note only EMS can control the connection between FortiClient and EMS. Any changes to the connection must be made 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

In this configuration, FortiClient Telemetry is connected to FortiGate, and FortiClient receives a profile from FortiGate. The profile contains the compliance rules for FortiClient, but not any configuration information for FortiClient. NAC and compliance can be supported.



FortiGate and EMS integration

In this configuration, FortiClient Telemetry connects to FortiGate to confirm compliance. NAC and compliance are supported. FortiClient Telemetry also connects to EMS to receive a profile of configuration information. This configuration is sometimes called integrated mode.

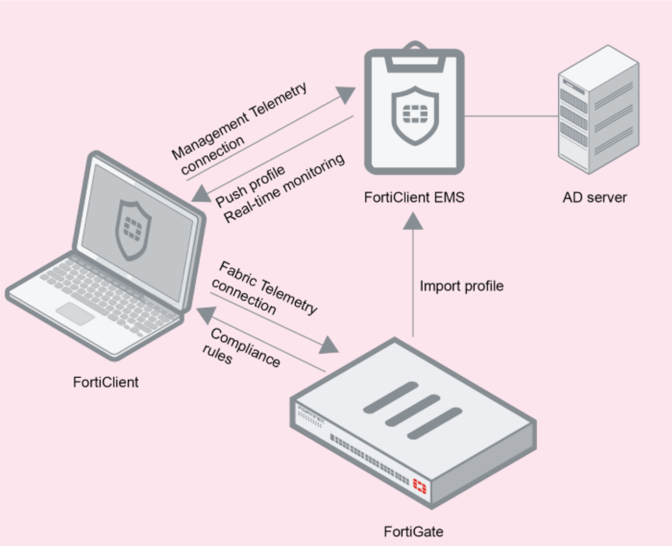
FortiGate does not provide configuration information for FortiClient and the endpoint. Endpoint users must manually configure FortiClient or an administrator must configure FortiClient using an EMS endpoint profile.

Following is a summary of how the FortiClient Telemetry connection works in integrated mode:

- FortiClient Telemetry connects to FortiGate. This is the Fabric Telemetry connection.
- FortiClient Telemetry connects to EMS. This is the Management Telemetry connection.
- FortiClient connects to FortiGate. Depending on the FortiGate configuration, one of the following happens:
  - FortiGate considers the endpoint compliant if FortiClient is installed and is being managed by the EMS server authorized in FortiOS.
  - FortiClient receives a profile of specific compliance rules from the FortiGate.
- FortiClient receives a profile of configuration information from EMS.

Administrators should ensure the configuration information from EMS matches the compliance rules set on FortiGate to avoid conflicting settings.

EMS can also import a profile from FortiOS, then push it to FortiClient.



Telemetry gateway IP lists

The Telemetry gateway IP list is a list of gateway IP addresses that FortiClient in managed mode can use to connect Telemetry to FortiGate 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.

After FortiClient is installed on the endpoint and Telemetry is connected to FortiGate and/or EMS, endpoint users can view the Telemetry gateway IP list in FortiClient. See View gateway IP lists on page 1.

Configure Telemetry gateway IP lists (EMS)

FortiClient EMS includes the option to create one or more Telemetry gateway IP lists. The list can include IP addresses for EMS and for FortiGate. 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*.

Configure Telemetry gateway IP lists (FortiGate)

If administrators are using FortiGate without EMS, administrators can add Telemetry gateway IP addresses to the FortiClient installer using the Configurator Tool. See Custom FortiClient installation files on page 31.

EMS and automatic upgrade of FortiClient

When managing FortiClient endpoints via EMS, 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. If installing FortiClient in managed mode, administrators should also be aware of the licensing requirements.

This section also identifies the firmware images and tools available for FortiClient and where you can download FortiClient installers.

- Installation requirements on page 24
- Licensing on page 26
- Required services and ports on page 26
- FortiClient setup types and modules on page 28
- Firmware images and tools on page 29
- Where to download FortiClient installation files on page 31
- Custom FortiClient installation files on page 31

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 6.0.0 does not support Microsoft Windows XP, Microsoft Windows Vista, or Microsoft Windows 8.	• Microsoft Windows compatible computer with Intel processor or equivalent • 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 dial-up 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 • 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 dial-up connections • Ethernet NIC for network connections • Wireless adapter for wireless network connections • Adobe Acrobat Reader for viewing documentation • MSI installer 3.0 or later
• macOS Sierra (version 10.12) • macOS High Sierra (version 10.13)	• 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

For Microsoft Windows servers, FortiClient supports the AntiVirus and Vulnerability Scan features.

Licensing

FortiClient in standalone mode does not require a license.

FortiClient in managed mode requires a license. In managed mode, FortiClient licensing is applied to FortiGate or EMS.

When using the ten (10) free licenses for FortiClient in managed mode, support is provided on the Fortinet Forums. Phone support is not provided when using the free licenses. Phone support is provided for paid licenses.

FortiClient licenses for FortiGate

FortiGate 30 series and higher models include a FortiClient license for ten (10) free connected endpoints. For additional connected endpoints, you must purchase a FortiClient license subscription.

Note that FortiOS 6.0.0 and later versions only support the à la carte FortiClient Telemetry license available in batches of 100 clients. This license is compatible with FortiOS 5.6.0 and later versions. FortiOS 6.0.0 does not support other older FortiOS-side Telemetry and Compliance licenses.

If upgrading FortiOS 5.4 or 5.6 with a license other than the à la carte license to 6.0.0, the license is retained until its expiry, after which you must purchase the à la carte FortiClient Telemetry license. Contact your Fortinet sales representative for information.

For a video about applying FortiClient licenses to FortiGate, see the*How to Purchase or Renew FortiClient Endpoint Subscription* video.

FortiClient licenses for EMS

EMS includes a FortiClient license for ten (10) free connected endpoints for evaluation. For additional connected endpoints, you must purchase a FortiClient license subscription. Contact your Fortinet sales representative for information about FortiClient licenses.

For a video about applying FortiClient licenses to EMS, see the *How to License FortiClient EMS video*.

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 (FortiClient EMS) and/or compliance enforcement (FortiGate)	TCP	8013	Outgoing	GUI
FortiClient upload	Used for FortiClient to upload logs and diagnostics to the EMS server	TCP	8014	Outgoing	N/A
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 FortiGate	TCP	443 (default)	Outgoing	GUI
FortiAnalyzer/FortiManager	Upload logs to FortiAnalyzer or FortiManager. FortiClient must connect to FortiGate or EMS to send logs to FortiAnalyzeror FortiManager.	TCP	514	Outgoing	N/A
Remote access - IPsec VPN	Establish VPN connection to FortiGate	UDP	IKE 500 ESP (IP 50) NAT-T 4500	Outgoing	N/A
FortiAuthenticator/FortiGate	Single Sign On mobility agent, FSSO	TCP	8001 (default)	Outgoing	GUI
FortiGuard	URL rating	UDP	8888 (default)	Outgoing	Change to port 53 via XML config file
	Antivirus/vulnerability signatures update	TCP	80	Outgoing	N/A
	Cloud-based	TCP	80	Outgoing	N/A

Communication	Usage	Protocol	Port	Incoming/Outgoing	How to customize
	behavior scan (CBBS)/applications that use cloud services				
FortiManager	Use a FortiManager device 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 FortiClient EMS, see the *FortiClient EMS Administration Guide* on the Fortinet Document Library.

FortiClient setup types and modules

The Advanced Persistent Threat (APT) module is available only for FortiClient (Windows).

When you install FortiClient, you can choose which setup type and modules to install:

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

The following table summarizes the impact of the options:

Setup type	Description	Impact on FortiClient console
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: • *Compliance & Telemetry* • *Vulnerability Scan*
Secure Remote Access	Optional. Supports SSL and IPsec VPN access.	Displays the *Remote Access* tab.
Advanced Persistent Threat (APT) Components	Optional. Supports FortiSandbox.	Enables *Sandbox Detection* on the *Malware Protection* tab to connect to a FortiSandbox unit.

Setup type	Description	Impact on FortiClient console
Additional Security Features	Optional. Supports AntiVirus, Web Filtering, Application Firewall, and Single Sign On. You can 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 single sign on feature. When a security feature is not selected, the tab is hidden from view in FortiClient Console.

EMS and FortiClient setups

For FortiClient in managed mode, you can use an EMS profile to disable installed components in FortiClient Console but you cannot use an EMS profile to enable uninstalled components in FortiClient Console. See EMS and endpoint profiles on page 20.

For example, if you install FortiClient with APT components selected, *Sandbox Detection* is enabled on the *Malware Protection* tab in FortiClient Console, and you can use an EMS profile to disable *Sandbox Detection*. However, if you install FortiClient with APT components cleared, *Sandbox Detection* is disabled on the *Malware Protection* tab inFortiClient Console and you cannot use an EMS profile to enable *Sandbox Detection*.

FortiGate compliance and FortiClient setups

For endpoints that will have FortiClient Telemetry connected to FortiGate with endpoint compliance enabled, ensure FortiClient is installed with the setup required by the FortiGate compliance rules. See Compliance rules on page 18.

For example, if the FortiGate compliance rules require the *Web Filter* tab to be enabled in FortiClient Console, FortiClient must be installed with *Additional Features* and *Web Filtering* selected to meet the compliance rules. If FortiClient is installed with an incorrect setup for the compliance rules, you must uninstall then FortiClient with the setup required by the compliance rules.

Firmware images and tools

Firmware images and tools are available for Microsoft Windows, Mac OS X, and Linux. See Custom FortiClient installation files on page 31.

Microsoft Windows

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

- FortiClientSetup_6.0.xx.xxxx.exe
  Standard installer for Microsoft Windows (32-bit).
- FortiClientSetup_6.0.xx.xxxx.zip
  A zip package containing FortiClient.msi and language transforms for Microsoft Windows (32-bit). Some properties of the MSI package can be customized with FortiClient Configurator tool.
- FortiClientSetup_6.0.xx.xxxx_x64.exe
  Standard installer for Microsoft Windows (64-bit).
- FortiClientSetup_6.0.xx.xxxx_x64.zip
  A zip package containing FortiClient.msi and language transforms for Microsoft Windows (64-bit). Some properties of the MSI package can be customized with FortiClient Configurator tool.
- FortiClientTools_6.0.xx.xxxx.zip
  A zip package containing miscellaneous tools, including VPN Automation files:

The following tools and files are available in the FortiClientTools_6.0.xx.xxxx.zip file:

- FortiClientVirusCleaner
  A virus cleaner.
- OnlineInstaller
  This file downloads and installs the latest FortiClient file from the public FDS.
- SSLVPNcmdline
  Command line SSL VPN client.
- SupportUtils
  Includes diagnostic, uninstallation, and reinstallation tools.
- VPNAutomation
  A VPN automation tool.

Mac OS X

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

- FortiClient_6.0.x.xxx_macosx.dmg
  Standard installer for Mac OS X.
- FortiClientTools_6.0.x.xxx_macosx.tar
  FortiClient includes various utility tools and files to help with installations.

The following file is available in the FortiClientTools `.tar` file:

- OnlineInstaller
  This file downloads and installs the latest FortiClient file from the public FDS.

Linux

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

- forticlient_6.0.0.xxxx_amd64.deb
  Standard installer package for Ubuntu.
- forticlient_6.0.0.xxxx_x86_64.rpm
  Standard installer package for Red Hat and CentOS.

Where to download FortiClient installation files

You can download the FortiClient installation files from the following sites:

- Fortinet Customer Service & Support
  Requires a support account with a valid support contract. Download the Microsoft Windows (32-bit/64-bit), Mac OS X, or Linux installation file.
- FortiClient homepage
  Download the FortiClient online installation file. The installer file performs a virus and malware scan of the target system prior to installing FortiClient.

Custom FortiClient installation files

The FortiClient Configurator Tool is available from the Fortinet Developer Network.

An account is required to access the Fortinet Developer Network. Information about creating an account is available on FNDN

You can use the free FortiClient Configurator Tool to create customized FortiClient installation files. See FNDN for details.

Starting with FortiClient 5.6.0, the FortiClient Configurator Tool is available for free download from the *Tools > Personal Toolkit* section of FNDN.

Note FortiClient 6.0.0 does not support the FortiClient Rebranding Tool.

Provisioning

FortiClient can be installed on a standalone computer using the installation wizard or deployed to multiple Microsoft Windows systems using Microsoft Active Directory (AD).

You can use EMS to deploy FortiClient to multiple Microsoft Windows systems. See the *FortiClient EMS Administration Guide*.

Installing FortiClient on computers

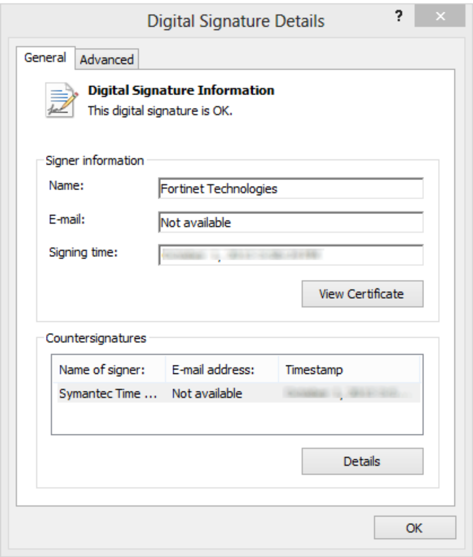
The following section describes how to install FortiClient on a computer running a Microsoft Windows, Mac OS X, or Linux operating system.

Microsoft Windows computer

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

When installing FortiClient, it is recommended to use the FortiClientOnlineInstaller file. This file launches the FortiClient Virus Cleaner which scans the target system prior to installing the FortiClient application. The FortiClientOnlineInstaller file always installs the latest version of FortiClient available on the FortiGuard Distribution Network (FDN), not the version of FortiClient referenced in the filename or listed on the Customer Service & Support site.

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.



Digital Signature Details

General | Advanced

Digital Signature Information
This digital signature is OK.

Signer information

Name: Fortinet Technologies
E-mail: Not available
Signing time: [redacted]

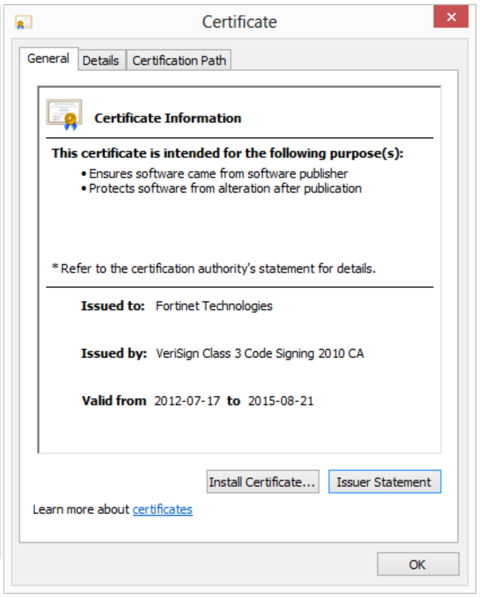
View Certificate

Countersignatures

Name of signer:	E-mail address:	Timestamp
Symantec Time ...	Not available	[redacted]

Details

OK



Certificate

General | Details | Certification Path

Certificate Information

This certificate is intended for the following purpose(s):
- Ensures software came from software publisher
- Protects software from alteration after publication

* Refer to the certification authority's statement for details.

Issued to: Fortinet Technologies

Issued by: VeriSign Class 3 Code Signing 2010 CA

Valid from 2012-07-17 **to** 2015-08-21

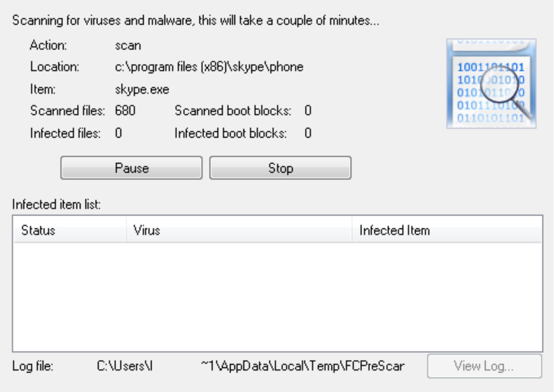
Install Certificate... | Issuer Statement

Learn more about certificates

OK

To install FortiClient (Windows):

1. Double-click the FortiClient executable file. The *Setup Wizard* launches.
   When using the FortiClientOnlineInstaller file, the FortiClient Virus Cleaner runs before launching the *Setup Wizard*.
   If a virus is found that prevents the infected system from downloading the new FortiClient package, see Installing FortiClient on infected systems on page 37.



Scanning for viruses and malware, this will take a couple of minutes...

Action: scan
Location: c:\program files (x86)\skype\phone
Item: skype.exe
Scanned files: 680   Scanned boot blocks: 0
Infected files: 0   Infected boot blocks: 0

Infected item list:

Status	Virus	Infected Item

Log file: C:\Users\l ~1\AppData\Local\Temp\FCPreScar

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 *Choose Setup Type* screen displays.
4. Select one or more of the following setup types:
   The *Security Fabric Agent* option is enabled by default, and you cannot deselect it. See FortiClient setup types and modules on page 28.
   - *Security Fabric Agent*: Endpoint telemetry, host vulnerability scanning and remediation
   - *Secure Remote Access*: VPN components (IPsec and SSL) will be installed

  - *Advanced Persistent Threat (APT) Components*: FortiSandbox detection and quarantine features
  - *Additional Security Features*: AntiVirus, Web Filtering, Single Sign On, Application Firewall

5. Click *Next* to continue.
   The *Destination Folder* screen displays.
6. (Optional) Click *Change* to choose an alternate folder destination for installation.
7. Click *Next* to continue.
   FortiClient searches the target system for other installed antivirus software. If found, FortiClient displays the *Conflicting Antivirus Software* page. You can exit the current installation and uninstall the antivirus software, disable the antivirus feature of the conflicting software, or continue with the installation with FortiClient realtime protection disabled.

   Note FortiClient automatically disables realtime protection when:
   a. The OS is a server, or
   b. Exchange Server is detected, or
   c. SQL Server is detected.

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

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

8. Click *Next*. The *Ready to install FortiClient* screen displays.
9. Click *Install*.
10. 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.
11. FortiClient attempts to connect FortiClient Telemetry to the FortiGate.
    If the FortiGate cannot be located on the network, manually connect FortiClient Telemetry. See Connecting FortiClient Telemetry manually on page 47.

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

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

Microsoft Server

You can install FortiClient on a Microsoft Windows Server 2008 R2, 2012, or 2012 R2 server. You can use the regular FortiClient Windows image for Server installations.

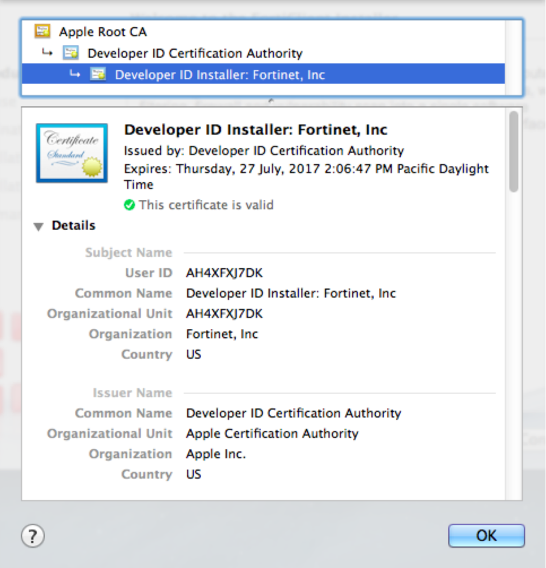
Refer to the Microsoft knowledge base for caveats on installing antivirus software in a server environment. See the Microsoft Anti-Virus exclusion list.

Mac OS X computer

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

To install FortiClient (Mac OS X):

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



Apple Root CA
↳ Developer ID Certification Authority
↳ Developer ID Installer: Fortinet, Inc

Developer ID Installer: Fortinet, Inc
Issued by: Developer ID Certification Authority
Expires: Thursday, 27 July, 2017 2:06:47 PM Pacific Daylight Time
✓ This certificate is valid

▼ **Details**

Subject Name
User ID AH4XFXJ7DK
Common Name Developer ID Installer: Fortinet, Inc
Organizational Unit AH4XFXJ7DK
Organization Fortinet, Inc
Country US

Issuer Name
Common Name Developer ID Certification Authority
Organizational Unit Apple Certification Authority
Organization Apple Inc.
Country US

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. Perform one of the following actions:
   - Click *Install* to perform a standard installation on this computer, which includes the following modules: Security Fabric Agent and Secure Remote Access.
   - Click *Customize* to choose which FortiClient modules to install. See FortiClient setup types and modules on page 28.
8. Depending on your system, you may be prompted to enter your system password.
9. After the installation completes successfully, Click *Close* to exit the installer.
   FortiClient has been saved to the *Applications* folder.

10. Double-click the FortiClient icon to launch the application. The application console loads to your desktop. Click the lock icon in FortiClient Console to make changes to the FortiClient configuration.

Linux computer

The following instructions will 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*.

Installing FortiClient from repo.fortinet.com

You can install FortiClient from the repository at repo.fortinet.com.

Installing on Red Hat or CentOS

1. Add the repository by using the following command:
```
sudo yum-config-manager --add-repo http://repo.fortinet.com/repo/centos/7/os/x86_
     64/fortinet.repo
```
2. Install FortiClient by using the following command:
```
sudo yum install forticlient
```

Installing on Ubuntu

1. Install the gpg key by using the following command:
```
wget -O - http://repo.fortinet.com/repo/ubuntu/DEB-GPG-KEY | sudo apt-key add -
```
2. Add the following line in `/etc/apt/sources.list`:
```
deb [arch=amd64] http://repo.fortinet.com/repo/ubuntu/ xenial multiverse
```
3. Update package lists by using the following command:
```
sudo apt-get update
```
4. Install FortiClient by using the following command:
```
sudo apt install forticlient
```

Installing FortiClient using a downloaded installation file

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.

Installing 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.

   If installing FortiClient on Ubuntu 17.10 or 18.04, install the dependencies: `libgconf2-4` and `libgconf-2-4` by using the following command:

```
$ sudo apt-get install <FortiClient deb file> libgconf2-4 libgconf-2-4
```

Installation folder and running processes

The FortiClient installation folder is `/usr/bin/forticlient`. The config.xml file is in the `/etc/forticlient` directory. 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 antivirus 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 of the new FortiClient package, use the following process:

- Boot into “safe mode with networking” (which is required for the FortiClient installer to download the latest signature packages from the Fortinet Distribution Network).
- Run the FortiClient installer.

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

Microsoft Windows will not allow FortiClient installation to complete in safe mode. An error message is generated. It is necessary to reboot back 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 need to remove the unique identifier from the FortiClient application. You will encounter problems with 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 will generate its own unique identifier the first time the computer is started.

To include a FortiClient installation in a hard disk image:

1. Install and configure the FortiClient application to suit your requirements.
   You can use a standard or a customized installation package.
2. Right-click the FortiClient icon in the system tray and select *Shutdown FortiClient*.
3. From the folder where you expanded the 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 the user to restart the machine if necessary.
`/forcerestart`	Always restarts the machine after installation.
`/uninstall`	Uninstalls FortiClient.
`/log"<LogFile>"`	Creates a log file with the specified name.

The following example installs FortiClient build 1131 in quiet mode, creating a log file with the name "Log":

```
FortiClientSetup_6.0.0.1131_x64.exe /quiet /log"Log"
```

Deploying FortiClient using Microsoft AD servers

There are multiple ways to deploy FortiClient MSI packages to endpoints including using Microsoft Active Directory (AD). See Firmware images and tools on page 29.

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

To use Microsoft AD to deploy FortiClient:

1. On your domain controller, create a distribution point.
2. Log on to the server computer as an administrator.
3. Create a shared network folder where the FortiClient MSI installer file will be 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 wish to distribute the FortiClient software to into the newly-created OU.
8. 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*.
9. Expand the Group Policy Object container and find the GPO you just created. Right-click the GPO and select *Edit*. The Group Policy Management Editor MMC Snap-in opens.
10. Expand *Computer Configuration* > *Policies* > *Software Settings*. Right-click *Software Settings* and select *New* > *Package*.
11. 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.
12. If you wish to expedite the installation process, on the server and client computers, force a GPO update.
13. 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

To use 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 will now be able to 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.

Upgrading FortiClient

For information about supported upgrade paths for FortiClient, see the *FortiClient Release Notes*.

For FortiClient in managed mode, an administrator may control FortiClient upgrades for you, and you may be unable to manually upgrade FortiClient. See EMS and automatic upgrade of FortiClient on page 23.

During a FortiClient upgrade to 6.0.0, FortiClient installs the same features that were previously installed. If you want to install different features, you must uninstall the previous version of FortiClient, and install FortiClient 6.0.0 with the desired features.

For FortiClient in managed mode, when an administrator deploys a FortiClient upgrade from EMS to endpoints running a Windows operating system, an *Upgrade Schedule* dialog box 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 box displays. The endpoint user can postpone the reboot for a maximum of 24 hours. Before the mandatory reboot occurs, a FortiClient dialog box 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 Console.

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 to FortiAnalyzer or FortiManager on page 117.

To view user details:

1. Click the user avatar in the upper left corner of FortiClient Console 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 42 and Adding phone number and email address manually on page 43.
Email	Displays the endpoint user's email address if added by the endpoint user. See Retrieving user details from cloud applications on page 42 and Adding phone number and email address manually on page 43.
Get personal info from	Displays the source of the endpoint user's personal information. The options are user-specified, from the OS, and from cloud applications: LinkedIn, Google, and Salesforce. The user can click *User Specified* to select an image 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, picture, phone number, and email address. See Retrieving user details from cloud applications on page 42.
Status	Displays whether the endpoint is online or offline, on-net or off-net. See On-net / off-net status with FortiGate and EMS on page 52.
Hostname	Displays the name of the endpoint where FortiClient is installed.
Domain	Displays the name of the domain to which the endpoint is connected, if applicable.

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 Console displays the retrieved information. The information is encrypted and can only be accessed by FortiClient. FortiClient does not retrieve or save the password for the user's 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 Console 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 Console.
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 Console. 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 to FortiAnalyzer or FortiManager on page 117.

You can manually specify a picture for FortiClient to use and edit the phone number and email address. See Specifying user picture manually on page 43 and Adding phone number and email address manually on page 43.

To retrieve user details from a cloud application:

1. Click the user avatar in the upper left corner of FortiClient Console.
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 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 Console.

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 Console.
2. Click *Add Phone*, type a phone number, and press Enter.
3. Click *Add Email*, type an 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 Console.
2. Click the phone number or email address, edit the information, and press Enter.

Specifying user picture manually

Although FortiClient can retrieve a picture from Windows, Active Directory, or a cloud application, you can add a picture to FortiClient by taking a photo or uploading a picture.

To specify a user picture:

1. Click the user avatar in the upper left corner of FortiClient Console.
2. Under *Get personal info from*, click *User Input*.
3. Select an image file.

Compliance & Telemetry

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

When FortiClient Telemetry is connected to FortiGate and endpoint control is enabled by the FortiGate administrator, the *Compliance & Telemetry* tab displays whether FortiClient and the endpoint are compliant with the FortiGate compliance rules and provides information about maintaining a compliant endpoint.

FortiClient Telemetry

In managed mode, FortiClient uses a gateway IP address to connect FortiClient Telemetry to FortiGate or EMS.

When your administrator has configured FortiGate for network access control (NAC), you must connect FortiClient Telemetry to FortiGate to access the network, and you must also maintain a compliant status to retain access to the network. See Compliance on page 47.

For information about creating Telemetry gateway IP lists, see Telemetry gateway IP lists on page 22.

This section applies only to FortiClient in managed mode.

Telemetry data

When FortiClient Telemetry is connected to FortiGate and/or EMS, the following data about the endpoint and its workload is collected and sent to FortiGate and/or EMS:

- Hardware information, such as MAC addresses
- Software information, such as the version of operating system on the endpoint
- Identification information, such as user name, user picture, and host name
- Vulnerability information reported by the vulnerability scanning module

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

How FortiClient locates FortiGate or EMS

FortiClient uses the following methods in the following order to locate FortiGate or EMS for Telemetry connection:

- Manually entering the gateway IP address, which means the endpoint user enters the gateway IP address of FortiGate or EMS into FortiClient Console. See Connecting FortiClient Telemetry manually on page 47.

- Telemetry gateway IP list
  FortiClient Telemetry searches for IP addresses in its subnet in the gateway IP list. It connects to the FortiGate in the list that is also in the same subnet as the host system.

  If FortiClient cannot find any FortiGates in its subnet, it attempts to connect to the first reachable FortiGate in the list, starting from the top. The order of the list is maintained as configured in the gateway IP list.
- Default gateway IP address
  The default gateway IP address is specified on the FortiClient endpoint and is used to automatically connect to FortiGate. This method does not support connection to EMS.

  > FortiClient obtains the default gateway IP address from the operating system on the endpoint. The default gateway IP address of the endpoint should be the IP address for the FortiGate interface with Telemetry enabled.

- VPN
- Remembered gateway IP list
  You can configure FortiClient to remember gateway IP addresses when you connect Telemetry to FortiGate or EMS. Later FortiClient can use the remembered IP addresses to automatically connect Telemetry to FortiGate or EMS.

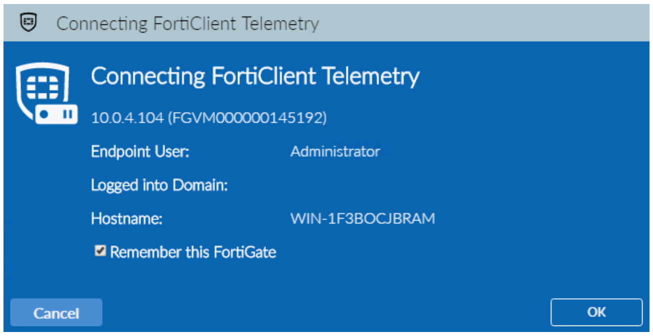
> FortiClient uses the same process to connect Telemetry to FortiGate or EMS after the FortiClient endpoint reboots, rejoins the network, or encounters a network change.

Connecting FortiClient Telemetry after installation

After FortiClient software installation completes on an endpoint, FortiClient automatically launches and searches for FortiGate or EMS to connect FortiClient Telemetry. See How FortiClient locates FortiGate or EMS on page 44.

To connect FortiClient Telemetry after installation:

1. When FortiClient locates a FortiGate or EMS, the *Connecting FortiClient Telemetry* dialog box displays.
   Following is an example of the *Connecting FortiClient Telemetry* dialog box when connecting to a FortiGate:



Connecting FortiClient Telemetry

Connecting FortiClient Telemetry

10.0.4.104 (FGVM000000145192)

Endpoint User: Administrator

Logged into Domain:

Hostname: WIN-1F3BOCJBRAM

☑ Remember this FortiGate

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.
Profile Details	Available only when EMS is detected. Click to display details of the profile that FortiClient will receive after you accept connection to EMS. See EMS and endpoint profiles on page 20.
Remember this FortiGate	Available only when FortiGate is detected. Select this checkbox for FortiClient to remember the gateway IP address of the FortiGate to which you are connecting Telemetry. See Remembering gateway IP addresses on page 46.
Remember this Server	Available only when EMS is detected. Select for FortiClient to remember the gateway IP address of the EMS to which you are connecting Telemetry. See Remembering gateway IP addresses on page 46.

2. Click *OK* to connect FortiClient Telemetry to the identified FortiGate or EMS.
   Alternately, you can click *Cancel* to launch FortiClient software without connecting FortiClient Telemetry. FortiClient launches in standalone mode. You can manually connect FortiClient Telemetry later.

   After FortiClient Telemetry is connected to FortiGate or EMS, FortiClient receives compliance rules from FortiGate and/or a profile from EMS. A system tray bubble message displays once the download is complete.

Remembering gateway IP addresses

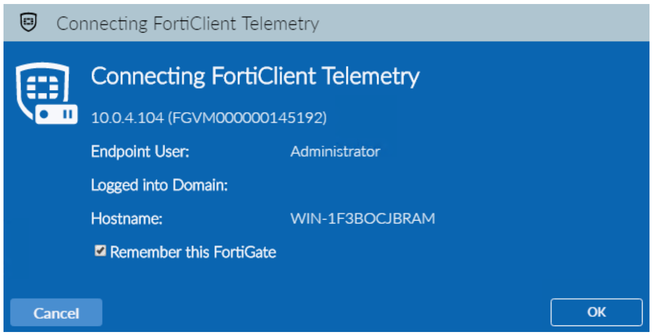
When you confirm Telemetry connection to FortiGate or EMS, you can instruct FortiClient to remember the gateway IP address of the FortiGate or EMS. If a connection key is required, FortiClient remembers the connection password too. FortiClient can remember up to 20 gateway IP addresses for FortiGate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

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

See Forget gateway IP addresses on page 1.

To remember IP addresses for FortiGate or EMS:

1. In the *Connecting FortiClient Telemetry* dialog box, select the *Remember this FortiGate* or *Remember this EMS* (not shown) checkbox.



Connecting FortiClient Telemetry

Connecting FortiClient Telemetry

10.0.4.104 (FGVM000000145192)

Endpoint User: Administrator

Logged into Domain:

Hostname: WIN-1F3BOCJBRAM

☑ Remember this FortiGate

2. Click *Accept*.
   FortiClient remembers the IP address and password, if applicable.

Compliance

Enabling compliance

For FortiClient in standalone mode, the *Compliance & Telemetry* tab is visible, but not used.

For FortiClient in managed mode, an administrator enables and configures the *Compliance & Telemetry* tab using FortiOS.

Connecting FortiClient Telemetry manually

FortiClient Telemetry must be connected to FortiGate to use the compliance feature. Alternately, FortiClient Telemetry can be connected to EMS, but you cannot use the compliance feature when FortiClient Telemetry is connected to EMS. See Telemetry connection options on page 20.

If FortiClient Telemetry was not automatically connected after FortiClient installation, you can manually connect FortiClient Telemetry to FortiGate or EMS.

To manually connect FortiClient Telemetry to FortiGate:

1. Go to the *Compliance & Telemetry* tab.
2. In the *FortiGate or EMS IP* box, type the FortiGate's IP address or FQDN, and click *Connect*.
   FortiClient Telemetry connects to FortiGate, and FortiClient receives a profile of compliance rules from FortiGate.

To manually connect FortiClient Telemetry to EMS:

1. Go to the *Compliance & Telemetry* tab.
2. In the *FortiGate or EMS IP* box, type the EMS's IP address or FQDN, and click *Connect*.
   FortiClient Telemetry connects to EMS, and FortiClient receives a profile of configuration information from EMS.

Note it is considered best practice to connect FortiClient to EMS through deployment from EMS. Connecting FortiClient to FortiClient EMS manually is only recommended for troubleshooting purposes. See the *FortiClient EMS Administration Guide*.

To manually connect FortiClient Telemetry to FortiGate and EMS:

1. Go to the *Compliance & Telemetry* tab.
2. In the *FortiGate or EMS IP* box, type the FortiGate's IP address or FQDN, and click *Connect*.
   FortiClient Telemetry establishes the Fabric Telemetry connection to FortiGate, and FortiClient receives a profile of compliance rules from FortiGate. FortiClient Telemetry also automatically establishes a Management Telemetry connection to EMS, and FortiClient receives a profile of configuration information from EMS.

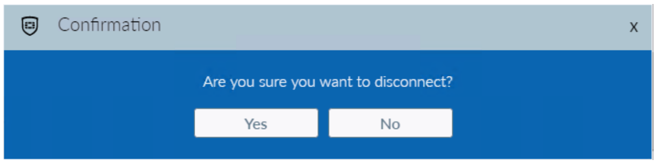
Disconnecting FortiClient Telemetry

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

When FortiClient Telemetry is connected to EMS, 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. See View gateway IP lists on page 1.

To disconnect FortiClient Telemetry:

1. On the *Compliance & Telemetry* tab, click *Disconnect* link. A confirmation dialog box displays.



Are you sure you want to disconnect?

2. Click *Yes* to disconnect FortiClient Telemetry from FortiGate or EMS.

After you disconnect FortiClient Telemetry from FortiGate or EMS, FortiClient Telemetry automatically connects with the FortiGate or EMS when you rejoin the network. See Forget gateway IP addresses on page 1.

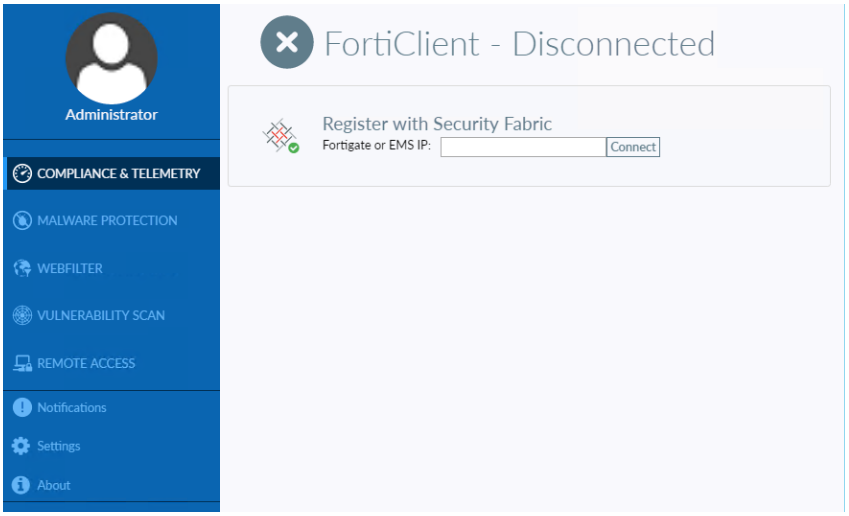
Viewing compliance status

Information available on the *Compliance & Telemetry* tab depends on whether FortiClient is running in standalone mode or managed mode. In managed mode, the information displayed on the *Compliance & Telemetry* tab also depends on whether FortiClient Telemetry is connected to FortiGate or EMS.

Standalone mode

When FortiClient is running in standalone mode, the *Compliance & Telemetry* tab is visible, but not used. The *Compliance & Telemetry* tab is labeled *Disconnected*.

If you want to use the compliance feature, you must connect FortiClient Telemetry to FortiGate.

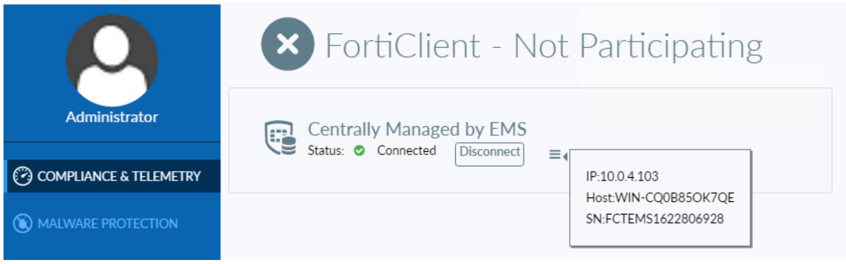


The *Compliance & Telemetry* tab displays the following information:

FortiGate or EMS IP	Type the IP address or FQDN of FortiGate or EMS, and click *Connect* to connect FortiClient Telemetry.
Connect	Click to connect to FortiGate or EMS after populating the *FortiGate or EMS* box with an IP address.

Managed mode with EMS

When FortiClient Telemetry is connected to EMS, compliance is not enforced. The *Compliance & Telemetry* tab is labeled *Centrally Managed by EMS*.



FortiClient - Not Participating

Centrally Managed by EMS

Status: Connected

IP:10.0.4.103
Host:WIN-CQ0B85OK7QE
SN:FCTEMS1622806928

The *Compliance* tab displays the following information:

Compliance information	✕	Indicates FortiClient is not participating in compliance enforcement. Compliance enforcement requires FortiClient Telemetry connection to FortiGate.
EMS information	≡	Displays the host name, IP address, and serial number of the EMS to which FortiClient Telemetry is connected. You can disconnect by clicking *Disconnect*.

Managed mode with FortiGate

When FortiClient Telemetry is connected to FortiGate and the FortiGate administrator has disabled compliance, network access compliance (NAC) is not enforced. The *Compliance & Telemetry* tab displays *Not Participating* and you are not required to maintain a compliant status to access the network.

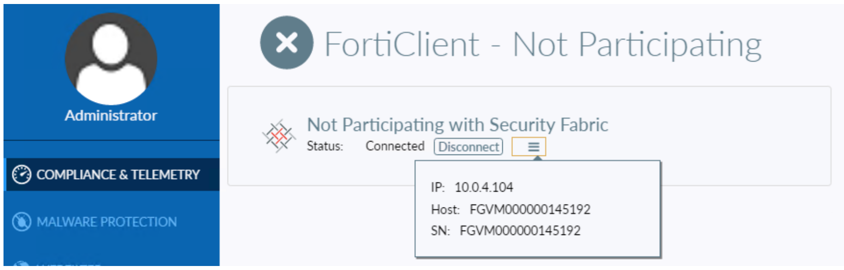
When FortiClient Telemetry is connected to FortiGate and the FortiGate administrator has enabled compliance, NAC is enforced and you may be required to maintain a compliant status to access the network, depending on how FortiGate enforces NAC.

If FortiGate is configured to block network access for endpoints with non-compliant status, certain requirements must be met to maintain a compliant status and network access. See FortiGate and FortiClient profiles on page 18.

When FortiGate is integrated with EMS, the endpoint may also receive a profile from EMS that contains FortiClient configuration information.

If FortiGate is configured to warn endpoints about non-compliant status, you can acknowledge the status and access the network without fixing the issues causing a non-compliant status.

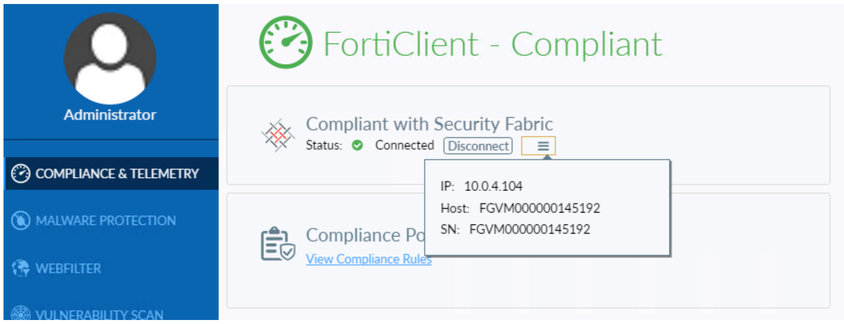
The following dialog box shows an example of an endpoint connected to a FortiGate with the compliance feature disabled.


Administrator
COMPLIANCE & TELEMETRY
MALWARE PROTECTION
FortiClient - Not Participating
Not Participating with Security Fabric
Disconnect

Status: Connected

IP: 10.0.4.104
Host: FGVM000000145192
SN: FGVM000000145192

The following dialog box shows an example of an endpoint connected to a FortiGate with the compliance feature enabled, and the endpoint is in compliance with the FortiGate compliance rules.



Status: Connected

IP: 10.0.4.104
Host: FGVM000000145192
SN: FGVM000000145192

The *Compliance & Telemetry* tab displays the following information:

Compliance	⏲	Indicates the endpoint compliance feature is enabled on FortiGate and the endpoint is in compliance with FortiGate compliance rules. See Fixing non compliance (blocked) on page 54 and Fixing non compliance (warning) on page 57.
	✕	Indicates the compliance enforcement feature is not enabled on FortiGate.
FortiGate information		Displays the IP address, hostname, and serial number of the FortiGate to which FortiClient Telemetry is connected. You can disconnect by clicking *Disconnect*.
Compliance Policy	📋	Click the *View Compliance Rules* to display the compliance rules for FortiGate.

Accessing endpoint details

When FortiClient is in managed mode, you can access details on the *Compliance & Telemetry* tab about the endpoint and FortiGate or EMS.

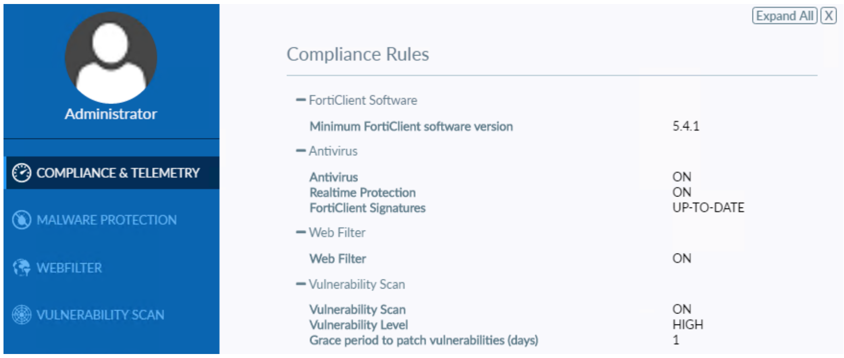
Viewing FortiGate compliance rules

When FortiClient Telemetry is connected to FortiGate, you can view the compliance rules from FortiGate. The compliance rules communicate the configuration required for FortiClient Console and the endpoint to remain compliant.

When the endpoint has a non-compliant status, an exclamation mark indicates which compliance rules are not met. See Viewing unmet compliance rules on page 55.

To view compliance rules:

1. On the *Compliance & Telemetry* tab, click *View Compliance Rules*.
   The compliance rules from FortiGate display.



Compliance Rules

− FortiClient Software	
Minimum FortiClient software version	5.4.1
− Antivirus	
Antivirus	ON
Realtime Protection	ON
FortiClient Signatures	UP-TO-DATE
− Web Filter	
Web Filter	ON
− Vulnerability Scan	
Vulnerability Scan	ON
Vulnerability Level	HIGH
Grace period to patch vulnerabilities (days)	1

2. Click *Close* to return to the *Compliance & Telemetry* tab.

On-net / off-net status with FortiGate and EMS

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

The following rules identify when FortiGate, EMS, or FortiClient determine the status:

When FortiClient 6.0.0 connects Telemetry to FortiOS 6.0.0 or later and/or EMS 6.0.0 or later, FortiClient determines whether the endpoint has an on-net or off-net status.

The following applies when FortiClient 6.0.0 is used with versions of FortiOS and/or EMS earlier than 6.0.0:

- When FortiClient connects Telemetry to FortiOS or EMS, FortiGate or EMS determines whether the endpoint has an on-net or off-net status.
- When FortiClient cannot connect FortiClient Telemetry to FortiOS or EMS, FortiClient determines the on-net or off-net status, based on the on-net subnets.

If FortiClient receives an on-net/off-net status from FortiOS or EMS, it assumes it is connected to a version of FortiOS or EMS prior to 6.0.0 and follows the received status information.

FortiGate and EMS

The version of FortiOS and EMS affects how on-net, off-net, or online status is determined.

FortiClient 6.0.0 with FortiGate and EMS 6.0.0 and later

When FortiClient 6.0.0 with FortiGate and EMS 6.0.0 and later, FortiClient calculates on-net/off-net information. The following examples show how FortiClient determines the endpoint status.

1. The endpoint has an on-net status when the endpoint is behind a FortiGate and receives option 224 with the FortiGate serial number. In this case, FortiGate is the DHCP server, and FortiGate checks that the serial number matches its own serial number.
2. If option 224 is not received or there is no match with the currently registered serial number, FortiClient determines on-net/off-net status based on the DHCP on-net/off-net setting in EMS. See EMS only on page 53.
3. Otherwise, FortiClient determines on-net/off-net status based on the on-net subnets received from EMS. See EMS only on page 53.
4. FortiClient sends the determined on-net/off-net status to EMS.

FortiClient 6.0.0 with FortiGate and EMS versions prior to 6.0.0

1. FortiGate determines the on-net/off-net status. See FortiGate only on page 52.
2. FortiClient sends the on-net/off-net status to EMS.

FortiGate only

The version of FortiClient and FortiOS do not affect the on-net, off-net, or online status. The following examples show how the endpoint status is determined when FortiClient is connected to FortiGate only:

- The endpoint has an on-net status when the endpoint is behind a FortiGate and receives option 224 with the FortiGate serial number. In this case, FortiGate is the DHCP server, and FortiGate checks that the serial number matches its own serial number.
- The endpoint has an on-net status when the endpoint is inside one of the on-net subnets defined by FortiGate. You can configure on-net subnets in the FortiClient profile using the FortiOS CLI and the `set on-net addr` command.
- The endpoint has an off-net status when the endpoint is outside of the FortiGate network, such as connected through an external interface or has not received option 224 with the FortiGate serial number.
- The endpoint has an offline status when the endpoint cannot connect FortiClient Telemetry to FortiGate and the endpoint is outside one of the on-net networks, even when option 224 and the FortiGate serial number are configured.
- The endpoint has an offline on-net status when the endpoint is inside one of the on-net networks, but cannot connect FortiClient Telemetry to FortiGate.

For FortiClient to be in an on-net network, the IP address of FortiGate or EMS should be routed via the IP address from the on-net network.

EMS only

The FortiClient and EMS versions do not affect the on-net, off-net, or online status. The following table shows how various configurations determine the endpoint status when FortiClient Telemetry is connected to EMS:

EMS DHCP on-net / off-net setting	On-net subnet	Option 224 serial number	Endpoint status
Off	No	N/A	On-net
On	No	Option not configured	Off-net
On	No	Option configured	On-net
Off or on	Yes and match	Configured or not	On-net
Off or on	Yes and do not match	Configured or not	Off-net

The following examples show how endpoint status is determined when FortiClient is connected to EMS only:

- The endpoint has an offline status when the endpoint cannot connect FortiClient Telemetry to EMS and is outside one of the on-net networks.
- The endpoint has an offline on-net status when the endpoint cannot connect FortiClient Telemetry to EMS but is inside one of the on-net networks.

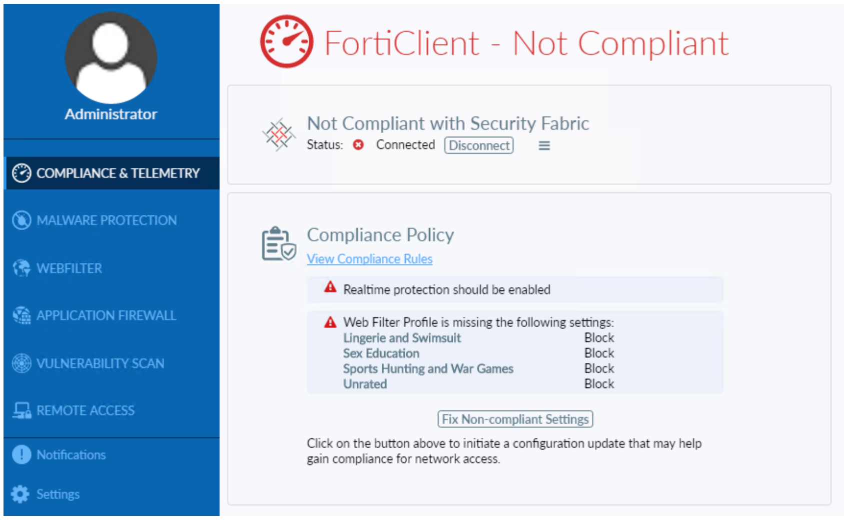
On-net subnets have higher priority over other settings. In addition, EMS does not compare the Option 224 serial number. As long as the endpoint has the serial number, EMS assumes the endpoint is behind a FortiGate and is on-net.

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*.

Fixing non compliance (blocked)

When an endpoint is not compliant with FortiGate compliance rules, and FortiGate is configured with a non-compliance action of block, the endpoint is blocked from accessing the network, and the *Compliance & Telemetry* tab displays a not-compliant status:



FortiClient - Not Compliant

Not Compliant with Security Fabric

Status: Connected [Disconnect]

Compliance Policy

View Compliance Rules

Realtime protection should be enabled

Web Filter Profile is missing the following settings:

Lingerie and Swimsuit	Block
Sex Education	Block
Sports Hunting and War Games	Block
Unrated	Block

[Fix Non-compliant Settings]

Click on the button above to initiate a configuration update that may help gain compliance for network access.

The following information displays on the *Compliance & Telemetry* tab:

Compliance status		Indicates the endpoint is not compliant with FortiGate compliance rules and may be blocked from accessing the network. You have some time to fix the non-compliant issues before FortiGate blocks network access. See Compliance and vulnerability scanning on page 93.
Compliance rules		View all compliance rules by clicking *View Compliance Rules* and see which rules are unmet. Displays compliance rules that FortiClient is currently not compliant with, as well as the non-compliance action configured on the FortiGate.
Fix Non-compliant Settings		Click the *Fix Non-Compliant Settings* button to try and return FortiClient to a compliant status. This option is not available when FortiClient settings are locked by EMS.

You can take the following steps to fix the not-compliant status and return the endpoint to a compliant status:

- View which compliance rules are unmet. See Viewing unmet compliance rules on page 55.
- Update the FortiClient configuration, if the option is available. See Fixing non-compliant settings on page 55.

- Fix detected vulnerabilities by using the automatic patching features. See Automatically fixing detected vulnerabilities on page 95.
- Manually install software patches, if required. See Manually fixing detected vulnerabilities on page 97.
- Manually fix system compliance:
- Create or modify the requested registry
- Create or modify the requested files or folders
- Start the requested processes

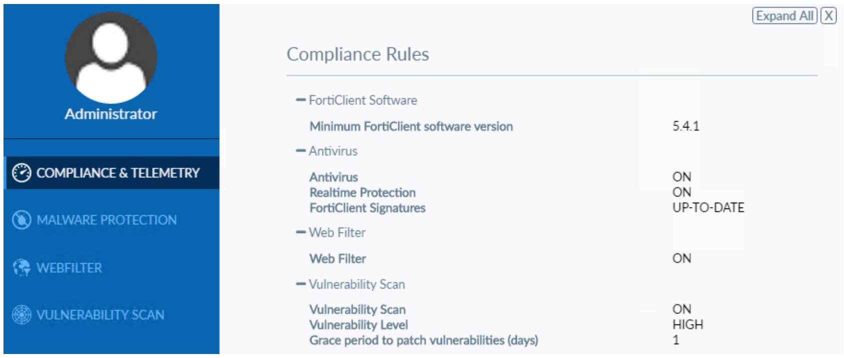
FortiClient must be installed with the correct setup to adhere to the compliance rules. See FortiClient setup types and modules on page 28.

Viewing unmet compliance rules

When an endpoint has a not-compliant (blocked) status, you can view the compliance rules from FortiGate and identify which ones are causing the not-compliant status.

To view not-compliant rules:

1. On the *Compliance & Telemetry* tab, click *View Compliance Rules*.
   The compliance rules from FortiGate display. Identify which part of the FortiClient configuration is not compliant by comparing the current configuration with the defined compliance rules.



Compliance Rules

− FortiClient Software	
Minimum FortiClient software version	5.4.1
− Antivirus	
Antivirus	ON
Realtime Protection	ON
FortiClient Signatures	UP-TO-DATE
− Web Filter	
Web Filter	ON
− Vulnerability Scan	
Vulnerability Scan	ON
Vulnerability Level	HIGH
Grace period to patch vulnerabilities (days)	1

2. Click *Close* to return to the *Compliance & Telemetry* tab.

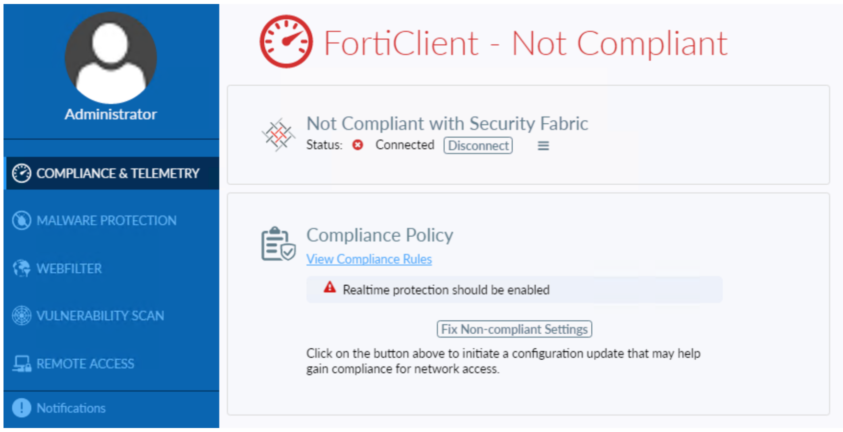
Fixing non-compliant settings

When the endpoint has a not-compliant status, and settings are unlocked, the *Fix Non-Compliant Settings* option displays on the *Compliance* tab. You can click the option to try and return FortiClient to a compliant state.

When FortiClient has a not-compliant status, and the *Fix Non-Compliant Settings* link does not display, endpoint users should contact their system administrator for help with configuring the endpoint and FortiClient Console to remain compliant with FortiGate.

To fix not-compliant settings:

1. On the *Compliance & Telemetry* tab, click *Fix Non-compliant Settings*.
   FortiClient attempts to return the endpoint to a compliant status by updating FortiClient settings to match the compliance rules from FortiGate, updating the FortiClient signatures, and patching detected vulnerabilities.

   FortiClient - Not Compliant

   Not Compliant with Security Fabric

   Status: Connected

   Compliance Policy

   Realtime protection should be enabled

   Click on the button above to initiate a configuration update that may help gain compliance for network access.

   The not-compliant settings are fixed, and the endpoint returns to a compliant status.

Patching software vulnerabilities

Endpoints can become not-compliant when vulnerabilities are detected for software installed on the endpoint, but software patches for the vulnerabilities are not yet installed. The vulnerabilities must be patched for FortiClient to return to a compliant status. See Automatically fixing detected vulnerabilities on page 95 and Manually fixing detected vulnerabilities on page 97.

Examples of blocked network access

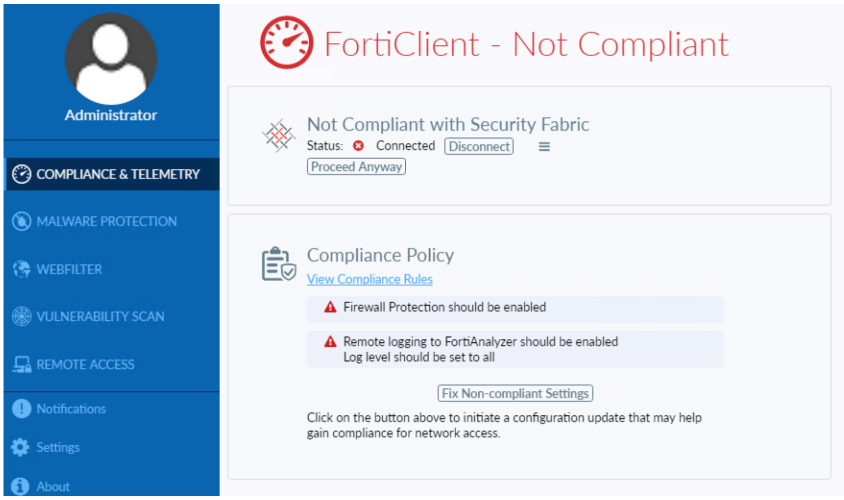
The following table provides examples of when endpoints are blocked from accessing the network and how you can regain access.

Symptom	Cause of blocked access	Solution
No network access and no FortiClient software installed	FortiClient is not installed and FortiClient Telemetry is not connected.	FortiGate displays a portal in a web browser and the portal includes a link to the FortiClient installer. Download and install FortiClient software and connect FortiClient Telemetry to FortiGate. See Connecting FortiClient Telemetry after installation on page 45
No network access and a *Not Participating* status on the *Compliance* tab in FortiClient Console	FortiClient Telemetry is not connected	In FortiClient console, connect FortiClient Telemetry to FortiGate. See Connecting FortiClient Telemetry manually on page 47.
No network access and *Not Compliant* status on the	Endpoint software or FortiClient configuration does not meet	View unmet compliance rules and configure FortiClient to meet them. In

Symptom	Cause of blocked access	Solution
Compliance tab in FortiClient Console	compliance rules.	some cases, you may need to contact your system administrator for help. See Viewing unmet compliance rules on page 55.
	The *Vulnerability Scan* tab shows detected vulnerabilities	Fix detected vulnerabilities. See Automatically fixing detected vulnerabilities on page 95. You may also need to manually fix detected vulnerabilities. See Manually fixing detected vulnerabilities on page 97.
No network access and *Compliant* status on the *Compliance* tab in FortiClient Console	FortiGate is configured to warn endpoint users about network access and you have not clicked the *I Agree* button.	Click the *I Agree* button in the web portal browser displayed by FortiGate. See Fixing non compliance (warning) on page 57.

Fixing non compliance (warning)

When an endpoint is not compliant with FortiGate compliance rules, and FortiGate is configured with a non-compliance action of to warn, the *Compliance* tab displays the following information icon with not-compliant status:



FortiClient - Not Compliant

Not Compliant with Security Fabric

Status: Connected

Compliance Policy

Firewall Protection should be enabled

Remote logging to FortiAnalyzer should be enabled
Log level should be set to all

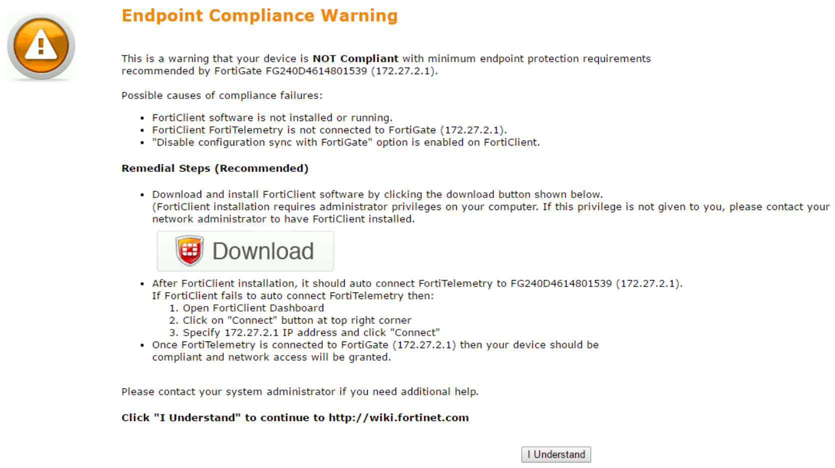
Click on the button above to initiate a configuration update that may help gain compliance for network access.

The following information displays on the *Compliance & Telemetry* tab:

Compliance status	✖	Indicates the endpoint is warned about the not-compliant status with FortiGate compliance rules. Access to the network is blocked until the endpoint user acknowledges the warning by clicking the *Proceed Anyway* button in FortiClient Console or the *I Agree* button in the FortiGate web portal.
Proceed Anyway		Click *Proceed Anyway* to acknowledge the not-compliant status and access the network without fixing all reported issues.
View Compliance		View the compliance rules by clicking and see which compliance rules are unmet.

Rules	
Fix Non-compliant Settings	Click the *Fix Non-Compliant Settings* button to try and return FortiClient to a compliant status. This option is not available when EMS has locked FortiClient settings.

FortiGate also displays a warning portal that includes an *I Agree* button at the bottom of the page:



Endpoint Compliance Warning

This is a warning that your device is **NOT Compliant** with minimum endpoint protection requirements recommended by FortiGate FG240D4614801539 (172.27.2.1).

Possible causes of compliance failures:

- FortiClient software is not installed or running.
- FortiClient FortiTelemetry is not connected to FortiGate (172.27.2.1).
- "Disable configuration sync with FortiGate" option is enabled on FortiClient.

Remedial Steps (Recommended)

- Download and install FortiClient software by clicking the download button shown below.
  (FortiClient installation requires administrator privileges on your computer. If this privilege is not given to you, please contact your network administrator to have FortiClient installed.

- After FortiClient installation, it should auto connect FortiTelemetry to FG240D4614801539 (172.27.2.1).
  If FortiClient fails to auto connect FortiTelemetry then:
  1. Open FortiClient Dashboard
  2. Click on "Connect" button at top right corner
  3. Specify 172.27.2.1 IP address and click "Connect"
- Once FortiTelemetry is connected to FortiGate (172.27.2.1) then your device should be compliant and network access will be granted.

Please contact your system administrator if you need additional help.

Click "I Understand" to continue to http://wiki.fortinet.com

When FortiGate warns endpoints about a not-compliant status, you can choose one of the following actions:

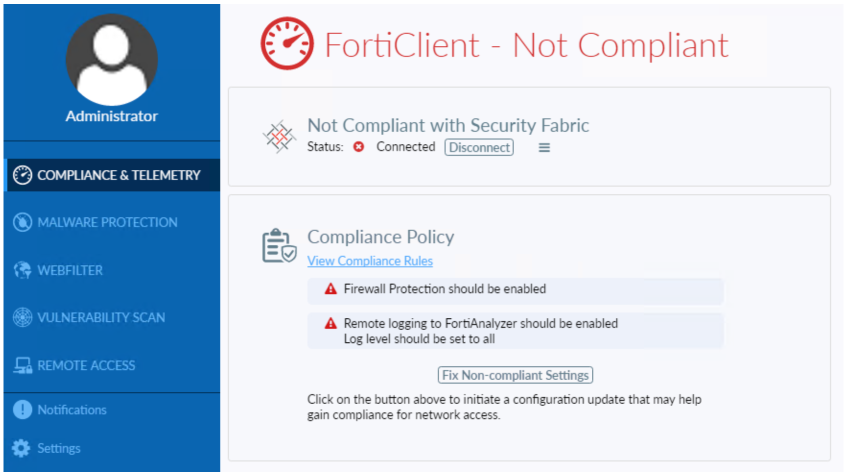
- Fix the not-compliant issues and return the endpoint to a compliant status, then access the network with a compliant status.
- Acknowledge the not-compliant status and access the network by clicking *Proceed Anyway* in FortiClient Console or *I Understand* in the warning portal.

If you choose to access the network without fixing the not-compliant issues, you must acknowledge the warning before you can access the network.

You only need to click *Proceed Anyway* in the FortiClient Console or *I Understand* in the warning portal. You do not need to click both buttons. After you click one button, the software communicate with each other to relay the acknowledgment. For example, if you click *Proceed Anyway* in the FortiClient Console, FortiClient communicates the acknowledgment to FortiGate, and you are not required to click *I Understand* in the warning portal.

To proceed anyway:

1. On the *Compliance & Telemetry* tab, click *Proceed Anyway*.
   The not-compliant issues remain unfixed, but you are granted network access.



FortiClient - Not Compliant

Not Compliant with Security Fabric

Status: Connected [Disconnect]

Compliance Policy

View Compliance Rules

Firewall Protection should be enabled

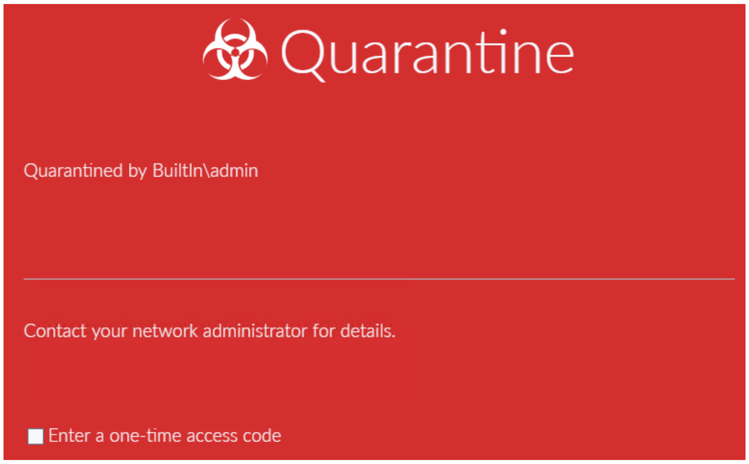
Remote logging to FortiAnalyzer should be enabled
Log level should be set to all

[Fix Non-compliant Settings]

Click on the button above to initiate a configuration update that may help gain compliance for network access.

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.



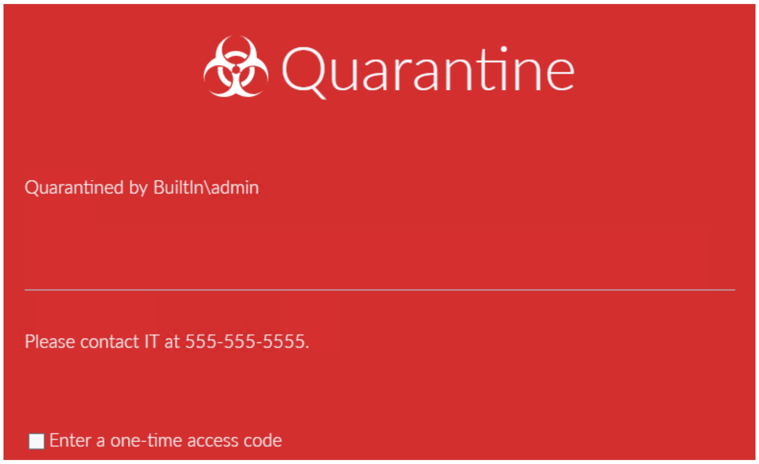
Quarantine

Quarantined by BuiltIn\admin

Contact your network administrator for details.

□ Enter a one-time access code

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

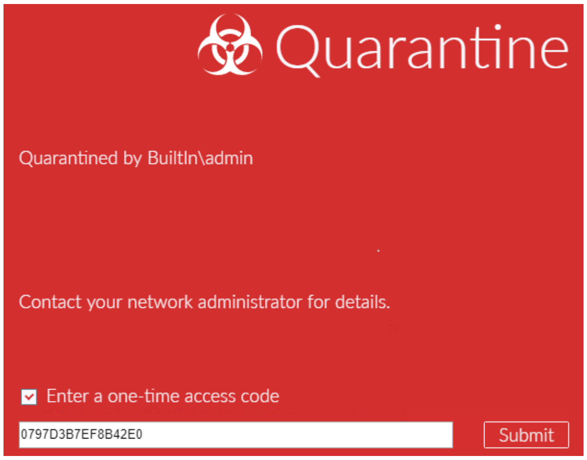

Quarantine

Quarantined by BuiltIn\admin

Please contact IT at 555-555-5555.

□ Enter a one-time access code

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.


Quarantine

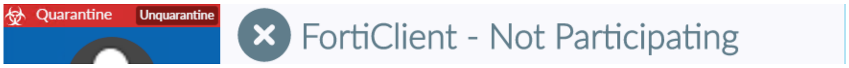
Quarantined by BuiltIn\admin

Contact your network administrator for details.

☑ Enter a one-time access code

0797D3B7EF8B42E0

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, AntiExploit, and Sandbox Detection.

> The *Malware Protection* tab displays in FortiClient Console when FortiClient is installed with *Additional Security Features* or *Advanced Persistent Threat (APT) Components* selected.

Antivirus

FortiClient includes an antivirus 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 antivirus component.

Enabling realtime protection

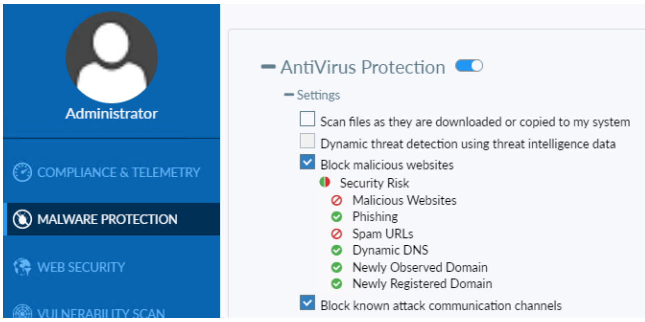
For FortiClient in managed mode, when FortiClient Telemetry is connected to FortiGate or EMS, an administrator may enable, configure, and lock realtime protection. You can enable realtime protection if EMS has not locked FortiClient Console and realtime protection is excluded from FortiGate compliance rules.

If registered to EMS, FortiClient automatically disables realtime protection until it receives a profile from EMS. Standalone FortiClient automatically disables realtime protection when one of the following is true:

1. The OS is a server
2. Exchange Server is detected
3. SQL Server is detected

To enable realtime protection:

1. On the *Malware Protection* tab, click the *Settings* icon.
   The settings page opens.
2. Select the *Scan files as they are downloaded or copied to my system* checkbox.



− AntiVirus Protection
− Settings
☐ Scan files as they are downloaded or copied to my system
☐ Dynamic threat detection using threat intelligence data
☑ Block malicious websites
Security Risk
⊘ Malicious Websites
✓ Phishing
⊘ Spam URLs
✓ Dynamic DNS
✓ Newly Observed Domain
✓ Newly Registered Domain
☑ Block known attack communication channels

3. (Optional) Set the following options:

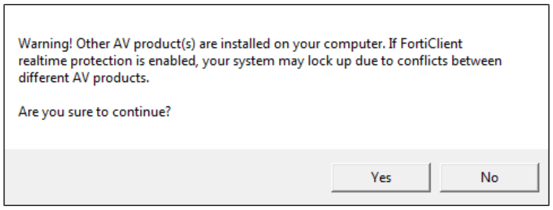
Dynamic threat detection using threat intelligence data	Select to use threat intelligence data to provide dynamic threat detection. The *Scan files as they are downloaded or copied to my system* checkbox must be selected to enable dynamic threat detection. Clear to disable dynamic threat detection.
Block malicious websites	Select to block all access to malicious websites. Clear to allow access to malicious websites. You can configure an action for all websites categorized as security risks, or configure individual actions for each subcategory. See Blocking malicious websites on page 63.
Block known attack communication channels	Select to block known communication channels uses by attackers. Clear to allow access to known communication channels used by attackers. See Blocking known attack communication channels on page 64.

4. Click *OK*.

If your system has another antivirus program installed, FortiClient displays a warning that your system may lock up due to conflicts between different antivirus products. See Third party antivirus software and realtime protection on page 62.

Third party antivirus software and realtime protection

For FortiClient in standalone mode, it is recommended to remove third party antivirus products before installing FortiClient or enabling the antivirus realtime protection feature. Otherwise you may see the following conflicting antivirus warning when you enable realtime protection:


Warning! Other AV product(s) are installed on your computer. If FortiClient realtime protection is enabled, your system may lock up due to conflicts between different AV products.

Are you sure to continue?

In managed mode, when FortiClient Telemetry is connected to FortiGate, the FortiGate compliance rules may allow third party antivirus software to be used as part of the compliance rules. In this case, you should disable realtime protection in FortiClient Console.

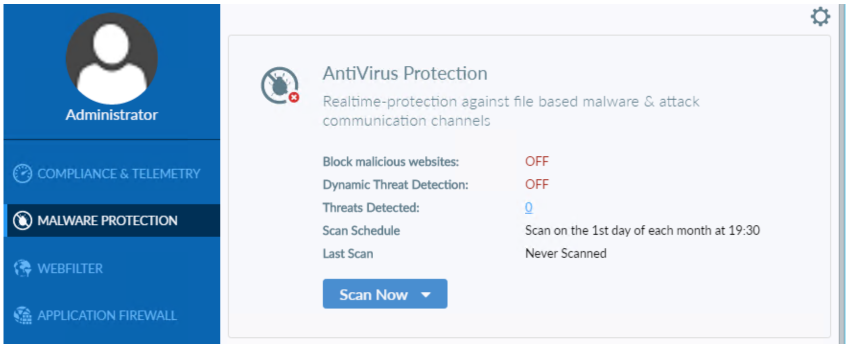
Disabling realtime protection

When FortiClient Telemetry is connected to FortiGate or EMS, you may be unable to disable realtime protection. You can disable realtime protection when EMS has not locked FortiClient Console and realtime protection is excluded from FortiGate compliance rules.

You can disable realtime protection but leave the following options enabled: *Block malicious websites* and *Block known attack communication channels*.

To disable realtime protection:

1. On the *Malware Protection* tab, click the *Settings* icon.
   The realtime protection settings page opens.
2. Clear the *Scan files as they are downloaded or copied to my system* checkbox and close the settings window.



AntiVirus Protection

Realtime-protection against file based malware & attack communication channels

Block malicious websites: OFF
Dynamic Threat Detection: OFF
Threats Detected: 0
Scan Schedule Scan on the 1st day of each month at 19:30
Last Scan Never Scanned

Configuring AntiVirus

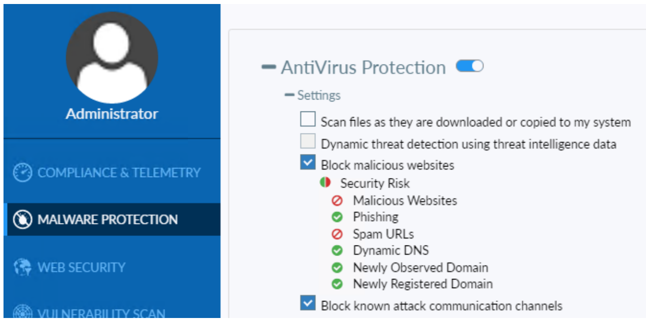
You can block access and communication channels, update the antivirus database, schedule antivirus scanning, add files or folders to exclusion lists, and configure additional antivirus options.

Blocking malicious websites

The Web Filter module must be installed before you can enable *Block malicious websites*.

To block access and communication channels:

1. On the *Malware Protection* tab, select the settings icon.
2. Select the *Block malicious websites* checkbox.
3. To configure an action for all websites categorized as security risks, click the icon beside *Security Risk* and select *Block*, *Warn*, *Allow*, or *Monitor*.
4. To configure an action for security risk subcategories, click the icon beside the desired subcategory and select *Block*, *Warn*, *Allow*, or *Monitor*.



− AntiVirus Protection

− Settings

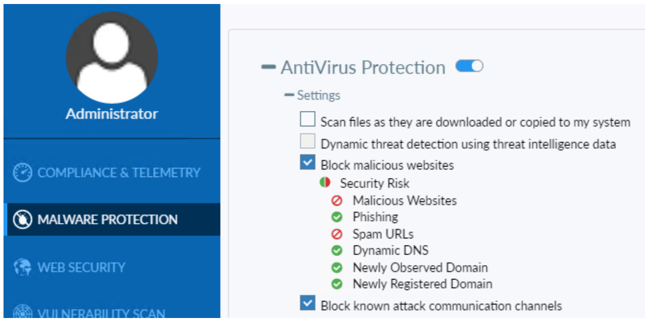
- □ Scan files as they are downloaded or copied to my system
- □ Dynamic threat detection using threat intelligence data
- ☑ Block malicious websites
  - Security Risk
    - ⊘ Malicious Websites
    - ✓ Phishing
    - ⊘ Spam URLs
    - ✓ Dynamic DNS
    - ✓ Newly Observed Domain
    - ✓ Newly Registered Domain
- ☑ Block known attack communication channels

Blocking known attack communication channels

The Application Firewall module must be installed before you can enable *Block known attack communication channels*.

To block known attack communication channels:

1. On the *Malware Protection* tab, select the settings icon.
2. Select the *Block known attack communication channels* checkbox.



− AntiVirus Protection

− Settings

☐ Scan files as they are downloaded or copied to my system
☐ Dynamic threat detection using threat intelligence data
☑ Block malicious websites
- Security Risk
  - Malicious Websites
  - Phishing
  - Spam URLs
  - Dynamic DNS
  - Newly Observed Domain
  - Newly Registered Domain

☑ Block known attack communication channels

Updating Antivirus database

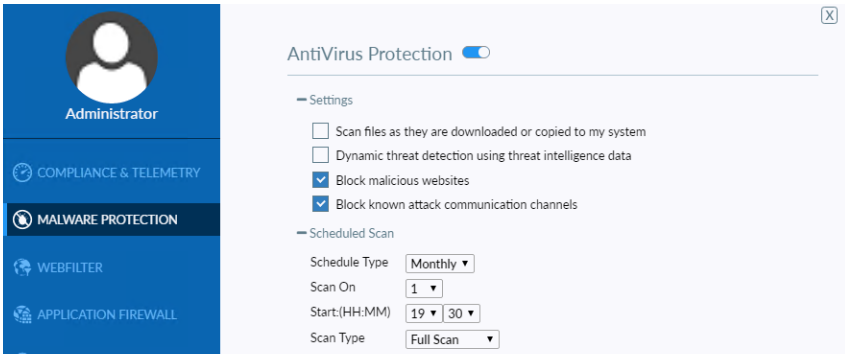
FortiClient informs you if the AntiVirus database is out of date. FortiClient automatically updates signatures. However, if you see the signatures are outdated, you can go to *About* to download updates from FortiGuard. See Viewing FortiClient engine and signature versions on page 71.

Scheduling antivirus scanning

If you configure monthly scans to occur on the 31st of each month, the scan occurs on the first day of the month for months with fewer than 31 days.

To schedule antivirus scanning:

1. On the *Malware Protection* tab, click the *Settings* icon.
2. Configure the following settings under *Scheduled Scan*:



AntiVirus Protection

− Settings

☐ Scan files as they are downloaded or copied to my system
☐ Dynamic threat detection using threat intelligence data
☑ Block malicious websites
☑ Block known attack communication channels

− Scheduled Scan

Schedule Type	Monthly ▾
Scan On	1 ▾
Start:(HH:MM)	19 ▾ 30 ▾
Scan Type	Full Scan ▾

Schedule Type	Select *Daily*, *Weekly*, or *Monthly* from the dropdown list.
Scan On	For weekly scheduled scans, select the day of the week in the dropdown list. For monthly scheduled scans, select the day of the month in the dropdown list.
Start	Select the time of day to start the scan. The time format uses a 24-hour clock.
Scan Type	Select the scan type: • *Full Scan* runs the rootkit detection engine to detect and remove rootkits. It then performs a full system scan of all files, executable files, DLLs, and drivers. • *Quick Scan* runs the rootkit detection engine to detect and remove rootkits. It only scans the following items for threats: executable files, DLLs, and drivers that are currently running. • *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. You cannot schedule a removable media scan. A full scan scans removable media.
Disable Scheduled Scan	Select to disable scheduled scan.

Managing the AntiVirus exclusion list

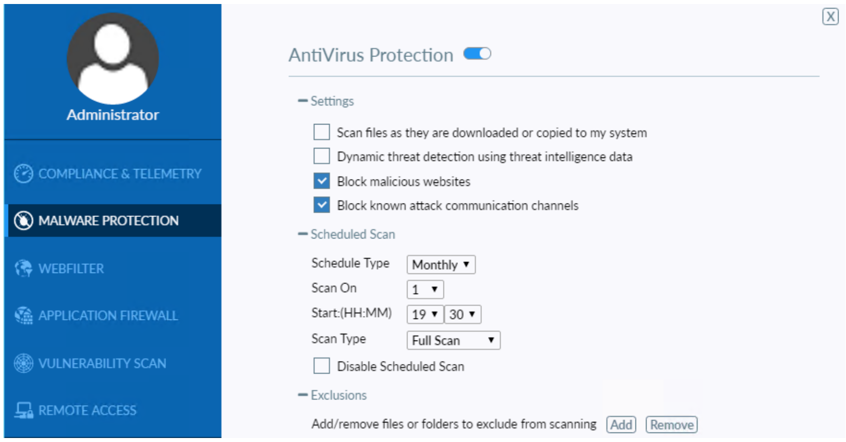
FortiClient supports using wildcards and path variables to specify files and folders to exclude from scanning. The following wildcards and variables are supported, among others:

- Using wildcards to exclude a range of file names with a specified extension, such as Edb*.jrs
- Using wildcards to exclude all files with a specified extension, such as *.jrs
- Path variable %windir%
- Path variable %allusersprofile%
- Path variable %systemroot%
- Path variable %systemdrive%

Combinations of wildcards and variables are not supported.

To add files or folders to the AntiVirus exclusion list:

1. On the *Malware Protection* tab, click the *Settings* icon.
2. Under *Exclusions*, click *Add*. Select *File* or *Folder*.



AntiVirus Protection

− Settings

□ Scan files as they are downloaded or copied to my system
□ Dynamic threat detection using threat intelligence data
☑ Block malicious websites
☑ Block known attack communication channels

− Scheduled Scan

Schedule Type Monthly ▾
Scan On 1 ▾
Start:(HH:MM) 19 ▾ 30 ▾
Scan Type Full Scan ▾
□ Disable Scheduled Scan

− Exclusions

Add/remove files or folders to exclude from scanning [Add] [Remove]

A Browse dialog box displays.

3. Locate and select the file or folder, and click *Open*.
   The file or folder is added to the exclusion list, and will not be scanned by the AntiVirus engine.

To remove files or folders from the AntiVirus exclusion list:

1. On the *Malware Protection* tab, click the *Settings* icon.
   The Settings page displays.
2. Under *Exclusions*, select the desired item(s).
3. Click *Remove*. The selected items are removed from the exclusion list.

Configuring additional Antivirus options

You can configure additional settings for the *Antivirus* tab by going to *Settings* in FortiClient Console. See Antivirus options on page 119.

Scanning with AntiVirus on demand

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

Scanning now

To perform on-demand antivirus scanning:

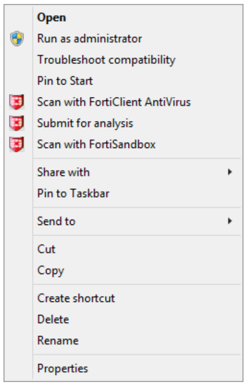
1. On the *Malware Protection* tab, under *AntiVirus Protection*, click the *Scan Now* button.
2. Use the dropdown list to select *Quick Scan*, *Full Scan*, *Custom Scan*, or *Removable media Scan*.

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

To scan files or folders:

1. 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 submitted for analysis and determined to be malicious.

To submit files for analysis:

1. On your workstation, right-click a file or executable, and select *Submit for analysis* from the menu.
   A dialog box 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.

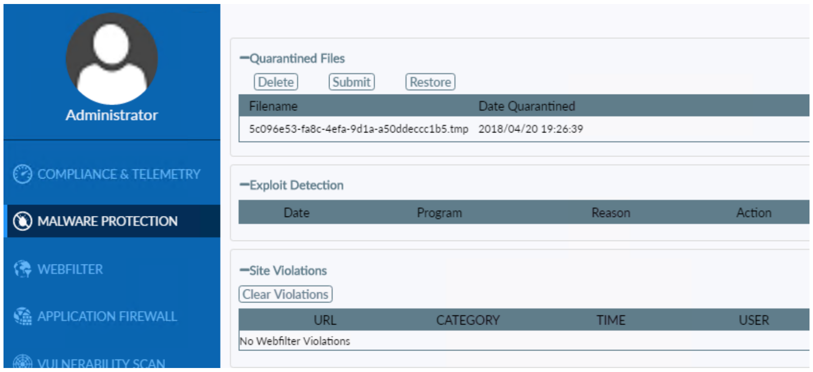
Viewing AntiVirus scan results

You can view quarantined threats, site violations, alerts, and realtime protection events when FortiClient is in standalone or managed mode.

Viewing quarantined threats

To view quarantined threats:

1. On the *Malware Protection* tab, click *X Threats Detected*.
   You can view the original file location, virus name, and logs, and submit the suspicious file to FortiGuard. If using FortiClient in standalone mode or FortiClient in managed mode with FortiGate only, you can also view, restore, or delete the quarantined file in this page. If FortiClient is connected to FortiClient EMS, you cannot restore or delete the quarantined file.



Filename	Date Quarantined
5c096e53-fa8c-4efa-9d1a-a50ddeccc1b5.tmp	2018/04/20 19:26:39

Date	Program	Reason	Action

URL	CATEGORY	TIME	USER
No Webfilter Violations			

2. The following information displays:

Filename	Lists the names of the quarantined files.
Date Quarantined	Lists the 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.
Restore	Click to remove the selected file from quarantine.
Delete	Click to delete the selected file from the device.
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*.

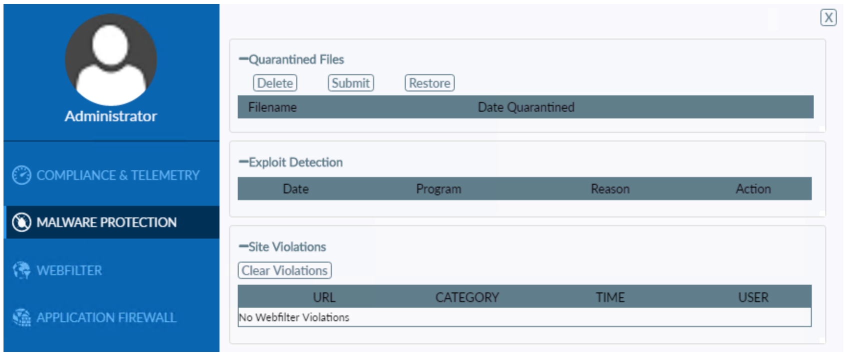
When EMS manages FortiClient, FortiClient sends quarantined file information to EMS. If the EMS administrator whitelists the file (in the case of a false positive), EMS sends the whitelist information to FortiClient. After FortiClient receives the whitelist information, it releases the file from quarantine.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

Viewing site violations

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

To view site violations:

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



No Webfilter Violations

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 antivirus 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.

⚠ You must select *Alert when viruses are detected* under *Antivirus Options* on the *Settings* page to receive the virus alert dialog box when attempting to download a virus in a web browser. If *Alert when viruses are detected* is disabled, the virus alert dialog box does not display when you attempt to download a virus in a web browser.

Viewing realtime protection events

When an antivirus realtime protection event has occurred, you can view these events in FortiClient Console.

To view realtime protection events:

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

```
Realtime scan result:
time: 09/29/15 10:46:07, virus found: EICAR_TEST_FILE, action: Quarantined,
     c:\users\user\desktop\eicar.com
```

```
time: 09/29/15 10:46:07, virus found: EICAR_TEST_FILE, action: Quarantined,
      c:\users\user\desktop\eicar.com.txt
time: 09/29/15 10:46:07, virus found: EICAR_TEST_FILE, action: Quarantined,
      c:\users\user\desktop\eicarcom2.zip
time: 09/29/15 10:46:08, virus found: EICAR_TEST_FILE, action: Quarantined,
      c:\users\user\desktop\eicar_com.zip
time: 09/29/15 10:46:39, virus found: EICAR_TEST_FILE, action: Quarantined,
      c:\users\user\appdata\local\temp\3g_bl8y9.com.part
time: 03/18/15 10:48:13, virus found: EICAR_TEST_FILE, action: Quarantined,
      c:\users\user\appdata\local\temp\xntwh8q1.zip.part
```

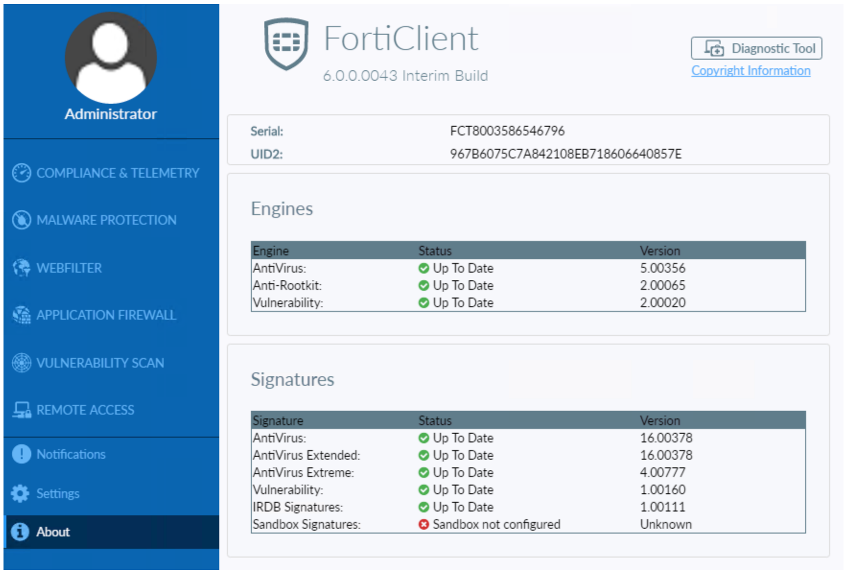
Viewing FortiClient engine and signature versions

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

When EMS manages FortiClient, you can select to use a FortiManager 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 the IP address of your FortiManager device. You can select to failover to FDN when FortiManager is unavailable.

To view FortiClient engine and signature versions:

1. Go to *About*.



6.0.0.0043 Interim Build

Serial: FCT8003586546796
UID2: 967B6075C7A842108EB718606640857E

Engines

Engine	Status	Version
AntiVirus:	✓ Up To Date	5.00356
Anti-Rootkit:	✓ Up To Date	2.00065
Vulnerability:	✓ Up To Date	2.00020

Signatures

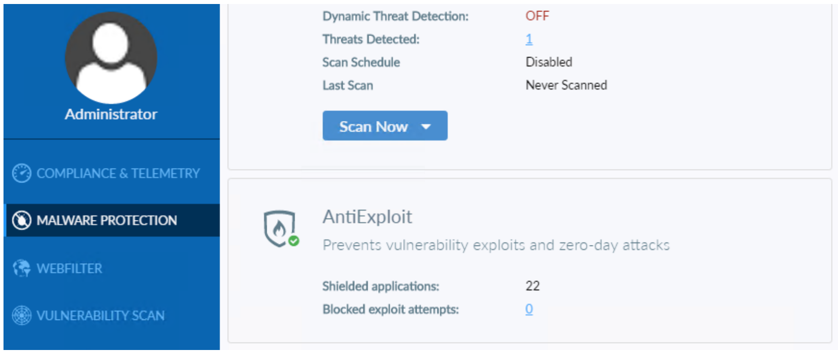
Signature	Status	Version
AntiVirus:	✓ Up To Date	16.00378
AntiVirus Extended:	✓ Up To Date	16.00378
AntiVirus Extreme:	✓ Up To Date	4.00777
Vulnerability:	✓ Up To Date	1.00160
IRDB Signatures:	✓ Up To Date	1.00111
Sandbox Signatures:	✗ Sandbox not configured	Unknown

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

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 plug-ins, 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.



Dynamic Threat Detection: OFF
Threats Detected: 1
Scan Schedule Disabled
Last Scan Never Scanned

AntiExploit
Prevents vulnerability exploits and zero-day attacks
Shielded applications: 22
Blocked exploit attempts: 0

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

Enabling and disabling exploit prevention

You can enable and disable exploit prevention if EMS has not locked FortiClient Console.

To enable and disable exploit prevention:

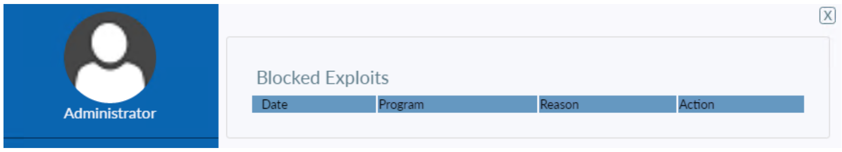
1. On the *Malware Protection* tab, click the *Settings* icon.
   The settings page displays.
2. Toggle AntiExploit on/off to enable/disable exploit prevention.

Viewing detected exploit attempts

You can view the exploit attempts FortiClient has blocked. See Enabling and disabling exploit prevention on page 72.

To view detected exploit attempts:

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.



Blocked Exploits

Date	Program	Reason	Action

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

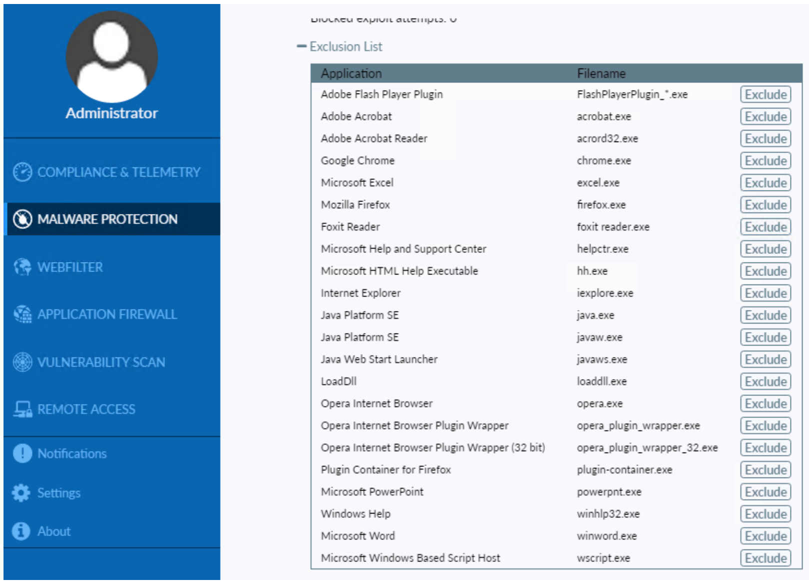
When you view the list of applications, you can use the following button names to determine which applications are protected from exploits:

- 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 Excluding applications from protection on page 74.

See Viewing detected exploit attempts on page 72.

To view protected applications:

1. From the *Malware Protection* tab, click the *Settings* icon. Scroll to *AntiExploit* and expand the *Exclusion List*. The list of protected applications displays.



— Exclusion List

Application	Filename	
Adobe Flash Player Plugin	FlashPlayerPlugin_*.exe	Exclude
Adobe Acrobat	acrobat.exe	Exclude
Adobe Acrobat Reader	acrord32.exe	Exclude
Google Chrome	chrome.exe	Exclude
Microsoft Excel	excel.exe	Exclude
Mozilla Firefox	firefox.exe	Exclude
Foxit Reader	foxit reader.exe	Exclude
Microsoft Help and Support Center	helpctr.exe	Exclude
Microsoft HTML Help Executable	hh.exe	Exclude
Internet Explorer	iexplore.exe	Exclude
Java Platform SE	java.exe	Exclude
Java Platform SE	javaw.exe	Exclude
Java Web Start Launcher	javaws.exe	Exclude
LoadDll	loaddll.exe	Exclude
Opera Internet Browser	opera.exe	Exclude
Opera Internet Browser Plugin Wrapper	opera_plugin_wrapper.exe	Exclude
Opera Internet Browser Plugin Wrapper (32 bit)	opera_plugin_wrapper_32.exe	Exclude
Plugin Container for Firefox	plugin-container.exe	Exclude
Microsoft PowerPoint	powerpnt.exe	Exclude
Windows Help	winhlp32.exe	Exclude
Microsoft Word	winword.exe	Exclude
Microsoft Windows Based Script Host	wscript.exe	Exclude

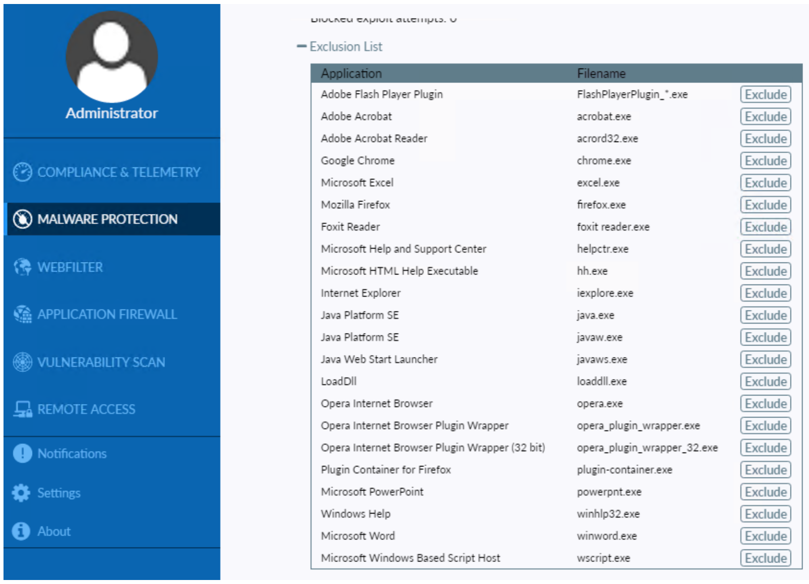
Excluding applications from protection

You can exclude applications from the list of software protected from evasive exploits. You can also add excluded applications back to the list of protected software.

For FortiClient in managed mode, when FortiClient Telemetry is connected to FortiGate or EMS, an administrator may lock the list of protected applications. You can exclude applications from protection if EMS has not locked FortiClient Console.

To exclude applications from protection:

1. On the *Malware Protection* tab, click the *Settings* icon.
   The list of protected applications displays under *AntiExploit* > *Exclusion List*.



Blocked exploit attempts: 0

− Exclusion List

Application	Filename	
Adobe Flash Player Plugin	FlashPlayerPlugin_*.exe	Exclude
Adobe Acrobat	acrobat.exe	Exclude
Adobe Acrobat Reader	acrord32.exe	Exclude
Google Chrome	chrome.exe	Exclude
Microsoft Excel	excel.exe	Exclude
Mozilla Firefox	firefox.exe	Exclude
Foxit Reader	foxit reader.exe	Exclude
Microsoft Help and Support Center	helpctr.exe	Exclude
Microsoft HTML Help Executable	hh.exe	Exclude
Internet Explorer	iexplore.exe	Exclude
Java Platform SE	java.exe	Exclude
Java Platform SE	javaw.exe	Exclude
Java Web Start Launcher	javaws.exe	Exclude
LoadDll	loaddll.exe	Exclude
Opera Internet Browser	opera.exe	Exclude
Opera Internet Browser Plugin Wrapper	opera_plugin_wrapper.exe	Exclude
Opera Internet Browser Plugin Wrapper (32 bit)	opera_plugin_wrapper_32.exe	Exclude
Plugin Container for Firefox	plugin-container.exe	Exclude
Microsoft PowerPoint	powerpnt.exe	Exclude
Windows Help	winhlp32.exe	Exclude
Microsoft Word	winword.exe	Exclude
Microsoft Windows Based Script Host	wscript.exe	Exclude

2. Beside each application you want to exclude, click *Exclude*.
   The application is excluded, and the button name changes to *Unexclude*. Click *Unexclude* to protect the application again.

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 93.

Sandbox Detection

FortiClient supports integration with FortiSandbox. When configured, FortiSandbox automatically scans files downloaded on the endpoint or from removable media attached to the endpoint or mapped network drives. FortiSandbox can also automatically scan files downloaded from the Internet or emailed to the endpoint. Endpoint users can also manually submit files to FortiSandbox for scanning.

Access to files can be blocked until the FortiSandbox scanning result is returned.

When scanning is complete, FortiSandbox can quarantine infected files or alert and notify the endpoint user of infected files without quarantining the files.

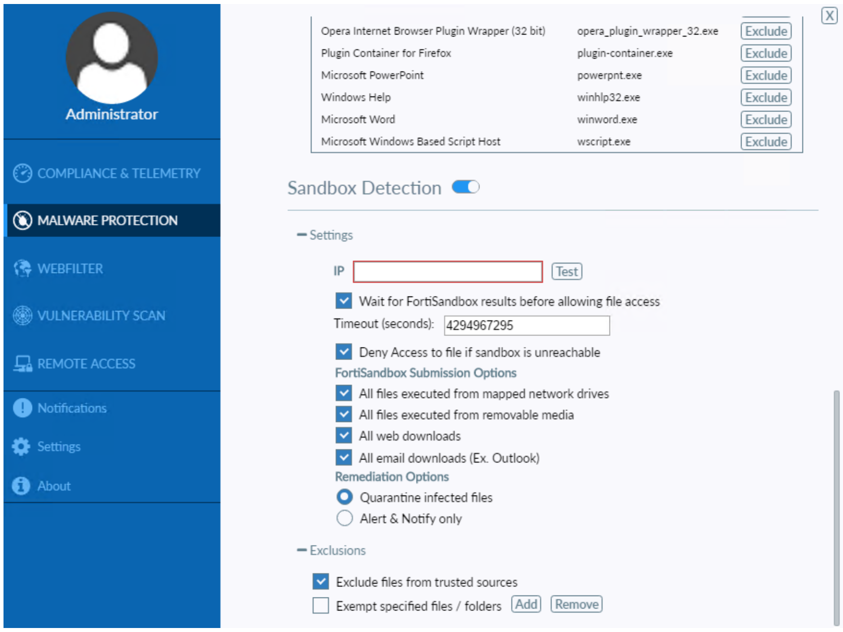
As FortiSandbox receives files for scanning from various sources, it collects and generates AV signatures for such samples. FortiClient periodically downloads the latest AV signatures from FortiSandbox, and applies them locally to all realtime and on-demand AntiVirus scanning.

Enabling Sandbox Detection

If you have a FortiSandbox unit, you can enable FortiClient to work with FortiSandbox.

To enable Sandbox Detection:

1. On the *Malware Protection* tab, click the settings icon.
2. If the *Administrative privileges are required to change settings. Press Elevate to obtain these privileges.* message displays, click *Elevate*.
   The settings page displays.



Opera Internet Browser Plugin Wrapper (32 bit)	opera_plugin_wrapper_32.exe	Exclude
Plugin Container for Firefox	plugin-container.exe	Exclude
Microsoft PowerPoint	powerpnt.exe	Exclude
Windows Help	winhlp32.exe	Exclude
Microsoft Word	winword.exe	Exclude
Microsoft Windows Based Script Host	wscript.exe	Exclude

Sandbox Detection

− Settings

IP Test

☑ Wait for FortiSandbox results before allowing file access

Timeout (seconds): 4294967295

☑ Deny Access to file if sandbox is unreachable

FortiSandbox Submission Options

☑ All files executed from mapped network drives

☑ All files executed from removable media

☑ All web downloads

☑ All email downloads (Ex. Outlook)

Remediation Options

● Quarantine infected files

○ Alert & Notify only

− Exclusions

☑ Exclude files from trusted sources

□ Exempt specified files / folders Add Remove

3. Toggle *Sandbox Detection* on if needed.
4. In the *IP* box, type the IP address for FortiSandbox, and click *Test* to ensure the IP address is valid.
   If the IP address is valid, a confirmation dialog box displays.

5. Click *OK* to close the confirmation dialog box.
   For information about configuring FortiSandbox, see Configuring Sandbox Detection on page 77.
   FortiSandbox Detection is enabled.

Checking FortiClient authorization for FortiSandbox scanning

This feature requires FortiSandbox 2.5.0 or later. If you are using EMS, EMS 1.2.2 or later is required.

Depending on the FortiSandbox configuration, FortiSandbox may only scan submitted files when FortiClient is authorized. The *Malware Protection* tab in FortiClient Console displays the authorization status.

The following table summarizes how FortiSandbox receives the authorization status for FortiClient:

Mode	FortiClient Telemetry connection	FortiClient authorization
Standalone mode	N/A	The FortiSandbox administrator can choose to disable authorization of FortiClient. When authorization is disabled, all authorization requests are accepted. When authorization is enabled, the FortiSandbox administrator must manually authorize each FortiClient using the FortiSandbox GUI.
Managed mode	EMS only	EMS provides authorization to FortiSandbox for FortiClient. The FortiSandbox administrator must authorize the EMS server managing FortiClient.
	EMS and FortiGate	EMS provides authorization to FortiSandbox for FortiClient. The FortiSandbox administrator can authorize EMS or FortiGate.
	FortiGate only	FortiGate provides authorization to FortiSandbox for FortiClient. The FortiSandbox administrator must authorize FortiGate.

To check Sandbox authorization status:

1. On the *Malware Protection* tab, click the settings icon.
2. If the *Administrative privileges are required to change settings. Press Elevate to obtain these privileges.* message displays, click *Elevate*.
   The settings page displays.
3. Under *Sandbox Detection*, click the *Test* button.
   A dialog box communicating the authorization status displays.
4. Click *OK* to close the confirmation dialog box.

Disabling Sandbox Detection

To disable Sandbox Detection:

1. On the *Malware Protection* tab, click the settings icon.
   The settings page displays.
2. Toggle *Sandbox Detection* off.
   FortiSandbox Detection is disabled.

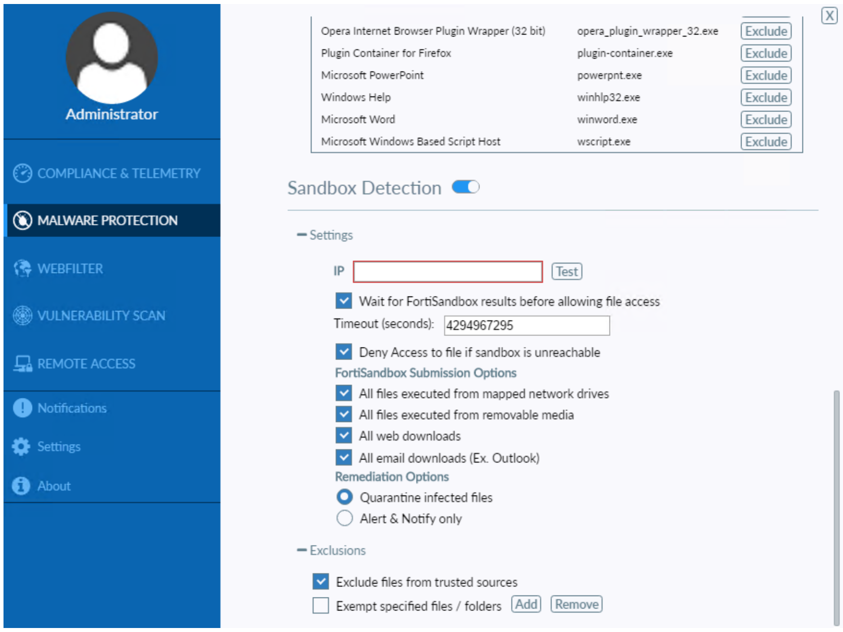
Configuring Sandbox Detection

You can configure what files are automatically submitted from the endpoint to FortiSandbox for scanning. You can also configure whether FortiSandbox quarantines infected files and whether to exclude any files or folders from FortiSandbox scanning.

Configuring submission, access, and remediation

To configure submission, access, and remediation:

1. On the *Malware Protection* tab, click the *Settings* icon.
   The settings page displays.



Opera Internet Browser Plugin Wrapper (32 bit)	opera_plugin_wrapper_32.exe	Exclude
Plugin Container for Firefox	plugin-container.exe	Exclude
Microsoft PowerPoint	powerpnt.exe	Exclude
Windows Help	winhlp32.exe	Exclude
Microsoft Word	winword.exe	Exclude
Microsoft Windows Based Script Host	wscript.exe	Exclude

Sandbox Detection

− Settings

IP [ ] Test

☑ Wait for FortiSandbox results before allowing file access

Timeout (seconds): 4294967295

☑ Deny Access to file if sandbox is unreachable

FortiSandbox Submission Options

☑ All files executed from mapped network drives

☑ All files executed from removable media

☑ All web downloads

☑ All email downloads (Ex. Outlook)

Remediation Options

● Quarantine infected files

○ Alert & Notify only

− Exclusions

☑ Exclude files from trusted sources

□ Exempt specified files / folders Add Remove

2. Set the following options, and click *OK*:

	Wait for FortiSandbox results before allowing file access	Select to wait for FortiSandbox analysis results before files can be accessed. Clear the checkbox to allow file access before FortiSandbox results are known.
	Timeout (seconds)	Specify the timeout duration in seconds. After the time expires, file access is allowed, even if FortiSandbox has not returned results and if the *Deny Access to file if Sandbox unreachable* option is disabled. When set to *0*, the downloaded file is always released and the popup never displays. See Using the popup window on page 84.
	Deny Access to file if Sandbox is unreachable	Select to deny access to files when FortiClient cannot reach FortiSandbox for file analysis. Clear the checkbox to allow file access if the FortiSandbox unit cannot be reached for scanning. See Examples of FortiSandbox availability and scanning results on page 78.
FortiSandbox Submission Options		
	All files executed from mapped network drives	Select to submit all files that are executed on mapped network drives to FortiSandbox for analysis. Clear the checkbox to disable this feature.
	All files executed from removable media	Select to submit all files executed on removable media, such as USB drives, to FortiSandbox for analysis. Clear the checkbox to disable this feature.
	All web downloads	Select to submit all web downloads on the endpoint to FortiSandbox for analysis. Clear the checkbox to disable this feature.
	All email downloads (Ex. Outlook)	Select to submit all email downloads on the endpoint to FortiSandbox for analysis. Clear the checkbox to disable this feature.
Remediation Options		
	Quarantine infected files	Select to quarantine infected files.
	Alert & Notify only	Select to alert and notify the endpoint user about infected files, but not quarantine infected files.

Examples of FortiSandbox availability and scanning results

The following table identifies how the FortiSandbox settings and availability affect file scanning results when the Sandbox `<timeout>` setting is not zero.

Deny access to file if unreachable	FortiSandbox reachable?	FortiSandbox timed out?	FortiSandbox final action	FortiSandbox message
Disabled	Yes	No	Based on FortiSandbox verdict	Scanning verdict is displayed
Disabled	Yes	Yes	Release file	Scanning timed out
Disabled	No	N/A	Release file	Scanning skipped - FortiSandbox unreachable
Enabled	Yes	No	Based on FortiSandbox verdict	Scanning verdict is displayed
Enabled	Yes	Yes	Block file	Scanning timed out - access denied
Enabled	No	N/A	Block file	Scanning skipped - FortiSandbox unreachable - access denied

Configuring exceptions

To configure exceptions:

1. On the *Malware Protection* tab, click the *Settings* icon.
   The settings page displays.
2. Set the following options and click *OK*:

Exceptions		
	Exclude files from trusted sources	Select to exclude files from trusted sources from FortiSandbox analysis.
	Exempt specified files / folders	Select to exempt specified files and/or folders from FortiSandbox analysis. You must also create the exclusion list.

3. If you selected the *Exempt specified files /folders*, you must create the exclusion list. See Managing the Sandbox Detection exclusion list on page 79.

Managing the Sandbox Detection exclusion list

You can add files and folders to the exclusion list for FortiSandbox. FortiSandbox does not scan the identified files or folders when the *Exempt specified files / folders* checkbox is selected. See Configuring exceptions on page 79.

You can also remove files and folders from the exclusion list.

To add files or folders to the exclusion list:

1. On the *Malware Protection* tab, click the *Settings* icon.
   The Settings page displays.

2. Beside *Exempt specified files / folders*, click *Add*, and select *File* or *Folder*.
   A Browse dialog box displays.
3. Locate and select the file or folder, and click *Open*.
   The file or folder is added to the exclusion list, and will not be scanned by FortiSandbox.

To remove files or folders from the exclusion list:

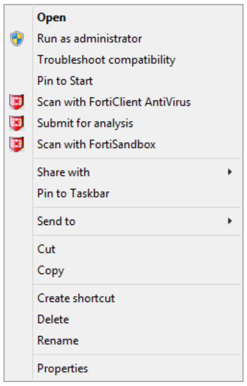
1. On the *Malware Protection* tab, click the *Settings* icon.
   The Settings page displays.
2. Beside *Exempt specified files / folders*, click one or more items in the exclusion list.
3. Click *Remove*.
   The selected items are removed from the exclusion list.

Scanning with FortiSandbox on demand

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

To scan with FortiSandbox on demand:

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



Viewing Sandbox Detection results

FortiSandbox scan results display on the *Malware Protection* tab and in a popup.

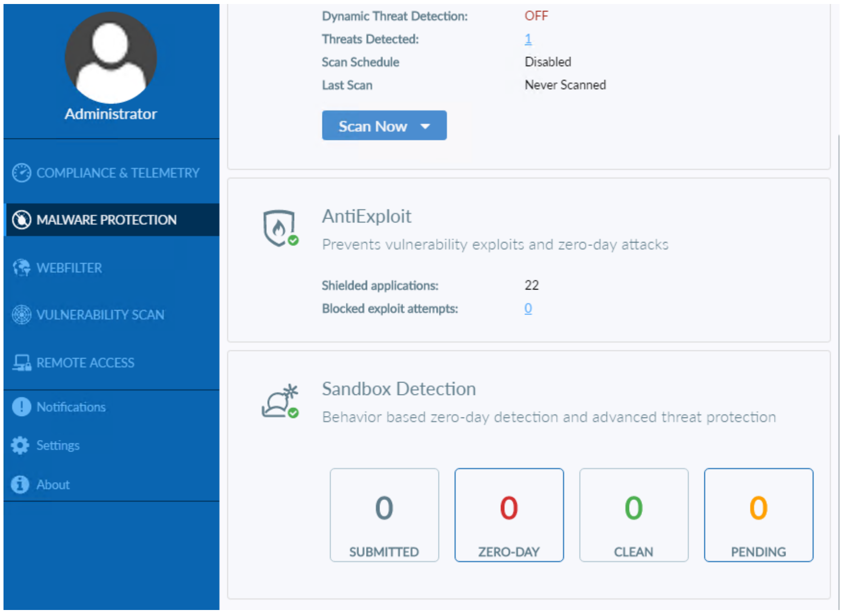
When a virus is detected, FortiClient creates a notification alert. See Viewing notifications on page 85.

When EMS manages FortiClient, 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.

Viewing FortiSandbox scan results

To view FortiSandbox scan results:

1. Go to the *Malware Protection* tab.



Dynamic Threat Detection: OFF
Threats Detected: 1
Scan Schedule Disabled
Last Scan Never Scanned

AntiExploit
Prevents vulnerability exploits and zero-day attacks
Shielded applications: 22
Blocked exploit attempts: 0

Sandbox Detection
Behavior based zero-day detection and advanced threat protection

0	0	0	0
SUBMITTED	ZERO-DAY	CLEAN	PENDING

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.

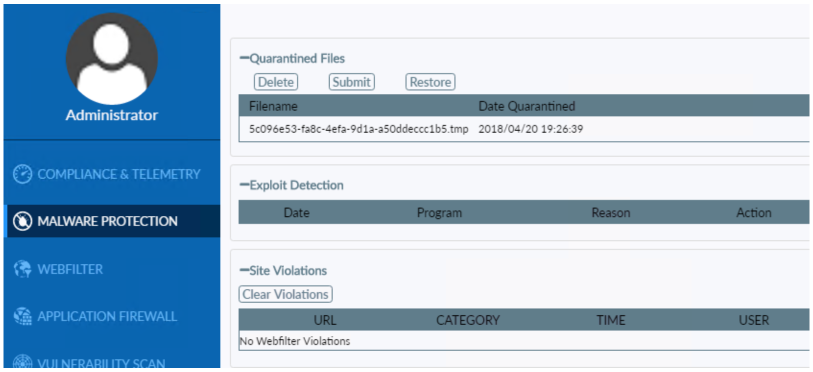
Viewing quarantined files

You can view files quarantined by FortiSandbox. You can also restore and delete quarantined files and submit them for another analysis.

You cannot restore and delete quarantined files when FortiClient is in managed mode.

To view quarantined files:

1. Go to the *Malware Protection* tab.
2. Under *Sandbox Detection*, click *Zero-Day* to view quarantined files.
   The list of files displays.



Filename	Date Quarantined
5c096e53-fa8c-4efa-9d1a-a50ddeccc1b5.tmp	2018/04/20 19:26:39

Date	Program	Reason	Action

URL	CATEGORY	TIME	USER
No Webfilter Violations			

The following information displays:

Filename	Lists the names of the quarantined files.
Date Quarantined	Lists the date 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.
Restore	Click to remove the selected file from quarantine.
Delete	Click to delete the selected file from the device.
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*.

Submitting quarantined files for scanning

You can submit quarantined files to FortiSandbox for scanning.

To submit quarantined files for scanning:

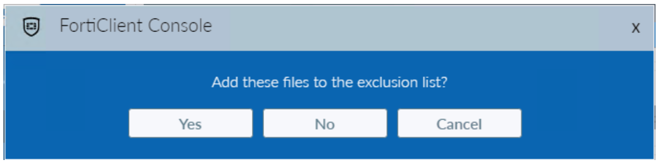
1. Go to the *Malware Protection* tab.
2. Under *Sandbox Detection*, click *Zero-day* to view quarantined files.
   The list of files displays.
3. Select the file and click *Submit*.

Restoring quarantined files

Endpoint users can only restore quarantined files with FortiClient in standalone mode. When you restore a quarantined file, you can choose whether to add the file to the exclusion list.

To restore quarantined files:

1. Go to the *Malware Protection* tab.
2. Under *Sandbox Detection*, click *Zero-day* to view quarantined files.
   The list of files displays.
3. Select the file and click *Restore*.
   A confirmation dialog box displays.



FortiClient Console

Add these files to the exclusion list?

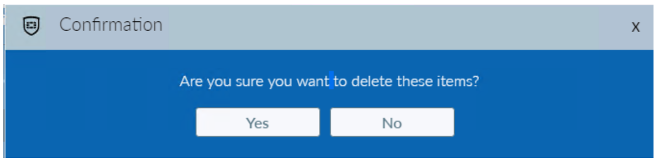
4. Click *Yes* to restore the file and add it to the exclusion list or *No* to restore the file without adding it to the exclusion list.
5. If the *Administrative privileges are required to change settings. Press Elevate to obtain these privileges.* message displays, click *Elevate*.
   The file is restored.

Deleting quarantined files

Endpoint users can only restore quarantined files with FortiClient in standalone mode.

To delete quarantined files:

1. Go to the *Malware Protection* tab.
2. Under *Sandbox Detection*, click *Zero-day* to view quarantined files.
   The list of files displays.
3. Select the file, and click *Delete*.
   A confirmation dialog box displays.



Confirmation

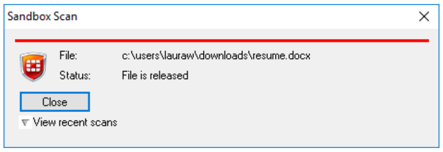
Are you sure you want to delete these items?

4. Click *Yes*.
   The file is deleted.

Using the popup window

The settings for the *Wait for FortiSandbox scan result before allowing file access* and *Timeout seconds* options affect when the popup displays. See Configuring Sandbox Detection on page 77.

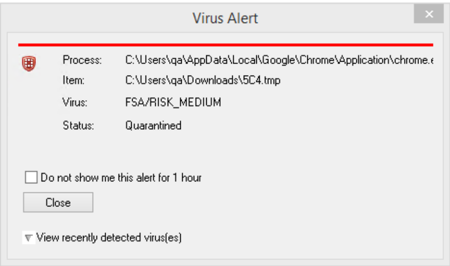
As FortiSandbox scans and releases files, a popup displays to inform you. You can view the recent scans by clicking the *View recent scans* option.



Sandbox Scan

File: c:\users\lauraw\downloads\resume.docx
Status: File is released

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

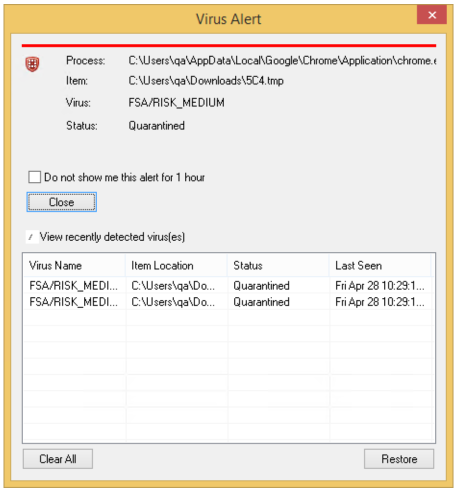


Virus Alert

Process: C:\Users\qa\AppData\Local\Google\Chrome\Application\chrome.e
Item: C:\Users\qa\Downloads\5C4.tmp
Virus: FSA/RISK_MEDIUM
Status: Quarantined

□ Do not show me this alert for 1 hour

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.e
Item: C:\Users\qa\Downloads\5C4.tmp
Virus: FSA/RISK_MEDIUM
Status: Quarantined

□ Do not show me this alert for 1 hour

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...

With the information expanded, you can select a quarantined file and click the *Restore* button to restore the file.

Endpoint users can only restore quarantined files with FortiClient in standalone mode.

Viewing notifications

Click the notifications icon in FortiClient Console to view notifications. When a virus has been detected, the notifications icon changes from gray to yellow or red.

Event notifications include:

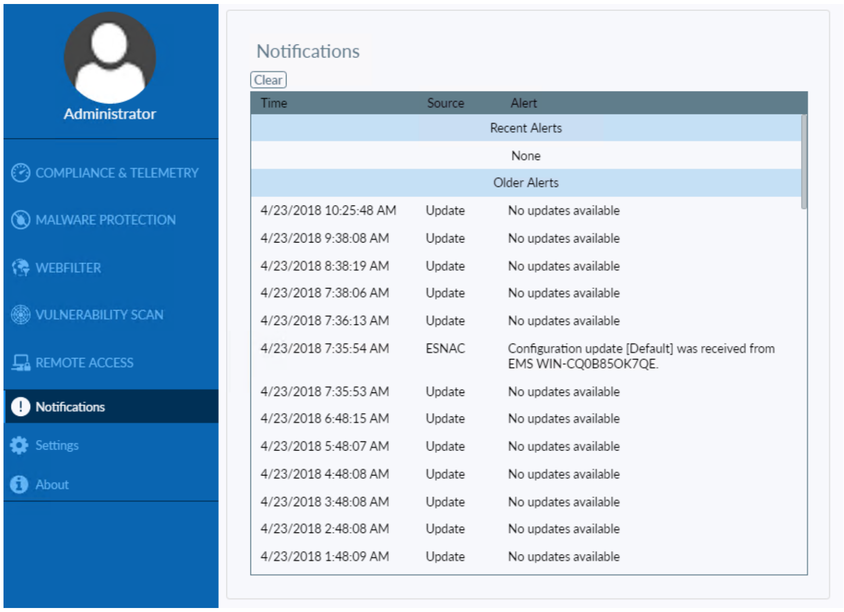
- Sandbox Detection events, including detected malware
- Antivirus events, including scheduled scans and detected malware.
- Endpoint Control events, including configuration updates received from FortiGate or EMS.
- Web Filter events, including blocked web site access attempts.
- System events, including signature and engine updates and software upgrades.

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

For FortiClient in standalone mode, you can clear the entries by clicking the *Clear* button. This option is not available for FortiClient in managed mode.

To view notifications:

1. In FortiClient Console, click *Notifications*.
   The list of notifications displays.



Time	Source	Alert
Recent Alerts		
None		
Older Alerts		
4/23/2018 10:25:48 AM	Update	No updates available
4/23/2018 9:38:08 AM	Update	No updates available
4/23/2018 8:38:19 AM	Update	No updates available
4/23/2018 7:38:06 AM	Update	No updates available
4/23/2018 7:36:13 AM	Update	No updates available
4/23/2018 7:35:54 AM	ESNAC	Configuration update [Default] was received from EMS WIN-CQ0B85OK7QE.
4/23/2018 7:35:53 AM	Update	No updates available
4/23/2018 6:48:15 AM	Update	No updates available
4/23/2018 5:48:07 AM	Update	No updates available
4/23/2018 4:48:08 AM	Update	No updates available
4/23/2018 3:48:08 AM	Update	No updates available
4/23/2018 2:48:08 AM	Update	No updates available
4/23/2018 1:48:09 AM	Update	No updates available

2. Click *Close* to close the list.

Web Filter

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

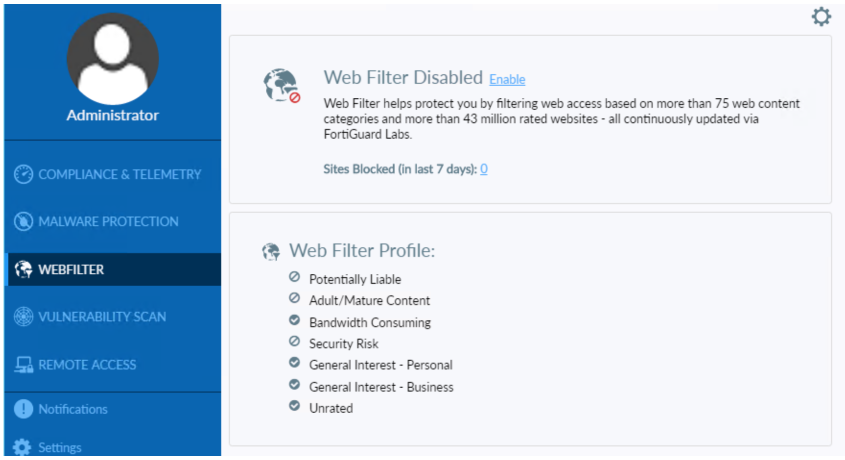
Enabling Web Filter

For FortiClient in managed mode, when FortiClient Telemetry is connected to a FortiGate or EMS, an administrator may enable, configure, and lock the web filter settings.

You can enable web filtering when EMS has not locked FortiClient Console and web filtering is excluded from FortiGate compliance rules.

To enable web filtering:

1. On the *Web Filter* tab, click *Enable* in FortiClient Console.



Web Filter Disabled Enable

Web Filter helps protect you by filtering web access based on more than 75 web content categories and more than 43 million rated websites - all continuously updated via FortiGuard Labs.

Sites Blocked (in last 7 days): 0

Web Filter Profile:

- Potentially Liable
- Adult/Mature Content
- Bandwidth Consuming
- Security Risk
- General Interest - Personal
- General Interest - Business
- Unrated

The following options are available:

Enable/Disable	Enable or disable Web Filter.
Sites Blocked (in last 7 days)	View Web Filter log entries of the violations that have occurred in the last seven days.
Web Filter Profile	Displays the Web Filter profile settings. You can also view violations.

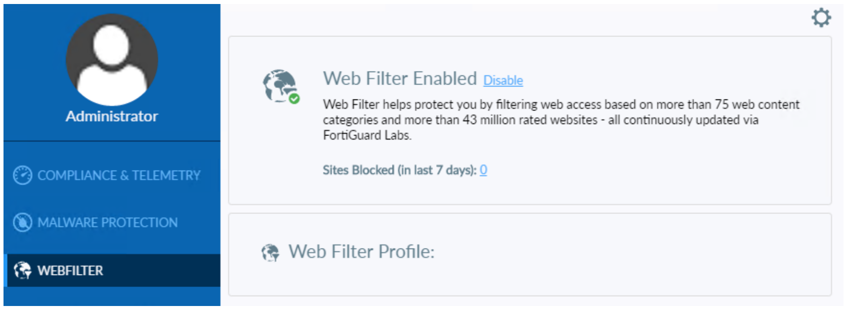
Disabling Web Filter

When FortiClient Telemetry is connected to FortiGate or EMS, you may be unable to disable web filtering.

You can disable web filtering if EMS has not locked FortiClient Console and web filtering is excluded from FortiGate compliance rules.

To disable web filtering:

1. On the *Web Filter* tab, click *Disable*.



Web Filter Enabled

Web Filter helps protect you by filtering web access based on more than 75 web content categories and more than 43 million rated websites - all continuously updated via FortiGuard Labs.

Sites Blocked (in last 7 days): 0

Web Filter Profile:

Configuring web filtering

You can configure web filtering settings, profiles, and exclusion lists.

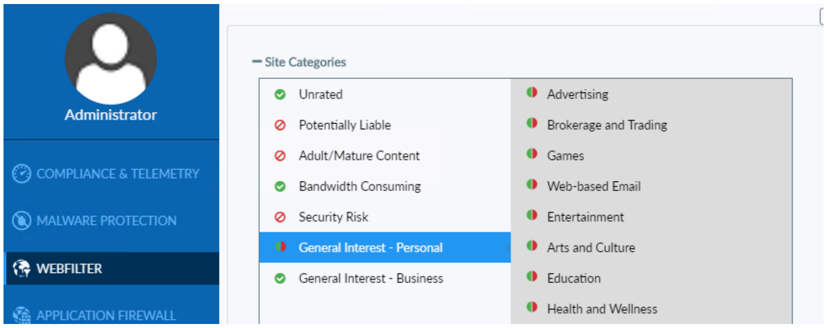
When FortiClient Telemetry is connected to FortiGate or EMS, you may be unable to configure web filtering.

Configuring site categories

You can configure FortiClient to allow, block, warn, or monitor web traffic based on site categories.

To configure site categories:

1. On the *Web Filter* tab, click the *Settings* icon.
2. Click a site category.
3. Click the action icon beside the desired sub-category.



− Site Categories

✓ Unrated	● Advertising
⊘ Potentially Liable	● Brokerage and Trading
⊘ Adult/Mature Content	● Games
✓ Bandwidth Consuming	● Web-based Email
⊘ Security Risk	● Entertainment
● General Interest - Personal	● Arts and Culture
✓ General Interest - Business	● Education
	● Health and Wellness

The following actions are available:

✓	**Allow**	Set the category or sub-category to *Allow* to allow access.
⊘	**Block**	Set the category or sub-category to *Block* to block access. The user receives a *Web Page Blocked* message in the web browser.
✓	**Warn**	Set the category or sub-category to *Warn* but allow access. The user receives a *Web Page Warning* message in the web browser. The user can proceed or go back to the previous web page.
◐	**Monitor**	Set the category or sub-category to *Monitor* to allow access. The site is logged.

You can enable or disable *Site Categories* in the *Web Filter* settings page. When site categories are disabled, the exclusion list protects FortiClient.

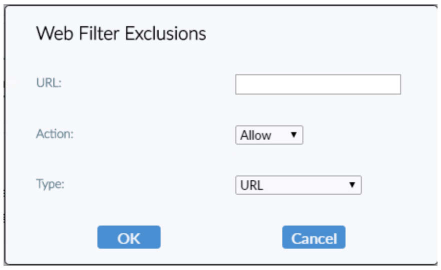
Managing the Web Filter exclusion list

You can add websites to the exclusion list and set the permission to allow, block, monitor, or exempt.

For information on URL formats, type, and action, see the *FortiOS Handbook* in the Fortinet Document Library.

To add items to the exclusion list:

1. On the *Web Filter* tab, click the *Settings* icon.
2. Under *Exclusion List*, click *Add* to add URLs to the exclusion list.
   If the website is part of a blocked category, an allow permission in the *Exclusion List* would allow the user to access the specific URL.



Web Filter Exclusions

URL:

Action: Allow

Type: URL

3. Configure the following settings:

Exclusion List		Select to exclude URLs that are explicitly blocked or allowed. Use the add icon to add URLs and the delete icon to delete URLs from the list. Select a URL and select the edit icon to edit the selection.
	URL	Enter a URL or IP address.
	Action	Select one of the following actions: • *Allow*: Allow access to the website regardless of the URL category or sub-category action. • *Deny*: Deny access to the website regardless of the URL category or sub-category action. • *Monitor*: Allow access to the website regardless of the URL category or sub-category action. A log message is generated each time a matching traffic session is established.
	Type	Select one of the following pattern types: • *Regular Expression* • *Wildcard* • *URL*

4. Click *OK*.

To edit items in the exclusion list:

1. On the *Web Filter* tab, click the *Settings* icon.
   The Settings page displays.
2. Under *Exclusion List*, click an item, and click *Edit*.
   The Edit dialog box displays.
3. Edit the settings and click *OK* to save the changes.

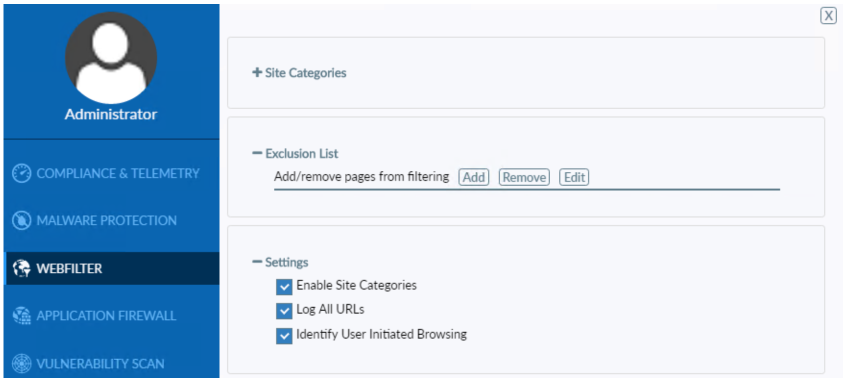
To remove items from the exclusion list:

1. On the *Web Filter* tab, click the *Settings* icon.
   The Settings page displays.
2. Under *Exclusion List*, click one or more items in the exclusion list.
   A checkmark displays beside the selected items.
3. Click *Remove*.
   The selected items are removed from the exclusion list.

Configuring settings

To configure settings:

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



Add/remove pages from filtering

☑ Enable Site Categories
☑ Log All URLs
☑ Identify User Initiated Browsing

2. Under Settings, configure the following settings:

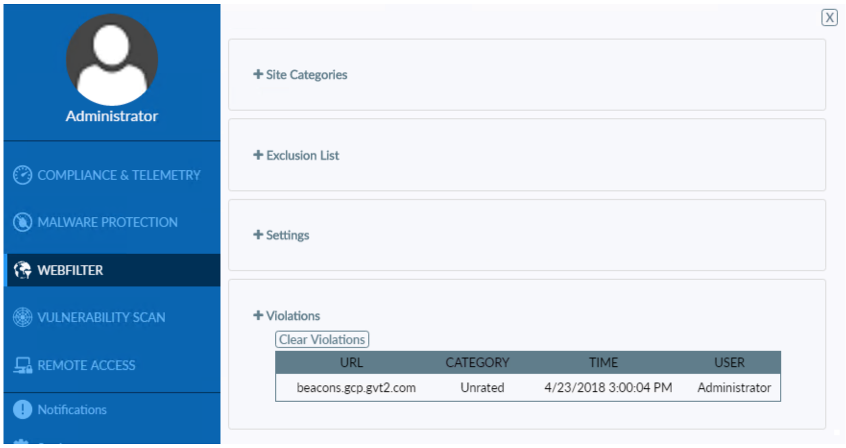
Enable Site Categories	Select to enable site categories. When site categories are disabled, the exclusion list protects FortiClient.
Log All URLs	Select to log all URLs.
Identify User Initiated Browsing	Select to identify web browsing that is user-initiated.

Viewing violations

You can view web filtering violations in FortiClient Console.

To view violations:

1. On the *Web Filter* tab, click the *Settings* icon.
   Alternately, you can click the *Sites Blocked (in last 7 days)* link



URL	CATEGORY	TIME	USER
beacons.gcp.gvt2.com	Unrated	4/23/2018 3:00:04 PM	Administrator

The following information displays under *Violations*.

URL	Website URL.
Category	Website sub-category.
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.

Application Firewall

This section applies only to FortiClient in managed mode.

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

Viewing blocked applications

To view blocked applications:

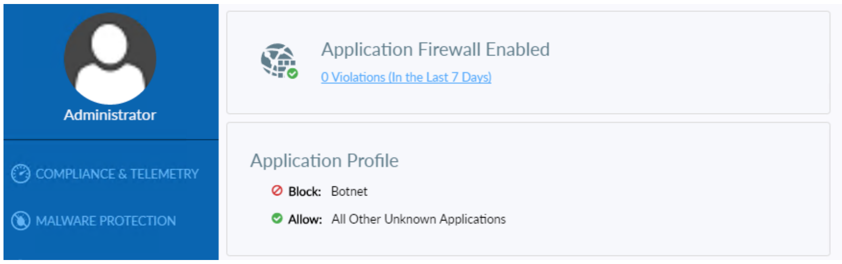
1. On the *Application Firewall* tab, click the *<number> Violations (In the Last 7 Days)* link.
   A page of all blocked applications blocked applications displays.

Viewing application firewall profiles

You can view the application firewall profile when FortiClient Telemetry is connected to EMS.

To view the application firewall profile:

1. Go to the *Application Firewall* tab.



Application Firewall Enabled
0 Violations (In the Last 7 Days)

Application Profile
Block: Botnet
Allow: All Other Unknown Applications

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 (FortiGuard.com)
- One-click link to install patches and resolve as many identified vulnerabilities as possible
- List of patches that require manual installation by the endpoint user to resolve vulnerabilities

FortiClient can detect known vulnerabilities for many software. For the list of software, see Vulnerability Patches on page 129.

When FortiClient is connected to FortiClient EMS, 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*.

Compliance and vulnerability scanning

If compliance is enabled for FortiClient in managed mode, and FortiGate compliance rules require it, all automatic and manual software patches must be installed within a time frame to maintain compliant status and network access. The default time frame is one day; however, the FortiGate administrator may choose a different time frame. Contact your system administrator to learn how long you have to fix vulnerabilities. For information about compliance, see Compliance on page 47.

Enabling vulnerability scan

Vulnerability scanning is enabled by default. You cannot disable or configure the vulnerability scan feature in FortiClient Console.

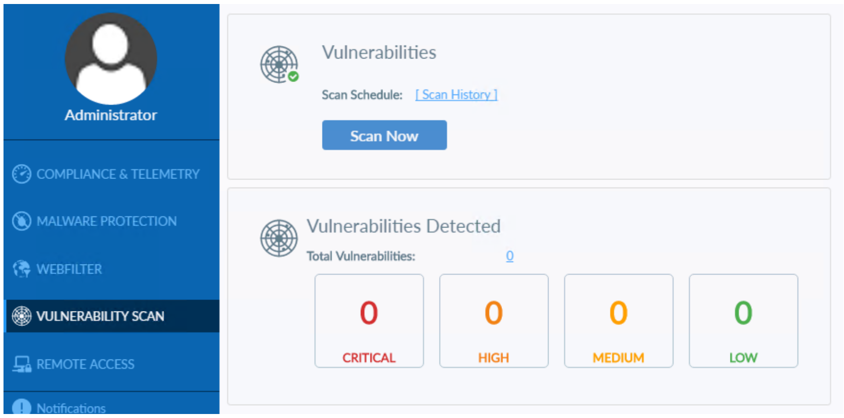
When FortiClient is in managed mode and managed by EMS, an administrator may configure and lock vulnerability scanning for you. An administrator may also disable vulnerability scanning.

Scanning now

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.

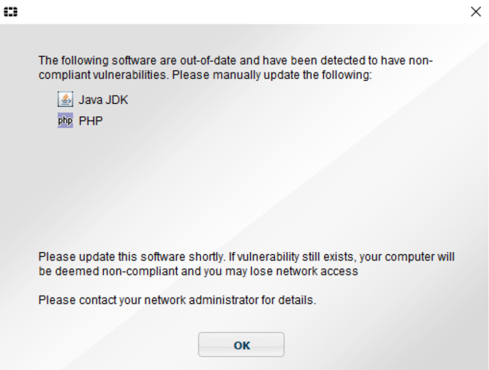
To scan now:

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 box 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 box:



The following software are out-of-date and have been detected to have non-compliant vulnerabilities. Please manually update the following:

Java JDK
PHP

Please update this software shortly. If vulnerability still exists, your computer will be deemed non-compliant and you may lose network access

Please contact your network administrator for details.

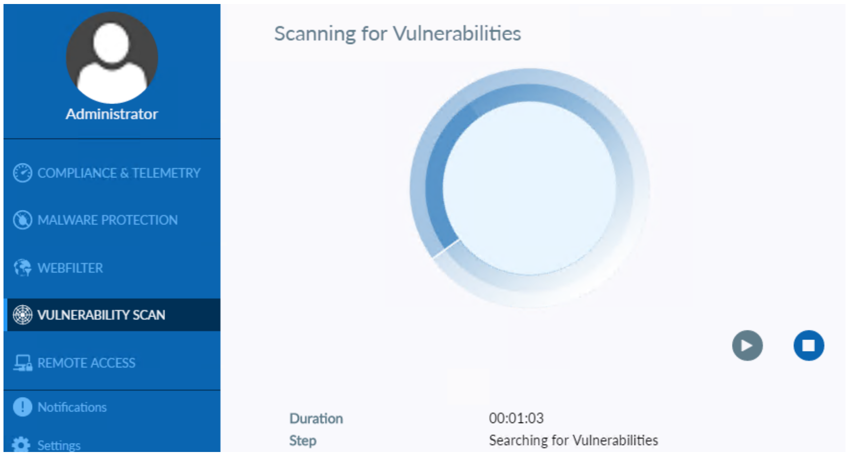
2. If applicable, read the list of software that requires manual installation of software patches, and click *OK*. See Manually fixing detected vulnerabilities on page 97.

Canceling scans

In standalone mode, when FortiClient is scanning for vulnerabilities, a *Cancel Scan* button displays, and you can click the button to cancel the scan.

To cancel a vulnerability scan:

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



Duration 00:01:03
Step Searching for Vulnerabilities

The vulnerability scan is canceled.

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.

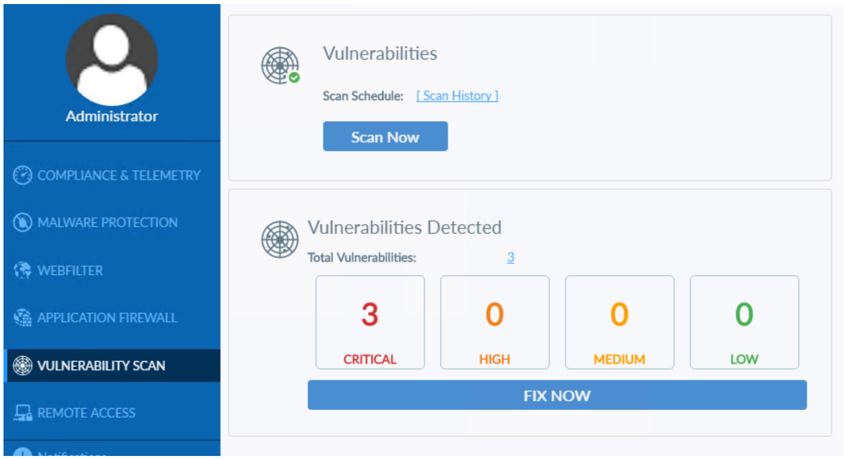
Any software patches that cannot be automatically installed are listed on the *Vulnerability Scan* tab and you should manually download and install software patches for the vulnerable software.

If compliance is enabled for FortiClient in managed mode and FortiGate compliance rules require it, all software patches must be installed within a time frame to maintain compliant status and network access. See Compliance and vulnerability scanning on page 93.

In managed mode, you may be unable to automatically fix vulnerabilities. An administrator may have the vulnerabilities automatically fixed for you.

To automatically fix detected vulnerabilities:

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



Scan Schedule:

Total Vulnerabilities: 3

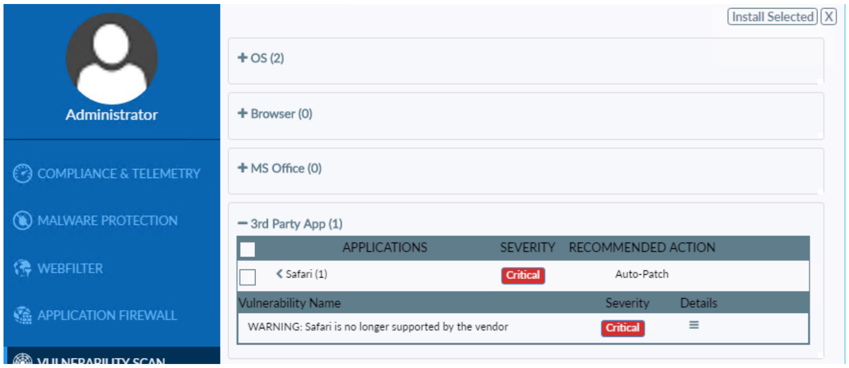
3	0	0	0
CRITICAL	HIGH	MEDIUM	LOW

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.



+ OS (2)

+ Browser (0)

+ MS Office (0)

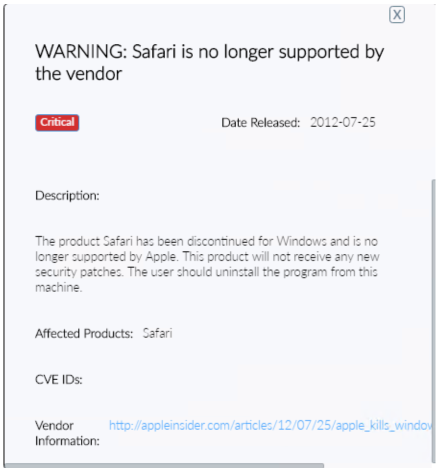
− 3rd Party App (1)

□	APPLICATIONS	SEVERITY	RECOMMENDED ACTION
□	< Safari (1)	Critical	Auto-Patch

Vulnerability Name	Severity	Details
WARNING: Safari is no longer supported by the vendor	Critical	≡

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.



WARNING: Safari is no longer supported by the vendor

Critical

Date Released: 2012-07-25

Description:

The product Safari has been discontinued for Windows and is no longer supported by Apple. This product will not receive any new security patches. The user should uninstall the program from this machine.

Affected Products: Safari

CVE IDs:

Vendor Information: http://appleinsider.com/articles/12/07/25/apple_kills_windov

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 now on page 93.

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 98.

If compliance is enabled for FortiClient in managed mode, and FortiGate compliance rules require it, all software patches must be installed within a time frame to maintain compliant status and network access. See also Compliance and vulnerability scanning on page 93.

To manually fix detected vulnerabilities:

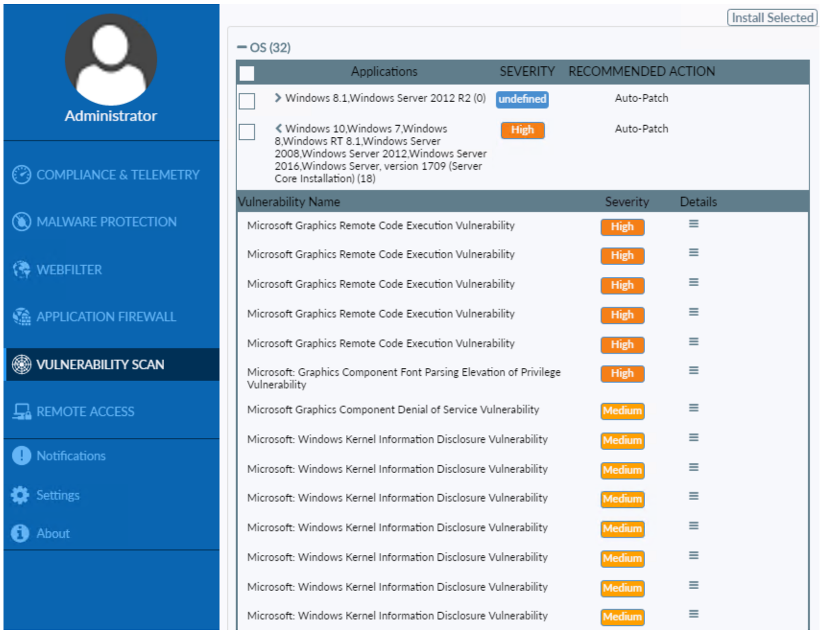
1. On the *Vulnerability Scan* tab, identify the software that requires manual fixing.
   Any software with detected vulnerabilities that requires you to manually download and install software patches is displayed in the *Vulnerabilities Detected* area.
2. Download the latest software patch for each 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:

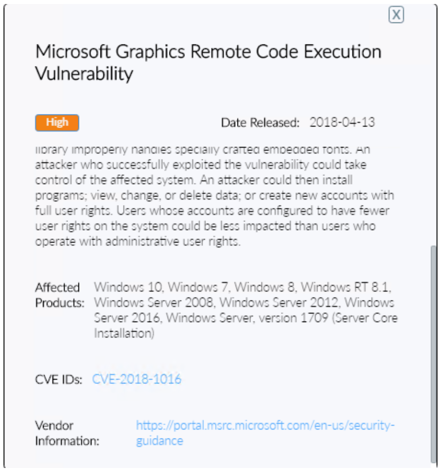
1. On the *Vulnerability Scan* tab, any software with detected vulnerabilities that requires you to manually download and install software patches displays in the *Vulnerabilities Detected* area.
2. You can view more details on all vulnerabilities by clicking the number of total vulnerabilities detected.
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.



☐	Applications	SEVERITY	RECOMMENDED ACTION
☐	> Windows 8.1,Windows Server 2012 R2 (0)	undefined	Auto-Patch
☐	< Windows 10,Windows 7,Windows 8,Windows RT 8.1,Windows Server 2008,Windows Server 2012,Windows Server 2016,Windows Server, version 1709 (Server Core Installation) (18)	High	Auto-Patch

Vulnerability Name	Severity	Details
Microsoft Graphics Remote Code Execution Vulnerability	High	≡
Microsoft Graphics Remote Code Execution Vulnerability	High	≡
Microsoft Graphics Remote Code Execution Vulnerability	High	≡
Microsoft Graphics Remote Code Execution Vulnerability	High	≡
Microsoft Graphics Remote Code Execution Vulnerability	High	≡
Microsoft: Graphics Component Font Parsing Elevation of Privilege Vulnerability	High	≡
Microsoft Graphics Component Denial of Service Vulnerability	Medium	≡
Microsoft: Windows Kernel Information Disclosure Vulnerability	Medium	≡
Microsoft: Windows Kernel Information Disclosure Vulnerability	Medium	≡
Microsoft: Windows Kernel Information Disclosure Vulnerability	Medium	≡
Microsoft: Windows Kernel Information Disclosure Vulnerability	Medium	≡
Microsoft: Windows Kernel Information Disclosure Vulnerability	Medium	≡
Microsoft: Windows Kernel Information Disclosure Vulnerability	Medium	≡
Microsoft: Windows Kernel Information Disclosure Vulnerability	Medium	≡

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>*.



Microsoft Graphics Remote Code Execution Vulnerability

High Date Released: 2018-04-13

library improperly handles specially crafted embedded fonts. An attacker who successfully exploited the vulnerability could take control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

Affected Products: Windows 10, Windows 7, Windows 8, Windows RT 8.1, Windows Server 2008, Windows Server 2012, Windows Server 2016, Windows Server, version 1709 (Server Core Installation)

CVE IDs: CVE-2018-1016

Vendor Information: https://portal.msrc.microsoft.com/en-us/security-guidance

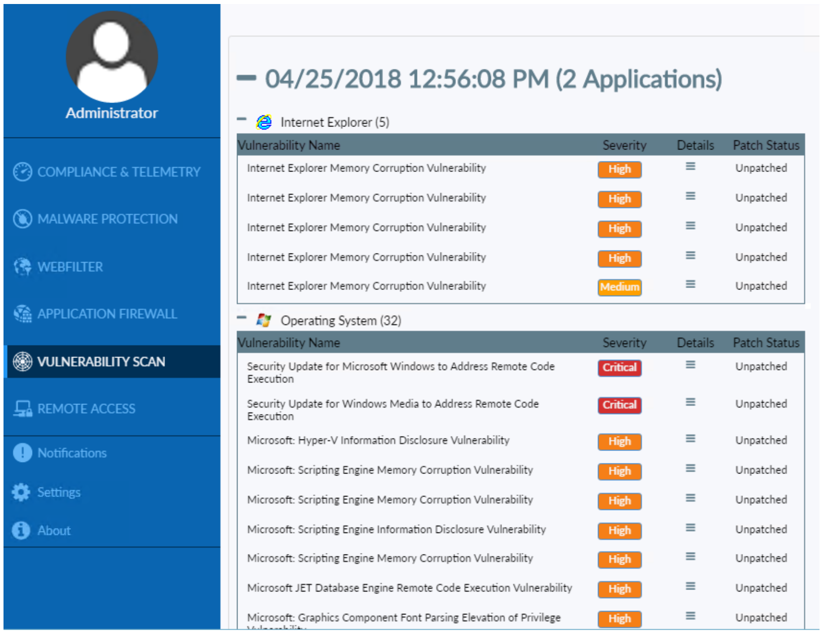
5. Click *Close*.

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 patch history:

1. In FortiClient Console, 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.



— 04/25/2018 12:56:08 PM (2 Applications)

— Internet Explorer (5)

Vulnerability Name	Severity	Details	Patch Status
Internet Explorer Memory Corruption Vulnerability	High	≡	Unpatched
Internet Explorer Memory Corruption Vulnerability	High	≡	Unpatched
Internet Explorer Memory Corruption Vulnerability	High	≡	Unpatched
Internet Explorer Memory Corruption Vulnerability	High	≡	Unpatched
Internet Explorer Memory Corruption Vulnerability	Medium	≡	Unpatched

— Operating System (32)

Vulnerability Name	Severity	Details	Patch Status
Security Update for Microsoft Windows to Address Remote Code Execution	Critical	≡	Unpatched
Security Update for Windows Media to Address Remote Code Execution	Critical	≡	Unpatched
Microsoft: Hyper-V Information Disclosure Vulnerability	High	≡	Unpatched
Microsoft: Scripting Engine Memory Corruption Vulnerability	High	≡	Unpatched
Microsoft: Scripting Engine Memory Corruption Vulnerability	High	≡	Unpatched
Microsoft: Scripting Engine Information Disclosure Vulnerability	High	≡	Unpatched
Microsoft: Scripting Engine Memory Corruption Vulnerability	High	≡	Unpatched
Microsoft JET Database Engine Remote Code Execution Vulnerability	High	≡	Unpatched
Microsoft: Graphics Component Font Parsing Elevation of Privilege	High	≡	Unpatched

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 Console and endpoint users can configure new VPN connections using FortiClient Console.

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

Enabling remote access

The *Remote Access* tab displays in FortiClient Console when FortiClient is installed with *Secure Remote Access* selected.

When FortiClient is in managed mode and managed by EMS, FortiClient may include VPN connection configurations for you to use.

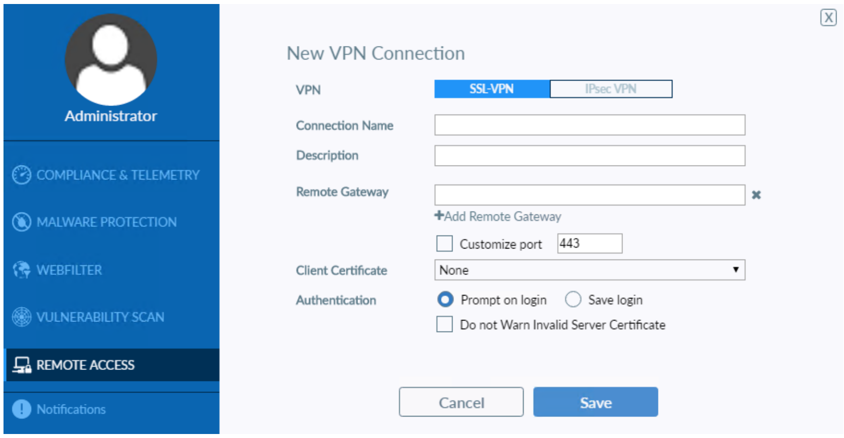
Configuring VPN connections

You can configure SSL VPN connections and IPsec VPN connections using FortiClient Console.

Configuring SSL VPN connections

To configure SSL VPN connections:

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



New VPN Connection

VPN: SSL-VPN

Connection Name

Description

Remote Gateway

□ Customize port 443

Client Certificate: None

Authentication: ● Prompt on login ○ Save login

□ Do not Warn Invalid Server Certificate

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

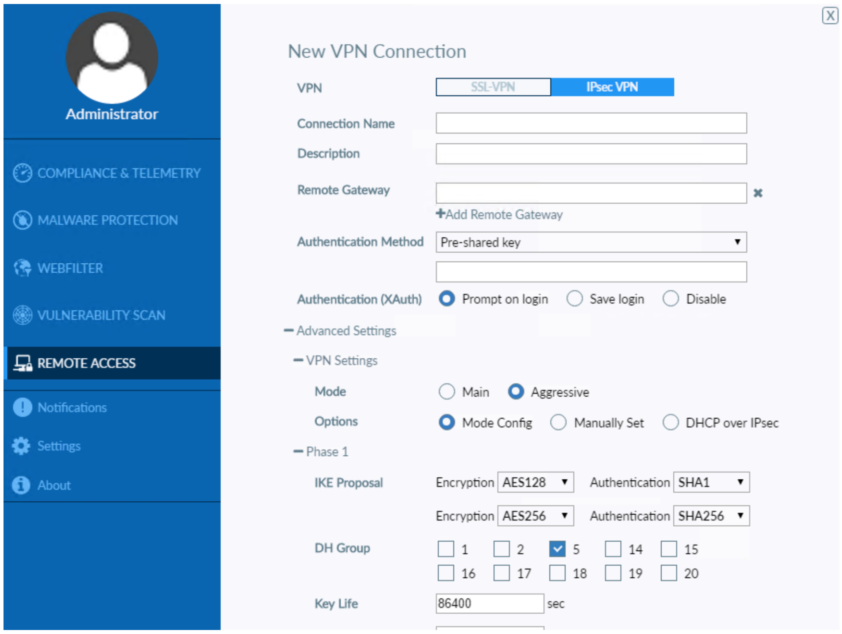
Connection Name	Enter a name for the connection.
Description	(Optional) Enter a description for the connection.
Remote Gateway	Enter the IP address/hostname of the remote gateway. Multiple remote gateways can be configured by separating each entry with a semicolon. If one gateway is not available, the VPN connects to the next configured gateway.
Customize port	Select to change the port. The default port is 443.
Client Certificate	Select to enable client certificates, then select *Prompt on connect* or the certificate from the dropdown list.
Authentication	Select to *Prompt on login* or *Save login*. The *Disable* option is available when *Client Certificate* is enabled.
Username	If you selected *Save login*, type 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.

Configuring IPsec VPN connections

To configure IPsec VPN connections:

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



New VPN Connection

VPN: IPsec VPN

Connection Name

Description

Remote Gateway

Authentication Method: Pre-shared key

Authentication (XAuth): ● Prompt on login ○ Save login ○ Disable

Mode: ○ Main ● Aggressive

Options: ● Mode Config ○ Manually Set ○ DHCP over IPsec

IKE Proposal: Encryption AES128 Authentication SHA1

Encryption AES256 Authentication SHA256

DH Group: □ 1 □ 2 ☑ 5 □ 14 □ 15 □ 16 □ 17 □ 18 □ 19 □ 20

Key Life: 86400 sec

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. Multiple remote gateways can be configured by separating each entry with a semicolon. 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*.
Username	If you selected *Save login*, type the username to save for the login.
Advanced Settings	Configure VPN settings, phase 1, and phase 2 settings.
VPN Settings	
Mode	Select one of the following: • *Main*: In main mode, the phase 1 parameters are exchanged in multiple rounds with encrypted authentication information. • *Aggressive*: In aggressive mode, the 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, assign IP address, and subnet values. 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 will result 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 will be

		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 SSL and IPsec VPNs

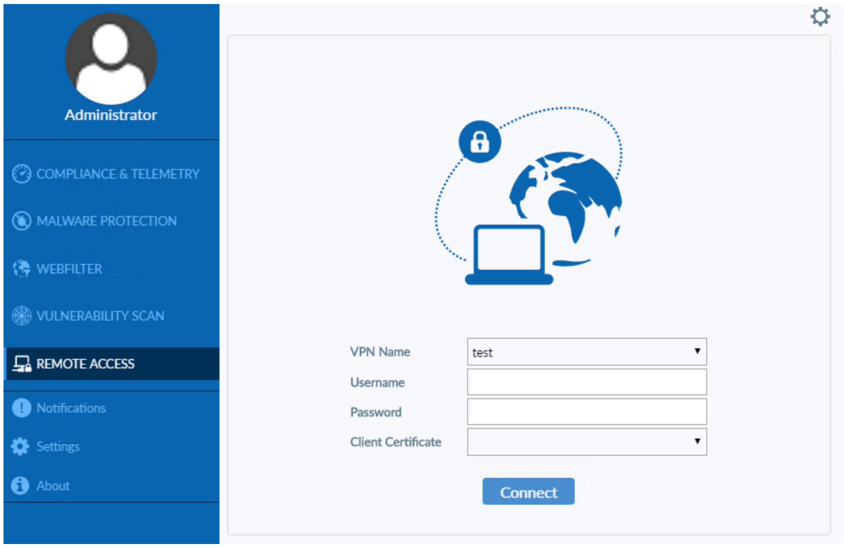
Depending on the FortiClient configuration, you may also have permission to edit an existing VPN connection and delete an existing VPN connection.

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

To connect to VPNs:

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

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



VPN Name: test
Username:
Password:
Client Certificate:

2. Type 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 Console.

   Your administrator may have configure FortiClient to automatically locate a certificate for you.
4. Click the *Connect* button.
   When connected, FortiClient Console 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.

Connecting VPNs with FortiToken Mobile

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

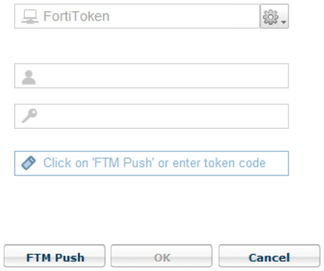
FortiGate can be configured to let you push a token from FortiToken Mobile to FortiGate to complete network authentication when connecting VPNs. When configured, you can select the push token option by clicking the FTM Push button in FortiClient Console. This notifies the FortiGate that you choose to use the push token option. Following this, you will 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 type a token code from FortiToken Mobile into FortiClient Console when connecting VPNs.

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

To connect VPNs 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 VPNs with FortiToken Mobile by typing token codes:

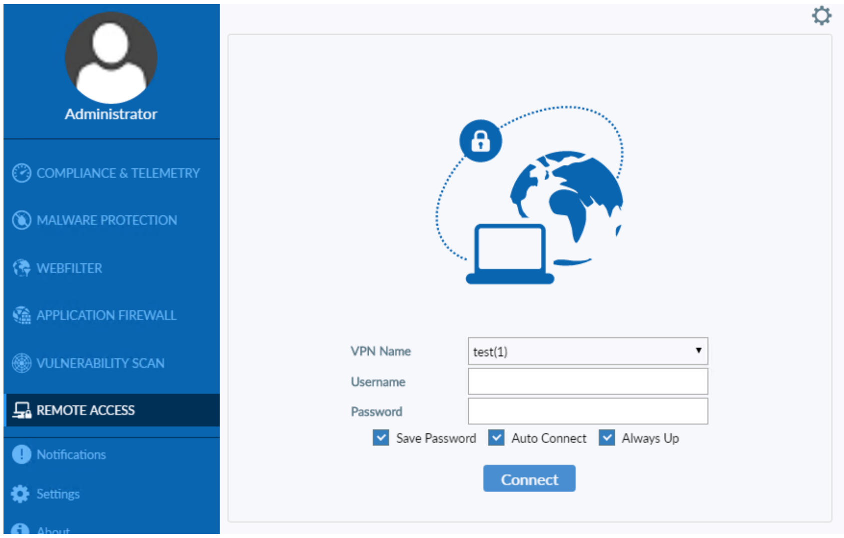
1. On the *Remote Access* tab, select the VPN connection from the dropdown list.
2. Enter your username and password and click the *Connect* button.
   The *Enter token code* box displays.
3. Type the token code from your FortiToken Mobile and click *OK* to complete network authentication.

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 the console.
- *Auto Connect*: When FortiClient is launched, the VPN connection automatically connects.
- *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)*.



VPN Name: test(1)

Username:

Password:

☑ Save Password ☑ Auto Connect ☑ Always Up

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, and they will 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 (Microsoft 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. For information, see the *FortiClient XML Reference*.

Activating VPN before Windows log on

When using VPN before Windows log on, the user is offered a list of preconfigured VPN connections to select from on the Windows log on screen. This requires that the Windows log on screen is not bypassed. As such, if VPN before Windows log on 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 box.

To make this change, proceed as follows:

In FortiClient:

1. Create the VPN tunnels of interest or connect to FortiClient EMS, which provides the VPN list of interest.
2. Enable VPN before log on to the FortiClient Settings page, see VPN options on page 119.

On the Microsoft Windows system,

1. Start an elevated command line prompt.
2. Enter `control passwords2` and press `Enter`. Alternatively, you can enter `netplwiz`.
3. Check the checkbox for *Users must enter a user name and password to use this computer*.
4. 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>
      <options>
         <show_vpn_before_logon>1</show_vpn_before_logon>
         <use_windows_credentials>1</use_windows_credentials>
      </options>
   </vpn>
</forticlient_configuration>
            ...
            </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. All closing tags are included but some important elements to complete the IPsec VPN configuration are omitted.

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. All closing tags are included, but some important elements to complete the IPsec VPN configuration are omitted.

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.

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

This is a balanced but incomplete XML configuration fragment. All closing tags are included, but some important elements to complete the SSL VPN configuration are omitted.

For SSL VPN, all FortiGates 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. All closing tags are included, but some important elements to complete the SSL VPN configuration are omitted.

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

Advanced features (Mac OS X)

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*.

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. All closing tags are included, but some important elements to complete the IPsec VPN configuration are omitted.

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. All closing tags are included, but some important elements to complete the SSL VPN configuration are omitted.

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. All closing tags are included, but some important elements to complete the SSL VPN configuration are omitted.

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

VPN tunnel and script

This feature supports auto running a user-defined script after the configured VPN tunnel is connected or disconnected. The scripts are batch scripts in Windows and shell scripts in Mac OS X. 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. When FortiClient's VPN tunnel is connected or disconnected, the respective script defined under that tunnel is executed.

Windows

Map 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>
```

Delete a network drive after tunnel is disconnected

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>
```

Delete a network drive after tunnel is disconnected

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>
```

OS X

Map 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>
```

Delete a network drive after tunnel is disconnected

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 SSL VPN client

Windows and Mac OS X

There is no VPN-only installer for Windows and Mac. Customers can install VPN-only features manually during installation, or create a VPN-only installer using the FortiClient Configurator Tool. The FortiClient Configurator Tool is available from Fortinet Developer Network.

Alternatively, to use only SSL VPN on a Windows endpoint, you can download the SSL VPN-only FortiClient App from the Microsoft App Store.

Linux

An SSL VPN tunnel client standalone installer for Linux operating systems is available from the Fortinet Developer Network. For details, see the *FortiOS Release Notes*.

Settings

This section describes the options on the *Settings* page.

What options you can change on the *Settings* page depends on whether FortiClient is in standalone or managed mode. In managed mode, FortiGate or EMS may lock settings.

System

You can back up or restore a FortiClient configuration.

Backing up or restoring full configuration files

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

To backup or restore the full configuration 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

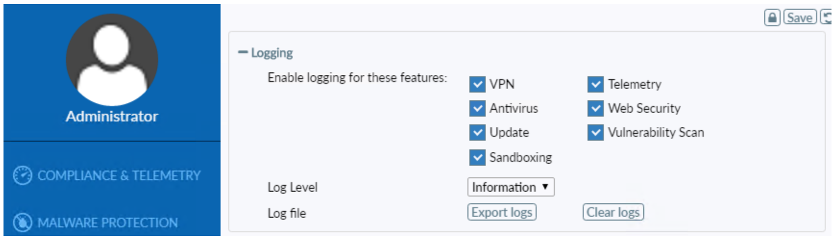
This setting can only be configured when FortiClient is in standalone mode.

Enabling logging for features

You can enable logging for modules available in FortiClient Console. Logging options are hidden for modules not available in FortiClient Console.

To enable logging for features:

1. Go to *Settings*.
2. Expand the *Logging* section.



− Logging

Enable logging for these features: ☑ VPN ☑ Antivirus ☑ Update ☑ Sandboxing ☑ Telemetry ☑ Web Security ☑ Vulnerability Scan

Log Level: Information ▾

Log file: Export logs Clear logs

3. Select the features for which you want to add entries to the log file:

VPN	Select *VPN* to enable logging for this feature.
AntiVirus	Select *AntiVirus* to enable logging for this feature.
Update	Select *Update* to enable logging for FortiClient software updates.
Sandboxing	Select *Sandboxing* to enable logging for this feature.
Telemetry	Select *Telemetry* to enable logging for this feature.
Web Security	Select *Web Security* to enable logging for this feature.
Vulnerability Scan	Select *Vulnerability Scan* to enable logging for this feature.

4. Select a logging level, and click *Save*.

Emergency	The system becomes unstable.
Alert	Immediate action is required.
Critical	Functionality is affected.
Error	An error condition exists and functionality could be affected.
Warning	Functionality could be affected.
Notice	Information about normal events.
Information	General information about system operations.
Debug	Debug FortiClient.

⚠ It is recommended to use the debug logging level only when needed. Do not leave the debug logging level permanently enabled in a production environment to avoid unnecessarily consuming disk space.

Sending logs to FortiAnalyzer or FortiManager

The following products are required for an administrator to configure FortiClient in managed mode to send logs to FortiAnalyzer or FortiManager:

- FortiClient
- FortiGate or EMS
- FortiAnalyzer or FortiManager

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

Where you locate FortiClient logs in FortiAnalyzer depends on where FortiClient Telemetry is connected:

- When FortiClient connects Telemetry to EMS, the FortiClient logs are displayed in the FortiClient ADOM in FortiAnalyzer. In this scenario FortiGate is not used.
- When FortiClient connects Telemetry to FortiGate, the FortiClient logs are displayed in the FortiGate ADOM. Even if EMS is used with FortiGate to manage FortiClient endpoints, the FortiClient logs still display in the FortiGate ADOM.

FortiClient Telemetry must connect to FortiGate or EMS for FortiClient to upload logs to FortiAnalyzer or FortiManager.

Exporting the log file

You can export the log file (`.log`) from FortiClient.

To export log files:

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

Clearing entries in the log file

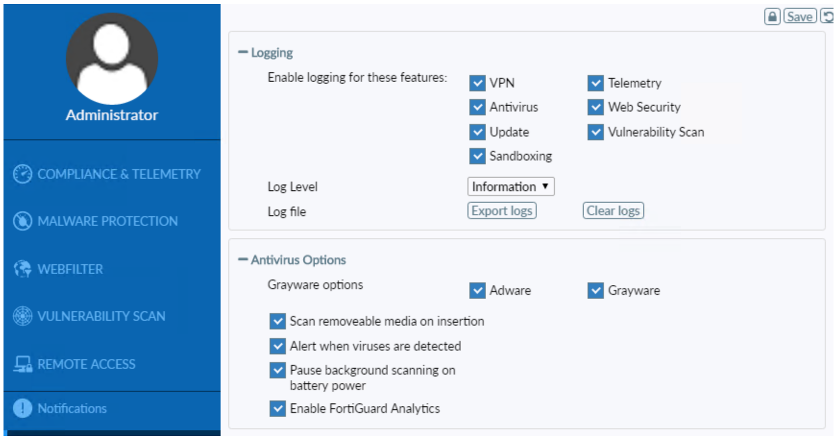
To clear entries in the log file:

1. Go to *Settings*.
2. Expand the *Logging* section, and click *Clear logs*.
   A confirmation dialog box displays.
3. Click *Yes* to confirm.

Antivirus options

To configure antivirus options:

1. Go to *Settings*, and expand the *Antivirus Options* section.



− Logging

Enable logging for these features: ☑ VPN ☑ Telemetry ☑ Antivirus ☑ Web Security ☑ Update ☑ Vulnerability Scan ☑ Sandboxing

Log Level: Information ▾

Log file: Export logs Clear logs

− Antivirus Options

Grayware options: ☑ Adware ☑ Grayware

☑ Scan removeable media on insertion

☑ Alert when viruses are detected

☑ Pause background scanning on battery power

☑ Enable FortiGuard Analytics

2. Configure the following settings, and click *Save*:

Grayware options	Grayware is an umbrella term applied to a wide range of malicious applications such as spyware, adware, and key loggers that are often secretly installed on a user's computer to track and/or report certain information back to an external source without the user's permission or knowledge.
Adware	Select to enable adware detection and quarantine during the antivirus scan.
Riskware	Select to enable riskware detection and quarantine during the antivirus scan.
Scan removable media on insertion	Select to scan removable media when it is inserted.
Alert when viruses are detected	Select to have FortiClient provide a notification alert when a threat is detected on your personal computer. When *Alert when viruses are detected* under *AntiVirus Options* is not selected, you will not receive the virus alert dialog box when attempting to download a virus in a web browser.
Pause background scanning on battery power	Select to pause background scanning when your computer is operating on battery power.
Enable FortiGuard Analytics	Select to automatically send suspicious files to the FortiGuard Network for analysis.

VPN options

To configure VPN options:

1. Go to *Settings* and expand the *VPN Options* section.
2. Select *Enable VPN before logon* to enable VPN before log on.

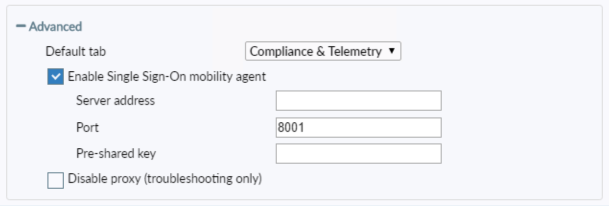
3. Click *Save*.

Advanced options

These settings can be configured only when FortiClient is in standalone mode. When FortiClient Telemetry is connected to FortiGate or EMS, these settings are set by the XML configuration (if configured).

To configure advanced options:

1. Go to *Settings*, and expand the *Advanced* section.



− Advanced

Default tab: Compliance & Telemetry ▾

☑ Enable Single Sign-On mobility agent

Server address:

Port: 8001

Pre-shared key:

☐ Disable proxy (troubleshooting only)

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	Select to enable single sign-on mobility agent for FortiAuthenticator. To use this feature you need to apply a FortiClient SSO mobility agent license to your FortiAuthenticator device.
Server address	Enter the FortiAuthenticator IP address.
Port	Enter the port number. The default port is 8001.
Pre-shared key	Enter the preshared key. The preshared key should match the key configured on your FortiAuthenticator device.
Disable proxy (troubleshooting only)	Select to disable proxy when troubleshooting FortiClient.

Single Sign-On mobility agent

The FortiClient Single Sign-On (SSO) mobility agent is a client that updates FortiAuthenticator with user logon and network information.

FortiClient/FortiAuthenticator protocol

FortiAuthenticator listens on a configurable TCP port. FortiClient connects to FortiAuthenticator using TLS/SSL with two-way certificate authentication. FortiClient sends a logon packet to FortiAuthenticator, which replies with an acknowledgment packet.

FortiClient/FortiAuthenticator communication requires the following:

- The IP address should be unique in the entire network.
- FortiAuthenticator should be accessible from clients in all locations.
- All FortiGates should be able to access FortiAuthenticator.

FortiClient Single Sign-On mobility agent requires FortiAuthenticator running 2.0.0 or later, or 3.0.0 or later. Enter the FortiAuthenticator (server) IP address, port number, and the preshared key configured on FortiAuthenticator.

To enable Single Sign-On mobility agent on FortiClient:

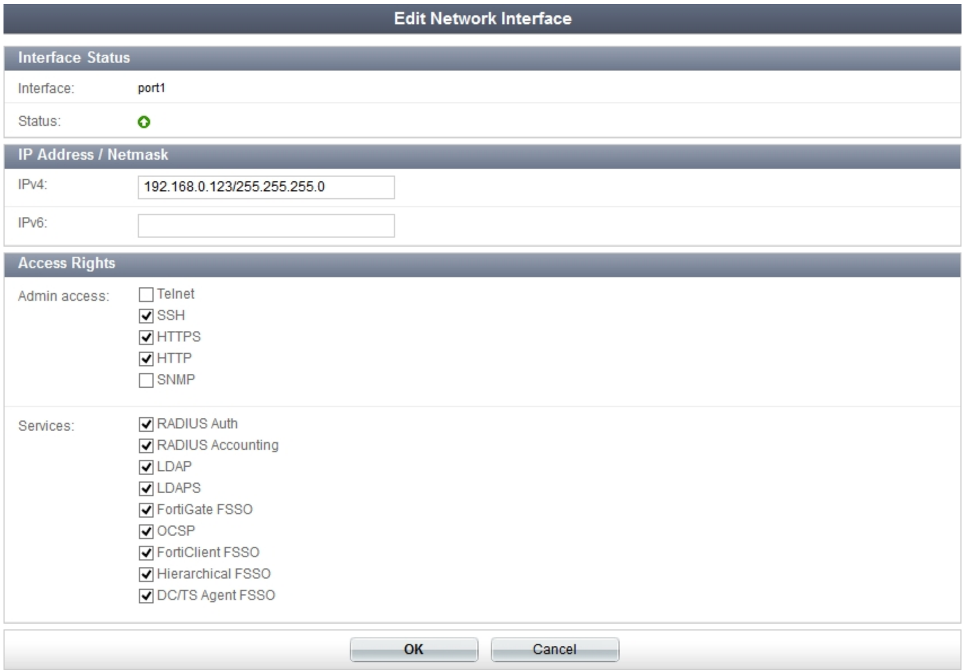
1. In FortiClient Console, go to *Settings*.
2. Expand the *Advanced* section and select *Enable Single Sign-On mobility agent*.
3. Enter the FortiAuthenticator server address and the preshared key.
4. Click *Save*.

To enable FortiClient SSO mobility agent service on the FortiAuthenticator:

1. In FortiAuthenticator, select *Fortinet SSO Methods > SSO > General*. The *Edit SSO Configuration* page opens.
2. Select *Enable FortiClient SSO Mobility Agent Service* and enter a TCP port value for the listening port.
3. Select *Enable authentication* and enter a secret key or password.
4. Select *OK* to save the setting.

To enable FortiClient FSSO services on the interface:

1. Select *System > Network > Interfaces*. Select the interface and select *Edit* from the toolbar. The *Edit Network Interface* window opens.



Edit Network Interface

Interface Status

Interface: port1

Status: ●

IP Address / Netmask

IPv4: 192.168.0.123/255.255.255.0

IPv6:

Access Rights

Admin access:
☐ Telnet
☑ SSH
☑ HTTPS
☑ HTTP
☐ SNMP

Services:
☑ RADIUS Auth
☑ RADIUS Accounting
☑ LDAP
☑ LDAPS
☑ FortiGate FSSO
☑ OCSP
☑ FortiClient FSSO
☑ Hierarchical FSSO
☑ DC/TS Agent FSSO

2. Select the checkbox to enable *FortiClient FSSO*.
3. Click *OK* to save the setting.

To enable the FortiClient SSO mobility agent service on FortiAuthenticator, you must first apply the applicable FortiClient license for FortiAuthenticator. See the *FortiAuthenticator Administration Guide* in the Fortinet Document Library.

For information on purchasing a FortiClient license for FortiAuthenticator, contact your authorized Fortinet reseller.

Configuration lock

This setting can only be configured when FortiClient is in standalone mode.

You can prevent unauthorized changes to the FortiClient configuration by locking the configuration. When the configuration is locked, configuration changes are restricted and FortiClient cannot be shut down or uninstalled.

When the configuration is locked, you can perform the following actions on the *Settings* page:

- Back up the FortiClient configuration
- Export FortiClient logs

If you want to change the configuration or shut down FortiClient, you must unlock the configuration first.

To lock the configuration:

1. Go to *Settings*.
2. Click the lock icon in the upper right corner.
3. In the *Password* box, type a password.
   Ensure you remember the password. You will need to use it to unlock the configuration.
4. In the *Re-enter Password* box, retype the password.
5. Click *Lock*.

To unlock the configuration:

1. Go to *Settings*.
2. Click the lock icon in the bottom left corner.
3. In the *Password* box, type the password used to lock the configuration.
4. Click *Unlock*.

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 Console is closed.

- Default menu options:
  - Open FortiClient Console
  - Shut down FortiClient

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

If you hover the mouse cursor over the FortiTray icon, you will receive various notifications including the version, antivirus signature, and antivirus engine.

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

Establishing VPN connections from FortiTray

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. Type your username and password in the authentication window, and click *OK* to connect.

Diagnostic Tool

You can access the FortiClient Diagnostic Tool from FortiClient Console. 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.

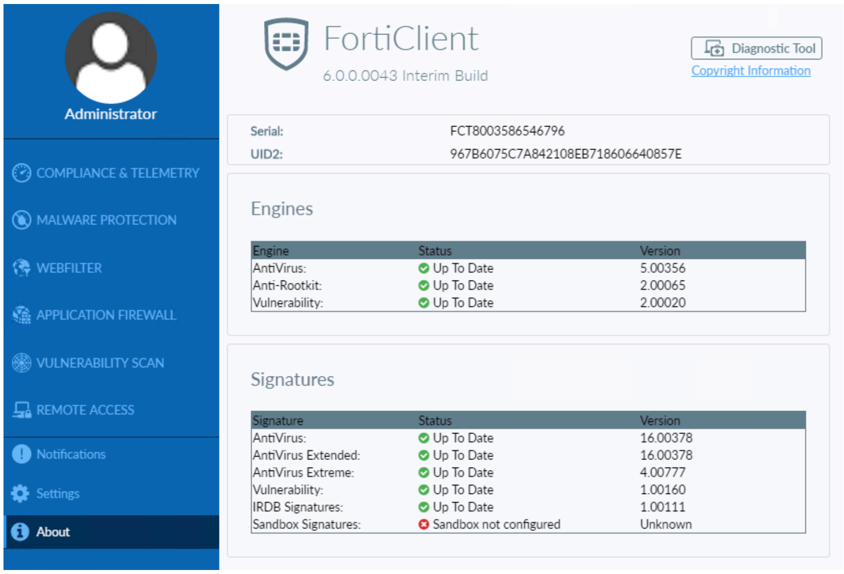
The FortiClient Diagnostic Tool does not record sensitive information. It contains information about the endpoint such as:

- 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 created by FortiClient Diagnostic Tool, you can open and read the package.

To generate debug reports:

1. Go to *About*.



Serial: FCT8003586546796
UID2: 967B6075C7A842108EB718606640857E

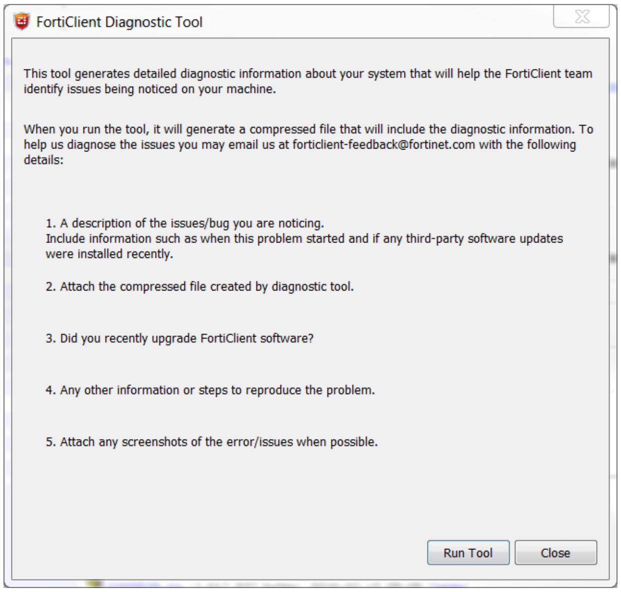
Engines

Engine	Status	Version
AntiVirus:	✓ Up To Date	5.00356
Anti-Rootkit:	✓ Up To Date	2.00065
Vulnerability:	✓ Up To Date	2.00020

Signatures

Signature	Status	Version
AntiVirus:	✓ Up To Date	16.00378
AntiVirus Extended:	✓ Up To Date	16.00378
AntiVirus Extreme:	✓ Up To Date	4.00777
Vulnerability:	✓ Up To Date	1.00160
IRDB Signatures:	✓ Up To Date	1.00111
Sandbox Signatures:	✗ Sandbox not configured	Unknown

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



FortiClient Diagnostic Tool

This tool generates detailed diagnostic information about your system that will help the FortiClient team identify issues being noticed on your machine.

When you run the tool, it will generate a compressed file that will include the diagnostic information. To help us diagnose the issues you may email us at forticlient-feedback@fortinet.com with the following details:

1. A description of the issues/bug you are noticing.
   Include information such as when this problem started and if any third-party software updates were installed recently.

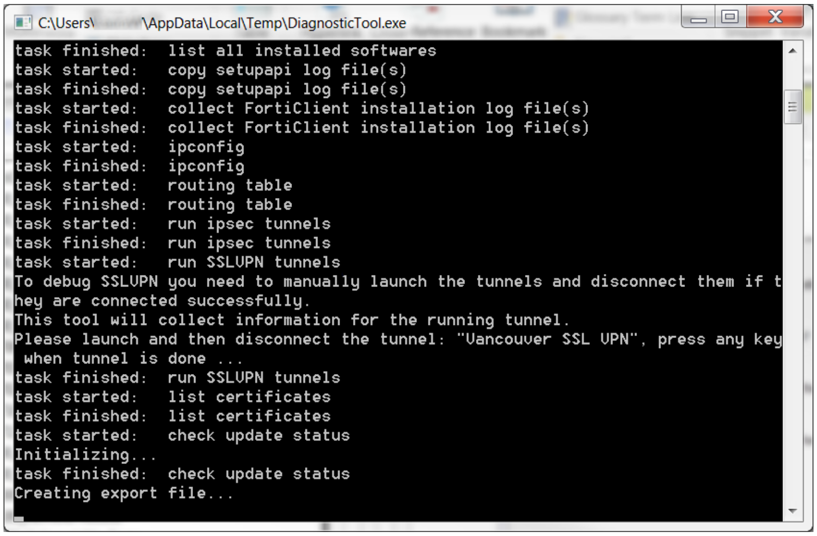
2. Attach the compressed file created by diagnostic tool.

3. Did you recently upgrade FortiClient software?

4. Any other information or steps to reproduce the problem.

5. Attach any screenshots of the error/issues when possible.

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



C:\Users\[redacted]\AppData\Local\Temp\DiagnosticTool.exe

```
task finished:  list all installed softwares
task started:   copy setupapi log file(s)
task finished:  copy setupapi log file(s)
task started:   collect FortiClient installation log file(s)
task finished:  collect FortiClient installation log file(s)
task started:   ipconfig
task finished:  ipconfig
task started:   routing table
task finished:  routing table
task started:   run ipsec tunnels
task finished:  run ipsec tunnels
task started:   run SSLVPN tunnels
To debug SSLVPN you need to manually launch the tunnels and disconnect them if t
hey are connected successfully.
This tool will collect information for the running tunnel.
Please launch and then disconnect the tunnel: "Vancouver SSL VPN", press any key
 when tunnel is done ...
task finished:  run SSLVPN tunnels
task started:   list certificates
task finished:  list certificates
task started:   check update status
Initializing...
task finished:  check update status
Creating export file...
```

4. (Optional) When prompted, launch and disconnect the VPN tunnels for which you want to collect information.
   A *Diagnostic_Result* file is created and displays 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. The API can be used with IPsec VPN only. SSL VPN is currently not supported.

Overview

The FortiClient COM library provides functionality to:

- Retrieve a list of the VPN tunnels configured in the FortiClient application.
- Start and stop any of the configured VPN tunnels.
- Send XAuth credentials.
- Retrieve status information:
  - configured tunnel list
  - active tunnel name
  - connected or not
  - idle or not
  - 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 Automation 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 is deprecated in FortiClient v5.0.
`GetRemainingKeyLife(bstrTunnelName As String, pSecs As Long, pKBytes As Long)`	Retrieve the remaining key life for the named connection. Whether keylife time (pSecs) or data (pKBytes) are significant depends on the detailed settings in the FortiClient application.

`MakeSystemPolicyCompliant()`	Command is deprecated in FortiClient v5.0.
`SendXAuthResponse (tunnelName As String, userName As String, password As String, savePassword As Boolean)`	Send XAuth credentials for the named connection: • User name, Password • True if password should be saved.
`SetPolicy (bAV As Boolean, bAS As Boolean, bFW As Boolean, bWF As Boolean)`	Command is deprecated in FortiClient v5.0.

`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 is deprecated in FortiClient v5.0.
`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 6.0.0 Online Help. The table of log messages is too wide to fit into the page size of the *FortiClient 6.0.0 Administration Guide*.

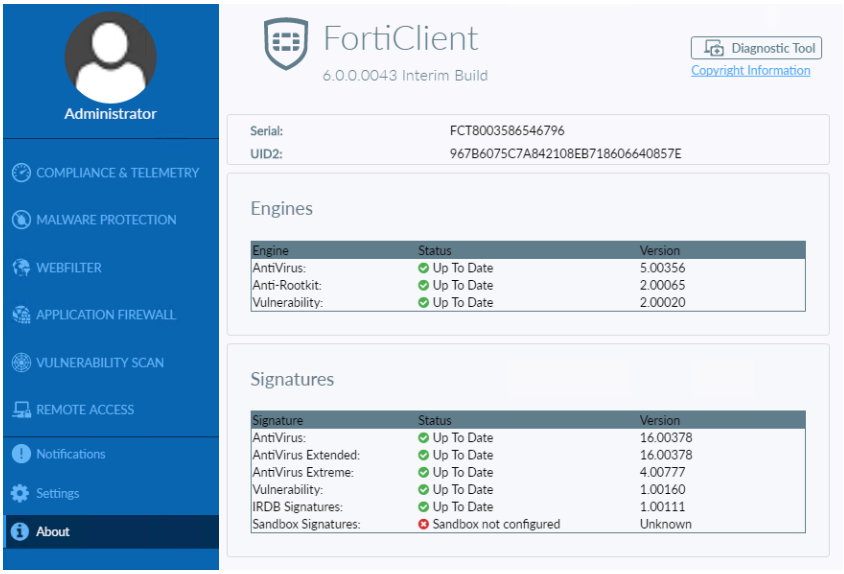
Appendix C - Vulnerability Patches

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

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

To view the list of supported software:

1. In FortiClient, go to *About* to check the Vulnerability signature version number. In the example, the version number is 1.00160.



6.0.0.0043 Interim Build

Serial: FCT8003586546796
UID2: 967B6075C7A842108EB718606640857E

Engines

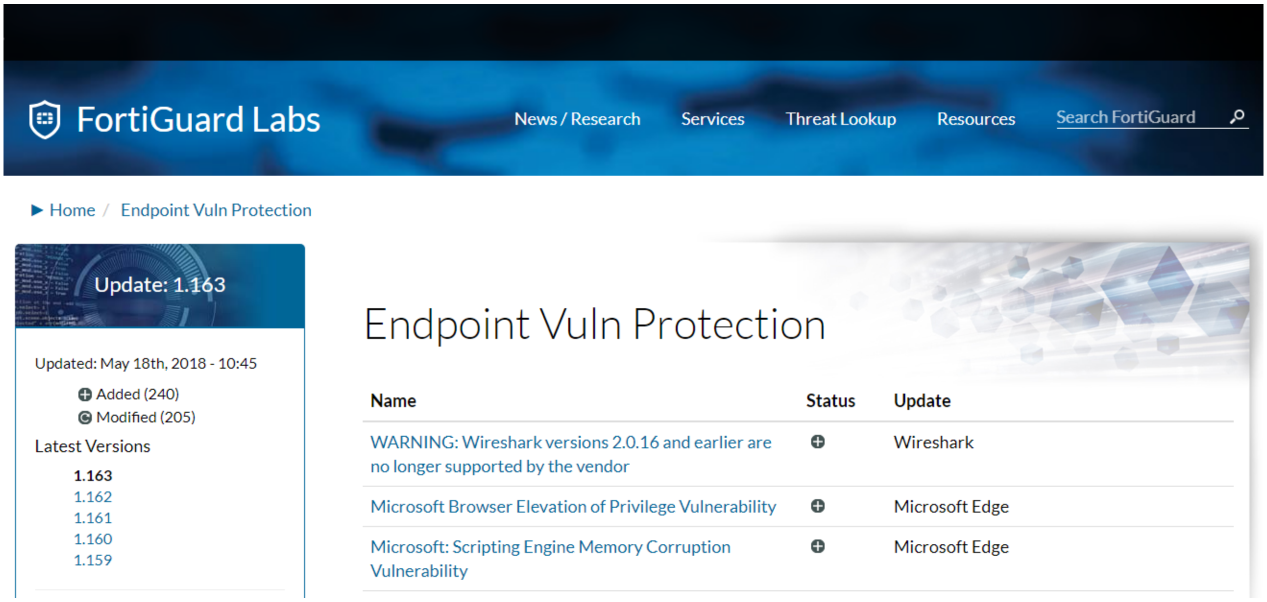
Engine	Status	Version
AntiVirus:	✓ Up To Date	5.00356
Anti-Rootkit:	✓ Up To Date	2.00065
Vulnerability:	✓ Up To Date	2.00020

Signatures

Signature	Status	Version
AntiVirus:	✓ Up To Date	16.00378
AntiVirus Extended:	✓ Up To Date	16.00378
AntiVirus Extreme:	✓ Up To Date	4.00777
Vulnerability:	✓ Up To Date	1.00160
IRDB Signatures:	✓ Up To Date	1.00111
Sandbox Signatures:	✗ Sandbox not configured	Unknown

2. Go to FortiGuard Labs > Endpoint Vulnerabilities.
3. At the bottom of the page, click the desired Vulnerability signature version.

4. The supported software is listed.



Update: 1.163

Updated: May 18th, 2018 - 10:45

- ⊕ Added (240)
- Ⓒ Modified (205)

Latest Versions

- **1.163**
- 1.162
- 1.161
- 1.160
- 1.159

Endpoint Vuln Protection

Name	Status	Update
WARNING: Wireshark versions 2.0.16 and earlier are no longer supported by the vendor	⊕	Wireshark
Microsoft Browser Elevation of Privilege Vulnerability	⊕	Microsoft Edge
Microsoft: Scripting Engine Memory Corruption Vulnerability	⊕	Microsoft Edge

Appendix D - FortiClient Processes

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

FortiClient (Windows) processes

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

Name	Description	Purpose
fcappdb.exe	FortiClient Application Database Service	Network Access Control (NAC) and Antivirus
FortiClient.exe	FortiClient Console	FortiClient GUI
	FortiClient IPsec VPN Service	Remote Access for IPsec VPN
fortifws.exe	FortiClient Firewall Service	Application Firewall
FCDBLog.exe	FortiClient Logging Daemon	Logging
FortiClient_Diagnostic_Tool.exe	FortiClient Diagnostic Tool	Diagnostic Tool
FortiESNAC.exe	FortiClient Network Access Control	FortiClient Telemetry
FortiProxy.exe	FortiClient Proxy Service	Antivirus and Web Filter
fmon.exe	FortiClient Realtime AntiVirus Protection	Antivirus
fcaptmon.exe	FortiClient Sandbox Agent	Sandbox Detection
FortiScand.exe	FortiClient Scan Server	Antivirus to offload Antivirus scanning to a separate process
scheduler.exe	FortiClient Scheduler	Windows ensures FortiClient services are running when needed
FortiSSLVPNdaemon.exe	FortiClient SSLVPN daemon	Remote Access for SSL VPN

Name	Description	Purpose
FCHelper64.exe	FortiClient System Helper	FortiClient ensures 32-bit processes can access 64-bit resources
FortiTray.exe	FortiClient System Tray Controller	FortiTray
	FortiClient User Avatar Agent	Used by FortiClient Console and FortiClient Telemetry to obtain avatar images for users
	FortiClient Virus Feedback Service	Antivirus and FortiClient Console use to submit samples to FortiGuard
	FortiClient Vulnerability Scan Daemon and Engine	FortiClient Vulnerability Scan engine
FortiWF.exe	FortiClient Web Filter Service	Used by Web Filter

FortiClient (OS X) processes

FortiClient (OS X) uses the following processes:

- The process for 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 (OS X):

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

Name	Purpose
fctservctl	FortiClient Service Controller
epctrl	FortiClient endpoint control daemon
ftgdagent	Web Filter
fmon	AntiVirus scan main program
scanunit	AntiVirus scan scanner
vulscan	Vulnerability scan

Name	Purpose
fctappfw	Firewall Service
fssoavgent_launchagent	FortiClient single sign on agent
fssoavgent_launchdaemon	FortiClient single sign on daemon
fctctld	VPN controller
sslvpnd	SSL VPN Daemon
racoon	IPsec VPN Service
racoonctl	IPsec VPN Controller
fctupdate	FortiClient update tool
fctupgrade	FortiClient upgrade tool
fcconfig	FortiClient Configurator tool