



# FortiClient & FortiClient EMS - New Features Guide

Version 6.2.0

**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 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: [techdoc@fortinet.com](mailto:techdoc@fortinet.com)



June 01, 2020

FortiClient & FortiClient EMS 6.2.0 New Features Guide

04-620-548127-20200601

# TABLE OF CONTENTS

<b>Expanding Fabric family</b>	<b>4</b>
Dynamic endpoint grouping/tagging and EMS connector (endpoint compliance)	4
Software Inventory logging to FortiAnalyzer	7
Remote logging support for FortiClient (Linux)	9
Automated syncing of the FortiGate Web Filter profile	12
<b>Advanced threats</b>	<b>14</b>
Client handling for HTTPS (browser plugin) for Google Chrome browser	14
FortiSandbox Cloud support	15
FortiSandbox support for FortiClient (macOS)	17
Cloud-based threat detection	20
<b>SOC adoption</b>	<b>23</b>
Vulnerability dashboard	23
Current Vulnerabilities Summary	23
Top 10 Vulnerable Endpoints With High Risk Vulnerabilities	24
Endpoint Scan Status	25
Top 10 Vulnerabilities	26
<b>UX/Usability</b>	<b>28</b>
Endpoint policy	28
<b>Other</b>	<b>30</b>
Free VPN client	30
CLI support for FortiClient (Linux)	31
Endpoint control	32
AV scanning	33
Vulnerability scanning	34
FortiClient updates	36
Installer creation enhancements	38
Administrator settings improvements	41
Support for three types of administrators	41
Support for multiple LDAP servers	42
Permission management based on administrator roles	43
Categorized and refined administrator permissions	44
Restricting login to trusted hosts	45
Automatic license retrieval from FortiCare	46
Renaming of FortiClient EMS	48
Automatic group assignment	48
<b>Change log</b>	<b>50</b>

# Expanding Fabric family

## Dynamic endpoint grouping/tagging and EMS connector (endpoint compliance)

As part of the Security Fabric, you can now configure categorization rules on EMS to dynamically group/tag FortiClient Fabric Agent endpoints. You can then share these endpoint groups with FortiGate over the EMS connector. EMS dynamically updates these endpoint groups when host compliance or other events happen. You can combine the endpoint groups with FortiGate firewall policies to provide dynamic access control based on endpoint status.

You can dynamically group endpoints by OS type, OS version, certificate, logged in domain, files, running applications/processes, registry keys, and more. When a FortiClient endpoint registers to EMS, EMS dynamically groups the endpoint based on the compliance verification rules.

You can selectively block, allow, or captive portal display endpoint groups based on their real-time compliance statuses.

You can configure EMS to send requests for tags to registered endpoints. Each endpoint responds by sending the values of matching tags to EMS in the endpoint control protocol keepalive messages. You can configure FortiGates to retrieve endpoint tags from EMS. You can use the tags in FortiGate firewall policies.

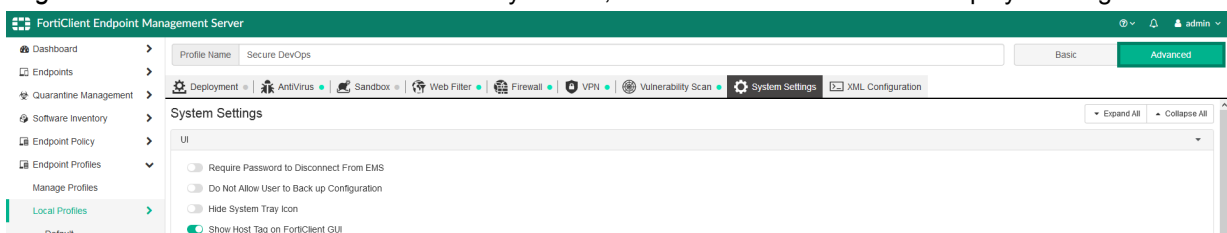
This feature requires three main components:

- FortiClient (Windows, macOS, or Linux)
- EMS
- FortiGate

This feature is new to 6.2.0 and requires that all components are running 6.2.0 or a newer version.

### To configure EMS for dynamic endpoint grouping:

1. Create a profile:
  - a. Go to *Endpoint Profiles > Manage Profiles*.
  - b. Click *Add*.
  - c. Configure the security features in the profile as desired.
  - d. If you want the host tags to display on the FortiClient GUI, on the *System Settings* tab, enable *Show Host Tag on FortiClient & FortiClient EMS GUI*. By default, the FortiClient GUI does not display host tags.



2. Create a policy:
  - a. Go to *Endpoint Policy > Manage Policies*.
  - b. Click *Add*.

- c. Configure the new policy. Select the desired group or Active Directory organizational unit (OU), profile, and Telemetry gateway list.

### 3. Create host verification rules:

- a. Go to *Compliance Verification > Compliance Verification Rules*.
- b. Click *Add*.
- c. Configure rules and tags as desired.

For details on compliance verification rule types, see the [EMS Administration Guide](#).

### To configure FortiOS for dynamic endpoint grouping:

```
config user fsso
  edit "ems_name"
    set server 10.127.121.21
    set type fortiems
    set ssl enable
    set ssl-trusted-cert "Fortinet_CA"
    set group-poll-interval <desired interval in minutes>
  next
end
config user group
  edit "group_name"
    set group-type fsso-service
    set member "ems_group"
  next
end
```

In the above CLI sample, `set ssl-trusted cert` is optional. For this option to function, you must upload a certificate in *System Settings > Server > EMS FSSO Settings*.

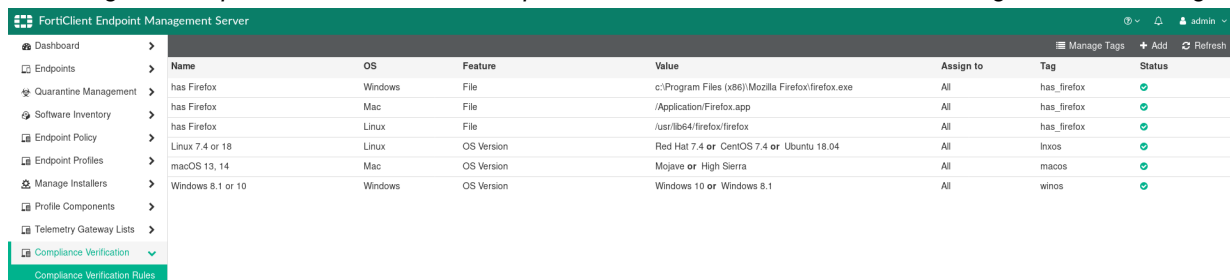
`group-poll-interval` is only available for FortiOS 6.2.2 and later versions. In FortiOS 6.2.0 and 6.2.1, you can go to *Security Fabric > Fabric Connectors*, open the EMS connector editing page, then click *Apply & Refresh* to fetch endpoint grouping data from EMS.

### To configure FortiClient for dynamic endpoint grouping:

Ensure that FortiClient is registered to EMS. If FortiClient is not registered to EMS, manually enter the EMS IP address in the FortiClient GUI on the *Fabric Telemetry* tab. FortiClient receives the assigned Telemetry gateway list and registers to the FortiGate on the gateway list. FortiClient then sends the tags to EMS.

### To view the results:

1. In EMS, go to *Compliance Verification > Compliance Verification Rules* to view all configured rules and tags.



FortiClient Endpoint Management Server							
	Name	OS	Feature	Value	Assign to	Tag	Status
Quarantine Management	has Firefox	Windows	File	c:\Program Files (x86)\Mozilla Firefox\firefox.exe	All	has_firefox	●
Software Inventory	has Firefox	Mac	File	/Application/Firefox.app	All	has_firefox	●
Endpoint Policy	has Firefox	Linux	File	/usr/lib64/firefox/firefox	All	has_firefox	●
Endpoint Profiles	Linux 7.4 or 18	Linux	OS Version	Red Hat 7.4 or CentOS 7.4 or Ubuntu 18.04	All	linuxos	●
Manage Installers	macOS 13, 14	Mac	OS Version	Mojave or High Sierra	All	macos	●
Profile Components	Windows 8.1 or 10	Windows	OS Version	Windows 10 or Windows 8.1	All	winos	●

2. Go to **Compliance Verification > Host Tag Monitor** to view all tags and the endpoints that are currently applicable.

The screenshot shows the FortiClient Endpoint Management Server interface. The left sidebar has a menu with 'Compliance Verification' expanded, showing 'Compliance Verification Rules' and 'Host Tag Monitor'. The main area displays a table of endpoints with tags.

Endpoint	User	OS	IP	Tagged on
<b>has_firefox (2)</b>				
Alderwood	dlamberson	Linux CentOS 7.5.1804	10.127.131.108	2019-03-21 19:26:21
Cherrywood	LEdington	Microsoft Windows 8.1 Enterprise	10.127.131.102	2019-03-21 19:00:49
<b>winos (1)</b>				
Cherrywood	LEdington	Microsoft Windows 8.1 Enterprise	10.127.131.102	2019-03-21 19:00:49

3. Go to **Compliance Verification > Fabric Device Monitor** to view connected FortiGates.

The screenshot shows the FortiClient Endpoint Management Server interface. The left sidebar has a menu with 'Compliance Verification' expanded, showing 'Compliance Verification Rules' and 'Fabric Device Monitor'. The main area displays a table of connected FortiGates.

IP Address	Version	Last Sync Time
10.127.121.1	v6.0.0859-0859	2019-03-21 09:53:34

4. View the endpoint details. You can see that host verification tags have been applied. In this example, the endpoint is running Firefox and has Windows 8.1 or 10 installed, and therefore has the has\_firefox and winos tags applied according to the compliance verification rules.

The screenshot shows the FortiClient Endpoint Management Server interface. The left sidebar has a menu with 'Workgroups' expanded, showing 'All Groups' and 'Smart PowerGrid'. The main area displays the details for the endpoint 'LEdington'.

Device	OS	IP	MAC	Last Seen	Location	Host Verification Tags
Cherrywood	Microsoft Windows 8.1 Enter...	10.127.131.102	00-15-5d-a1-a6-0d	2019-03-21 20:14:41	On-Net	has_firefox winos

**Connection**

- FortiTelemetry to FGVM010000168979
- Managed by EMS

**Configuration**

- Profile: Secure DevOps
- Installer: Not Assigned
- Telemetry Gateway List: FortiGate Edge
- FortiClient Version: 6.2.0.0760
- FortiClient Serial Number: FCT8001610133015

**Status**

- Registered

**Features**

- AntiVirus enabled (hidden)
- Sandbox Detection installed
- Web Filter enabled (hidden)
- Application Firewall enabled (hidden)
- Remote Access configured (hidden)
- Vulnerability Scan enabled (hidden)
- SSOMA installed

5. In the FortiOS CLI, run the `diag debug authd fsso list` command to view received endpoint tags:

```

----FSSO logons----
IP: 10.127.131.102 User: LEDINGTON Groups: 6E813333919A475F9AA7C9B640A8B871+HAS_
FIREFOX+WINOS Workstation: CHERRYWOOD
IP: 10.127.131.108 User: DLAMBERSON Groups: F3C5191D4F6E47B996467A25AB12C4A4+HAS_FIREFOX
Workstation: ALDERWOOD
Total number of logons listed: 2, filtered: 0
----end of FSSO logons----

```

6. Run the `diag debug enable` command, then the `diag debug authd fsso server-status` command to view the EMS that the FortiGate is connected to:

FGVM010000168979 #			
Server Name	Connection Status	Version	Address
ems_user	connected	FSSO 5.0.0269	10.127.121.21

7. Disable debug mode by running the `diag debug disable` command.
8. View the tags that FortiClient sends on the avatar page in the FortiClient GUI.

### To create a dynamic firewall policy for the user group:

You can now create a dynamic firewall policy in FortiOS for the user group. In this example, an IPv4 policy is created for the user group.

1. In FortiOS, go to *Policy & Objects > IPv4 Policy*. Click *Create New*.
2. In the *Source* field, click *+*. The *Select Entries* pane appears. On the *User* tab, select the user group configured above.
3. Configure other options as desired. Click *OK*.
4. Go to *Policy & Objects > IPv4 Policy* to ensure the policy was created and applied to the desired user group. FortiOS will update this policy when it receives updates from EMS.

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
3	33	all	EMS_server_01 EMS_server_02 EMS_server_03 dns_internal dns_server	always	ALL	ACCEPT	Enabled	no-inspection	UTM	3.20 GB
1	111	all test-ems-group	pc155_address	always	ALL	ACCEPT	Enabled	no-inspection	UTM	6.68 GB
4	44	all ems_03_group	pc5_address	always	ALL	ACCEPT	Enabled	no-inspection	UTM	21.37 MB

## Software Inventory logging to FortiAnalyzer

FortiClient endpoints can now send Software Inventory logs to FortiAnalyzer for real time and historic logging and reporting.

FortiClient collects information on regular software installed on the endpoint and sends the information to EMS and FortiAnalyzer. FortiClient sends the Software Inventory information when it first registers to EMS and when it first sends data to FortiAnalyzer. If software changes occur on the endpoint, such as installing new software, updating existing software, or removing existing software, FortiClient sends an updated inventory to EMS and FortiAnalyzer.

This feature requires the following configuration:

1. In EMS, enable *Send Software Inventory* on an endpoint profile.
2. If needed, create a Fabric ADOM in FortiAnalyzer.

### To configure the endpoint profile in EMS:

1. In EMS, create a new endpoint profile or edit an existing profile.
2. On the *System Settings* tab, enable *Send Software Inventory*.
3. Save the profile.
4. Ensure that the profile is used in the endpoint policy assigned to the desired group or OU.

### To create a Fabric ADOM in FortiAnalyzer:

1. In FortiAnalyzer, go to *System Settings > All ADOMs*.
2. Click *Create New*.
3. From the *Type* dropdown list, select *Fabric*.
4. Click *+ Select Device*.
5. Add at least one FortiGate and the EMS server that the FortiClient endpoint is registered to.
6. Configure other options as desired.
7. Click *OK*.

**Create New ADOM**

Name: Smart\_PowerGrid

Type: Fabric

Comments: 0/128

Devices:

Name	IP Address	Platform
FCTEM50176860796	0.0.0.0	FortiClient-EMS
FGT_Edge	10.127.121.1	FortiGate-VM64

**Data Policy**

Keep Logs for Analytics: 60 Days

Keep Logs for Archive: 365 Days

**Disk Utilization**

Maximum Allowed: 0 MB Available: 0.0 KB

Analytics - Archive: 70%

Alert and Delete When Usage Reaches: 90%

\*If analytic or archive log usages exceed the configured disk quota before the retention period expires, the oldest logs will be deleted.

Buttons: OK, Cancel

8. After creation, switch to the newly created ADOM. Go to *SOC*, then go to the *Monitors* tab. The *FortiClient Software Inventory* option is available in the left pane.



## To view the results:

1. In EMS, go to *Software Inventory*. You can view the Software Inventory by application or host.

FortiClient Endpoint Management Server

103 Applications | 4 Operating Systems

Display by Host

Host	User	OS	IP	Application Count	Last Installation
Cherrywood	ledington	Microsoft Windows 8.1 Enterprise	10.127.131.102	8	2019-03-31

Name	Vendor	Version	Install Date
7-Zip 16.04 (x64)	Igor Pavlov	16.04	2016-10-04
FortiClient	Fortinet Technologies Inc	6.2.0.0769	2019-03-30
Google Chrome	Google, Inc.	73.0.3683.86	2019-03-30
Google Update Helper	Google LLC	1.3.34.7	2019-03-30
Mozilla Firefox 66.0.2 (x86 en-US)	Mozilla	66.0.2	2019-03-31
Mozilla Maintenance Service	Mozilla	63.0.1	2019-03-31
Mozilla Maintenance Service	Mozilla	52.8.0	2019-03-31
Mozilla Thunderbird 52.8.0 (x86 en-US)	Mozilla	52.8.0	2018-05-16

2. In FortiAnalyzer, in the Fabric ADOM created earlier, go to *SOC > Monitors > FortiClient Software Inventory*. You can view the data that endpoints sent to FortiAnalyzer.

SOC View Monitors

ADOM: Smart\_PowerGrid

FortiClient Software Inventory

Total Apps Installed: 7 (+7)

New Apps Installed: 7 (+7)

#	Application	Host Count
1	7-Zip 16.04 (x64)	1
2	FortiClient	1
3	Google Chrome	1
4	Google Update Helper	1
5	Mozilla Firefox 66.0.2 (x86 en-US)	1
6	Mozilla Maintenance Service	1
7	Mozilla Thunderbird 52.8.0 (x86 en-US)	1

#	Host Name	User	OS	# of Apps
1	Cherrywood	ledington		7

## Remote logging support for FortiClient (Linux)

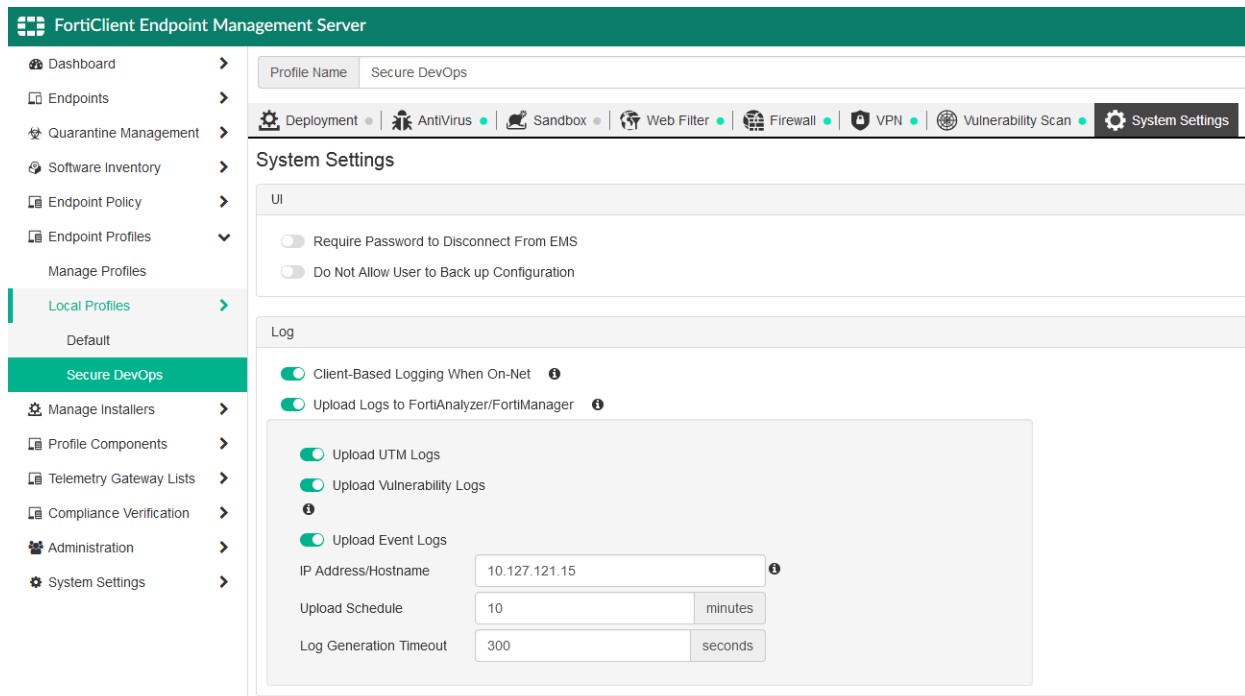
FortiClient (Linux) endpoints can now send logs to FortiAnalyzer for historical logging and reporting.

The EMS administrator can provide a FortiAnalyzer's IP address in an endpoint profile. All endpoints registered to the EMS that have this endpoint profile applied send logs to the specified FortiAnalyzer. FortiClient (Linux) also sends vulnerability and antivirus (AV) scan results, the user avatar, and Telemetry messages to FortiAnalyzer. The logs and vulnerability scan results display in FortiView and Log View in FortiAnalyzer.

This feature is new for FortiClient (Linux) 6.2.0, but is available for earlier versions of FortiClient (Windows) and FortiClient (macOS).

### To configure the endpoint profile in EMS:

1. In EMS, go to *Endpoint Profiles* and select the desired endpoint profile.
2. On the *System Settings* tab, enable *Upload Logs to FortiAnalyzer/FortiManager*.
3. In the *IP Address/Hostname* field, enter the FortiAnalyzer's IP address. In this example, the FortiAnalyzer's IP address is 10.127.121.15.



4. Update other settings, such as *Upload UTM Logs*, *Upload Vulnerability Logs*, *Log Generation Timeout*, and so on, as desired.
5. Save the profile.
6. If the profile has not already been configured as part of an endpoint policy, go to *Endpoint Policy* and configure this profile as part of a policy that is assigned to an endpoint group. All endpoints in this group will now send logs to FortiAnalyzer. Endpoints only send logs to FortiAnalyzer as long as they are registered to EMS.

When a vulnerability scan completes, FortiClient sends logs to FortiAnalyzer. You can review the logs in Log View or FortiView in FortiAnalyzer.

Log View

ADOM: root

Log Details

#	Date/Time	Level	Device ID	User	FortiClient UUID	Scan Time	Vulnerability Category
1	12-49-41	notice	FGVM010000168979	dlamberson	F3C5191D4F6E47B99...	1553212865	OS
2	12-49-41	notice	FGVM010000168979	dlamberson	F3C5191D4F6E47B99...	1553212865	OS
3	12-49-41	notice	FGVM010000168979	dlamberson	F3C5191D4F6E47B99...	1553212865	OS
4	12-49-41	notice	FGVM010000168979	dlamberson	F3C5191D4F6E47B99...	1553212865	OS
5	12-49-41	notice	FGVM010000168979	dlamberson	F3C5191D4F6E47B99...	1553212865	OS
6	12-49-41	notice	FGVM010000168979	dlamberson	F3C5191D4F6E47B99...	1553212865	OS
7	12-49-41	notice	FGVM010000168979	dlamberson	F3C5191D4F6E47B99...	1553212865	OS
8	12-49-41	notice	FGVM010000168979	dlamberson	F3C5191D4F6E47B99...	1553212865	OS
9	12-49-41	notice	FGVM010000168979	dlamberson	F3C5191D4F6E47B99...	1553212865	OS
10	12-49-41	notice	FGVM010000168979	dlamberson	F3C5191D4F6E47B99...	1553212865	OS
11	12-49-41	notice	FGVM010000168979	dlamberson	F3C5191D4F6E47B99...	1553212865	Web Client
12	12-49-41	notice	FGVM010000168979	dlamberson	F3C5191D4F6E47B99...	1553212865	Web Client
13	12-49-41	notice	FGVM010000168979	dlamberson	F3C5191D4F6E47B99...	1553212865	Applications
14	12-49-41	notice	FGVM010000168979	dlamberson	F3C5191D4F6E47B99...	1553212865	Web Client
15	12-49-41	notice	FGVM010000168979	dlamberson	F3C5191D4F6E47B99...	1553212865	OS
16	12-49-41	notice	FGVM010000168979	dlamberson	F3C5191D4F6E47B99...	1553212865	Web Client
17	12-49-41	notice	FGVM010000168979	dlamberson	F3C5191D4F6E47B99...	1553212865	OS
18	12-49-41	notice	FGVM010000168979	dlamberson	F3C5191D4F6E47B99...	1553212865	Web Client
19	12-49-41	notice	FGVM010000168979	dlamberson	F3C5191D4F6E47B99...	1553212865	OS
20	12-49-41	notice	FGVM010000168979	dlamberson	F3C5191D4F6E47B99...	1553212865	Web Client
21	12-49-41	notice	FGVM010000168979	dlamberson	F3C5191D4F6E47B99...	1553212865	OS
22	12-49-41	notice	FGVM010000168979	dlamberson	F3C5191D4F6E47B99...	1553212865	OS
23	12-49-41	notice	FGVM010000168979	dlamberson	F3C5191D4F6E47B99...	1553212865	OS
24	12-49-41	notice	FGVM010000168979	dlamberson	F3C5191D4F6E47B99...	1553212865	OS
25	12-49-41	notice	FGVM010000168979	dlamberson	F3C5191D4F6E47B99...	1553212865	OS
26	12-49-41	notice	FGVM010000168979	dlamberson	F3C5191D4F6E47B99...	1553212865	OS
27	12-49-41	notice	FGVM010000168979	dlamberson	F3C5191D4F6E47B99...	1553212865	OS
28	12-49-41	notice	FGVM010000168979	dlamberson	F3C5191D4F6E47B99...	1553212865	OS
29	12-49-41	notice	FGVM010000168979	dlamberson	F3C5191D4F6E47B99...	1553212865	OS
30	12-49-41	notice	FGVM010000168979	dlamberson	F3C5191D4F6E47B99...	1553212865	OS
31	12-49-41	notice	FGVM010000168979	dlamberson	F3C5191D4F6E47B99...	1553212865	OS
32	12-49-41	notice	FGVM010000168979	dlamberson	F3C5191D4F6E47B99...	1553212865	OS
33	12-49-41	notice	FGVM010000168979	dlamberson	F3C5191D4F6E47B99...	1553212865	OS
34	12-49-41	notice	FGVM010000168979	dlamberson	F3C5191D4F6E47B99...	1553212865	OS
35	12-49-41	notice	FGVM010000168979	dlamberson	F3C5191D4F6E47B99...	1553212865	Web Client
36	12-49-41	notice	FGVM010000168979	dlamberson	F3C5191D4F6E47B99...	1553212865	Web Client
37	12-49-41	notice	FGVM010000168979	dlamberson	F3C5191D4F6E47B99...	1553212865	Applications
38	12-49-41	notice	FGVM010000168979	dlamberson	F3C5191D4F6E47B99...	1553212865	Web Client

Total logs for analytics: 60 days 15 hours. More

50 Items per page 1 0.02 Second

FortiView

ADOM: root

Summary

Device: Alderwood  
Source: dlamberson (10.127.131.108)

Vulnerabilities: 24  
Applications (1), OS (17), Web Client (6)

#	Vulnerability Name	Severity	Category	Vulnerability ID	CVE ID	Remediation Action
1	RHSA-2018-3005: firefox security and bug fix update (Critical)	Critical	Web Client	55283	CVE-2018-12389, CVE-2018-12390, CVE-2018-12392, CVE-2018-12393, CVE-2018-12395, CVE-2018-12396, CVE-2018-12397	
2	RHSA-2017-0372: kernel-arch64 security and bug fix update (Important)	High	OS	40717	CVE-2016-5195, CVE-2016-7039	
3	RHSA-2018-0654: kernel-alt security, bug fix, and enhancement update (Important)	High	OS	49326	CVE-2017-1000255, CVE-2017-1000410, CVE-2017-11473, CVE-2017-12190, CVE-2017-12192, CVE-2017-15129, CVE-2017-15299, CVE-2017-15306, CVE-2017-17448, CVE-2017-17449, CVE-2018-1000004, CVE-2018-6927	
4	RHSA-2018-0180: kernel-alt security and bug fix update (Important)	Medium	OS	49204	CVE-2017-1000405	
5	RHSA-2018-0549: firefox security update (Critical)	Medium	Web Client	49207	CVE-2018-5146	
6	RHSA-2018-1099: firefox security update (Important)	Medium	Web Client	49341	CVE-2018-5148	
7	RHSA-2018-1396: libvirt security and bug fix update (Low)	Medium	OS	49976	CVE-2018-1064, CVE-2018-5748	
8	RHSA-2018-1415: firefox security update (Critical)	Medium	Web Client	49978	CVE-2018-5150, CVE-2018-5154, CVE-2018-5155, CVE-2018-5157, CVE-2018-5158, CVE-2018-5159, CVE-2018-5168, CVE-2018-5178, CVE-2018-5183	
9	RHSA-2018-1374: kernel-alt security and bug fix update (Important)	Medium	OS	50117	CVE-2018-1000199	
10	RHSA-2018-2113: firefox security update (Critical)	Medium	Web Client	50122	CVE-2017-7762, CVE-2018-12359, CVE-2018-12360, CVE-2018-12362, CVE-2018-12363, CVE-2018-12364, CVE-2018-12365, CVE-2018-12366, CVE-2018-5156, CVE-2018-5188, CVE-2018-6126	
11	RHSA-2018-2439: mariadb security and bug fix update (Moderate)	Medium	Applications	50639	CVE-2017-10268, CVE-2017-10378, CVE-2017-10379, CVE-2017-10384, CVE-2017-3636, CVE-2017-3641	

Total logs stored for analytics: 60 days 16 hours. More

Show 100 Total 24

FortiClient also sends vulnerability scan results to EMS. These display on the *Vulnerability Events* tab when viewing endpoint details.

The screenshot displays the FortiClient Endpoint Management Server (EMS) interface. The top navigation bar includes a dashboard, endpoints, domains, and workgroups. The main content area shows a list of vulnerabilities under the 'Vulnerability Events' tab. The table lists various security updates with columns for Vulnerability, Category, Application, Severity, Patch Type, and FortiGuard. The vulnerabilities include updates for Firefox, Xorg, Kernel, libvirt, Gnutls, WPA, and SSD security.

Vulnerability	Category	Application	Severity	Patch Type	FortiGuard
RHSA-2018.3005: firefox security and bug fix update (Critical)	Web Client		Critical	Auto	55283
RHSA-2018.3410: xorg-x11-server security update (Important)	Operating System		Medium	Auto	55321
RHSA-2018.1374: kernel-alt security and bug fix update (Important)	Operating System		Medium	Manual	50117
RHSA-2018.0029: libvirt security update (Important)	Operating System		Medium	Manual	43542
RHSA-2018.3050: gnutls security, bug fix, and enhancement update (Medium)	Operating System		Medium	Auto	55286
RHSA-2018.3107: wpa_supplicant security and bug fix update (Moderate)	Operating System		Medium	Auto	55299
RHSA-2018.0502: kernel-alt security and bug fix update (Important)	Operating System		High	Manual	48618
RHSA-2018.0180: kernel-alt security and bug fix update (Important)	Operating System		High	Manual	49204
RHSA-2018.1396: libvirt security and bug fix update (Low)	Operating System		High	Manual	49976
RHSA-2018.3242: glusterfs security, bug fix, and enhancement update (Low)	Operating System		High	Manual	55304
RHSA-2018.3158: ssd security, bug fix, and enhancement update (Low)	Operating System		High	Manual	55304

## Automated syncing of the FortiGate Web Filter profile

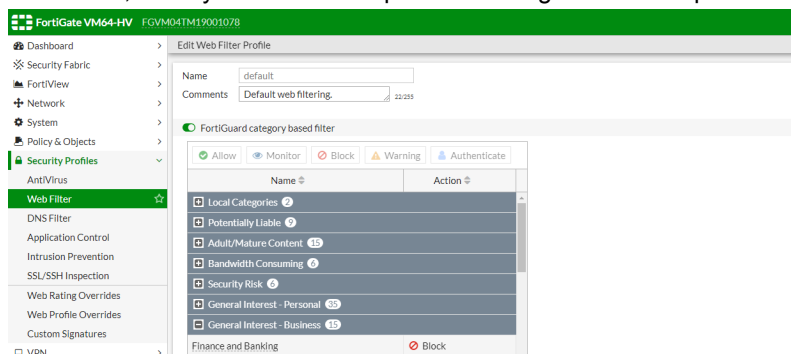
EMS 6.2.0 uses a new FortiOS API to import and sync Web Filter profiles from FortiGate.



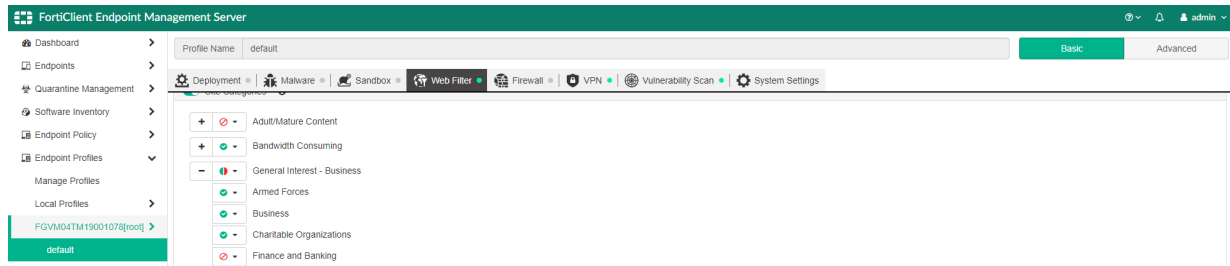
FortiOS 6.2.0 no longer supports the endpoint compliance profile available in earlier versions of FortiOS. EMS 6.2.0 can therefore only import Web Filter profiles from FortiGate and no longer supports importing the compliance profile.

### To import a FortiGate Web Filter profile to EMS:

1. In FortiOS 6.2.0, go to *Security Profiles > Web Filter*. Modify an existing Web Filter profile or create a new Web Filter profile to export to EMS.
2. In EMS, go to *Endpoint Profiles > Manage Profiles > Import > From FortiGate/FortiManager*.
3. On the *Connect to FortiGate/FortiManager* tab, provide the FortiGate IP address, the default port 8013, and the FortiGate username and password, then click *Next*.
4. On the *Preview and Select* tab, select the profile selected or created in step 1. Click *Next*.
5. On the *Configure Synchronization* tab, configure the synchronization frequency as desired. Click *Import*.
6. After EMS has imported the profile from FortiGate, select the imported profile and confirm that the profile's Web Filter settings in FortiOS and in EMS are identical.
7. In FortiOS, modify the Web Filter profile's settings. This example blocks the Finance and Banking site category.



8. After the synchronization interval configured in step 5, check the profile in EMS. EMS has received the profile changes from FortiOS. The profile now blocks the Finance and Banking site category.



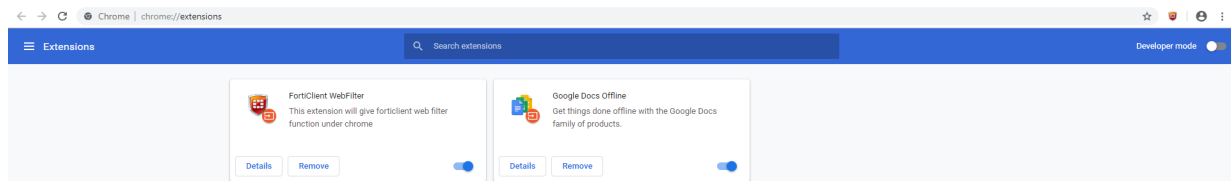
# Advanced threats

## Client handling for HTTPS (browser plugin) for Google Chrome browser

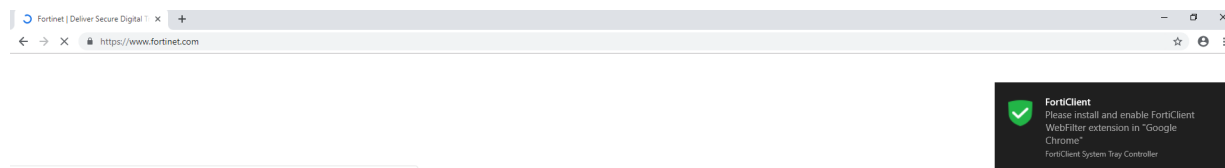
FortiClient now supports a Web Filter plugin that improves detection and enforcement of Web Filter rules on HTTPS sites. The plugin is currently available on the Chrome browser for Windows endpoints and will be available for other major browsers in future releases. There is currently no implementation for macOS or Linux platforms.

**To enable the plugin for HTTPS web filtering:**

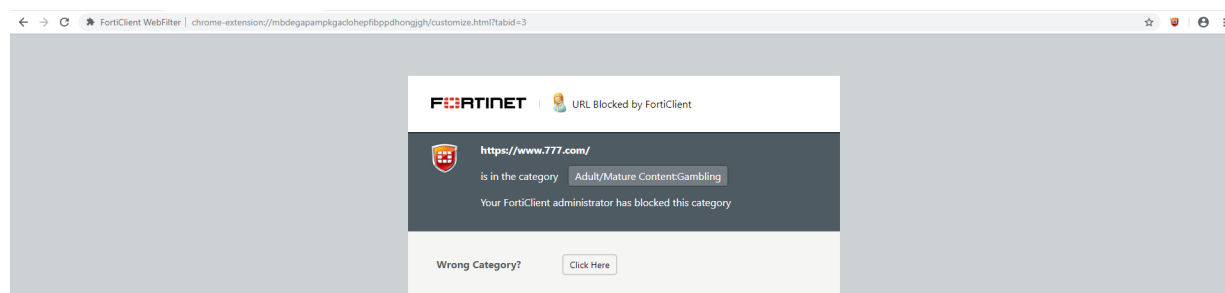
1. In EMS, go to *Endpoint Profiles > Manage Profiles*. Create a new profile or edit an exiting profile.
2. On the *Web Filter* tab, enable *Enable Web Browser Plugin for HTTPS Web Filtering*. Click *Save*.
3. Create a new endpoint policy or edit an existing one to assign the profile to a group or OU. FortiClient receives the profile changes with the next Telemetry communication.
4. In FortiClient on the endpoint, open the Chrome browser and go to `chrome://extensions`.
5. Install or enable the FortiClient WebFilter extension.



When the FortiClient WebFilter extension is not installed or enabled on an endpoint and the end user attempts to browse to a webpage in Chrome, the following notification displays.



After enabling the extension, a FortiClient Web Filter icon appears on the right side of the URL address bar. Web Filter rules function as configured.



You can view the Web Filter events on EMS. If configured, the Web Filter events are also sent to FortiAnalyzer.

## FortiSandbox Cloud support

Licensed endpoints running FortiClient 6.2.0 can now use the FortiSandbox Cloud service for deep inspection of zero-day threats.

Earlier versions of FortiClient supported sending files to FortiSandbox appliances. FortiClient 6.2.0 introduces support for FortiSandbox Cloud. The EMS administrator can now configure FortiClient to use an on-premise FortiSandbox appliance or point to FortiSandbox Cloud. To use this new feature, the following requirements must be met:

- FortiClient must be registered to EMS.
- The Sandbox Cloud license, newly introduced in FortiClient 6.2.0, must be configured on EMS. The Fabric Agent license does not support this feature.
- The EMS administrator has configured the endpoint's assigned profile to use FortiSandbox Cloud as shown below.

**FortiClient Endpoint Management Server**

Profile Name: Secure DevOps

Deployment | AntiVirus | **Sandbox** | Web Filter | Firewall | VPN | Vulnerability Scan | System Settings

**Sandbox Detection** ☒

**Server**

FortiSandbox: Appliance | **Cloud**

Region: Global

License Status: Licensed 2019-07-24

Inspection Mode: None | **High-Risk Files**

Excluded File Extensions: Select an extension

**File Submission Options**

☒ All Files Executed from Removable Media

☒ All Web Downloads

☒ All Email Downloads

**Remediation Actions**

Action: **Quarantine** | Alert & Notify

**Exceptions**

☐ Exclude Files from Trusted Sources ⓘ

☐ Exclude Specified Folders/Files

**Save** **Discard Changes**

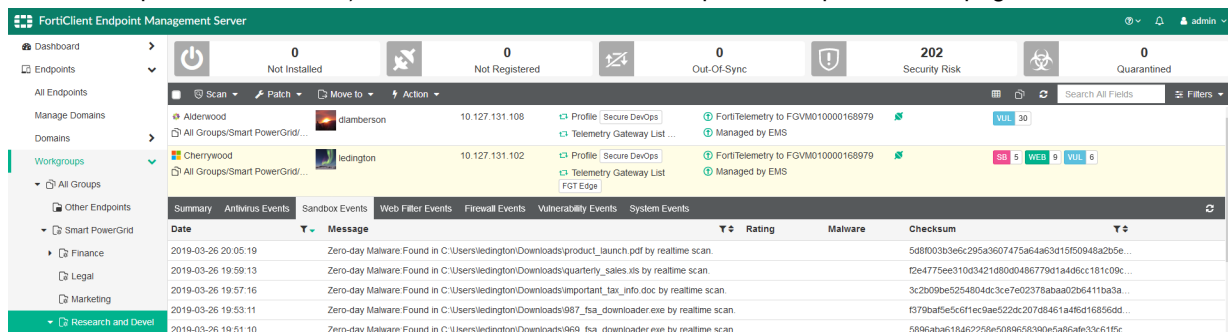
Once FortiClient has received the profile from EMS, FortiClient displays the *Sandbox Detection* tab. FortiSandbox Cloud support functions similarly to the existing FortiSandbox appliance support in earlier versions of FortiClient, except FortiClient sends files to FortiSandbox Cloud instead of an on-premise FortiSandbox appliance.

As the end user goes about their daily activities, FortiClient monitors new files introduced to the system. When FortiClient detects that a new file matches the monitored file type configured in EMS, the following occurs:

1. If enabled, FortiClient AV Real Time Protection (RTP) scans the file. Scanning uses signatures from FortiGuard and FortiSandbox Cloud.
2. One of the following occurs:
  - a. AV RTP detects that the file is malicious. FortiClient quarantines or denies access to the file, depending on the configuration from EMS.
  - b. AV RTP detects that the file is clean. The FortiClient Sandbox feature sends a checksum query to FortiSandbox Cloud. If FortiSandbox Cloud processed the file recently, it quickly returns a verdict. If the file is new to FortiSandbox Cloud, the FortiClient Sandbox feature uploads the file to FortiSandbox Cloud. The FortiClient Sandbox feature queries the file from FortiSandbox Cloud until it receives a verdict or reaches a timeout. Based on the received verdict, FortiClient quarantines or releases the file.

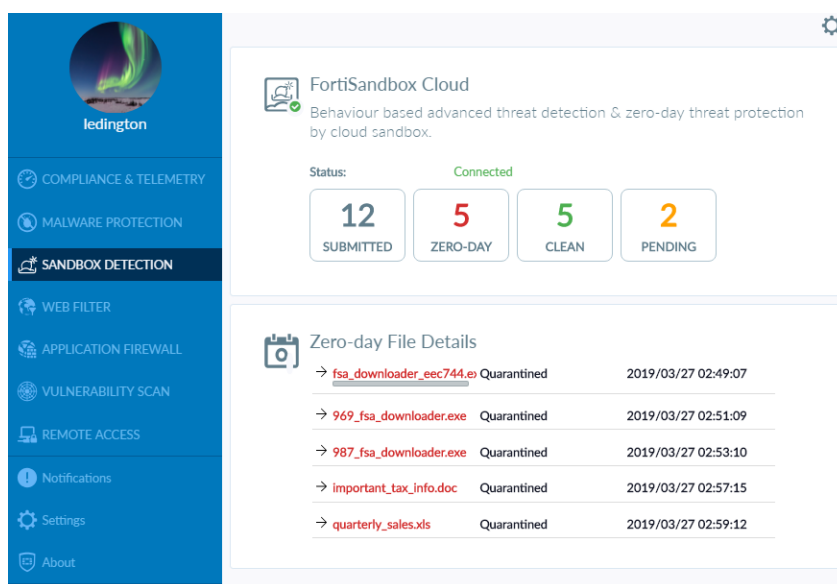
The FortiClient *Sandbox Detection* tab updates as FortiClient processes the file with FortiSandbox:

- If FortiSandbox Cloud returns a verdict that the file is clean, the *Sandbox Detection* tab shows the updated results, and FortiClient does not send logs or results to EMS.
- If FortiSandbox Cloud returns a verdict that the file is not clean, the *Sandbox Detection* tab shows the updated results, and FortiClient sends the results to EMS. You can view the results in EMS in *Quarantine Management* (if FortiClient quarantined the file) or the *Sandbox* tab for the endpoint's endpoint details page.



Each endpoint can send a maximum of 300 files daily. If multiple files are submitted around the same time, FortiClient sends one file to FortiSandbox Cloud, waits until it receives the verdict for that file, then sends the next file to FortiSandbox Cloud.

The following shows the FortiClient GUI when used with FortiSandbox Cloud.





## FortiSandbox support for FortiClient (macOS)

FortiClient (macOS) endpoints can now submit high-risk files to FortiSandbox for analysis. If FortiSandbox detects the submitted file as malicious, then FortiClient quarantines the file. FortiClient (macOS) can submit files to on-premise FortiSandbox appliances only, and cannot submit files to FortiSandbox Cloud.

The FortiClient (macOS) endpoint must be registered to EMS 6.2.0. The FortiSandbox server that FortiClient uses for file submission must authorize EMS.

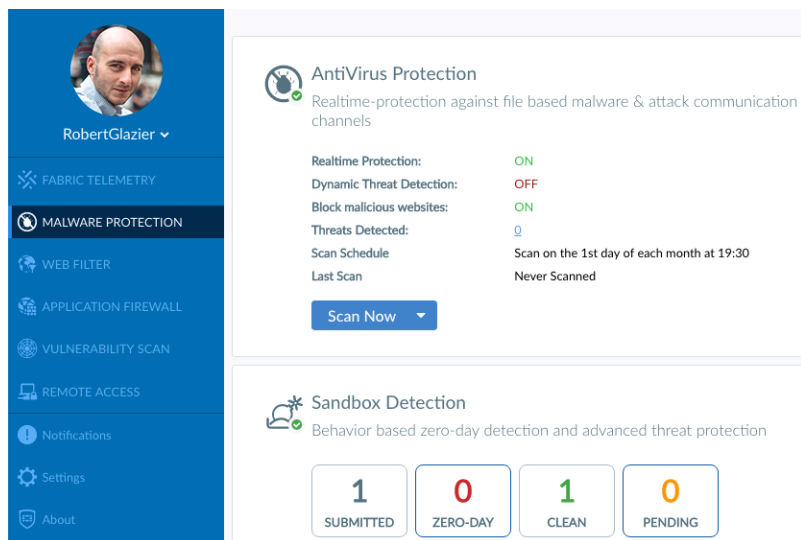
This feature currently has the following limitations:

- FortiClient (macOS) does not support real-time blocking the file being submitted to FortiSandbox. Therefore, the *Wait for FortiSandbox Results before Allowing File Access* option does not apply to FortiClient (macOS). Only if FortiSandbox detects the file as malicious does FortiClient (macOS) quarantine the file.
- FortiClient (macOS) does not automatically include files signed by Apple Inc. as files from trusted sources.
- FortiClient (macOS) does not submit Sandbox detection logs to FortiAnalyzer.

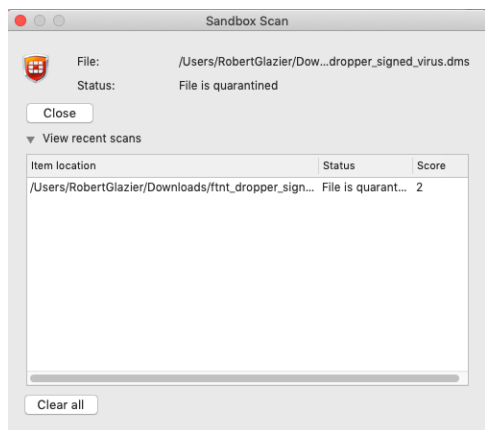
### To configure FortiSandbox scanning for FortiClient (macOS):

1. In EMS, select the desired endpoint profile.
2. On the profile's *Sandbox* tab, enable *Sandbox Detection*.
3. Configure *Server* options:
  - a. Under *FortiSandbox*, select *Appliance*.
  - b. In the *IP address/Hostname* field, enter the FortiSandbox IP address.
  - c. Click *Test Connection*.
  - d. In FortiSandbox, go to *Scan Input > Devices*. Search for and authorize the EMS serial number. You can find the EMS serial number in the *System Information* widget on the EMS dashboard.
  - e. EMS displays that FortiSandbox has authorized EMS. You can now configure the inspection mode. For macOS, it is recommended to select *All Supported Extensions*.
4. Under *File Submission Options*, select *All Web Downloads* and *All Email Downloads*. FortiClient (macOS) only supports submitting web and email downloads.
5. Under *Remediation Actions*, select *Quarantine* or *Alert & Notify*. The user can access the file after FortiClient submits the file for analysis. FortiClient only quarantines the file if FortiSandbox analysis reports the file as malicious.
6. Under *Exceptions*, exclude files from submission based on folder paths or filenames.
7. Click *Save*. EMS applies the profile changes to the endpoint with the next Telemetry communication.

After FortiClient (macOS) receives the Sandbox configuration from EMS, it can submit files for analysis to FortiSandbox. In this example, FortiClient submits a clean file downloaded from a web browser to FortiSandbox. FortiClient displays that one file has been submitted in the *SUBMITTED* tile. FortiClient waits for the results from FortiSandbox. FortiClient receives the verdict from FortiSandbox that the file is not malicious, and displays that one file has been detected as *CLEAN*.



When FortiClient submits a malicious file to FortiSandbox and FortiSandbox detects it as malicious, FortiClient quarantines the file and displays the following dialog.



FortiClient also displays that FortiSandbox has detected a zero-day file.

**RobertGlazier** ▾

- FABRIC TELEMETRY
- MALWARE PROTECTION**
- WEB FILTER
- APPLICATION FIREWALL
- VULNERABILITY SCAN
- REMOTE ACCESS
- Notifications
- Settings
- About

### AntiVirus Protection

Realtime-protection against file based malware & attack communication channels

Realtime Protection: **OFF**

Dynamic Threat Detection: **ON**

Block malicious websites: **ON**

Threats Detected: **0**

Scan Schedule: Scan on the 1st day of each month at 19:30

Last Scan: Never Scanned

**Scan Now** ▾

### Sandbox Detection

Behavior based zero-day detection and advanced threat protection

**7** SUBMITTED

**2** ZERO-DAY

**5** CLEAN

**0** PENDING

The FortiSandbox administrator can see the quarantined file's details.

**High Risk Dropper**

Overview Tree View Details

#### Basic Information

Received:	Apr 22 2019 18:17:39
Started:	Apr 22 2019 18:17:42-07:00
Status:	Done
Rated By:	VM Engine
Submit Type:	FortiClient
Source IP:	172.17.61.114
Digital Signature:	No
SIMNET:	OFF
Virus Total:	<a href="#">Q</a>

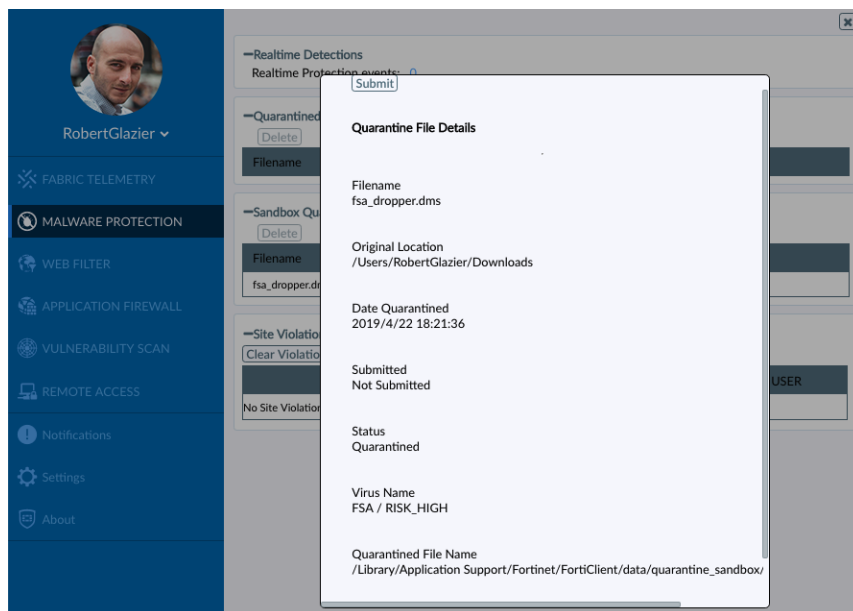
#### Indicators

- The file contains virus
- This file doesn't have a digital signature.

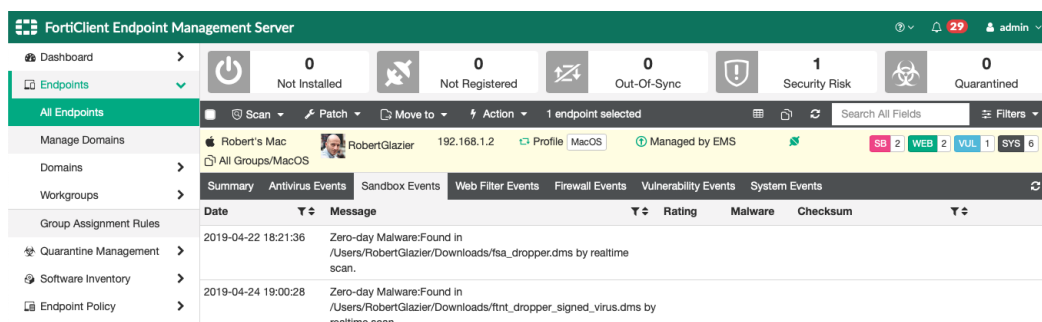
#### Details Information

File Type:	mac
File Size:	8528 (bytes)
MD5:	301071e81daeb064025366d88ce3fd43
SHA1:	450b21bdc204d27bcd26ca39e1154ab1bf19e6a
SHA256:	978837b4eba1edac93fa4a0f3aa5855a81a78c617c04c146cd782e29c6b249b8
ID:	4397741735400602505
Submitted By:	RobertGlazier
Submitted Filename:	fsa_dropper.dms
Filename:	fsa_dropper.dms
Start Time:	Apr 22 2019 18:17:42-07:00
Detection Time:	Apr 22 2019 18:20:21-07:00
Scan Time:	159 seconds
Scan Unit:	FSA3KE3R17000194
Device:	FCT8001784841447
Launched OS:	MACOSX
Infected OS:	MACOSX

The FortiClient user can see the file details in *Malware Protection > Zero Day > Sandbox Quarantined Files*.



The EMS administrator can view the Sandbox event for the FortiClient endpoint.



## Cloud-based threat detection

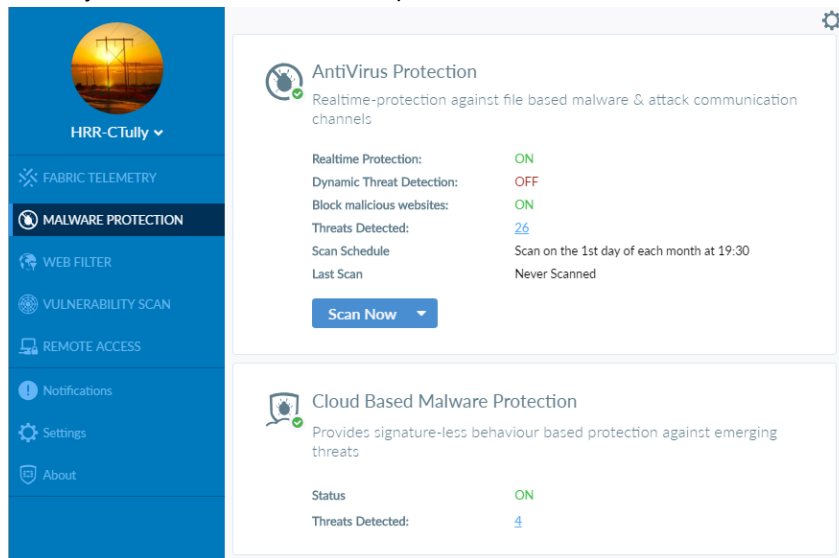
FortiClient's outbreak protection service provides another layer of protection, where FortiClient initiates a real-time cloud lookup of Fortinet's Global Threat Intelligence database so it can detect and block emerging threats and continue to provide the latest protection measures to the endpoint.

FortiClient 6.2.0's malware protection feature includes virus outbreak protection. For each new file downloaded to the endpoint, FortiClient calculates the SHA1 checksum, sends a query to FortiGuard, and temporarily blocks access to the file. If the result from the query indicates that the file is malicious, FortiClient quarantines the newly downloaded file or denies access to it.

### To configure cloud-based threat detection:

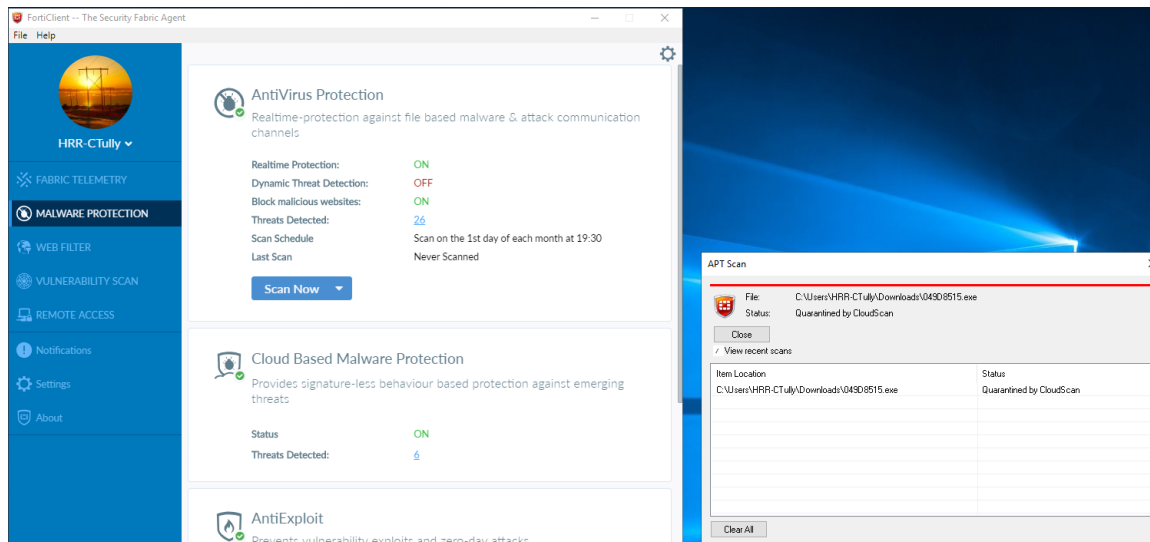
1. In EMS, go to *Endpoint Profiles > Manage Profiles*. Create a new profile or edit an existing one. Enable *Cloud Based Malware Detection* and save the profile.
2. Create a new endpoint policy or edit an existing one to assign the profile from step 1 to a group or OU.

3. In FortiClient, connect to EMS. Once FortiClient receives the profile from EMS, go to the *Malware Protection* tab to verify that cloud-based malware protection is enabled.



### To test the configuration:

1. Download a malware file using a web browser. FortiClient detects and quarantines the file using cloud-based threat detection.



2. To view more information for the quarantined file, click the number of *Threats Detected* on the *Malware Protection* tab. Click the file name to review it.
3. You can also view information about the quarantined file in *Quarantine Management > Files* in EMS.

FortiClient Endpoint Management Server

Dashboard

Endpoints

Quarantine Management

18

Quarantined Files

0

Restored Files

5

Affected Hosts

18

New Detections

Files

Whitelist

Software Inventory

Endpoint Policy

Host

File

Size

Threat

Source

Status

Summary

DESKTOP-QB7QHUM

Other Endpoints

f95f1ebdddb9e9deb21dc8b4bf877da8c1cf...

049D8515.exe

9.0 KB

CLOUDSCAN\_DET...

Sandbox Scan

Quarantined

2019-06-14 17:27:53

1 instance  
1 host affected

DESKTOP-K2KPL7D

Other Endpoints

066\_fsa\_downloader.exe

4.0 KB

FSA / RISK\_HIGH

Sandbox Scan

Quarantined

2019-06-14 11:18:44

1 instance  
1 host affected

4. If configured, you can view the event on FortiAnalyzer.

The screenshot displays the FortiAnalyzer 'Log View' interface. The left sidebar contains navigation options: Traffic, Event (selected), Vulnerability Scan, Custom View, Log Browse, and Log Group. The main area shows a list of log entries. The selected entry is expanded, showing the following details:

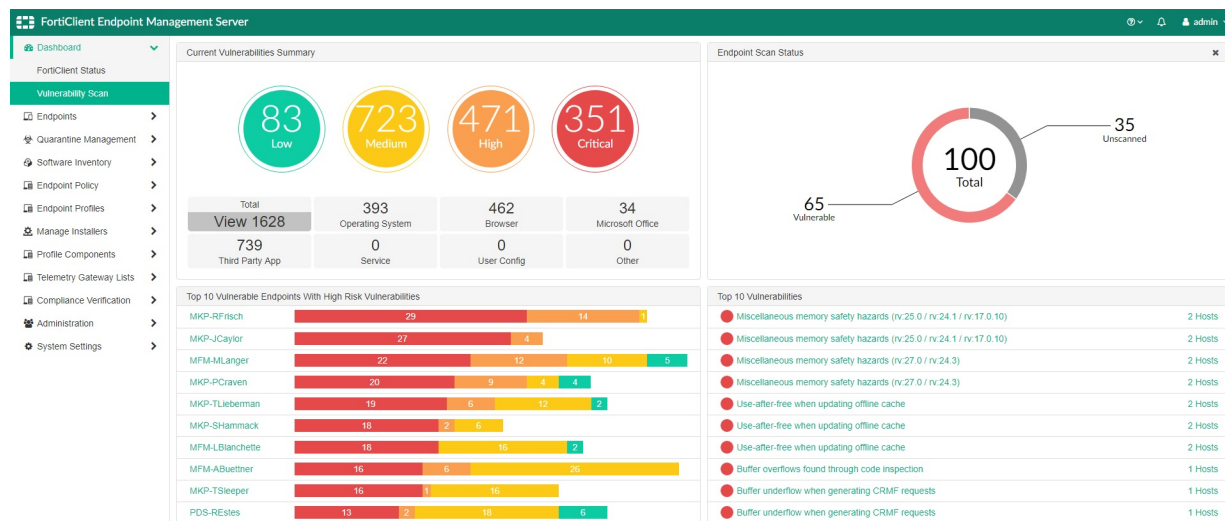
Field	Value
Action	quarantined
Checksum	0x00000000
Client Feature	av
Date/Time	18:06:04
Destination End User ID	0
Destination Endpoint ID	3
Device ID	FCT8001830333942
Device IP	172.17.81.46
Device MAC	00-15-5d-01-98-02
Device Name	FCT8001830333942
Device Time	2019-04-29 18:06:04
End User ID	3
Endpoint ID	1443
File	C:\Users\HRR-CTully\Downloads\049D8515.exe
File Size	9216
FortiClient Version	6.2.0.0780
FortiClientEMS Serial	FCTEMS2637713902
FortiGate Serial	N/A
Host Name	DESKTOP-HUTJE09
Level	warning
Message	Found virus by cloudscan, in filesystem
OS	Microsoft Windows 10 Enterprise Edition, 64-bit (build 17763)
Policy Name	Default
Registered to Device	FCTEMS2637713902
Time Stamp	2019-04-29 18:06:04
Type	event
UID	93AB4EF0D0414B4F9838954351245D7E
User	N/A
Virtual Domain	root
bid	22758569
dvid	1166
idseq	257918120876834816

# SOC adoption

## Vulnerability dashboard

The vulnerability scan dashboard has been improved to support drilldown charts that allow you to easily get more filtered endpoint information.

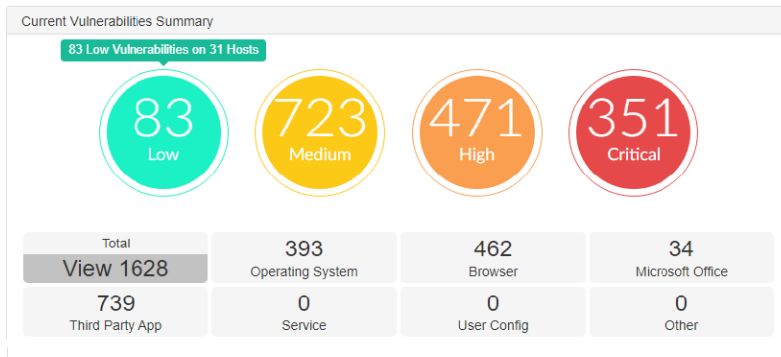
In EMS, go to *Dashboard > Vulnerability Scan*. This page contains charts about connected endpoints' vulnerability scan information.



## Current Vulnerabilities Summary

Go to *Dashboard > Vulnerability Scan > Current Vulnerabilities Summary*. This chart categorizes vulnerabilities based on severity levels, represented in colored circles. It also categorizes vulnerabilities by the following types:

- Total
- Operating System
- Browser
- Microsoft Office
- Third Party App
- Service
- User Config
- Other



Hovering the cursor over the colored circles highlights the circle. Clicking the severity level circle loads a detailed vulnerability page filtered per severity. The detailed page contains the following information:

- Vulnerability Name
- FortiGuard ID
- CVE ID
- Category
- Affected Endpoints
- Patch Status: You can individually patch a vulnerability on an endpoint.
- Patch All: You can patch all displayed vulnerabilities.

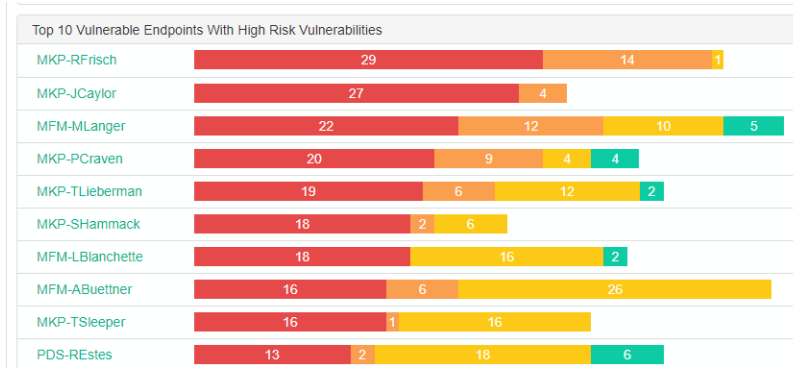
FortiClient Endpoint Management Server						
Low Severity Vulnerabilities Patch All						
	Vulnerability Name	FortiGuard ID	CVE ID	Category	Affected Endpoints	Patch Status
	Security Vulnerability CVE-2013-5772 in Oracle JRE	25334	CVE-2013-5772	Application	1	Patch
	Security Vulnerability CVE-2013-5797 in Oracle JRE	25348	CVE-2013-5797	Application	1	Full Patch
	Security Vulnerability CVE-2013-5803 in Oracle JRE	25352	CVE-2013-5803	Application	1	Patch
	Security Vulnerability CVE-2012-3160 in MySQL	31050	CVE-2012-3160	Application	1	Manual Patch
	Security Vulnerability CVE-2012-3167 in MySQL	31053	CVE-2012-3167	Application	1	Manual Patch
	Security Vulnerability CVE-2012-3197 in MySQL	31057	CVE-2012-3197	Application	1	Manual Patch
	Security Vulnerability CVE-2014-6568 in MySQL	31058	CVE-2014-6568	Application	1	Manual Patch
	Security Vulnerability CVE-2014-0393 in MySQL	31129	CVE-2014-0393	Application	1	Manual Patch
	Security Vulnerability CVE-2014-0420 in MySQL	31133	CVE-2014-0420	Application	1	Manual Patch
	Security Vulnerability CVE-2014-0427 in MySQL	31134	CVE-2014-0427	Application	1	Manual Patch
	Security Vulnerability CVE-2014-0430 in MySQL	31135	CVE-2014-0430	Application	1	Manual Patch
	Security Vulnerability CVE-2014-0431 in MySQL	31136	CVE-2014-0431	Application	1	Manual Patch
	Security Vulnerability CVE-2014-0437 in MySQL	31138	CVE-2014-0437	Application	1	Manual Patch
	Security Vulnerability CVE-2016-0643 in MySQL	31144	CVE-2016-0643	Application	1	Manual Patch
	Security Vulnerability CVE-2016-3452 in MySQL	31172	CVE-2016-3452	Application	1	Manual Patch
	Security Vulnerability CVE-2016-5444 in MySQL	31190	CVE-2016-5444	Application	1	Manual Patch
	Security Vulnerability CVE-2013-3810 in MySQL	33294	CVE-2013-3810	Application	1	Manual Patch
	Security Vulnerability CVE-2013-3811 in MySQL	33295	CVE-2013-3811	Application	1	Manual Patch
	Security Vulnerability CVE-2013-3812 in MySQL	33296	CVE-2013-3812	Application	1	Manual Patch
	Security Vulnerability CVE-2016-0605 in MySQL	33331	CVE-2016-0605	Application	1	Manual Patch
	Security Vulnerability CVE-2016-0608 in MySQL	33334	CVE-2016-0608	Application	1	Manual Patch
	Security Vulnerability CVE-2016-0610 in MySQL	33336	CVE-2016-0610	Application	1	Manual Patch
	Security Vulnerability CVE-2015-4766 in MySQL	33530	CVE-2015-4766	Application	1	Manual Patch
	Security Vulnerability CVE-2014-6502 in Oracle JDK	33718	CVE-2014-6502	Application	1	Manual Patch
	Security Vulnerability CVE-2014-6502 in Oracle JRE	33719	CVE-2014-6502	Application	1	Manual Patch
	Security Vulnerability CVE-2013-5803 in Oracle JDK	34081	CVE-2013-5803	Application	1	Manual Patch
	Security Vulnerability CVE-2013-5803 in Oracle JRE	34082	CVE-2013-5803	Application	1	Manual Patch
	Security Vulnerability CVE-2016-5444 in MySQL	34390	CVE-2016-5444	Application	1	Manual Patch
	Security Vulnerability CVE-2016-5542 in Oracle JDK	34394	CVE-2016-5542	Application	1	Manual Patch
	Security Vulnerability CVE-2016-5542 in Oracle JRE	34395	CVE-2016-5542	Application	1	Manual Patch

83 vulnerabilities with 83 affected endpoint instances loaded

## Top 10 Vulnerable Endpoints With High Risk Vulnerabilities

Go to *Dashboard > Vulnerability Scan > Top 10 Vulnerable Endpoints With High Risk Vulnerabilities*. The bar graph displays the top ten vulnerable endpoints and their vulnerabilities:





You can view all of an endpoint's vulnerabilities by clicking the endpoint name, or view only vulnerabilities of the desired severity level by clicking the corresponding bar. The detailed page contains the following information:

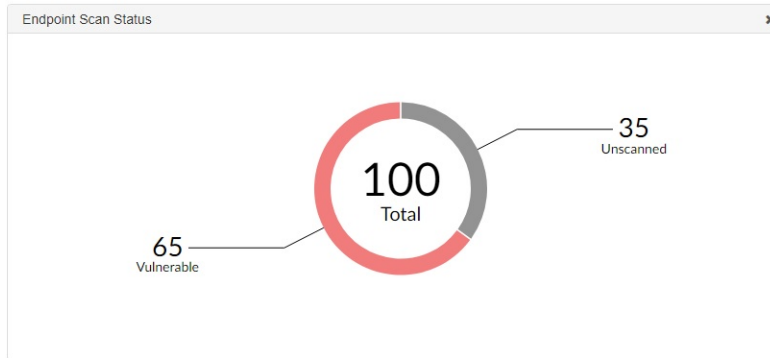
- Vulnerability
- Category
- Severity
- Patch Status: You can patch the endpoint by clicking the *Patch* button.

FortiClient Endpoint Management Server					admin
Dashboard	Vulnerabilities for MKP-RFrisch				Refresh Clear Filters
FortiClient Status	Vulnerability	Category	Severity	Patch Status	
Vulnerability Scan	Security Vulnerabilities in APSB14-14 for Adobe Flash Player	Application	Critical	Patch	
Endpoints	Security Vulnerabilities in APSB14-16 for Adobe Flash Player	Application	Critical	Scheduled	
Quarantine Management	Security Vulnerabilities in APSB14-18 for Adobe Flash Player	Application	Critical	Patch	
Software Inventory	Security Vulnerabilities in APSB14-21 for Adobe Flash Player	Application	Critical	Patch	
Endpoint Policy	Security Vulnerabilities in APSB14-22 for Adobe Flash Player	Application	Critical	Patch	
Endpoint Profiles	Security Vulnerabilities in APSB14-24 for Adobe Flash Player	Application	Critical	Patch	
Manage Installers	Security Vulnerabilities in APSB14-26 for Adobe Flash Player	Application	Critical	Patch	
Profile Components	Security Vulnerabilities in APSB14-27 for Adobe Flash Player	Application	Critical	Patch	
Telemetry Gateway Lists	Security Vulnerabilities in APSB15-01 for Adobe Flash Player	Application	Critical	Patch	
Compliance Verification	Security Vulnerabilities in APSB15-02 for Adobe Flash Player	Application	Critical	Patch	
Administration	Security Vulnerabilities in APSB15-03 for Adobe Flash Player	Application	Critical	Patch	
System Settings	Security Vulnerabilities in APSB15-04 for Adobe Flash Player	Application	Critical	Patch	
	Security Vulnerabilities in APSB15-05 for Adobe Flash Player	Application	Critical	Patch	
	Security Vulnerabilities in APSB15-06 for Adobe Flash Player	Application	Critical	Patch	
	Security Vulnerabilities in APSB15-09 for Adobe Flash Player	Application	Critical	Patch	
	Security Vulnerabilities in APSB15-11 for Adobe Flash Player	Application	Critical	Patch	
	Security Vulnerabilities in APSB15-14 for Adobe Flash Player	Application	Critical	Patch	
	Security Vulnerabilities in APSB15-16 for Adobe Flash Player	Application	Critical	Patch	
	Security Vulnerabilities in APSB15-18 for Adobe Flash Player	Application	Critical	Patch	
	Security Vulnerabilities in APSB15-19 for Adobe Flash Player	Application	Critical	Patch	
	Security Vulnerabilities in APSB15-23 for Adobe Flash Player	Application	Critical	Patch	
	Security Vulnerabilities in APSB15-25 for Adobe Flash Player	Application	Critical	Patch	
	Security Vulnerabilities in APSB15-27 for Adobe Flash Player	Application	Critical	Patch	
	Security Vulnerabilities in APSB15-28 for Adobe Flash Player	Application	Critical	Patch	
	Security Vulnerabilities in APSB15-32 for Adobe Flash Player	Application	Critical	Patch	
	Security Vulnerabilities in APSB16-01 for Adobe Flash Player	Application	Critical	Patch	
	Security Vulnerabilities in APSB16-04 for Adobe Flash Player	Application	Critical	Patch	
	Security Vulnerabilities in APSB16-08 for Adobe Flash Player	Application	Critical	Patch	
	Out-of-bounds read in HTML parser following a failed allocation	Application	High	Patch	

## Endpoint Scan Status

Go to *Dashboard > Vulnerability Scan > Endpoint Scan Status*. This chart categorizes endpoints into the following types:

- Secured
- Vulnerable
- Scanning
- Unscanned



Clicking the *Vulnerable* section of the chart loads the list of endpoints affected with vulnerabilities. This page contains the following information:











- Hostname
- User
- Scan Status
- Vulnerabilities: This is represented as a bar chart segmented per severity.
- Patch Status: You can individually patch a vulnerability on an endpoint.
- Patch All: You can patch all displayed vulnerabilities.

FortiClient Endpoint Management Server						
Vulnerability Endpoint Patch All						
Hostname	User	Scan Status	Vulnerabilities			
MKP-RMunro	Robbie Munro	Vulnerable	9	3	11	3
MKP-RWinchell	Rickey Winchell	Vulnerable	10	1	9	
MKP-GBechtel	Gordon Bechtel	Vulnerable	1	12	3	
MKP-LBramlett	Loma Bramlett	Vulnerable	9	5	13	
MKP-Rittenhouse	Paige Rittenhouse	Vulnerable	18		18	
MKP-RHock	Rachelle Hock	Vulnerable	4	11	14	1
MKP-DRichey	Dexter Richey	Vulnerable	2	24	11	1
MKP-ECoble	Elva Coble	Vulnerable	4	15	9	2
MKP-TSleeper	Tony Sleeper	Vulnerable	10	1	16	
MKP-LTweed	Leonel Tweed	Vulnerable	4			
MKP-RBillington	Reginald Billington	Vulnerable	1	9	7	
MKP-RFrisch	Raymond Frisch	Vulnerable	29		14	1
MKP-PShortt	Pat Shortt	Vulnerable	3	2	20	1
MKP-LMidkiff	Loia Midkiff	Vulnerable	4	1	13	1
MKP-ELowther	Edwin Lowther	Vulnerable	9		12	
MKP-PCraven	Patrick Craven	Vulnerable	20	9	4	2
MKP-RHaring	Raul Haring	Vulnerable	13	1	20	1
MKP-JCaylor	Jesse Caylor	Vulnerable	27		4	
MKP-RSabo	Robyn Sabo	Vulnerable	9	12	26	
MKP-SHammack	Shirley Hammack	Vulnerable	18	2	6	
MKP-TLieberman	Tyler Lieberman	Vulnerable	19	6	12	2
MKP-DShull	Drew Shull	Vulnerable	4	21	14	1

65 entries loaded





## Top 10 Vulnerabilities

Go to *Dashboard > Vulnerability Scan > Top 10 Vulnerabilities*. This chart lists the top ten vulnerabilities and affected endpoints.

Top 10 Vulnerabilities	
 Miscellaneous memory safety hazards (rv:25.0 / rv:24.1 / rv:17.0.10)	2 Hosts
 Miscellaneous memory safety hazards (rv:25.0 / rv:24.1 / rv:17.0.10)	2 Hosts
 Miscellaneous memory safety hazards (rv:27.0 / rv:24.3)	2 Hosts
 Miscellaneous memory safety hazards (rv:27.0 / rv:24.3)	2 Hosts
 Use-after-free when updating offline cache	2 Hosts
 Use-after-free when updating offline cache	2 Hosts
 Use-after-free when updating offline cache	2 Hosts
 Buffer overflows found through code inspection	1 Hosts
 Buffer underflow when generating CRMF requests	1 Hosts
 Buffer underflow when generating CRMF requests	1 Hosts

Clicking the vulnerability loads the FortiGuard page with detailed information about the vulnerability.

Clicking the number of hosts affected displays the endpoints affected by this particular vulnerability.

FortiClient Endpoint Management Server				
Affected Endpoints				
Hostname	Username	Last Seen	Scan Time	
 MKP-TSleeper	 Tony Sleeper	2019-04-22 17:13:56	2019-04-22 11:36:59	
 MKP-RWinchell	 Rickey Winchell	2019-04-22 17:13:56	2019-04-22 11:36:59	

# UX/Usability

## Endpoint policy

EMS now has an *Endpoint Policy* section for managing endpoint profile assignment. This dedicated policy page makes it simpler to provision endpoints. You can now create and manage endpoint policies to assign profiles and/or Telemetry gateway lists to domains, OUs, and workgroups. You can also create and manage Chromebook policies to assign profiles to Google domains.

### To add an endpoint policy for Windows, macOS, and Linux endpoints:

1. In EMS, go to *Endpoint Policy > Manage Policies*. Click *Add*.
2. In the *Endpoint policy name* field, enter the desired name.
3. In the *Endpoint domains* field, select the desired domain(s) and/or OU(s).
4. In the *Endpoint workgroups* field, select the desired workgroup(s).
5. From the *Endpoint profile* dropdown list, select the desired profile.
6. From the *Telemetry gateway list* dropdown list, select the desired Telemetry gateway list.

FortiClient Endpoint Management Server

Dashboard > Endpoint Policy > Manage Policies > Windows 10

Endpoint Policy

Endpoint policy name: Windows 10

Endpoint domains: fortinetqa.com/Computers

Endpoint workgroups: All Groups/Windows/Desktop/Windows 10

Endpoint profile: profile\_Windows10

Telemetry gateway list: FortiGate VM

Comments:

Enable the policy: ☒

Save Cancel

7. Save the policy. You can view the new policy on the *Endpoint Policy* page. You can view all policies on this page, as well as edit existing policies. EMS applies the policy (and its associated profile and Telemetry gateway list) to

the selected domain(s), OU(s), and workgroup(s).

Name	Endpoint Groups	Endpoint Profile	Telemetry Gateway List	Usage Count	Enabled
Windows 10	<ul style="list-style-type: none"> <li>fortinetqa.com/Computers</li> <li>All Groups/Windows/Desktop/Windows 10</li> </ul>	profile_Windows10	FortiGate VM	2	<input checked="" type="checkbox"/>
Window 8	<ul style="list-style-type: none"> <li>All Groups/Windows/Desktop/Windows 8</li> <li>earth.galaxy/Computers</li> </ul>	profile_Windows8	FortiWiFi 92D	2	<input checked="" type="checkbox"/>
Windows 10 External	All Groups/Windows/Desktop/External	profile_Windows10	FortiGate VM External	1	<input checked="" type="checkbox"/>
Android	All Groups/Linux/Android	profile_Android		1	<input checked="" type="checkbox"/>
Linux	All Groups/Linux	profile_Linux	FortiGate VM	1	<input checked="" type="checkbox"/>
MacOS	All Groups/MacOS	profile_MacOS	FortiGate VM External	1	<input checked="" type="checkbox"/>
iOS	All Groups/MacOS/iOS	profile_iOS		1	<input checked="" type="checkbox"/>
Servers	<ul style="list-style-type: none"> <li>All Groups/Windows/Server</li> <li>fortinetqa.com/Domain Controllers</li> <li>earth.galaxy/Domain Controllers</li> </ul>	WebFilter-JB		3	<input checked="" type="checkbox"/>
Deployment	<ul style="list-style-type: none"> <li>fortinetqa.com/Computers/Deployment</li> <li>All Groups/Windows/Deployment</li> </ul>	profile_Deployment		2	<input checked="" type="checkbox"/>

### To add an endpoint policy for Chromebook endpoints:

You can configure Chromebook policies only if you have enabled *EMS for Chromebooks Settings* in *System Settings* > *Server*.

1. In EMS, go to *Chromebook Policy* > *Manage Policies*. Click *Add*.
2. In the *Chromebook policy name* field, enter the desired name.
3. In the *Google domains* field, select the desired Google domain(s).
4. From the *Chromebook profile* dropdown list, select the desired Chromebook profile.

**FortiClient Endpoint Management Server**

**Chromebook Policy**

Chromebook policy name: Schoolzones

Google domains: schoolzones.ca

Chromebook profile: Schoolzones

Comments:

Enable the policy:

**Local Chromebook Profiles**

- Default - Chromebooks
- FortiClient
- Schoolzones

Save Cancel

5. Save the policy. You can view the new policy on the *Chromebook Policy* page. You can view all Chromebook policies on this page, as well as edit existing policies. EMS applies the policy (and its associated profile) to the selected domain(s).

Name	Chromebook Groups	Chromebook Profile	Usage Count	Enabled
Schoolzones	<ul style="list-style-type: none"> <li>schoolzones.ca</li> </ul>	Schoolzones	1	<input checked="" type="checkbox"/>
FortiClient	<ul style="list-style-type: none"> <li>fortinetqa.com</li> </ul>	FortiClient	1	<input checked="" type="checkbox"/>

# Other

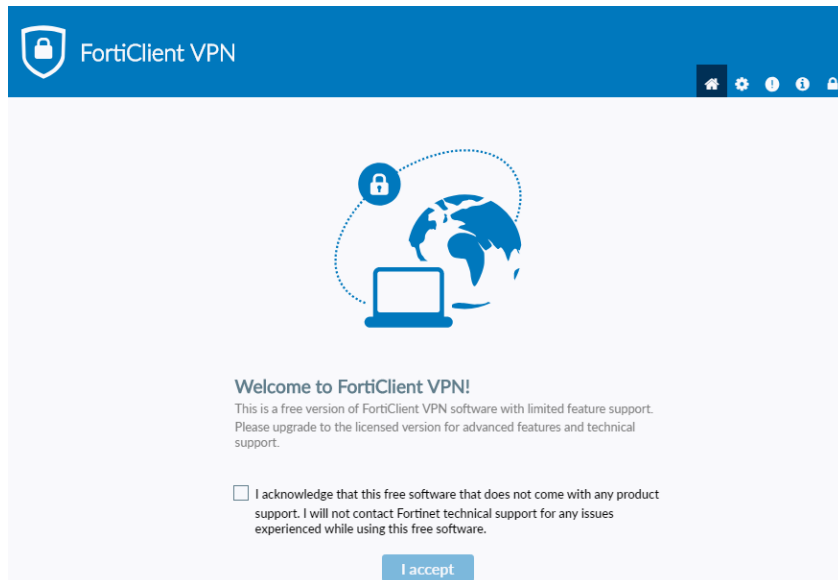
## Free VPN client

For FortiGate administrators, a free version of FortiClient VPN is available which supports basic IPsec and SSL VPN and does not require registration with EMS. This version does not include central management, technical support, or some advanced features.

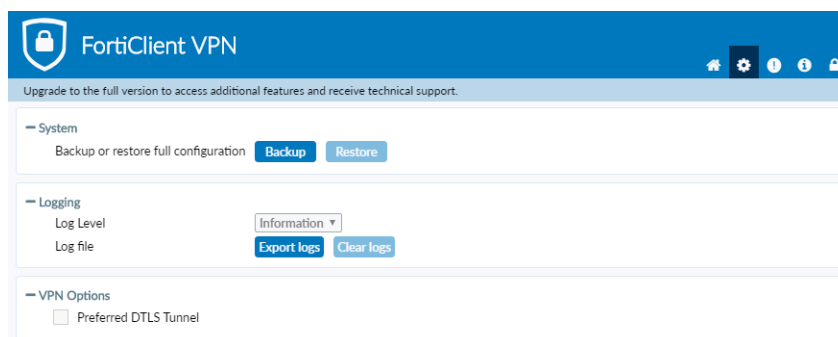
Full-featured FortiClient 6.2.0 requires registration to EMS. Each endpoint registered with EMS requires a license seat on EMS.

The FortiClient VPN installer differs from the installer for full-featured FortiClient.

When the free VPN client is run for the first time, it displays a disclaimer. You cannot configure or create a VPN connection until you accept the disclaimer:



Only the VPN feature is available. You can access the *Settings*, *About*, and *Notifications* pages from a toolbar.



Configuring settings for a new VPN connection on the free VPN client resembles doing the same on a full FortiClient installation:

You can establish a VPN connection from the homepage:

## CLI support for FortiClient (Linux)

FortiClient (Linux) now supports an installer targeted towards the headless version of Linux server. FortiClient (Linux) 6.2.0 for servers (forticlient\_server\_6.2.0.0xxx) offers a command line interface and is intended to be used with the CLI-only (headless) installation. The same set of CLI commands also work with a FortiClient (Linux) GUI installation.

The following summarizes the CLI commands available for FortiClient (Linux) 6.2.0:

## Endpoint control

FortiClient 6.2.0 must establish a Telemetry connection to EMS to receive license information. FortiClient features are only enabled after connecting to EMS.

### Usage

You can access endpoint control features through the `epctrl` CLI command. This command offers the end user the ability to connect or disconnect from EMS and check the connection status. You can access usage information by using the following commands:

```
jameslee@sunshine:~$ /opt/forticlient/epctrl -h
FortiClient Endpoint Control
```

Usage:

```
/opt/forticlient/epctrl -r|--register <address> [-p|--port ]
/opt/forticlient/epctrl -u|--unregister
/opt/forticlient/epctrl -d|--details
```

Options:

```
-h --help          Show the help screen
-r --register      Register to an EMS using the IP address
-p --port         EMS port
-u --unregister    Unregister from the current EMS
-d --details      Show telemetry details and status
```

### Connecting to EMS

FortiClient can connect to EMS using the following commands. If EMS is listening on the default port, 8013, you do not need to specify the port number. If EMS is listening on another port, such as 8444, you must specify the port number with the EMS address. The example illustrates both use cases:

```
jameslee@sunshine:~$ /opt/forticlient/epctrl -r 172.17.60.251
Registering to EMS 172.17.60.251:8013.
```

```
jameslee@sunshine:~$ /opt/forticlient/epctrl -r 172.17.60.251 -p 8444
Registering to EMS 172.17.60.251:8444.
```

### Endpoint control status

You can check FortiClient endpoint control status details with the `-d` argument. When FortiClient is connected to EMS only, the command output is as follows:

```
jameslee@sunshine:~$ /opt/forticlient/epctrl -d
=====
FortiClient EMS Details
=====
IP: 172.17.60.251:8013
Host: DESKTOP-ID2CVUA
SN: FCTEMS3764894213
Status: Connected
```



If FortiClient is connected to EMS and notifying FortiGate, the endpoint control status displays the serial numbers and hostnames of the EMS and FortiGates as follows:

```
jameslee@sunshine:~$ /opt/forticlient/epctrl -d
```

```
=====
```

```
FortiClient EMS Details
```

```
=====
```

```
IP: ems.fortinet.net:80
```

```
Host: DESKTOP-ID2CVUA
```

```
SN: FCTEMS3764894213
```

```
Status: Connected
```

```
=====
```

```
FortiGate Details
```

```
=====
```

```
IP: 172.17.60.40
```

```
Host: FGVM02TM18001119
```

```
SN: FGVM02TM18001119
```

```
Status: Connected
```

When FortiClient is not connected to EMS, the endpoint control status has no Telemetry data available as shown below:

```
jameslee@sunshine:~$ /opt/forticlient/epctrl -d
```

```
No telemetry data available.
```

## Disconnecting from EMS

FortiClient can disconnect from EMS only if the configuration received from EMS allows it. You can disconnect using the `-u` argument.

```
jameslee@sunshine:~$ /opt/forticlient/epctrl -u
```

```
Unregistering from EMS.
```

## AV scanning

You may run an AV scan from the CLI on the entire file system or on a specified directory. You can only run an AV scan as the root user. After completing an AV scan, FortiClient prints the scan results and detailed log file locations. You can run the following command to run an AV scan, where `<dir>` is the directory to scan. You can perform a full scan by inputting `/` in place of `<dir>`.

```
sudo /opt/forticlient/fmon -s /opt/forticlient/vir_sig/ -o /opt/forticlient/ --unit /opt/forticlient -d <dir>
```

The following shows an AV scan performed on the `/var` directory:

```
jameslee@sunshine:/var$ sudo /opt/forticlient/fmon -s /opt/forticlient/vir_sig/ -o /opt/forticlient/ --unit /opt/forticlient -d /var
```

```
Signature dir : /opt/forticlient/vir_sig/
```

```
Log dir : /opt/forticlient/
```

```
Fmon on daemon mode.
```

```
Dest dir : /var
```

```
CPU number : 1
```

```
Server port : 40140
```

```
AV Engine path : /opt/forticlient/libav.so
```

```
AV Signature path : /opt/forticlient/vir_sig/vir_high:/opt/forticlient/vir_sig/vir_sandbox_sig
```

```
Load AV signature success.
```

```

<=== PID : 13821 Client Hello rc = 2185
Child : 13821 ready
===> Scan : /var/spool/anacron/cron.daily
===> Scan : /var/spool/anacron/cron.weekly
===> Scan : /var/spool/anacron/cron.monthly
===> Scan : /var/crash/_usr_bin_gedit.1001.crash
===> Scan : /var/crash/_opt_forticlient_fmon.1000.crash
===> Scan : /var/backups/apt.extended_states.1.gz
===> Scan : /var/backups/shadow.bak
===> Scan : /var/backups/dpkg.statoverride.2.gz
===> Scan : /var/backups/passwd.bak
===> Scan : /var/backups/dpkg.diversions.1.gz
===> Scan : /var/backups/apt.extended_states.0
===> Scan : /var/backups/dpkg.arch.2.gz
===> Scan : /var/backups/alternatives.tar.1.gz
===> Scan : /var/backups/dpkg.arch.0
===> Scan : /var/backups/dpkg.status.1.gz
===> Scan : /var/backups/dpkg.statoverride.0
===> Scan : /var/backups/dpkg.arch.1.gz
===> Scan : /var/backups/gshadow.bak
===> Scan : /var/backups/dpkg.diversions.2.gz
===> Scan : /var/backups/alternatives.tar.2.gz
.....
.....
.....
----- scan_dispatch_worker finished -----

Scan started at Mon Apr 22 14:43:45 2019

Found virus : EICAR_TEST_FILE
In file : /var/eicar.com
Action : Quarantine success
Quarantine file : /opt/forticlient/quarantine/eicar.com.1

----- Scan summary -----
Total scan files : 10947
Found virus : 1
Worker crash : 0
Worker timeout : 0
-----

Scan ended at Mon Apr 22 14:44:01 2019

Full results can be found in /opt/forticlient/Daemon - Mon Apr 22 14:43:45 2019.log

```

## Vulnerability scanning

You can run a vulnerability scan from the CLI to check for vulnerable applications on the machine. You can only run a vulnerability scan as the root user. After completing a vulnerability scan, FortiClient prints the number of vulnerabilities present on the machine, their severity levels, and detailed log file locations. You can run a vulnerability scan by running the following command:

```

jameslee@sunshine:/home/jameslee$ sudo /opt/forticlient/vulscan -v /opt/forticlient/vcm_sig/ -
c -o /var/log/forticlient/vcm_log/
[INfo} Distribution name is Ubuntu
[INFO] Distribution version is 18.04.1 LTS (Bionic Beaver)
[INFO] LoadVulSig
[INFO] Decryption success!

```

```

[INFO] LoadFromDb
[INFO] Total sig : 13163
[INFO] Signature version=1.38
[INFO] Engine version=2.0.0.22
[INFO] Build install list
.....
.....
[INFO] Output directory: /var/log/forticlient/vcm_log/2019-04-18 18-45-42/
----- Scan summary -----
Critical : 7
High : 2
Medium : 7
Low : 0
-----

```

You can patch existing vulnerabilities using FortiClient. FortiClient runs a vulnerability scan again after patching the vulnerabilities and prints the results. You can patch vulnerabilities as below:

```

jameslee@sunshine:/home/jameslee$ sudo /opt/forticlient/vulscan -v /opt/forticlient/vcm_sig/ -
c -o /var/log/forticlient/vcm_log/ -p
[INFO] Distribution name is Ubuntu
[INFO] Distribution version is 18.04.1 LTS (Bionic Beaver)
[INFO] LoadVulSig
[INFO] Decryption success!
[INFO] LoadFromDb
[INFO] Total sig : 13163
[INFO] Signature version=1.38
[INFO] Engine version=2.0.0.22
[INFO] Build install list
...

Patching vid 55441
Hit:1 http://ca.archive.ubuntu.com/ubuntu bionic InRelease
Get:2 http://ca.archive.ubuntu.com/ubuntu bionic-updates InRelease [88.7 kB]
Get:3 http://security.ubuntu.com/ubuntu bionic-security InRelease [88.7 kB]
Get:4 http://ca.archive.ubuntu.com/ubuntu bionic-backports InRelease [74.6 kB]
Get:5 http://ca.archive.ubuntu.com/ubuntu bionic-updates/main amd64 DEP-11 Metadata [278 kB]
Get:6 http://security.ubuntu.com/ubuntu bionic-security/main amd64 DEP-11 Metadata [9,364 B]
Get:7 http://ca.archive.ubuntu.com/ubuntu bionic-updates/main DEP-11 48x48 Icons [66.7 kB]
Get:8 http://ca.archive.ubuntu.com/ubuntu bionic-updates/main DEP-11 64x64 Icons [123 kB]
Get:9 http://ca.archive.ubuntu.com/ubuntu bionic-updates/universe amd64 DEP-11 Metadata [222
kB]
Get:10 http://security.ubuntu.com/ubuntu bionic-security/main DEP-11 48x48 Icons [7,788 B]
Get:11 http://security.ubuntu.com/ubuntu bionic-security/universe amd64 DEP-11 Metadata [35.7
kB]
Get:12 http://ca.archive.ubuntu.com/ubuntu bionic-updates/universe DEP-11 48x48 Icons [194 kB]
Get:13 http://security.ubuntu.com/ubuntu bionic-security/universe DEP-11 48x48 Icons [16.4 kB]
Get:14 http://security.ubuntu.com/ubuntu bionic-security/universe DEP-11 64x64 Icons [92.2 kB]
Get:15 http://ca.archive.ubuntu.com/ubuntu bionic-updates/universe DEP-11 64x64 Icons [406 kB]
Get:16 http://ca.archive.ubuntu.com/ubuntu bionic-updates/multiverse amd64 DEP-11 Metadata
[2,468 B]
Get:17 http://security.ubuntu.com/ubuntu bionic-security/multiverse amd64 DEP-11 Metadata
[2,464 B]
Get:18 http://ca.archive.ubuntu.com/ubuntu bionic-backports/universe amd64 DEP-11 Metadata
[7,352 B]
Fetched 1,716 kB in 3s (591 kB/s)
Reading package lists... Done

```

```

[INFO] install command is: apt-get -y install --only-upgrade firefox
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
fonts-lyx
The following packages will be upgraded:
firefox
1 upgraded, 0 newly installed, 0 to remove and 315 not upgraded.
Need to get 0 B/48.1 MB of archives.
After this operation, 7,509 kB of additional disk space will be used.
(Reading database ... 162206 files and directories currently installed.)
Preparing to unpack ../firefox_66.0.3+build1-0ubuntu0.18.04.1_amd64.deb ...
Unpacking firefox (66.0.3+build1-0ubuntu0.18.04.1) over (59.0.2+build1-0ubuntu1) ...
Processing triggers for mime-support (3.60ubuntu1) ...
Processing triggers for desktop-file-utils (0.23-1ubuntu3.18.04.1) ...
Setting up firefox (66.0.3+build1-0ubuntu0.18.04.1) ...
Installing new version of config file /etc/apparmor.d/usr.bin.firefox ...
Please restart all running instances of firefox, or you will experience problems.
Processing triggers for man-db (2.8.3-2) ...
Processing triggers for gnome-menus (3.13.3-11ubuntu1) ...
Processing triggers for hicolor-icon-theme (0.17-2) ...
[INFO] query command is: dpkg-query --show firefox
Package version found is 66.0.3+build1-0ubuntu0.18.04.1

Patching vid 55442
Hit:1 http://security.ubuntu.com/ubuntu bionic-security InRelease
Hit:2 http://ca.archive.ubuntu.com/ubuntu bionic InRelease
Hit:3 http://ca.archive.ubuntu.com/ubuntu bionic-updates InRelease
Hit:4 http://ca.archive.ubuntu.com/ubuntu bionic-backports InRelease
Reading package lists... Done
.....
.....
.....
----- Scan summary -----
Critical : 0
High : 0
Medium : 0
Low : 0
-----

```

## FortiClient updates

You can run a FortiClient update task from the CLI once FortiClient has connected to EMS and is licensed. The update task downloads the latest FortiClient engine and signatures. You can only run an update task as the root user. The command and its output are shown below:

```

root@sunshine:/home/jameslee# /opt/forticlient/update

*****Update starting*****
Sandbox test = 0
Sandbox host to test = (null)
log_level: 6
Enable custom fds server :80 failover port: 8000 failover to fdg: 1 allow sw update: 0
Updating FCTDATA: Update started forced update
[INFO] Engine version=2.0.0.22
[INFO] Distribution name is Ubuntu

```

```
[INFO] Distribution version is 18.04.1 LTS (Bionic Beaver)
[INFO] LoadVulSig [INFO] Decryption success!
[INFO] LoadFromDb [INFO] Total sig : 13163
[INFO] Signature version=1.38
Getting current FortiClient Components information
current av engine version: 6.2.126
av engine id: 06002000FVEN04100-00006.00126-9999999999
current av main sig full version: 67.1895
av main sig id: 06002000FVDB04000-00067.01895-9999999999
current av ext sig full version: 67.1892
...
...
user jameslee, type:7, session:0, pid:6913
user = jameslee
sandbox server not configured.
Updating FCTDATA: Update finished
[INFO] Engine version=2.0.0.22
[INFO] Distribution name is Ubuntu
[INFO] Distribution version is 18.04.1 LTS (Bionic Beaver)
[INFO] LoadVulSig
[INFO] Decryption success!
[INFO] LoadFromDb
[INFO] Total sig : 13163
[INFO] Signature version=1.38
Downloading done ret = 0
root@sunshine:/home/jameslee#
```

## Existing signature details

You can check details of the existing FortiClient engine and signatures by running the update task with the `-d` argument:

```
jameslee@sunshine:/home/jameslee$ /opt/forticlient/update -d

=====
Engines
=====
AntiVirus: 6.2.00126
Vulnerability: 2.00022

=====
Signatures
=====
AntiVirus: 67.01895
AntiVirus Extended: 67.01892
Vulnerability: 1.00038
Sandbox: 3.00442
```

## Update help

The update help option lists all options available for the update task. You can access this option as shown below:

```
jameslee@sunshine:~$ /opt/forticlient/update -h
FortiClient Update
```

## Usage:

```
/opt/forticlient/update
/opt/forticlient/update -d
```

## Options:

```
-h Show the help screen
-d Show engine and signature versions
```

## Installer creation enhancements

The EMS installer wizard has been improved so that administrators can now create custom FortiClient installers in a manner similar to the FortiClient Configurator Tool.

You can create deployment packages to deploy FortiClient to endpoints. Deployment packages include the FortiClient installer, which determines the FortiClient release and patch to install on the endpoint, as well as which FortiClient features are installed on the endpoint. Deployment packages can also include a Telemetry gateway list for connection to a FortiGate.

*Manage Installers > FortiClient Installers* displays FortiClient installers available from FortiGuard and uploaded custom FortiClient installers. These installers are available for selection when creating a FortiClient deployment package. EMS automatically connects to FortiGuard to provide access to FortiClient installers that you can use with EMS profiles. If a connection to FDN is not available, you must manually download FortiClient installers to use with EMS.

You can download FortiClient installers to use with EMS from Fortinet Customer Service & Support. This requires a support account with a valid support contract. Download the Windows, macOS, or Linux installation file.

### To add a custom FortiClient installer:

All uploaded Windows installers must be .msi or .zip files. All uploaded macOS installers must be .dmg files.

1. Download a FortiClient installer. You can also upload a previously customized installer.
2. Upload the custom installation files:
  - a. Go to *Manage Installers > FortiClient Installers*.
  - b. Click *Add*. The *Add FortiClient Installer* dialog displays.
  - c. Set the following options:

<b>Name</b>	Enter a name for the set of installation files.
<b>Upload Windows Installers</b>	Enable to upload FortiClient installers for the Windows operating system.
<b>Windows 64-Bit Installer (ZIP or MSI)</b>	Click the <i>Browse</i> button to locate and select a custom 64-bit installer for the Windows operating system.
<b>Windows 32-Bit Installer (ZIP or MSI)</b>	Click the <i>Browse</i> button to locate and select a custom 32-bit installer for the Windows operating system.
<b>Upload Mac Installer</b>	Enable to upload a FortiClient installer for the macOS operating system.
<b>Mac Installer (DMG)</b>	Click the <i>Browse</i> button to locate and select a custom installer for the macOS operating system.

- d. Click *Upload*. The custom installers are uploaded to EMS.

**To add a FortiClient deployment package:**

1. Go to *Manage Installers > Deployment Packages*.
2. Click *Add*.
3. On the *Version* tab, set the following options:

<b>Installer Type</b>	Configure the deployment package to use an official FortiClient installer or a custom FortiClient installer.
<b>Release</b>	Select the FortiClient release version to install.
<b>Patch</b>	Select the specific FortiClient patch version to install.
<b>Keep updated to the latest patch</b>	Select to enable FortiClient to automatically update to the latest patch release when FortiClient is installed on an endpoint.

4. On the *General* tab, set the following options:

<b>Name</b>	Enter the FortiClient installer's name.
<b>Notes</b>	(Optional) Enter any notes about the FortiClient installer.

5. Click *Next*. On the *Features* tab, set the following options:

<b>Security Fabric Agent (Mandatory Feature)</b>	Enabled by default and cannot be disabled. Installs FortiClient with Telemetry and Vulnerability Scan enabled.
<b>Secure Access Architecture Components</b>	Enable to install FortiClient with SSL and IPsec VPN enabled. Disable to omit SSL and IPsec VPN support from the FortiClient deployment package.
<b>Advanced Persistent Threat (APT) Components</b>	Enable to install FortiClient with APT components enabled. Disable to omit APT components from the FortiClient installer. Includes FortiSandbox detection and quarantine features.
<b>Additional Security Features</b>	<p>Enable to select one, two, or all of the following features:</p> <ul style="list-style-type: none"> <li>• AntiVirus</li> <li>• Web Filtering</li> <li>• Application Firewall</li> <li>• Single Sign-On mobility agent</li> <li>• Cloud Based Malware Outbreak Detection</li> </ul> <p>Disable to exclude the features from the FortiClient installer.</p>

6. Click *Next*. On the *Advanced* tab, set the following options:

<b>Enable automatic registration</b>	Enable to configure FortiClient to automatically connect Telemetry to EMS after FortiClient is installed on the endpoint. Disable to turn off this feature and require endpoint users to manually connect Telemetry to EMS.
<b>Enable desktop shortcut</b>	Enable to configure the FortiClient installer to create a desktop shortcut on the endpoint.
<b>Enable start menu shortcut</b>	Enable to configure the FortiClient installer to create a Start menu shortcut on the endpoint.

- 7.

**Enable Installer ID**

Enable to configure an installer ID. Select an existing installer ID or enter a new installer ID. If creating an installer ID, select a group path or create a new group in the *Group Path* field. EMS automatically groups endpoints according to installer ID group assignment rules.

This option is not available when the FortiClient installer selected or uploaded in step 3 is a version prior to 6.0.0.

**Enable Endpoint Profile**

Enable to select an endpoint profile to include in the installer. The profile is applied to the endpoint once it has installed FortiClient. This option is necessary if it is required to have certain security features enabled prior to contact with EMS, or if users require VPN connection to connect to EMS.

8. Click *Next*. The *Telemetry* tab displays the hostname and IP address of the EMS server, which will manage FortiClient once it is installed on the endpoint. Also configure the following option:

**Enable telemetry connection to Security Fabric (FortiGate)**

Enable this option, and select the name of the gateway list to use. The gateway list defines the IP address for the FortiGate.

If you have not created a gateway list, this option is not available.

9. Click *Finish*. The FortiClient installer is added to EMS and displays on the *Manage Installers > Deployment Packages* pane.

FortiClient Endpoint Management Server

Dashboard

Endpoints

Google Domains

Quarantine Management

Software Inventory

Endpoint Policy

Chromebook Policy

Endpoint Profiles

Manage Installers

Deployment Packages

Delete






Add

Refresh

Name	Versions	Auto Update	Download Link
FortiClient 6.0.5 GA	6.0.5 6.0.5	<input checked="" type="checkbox"/>	https://ems1.fortinetqa.com:18443/Installers/FortiClient_6.0.5_GA
FortiClient 6.2.0 GA	6.2.0 6.2.0	<input checked="" type="checkbox"/>	https://ems1.fortinetqa.com:18443/Installers/FortiClient_6.2.0_GA
FortiClient Latest Build	6.2.0	<input checked="" type="checkbox"/>	https://ems1.fortinetqa.com:18443/Installers/FortiClient_Latest_Build
Features	<ul style="list-style-type: none"><li>• AntiVirus</li><li>• Web Filtering</li><li>• Secure Access Architecture Components</li><li>• Application Firewall</li><li>• Security Fabric Agent</li><li>• Advanced Persistent Threat (APT) Components</li><li>• Single Sign-On mobility agent</li><li>• Cloud Based Malware Outbreak Detection</li></ul>		
Endpoint Profile	Default		
FortiClient Installers	Telemetry Gateway List		
Profile Components	FortiGate External		
Telemetry Gateway Lists	Telemetry Connection to FortiGate		
Compliance Verification	Managed by EMS		
Administration	Auto Registration		
System Settings	Desktop Shortcut		
	Start Menu Shortcut		
	Installer ID		
	Notes		

The deployment package may include .exe (32-bit and 64-bit), .msi, and .dmg files depending on the configuration. The following shows an example of a deployment package that includes .exe, .msi, and .dmg files. The end user can download these files to install FortiClient on their machine with the desired configuration.



Name	Last modified	Size
 Parent Directory		-
 msi/	2019-04-29 15:00	-
 FortiClient_6.2.0.DMG	2019-04-29 15:21	76M
 FortiClientSetup_6.2.0_x64.exe	2019-04-29 15:22	108M
 FortiClientSetup_6.2.0_x86.exe	2019-04-29 15:21	90M

## Administrator settings improvements

EMS 6.2.0 introduces five major improvements to administrator settings:

- Support for three types of administrators
- Support for multiple LDAP servers
- Permission management based on administrator roles
- Categorized and refined administrator permissions
- Restricting login to trusted hosts

### Support for three types of administrators

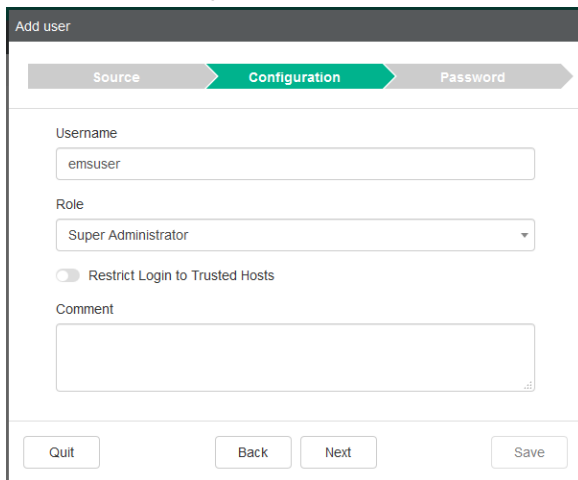
Administrators can be one of three types of users:

User type	Description
EMS	Created in EMS. This includes the built-in "admin" user.
Windows	Created by the local Windows system.
LDAP	Imported from the domain server.

**To create an EMS administrator:**

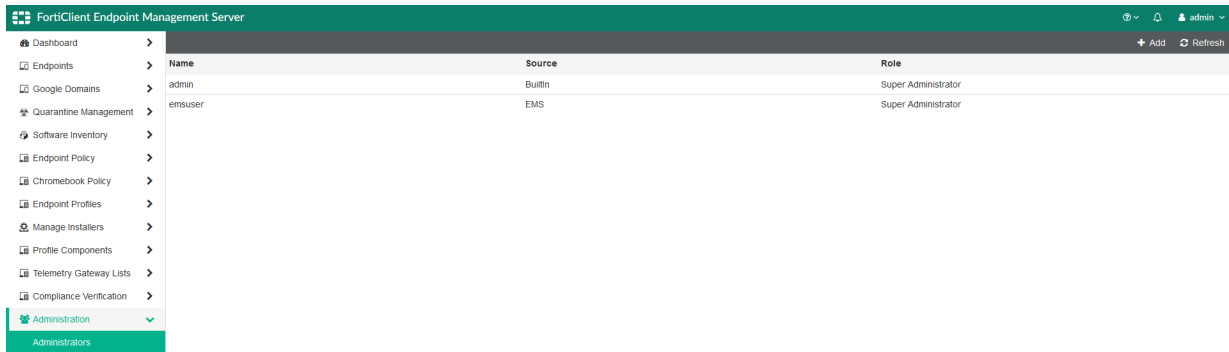
1. Go to *Administration > Administrators*. Click *Add*.
2. Under *User Source*, select *Create a new user*. Click *Next*.
3. In the *Username* field, enter the desired username.

4. From the *Role* dropdown list, select the desired role. Click *Next*.



The screenshot shows the 'Add user' dialog box with the 'Configuration' tab selected. The 'Username' field contains 'emsuser'. The 'Role' dropdown menu is set to 'Super Administrator'. There is an unchecked checkbox for 'Restrict Login to Trusted Hosts'. The 'Comment' field is empty. At the bottom, there are buttons for 'Quit', 'Back', 'Next', and 'Save'.

5. On the *Password* tab, create a password for the user. Click *Save*. Once you save the user, you can view the created user on the *Administration > Administrators* pane. The *Source* is listed as *EMS*.



The screenshot shows the FortiClient Endpoint Management Server interface. The left sidebar lists various management options, with 'Administration' and 'Administrators' highlighted. The main pane displays a table of administrators.

Name	Source	Role
admin	Builtin	Super Administrator
emsuser	EMS	Super Administrator

## Support for multiple LDAP servers

You can configure multiple LDAP servers on EMS to import users from.

## To configure an LDAP server:

1. Go to *Administration > User Servers*. Click *Add*.
2. Enter the domain credentials. Click *Test*. Once the test is successful, click *Save*.

**FortiClient Endpoint Management Server**

**User Server**

IP address/Hostname: 172.17.61.196

Port: 389

Distinguished name: Optional

Bind type: Simple Anonymous **Regular**

Username: qa

Password: .....

LDAPS connection: ☐

Sync every: 10 Minutes

**Test** **Cancel**

In this example, after EMS imports the LDAP server successfully, the *Administration > User Servers* pane lists two imported LDAP servers.

**FortiClient Endpoint Management Server**

Domain Name	NetBIOS Name	User Count	Last Sync	Sync Every	Address	Distinguished Name	Username
qa.fortinet.local	QA	20	2019-05-24 11:38:53	10 minutes	172.17.61.196:389	DC=qa,DC=fortinet,DC=local	qa
fortinet.local	FORTINET	20040	2019-05-24 11:46:06	10 minutes	172.17.61.48:389	DC=fortinet,DC=local	qa

## Permission management based on administrator roles

You can use administrator roles to manage permissions. There are four predefined roles configured with different permissions:

Name	Description
Super administrator	Most privileged admin role. Complete access to all EMS permissions, including modification, user permissions, approval, discovery, and deployment. Only built-in role that has access to the Administration section of the GUI. Has access to all configured Windows and LDAP servers and users and has the authority to configure user privileges and permissions.

Name	Description
	The default admin account is configured as a Super Administrator and cannot be changed to another admin role.
Standard administrator	Includes all endpoint and policy permissions, and read-only permissions to settings permissions.
Endpoint administrator	Includes all endpoint permissions and read-only permissions to policy and settings permissions.
Restricted administrator	No permissions enabled.

You can also define a new role with customized permissions.

**To define a custom admin role:**

1. Go to *Administration > Admin Roles*. Click *Add*.
2. In the *Name* field, enter the desired name.
3. Select the desired permission checkboxes.
4. Click *Save*. The role appears on the *Administration > Admin Roles* pane.

## Categorized and refined administrator permissions

When creating or modifying an admin role, all available permissions are categorized into endpoint, policy, and setting permissions. Permissions for new features include permissions related to endpoint policies, host verification, quarantine management, and software inventory.

You can click *Click here to hide permissions that are not applicable to Chromebook management* to view permissions that only apply to Windows, macOS, and Linux endpoint management.

FortiClient Endpoint Management Server

Dashboard

Endpoints

Google Domains

Quarantine Management

Software Inventory

Endpoint Policy

Chromebook Policy

Endpoint Profiles

Manage Installers

Profile Components

Telemetry Gateway Lists

Compliance Verification

Administration

Administrators

Admin Roles

User Servers

User Settings

Back up Database

Restore Database

Configure License

Logs

System Settings

Some permissions do NOT apply to Chromebook management. [Click here to hide permissions that are not applicable to Chromebook management](#)

Admin Role

Name

Required

Description

Enter the description here...

0/1024

Endpoint permissions (0/14)

☐ Manage LDAPs
☐ Manage custom groups
☐ Block/Unblock/Quarantine/Unquarantine/Reregister endpoints
☐ View group assignment rules
☐ View endpoint filter bookmarks
☐ View quarantine management
☐ View software inventory

☐ Manage Google domains
☐ Run commands on endpoints
☐ Manage and assign endpoint policies
☐ Manage group assignment rules
☐ Manage endpoint filter bookmarks
☐ Manage quarantine management
☐ Manage software inventory

Policy permissions (0/11)

☐ View endpoint policies
☐ Manage endpoint profiles
☐ Manage host verification rules
☐ Manage gateway lists
☐ Manage installers
☐ Manage CA certificates

☐ View endpoint profiles
☐ View host verification rules
☐ View gateway lists
☐ View installers
☐ View CA certificates

Setting permissions (0/12)

☐ View server settings
☐ View FortiGuard settings
☐ View endpoint settings
☐ View login banner settings
☐ View alert settings
☐ View custom message settings

☐ Manage server settings
☐ Manage FortiGuard settings
☐ Manage endpoint settings
☐ Manage login banner settings
☐ Manage alert settings
☐ Manage custom message settings

## Restricting login to trusted hosts

With the Trusted Hosts feature, you can allow remote access to EMS only on defined trusted hosts. You can define a trusted host using an IPv4 or IPv6 address or a fully qualified domain name (FQDN).

### To define trusted hosts:

1. Go to *Administration > Administrators*.
2. Create a new administrator or modify an existing administrator.

### 3. Enable *Restrict Login to Trusted Hosts*.

User configuration form showing the following details:

- User: emsuser
- Role: Super Administrator
- ☒ Restrict Login to Trusted Hosts
- Trusted Hosts: 172.17.60.93
- Comment: FortiClient QA Desktop 1

### 4. In the *Trusted Hosts* field, enter an IPv4 or IPv6 address or an FQDN. If desired, you can enter multiple hosts using the + button. The trusted host details appear on the administrator page.

Name	Source	Role
admin	Builtin	Super Administrator
emsuser	EMS	Super Administrator

Name	Type
emsuser	EMS

Role	Trusted hosts	Last login or activation	Comments
Super Administrator	172.17.60.93/32	2019-05-24 10:48	FortiClient QA Desktop 1

## Automatic license retrieval from FortiCare

When newly installed, EMS is not licensed, and FortiClient cannot connect to it. You must purchase a license through FortiCare. You can use one of two methods to apply the newly acquired license on EMS:

- Provide the FortiCare account information on EMS
- Download the license from FortiCare and upload it to EMS. This method is the same as earlier versions of EMS. You can also use this method in combination with providing the FortiCare account information on EMS.

When you provide the FortiCare account information on EMS, EMS retrieves the license file from FortiCare and applies it locally. When the license expires, EMS contacts FortiCare during the grace period to check for a license renewal, and, if available, downloads the new license.

#### To activate and retrieve the license from FortiCare:

1. Go to *Administration > Configure License*.
2. Under *License Source*, select *FortiCare*.

3. Do one of the following:
  - a. If you do not have a FortiCare account, click *Create Account* to create a FortiCare account. Enter your new login credentials in the *Account ID/Email* and *Password* fields.
  - b. If you have a FortiCare account, enter your login credentials in the *Account ID/Email* and *Password* fields.
4. Log into your FortiCare account to purchase the EMS license. You can view all of your license entitlements in FortiCare.

Customer Service & Support Home **Asset** Assistance Download Feedback 154750 Fortinet Inc

**Product Details** FortiClient EMS  
FCTEMS0000097193

FortiClient Fabric Agent Will Expire On **2020-02-27**

[Back To List](#)

**Information**

- General
- Location
- Entitlement**
- License & Key

**Registration**

- Renew Contract**

**Assistance**

- Ticket List
- Technical Request
- Customer Service
- DOA/RMA Request
- Anti Virus Ticket
- FortiConverter Service Ticket

**Product Entitlements**

Support Coverage

Support Type	Support Level	Activation Date	Expiration Date
FortiClient Fabric Agent	Web/Online	2019-02-27	2020-02-27
FortiClient Sandbox	Web/Online	2019-02-27	2020-02-27
FortiClient Chrome	Web/Online	2019-03-06	2020-03-05

Registered Support Contract

Contract Number	SKU	Creation Date	Registration Date	Units of Contract
555777591240	FC-15-EMS01-203-02-12	2018-09-23	2019-03-06	100
555777555808	FC-15-EMS01-199-02-12	2018-09-23	2019-02-27	100

5. In EMS, on the *Administration > Configure License* page, click *Update License*. EMS downloads the license from FortiCare. If the FortiCare account credentials change, you can click *Edit Account* to update the credentials. You can also click *Delete Account* to remove FortiCare credentials from EMS.

**FortiClient Endpoint Management Server**

Dashboard Endpoints Quarantine Management Software Inventory Endpoint Policy Endpoint Profiles Manage Installers Profile Components Telemetry Gateway Lists Compliance Verification **Administration** Administrators Admin Roles User Servers User Settings Back up Database Restore Database **Configure License**

FortiCare account created successfully. License updated successfully.

**Configure License**

Serial number FCTEMS0000097193

Hardware ID AA847FFF-3645-4CCD-A4DC-D5053EBE6F14-B339435C

Fabric Agent with Endpoint Protection Licensed 2020-02-27

Sandbox Cloud Licensed 2020-02-27

FortiClient Licenses Used 0 out of 100

Chromebook Licensed 2020-03-05

Chromebook Licenses Used 0 out of 100

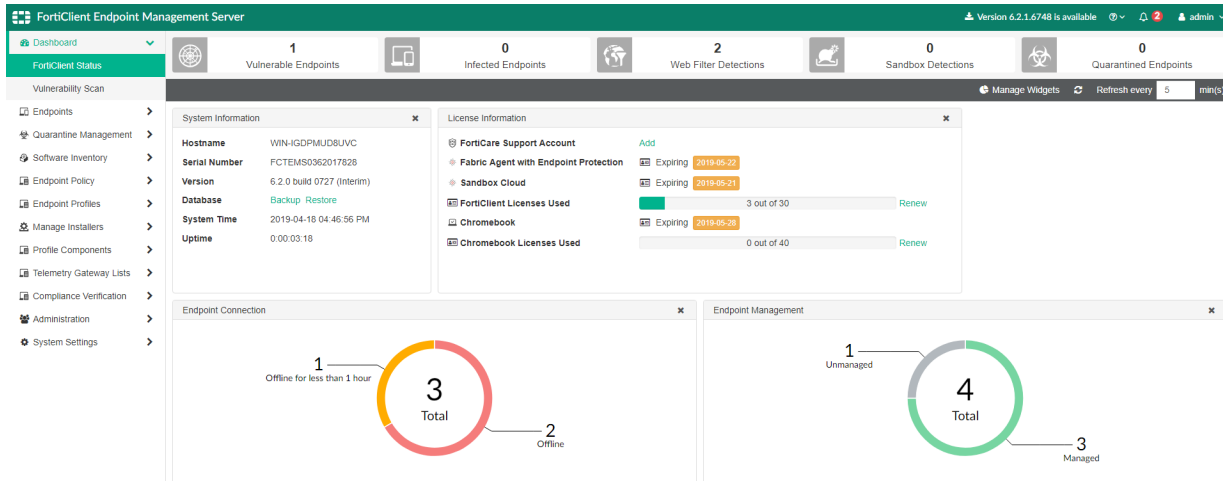
License Source **FortiCare** File Upload

FortiCare Support Account ledington@smartgrid.ca

**Update License** **Edit Account** **Delete Account** **Cancel**

## Renaming of FortiClient EMS

FortiClient EMS has been renamed to FortiClient Endpoint Management Server. This is reflected on the login page, banner, installer file name, and so on.



## Automatic group assignment

EMS 6.0.0 introduced the automatic group assignment feature to dynamically group endpoints based on user-defined automatic group assignment rules. This feature minimizes the process to manually create or move endpoints to custom groups, as EMS automatically moves endpoints to preassigned groups based on rules and their priority levels. EMS 6.2.0 adds support for two additional rule types: OS and AD group.

You can apply OS rules on endpoints in workgroups and AD group rules on endpoints in AD groups. You can configure one or multiple rules, but EMS applies only the first applicable rule to an endpoint. You can view the priority level for each rule in *Endpoints > Group Assignment Rules*.

### To configure an OS group assignment rule:

1. Go to *Endpoints > Group Assignment Rules*. Click *Add*.
2. In the *Group Assignment Rule* window, from the *Type* dropdown list, select *OS*.
3. In the *OS* field, enter the desired OS.
4. From the *Group* dropdown list, select or create the desired group. Click *Save*. This rule identifies the endpoint's OS version, and, if there is a match, places the endpoint in the configured group.

### To configure an AD group assignment rule:

You can use AD groups to categorize users into different groups and move endpoints into preassigned custom groups. EMS can then easily apply different policies in a domain.

1. Go to *Endpoints > Manage Domains*. Click *Add*.
2. Configure the desired domain to import.
3. Go to *Endpoints > Group Assignment Rules*. Click *Add*.



4. In the *Group Assignment Rule* window, from the *Type* dropdown list, select *AD Group*.
5. From the *AD Group* dropdown list, select the desired group.
6. From the *Group* dropdown list, select or create the desired custom group. Click *Save*.

Group Assignment Rule

Type: AD Group

AD Group: Users/Sales Department

Group: qa/Sales Department

Enable Rule: ☒

Save Cancel

7. Go to *Endpoints > Group Assignment Rules* to view the newly created rule.

Rule	Group	Priority	Enabled
Sales Department	Sales Department	1	<input checked="" type="checkbox"/>
Users/Sales Department	qa/Sales Department	2	<input checked="" type="checkbox"/>

Whenever an AD user logs in, FortiClient sends user login information to EMS. EMS checks the login information against the AD group rules and moves endpoints into custom groups accordingly. The custom group that EMS assigns an endpoint to depends on the AD group that the logged in user currently belongs to.

In the following example, the AD user, Dennis Auger, belongs to the Users/Sales Department AD group. Whenever Dennis logs in, EMS assigns the endpoint to the Sales Department group in the qa.fortinet.local domain.

FortiClient Endpoint Management Server

Endpoint: dennis.auger

IP: 192.168.10.204

Profile: Default

Managed by EMS

Status: Registered

Features: ☒

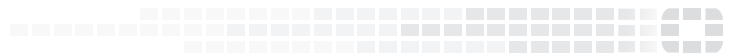
You can use the *Schedule Run* and *Run Rules Now* buttons in *Endpoints > Group Assignment Rules* to periodically or immediately run rules to adapt to endpoint changes, such as IP address or logged-in AD user changes.

# Change log

Date	Change Description
2019-04-16	Initial release.
2019-04-26	Added <a href="#">Endpoint policy</a> on page 28.
2019-04-29	Added <a href="#">FortiSandbox</a> support for FortiClient (macOS) on page 17 and Automatic license retrieval from FortiCare on page 46.
2019-05-06	Added <a href="#">Client handling for HTTPS (browser plugin)</a> for Google Chrome browser on page 14, <a href="#">CLI support for FortiClient (Linux)</a> on page 31, <a href="#">Vulnerability dashboard</a> on page 23, and <a href="#">Renaming of FortiClient EMS</a> on page 48.
2019-05-07	Added <a href="#">Automated syncing of the FortiGate Web Filter profile</a> on page 12.
2019-05-08	Updated <a href="#">Installer creation enhancements</a> on page 38.
2019-05-27	Updated <a href="#">Administrator settings improvements</a> on page 41.
2019-06-27	Added <a href="#">Cloud-based threat detection</a> on page 20.
2019-07-08	Added <a href="#">Automatic group assignment</a> on page 48.
2019-10-28	Updated <a href="#">Dynamic endpoint grouping/tagging and EMS connector (endpoint compliance)</a> on page 4.
2020-06-01	Updated <a href="#">CLI support for FortiClient (Linux)</a> on page 31.



**FORTINET®**



Copyright© 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.