

# Forticlient EMS Server & forticlient OPSDOC

## Overview

Antimalware software on every machine is a must these days. This anti malware solution should be manageable from a central server. The users shouldn't be able to disable the antimalware protection. We choose for the professional endpoint security management from Fortinet. This solution includes:

- Forticlient Endpoint Management Server (server for performing remote scans and remotely management for the endpoint like servers and computers)
- Forticlient client installation for interaction with the EMS server

This Forticlient solution provided our servers with:

- Application Firewall
- Webfilter
- Protection against botnets, zero-day malware,...
- Real time reporting and patching of vulnerabilities
- Real time Malware and antivirus protection
- For more specific details visit: [www.forticlient.com/](http://www.forticlient.com/)

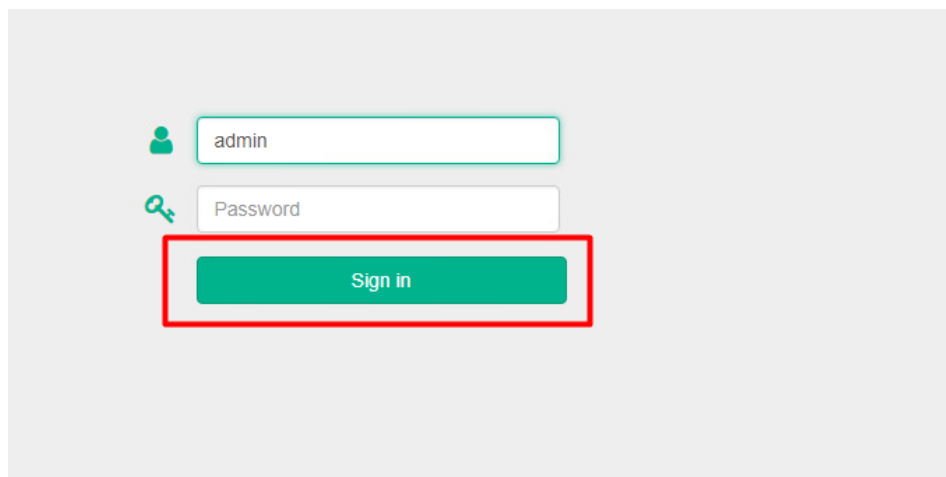
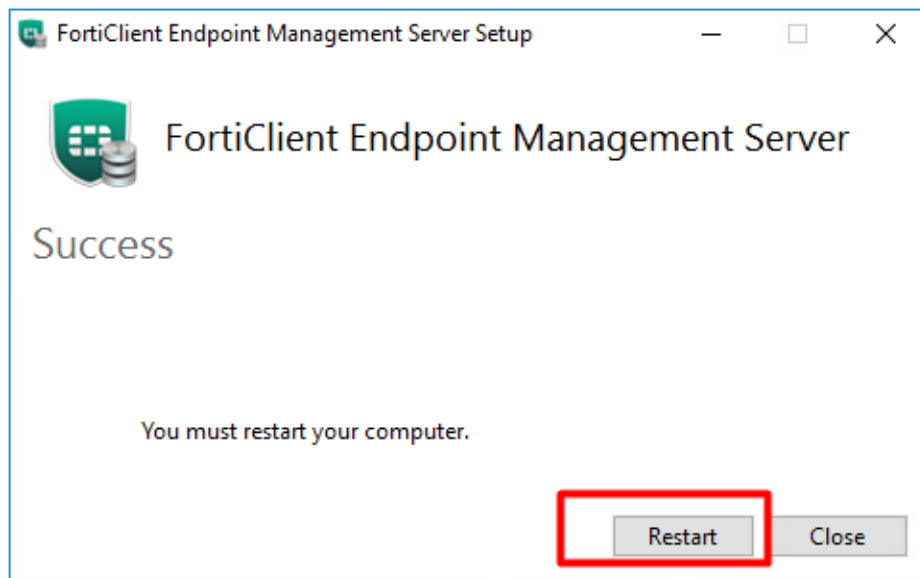
Bugs and problems can be reported using the bug tracker or the ticketing system. The guide for using these systems can be found in the OPSDoc bundle.

The primary contact person for this service is: Brent De Vos

## Prerequisites

- Windows server 2016 or newer virtual machine

## Installation



sign in with admin and the credentials you will find in the password safe.

## Forticlient client installation on ubuntu servers

```
ccs2@opensupport:~/forticlient$ wget http://172.27.66.125/forticlient_6.2.6.0356_amd64.deb
```

wget the custom .deb installation file from our own webserver using the command above.

```
sudo apt-get install /home/ccs2/forticlient/forticlient_6.2.6.0356_amd64.deb
```

Install .deb file

```
sudo /opt/forticlient/epctrl -r 172.27.66.124
```

Connect the machine to the endpoint management server using the ip address of the server.

```
ccs2@opensupport:~/forticlient$ sudo /opt/forticlient/epctrl -r 172.27.66.124
Registering to EMS 172.27.66.124:8013.
Connected!
```

You should get the 'Connected!' message. This machine is now succesfully connected to the EMS server.





For more information about the 'epctrl' command and the usage visit the website bellow:

<https://docs.fortinet.com/document/forticlient/6.2.0/administration-guide/41299/appendix-e-forticlient-linux-cli-commands>

## Forticlient client installation on windows servers

Browse with the webbrowser on the windows server to:

<https://172.27.66.124:10443/installers/win> installers

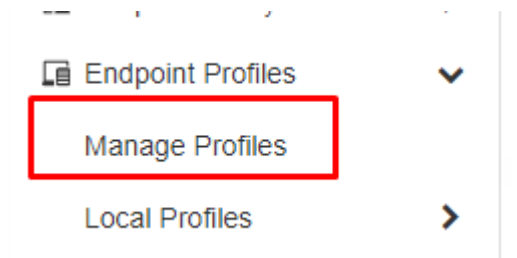
Name	Last modified	Size
 Parent Directory		-
 msi/	2020-05-13 12:53	-
 FortiClient_6.4.0.dmg	2020-05-13 12:55	84M
 FortiClientSetup_6.4.0_x64.exe	2020-05-13 12:53	123M
 FortiClientSetup_6.4.0_x86.exe	2020-05-13 12:53	101M

Download and run the x64.exe installation file. This is a customized installation file. The win client is after this installation automatically registered to our EMS server.

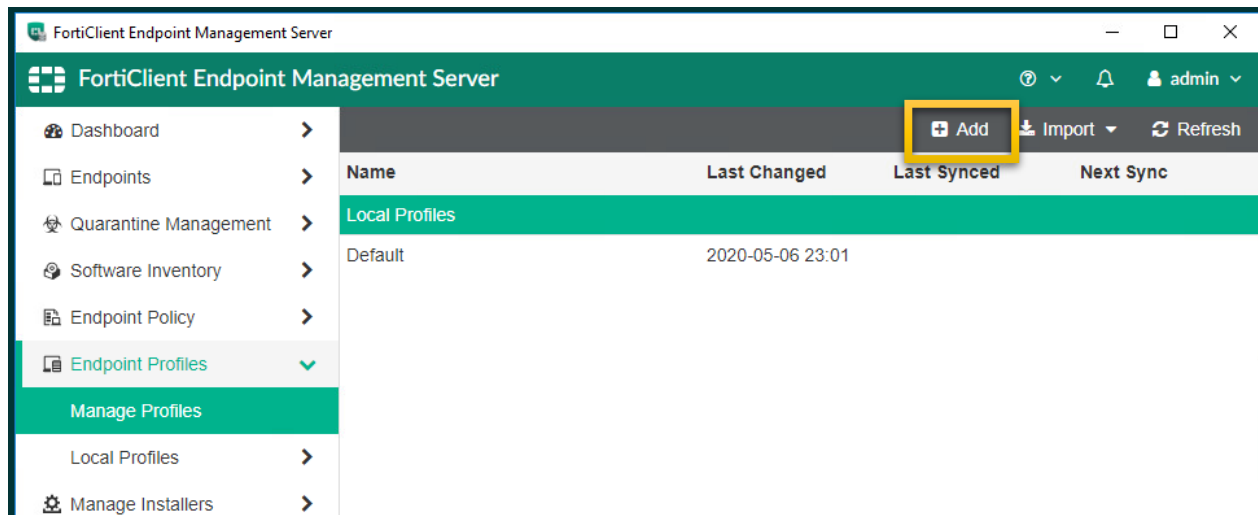
All of our registered clients appear in the all endpoints overview:

opensupport All Groups/Other Endpoints	(none)	172.27.66.123	Policy T02ServersPolicy	EMS	No Events
puppet All Groups/Other Endpoints	ccs2	172.27.66.122	Policy T02ServersPolicy	EMS	No Events
T02BackupSRV All Groups/Other Endpoints	Administrator	172.27.66.124	Policy T02ServersPolicy	EMS	No Events
T02Zabbix All Groups/Other Endpoints	ccs2	172.27.66.127	Policy T02ServersPolicy	EMS	No Events
webserver All Groups/Other Endpoints	ccs2	172.27.66.125	Policy T02ServersPolicy	EMS	No Events

## Applying security profiles to the registered clients in EMS Server



On EMS server dashboard browse to the endpoint profiles tab on the sidebar and click manage profiles.



By default we will only see the Default Profile which is automatically applied to all (new) registered endpoints. We can change this Default profile but we are going to create a new customized profile for our servers. We can do this by clicking on 'Add' in the bar at the top.

FortiClient Endpoint Management Server

Profile Name

T02ServersProfile

BasicAdvanced

Malware

Malware Protection

Expand AllCollapse All

Antivirus Protection

General

Real-Time Protection

Scheduled Scan

Schedule Type

Daily

Start At

07:30 PM

Scan Type

Quick

SaveDiscard Changes

At the malware tab we enable Antivirus protection, Real-Time protection and we will configure a daily quick av scan.

If we expand the Real-Time Protection tab make sure 'Alert when Viruses are detected' is checked' so we will get an alert in EMS server when a server has a virus.

Malware Protection

Expand AllCollapse All

Antivirus Protection

General

Real-Time Protection

Alert When Viruses Are Detected

Scan Compressed Files

Max Size

10

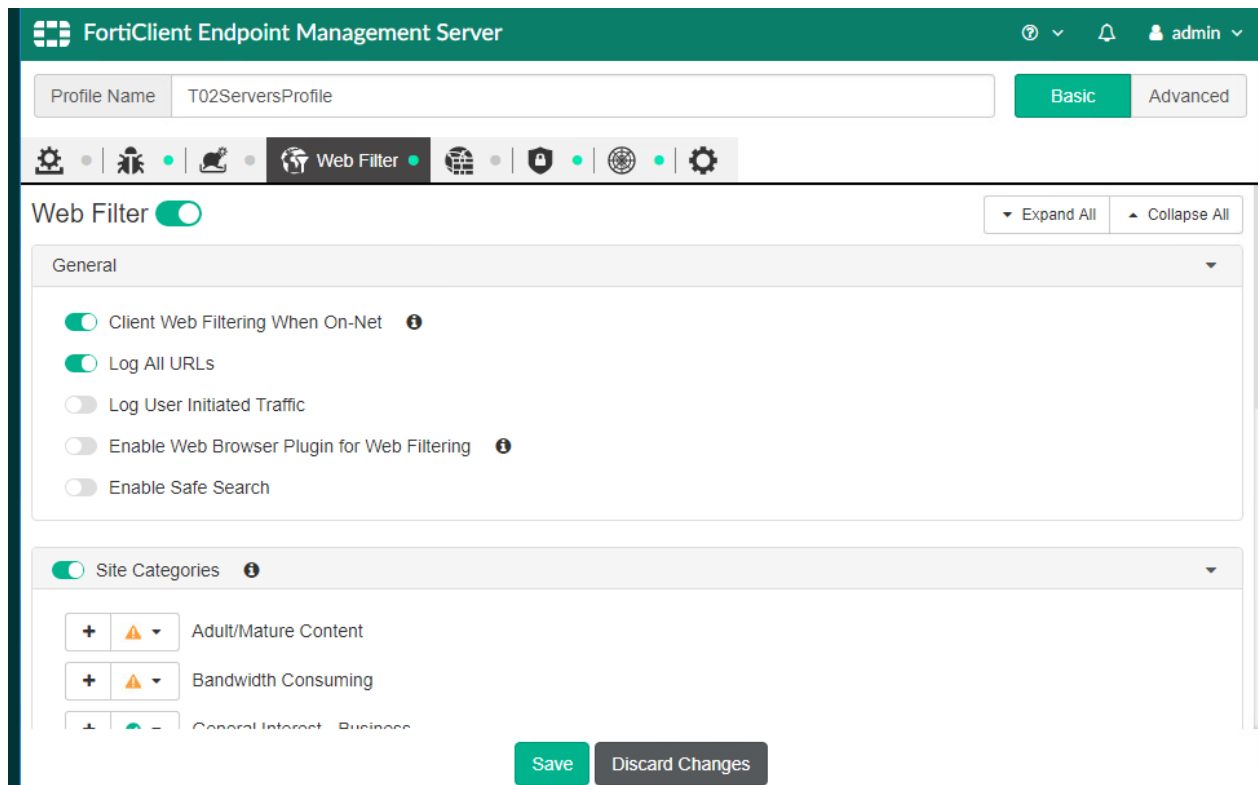
Mb

Only scan files under specified size. 0 means unlimited.

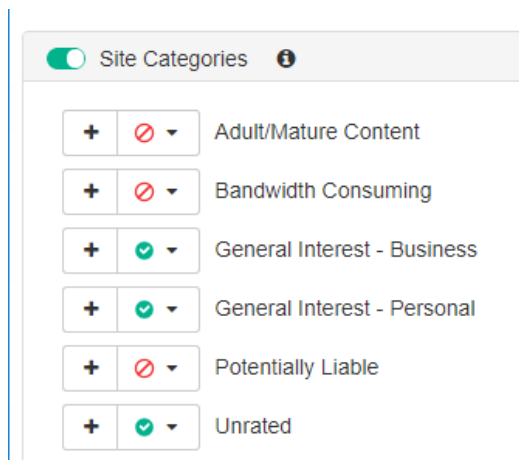
Scheduled Scan

SaveDiscard Changes

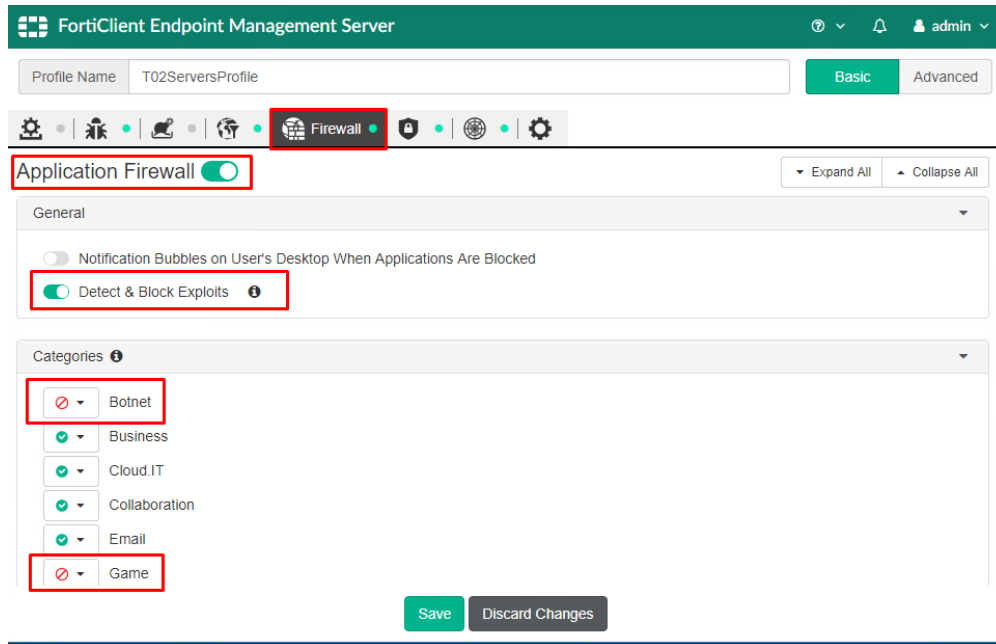
The next tab is Sandbox detection butt we don't have a license for fortinet fortisandbox so we can't configure sandbox detection.



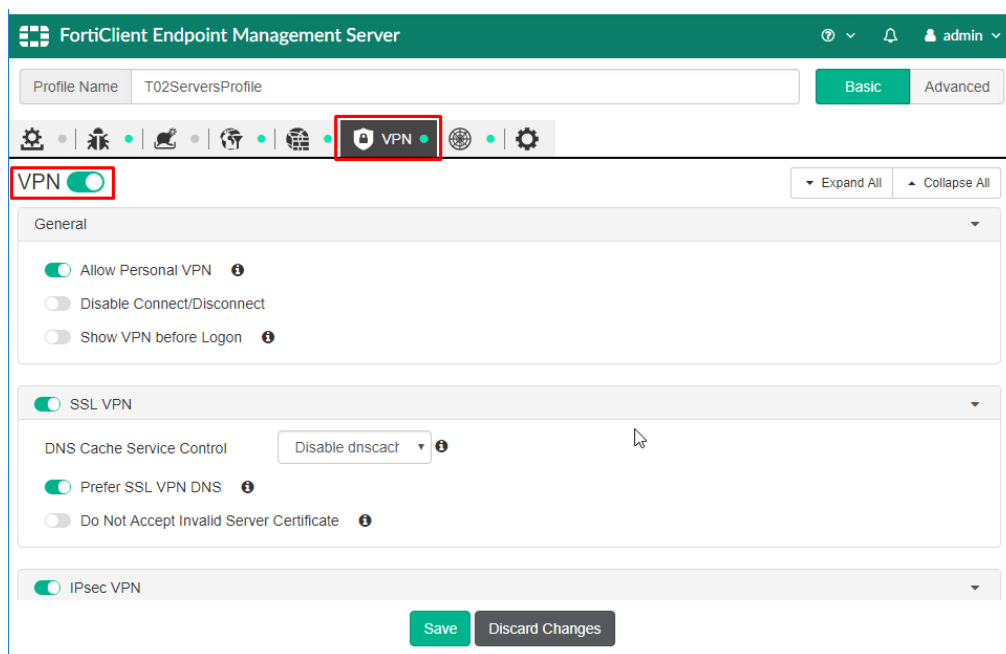
On the webfilter tab we enable webfilter and the options Log All URL's and client web filtering when On-Net because wedont want to visit malicious websites.



We will block adult /mature content, bandwith consuming websites and Potentially liable websites.



On the Firewall tab enable the Application Firewall. We want the firewall to detect and block Exploits. We will also block botnet connections and connection to Game services.



On the VPN tab enable the VPN service, we leave all options on default settings.

FortiClient Endpoint Management Server

Profile Name: T02ServersProfile

Basic Advanced

Vulnerability Scan

Vulnerability Scan ☒

Expand All Collapse All

Scanning

☒ Scan on Registration

☒ Scan on Vulnerability Signature Update

☒ Scan for OS Updates

☐ Automatic Maintenance

☒ Scheduled Scan

Schedule: Daily

Type:

Start At: 09:00 PM

Save Discard Changes

On the vulnerability scan tab enable Vulnerability Scan (this is normally done by default). We enable all scan options. We also configure a daily vulnerability scan.

FortiClient Endpoint Management Server

Profile Name: T02ServersProfile

Basic Advanced

System Settings

System Settings

Expand All Collapse All

UI

☒ Require Password to Disconnect From EMS

Password: \*\*\*\*\*

☐ Do Not Allow User to Back up Configuration

Log

☒ Client-Based Logging When On-Net

☐ Upload Logs to FortiAnalyzer/FortiManager

Update

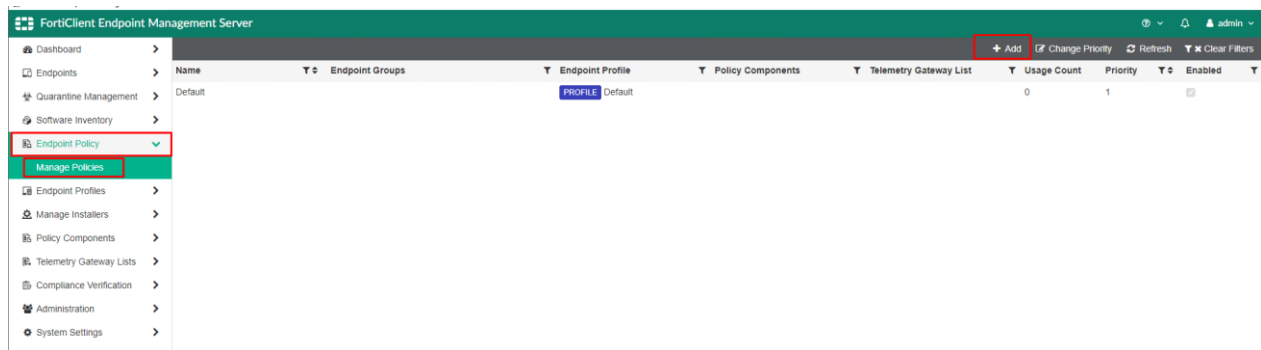
Use FortiManager for Client Signature Update

Save Discard Changes



The last tab is the system settings tab. We only want to make deregistering a client possible on the EMS server and not the client himself. So we will set a password so only persons who know this password can deregister a client.

Click Save to end this profile configuration.



Go to the endpoint policy, manage profiles tab and click on 'add' in the bar at the top

The screenshot shows the 'Endpoint Policy' configuration page in the FortiClient Endpoint Management Server. The left sidebar shows the 'Endpoint Policy' tab selected. The main form contains the following fields: 'Endpoint policy name' (text input with value 'T02ServersPolicy'), 'Endpoint domains' (text input with value 'Optional' and an 'Edit' button), 'Endpoint workgroups' (text input with value 'All Groups' and an 'Edit' button, highlighted with a red box), 'Endpoint profile' (dropdown menu with value 'T02ServersProfile', highlighted with a red box), 'Endpoint profile (Off-net)' (dropdown menu with value 'Optional'), 'On-Net Detection Rules' (dropdown menu with value 'Optional'), 'Telemetry gateway list' (dropdown menu with value 'Optional'), and 'Comments' (text area with value 'Optional'). At the bottom, there is a red box around the 'Enable the policy' toggle, which is currently turned on. Below the toggle are 'Save' and 'Cancel' buttons.

Select as endpoint profiles our previous configured profile and enable the policy. Click on Save.

opensupport All Groups/Other Endpoints	(none)	172.27.66.123	Policy T02ServersPolicy	EMS	No Events
puppet All Groups/Other Endpoints	ccs2	172.27.66.122	Policy T02ServersPolicy	EMS	No Events
T02BackupSRV All Groups/Other Endpoints	Administrator	172.27.66.124	Policy T02ServersPolicy	EMS	No Events
T02Zabbix All Groups/Other Endpoints	ccs2	172.27.66.127	Policy T02ServersPolicy	EMS	No Events
webserver All Groups/Other Endpoints	ccs2	172.27.66.125	Policy T02ServersPolicy	EMS	No Events

If go to the 'all endpoints' tab we will see that all of our servers now have our configured security policy. all our servers are now fully protected.

## 1. Performing remote AV, vulnerability, ... scans

We will add an EICAR Virus test file on two systems for testing purposes

Our systems do a full malware scan and vulnerability scan every day and are real time protected. But you can follow these steps if you want to do a manual remote scan of a system.

The screenshot shows the FortiClient Endpoint Management Server interface. The 'All Endpoints' tab is selected, and a 'Scan' dropdown menu is open, showing options for 'Quick AV Scan', 'Full AV Scan', and 'Vulnerability Scan'. The 'Full AV Scan' option is highlighted. The table below shows the endpoints and their status.

Endpoint	User	IP	Policy	EMS	Events
opensupport	(none)	172.27.66.123	T02ServersPolicy	EMS	No Events
puppet	ccs2	172.27.66.122	T02ServersPolicy	EMS	No Events
T02BackupSRV	Administrator	172.27.66.124	T02ServersPolicy	EMS	No Events
T02Zabbix	ccs2	172.27.66.127	T02ServersPolicy	EMS	No Events
webserver	ccs2	172.27.66.125	T02ServersPolicy	EMS	AV 1

Select the systems you want to scan and select the scan type you want. These systems are now going to do your selected scan type and will report the results to this dashboard.

T02BackupSRV	Administrator	172.27.66.124	Policy T02ServersPolicy	EMS	AV 2
All Groups/Other Endpoints					
Summary	Antivirus Events	Web Filter Events	Vulnerability Events	System Events	
Date	Count	Message			
2020-05-16 16:59:53	1	Malware:EICAR_TEST_FILE found in C:\Users\ADMINI~1\AppData\Local\Temp\MzpStarl.txt part by realtime scan. The fil...			
2020-05-16 17:00:02	1	Malware:EICAR_TEST_FILE found in C:\Users\ADMINI~1\AppData\Local\Temp\Hd76RCG.zip part by realtime scan. The...			

webserver	ccs2	172.27.66.125	Policy T02ServersPolicy	EMS	AV 1
All Groups/Other Endpoints					
Summary	Antivirus Events	Vulnerability Events	System Events		
Date	Count	Message			
2020-05-16 17:01:29	1	Malware:EICAR_TEST_FILE in /home/ccs2/eicartestvirus found by realtime scan. No action performed.			

As you can see our windows server and our webserver have some security problems. The 2 virus files our windows server was trying to download were automatically quarantined and deleted automatically according to the message. Our webserver needed some more time but was also able to quarantine the malicious file.

webserver	ccs2	172.27.66.125	Policy T02ServersPolicy	EMS	AV 2
All Groups/Other Endpoints					
Summary	Antivirus Events	Vulnerability Events	System Events		
Date	Count	Message			
2020-05-16 17:01:29	1	Malware:EICAR_TEST_FILE in /home/ccs2/eicartestvirus found by realtime scan. No action performed.			
2020-05-16 17:06:22	1	Malware:EICAR_TEST_FILE in /home/ccs2/eicartestvirus found by filesystem scan. Quarantine success.			

## 2. Requesting logs from clients

FortiClient Endpoint Management Server

Dashboard > Endpoints > All Endpoints

0 Not Installed 0 Not Registered

Scan Patch Action 1 endpoint selected

Endpoint	Status	Actions
opensupport	Not Installed	<ul style="list-style-type: none"> <li>Request FortiClient Logs</li> <li>Request Diagnostic Results</li> <li>Update Signatures</li> <li>Download Available FortiClient Logs</li> <li>Download Available Diagnostic Results</li> <li>Deregister</li> <li>Quarantine</li> <li>Exclude from Management</li> <li>Clear Events</li> <li>Mark as Uninstalled</li> </ul>

By selecting clients and select the request or download logs action you can manually request en view logs from specific clients

### 3. Viewing and deleting quarantined records

**FortiClient Endpoint Management Server**

Dashboard
Endpoints
Quarantine Management
Whitelist & Restore

11 Quarantined Files
0 Restored Files
1 Affected Hosts
11 New Detections

Host	File	Size	Threat	Source	Status	Summary
T02BackupSRV Other Endpoints	D650C85F7AAC085943C3B4A462AD9B453ED335 BB 34343F4885D0690087481E881F5959BADFESEFE43 8484DE30EB974EEEE10746	1.9 MB	EICAR_TEST_FILE	Manual Scan	Quarantined 2020-05-16 17:23:07	1 instance 1 host affected
T02BackupSRV Other Endpoints	B1BCC5E64F454C61B3DC2B36AC5F4813B6995 1B C7DDF75DEDF427DBD1566813A38DE3A7CF7CD266 9CB9FF18752F58BAE5858AA	2.2 MB	EICAR_TEST_FILE	Manual Scan	Quarantined 2020-05-16 17:23:00	1 instance 1 host affected
T02BackupSRV Other Endpoints	8768910B73B77252850985F64CF8FF0F9F6CA 3 271FA2982BD4961BE9A651E3862DC2C1D096FCFE8A 4318D900574839AAC15FC1F	2.2 MB	EICAR_TEST_FILE	Manual Scan	Quarantined 2020-05-16 17:22:52	1 instance 1 host affected
T02BackupSRV Other Endpoints	52AAAE0DDFDC9AC387B62B6551545DB5D6269 633 469D635E17130162997B6D43D09F21CA487730852 58ACD8385C28DFBB32EA8AA	2.2 MB	EICAR_TEST_FILE	Manual Scan	Quarantined 2020-05-16 17:22:43	1 instance 1 host affected
T02BackupSRV Other Endpoints	4FF06328E8A8DA209ADF8003D06174A45445 E2 CD4D46C8CF373C189159322EB4328AB4F1EE083390 2D709CC19F321C942D23898	1.9 MB	EICAR_TEST_FILE	Manual Scan	Quarantined 2020-05-16 17:22:43	1 instance 1 host affected
T02BackupSRV Other Endpoints	21C23BFF4541FCD5D0BF8FBC0FCA0E1E0BBB4 626 9CB937A8187D3A9D7CE741E1A06E48FCE86830A	1.9 MB	EICAR_TEST_FILE	Manual Scan	Quarantined 2020-05-16 17:22:35	1 instance 1 host affected


11 of 11 files loaded

Click on the settings icon in quarantine management.

### Quarantine Management Settings

Clean up Quarantine Management records older than

days



Age of record is determined by when its status was last updated.

Save

Close

click on the clear now icon or configure the days when the quarantine files have to be removed