DEPLOYMENT GUIDE

Fortinet and SentinelOne

Fortinet and SentinelOne

Overview

This document explains the installation and configuration steps required to install FortiClient Security Fabric agent and SentinelOne agent on a corporate endpoint device protected by a FortiGate appliance.

FortiGate is responsible for enforcing network compliance before allowing endpoints to connect to the network. Compliance rules are defined by the administration into a FortiGate Security Profiles. It contains the requirements the endpoint must satisfy prior to access the network. By forcing endpoints to match the security profile, FortiGate and FortiClient help to reduce the attack surface vector. In addition, FortiClient Security Fabric agent will feed FortiGate with telemetry data, enabling the automatic updates to the Security Fabric and providing comprehensive visibity of the endpoints.

These actions are complemented by the SentinelOne agent which employs dynamic behavior tracking and autonomous monitoring to keep the endpoint ahead of any advanced threat in real-time.

The joint solution combines SentinelOne's next generation total endpoint protection platform with Fortinet's best-in-class network security platform, to deliver unparalleled protection and security without compromise for your entire deployment.

Deployment Prerequisites

1. FortiGate appliance running FortiOS v5.6.0
2. FortiClient Software version 5.6.0 beta3
3. Credentials for accessing the SentinelOne cloud-based management portal from which will be downloaded SentineOne Agent v1.8.4. URL of the portal is in the form https://<customer>.sentinelone.net/

FORTINET
Fabric-Ready

Architecture Overview

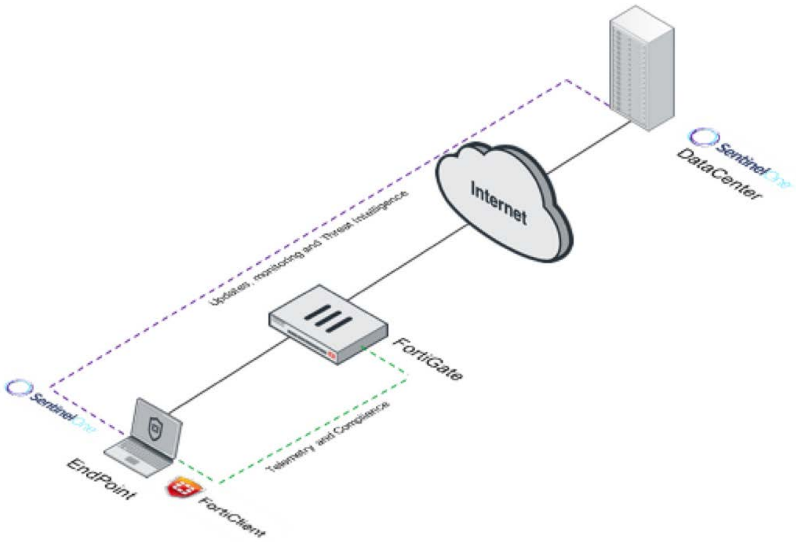


Figure 1: This topology shows the interactions of the two agents.

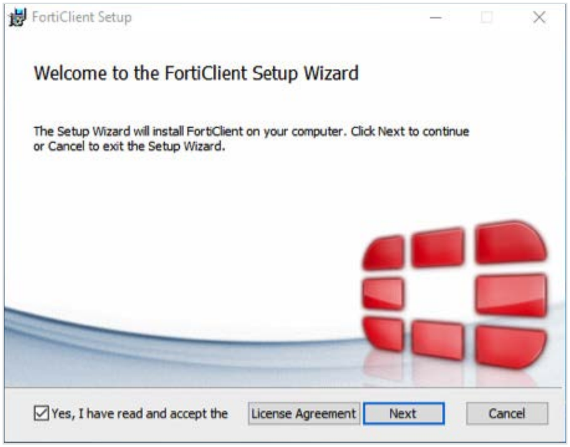
FortiClient Security Fabric agent registers on FortiGate and gets the FortiClient Security Profile in order to perform its compliance checks. It sends regular keep alive messages including telemetry information aiming to feed the Security Fabric computed by FortiGate.

SentinelOne agent connects to a dedicated server in the cloud from which it leverages cloud intelligence and machine learning to seamlessly adapt endpoint defenses against the latest malware, exploits and attacks.

FortiClient Installation

1. Download and run the FortiClient installer.

2. In window **Welcome to the FortiClient Setup Wizard,** check **Yes, I have read and accept the License Agreement,** click **Next.**



FortiClient Setup

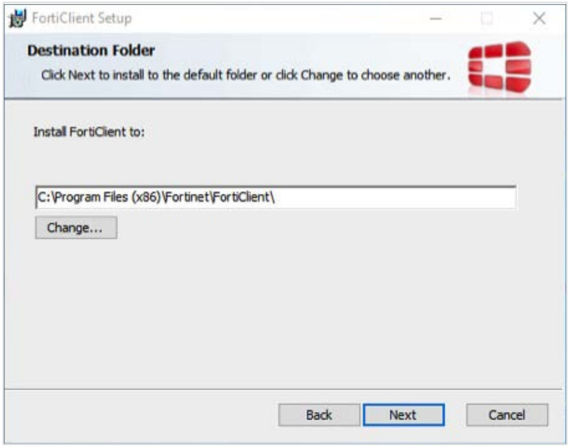
Welcome to the FortiClient Setup Wizard

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. In window **Choose Setup Type,** uncheck **Secure Remote Access,** then click **Next.**

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



FortiClient Setup

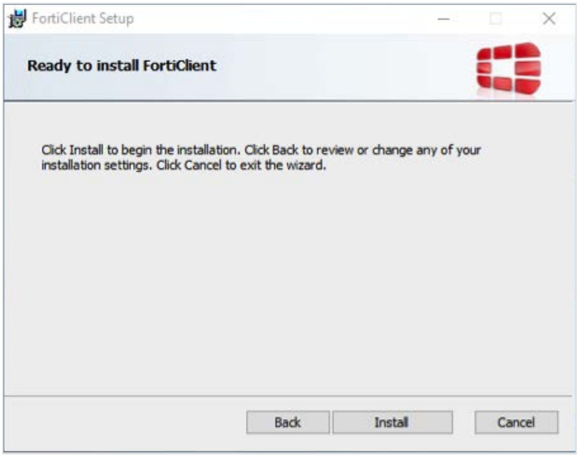
Destination Folder

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 window **Ready to install FortiClient,** click **Install.**

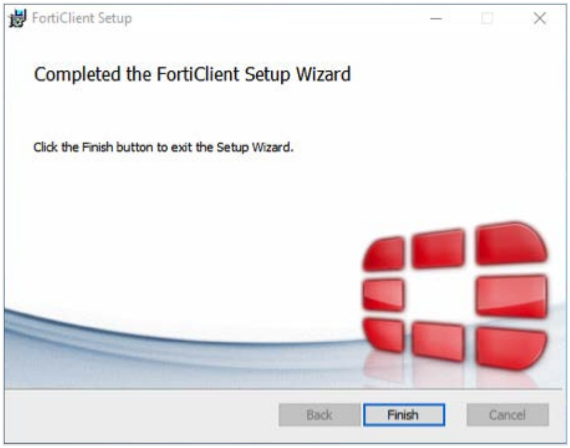


FortiClient Setup

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 window **Completed the FortiClient Setup Wizard,** click **Finish.**



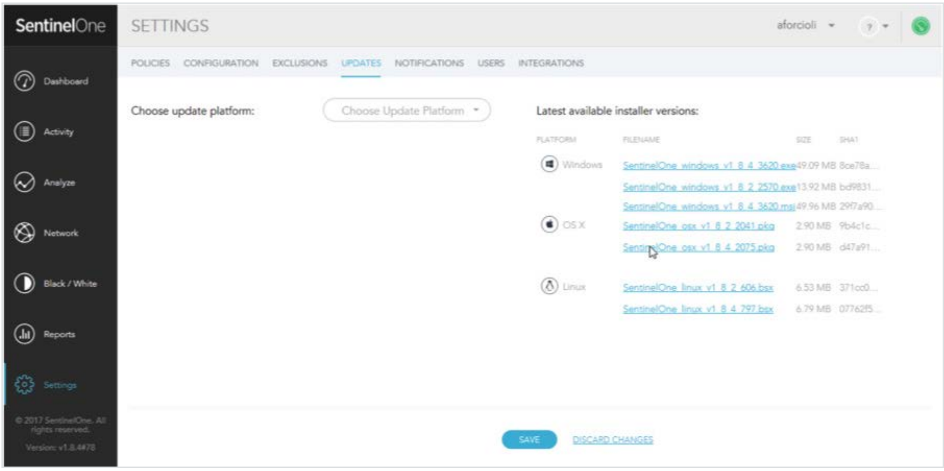
Completed the FortiClient Setup Wizard

Click the Finish button to exit the Setup Wizard.

SentinelOne Installation

Download the SentinelOne Agent Installer

1. Go to your SentinelOne cloud-based management portal.
2. Sign-in using your credentials.
3. Go to **Settings.**
4. Select tab **UPDATES.**
5. Download the SentinelOne Installer on your endpoint.



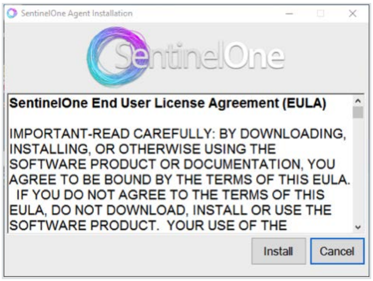
Choose update platform:

Latest available installer versions:

PLATFORM	FILENAME	SIZE	SHA1
Windows	SentinelOne_windows_v1_8_4_3620.exe	49.09 MB	8ce78a...
	SentinelOne_windows_v1_8_2_2570.exe	13.92 MB	bd9831...
	SentinelOne_windows_v1_8_4_3620.msi	49.96 MB	29f7a90...
OS X	SentinelOne_osx_v1_8_2_2041.pkg	2.90 MB	9b4c1c...
	SentinelOne_osx_v1_8_4_2075.pkg	2.90 MB	d47a91...
Linux	SentinelOne_linux_v1_8_2_606.bsx	6.53 MB	371cc0...
	SentinelOne_linux_v1_8_4_797.bsx	6.79 MB	077625...

Install the SentinelOne Agent

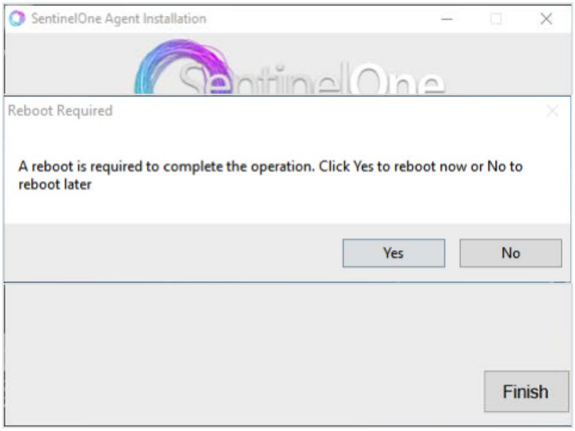
1. Run the SentinelOne installer.
2. Click **Install.**



SentinelOne End User License Agreement (EULA)

IMPORTANT-READ CAREFULLY: BY DOWNLOADING, INSTALLING, OR OTHERWISE USING THE SOFTWARE PRODUCT OR DOCUMENTATION, YOU AGREE TO BE BOUND BY THE TERMS OF THIS EULA. IF YOU DO NOT AGREE TO THE TERMS OF THIS EULA, DO NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE PRODUCT. YOUR USE OF THE

3. Click **Finish.**



SentinelOne Agent Installation

Reboot Required

A reboot is required to complete the operation. Click Yes to reboot now or No to reboot later

4. Click **Yes** in window **Reboot Required.**

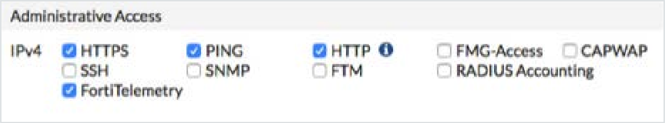
FortiGate Configuration

Enforce Endpoint Telemetry and Compliance

FortiGate needs the three 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 section **Administrative Access,** enable **FortiTelemetry.**

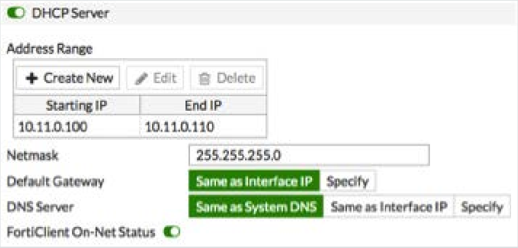


Administrative Access

IPv4 ☑ HTTPS ☑ PING ☑ HTTP ☐ 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
10.11.0.100	10.11.0.110

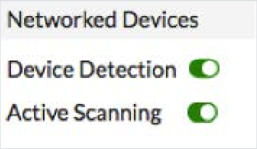
Netmask 255.255.255.0

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.**



Networked Devices

Device Detection

Active Scanning

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

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

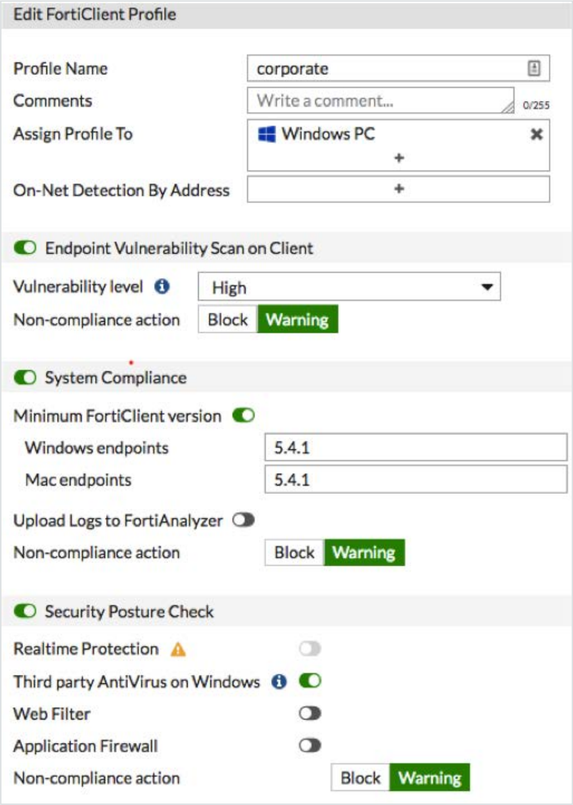
7. Click **OK.**

FortiClient Security Profile Definition

The FortiClient Security Profile contains the compliance rules the endpoint must satisfy prior to be granted 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
Window 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



Edit FortiClient Profile

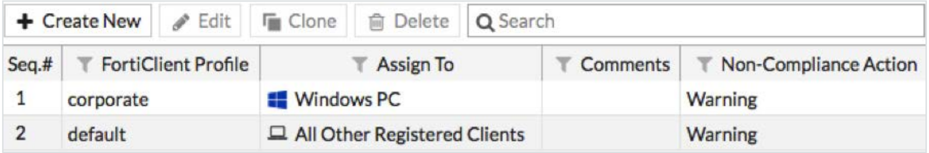
Profile Name: corporate
Comments: Write a comment... 0/255
Assign Profile To: Windows PC
On-Net Detection By Address

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]

The new profile appears before the default one.

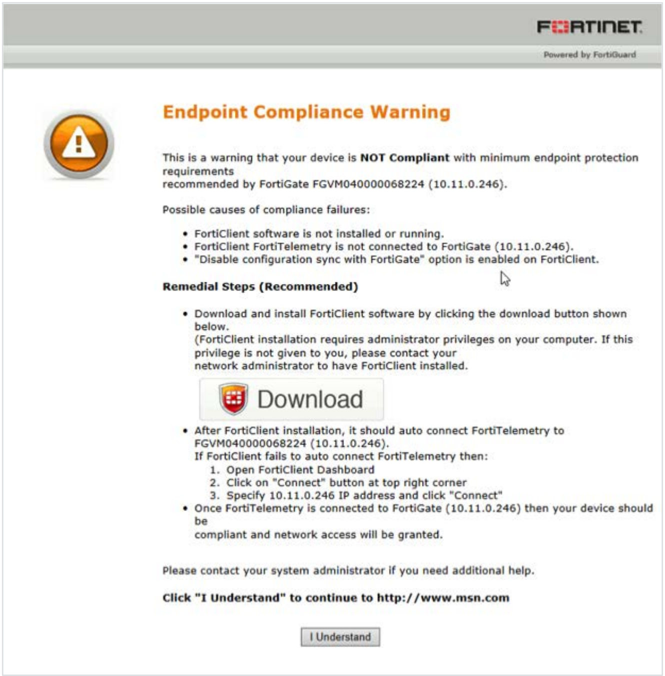


Seq.#	FortiClient Profile	Assign To	Comments	Non-Compliance Action
1	corporate	Windows PC		Warning
2	default	All Other Registered Clients		Warning

Check the FortiClient Security Fabric Agent

FortiGate is configured to enforce 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)

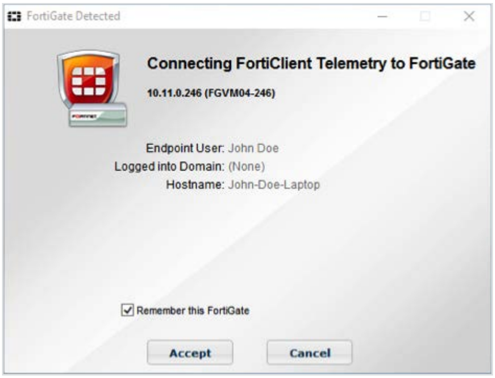
- Download and install FortiClient software by clicking the download button shown below.
  (FortiClient installation requires administrator privileges on your computer. If this privilege is not given to you, please contact your
  network administrator to have FortiClient installed.

  Download
- 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

FortiGate sends FortiTelemetry probes on the LAN network on a regular basis. Once FortiClient is started it detects these probes an displays a registration popup the user has to accept in order to register.



Connecting FortiClient Telemetry to FortiGate

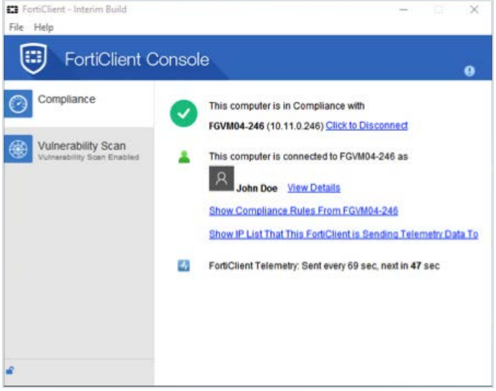
10.11.0.246 (FGVM04-246)

Endpoint User: John Doe
Logged into Domain: (None)
Hostname: John-Doe-Laptop

☑ Remember this FortiGate

Once registered, FortiGate sends the FortiClient Security profiles which has been defined. FortiClient performs the required checks and transmits the result to 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 this window.



This computer is in Compliance with FGVM04-246 (10.11.0.246) Click to Disconnect

This computer is connected to FGVM04-246 as John Doe View Details

Show Compliance Rules From FGVM04-246

Show IP List That This FortiClient is Sending Telemetry Data To

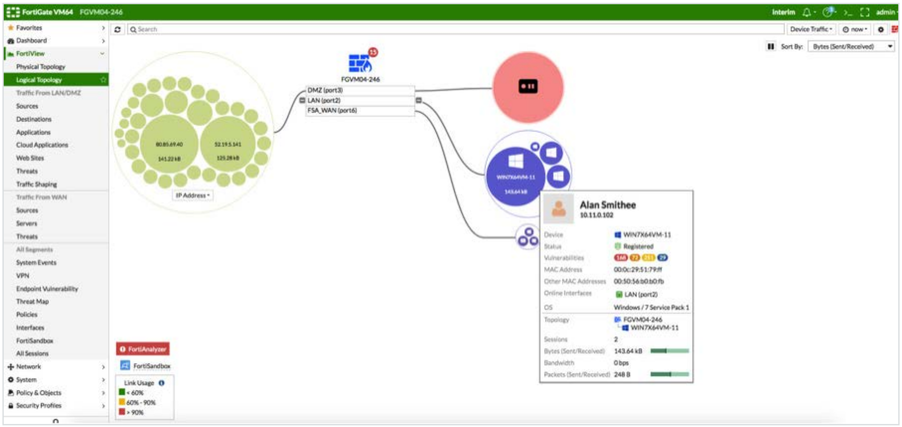
FortiClient Telemetry: Sent every 69 sec, next in 47 sec

Note: it is possible to configure the solution for a transparent and automatic registration.

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 device gives you the elements collected by FortiGate.

In the following screenshot, the detail for our endpoint is displayed. We can review some information like the user name, avatar, IP and MAC address, etc. More interesting we can also notice its vulnerability result.

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

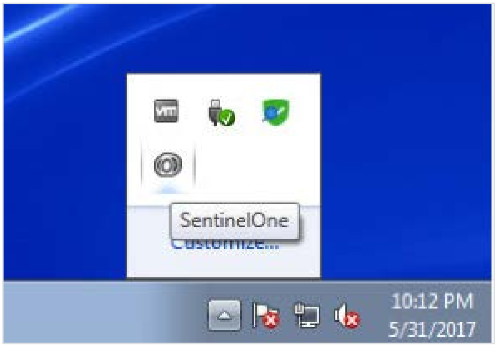


Alan Smithee
10.11.0.102

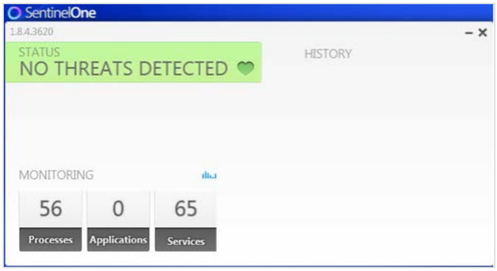
Device	WIN7X64VM-11
Status	Registered
Vulnerabilities	168 72 211 29
MAC Address	00:0c:29:51:79:ff
Other MAC Addresses	00:50:56:b0:b0:fb
Online Interfaces	LAN (port2)
OS	Windows / 7 Service Pack 1
Topology	FGVM04-246 WIN7X64VM-11
Sessions	2
Bytes (Sent/Received)	143.64 kB
Bandwidth	0 bps
Packets (Sent/Received)	248 B

Check the SentinelOne Agent

SentinelOne agent console can be opened with a right click on the its icon into the Windows task bar.



It displays essential information related to endpoint security.



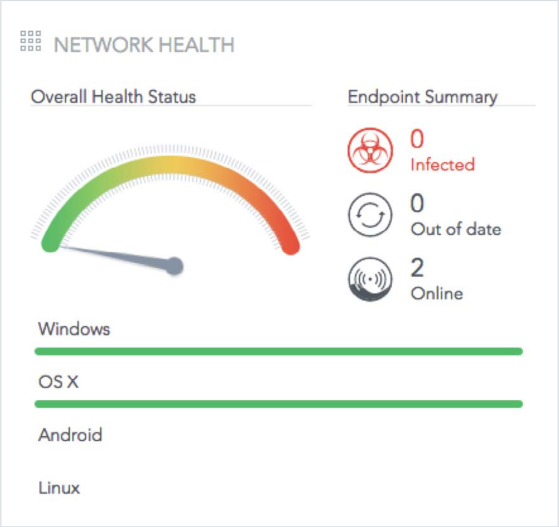
SentinelOne

1.8.4.3620

STATUS
NO THREATS DETECTED

56	0	65
Processes	Applications	Services

You can access more information from the cloud-based management portal. In the screenshot below, we clicked on the SentinelOne dashboard from which there is the **Network Health** widget.



NETWORK HEALTH

Overall Health Status

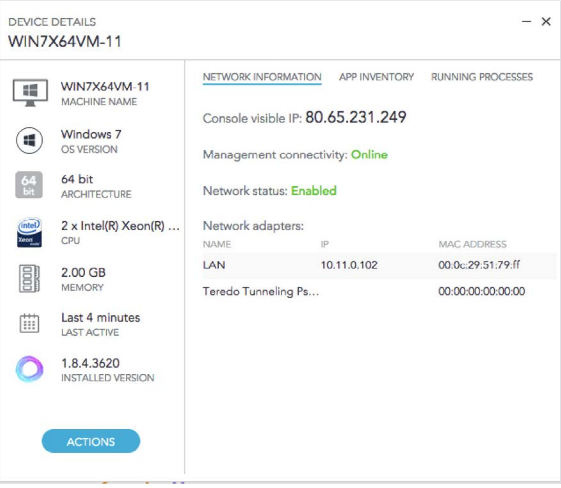
Endpoint Summary

0 Infected

0 Out of date

2 Online

Then we clicked on **2 Online** and we selected our deployed endpoint. The next screenshot shows the information collected by the agent and transmitted to the SentinelOne Management Console.



DEVICE DETAILS
WIN7X64VM-11

WIN7X64VM-11
MACHINE NAME

Windows 7
OS VERSION

64 bit
ARCHITECTURE

2 x Intel(R) Xeon(R) …
CPU

2.00 GB
MEMORY

Last 4 minutes
LAST ACTIVE

1.8.4.3620
INSTALLED VERSION

Console visible IP: 80.65.231.249

Management connectivity: Online

Network status: Enabled

Network adapters:

NAME	IP	MAC ADDRESS
LAN	10.11.0.102	00:0c:29:51:79:ff
Teredo Tunneling Ps…		00:00:00:00:00:00

www.fortinet.com

June 28, 2019 7:56 AM

D:\Fortinet\Deployment Guide\Sentinelone\DG - Fortinet and SentinelOne V1

440597-0-0-EN