



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

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 2

Refer to the exhibit, which shows the endpoint summary information on FortiClient EMS.

The screenshot shows the FortiClient EMS interface for a Remote-Client endpoint. The top navigation bar includes 'Remote-Client', 'Administrator', '10.0.2.20', 'Policy Default', 'EMS', 'VUL 99+', and 'SYS 1'. Below the navigation bar, there are tabs for 'Summary', 'Webfilter Events', 'Vulnerability Events', and 'System Events'. The main content area is divided into three columns:

- Left Column (User Profile):** Shows the user 'Administrator' with 'No User', 'No Email', and 'Other Endpoints' status. Below this, a list of attributes for the 'Remote-Client' device: OS (Microsoft Windows Server...), IP (10.0.2.20), MAC (00-50-56-01-ea-1a), Public IP (161.156.10.132), Status (Online), Location (Off-Fabric), Owner, Organization, Zero Trust Tags (Remote-Users, Windows-Endpoints), and Network Status (Ethernet0, Ethernet1 2).
- Middle Column (Configuration):** Shows 'Managed by EMS' and 'Configuration' details: Policy (Default), Profile (Training), Off-Fabric Profile (Default), Installer (Not assigned), FortiClient Version (7.0.0.0029), FortiClient Serial Number (FCT8000906335614), FortiClient ID (8B12DB30D20B4735AAA...), and ZTNA Serial Number (6FC0BEB5D562E778DA8...). Below this is a 'Classification Tags' section with a 'Low' tag and an '+ Add' button.
- Right Column (Status and Features):** Shows 'Status' as 'Managed' and a list of 'Features': Antivirus installed, Anti-Ransomware installed, Cloud Based Malware Outbreak Detection installed, Sandbox installed, Sandbox Cloud installed, Web Filter enabled (hidden), Application Firewall installed, Remote Access configured, Vulnerability Scan enabled, and SSOMA installed. Below this is a 'Third Party Features' section with 'Virus & Threat Protection' and 'Disk Encryption' both set to 'None'.

What two conclusions can you make based on the Remote-Client status shown above? (Choose two.)

- A. The endpoint is classified as at risk.
- B. The endpoint has been assigned the Default endpoint policy.



- C. The endpoint is configured to support FortiSandbox.
- D. The endpoint is currently off-net.

Correct Answer: BD

QUESTION 3

An administrator is required to maintain a software vulnerability on the endpoints, without showing the feature on the FortiClient dashboard. What must the administrator do to achieve this requirement?

- A. Disable select the vulnerability scan feature in the deployment package
- B. Use the default endpoint profile
- C. Select the vulnerability scan feature in the deployment package, but disable the feature on the endpoint profile
- D. Click the hide icon on the vulnerability scan tab

Correct Answer: D

QUESTION 4

Which three types of antivirus scans are available on FortiClient? (Choose three)

- A. Proxy scan
- B. Full scan
- C. Custom scan
- D. Flow scan
- E. Quick scan

Correct Answer: BCE

QUESTION 5

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. It 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 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.

[Latest NSE5_FCT-7.0 Dumps](#)

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