# Fortinet FCP_FCT_AD-7.4 NSE 6 Practice Questions

**Shared by Singleton on 17-08-2026**

**For More Free Questions and Preparation Resources**

Check the Links on Last Page

## Question 1

Question Type: MultipleChoice

What does FortiClient do as a fabric agent? (Choose two.)

### Options:

A- Provides IOC verdicts
B- Creates dynamic policies
C- Provides application inventory
D- Automates Responses



### Answer:

C, D

## Question 2

Question Type: MultipleChoice

Which two VPN types can a FortiClient endpoint user inmate from the Windows command prompt? (Choose two)

### Options:

A- L2TP
B- PPTP
C- IPSec
D- SSL VPN



### Answer:

C, D

### Explanation:

FortiClient supports initiating the following VPN types from the Windows command prompt:

IPSec VPN: FortiClient can establish IPSec VPN connections using command line instructions.

SSL VPN: FortiClient also supports initiating SSL VPN connections from the Windows command prompt.

These two VPN types can be configured and initiated using specific command line parameters provided by FortiClient.

Reference

FortiClient EMS 7.2 Study Guide, VPN Configuration Section

Fortinet Documentation on Command Line Options for FortiClient VPN

## Question 3

Question Type: MultipleChoice

An administrator configures ZTNA configuration on the FortiGate. Which statement is true about the firewall policy?

### Options:

A- It redirects the client request to the access proxy.
B- It uses the access proxy.
C- It defines ZTNA server.
D- It only uses ZTNA tags to control access for endpoints.

### Answer:

A

### Explanation:

'The firewall policy matches and redirects client requests to the access proxy VIP'
https://docs.fortinet.com/document/fortigate/7.0.0/new-features/194961/basic-ztna-configuration

## Question 4

Question Type: MultipleChoice

Which security fabric component sends a notification io quarantine an endpoint after IOC detection "n the automation process?

## Options:

A- FortiAnalyzer
B- FortiGate
C- FortiClient EMS
D- FortiClient

## Answer:

C

## Explanation:

Understanding the Automation Process:

In the Security Fabric, automation processes can include actions such as quarantining an endpoint after an IOC (Indicator of Compromise) detection.

Evaluating Responsibilities:

FortiClient EMS plays a crucial role in endpoint management and can send notifications to quarantine endpoints.

Conclusion:

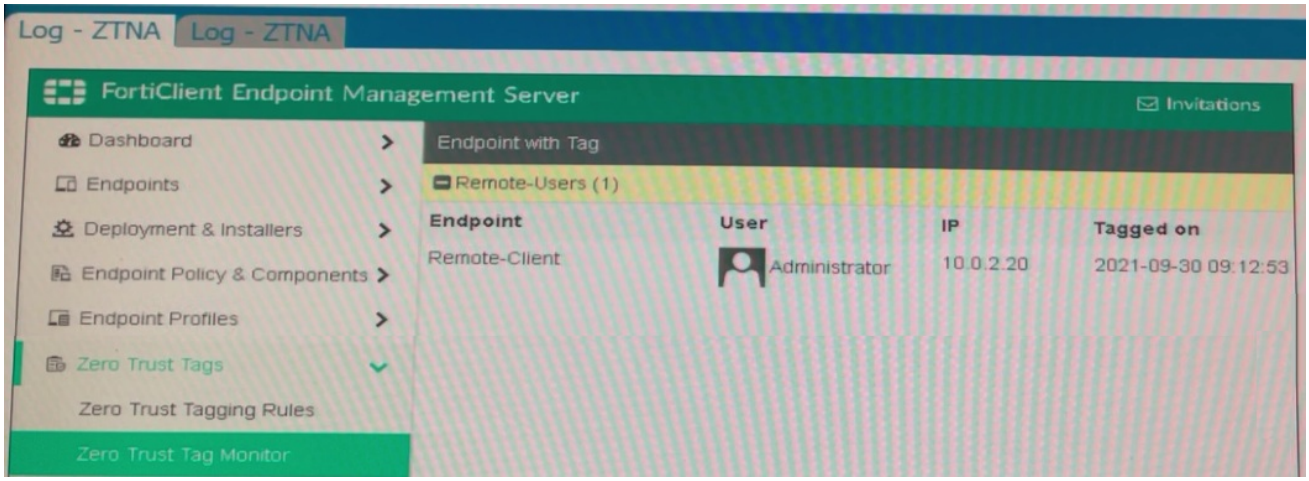
The correct security fabric component that sends a notification to quarantine an endpoint after IOC detection is FortiClient EMS.

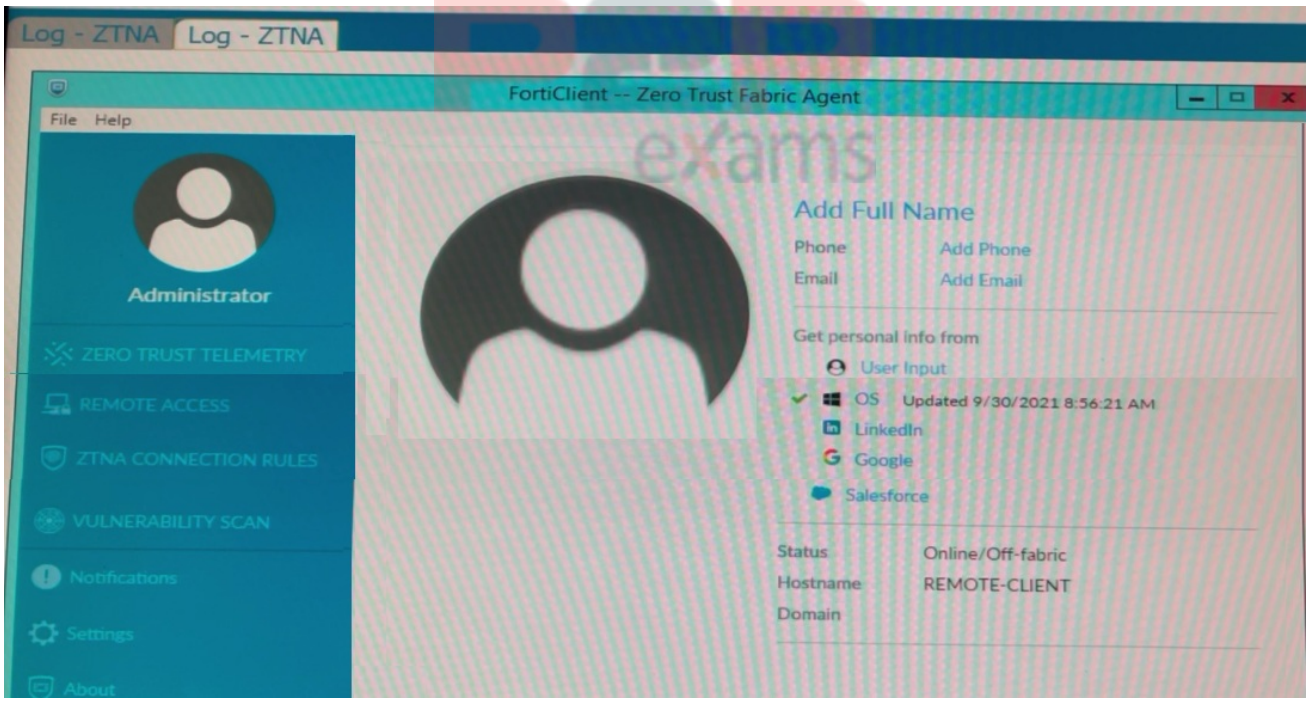
FortiClient EMS and automation process documentation from the study guides.

# Question 5

Question Type: MultipleChoice

Refer to the exhibits.




Which show the Zero Trust Tag Monitor and the FortiClient GUI status.

Remote-Client is tagged as Remote-Users on the FortiClient EMS Zero Trust Tag Monitor.

What must an administrator do to show the tag on the FortiClient GUI?

## Options:

A- Update tagging rule logic to enable tag visibility
B- Change the FortiClient system settings to enable tag visibility
C- Change the endpoint control setting to enable tag visibility
D- Change the user identity settings to enable tag visibility

## Answer:

B

## Explanation:

Based on the exhibits provided:

The 'Remote-Client' is tagged as 'Remote-Users' in the FortiClient EMS Zero Trust Tag Monitor.

To ensure that the tag 'Remote-Users' is visible in the FortiClient GUI, the system settings within FortiClient need to be updated to enable tag visibility.

The tag visibility feature is controlled by FortiClient system settings which manage how tags are displayed in the GUI.

Therefore, the administrator needs to change the FortiClient system settings to enable tag visibility.

Reference

FortiClient EMS 7.2 Study Guide, Zero Trust Tagging Section

FortiClient Documentation on Tag Management and Visibility Settings

# Question 6

Question Type: MultipleChoice

Refer to the exhibit, which shows FortiClient EMS deployment, profiles.


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

## Options:

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

## Answer:

A

## Explanation:

Deployment Profiles Analysis:

Deployment-1 has the 'First-Time-Installation' package and is assigned to 'All Groups' with a priority of 1 but is not enabled.

Deployment-2 has the 'To-Upgrade' package, is assigned to both 'All Groups' and 'trainingAD.training.lab,' with a priority of 2 and is enabled.

Evaluating Deployment-2:

Deployment-2 will upgrade FortiClient on both 'All Groups' and 'trainingAD.training.lab' since it is enabled and assigned to these groups. This includes both AD (Active Directory) groups and workgroups.

Conclusion:

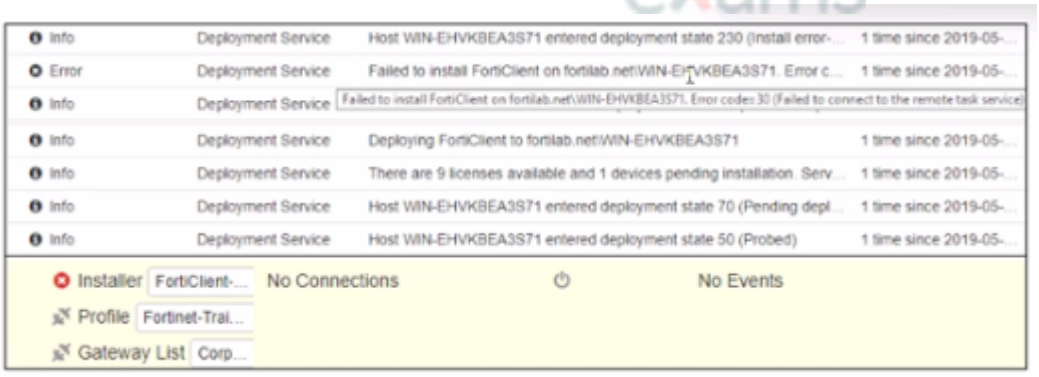
Since Deployment-2 is set to upgrade FortiClient on all the assigned groups and workgroups, the correct answer is A.

FortiClient EMS deployment and profile documentation from the study guides.

# Question 7

Question Type: MultipleChoice

Exhibit.




Based on the logs shown in the exhibit, why did FortiClient EMS tail to install FortiClient on the endpoint?

## Options:

A- The FortiClient antivirus service is not running.
B- The Windows installer service is not running.
C- The remote registry service is not running.
D- The task scheduler service is not running.

## Answer:

D

## Explanation:

https://community.fortinet.com/t5/FortiClient/Technical-Note-FortiClient-fails-to-install-from-FortiClient-EMS/ta-p/193680

The deployment service error message may be caused by any of the following. Try eliminating them all, one at a time.

1. Wrong username or password in the EMS profile

2. Endpoint is unreachable over the network

3. Task Scheduler service is not running

4. Remote Registry service is not running

5. Windows firewall is blocking connection