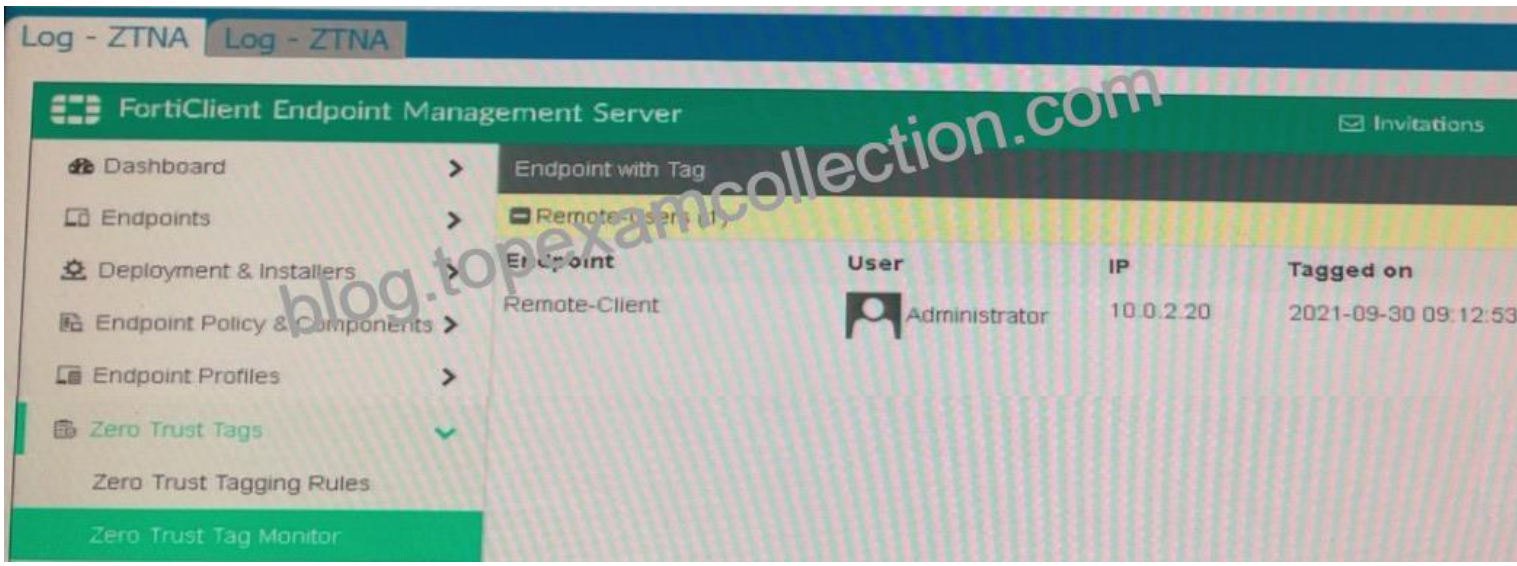
Get 100% Authentic Fortinet NSE5_FCT-7.0 Dumps with Correct Answers [Q11-Q33

Get 100% Authentic Fortinet NSE5_FCT-7.0 Dumps with Correct Answers New Training Course NSE5_FCT-7.0 Tutorial Preparation Guide

Fortinet NSE5_FCT-7.0 Exam Syllabus Topics:

TopicDetailsTopic 1- Deploy FortiClient on Windows, macOS, iOS, and Android endpoints- Provision and deploy FortiClient devicesTopic 2- Configure endpoint profiles to provision FortiClient devices- Configure FortiClient EMS featuresTopic 3- Install and perform the initial configuration of FortiClient EMS- Configure automatic quarantine of compromised endpoints
Topic 4- Resolve common FortiClient deployment and implementation issues- Apply IP- MAC ZTNA filtering to check the security posture of endpointsTopic 5- Configure security fabric integration with FortiClient EMS- Security Fabric integration - Deploy the full ZTNA solution

Q11. 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?

* Update tagging rule logic to enable tag visibility

* Change the FortiClient system settings to enable tag visibility
* Change the endpoint control setting to enable tag visibility
* Change the user identity settings to enable tag visibility

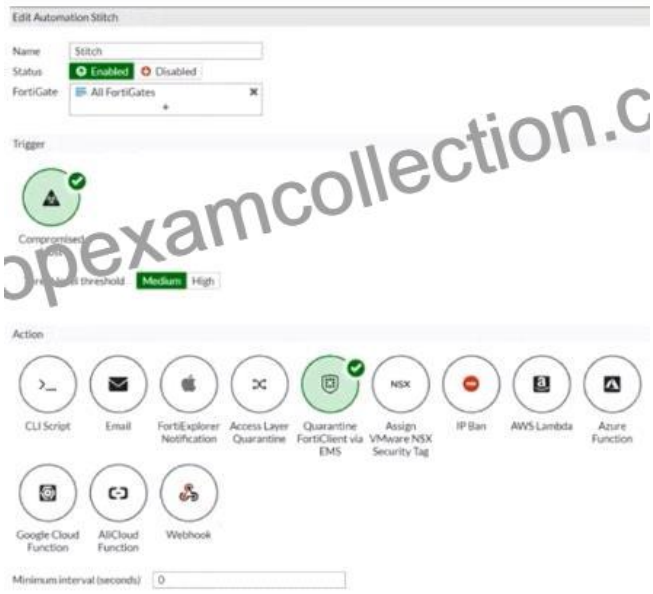
Q12. An administrator wants to simplify remote access without asking users to provide user credentials.

Which access control method provides this solution?
* SSL VPN
* ZTNA full mode
* L2TP
* ZTNA IP/MAC filtering mode

Q13. When site categories are disabled in FortiClient webfilter and antivirus (malicious websites), which feature can be used to protect the endpoint from malicious web access?
* Real-time protection list
* Block malicious websites on antivirus
* FortiSandbox URL list

Q14. Which two statements are true about ZTNA? (Choose two.)
* ZTNA provides role-based access
* ZTNA manages access for remote users only
* ZTNA manages access through the client only
* ZTNA provides a security posture check

Q15. Refer to the exhibit.



Based on the Security Fabric automation settings, what action will be taken on compromised endpoints?
* Endpoints will be quarantined through EMS
* Endpoints will be banned on FortiGate
* An email notification will be sent for compromised endpoints
* Endpoints will be quarantined through FortiSwitch

Q16. What does FortiClient do as a fabric agent? (Choose two.)
* Provides application inventory
* Provides IOC verdicts
* Automates Responses
* Creates dynamic policies

Q17. An administrator is required to maintain a software vulnerability on the endpoints, without showing the feature on the FortiClient dashboard. What must the administrator do to achieve this requirement?
* Disable select the vulnerability scan feature in the deployment package
* Use the default endpoint profile
* Select the vulnerability scan feature in the deployment package, but disable the feature on the endpoint profile
* Click the hide icon on the vulnerability scan tab

Q18. 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?
* Twitter
* Facebook
* Internet Explorer
* Firefox

Q19. What does FortiClient do as a fabric agent? (Choose two.)
* Provides application inventory
* Provides IOC verdicts
* Automates Responses
* Creates dynamic policies

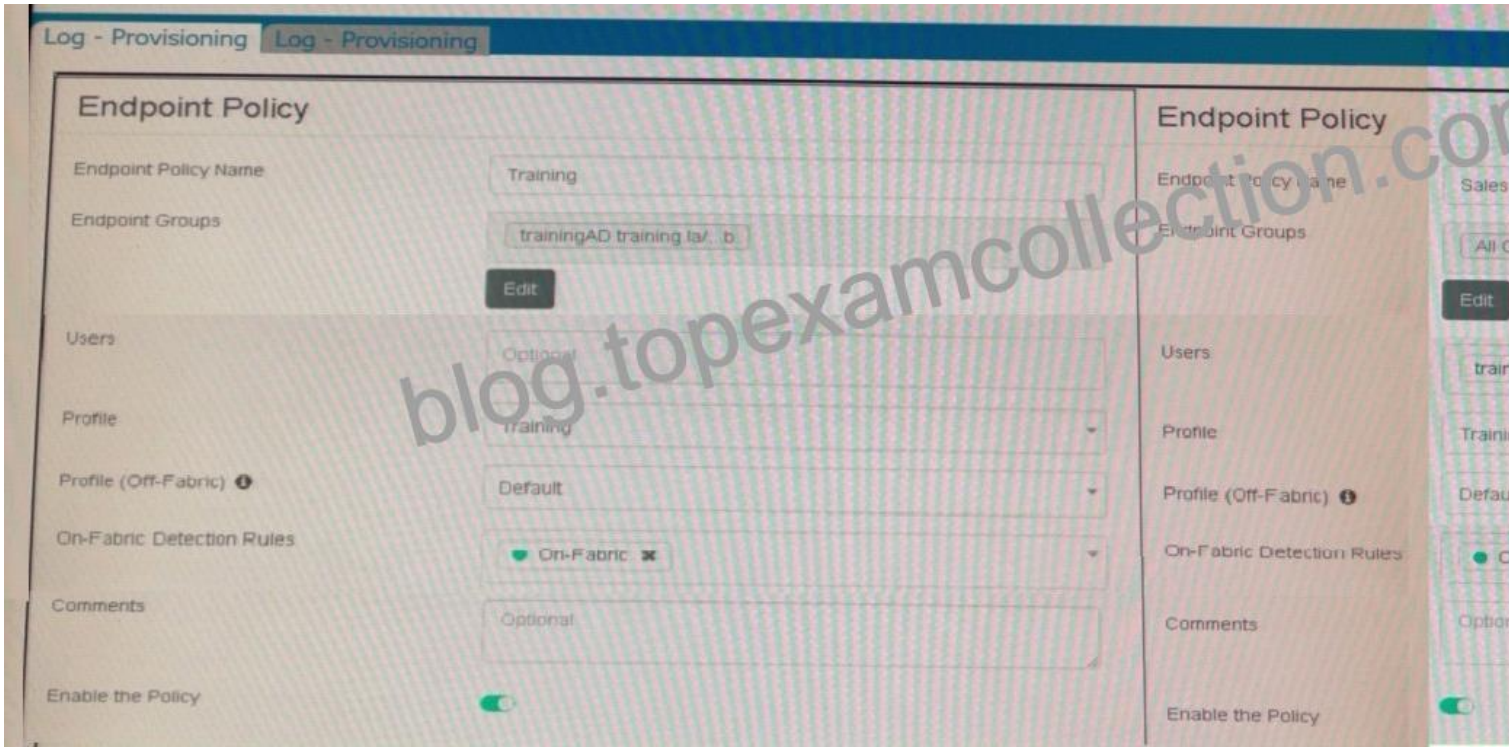
Q20. Which security fabric component sends a notification to quarantine an endpoint after IOC detection in the automation process?
* FortiAnalyzer
* FortiClient
* ForbClient EMS
* Forti Gate

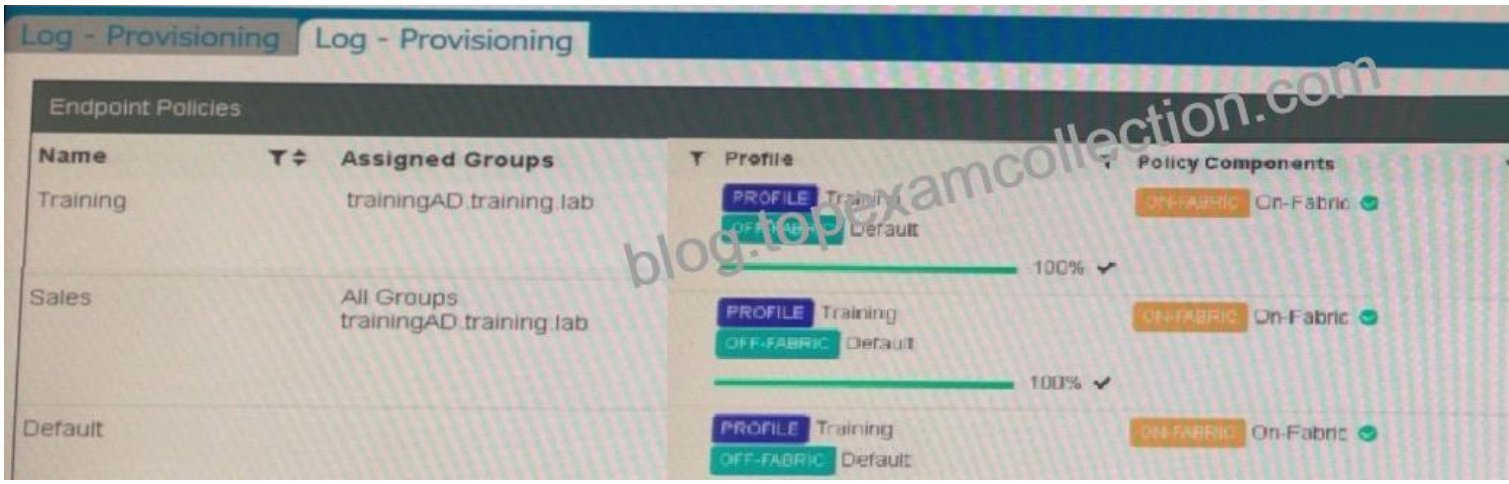
Q21. A new chrome book is connected in a school’s network.

Which component can the EMS administrator use to manage the FortiClient web filter extension installed on the Google Chromebook endpoint?

* FortiClient EMS
* FortiClient site categories
* FortiClient customer URL list
* FortiClient web filter extension

Q22. Refer to the exhibits.

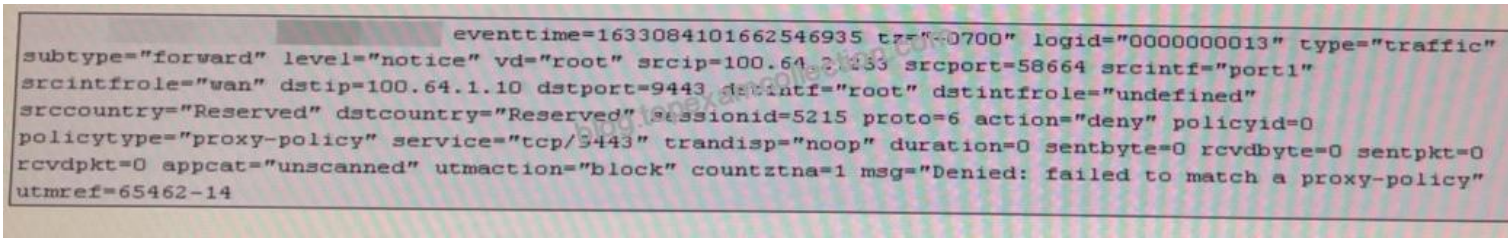




Which shows the configuration of endpoint policies.

Based on the configuration, what will happen when someone logs in with the user account student on an endpoint in the trainingAD domain?
* FortiClient EMS will assign the Sales policy
* FortiClient EMS will assign the Training policy
* FortiClient EMS will assign the Default policy
* FortiClient EMS will assign the Training policy for on-fabric endpoints and the Sales policy for the off-fabric endpoint

Q23. Refer to the exhibit.



Which shows the output of the ZTNA traffic log on FortiGate.

What can you conclude from the log message?
* The remote user connection does not match the explicit proxy policy.
* The remote user connection does not match the ZTNA server configuration.
* The remote user connection does not match the ZTNA rule configuration.
* The remote user connection does not match the ZTNA firewall policy

Q24. Which component or device shares ZTNA tag information through Security Fabric integration?
* FortiGate
* FortiGate Access Proxy
* FortiClient

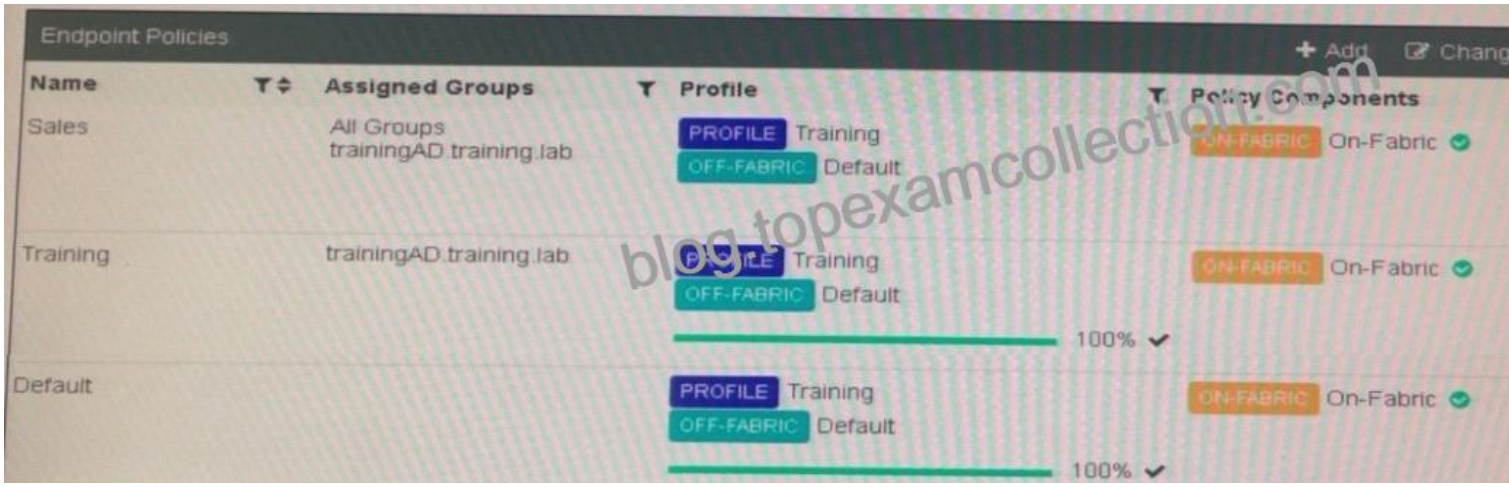
Q25. Refer to the exhibit.

An administrator has restored the modified XML configuration file to FortiClient and sees the error shown in the exhibit.

Based on the XML settings shown in the exhibit, what must the administrator do to resolve the issue with the XML configuration file?

* The administrator must resolve the XML syntax error.
* The administrator must use a password to decrypt the file
* The administrator must change the file size
* The administrator must save the file as FortiClient-config conf.

Q26. Refer to the exhibit.



Which shows multiple endpoint policies on FortiClient EMS.

Which policy is applied to the endpoint in the AD group trainingAD?
* The Sales policy
* The Training policy
* Both the Sales and Training policies because their priority is higher than the Default policy
* The Default policy because it has the highest priority

Q27. 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=99.59.148.82 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?
* Twitter
* Facebook
* Internet Explorer
* Firefox

Q28. 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?
* Blocks the infected files as it is downloading
* Quarantines the infected files and logs all access attempts
* Sends the infected file to FortiGuard for analysis
* Allows the infected file to download without scan

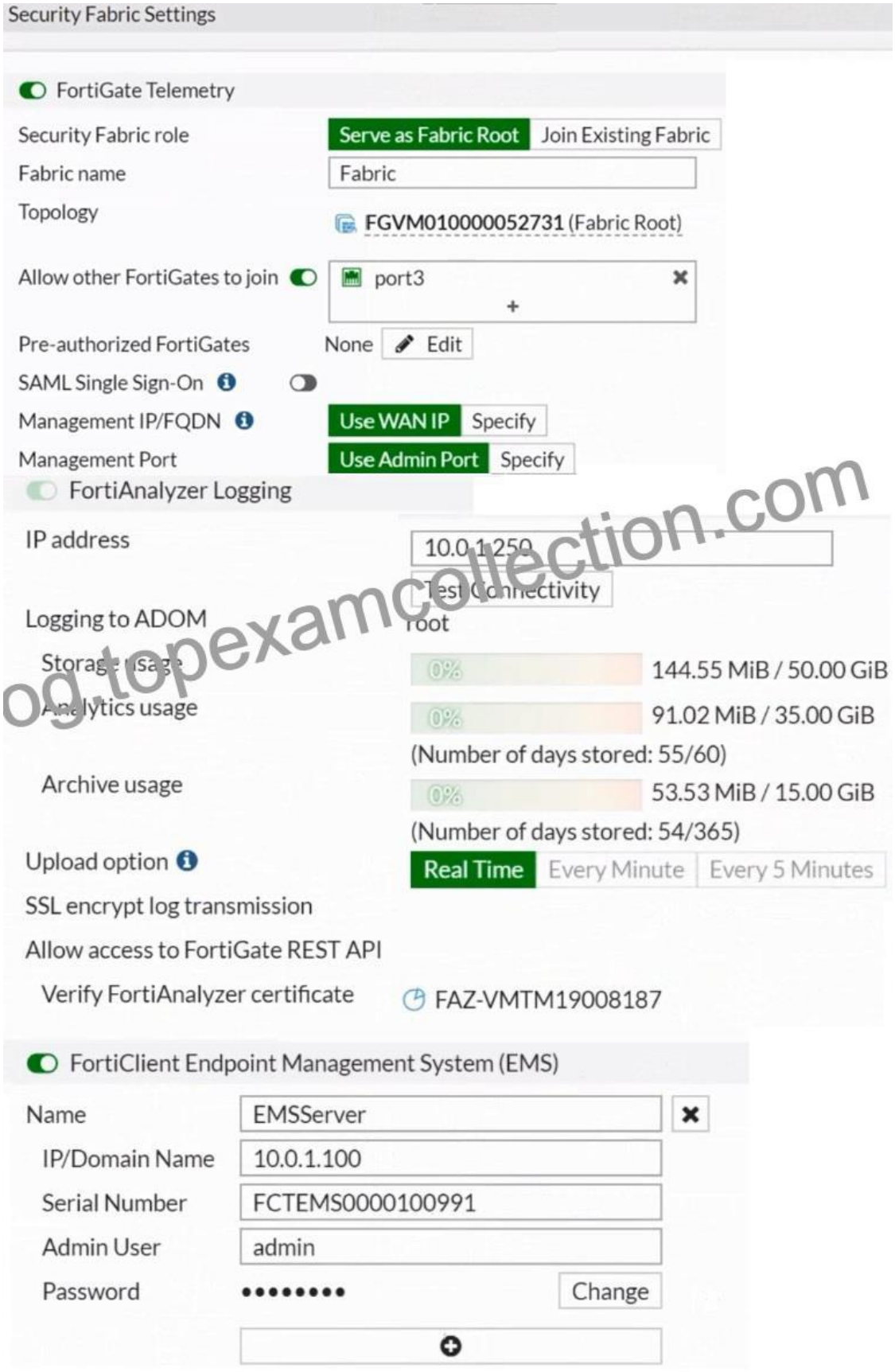
Q29. Why does FortiGate need the root CA certificate of FortiClient EMS?
* To sign FortiClient CSR requests
* To revoke FortiClient client certificates
* To trust certificates issued by FortiClient EMS
* To update FortiClient client certificates

Q30. 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?
* FortiGate FSSO
* FortiGate certificates
* FortiGate explicit proxy
* FortiGate endpoint control

Q31. What does FortiClient do as a fabric agent? (Choose two.)
* Provides IOC verdicts
* Automates Responses
* Creates dynamic policies

Q32. Which three features does FortiClient endpoint security include? (Choose three.)
* L2TP
* Real-time protection
* DLP
* Vulnerability management
* IPsec

Q33. Refer to the exhibits.



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 (loC)?

* The administrator must enable remote HTTPS access to EMS.
* The administrator must enable FQDN on EMS.
* The administrator must authorize FortiGate on FortiAnalyzer.
* The administrator must enable SSH access to EMS.