Fortinet

Exam Questions FCP_FCT_AD-7.4

FCP - FortiClient EMS 7.4 Administrator

NEW QUESTION 1
Which two third-party tools can an administrator use to deploy FortiClient? (Choose two.)

A. Microsoft Windows Installer
B. Microsoft SCCM
C. Microsoft Active Directory GPO
D. QR code generator

Answer: BC

NEW QUESTION 2
Which two statements about ZTNA destinations are true? (Choose two.)

A. FottiClient ZTNA destinations use an existing VPN tunnel to create a secure connection.
B. FortiClient ZTNA destinations provides access through TCP forwarding.
C. FortiClient ZTNA destinations do not support a wildcard FQDN.
D. FortiClient ZTNA destination encryption is disabled by default.
E. FortiClient ZTNA destination authentication is enabled by default.

Answer: CD

NEW QUESTION 3
In a ForliSandbox integration, what does the remediation option do?

A. Deny access to a tile when it sees no results
B. Alert and notify only
C. Exclude specified files
D. Wait for FortiSandbox results before allowing files

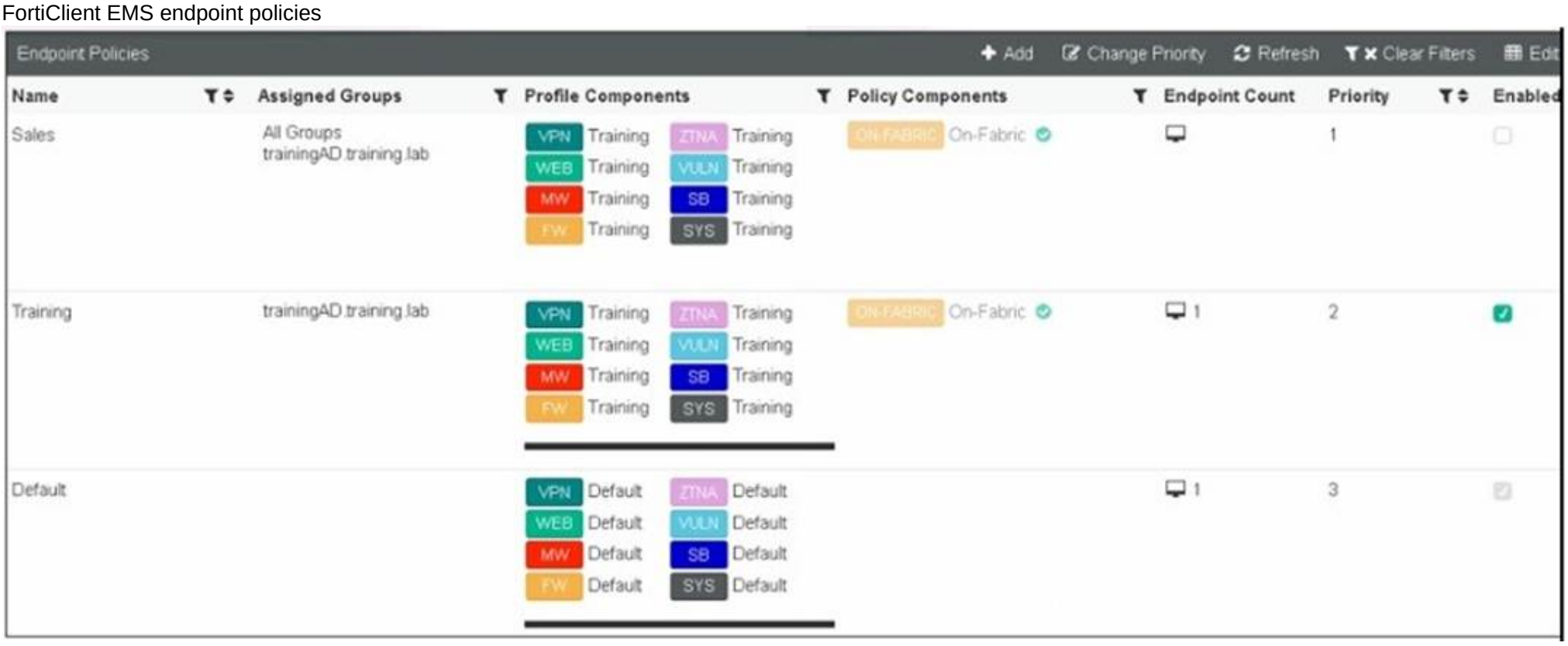
Answer: B

NEW QUESTION 4
When multitenancy is enabled on FortiClient EMS, which administrator role can provide access to the global site only? (Choose one answer)

A. Tenant administrator
B. Settings administrator
C. Standard administrator
D. Global administrator

Answer: B

NEW QUESTION 5
FortiClient EMS endpoint policies



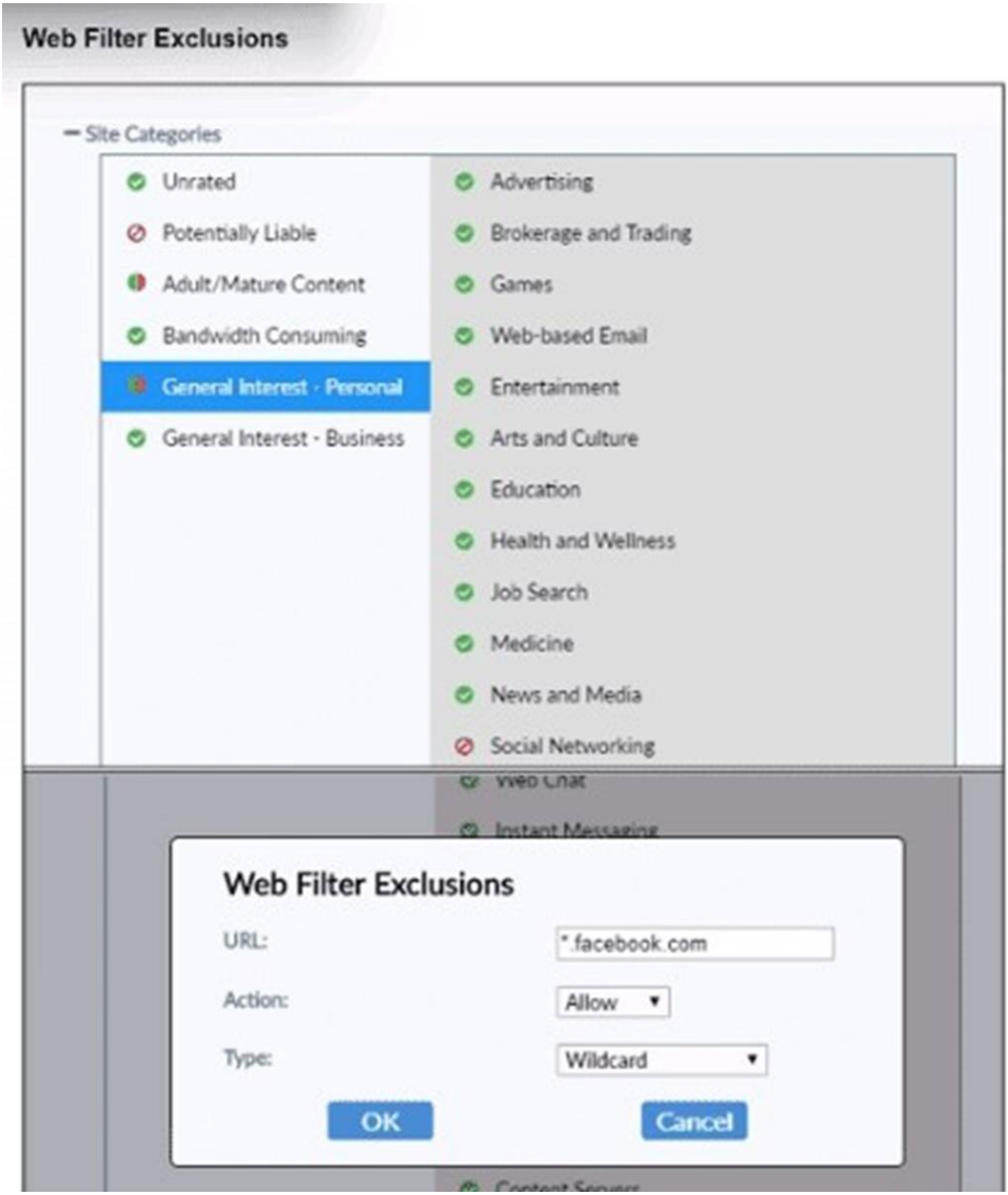
Refer to the exhibit, which shows multiple endpoint policies on FortiClient EMS. Which policy is applied to the endpoint in the AD group trainingAD

A. The Training policy
B. Both the Sales and Training policies because their priority is higher than the Default policy
C. The Default policy because it has the highest priority
D. The sales policy

Answer: A

NEW QUESTION 6

Refer to the exhibit.



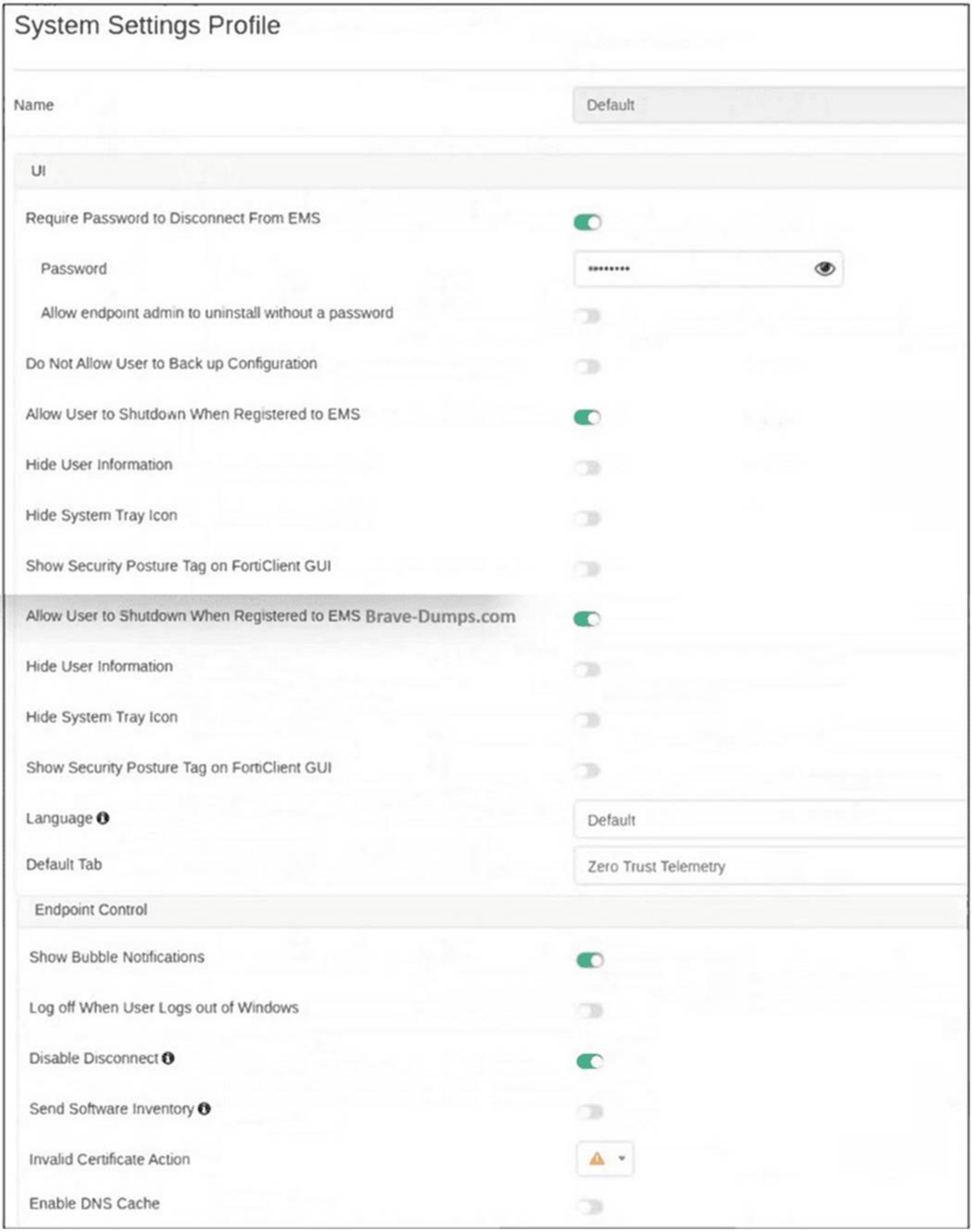
Based on the settings shown in the exhibit, which action will FortiClient take when users try to access www facebook com?

A. FortiClient will allow access to Facebook.
B. FortiClient will block access to Facebook and its subdomains.
C. FortiClient will monitor only the user's web access to the Facebook website
D. FortiClient will prompt a warning message to want the user before they can access the Facebook website

Answer: B

NEW QUESTION 7
Refer to the exhibit.

System settings profile



Which behavior should you expect when FortiClient with an invalid certificate is connecting to FortiClient EMS? (Choose one answer)

A. FortiClient is blocked from connecting to FortiClient EMS.
B. FortiClient requires an additional password to connect to FortiClient EMS.
C. FortiClient displays a warning message to the end user.
D. FortiClient EMS pushes a valid certificate to FortiClient.

Answer: C

NEW QUESTION 8
An administrator must deploy FortiClient for an organization that has BYOD and remote users.
What can the administrator use to deploy FortiClient? (Choose one answer)

A. FortiClient zero-touch provisioning
B. Microsoft System Center Configuration Manager (SCCM)
C. Microsoft Intune
D. Group Policy Object (GPO)

Answer: C

NEW QUESTION 9
An administrator must add an authentication server on FortiClient EMS in a different security zone that cannot allow a direct connection.
Which solution can provide secure access between FortiClient EMS and the Active Directory server?

A. Configure and deploy a FortiGate device between FortiClient EMS and the Active Directory server.
B. Configure Active Directory and install FortiClient EMS on the same VM.
C. Configure a slave FortiClient EMS on a virtual machine.
D. Configure an Active Directory connector between FortiClient EMS and the Active Directory server.

Answer: A

NEW QUESTION 10
An administrator deploys a FortiClient installation through the Microsoft AD group policy After installation is complete all the custom configuration is missing.
What could have caused this problem?

A. The FortiClient exe file is included in the distribution package
B. The FortiClient MST file is missing from the distribution package
C. FortiClient does not have permission to access the distribution package.
D. The FortiClient package is not assigned to the group

Answer: D

NEW QUESTION 10
Exhibit.

```
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 lo the ForliClient endpoint from the EMS server?

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

Answer: A

NEW QUESTION 11
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.

Answer: D

NEW QUESTION 14
Which two statements are true about the ZTNA rule? (Choose two.)

A. It applies security profiles to protect traffic
B. It applies SNAT to protect traffic.
C. It defines the access proxy.
D. It enforces access control.

Answer: AD

NEW QUESTION 16
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

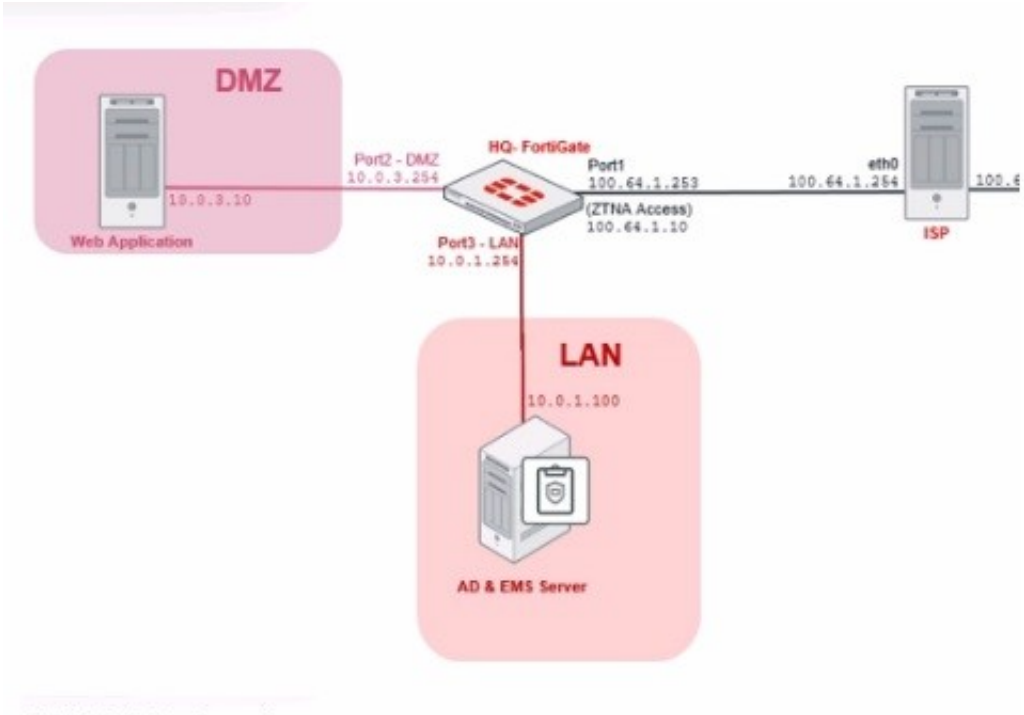
Answer: D

NEW QUESTION 21
Which three features does FortiClient endpoint security include? (Choose three.)

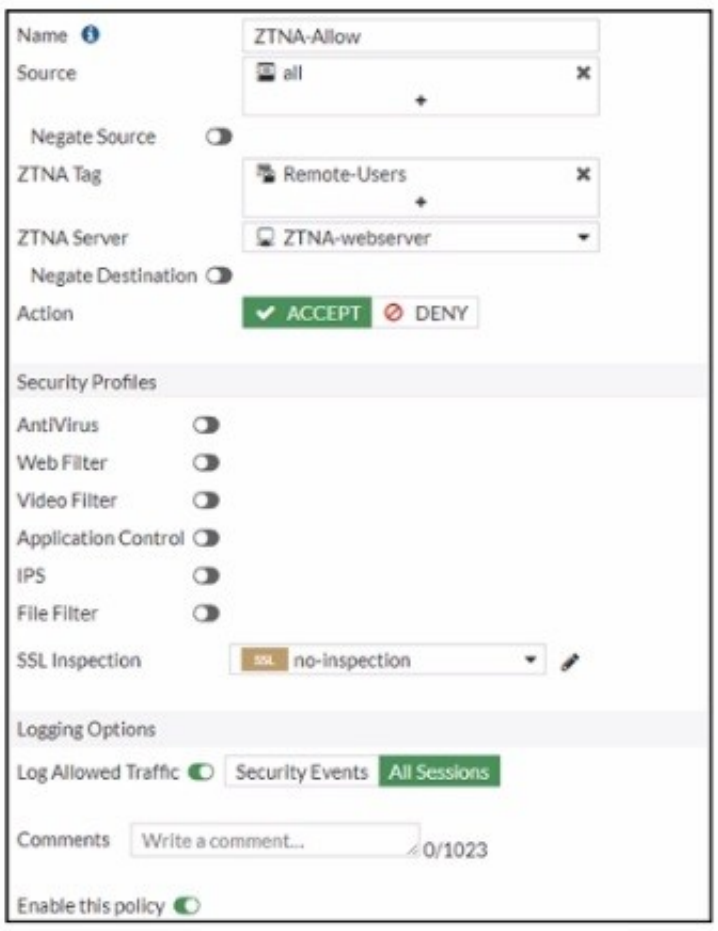
A. DLP
B. Vulnerability management
C. L2TP
D. lPsec
E. Real-lime protection

Answer: BDE

NEW QUESTION 24
ZTNA Network Topology



ZTNA Rule Configuration



Refer to the exhibits, which show a network topology diagram of ZTNA proxy access and the ZTNA rule configuration.
An administrator runs the diagnose endpoint record list CLI command on FortiGate to check Remote-Client endpoint information, however Remote-Client is not showing up in the endpoint record list.
What is the cause of this issue?

A. Remote-Client has not initiated a connection to the ZTNA access proxy.
B. Remote-Client provided an empty client certificate to connect to the ZTNA access proxy.
C. Remote-Client provided an invalid certificate to connect to the ZTNA access proxy.
D. Remote-Client failed the client certificate authentication.

Answer: D

NEW QUESTION 28
Which two statements are true about ZTNA? {Choose two.)

A. ZTNA manages access for remote users only.
B. ZTNA provides role-based access.
C. ZTNA provides a security posture check.
D. ZTNA manages access through the client only.

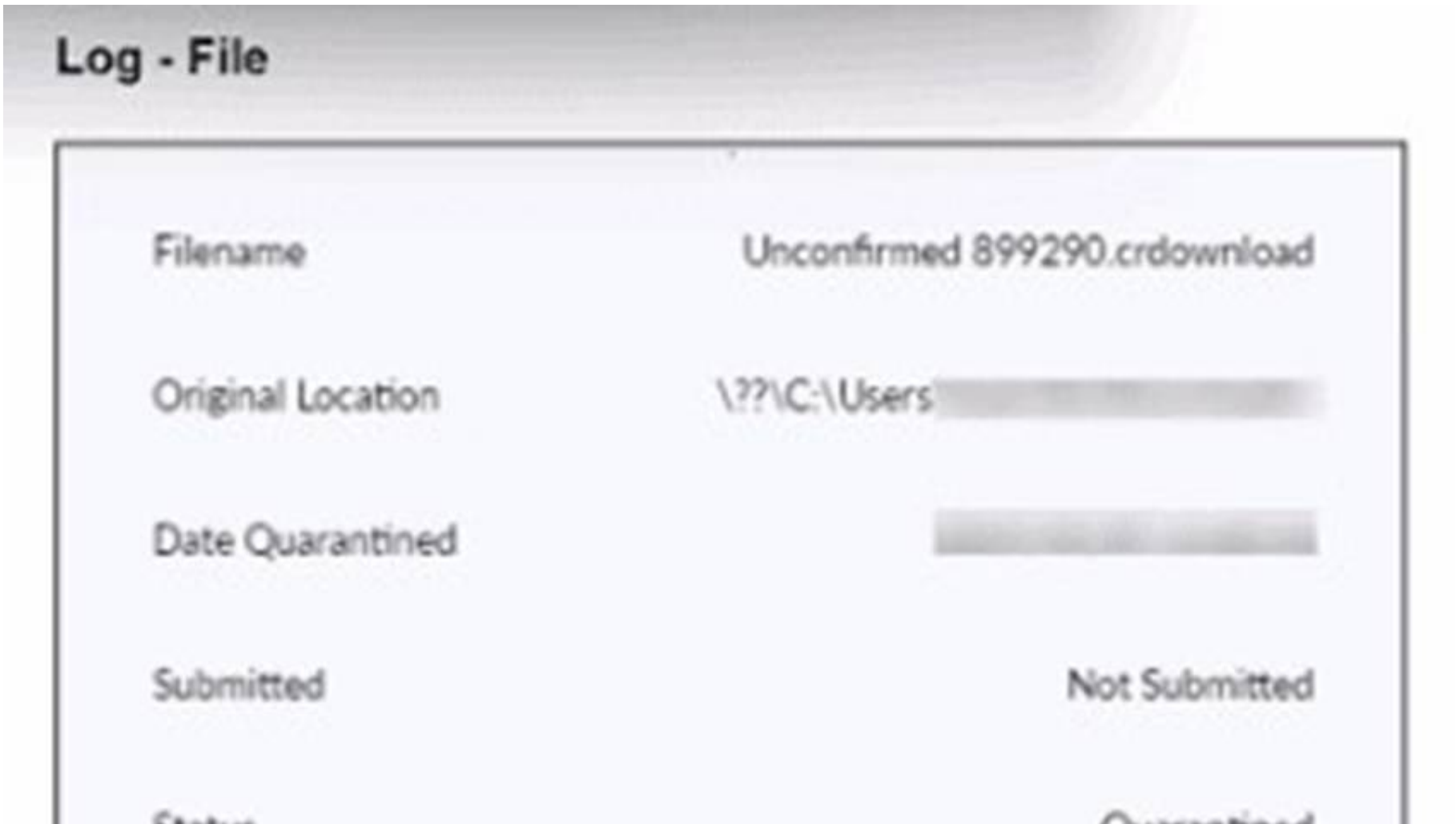
Answer: BC

NEW QUESTION 31
An administrator needs to connect FortiClient EMS as a fabric connector to FortiGate What is the prerequisite to get FortiClient EMS lo connect to FortiGate successfully?

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

Answer: A

NEW QUESTION 33
Refer to the exhibit.

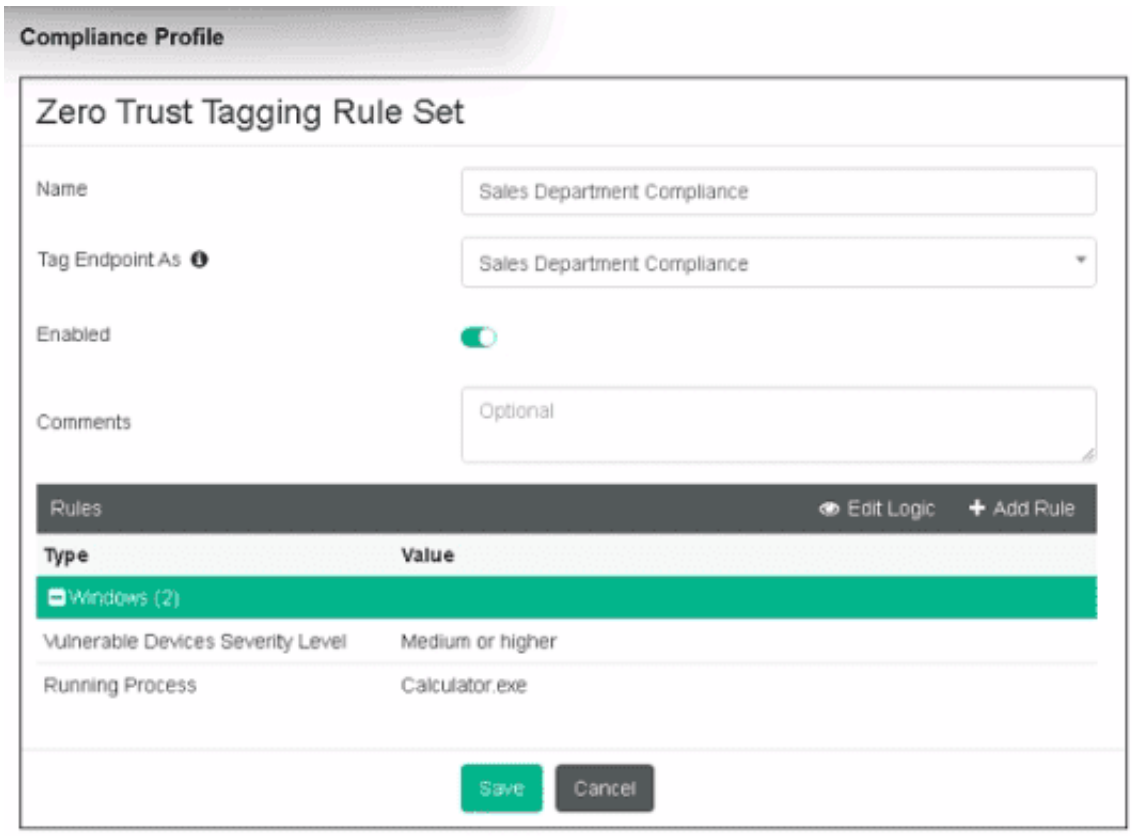


Based on the FortiClient tog details shown in the exhibit, which two statements ace true? (Choose two.)

A. The filename Is Unconfirmed 899290.crdovnload.
B. The file status is Quarantined
C. The filename is sent to FortiSandbox for further inspection.
D. The file location is \??\D:\Users\.

Answer: AB

NEW QUESTION 36
Refer to the exhibit.



Based on the settings shown in the exhibit, which two actions must the administrator take to make the endpoint compliant? (Choose two.)

A. Enable the web filter profile.
B. Run Calculator application on the endpoint.
C. Integrate FortiSandbox tor infected file analysis
D. Patch applications that have vulnerability rated as high or above.

Answer: BD

NEW QUESTION 37
Which two VPNtypes can a FortiClientendpoint user inmate from the Windows command prompt? (Choose two)

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

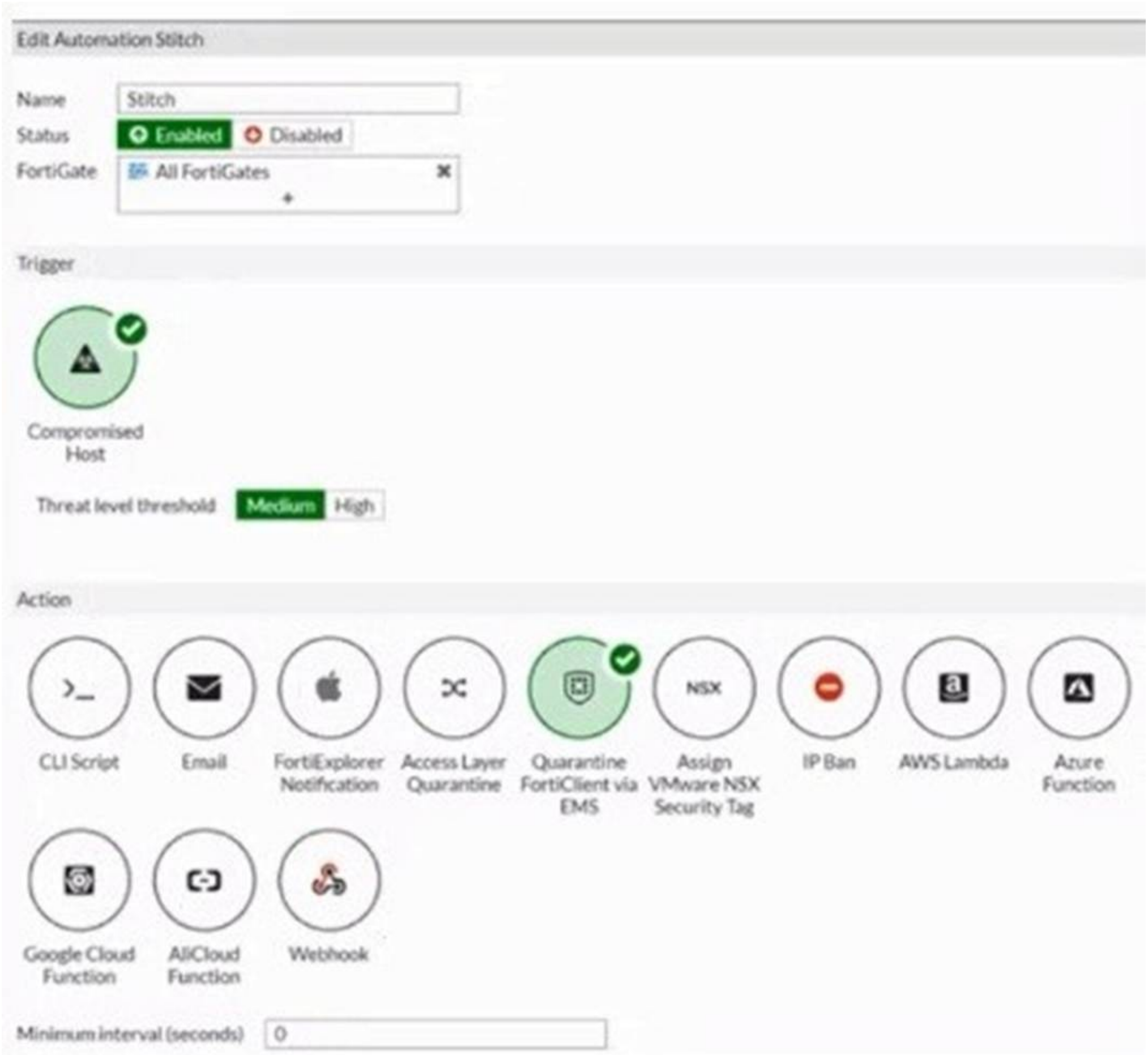
Answer: CD

NEW QUESTION 38
A company must integrate the FortiClient EMS with their existing identity management infrastructure for user authentication, and implement and enforce administrative access with multi-factor authentication (MFA). Which two authentication methods can they use in this scenario? (Choose two answers)

A. LDAPS
B. RADIUS
C. TACACS
D. SAML

Answer: BD

NEW QUESTION 40
Refer to the exhibit.



Based on the Security Fabric automation settings, what action will be taken on compromised endpoints?

A. Endpoints will be quarantined through EMS
B. Endpoints will be banned on FortiGate
C. An email notification will be sent for compromised endpoints
D. Endpoints will be quarantined through FortiSwitch

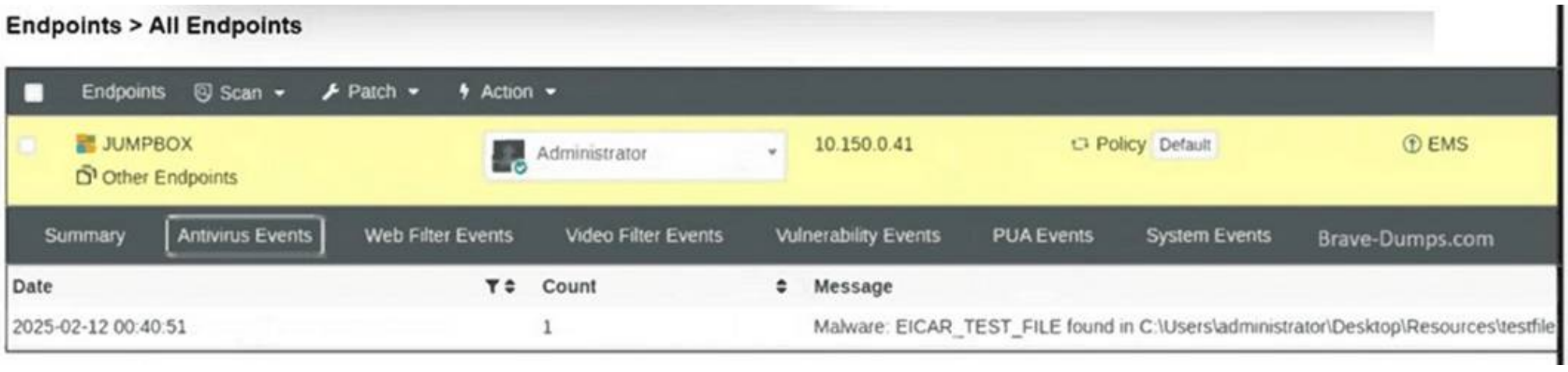
Answer: A

NEW QUESTION 41
What is the function of the quick scan option on FortiClient?

A. It scans programs and drivers that are currently running, for threats
B. It performs a full system scan including all files, executable file
C. DLLs, and drivers for throats.
D. It allows users to select a specific file folder on their local hard disk drive (HDD), to scan for threats.
E. It scans executable file
F. DLLs, and drivers that are currently running, for threats.

Answer: B

NEW QUESTION 46
Refer to the exhibit.



You provide a webserver hosting service. An endpoint downloads a test file, testfile.txt, that gets blocked by FortiClient.
Which configuration can you use to make the file accessible on the endpoint? (Choose one answer)

A. Restore access to file directly using FortiClient.
B. Allow the webserver URL in the exclusion list in the web filter profile.
C. Exclude testfile.txt from the malware protection profile.
D. Add the file to the allowlist in quarantine management on FortiClient EMS.

Answer: D

NEW QUESTION 49
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

FCP_FCT_AD-7.4 Practice Exam Features:

* FCP_FCT_AD-7.4 Questions and Answers Updated Frequently

* FCP_FCT_AD-7.4 Practice Questions Verified by Expert Senior Certified Staff

* FCP_FCT_AD-7.4 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* FCP_FCT_AD-7.4 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year