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
Which two statements about FortiClient EMS integration with Active Directory (AD) are true? (Choose two answers)

A. FortiClient EMS has full read-write access on the AD server.
B. FortiClient installations on domain endpoints can deployed from FortiClient EMS.
C. Endpoint profiles can be assigned to endpoints based on domain groups.
D. Imported AD endpoints cannot be directly deleted on FortiClient EMS

Answer: BC

NEW QUESTION 4
Refer to the exhibit.

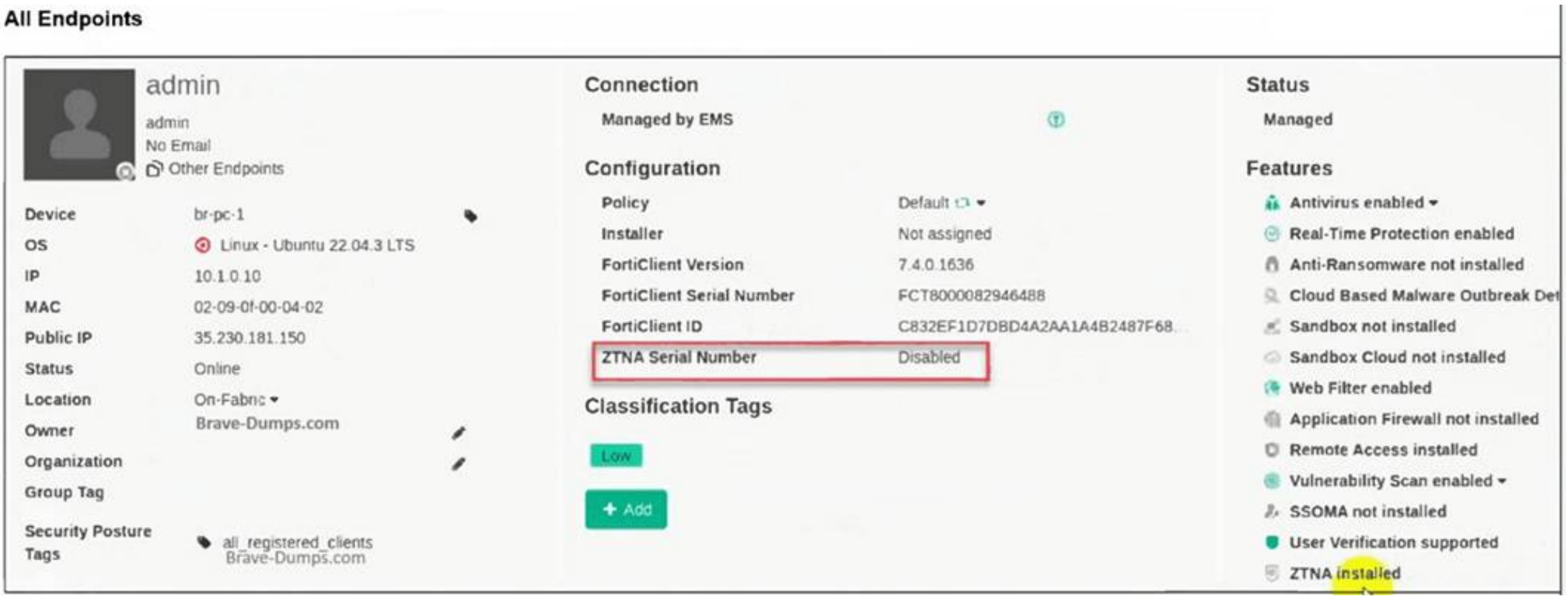
```
xx/xx/20xx 9:05:05 AM   Notice  Firewall        date=20xx-xx-xx time=09:05:04 logver=2 type=traffic level=notice sessionid=34252360
hostname=Win-Internal uid=C7F302B1D3EB4F05A77E38AD6202B8D7 devid=FCT8003611939390 fgtserial=FGVM010000042532 regip=N/A
srcname=firefox.exe srcproduct=Firefox srcip=10.0.1.10 srcport=62401 direction=outbound destinationip=199.59.148.82 remotename=N/A
destinationport=80 user=Administrator@TRAININGAD.TRAINING.LAB proto=6 rcvdbyte=N/A sentbyte=N/A utmaction=blocked utmevent=appfirewall
threat=Twitter vd=root fctver=5.4.0.0780 os="Microsoft Windows Server 2012 R2 Standard Edition, 64-bit (build 9600)"
usingpolicy="default" service=http

xx/xx/20xx 9:05:54 AM   Notice  Firewall        date=20xx-xx-xx time=09:05:53 logver=2 type=traffic level=notice sessionid=34252360
hostname=Win-Internal uid=C7F302B1D3EB4F05A77E38AD6202B8D7 devid=FCT8003611939390 fgtserial=FGVM010000042532 regip=N/A
srcname=firefox.exe srcproduct=Firefox srcip=10.0.1.10 srcport=62425 direction=outbound destinationip=104.25.62.28 remotename=N/A
destinationport=443 user=Administrator@TRAININGAD.TRAINING.LAB proto=6 rcvdbyte=N/A sentbyte=N/A utmaction=blocked
utmevent=appfirewall threat=Proxy.Websites vd=root fctver=5.4.0.0780 os="Microsoft Windows Server 2012 R2 Standard Edition, 64-bit
(build 9600)" usingpolicy="default" service=https


xx/xx/20xx 9:28:23 AM    Notice    Firewall    date=20xx-xx-xx time=09:28:22 logver=2 type=traffic level=notice sessionid=26453064
hostname=Win-Internal uid=C7F302B1D3EB4F05A77E38AD6202B8D7 devid=FCT8003611939390 fgtserial=FGVM010000042532 regip=N/A
srcname=firefox.exe srcproduct=Firefox srcip=10.0.1.10 srcport=62759 direction=outbound destinationip=208.71.44.31 remotename=N/A
destinationport=80 user=Administrator@TRAININGAD.TRAINING.LAB proto=6 rcvdbyte=N/A sentbyte=N/A utmaction=blocked utmevent=appfirewall
threat=Yahoo.Games vd=root fctver=5.4.0.0780 os="Microsoft Windows Server 2012 R2 Standard Edition, 64-bit (build 9600)"
usingpolicy="default" service=http
```

Based on the FortiClient logs shown in the exhibit which application is blocked by the application firewall?

A. Twitter
B. Facebook
C. Internet Explorer
D. Firefox

Answer: D

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
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

Answer: BCE

NEW QUESTION 7
An administrator is required to maintain a software vulnerability on the endpoints, without showing the feature on the FortiClient. What must the administrator do to

achieve this requirement?

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

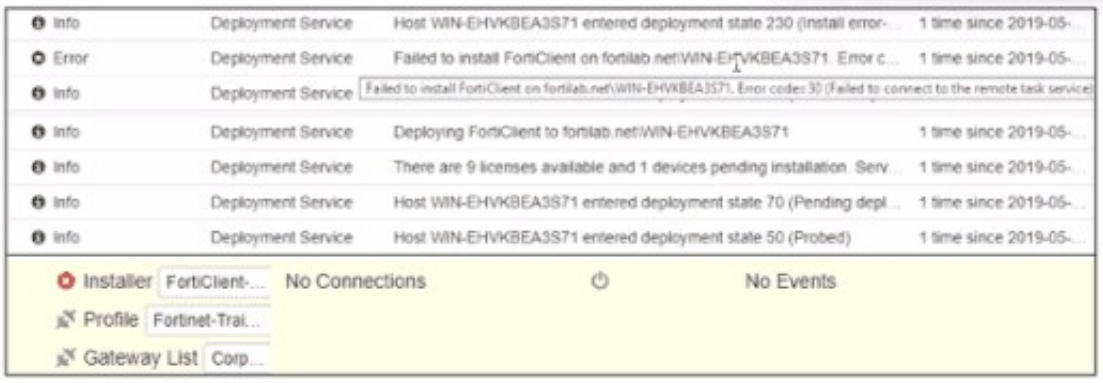
Answer: C

NEW QUESTION 8
A FortiClient EMS administrator is implementing additional security on FortiClient for compliance checks. Which tags can the administrator configure to detect endpoints based on vulnerability severity levels? (Choose one answer)

A. Outbreak alert tags
B. Classification tags
C. Fabric tags
D. Security posture tags

Answer: D

NEW QUESTION 9
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 10
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 10
An administrator installs FortiClient on Windows Server.
What is the default behavior of real-time protection control?

A. Real-time protection must update AV signature database
B. Real-time protection sends malicious files to FortiSandbox when the file is not detected locally
C. Real-time protection is disabled
D. Real-time protection must update the signature database from FortiSandbox

Answer: C

NEW QUESTION 14
When site categories are disabled in FortiClient web filter, which feature can be used to protect the endpoint from malicious web access?

A. Real-time protection list
B. Block malicious websites on antivirus
C. FortiSandbox URL list
D. Web exclusion list

Answer: D

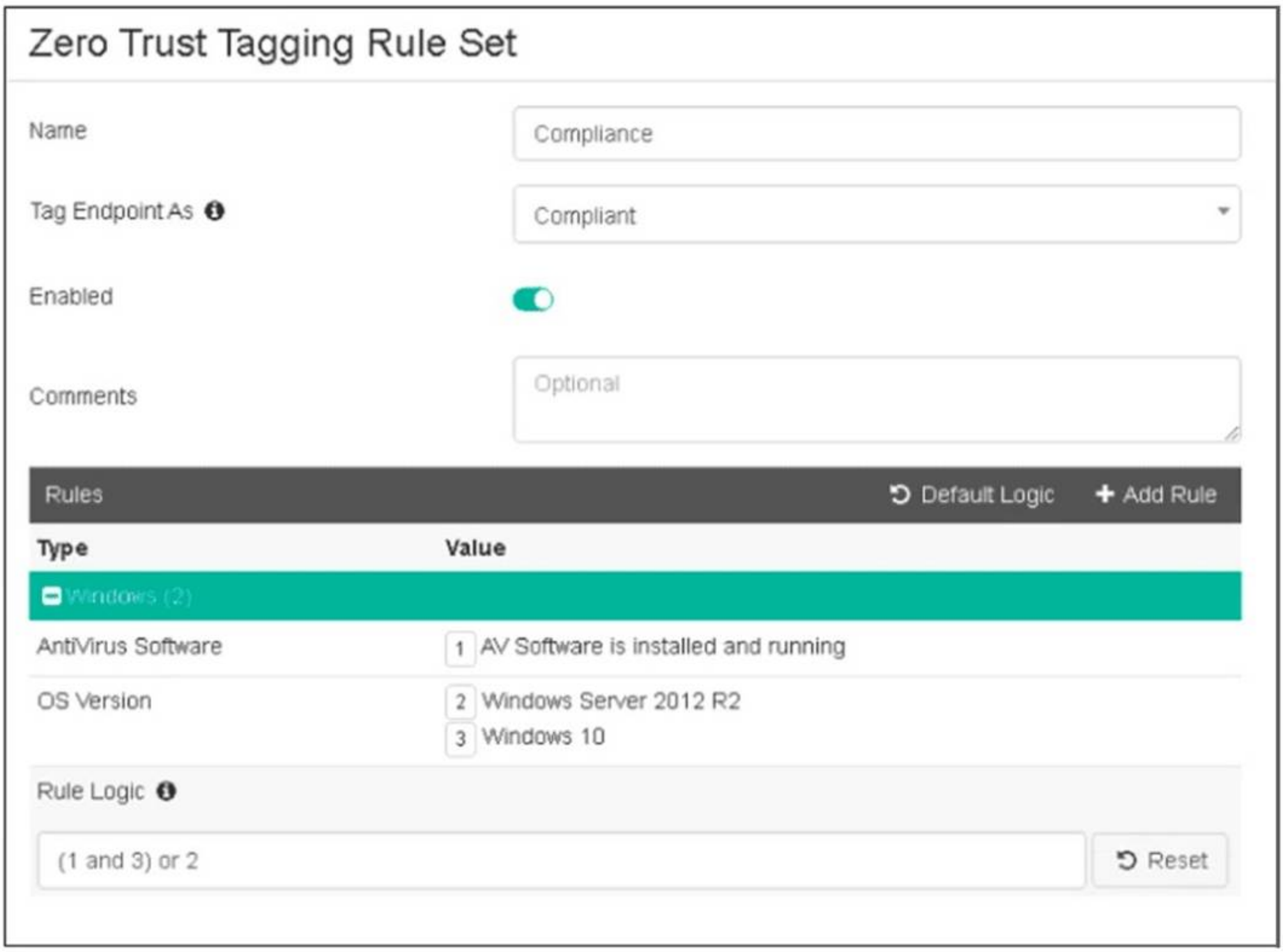
NEW QUESTION 19
An administrator deploys a FortiClient installation through the Microsoft AD group policy After installation is complete all the custom configuration is missing.

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 22
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 24
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 26
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 31
An administrator installs FortiClient EMS in the enterprise.
Which component is responsible for enforcing protection and checking security posture?

A. FortiClient EMS tags
B. FortiClient vulnerability scan
C. FortiClient
D. FortiClient EMS

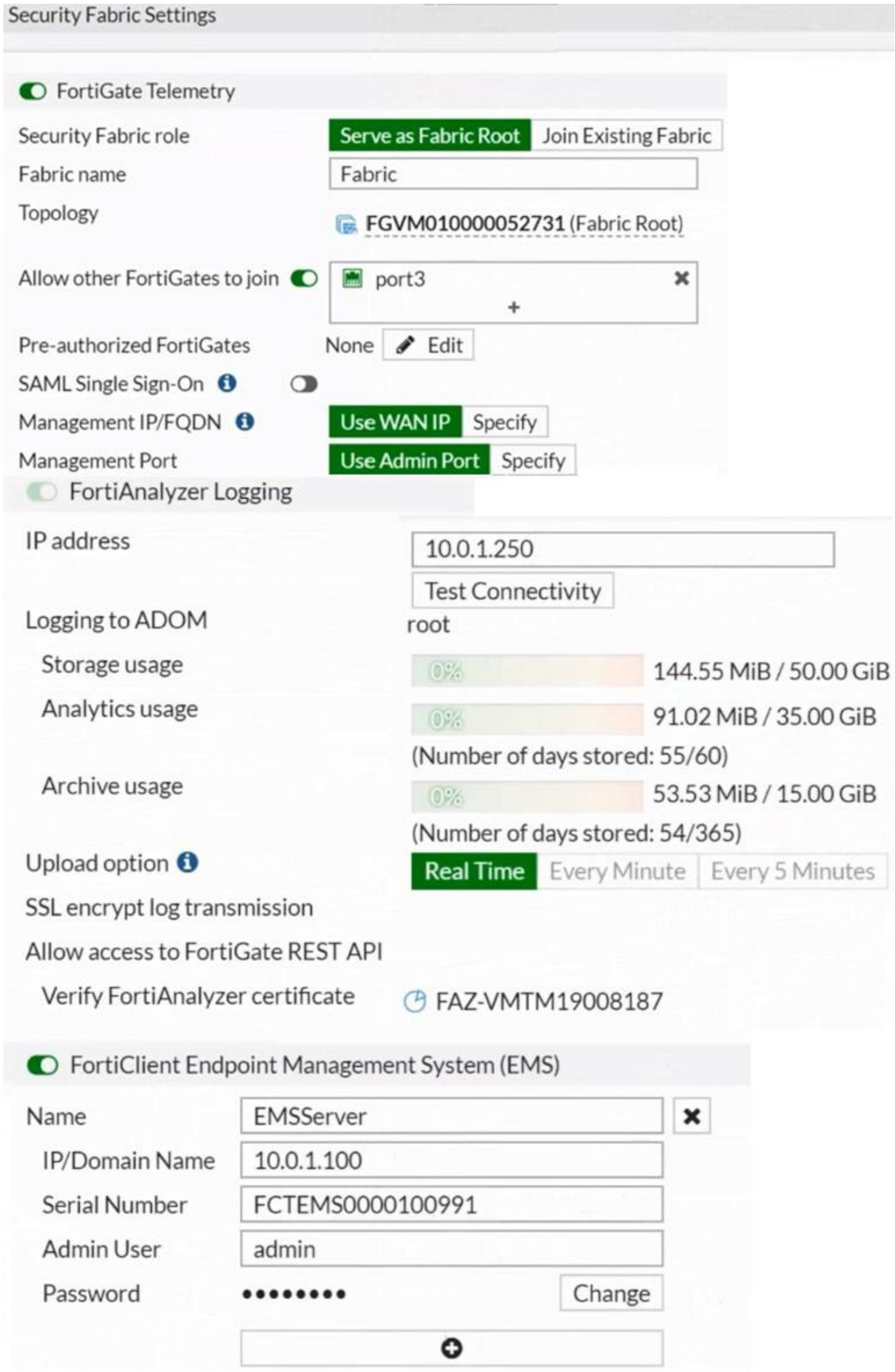
Answer: C

NEW QUESTION 34
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 39
Refer to the exhibits.

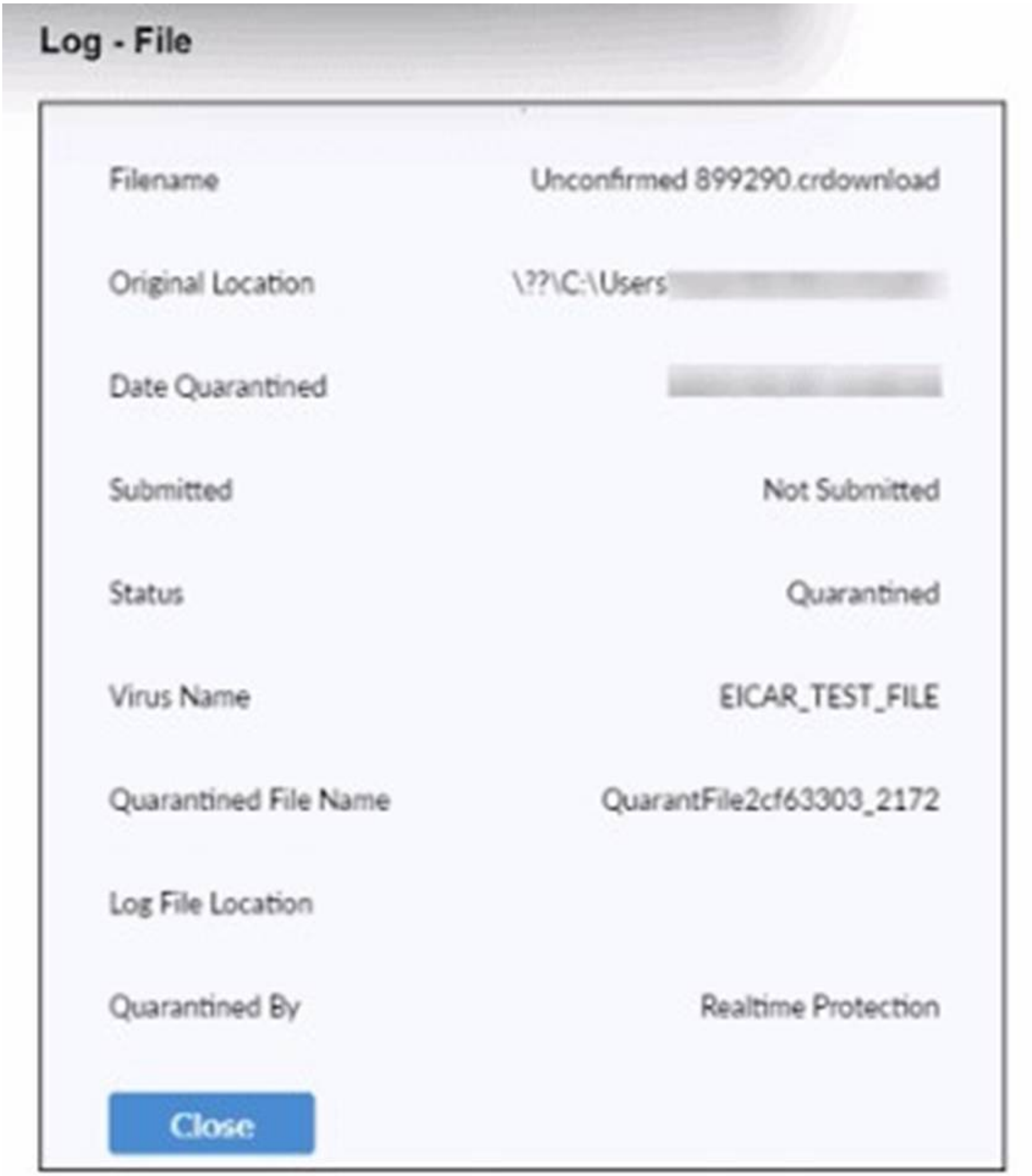

Security Fabric Settings
FortiGate Telemetry
Security Fabric role
Serve as Fabric Root
Join Existing Fabric
Fabric name
Fabric
Topology
FGVM010000052731 (Fabric Root)
Allow other FortiGates to join
port3
Pre-authorized FortiGates
None
Edit
SAML Single Sign-On
Management IP/FQDN
Use WAN IP
Specify
Management 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 44
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 46
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 50
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 53
Which component or device shares ZTNA tag information through Security Fabric integration?

A. FortiGate
B. FortiGate Access Proxy
C. FortiClient

Answer: A

NEW QUESTION 54
Which security attribute is verified during the SSL connection negotiation between FortiClient and FortiClient EMS to mitigate man-in-the-middle (MITM) attacks? (Choose one answer)

A. serial number (SN)
B. common name (CN)
C. location (L)
D. organization (O)

Answer: B

NEW QUESTION 56
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 58
.....

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