FORTINET

# FortiClient - Compliance Guide

Version 6.0

**FORTINET DOCUMENT LIBRARY**
http://docs.fortinet.com

**FORTINET VIDEO GUIDE**
http://video.fortinet.com

**FORTINET BLOG**
https://blog.fortinet.com

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

**FORTIGATE COOKBOOK**
http://cookbook.fortinet.com

**FORTINET TRAINING SERVICES**
http://www.fortinet.com/training

**FORTIGUARD CENTER**
http://www.fortiguard.com

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

**FEEDBACK**
Email: techdocs@fortinet.com

May 31, 2018
FortiClient 6.0 Compliance Guide
04-600-478178-20180531

# TABLE OF CONTENTS

# Change Log

| Date | Change Description |
|---|---|
| 2018-05-31 | Initial release |
| | |
| | |
| | |

# Introduction

This document clarifies compliance when using FortiClient in the following configurations:

- FortiClient with FortiGate and EMS on page 6
- FortiClient with FortiGate on page 7

The document also describes the following scenario, which does not support compliance:

- FortiClient with EMS on page 9

## Terminology

The following clarifies the terminology used in this document.

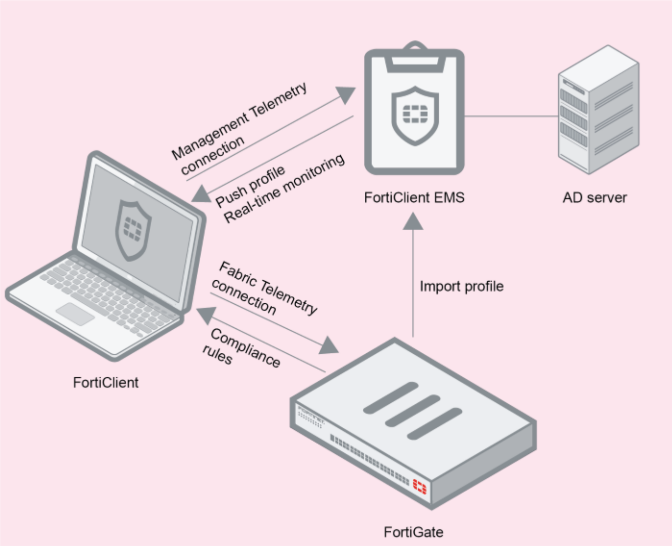
| Term | Definition |
|---|---|
| Managed mode | FortiClient used with FortiGate or EMS. |
| Integrated mode | FortiClient used with FortiGate and EMS. In this scenario, FortiClient connects FortiClient Telemetry to FortiOS and EMS. |
| Fabric Telemetry connection | Connection between FortiClient and FortiOS when FortiClient is used with FortiGate. |
| Management Telemetry connection | Connection between FortiClient and EMS when FortiClient is used with EMS. |
| 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.<br>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.<br>In EMS, administrators configure an *endpoint profile*. This profile defines the configuration for FortiClient software on endpoints.<br>Unless referring specifically to a profile created using FortiOS or EMS, this guide uses the term profile when referring to either a FortiClient Profile or an endpoint profile received by FortiClient. |

# Deployment Options

This section describes the following deployment options: FortiClient with FortiGate and EMS, FortiClient with FortiGate, and FortiClient with EMS. The first two options support compliance. The third option does not support compliance and only allows central management of endpoints through EMS.

## FortiClient with FortiGate and EMS

In this scenario, FortiClient establishes two FortiClient Telemetry connections: to FortiGate and to EMS. EMS pushes configuration information in an endpoint profile to FortiClient, while FortiOS provides compliance rules.



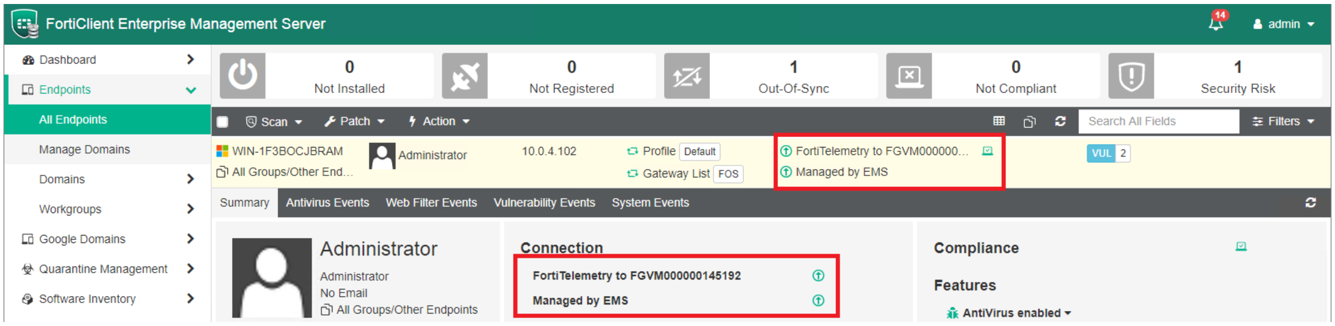
FortiClient follows the endpoint profile configuration received from EMS. FortiClient settings are locked so the endpoint user cannot change any configuration. EMS is expected to provide a profile that configures FortiClient to be compliant with rules received from FortiOS. If any configuration is not compliant, it must be fixed in EMS.

EMS can also import a FortiClient Profile from FortiOS and then push the profile to FortiClient.

In FortiClient Console, if allowed by the configuration, FortiClient can be disconnected from FortiOS. Only EMS can control the connection between FortiClient and EMS. Disconnecting FortiClient from EMS can only be done in EMS.

FortiClient installers created in EMS are embedded with the EMS server's IP address. This allows the endpoint to connect FortiClient Telemetry to the specified EMS server. The connection between FortiClient and EMS is a management Telemetry connection using a gateway IP list.

The following shows the EMS GUI in this scenario.



FortiClient Enterprise Management Server

14 admin

Dashboard
Endpoints
All Endpoints
Manage Domains
Domains
Workgroups
Google Domains
Quarantine Management
Software Inventory

| 0 | 0 | 1 | 0 | 1 |
|---|---|---|---|---|
| Not Installed | Not Registered | Out-Of-Sync | Not Compliant | Security Risk |

Scan ▾ Patch ▾ Action ▾ Search All Fields Filters ▾

WIN-1F3BOCJBRAM Administrator 10.0.4.102 Profile Default FortiTelemetry to FGVM000000... VUL 2
All Groups/Other End... Gateway List FOS Managed by EMS

Summary Antivirus Events Web Filter Events Vulnerability Events System Events

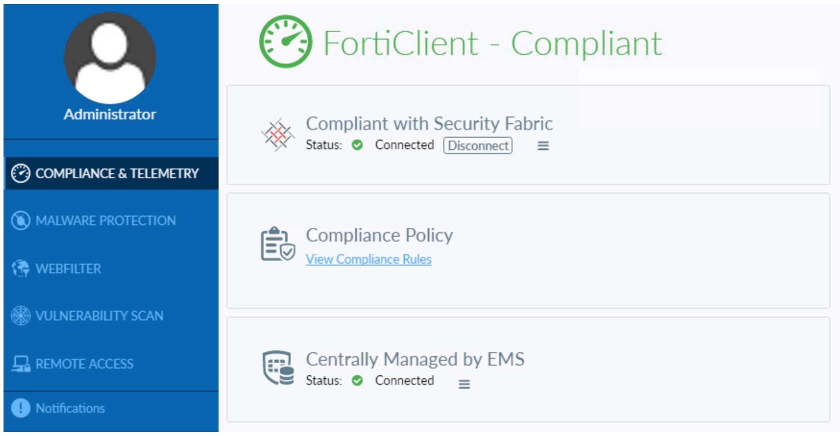
Administrator
Administrator
No Email
All Groups/Other Endpoints

Connection
FortiTelemetry to FGVM000000145192
Managed by EMS

Compliance

Features
AntiVirus enabled ▾

The following show the FortiClient 6.0 *Compliance & Telemetry* tab in this scenario when FortiClient is compliant with the compliance rules from FortiGate.



Administrator

COMPLIANCE & TELEMETRY
MALWARE PROTECTION
WEBFILTER
VULNERABILITY SCAN
REMOTE ACCESS
Notifications

FortiClient - Compliant

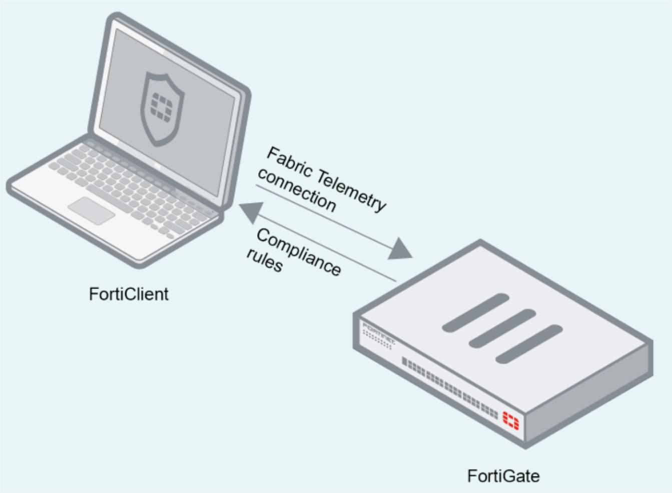
Compliant with Security Fabric
Status: Connected Disconnect

Compliance Policy
View Compliance Rules

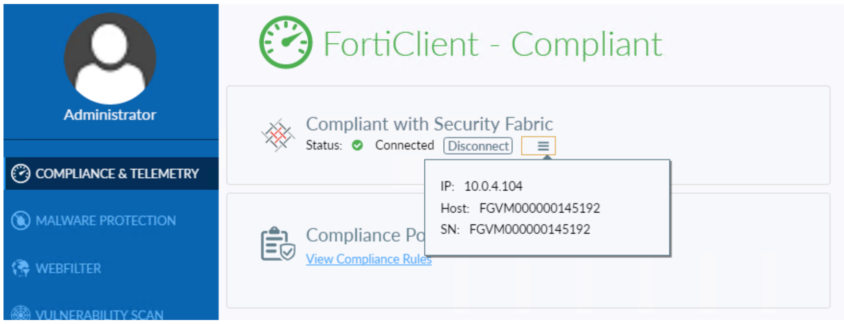
Centrally Managed by EMS
Status: Connected

## FortiClient with FortiGate

In this scenario, FortiClient connects FortiClient Telemetry to FortiGate and compliance is supported. There is no connection to EMS.



The following shows an example of the *Compliance & Telemetry* tab after FortiClient has connected FortiClient Telemetry to a FortiGate that has 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

FortiOS sends a FortiClient Profile to FortiClient. The FortiClient Profile includes compliance rules and some minimal configuration required to resolve non-compliance issues. The FortiClient Profile includes all compliance rules, whether enabled or disabled. FortiClient ignores disabled rules as they do not affect endpoint compliance.

You cannot configure FortiClient using FortiGate. To configure FortiClient, use EMS.

After receiving the FortiClient Profile, FortiClient compares its configuration with the compliance rules and reports to FortiOS which rules it is compliant with and which rules it is not compliant with. If the endpoint is not compliant, the following occurs.

- FortiOS blocks any endpoint where FortiClient is not installed or not connected to FortiOS. When FortiClient goes offline, it shows the compliance state, but the endpoint cannot access the Internet since FortiClient Telemetry is no longer connected.
- If FortiClient is not compliant due to configuration issues, the user can change any configuration to make the endpoint compliant. If allowed by configuration, FortiClient can also be disconnected from FortiOS.

# FortiGate compliance rules

When FortiClient is connected to FortiGate, FortiGate provides network security by defining compliance rules for FortiClient endpoints. 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

Depending on the FortiOS configuration, FortiOS uses one of the following methods to determine endpoint compliance. The first option is only available in FortiOS 6.0.0 and later versions. In both cases, FortiClient must be installed on the endpoint and there must be a Fabric Telemetry connection between FortiClient and FortiGate.

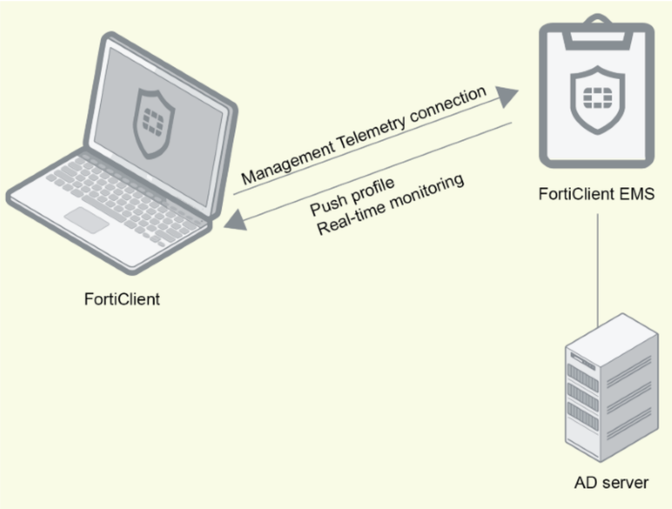
1. An endpoint is considered compliant if it FortiClient is managed by the EMS server authorized in FortiOS.
2. An endpoint is considered compliant if it complies with the specific compliance rules configured in FortiOS. The following list shows a sample of the compliance rules administrators can enable 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
  - Processes running on client
- Security posture check:
  - Realtime protection
  - Third party Antivirus on Windows
  - Web filter
  - Application firewall

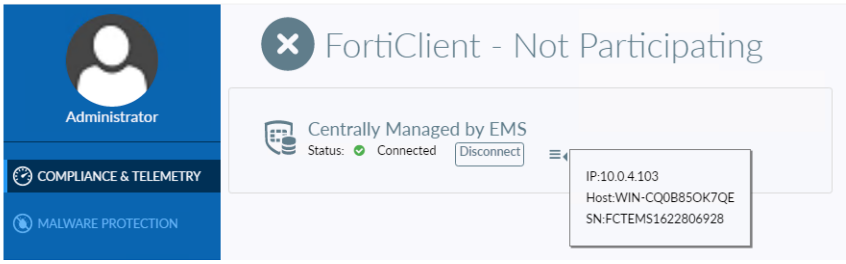
For information on configuring FortiGate compliance rules, see the *FortiOS Handbook - Security Profiles*.

## FortiClient with 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.



The following images show the FortiClient *Compliance & Telemetry* tab and the EMS GUI in this scenario.

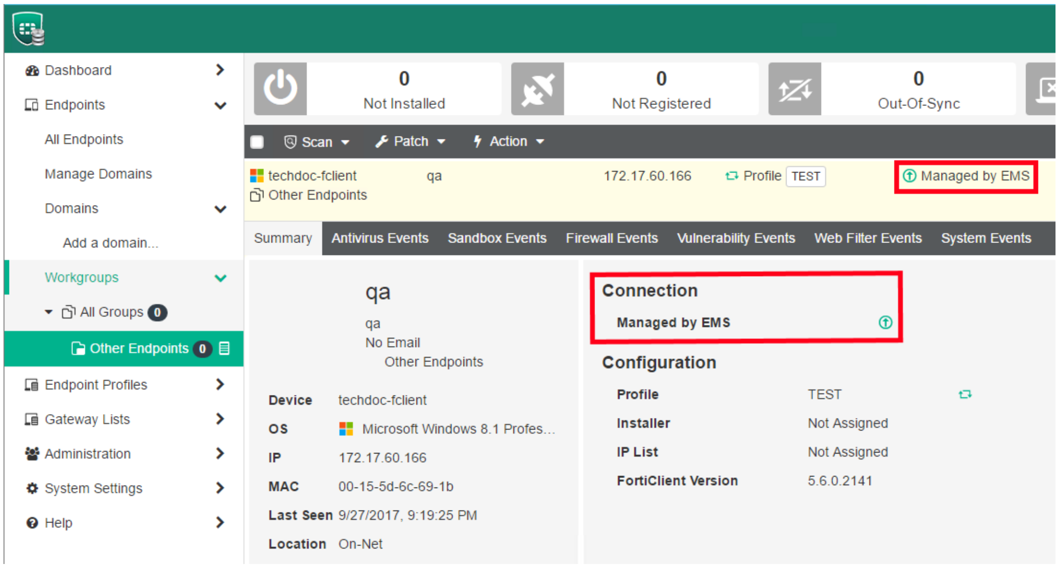


FortiClient - Not Participating

Centrally Managed by EMS

Status: Connected

IP:10.0.4.103
Host:WIN-CQ0B85OK7QE
SN:FCTEMS1622806928



techdoc-fclient qa 172.17.60.166 Profile TEST Managed by EMS
Other Endpoints

qa

qa
No Email
Other Endpoints

| | |
|---|---|
| Device | techdoc-fclient |
| OS | Microsoft Windows 8.1 Profes... |
| IP | 172.17.60.166 |
| MAC | 00-15-5d-6c-69-1b |
| Last Seen | 9/27/2017, 9:19:25 PM |
| Location | On-Net |

Connection

Managed by EMS

Configuration

| | |
|---|---|
| Profile | TEST |
| Installer | Not Assigned |
| IP List | Not Assigned |
| FortiClient Version | 5.6.0.2141 |

# How FortiClient Telemetry Connects to IP Addresses

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

- Manual entering of the gateway IP address, which means that the endpoint user enters the gateway IP address of FortiGate or EMS into FortiClient Console.
- 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 will attempt to connect to the first reachable FortiGate in the list, starting from the top. The order of the list is maintained as it was 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 device. The default gateway IP address of the endpoint device 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.

## Silent registration

When silent registration is enabled, FortiClient connects and reconnects Telemetry to FortiOS or EMS without any user interaction. FortiClient does not notify the user about the connection, and the user is not required to confirm the connection.

By default, silent registration is enabled in endpoint profiles in EMS. If desired, you can disable silent registration in EMS.

# Reregistration

The EMS administrator can assign a gateway IP list to endpoints. Receiving the gateway IP list triggers FortiClient to connect to a server using the order above, even if FortiClient Telemetry is already connected to FortiOS or EMS.