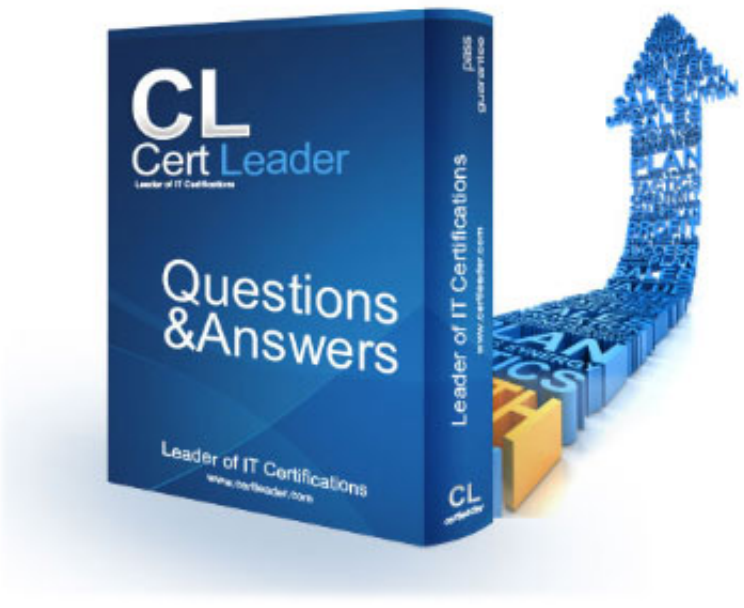
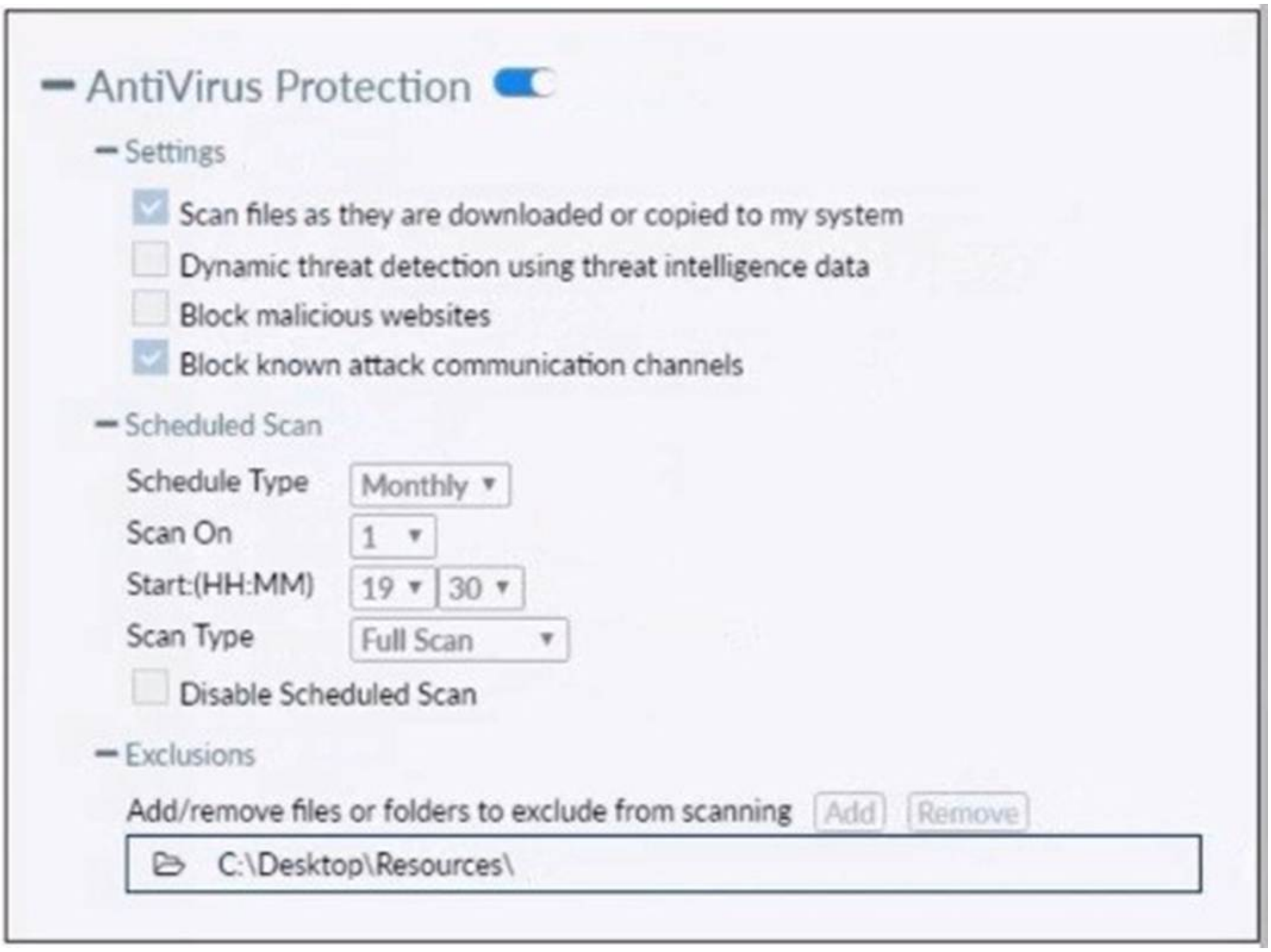
FCP_FCT_AD-7.4 Dumps

FCP - FortiClient EMS 7.4 Administrator

https://www.certleader.com/FCP_FCT_AD-7.4-dumps.html



NEW QUESTION 1
Refer to the exhibit.



Based on the settings shown in the exhibit which statement about FortiClient behavior is true?

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

Answer: A

NEW QUESTION 2
Which two are benefits of using multi-tenancy mode on FortiClient EMS? (Choose two.)

A. Separate host servers manage each site.
B. Licenses are shared among sites
C. The fabric connector must use an IP address to connect to FortiClient EMS.
D. It provides granular access and segmentation.

Answer: CD

NEW QUESTION 3
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 4
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 5
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

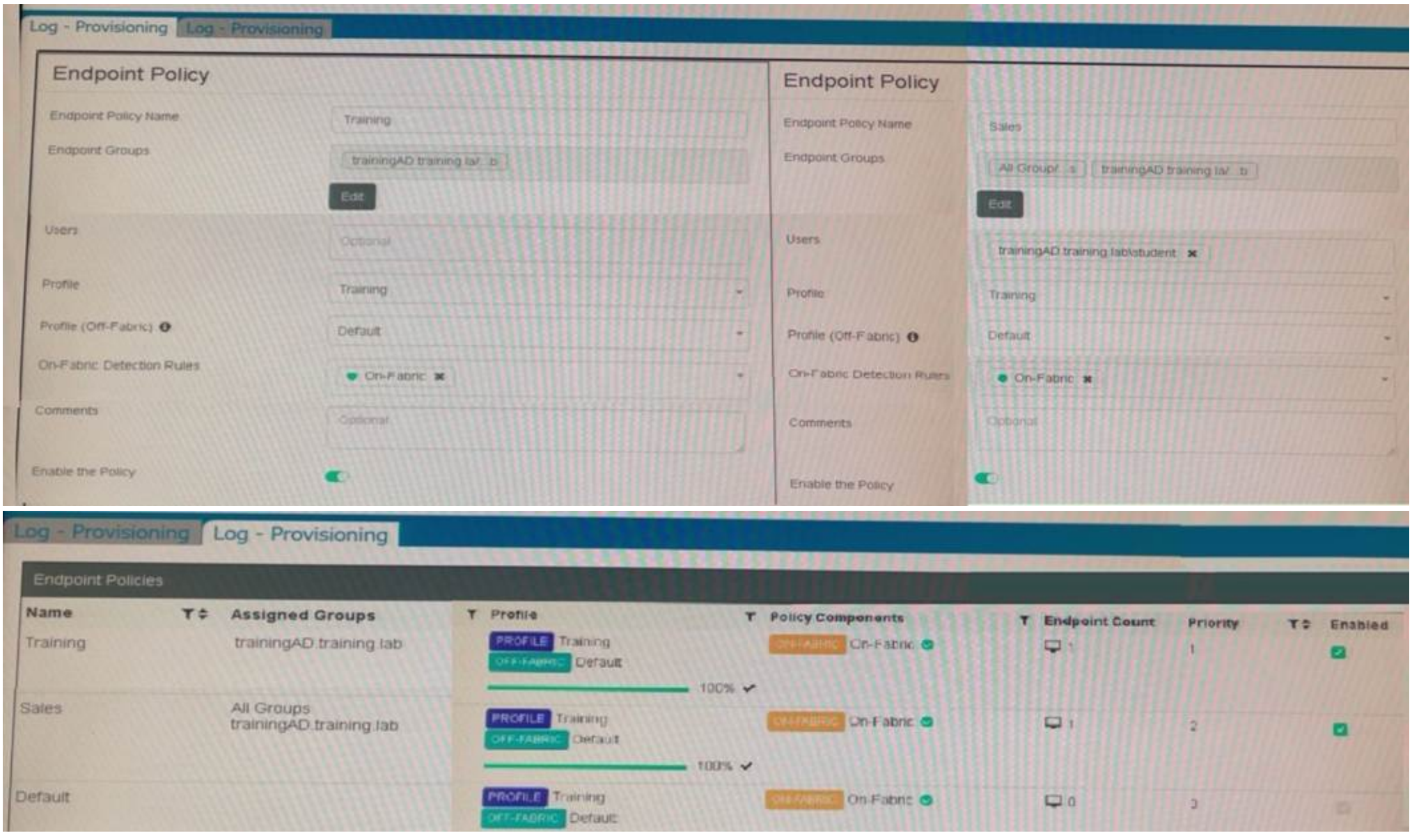
Answer: BC

NEW QUESTION 6
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 7
Refer to the exhibits.



Which shows the configuration of endpoint policies.
Based on the configuration, what will happen when someone logs in with the user account student on an endpoint in the trainingAD domain?

A. FortiClient EMS will assign the Sales policy
B. FortiClient EMS will assign the Training policy
C. FortiClient EMS will assign the Default policy
D. FortiClient EMS will assign the Training policy for on-fabric endpoints and the Sales policy for the off-fabric endpoint

Answer: B

NEW QUESTION 8
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 9
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 10
An administrator has a requirement to add user authentication to the ZTNA access for remote or off-fabric users Which FortiGate feature is required m addition to ZTNA?

A. FortiGate FSSO
B. FortiGate certificates
C. FortiGate explicit proxy
D. FortiGate endpoint control

Answer: C

NEW QUESTION 10
Which component or device shares device status information through ZTNA telemetry?

A. FortiClient
B. FortiGate
C. FortiGate Access Proxy
D. FortiClient EMS

Answer: A

NEW QUESTION 11
A new chrome book is connected in a school's network.
Which component can the EMS administrator use to manage the FortiClient web filter extension installed on the Google Chromebook endpoint?

A. FortiClient EMS
B. FortiClient site categories
C. FortiClient customer URL list
D. FortiClient web filter extension

Answer: D

NEW QUESTION 13
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 18
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 20
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 22
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 25
Which component or device defines ZTNA lag information in the Security Fabric integration?

A. FortiClient
B. FortiGate
C. FortiClient EMS
D. FortiGate Access Proxy

Answer: C

NEW QUESTION 28
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

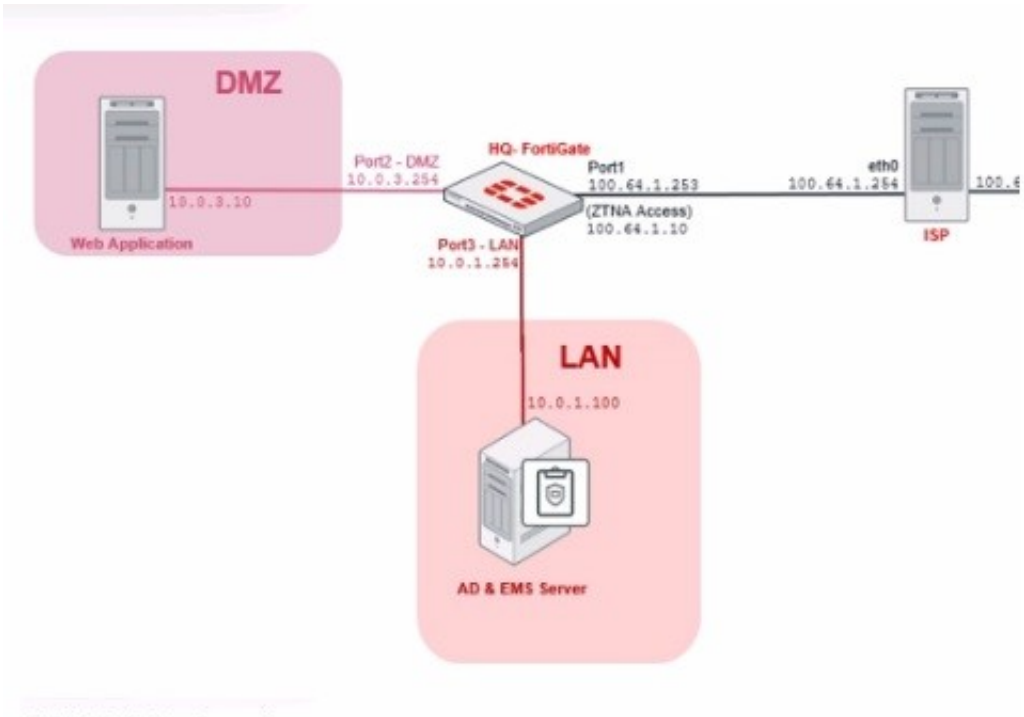
Answer: A

NEW QUESTION 30
Which statement about FortiClient comprehensive endpoint protection is true?

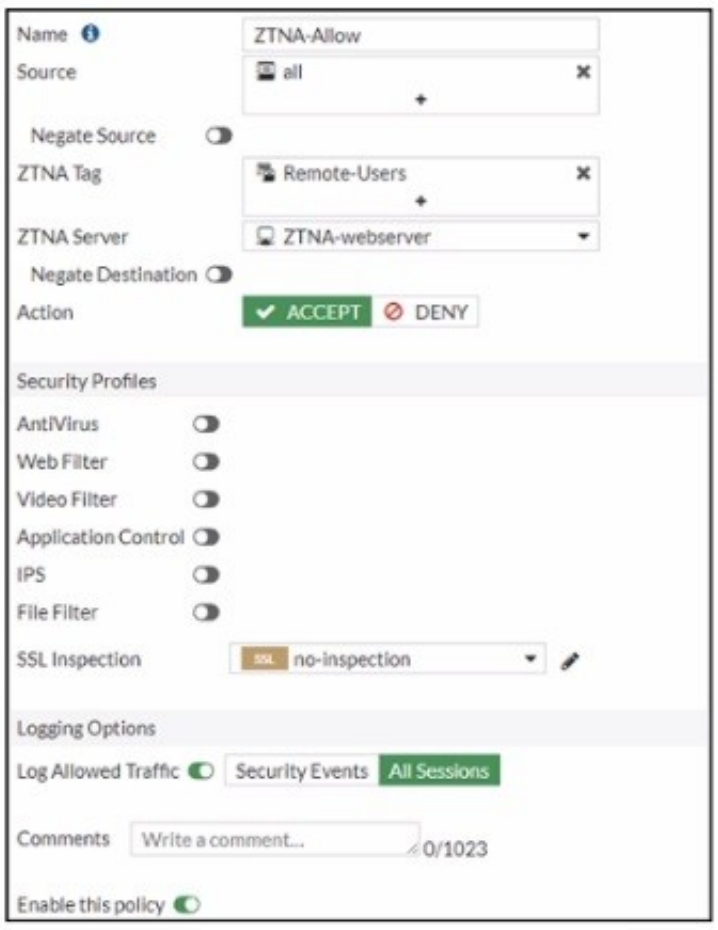
A. It helps to safeguard systems from email spam
B. It helps to safeguard systems from data loss.
C. It helps to safeguard systems from DDoS.
D. lt helps to safeguard systems from advanced security threats, such as malware.

Answer: D

NEW QUESTION 32
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 37
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.

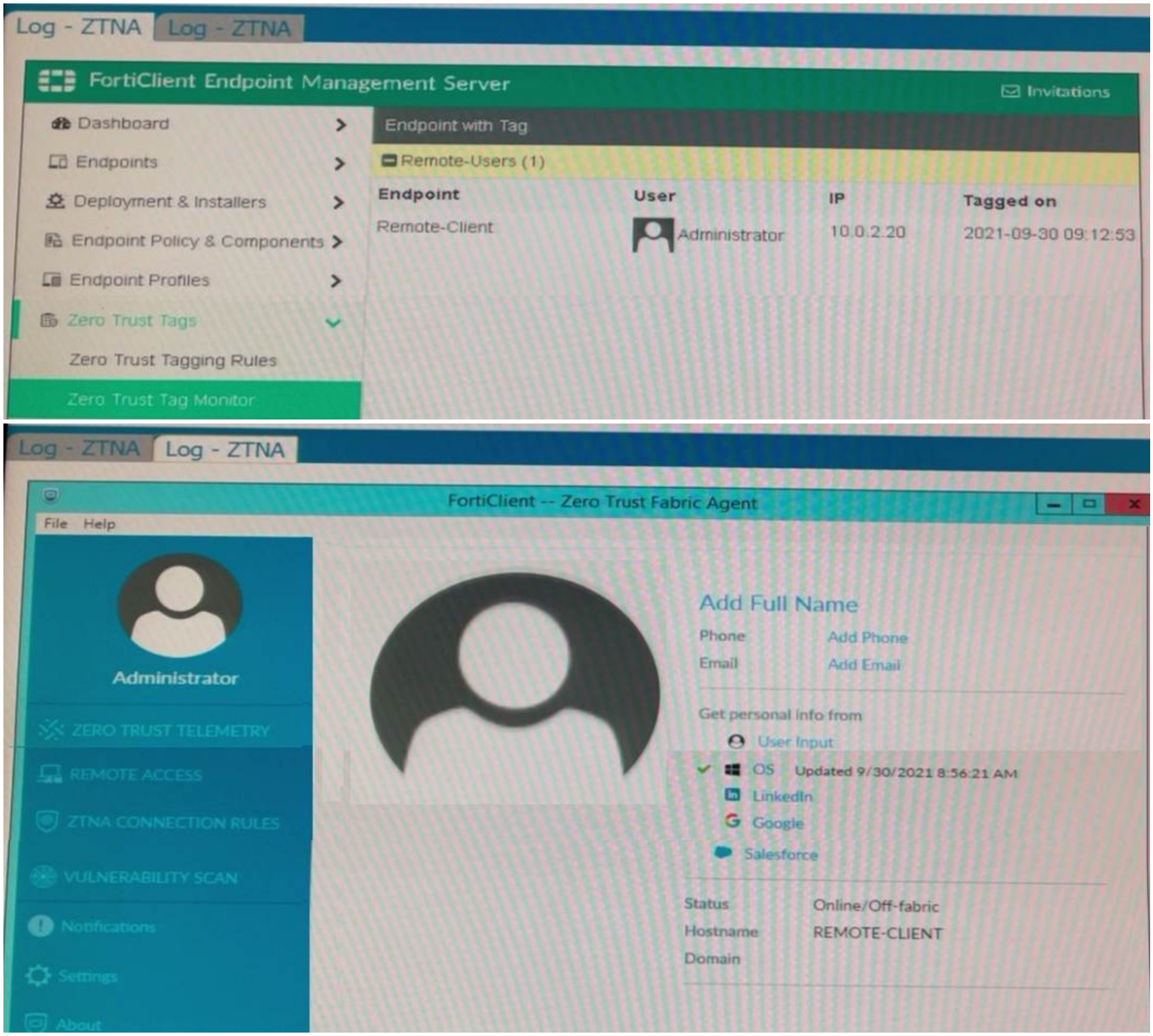
Answer: BC

NEW QUESTION 42
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 46
Refer to the exhibit.



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?

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

NEW QUESTION 51
Refer to the exhibit, which shows the output of the ZTNA traffic log on FortiGate.

```
eventtime=1633084101662546935 tz="-0700" logid="0000000013" type="traffic"
subtype="forward" level="notice" vd="root" srcip=100.64.2.253 srcport=58664 srcintf="port1"
srcintfrole="wan" dstip=100.64.1.10 dstport=9443 dstintf="root" dstintfrole="undefined"
srccountry="Reserved" dstcountry="Reserved" sessionid=5215 proto=6 action="deny" policyid=0
policytype="proxy-policy" service="tcp/9443" trandisp="noop" duration=0 sentbyte=0 rcvdbyte=0 sentpkt=0
rcvdpkt=0 appcat="unscanned" utmaction="block" countztna=1 msg="Denied: failed to match a proxy-policy"
utmref=65462-14
```

What can you conclude from the log message?

A. The remote user connection does not match the local-in policy.
B. The remote user connection does not match the ZTNA rule configuration.
C. The remote user connection does not match the ZTNA server configuration.

D. The remote user connection does not match the ZTNA firewall policy.

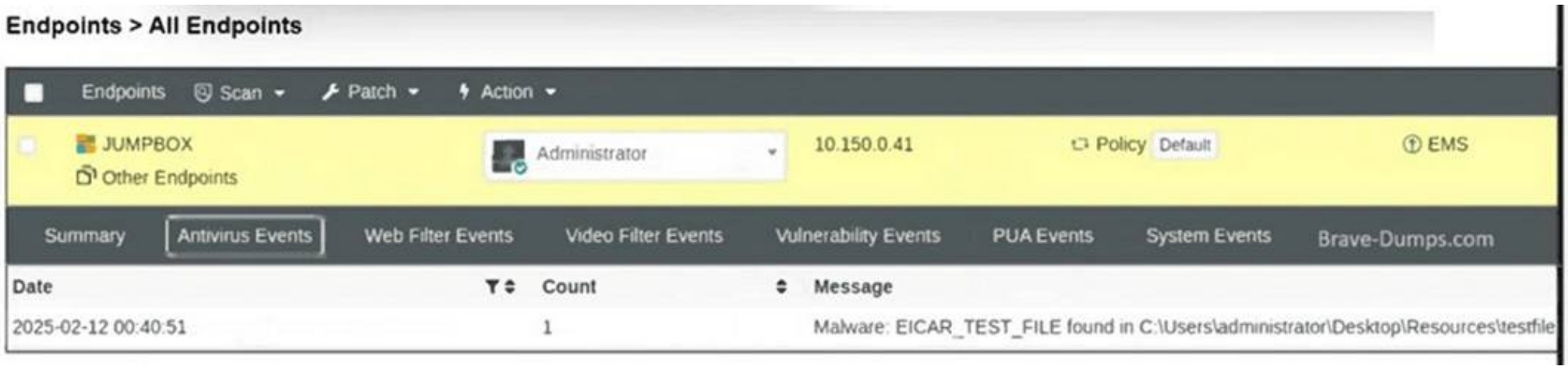
Answer: B

NEW QUESTION 56
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 61
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 63
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 68
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your FCP_FCT_AD-7.4 Exam with Our Prep Materials Via below:

https://www.certleader.com/FCP_FCT_AD-7.4-dumps.html