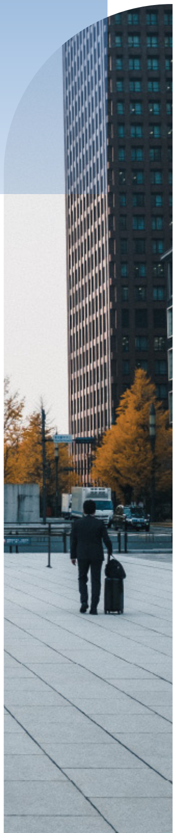
DEPLOYMENT GUIDE

Fortinet FortiClient and Symantec Endpoint Protection



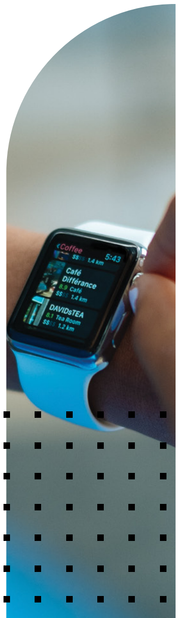


Table of Contents

Overview

This document is a deployment guide that explains the installation and configuration steps to install the FortiClient Security Fabric agent and Symantec Endpoint Protection (SEP) on a corporate endpoint device protected by a FortiGate appliance.

This integration allows customers who have Symantec Endpoint Protection in their environment to leverage the Fortinet Security Fabric with the FortiClient's capability to enforce network compliance with the FortiGate. Compliance rules are defined by the administration into a FortiGate Security Profile. It contains the requirements the endpoint must satisfy prior to accessing the network. By forcing endpoints to match the security profile, the FortiGate and FortiClient help to reduce the attack surface vector. In addition, the FortiClient Security Fabric agent will feed the FortiGate with telemetry data, enabling the automatic updates to the Security Fabric and providing comprehensive visibility of the endpoints.

These actions are complemented by Symantec Endpoint Protection, which blocks virus, malware, and other threats from infecting the endpoints.

The joint solution combines Symantec's enhanced endpoint protection platform with Fortinet's best-in-class network security platform, to deliver unparalleled protection and security without compromises for your entire deployment.

This guide will focus on the required components, the architectural overview, and the configurations on the FortiClient and Symantec Endpoint Protection. This guide also assumes an environment of FortiGate with FortiOS v5.6, FortiClient v5.6, and Symantec Endpoint Protection 14 MP2 (14.0.2415.0200) running on either Windows 7, 8, or 10 with Symantec Endpoint Protection Manager.

Deployment Prerequisites

1. FortiGate—on FortiOS v5.6+
2. FortiClient v5.6
3. Symantec Endpoint Protection Manager
4. Symantec Endpoint Protection Client
5. Optional
    - FortiClient EMS

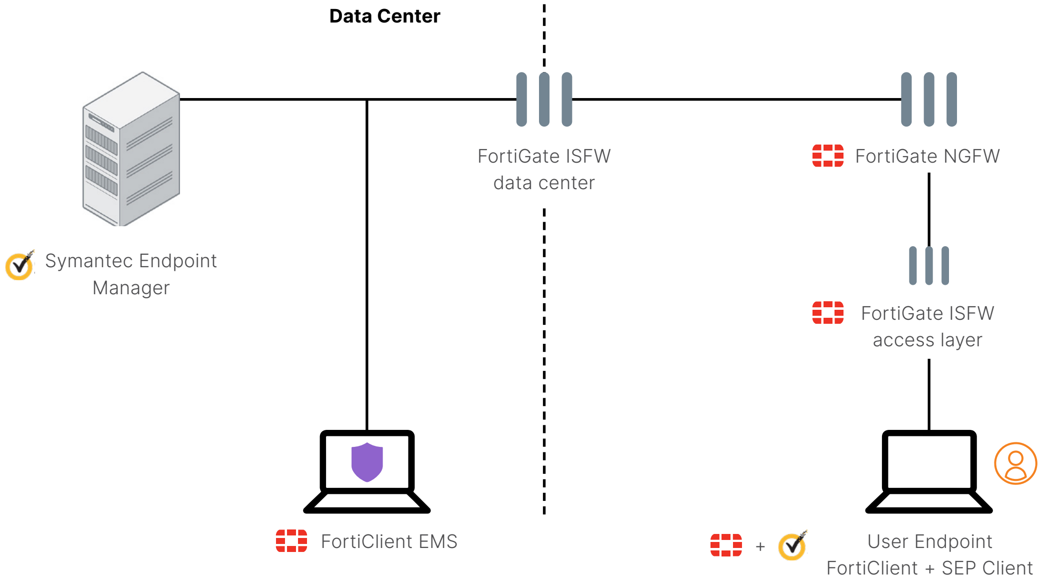
For licenses to Symantec Endpoint Protection, please contact Symantec's respective sales team.

FORTINET FABRIC-READY

NOTE: This guide is pertinent to the integration between the relevant portions of the FortiGate, the FortiClient, and Symantec Endpoint Protection Client only. For integration details on the Symantec Endpoint Protection Manager and further administration of the FortiGate, please refer to the relevant guides linked in the References section of this guide.

Architecture Overview

This is a simple topology of what an enterprise network may look like with Symantec Endpoint Protection and the FortiClient, where the Symantec Endpoint Protection Manager is located in the data center and the endpoints are located behind an Access Layer FortiGate ISFW, with the FortiGate NGFW at the core of the network.



The FortiClient Security Fabric agent registers on the FortiGate and gets the FortiClient Security Profile in order to perform its compliance checks. It sends regular keep-alive messages including telemetry information aiming to feed the Security Fabric computed by the FortiGate.

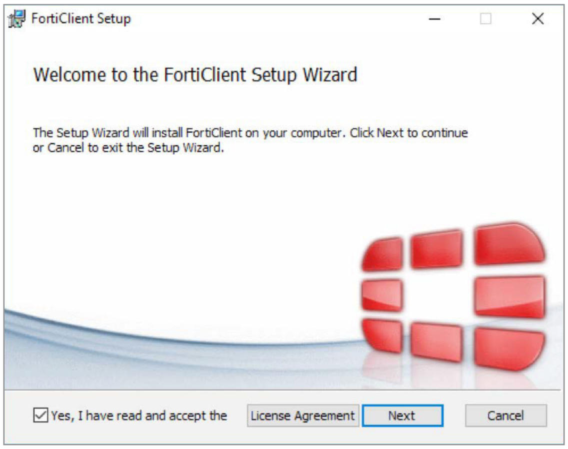
The Symantec Endpoint Protection Client is connected to the Symantec Endpoint Protection Manager, which administers the client with profiles and signature updates and receives reports on the client's malware, viruses, and other threat activity.

Note: The order of installation of either the FortiClient or Symantec Endpoint Protection does not matter. The joint solution works if either of the solutions is preinstalled on the endpoint.

FortiClient Installation

The latest version of FortiClient for Windows is available for download on http://www.forticlient.com/.

1. Download and run the FortiClient Installer.
2. In the initial Welcome window, select "**Yes, I have read and accept the License Agreement**," then click **Next**.

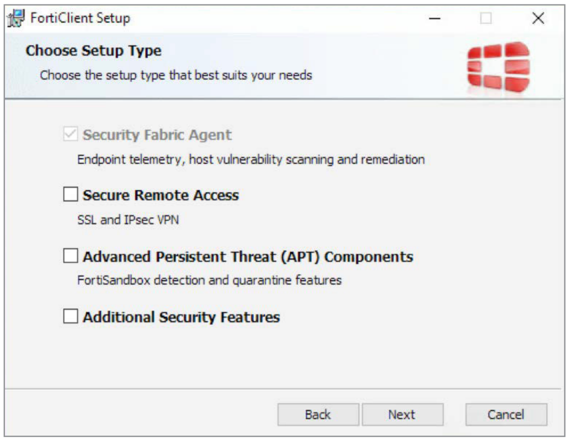


Welcome to the FortiClient Setup Wizard

The Setup Wizard will install FortiClient on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

☑ Yes, I have read and accept the License Agreement

3. Next, uncheck the "**Secure Remote Access**" option and click **Next**.



Choose Setup Type

Choose the setup type that best suits your needs

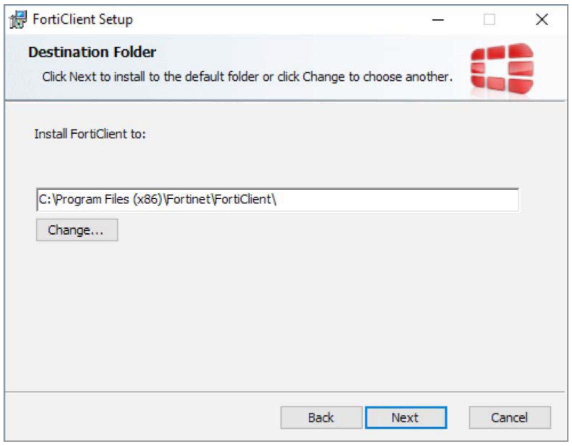
☑ Security Fabric Agent
Endpoint telemetry, host vulnerability scanning and remediation

☐ Secure Remote Access
SSL and IPsec VPN

☐ Advanced Persistent Threat (APT) Components
FortiSandbox detection and quarantine features

☐ Additional Security Features

4. In the "**Destination Folder**" window, click **Next**.



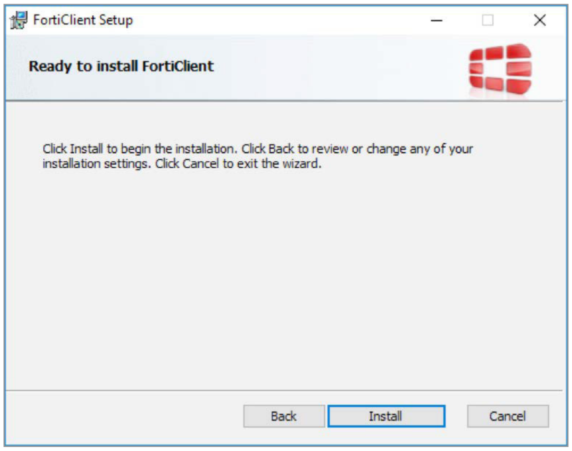
Destination Folder

Click Next to install to the default folder or click Change to choose another.

Install FortiClient to:

C:\Program Files (x86)\Fortinet\FortiClient\

5. In the “**Ready to install FortiClient**” window, click **Install**.



Ready to install FortiClient

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

6. In the “**Completed the FortiClient Setup Wizard**,” click **Finish**.

FortiGate Configuration

Enforce Endpoint Telemetry and Compliance

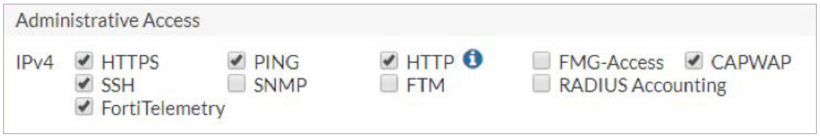
The FortiGate needs the following functionalities enabled in order to enforce compliance checking and gaining devices visibility in order to populate the Security Fabric:

- Telemetry Service
  - FortiClient On-net status
  - Device Detection
  - FortiClient Compliance Check Enforcement

1. Go to **Network** > **Interfaces**.

2. Edit the interface connected to the LAN network.

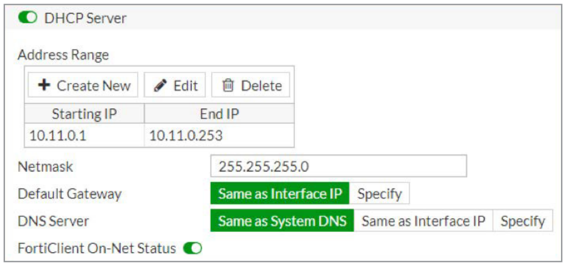
3. In the section **Administrative Access**, enable **FortiTelemetry**.



Administrative Access

IPv4 ☑ HTTPS ☑ PING ☑ HTTP ℹ ☐ FMG-Access ☑ CAPWAP
☑ SSH ☐ SNMP ☐ FTM ☐ RADIUS Accounting
☑ FortiTelemetry

4. Enable **DHCP Server**.
   - Define an **Address Range**.


DHCP Server

Address Range

Starting IP	End IP
10.11.0.1	10.11.0.253

Netmask: 255.255.255.0

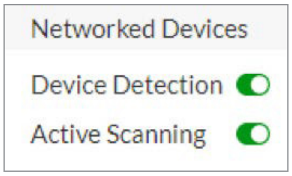
Default Gateway: Same as Interface IP | Specify

DNS Server: Same as System DNS | Same as Interface IP | Specify

FortiClient On-Net Status

   - Enable **FortiClient On-Net Status**.

5. In the section **Networked Devices**, enable **Device Detection** and **Active Scanning**.


Networked Devices

Device Detection

Active Scanning

6. In the section **Admission Control**, enable **Enforce FortiClient Compliant Check**.

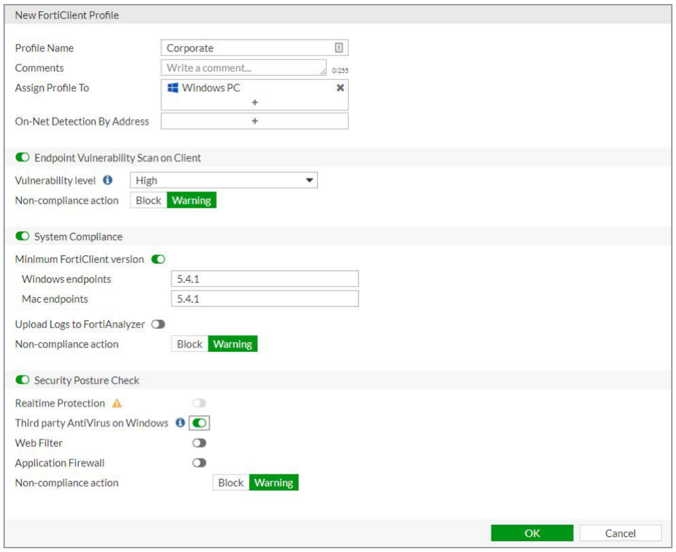
7. Click **OK**.

FortiClient Security Profile Definition

The FortiClient Security Profile contains the compliance rules the endpoint must satisfy prior to being granted access on the network.

1. Go to **Security Profiles** > **FortiClient Profiles**.
2. Create a new profile with the parameters listed in the table below.
3. Click **OK**.

Profile Name	Corporate
Assign Profile To	Windows PC
On-Net Detection By Address	Disabled
Endpoint Vulnerability Scan on Client	
Vulnerability level	High
Non-compliance action	Warning
System Compliance	
Minimum FortiClient version	Enabled
Windows endpoints	5.4.1
Mac endpoints	5.4.1
Upload Logs to FortiAnalyzer	Disabled
Non-compliance action	Warning
Security Posture Check	
Realtime Protection	Disabled
Third party AntiVirus on Windows	Enabled
Web Filter	Disabled
Application Firewall	Disabled
Non-compliance action	Warning


New FortiClient Profile

Profile Name: Corporate

Comments: Write a comment... 0/255

Assign Profile To: Windows PC

On-Net Detection By Address

Endpoint Vulnerability Scan on Client

Vulnerability level: High

Non-compliance action: Block | Warning

System Compliance

Minimum FortiClient version

Windows endpoints: 5.4.1

Mac endpoints: 5.4.1

Upload Logs to FortiAnalyzer

Non-compliance action: Block | Warning

Security Posture Check

Realtime Protection

Third party AntiVirus on Windows

Web Filter

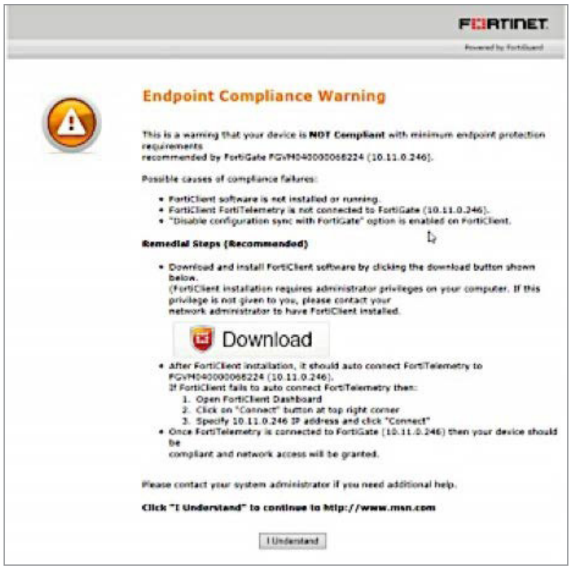
Application Firewall

Non-compliance action: Block | Warning

Check the FortiClient Security Fabric Agent

The FortiGate is configured to enforce the FortiClient compliance check. As such, it prevents connected devices, which are not registered, to access the internet.

Users who attempt to navigate the internet will be presented with a warning page in their browser.



Endpoint Compliance Warning

This is a warning that your device is **NOT Compliant** with minimum endpoint protection requirements
recommended by FortiGate FGVM040000068224 (10.11.0.246).

Possible causes of compliance failures:

- FortiClient software is not installed or running.
- FortiClient FortiTelemetry is not connected to FortiGate (10.11.0.246).
- "Disable configuration sync with FortiGate" option is enabled on FortiClient.

Remedial Steps (Recommended)

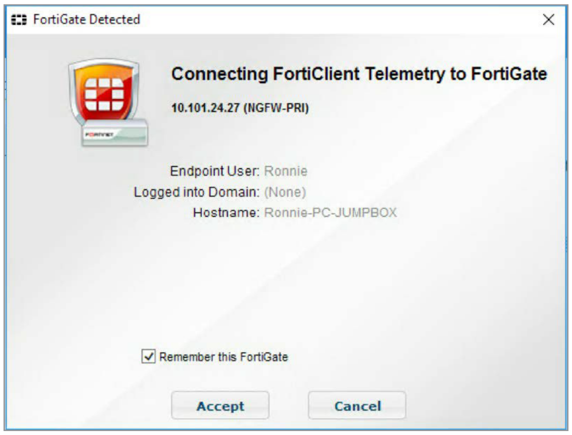
- Download and install FortiClient software by clicking the download button shown below.
  (FortiClient installation requires administrator privileges on your computer. If this privilege is not given to you, please contact your
  network administrator to have FortiClient installed.

- After FortiClient installation, it should auto connect FortiTelemetry to FGVM040000068224 (10.11.0.246).
  If FortiClient fails to auto connect FortiTelemetry then:
  1. Open FortiClient Dashboard
  2. Click on "Connect" button at top right corner
  3. Specify 10.11.0.246 IP address and click "Connect"
- Once FortiTelemetry is connected to FortiGate (10.11.0.246) 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://www.msn.com

The FortiGate sends FortiTelemetry probes on the LAN network on a regular basis. Once the FortiClient is started, it detects these probes and displays a registration pop-up the user has to accept in order to register.



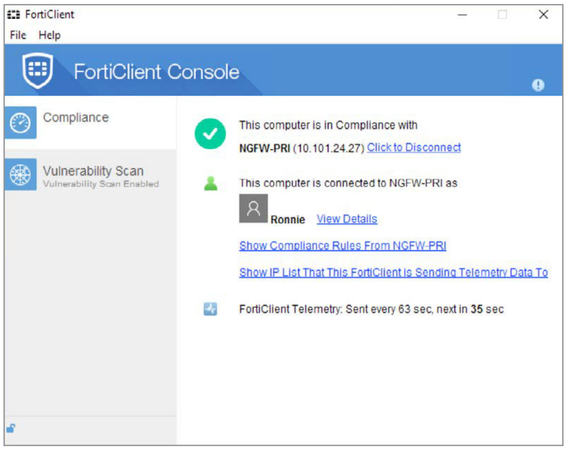
Connecting FortiClient Telemetry to FortiGate

10.101.24.27 (NGFW-PRI)

Endpoint User: Ronnie
Logged into Domain: (None)
Hostname: Ronnie-PC-JUMPBOX

☑ Remember this FortiGate

Once registered, the FortiGate sends the FortiClient Security profiles that have been defined. The FortiClient performs the required checks and transmits the result to the FortiGate, which decides whether or not the device is compliant.



This computer is in Compliance with

NGFW-PRI (10.101.24.27) Click to Disconnect

This computer is connected to NGFW-PRI as

Ronnie View Details

Show Compliance Rules From NGFW-PRI

Show IP List That This FortiClient is Sending Telemetry Data To

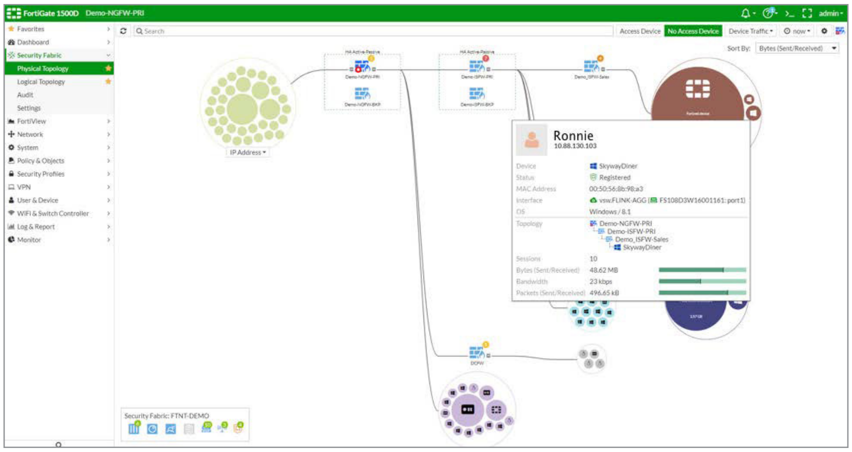
FortiClient Telemetry: Sent every 63 sec, next in 35 sec

Open FortiClient Console and go the Compliance tab in order to check your compliance status. A compliant registered endpoint should display in this window.

FortiGate FortiView drill-down pages are useful to view the relevant information in the Security Fabric. For instance, the logical view gives the detected topology and a mouse over one of the detected devices gives you the elements collected by the FortiGate.

In the following screenshot, the detail for our endpoint is displayed. We can review some information like the user name, avatar, IP address, and MAC address, etc. This will also display other important statistics about the client such as vulnerabilities discovered, malware quarantined, etc.

From here it is possible to drill down. For instance, you can right-click and access the details of the detected vulnerabilities.



Ronnie
10.88.130.103

Device SkywayDiner
Status Registered
MAC Address 00:50:56:8b:98:a3
Interface vsw.FLINK-AGG (FS108D3W16001161: port1)
OS Windows / 8.1
Topology Demo-NGFW-PRI
Demo-ISFW-PRI
Demo_ISFW-Sales
SkywayDiner
Sessions 10
Bytes (Sent/Received) 48.62 MB
Bandwidth 23 kbps
Packets (Sent/Received) 496.65 kB

Symantec's Installation and References

For instructions on the installation and configuration of Symantec Endpoint Protection 14 MP2, please refer to Symantec's guides:

System requirements for Endpoint Protection 14 MP1 and MP2

Best practices for Symantec Endpoint Protection

SEPM 14.0 Fresh install with SQL database - graphical overview

SEPM 14.0 Fresh install with Embedded database - graphical overview

Symantec™ Endpoint Protection 14 Installation and Administration Guide

Symantec™ Endpoint Protection 14 Windows Client Guide

References

How to get help:

FortiGate/FortiOS Administration Guides:
http://docs.fortinet.com/fortigate/admin-guides

FortiClient Administration Guides:

http://help.fortinet.com/fclient/olh/5-6-0/index.htm

http://docs.fortinet.com/d/forticlient-5.6.0-admin-guide

Fuse—FortiClient and Enterprise Management Server (EMS)

https://fuse.fortinet.com/p/fo/si/topic=476

www.fortinet.com

June 10, 2021 2:46 AM
116395-B-0-EN