Fortinet

Exam Questions FCP_FCT_AD-7.4

FCP - FortiClient EMS 7.4 Administrator

NEW QUESTION 1
An administrator wants to simplify remote access without asking users to provide user credentials Which access control method provides this solution?

A. ZTNA full mode
B. SSL VPN
C. L2TP
D. ZTNA IP/MAC littering mode

Answer: A

NEW QUESTION 2
Refer to the exhibit.

Based on The settings shown in The exhibit, which statement about FortiClient behaviour is Hue?

A. FortiClient scans infected files when the user copies files to the Resources folder.
B. FortiClient quarantines infected ties and reviews later, after scanning them.
C. FortiClient copies infected files to the Resources folder without scanning them.
D. FortiClient blocks and deletes infected files after scanning them.

Answer: A

NEW QUESTION 3
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

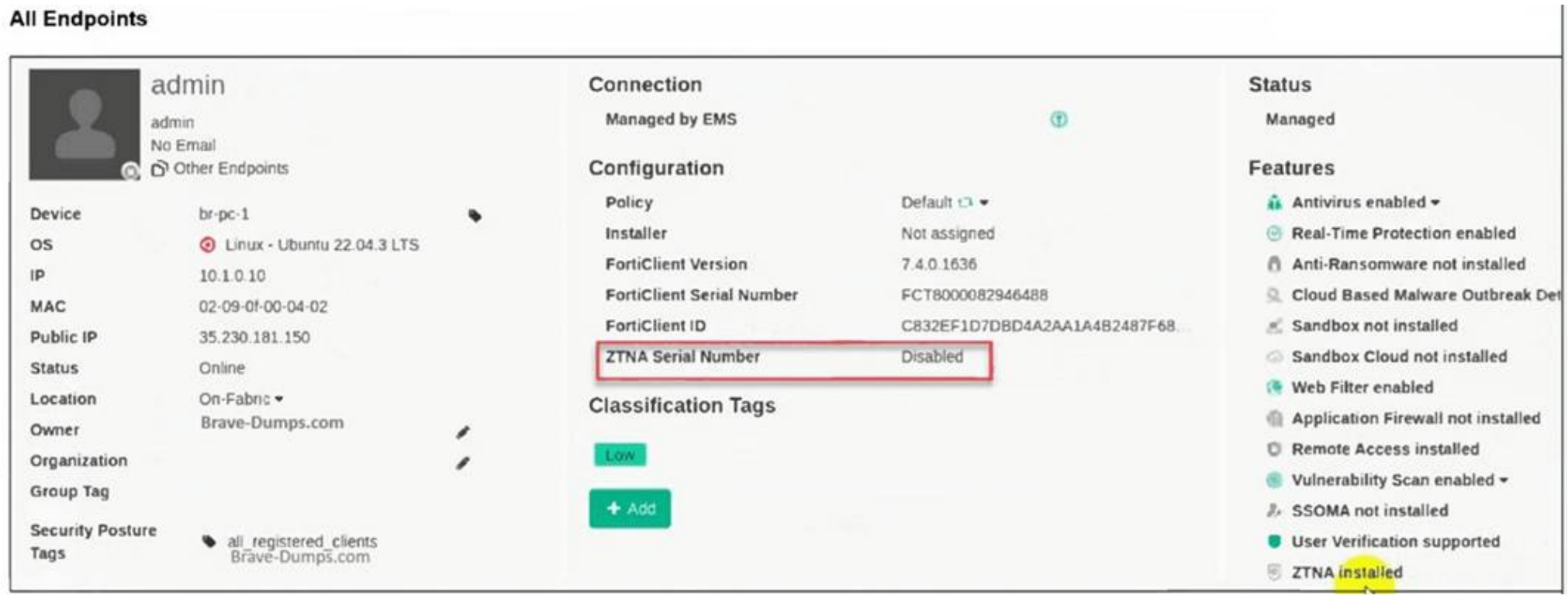
Answer: B

NEW QUESTION 4
A FortiClient EMS administrator has enabled the compliance rule for the sales department Which Fortinet device will enforce compliance with dynamic access control?

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

Answer: C

NEW QUESTION 5
Refer to the exhibit.

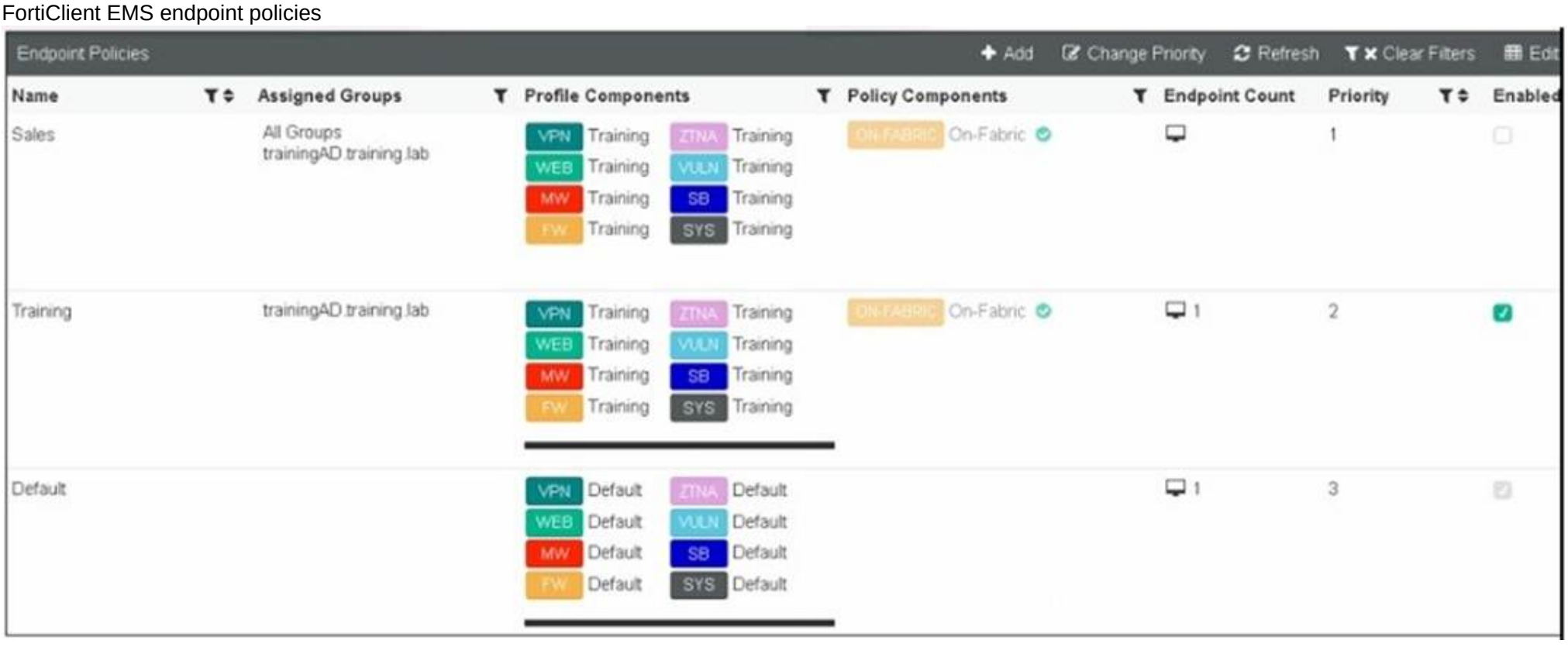


The zero trust network access (ZTNA) serial number on endpoint br-pc-1 is in a disabled state.
What is causing the problem? (Choose one answer)

A. The ZTNA feature is not installed on FortiClient.
B. The ZTNA destinations endpoint profile is disabled.
C. The ZTNA is disabled due to FortiClient disconnected from FortiClient EMS.
D. The ZTNA certificate has been revoked by administrator.

Answer: B

NEW QUESTION 6
FortiClient EMS endpoint policies



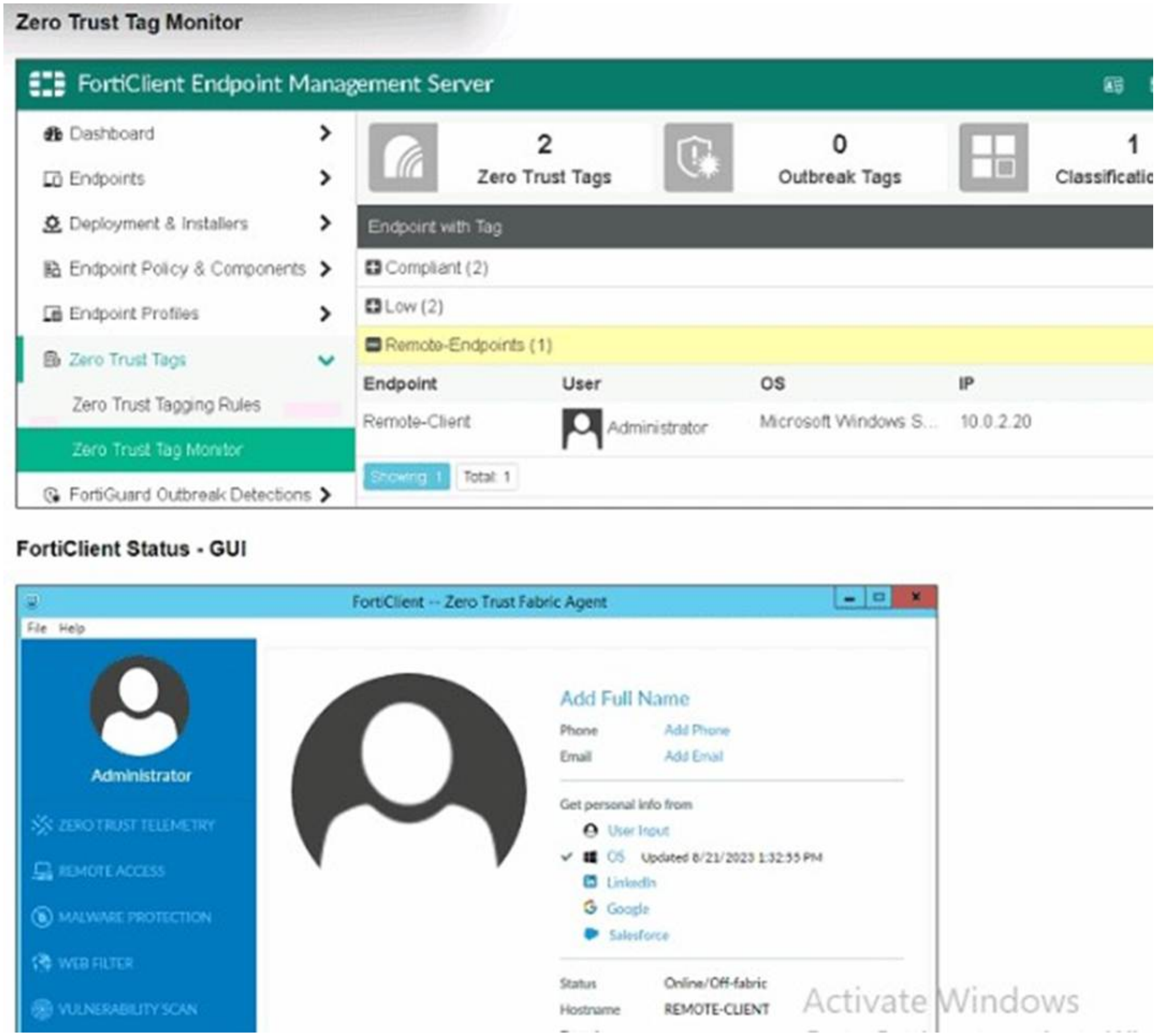
Refer to the exhibit, which shows multiple endpoint policies on FortiClient EMS. Which policy is applied to the endpoint in the AD group trainingAD

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 7

Exhibit.

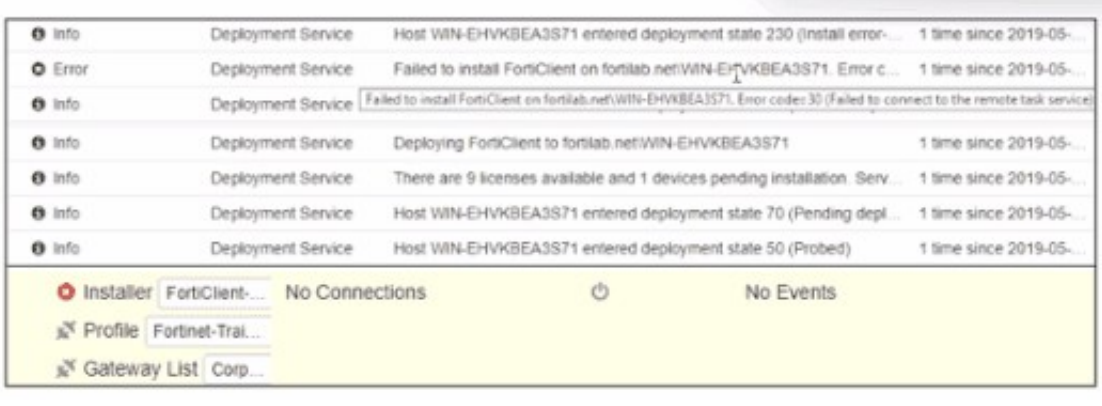


Refer to the exhibits, which show the Zero Trust Tag Monitor and the FortiClient GUI status.
Remote-Client is tagged as Remote-User* on the FortiClient EMS Zero Trust Tag Monitor. What must an administrator do to show the tag on the FortiClient GUI?

A. Change the FortiClient EMS shared settings to enable tag visibility.
B. Change the endpoint alerts configuration to enable tag visibility.
C. Update tagging rule logic to enable tag visibility.
D. Change the FortiClient system settings to enable lag visibility.

Answer: B

NEW QUESTION 8
Exhibit.



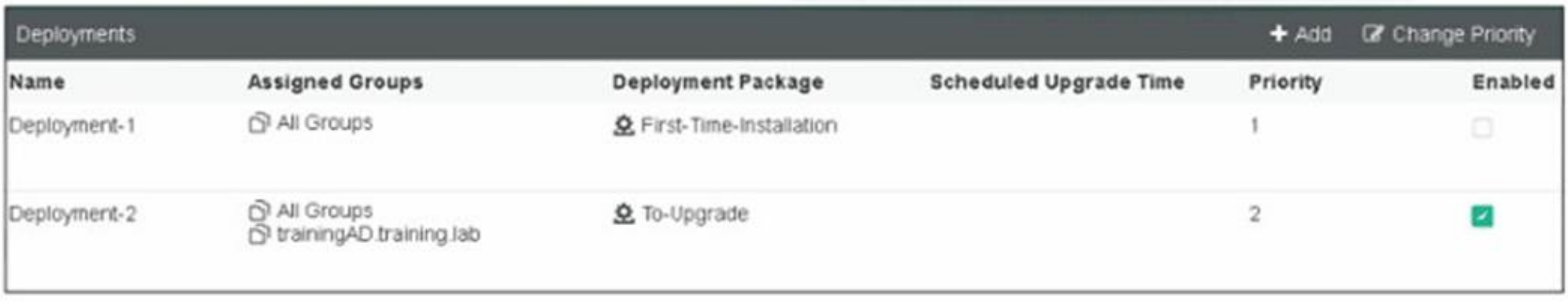
Based on the logs shown in the exhibit, why did FortiClient EMS tail to install FortiClient on the endpoint?

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

NEW QUESTION 9
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?

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

NEW QUESTION 10
Exhibit.

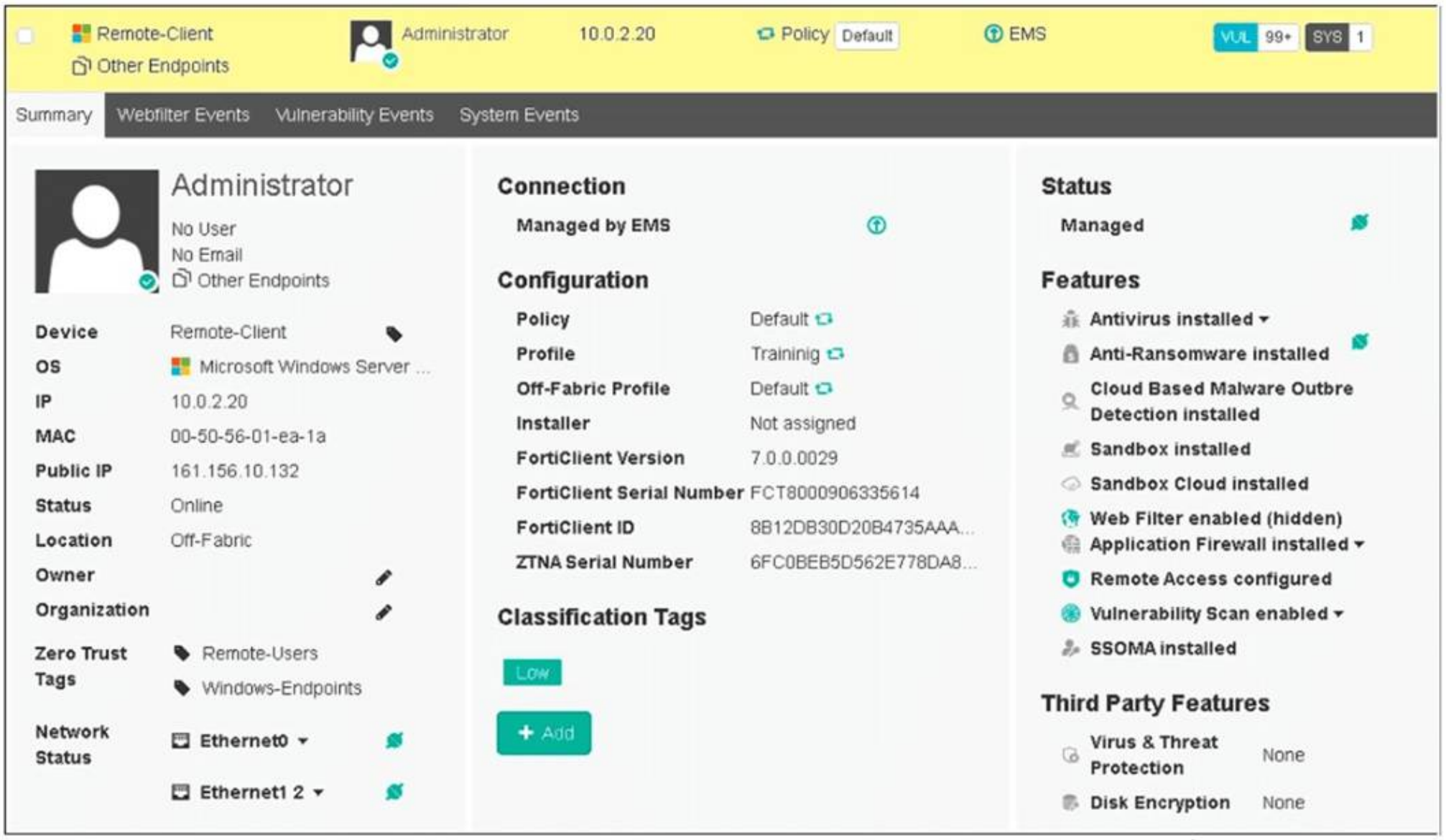
```
1:40:39 PM    Information    Vulnerability   id=96521 msg="A vulnerability scan result has been logged" status=N/A vulncat="Operating
1:40:39 PM    Information    Vulnerability   id=96520 msg="The vulnerability scan status has changed" status="scanning finished" vulnc
1:41:38 PM    Information    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 10
Refer to the exhibit, which shows the endpoint summary information on FortiClient EMS.

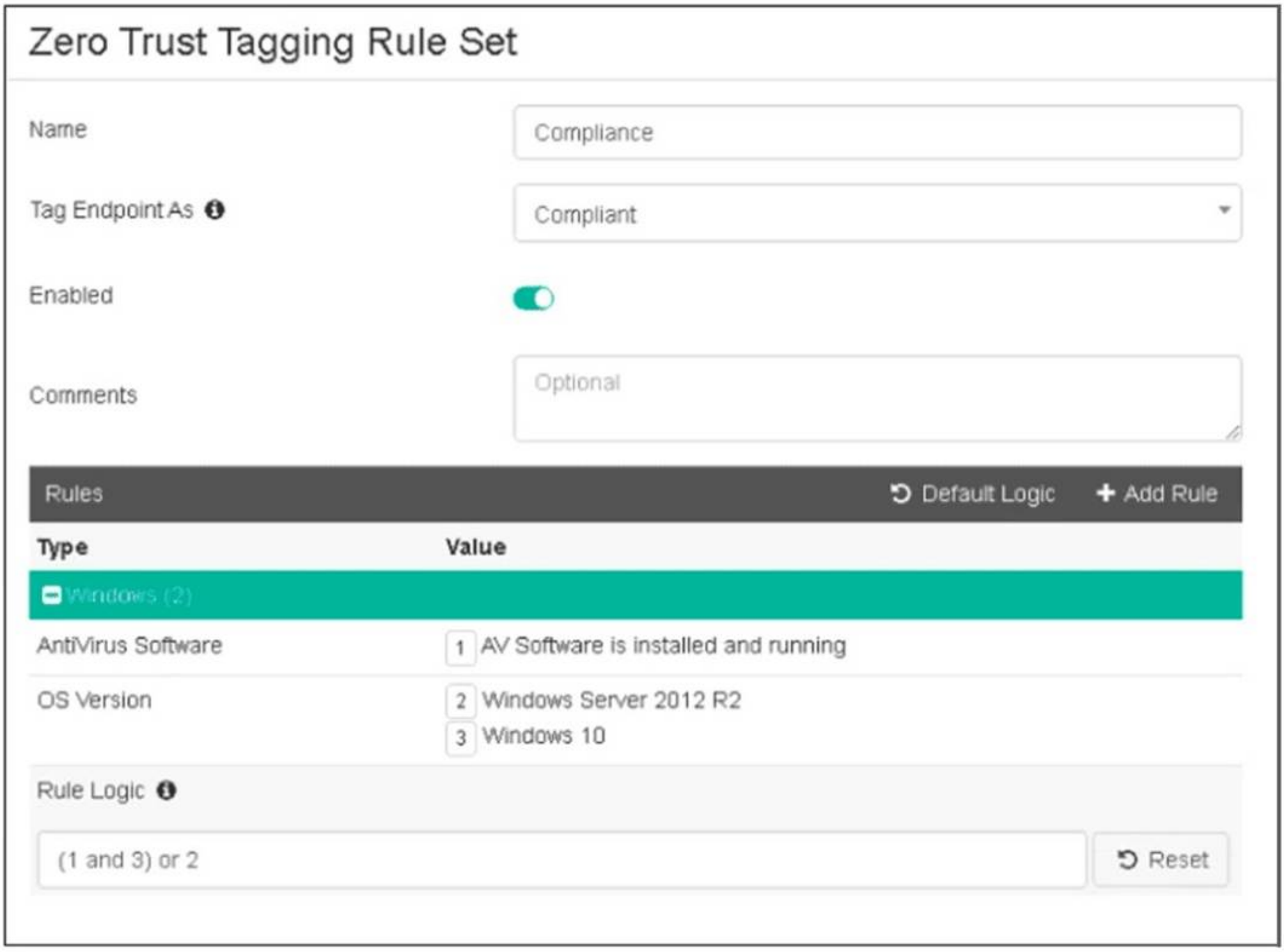


What two conclusions can you make based on the Remote-Client status shown above? (Choose two.)

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.

Answer: BD

NEW QUESTION 14
Refer to the exhibit, which shows the Zero Trust Tagging Rule Set configuration.

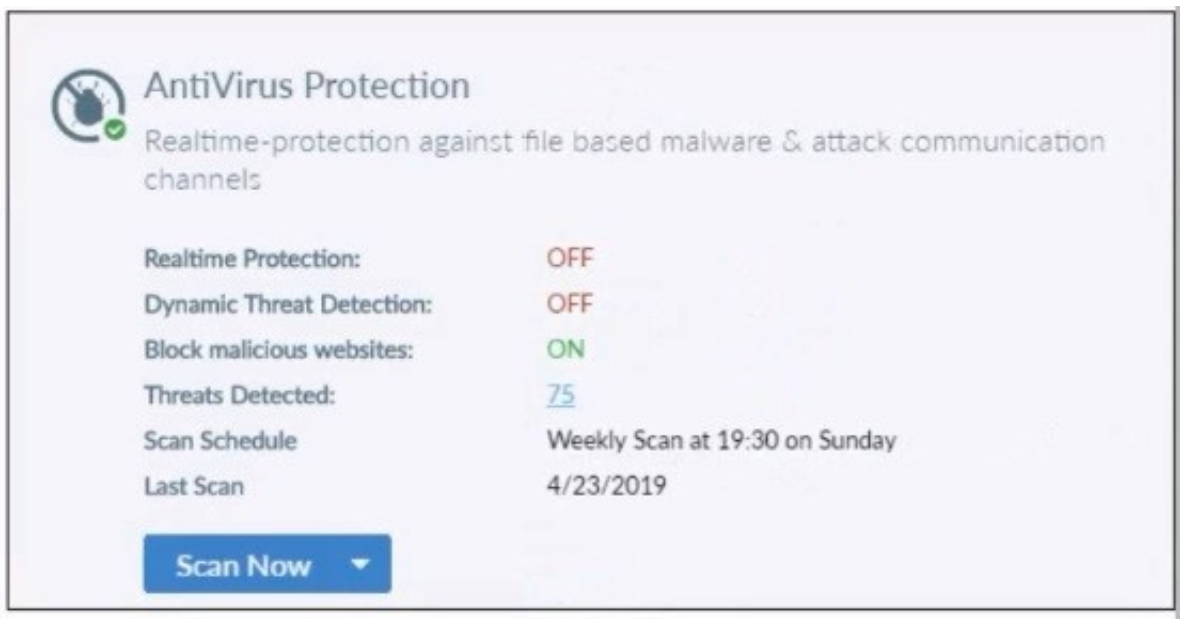


Which two statements about the rule set are true? (Choose two.)

A. The endpoint must satisfy that only Windows 10 is running.
B. The endpoint must satisfy that only AV software is installed and running.
C. The endpoint must satisfy that antivirus is installed and running and Windows 10 is running.
D. The endpoint must satisfy that only Windows Server 2012 R2 is running.

Answer: CD

NEW QUESTION 17
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 22
Which three features does FortiClient endpoint security include? (Choose three.)

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

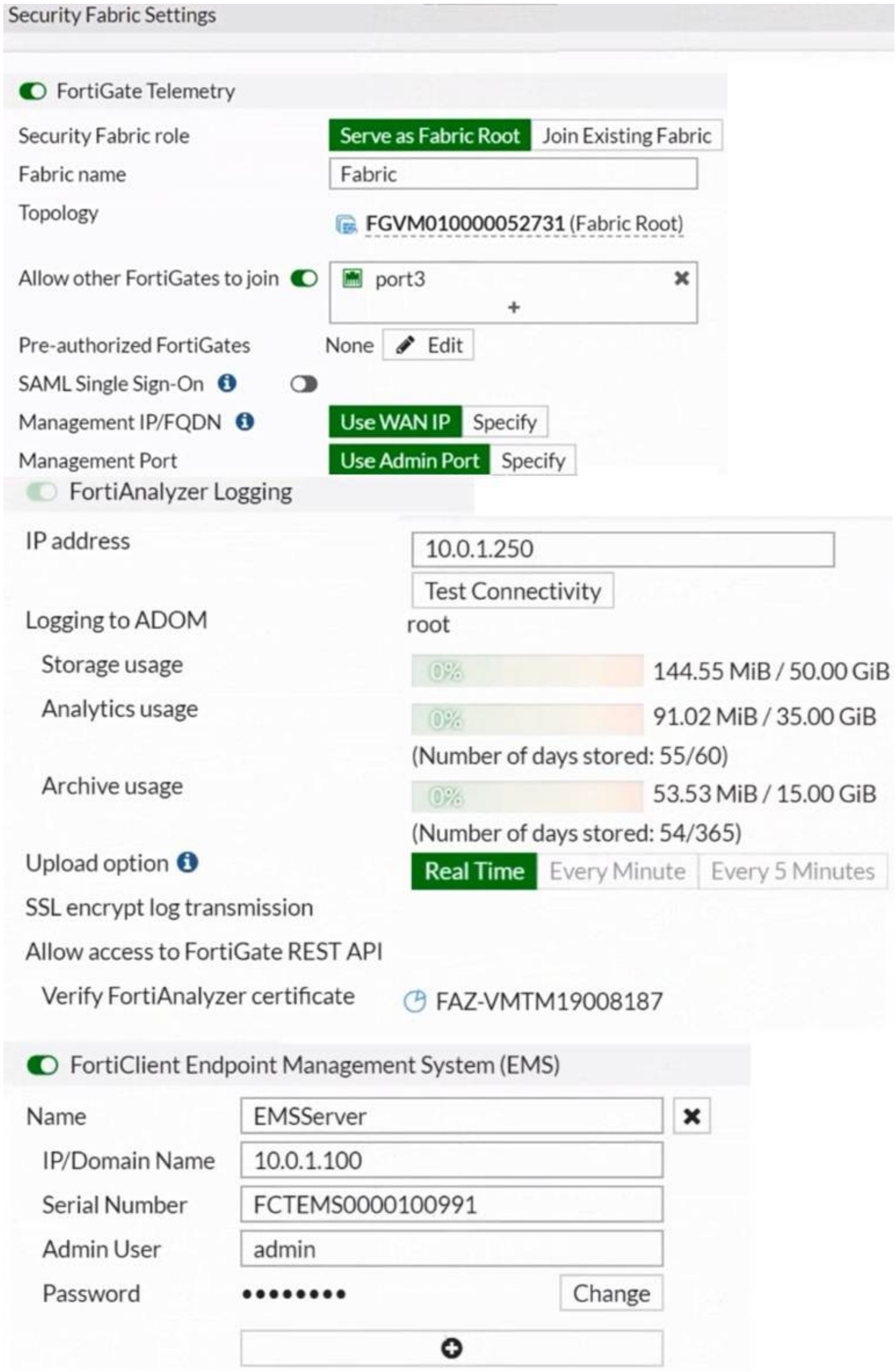
Answer: BDE

NEW QUESTION 23
What does FortiClient do as a fabric agent? (Choose two.)

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

Answer: CD

NEW QUESTION 25
Refer to the exhibits.


Security Fabric Settings
FortiGate Telemetry
Security Fabric role
Serve as Fabric Root
Join Existing Fabric
Fabric name
Fabric
Topology
FGVM010000052731 (Fabric Root)
Allow other FortiGates to join
port3
Pre-authorized FortiGates
None
Edit
SAML Single Sign-On
Management IP/FQDN
Use WAN IP
Specify
Management Port
Use Admin Port
Specify
FortiAnalyzer Logging
IP address
10.0.1.250
Test Connectivity
Logging to ADOM
root
Storage usage
0%
144.55 MiB / 50.00 GiB
Analytics usage
0%
91.02 MiB / 35.00 GiB
(Number of days stored: 55/60)
Archive usage
0%
53.53 MiB / 15.00 GiB
(Number of days stored: 54/365)
Upload option
Real Time
Every Minute
Every 5 Minutes
SSL encrypt log transmission
Allow access to FortiGate REST API
Verify FortiAnalyzer certificate
FAZ-VMTM19008187
FortiClient Endpoint Management System (EMS)
Name
EMSServer
IP/Domain Name
10.0.1.100
Serial Number
FCTEMS0000100991
Admin User
admin
Password
Change

Based on the FortiGate Security Fabric settings shown in the exhibits, what must an administrator do on the EMS server to successfully quarantine an endpoint. when it is detected as a compromised host (IoC)?

A. The administrator must enable remote HTTPS access to EMS.
B. The administrator must enable FQDN on EMS.
C. The administrator must authorize FortiGate on FortiAnalyzer.
D. The administrator must enable SSH access to EMS.

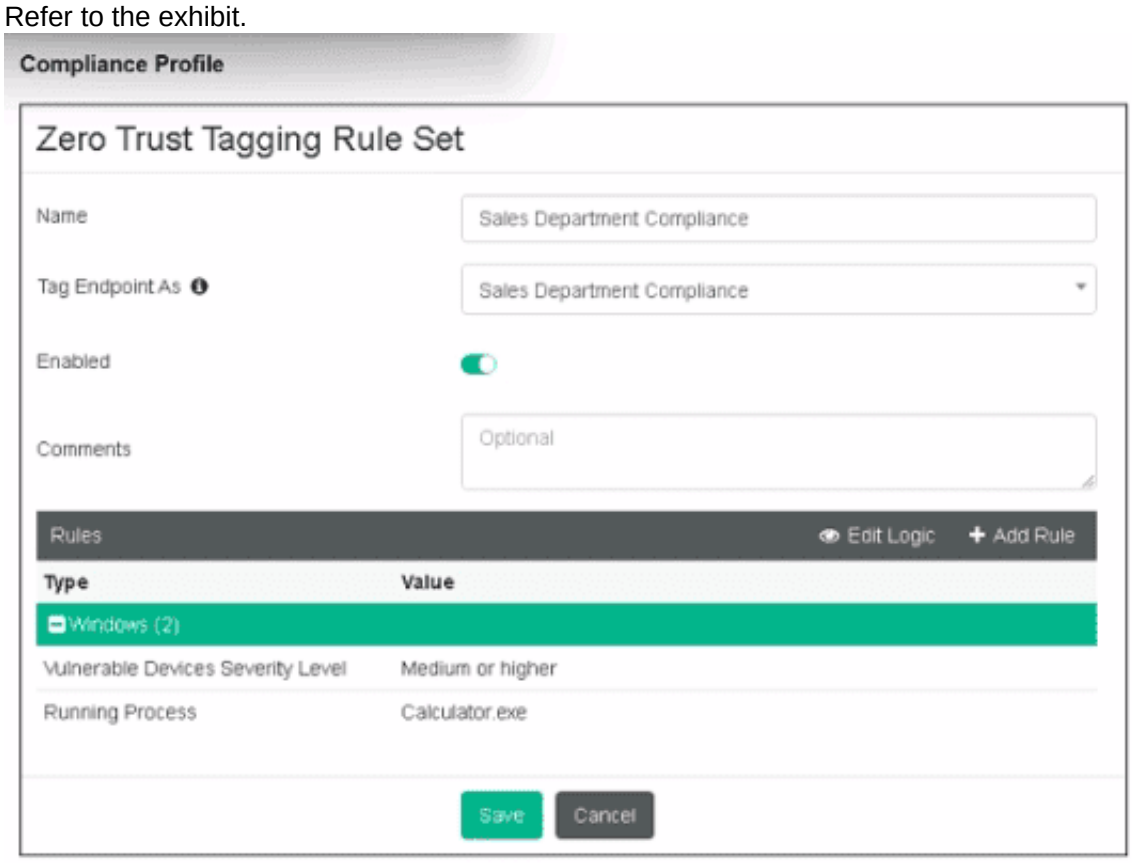
Answer: A

NEW QUESTION 29
Which statement about the FortiClient enterprise management server is true?

A. It receives the configuration information of endpoints from ForuGate.
B. It provides centralized management of multiple endpoints running FortiClient software.
C. It enforces compliance on the endpoints using tags
D. It receives the CA certificate from FortiGate to validate client certrficates.

Answer: C

NEW QUESTION 32
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 33
An administrator has lost web access to the FortiClient EMS console, and the web page to access to the console is timing out.
How can the administrator gather information to investigate the issue? (Choose one answer)

A. Use the CLI diagnostic tool on the EMS server.
B. Download the webserver logs from the PostgreSQL server.
C. Use the diagnostic logs option from the FortiClient EMS GUI.
D. Download the log generator from the support site and run it on the EMS server.

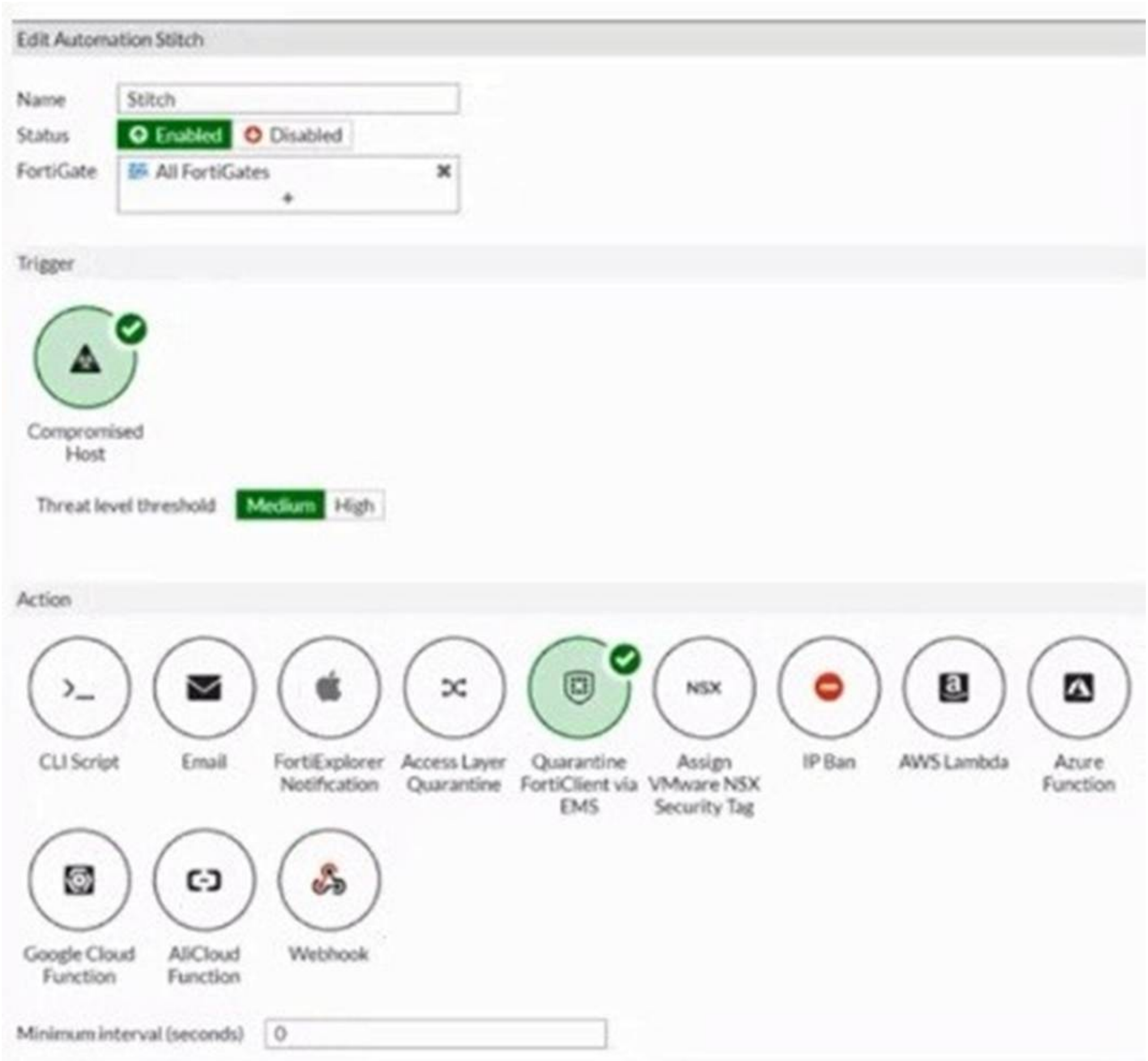
Answer: A

NEW QUESTION 35
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 39
Refer to the exhibit.

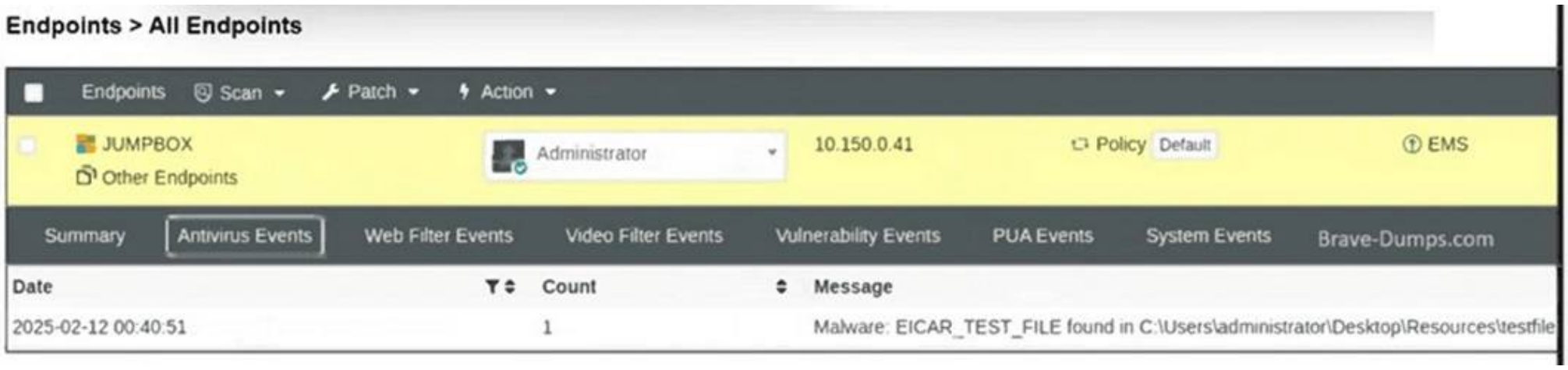


Based on the Security Fabric automation settings, what action will be taken on compromised endpoints?

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
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 43
Which component or device shares ZTNA tag information through Security Fabric integration?

A. FortiGate
B. FortiGate Access Proxy
C. FortiClient

Answer: A

NEW QUESTION 44
Why does FortiGate need the root CA certificate of FortiCient EMS?

A. To revoke FortiClient client certificates
B. To sign FortiClient CSR requests
C. To update FortiClient client certificates
D. To trust certificates issued by FortiClient EMS

Answer: A

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