

NSE5_FCT-6.2^{Q&As}

Fortinet NSE 5 - FortiClient EMS 6.2

Pass Fortinet NSE5_FCT-6.2 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/nse5_fct-6-2.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet
Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



QUESTION 1

An administrator installs FortiClient on Windows Server. What is the default behavior of real-time protection control?

- A. Real-time protection must update AV signature database
- B. Real-time protection sends malicious files to FortiSandbox when the file is not detected locally
- C. Real-time protection is disabled
- D. Real-time protection must update the signature database from FortiSandbox

Correct Answer: C

QUESTION 2

Refer to the exhibit.

```
1:40:39 PM Information Vulnerability id=96521 msg="A vulnerability scan result has been :
1:40:39 PM Information Vulnerability id=96520 msg="The vulnerability scan status has char
1:41:38 PM Information ESNAC id=96958 user=Admin msg="User social media information" soc:
2:12:22 PM Information Config id=96882 msg="Policy 'Default' was received and applied"
2:13:27 PM Information ESNAC id=96958 user=Admin msg="User social media information" soc:
2:14:32 PM Information ESNAC id=96959 emshostname=WIN-EHVKB3EA3S71 msg="Endpoint has AV w
2:14:54 PM Information Config id=96882 msg="Policy 'Default' was received and applied"
2:16:01 PM Information ESNAC id=96958 user=Admin msg="User social media information" soc:
2:20:19 PM Information Config id=96883 msg="Compliance rules 'default' were received and
2:20:23 PM Debug ESNAC PIPEMSG_CMD_ESNAC_STATUS_RELOAD_CONFIG
2:20:23 PM Debug ESNAC cb828898d1ae56916f84cc7909a1eb1a
2:20:23 PM Debug ESNAC Before Reload Config
2:20:23 PM Debug ESNAC ReloadConfig
2:20:23 PM Debug Scheduler stop_task() called
2:20:23 PM Debug Scheduler GUI change event
2:20:23 PM Debug Scheduler stop_task() called
2:20:23 PM Information Config id=96882 msg="Policy 'Fortinet-Training' was received and ap
2:20:23 PM Debug Config 'scan on registration' is disabled - delete 'on registration' vulne
2:20:23 PM Debug Config ImportConfig: tag <\forticlient_configuration\antiexploit\exclusion
```

Based on the FortiClient logs shown in the exhibit which endpoint profile policy is currently applied to the FortiClient endpoint from the EMS server?

- A. WIK-EKVK3EA3S71
- B. Fortinet-Training
- C. Default
- D. Default configuration policy

Correct Answer: C

QUESTION 3

Refer to the exhibit.



Based on the settings shown in the exhibit what action will FortiClient take when it detects that a user is trying to download an infected file?

- A. Blocks the infected files as it is downloading
- B. Quarantines the infected files and logs all access attempts
- C. Sends the infected file to FortiGuard for analysis
- D. Allows the infected file to download without scan

Correct Answer: D

QUESTION 4

Refer to the exhibit.

```
config user f330
  edit "Server"
    set type fortiems
    set server "10.0.1.200"
    set password ENC ebT9fHIMXIBykhWCSnG;P+Tpi/EjEdQu4hAa24LiKxHolWI7JyX
    set ssl enable
  next
end
```

Based on the CLI output from FortiGate, which statement is true?

- A. FortiGate is configured to pull user groups from FortiClient EMS
- B. FortiGate is configured with local user group

- C. FortiGate is configured to pull user groups from FortiAuthenticator
- D. FortiGate is configured to pull user groups from AD Server.

Correct Answer: A

QUESTION 5

When site categories are disabled on FortiClient webfilter and AV (malicious websites), which feature protects the endpoint?

- A. Web Exclusion list
- B. Endpoint host file
- C. FortiSandbox URL list
- D. Block malicious websites on Antivirus

Correct Answer: A

[NSE5_FCT-6.2 PDF Dumps](#)

[NSE5_FCT-6.2 Practice
Test](#)

[NSE5_FCT-6.2 Braindumps](#)