DEPLOYMENT GUIDE

Fortinet FortiClient and Symantec Endpoint Protection
Fortinet FortiClient and Symantec Endpoint Protection

Overview ................................................................. 3
Deployment Prerequisites ................................. 3
Architecture Overview ............................................. 3
FortiClient Installation ........................................... 4
FortiGate Configuration .......................................... 5
Enforce Endpoint Telemetry and Compliance ............... 5
FortiClient Security Profile Definition ......................... 6
Check the FortiClient Security Fabric Agent .................. 7
Symantec’s Installation and References ...................... 8
References ................................................................. 8
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.

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.

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.
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**


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**.

3. Next, uncheck the “Secure Remote Access” option and click **Next**.
4. In the “Destination Folder” window, click **Next**.

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

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

   ![DHCP Server](image)

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

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

   ![Networked Devices](image)

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**.

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

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.

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.
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.

![Screenshot of FortiGate FortiView drill-down pages](image)

### Symantec’s Installation and References

For instructions on the installation and configuration of Symantec Endpoint Protection 14 MP1 and 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**
  [http://www.symantec.com/docs/DOC9449](http://www.symantec.com/docs/DOC9449)

- **Symantec™ Endpoint Protection 14 Windows Client Guide**

### References

How to get help:

- **FortiGate/FortiOS Administration Guides:**
  [http://docs.fortinet.com/fortigate/admin-guides](http://docs.fortinet.com/fortigate/admin-guides)

- **FortiClient Administration Guides:**
  [http://help.fortinet.com/fclient/olh/5-6-0/index.htm](http://help.fortinet.com/fclient/olh/5-6-0/index.htm)
  [http://docs.fortinet.com/d/forticlient-5.6.0-admin-guide](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](https://fuse.fortinet.com/p/fo/si/topic=476)