

NSE5_FCT-7.0^{Q&As}

Fortinet NSE 5 - FortiClient EMS 7.0

Pass Fortinet NSE5_FCT-7.0 Exam with 100% Guarantee

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

https://www.leads4pass.com/nse5_fct-7-0.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 needs to connect FortiClient EMS as a fabric connector to FortiGate. What is the prerequisite to get FortiClient EMS to connect to FortiGate successfully?

- A. Revoke and update the FortiClient EMS root CA.
- B. Revoke and update the FortiClient client certificate on EMS.
- C. Import and verify the FortiClient client certificate on FortiGate.
- D. Import and verify the FortiClient EMS root CA certificate on FortiGate

Correct Answer: D

QUESTION 2

Refer to the exhibit.

Log - Policy

```
1:40:39 PM Information Vulnerability id=96521 msg="A vulnerability scan result has been logged" status=N/A vulncat="Operating
1:40:39 PM Information Vulnerability id=96520 msg="The vulnerability scan status has changed" status="scanning finished" vulnc
1:41:38 PM Information ESNAC id=96958 user=Admin msg="User social media information" social_srvc=os social_user=Admin
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" social_srvc=os social_user=Admin
2:14:32 PM Information ESNAC id=96959 emshostname=WIN-EHVKBEA3571 msg="Endpoint has AV whitelist engine version 6.00134 and si
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" social_srvc=os social_user=Admin
2:20:19 PM Information Config id=96883 msg="Compliance rules 'default' were received and applied"
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 applied"
2:20:23 PM Debug Config 'scan on registration' is disabled - delete 'on registration' vulnerability scan.
2:20:23 PM Debug Config ImportConfig: tag <\forticlient_configuration\antiexploit\exclusion_applications> value is empty.
```

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. Default
- B. Compliance rules default
- C. Fortinet- Training
- D. Default configuration policy

Correct Answer: C

QUESTION 3

Which two statements are true about the ZTNA rule? (Choose two.)

- A. It enforces access control
- B. It redirects the client request to the access proxy
- C. It defines the access proxy
- D. It applies security profiles to protect traffic

Correct Answer: AD

"A ZTNA rule is a proxy policy used to enforce access control. ZTNA tags or tag groups can be defined to enforce zero trust role based access. Security profiles can be configured to protect this traffic."

"ZTNA rules help control access by defining users and ZTNA tags to perform user authentication and security posture checks. And just like firewall policies, you can control the source and destination addresses, and apply appropriate security

profiles to scan the traffic."

<https://docs.fortinet.com/document/fortigate/7.0.0/ztna-deployment/899992/configuring-ztna-rules-to-control-access>

QUESTION 4

An administrator installs FortiClient EMS in the enterprise.

Which component is responsible for enforcing protection and checking security posture?

- A. FortiClient vulnerability scan
- B. FortiClient EMS tags
- C. FortiClient EMS
- D. FortiClient

Correct Answer: D

QUESTION 5

A new chrome book is connected in a school's network.

Which component can the EMS administrator use to manage the FortiClient web filter extension installed on the Google Chromebook endpoint?

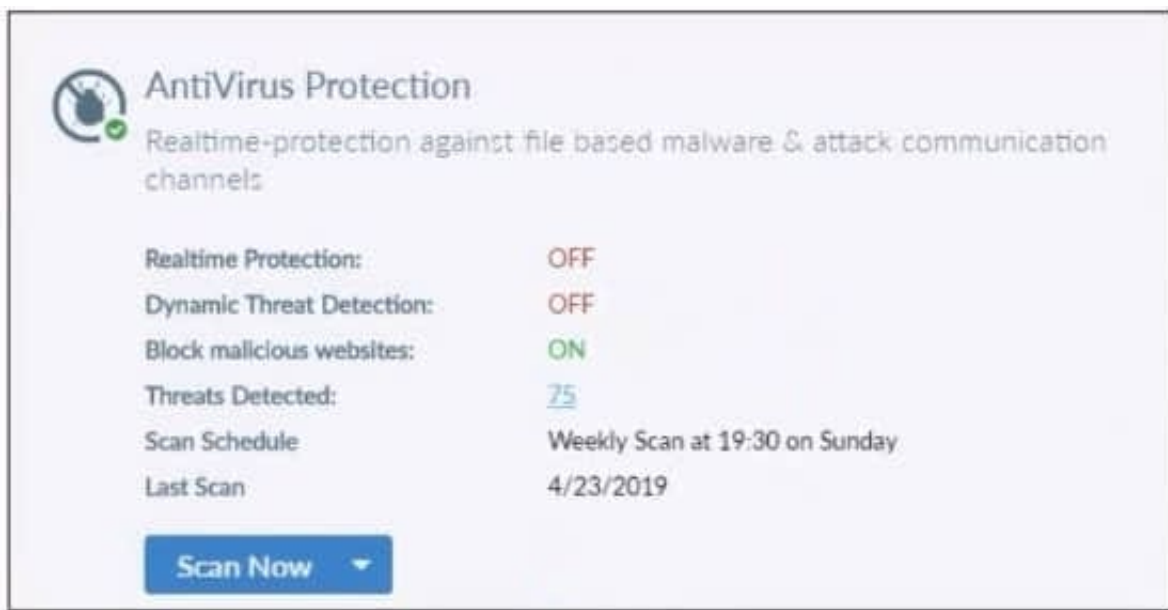
- A. FortiClient site categories
- B. FortiClient customer URL list
- C. FortiClient web filter extension

D. FortiClient EMS

Correct Answer: C

QUESTION 6

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 7

Which two benefits are benefits of using multi-tenancy mode on FortiClient EMS? (Choose two.)

- A. The fabric connector must use an IP address to connect to FortiClient EMS
- B. It provides granular access and segmentation.
- C. Licenses are shared among sites.

D. Separate host servers manage each site.

Correct Answer: BD

FCT-EMS 7,0 Page 101 : You would use multi-tenancy in an MSSP environment to conserve resources and use the same license (the total number of FortiClient licenses are shared between sites)

QUESTION 8

Which component or device shares device status information through ZTNA telemetry?

- A. FortiClient
- B. FortiGate
- C. FortiGate Access Proxy
- D. FortiClient EMS

Correct Answer: A

FortiClient communicates directly with FortiClient EMS to continuously share device status information through ZTNA telemetry.

QUESTION 9

Which security fabric component sends a notification to quarantine an endpoint after IOC detection in the automation process?

- A. FortiAnalyzer
- B. FortiClient
- C. FortiClient EMS
- D. Forti Gate

Correct Answer: D

QUESTION 10

Refer to the exhibit.

Log - Deployment

Deployments + Add <input type="checkbox"/> Change Priority					
Name	Assigned Groups	Deployment Package	Scheduled Upgrade Time	Priority	Enabled
Deployment-1	All Groups	First-Time-Installation		1	<input type="checkbox"/>
Deployment-2	All Groups trainingAD training.lab	To-Upgrade		2	<input checked="" type="checkbox"/>

Which shows FortiClient EMS deployment profiles.

When an administrator creates a deployment profile on FortiClient EMS, which statement about the deployment profile is true?

- A. Deployment-1 will install FortiClient on new AD group endpoints
- B. Deployment-2 will install FortiClient on both the AD group and workgroup
- C. Deployment-2 will upgrade FortiClient on both the AD group and workgroup
- D. Deployment-1 will upgrade FortiClient only on the workgroup

Correct Answer: B

[Latest NSE5_FCT-7.0 Dumps](#)

[NSE5_FCT-7.0 PDF Dumps](#) [NSE5_FCT-7.0 Braindumps](#)