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.pass4itsure.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

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 2

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 3

Which statement about FortiClient comprehensive endpoint protection is true?

A. It helps to safeguard systems from email spam

B. It helps to safeguard systems from data loss.

C. It helps to safeguard systems from DDoS.

D. lt helps to safeguard systems from advanced security threats, such as malware.

Correct Answer: D

FortiClient provides comprehensive endpoint protection for your Windows- based, Mac-based, and Linuxbased

https://www.pass4itsure.com/nse5_fct-7-0.html
2024 Latest pass4itsure NSE5_FCT-7.0 PDF and VCE dumps Download

desktops, laptops, file servers, and mobile devices such as iOS and Android. It helps you to safeguard your systems with advanced security technologies, all of which you can manage from a single management console.

QUESTION 4

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-EHVKBEA3S71 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 5

In a FortiSandbox integration, what does the remediation option do?

A. Wait for FortiSandbox results before allowing files

B. Exclude specified files

C. Alert and notify only

D. Deny access to a file when it sees no results

Correct Answer: C