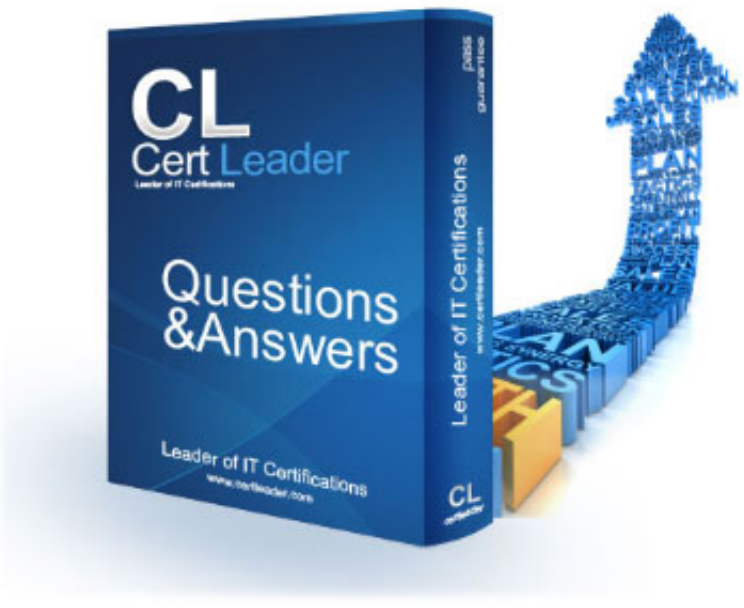
FCP_FCT_AD-7.4 Dumps

FCP - FortiClient EMS 7.4 Administrator

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



NEW QUESTION 1
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
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 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
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.


```
<sslvpn>
    <options>
        <enabled>1</enabled>
        <prefer_sslvpn_dns>1</prefer_sslvpn_dns>
        <dnscache_service_control>0</dnscache_service_control>
        <use_legacy_ssl_adapter>0</use_legacy_ssl_adapter>
        <preferred_dtls_tunnel>0</preferred_dtls_tunnel>
        <no_dhcp_server_route>0</no_dhcp_server_route>
        <no_dns_registration>0</no_dns_registration>
        <disallow_invalid_server_certificate>0</disallow_invalid_server_certificat
    </options>
    <connections>
        <connection>
            <name>Student-SSLVPN</name>
            <description>SSL VPN to Fortigate</description>
            <server>10.0.0.254:10443</server>
            <username />
            <single_user_mode>0</single_user_mode>
            <ui>
                <show_remember_password>0</show_remember_password>
            </ui>
            <password />
            <prompt_username>1</prompt_username>
            <on_connect>
                <script>
                    <os>windows</os>
                    <script>
                        <![CDATA[]]>
                    </script>
                </script>
            </on_connect>
            <on_disconnect>
                <script>
                    <os>windows</os>
                    <script>
                        <![CDATA[]]>
                    </script>
```

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?

A. The administrator must resolve the XML syntax error.

B. The administrator must use a password to decrypt the file
C. The administrator must change the file size
D. The administrator must save the file as FortiClient-config conf.

Answer: A

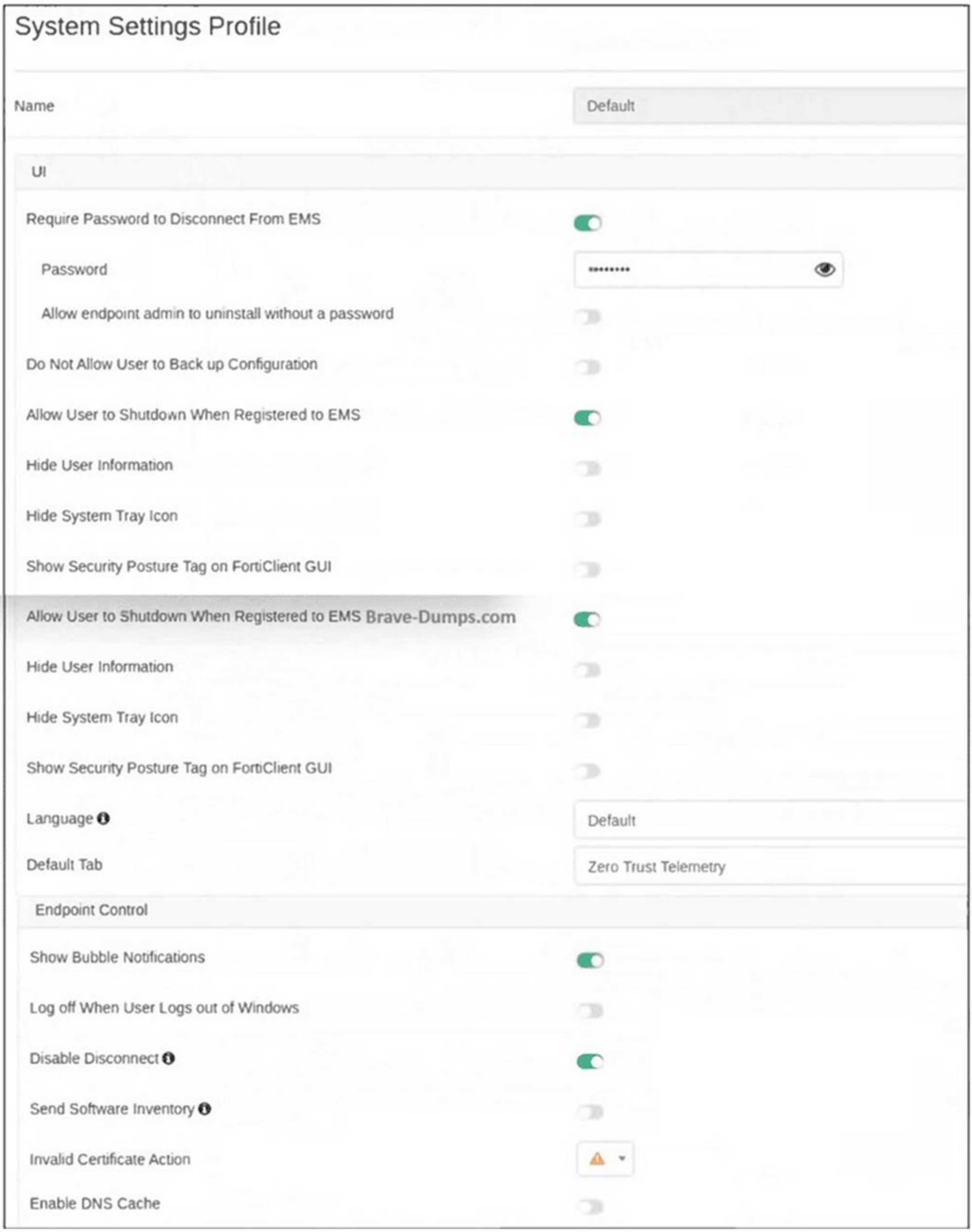
NEW QUESTION 7
An administrator is required to maintain a software vulnerability on the endpoints, without showing the feature on the FortiClient. What must the administrator do to achieve this requirement?

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
Refer to the exhibit.

System settings profile

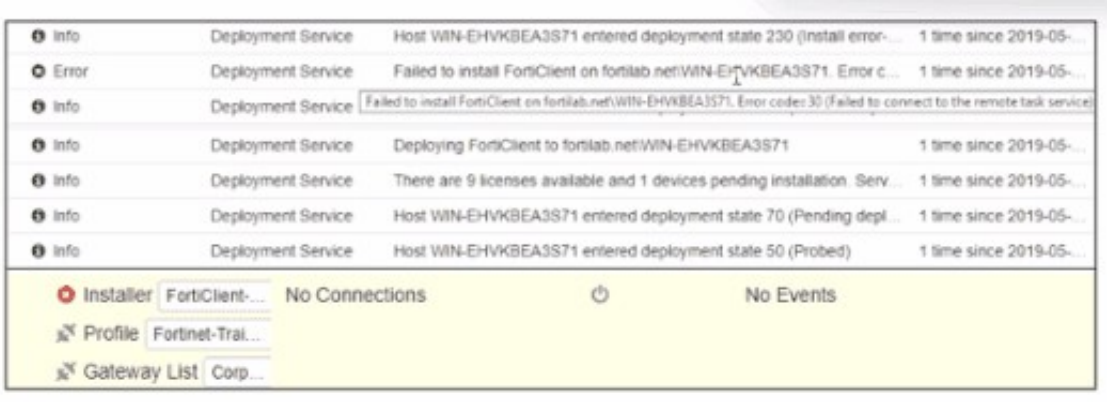


Which behavior should you expect when FortiClient with an invalid certificate is connecting to FortiClient EMS? (Choose one answer)

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 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
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
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 11
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 15
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 18
Which two statements apply to FortiClient forensics analysis? (Choose two answers)

A. FortiClient sends an alert notification when malicious activity is triggered.
B. The administrator must request analysis for the desired endpoint.
C. The endpoint is quarantined until forensics is completed.
D. Forensics analysis features must be enabled in the system settings profile.

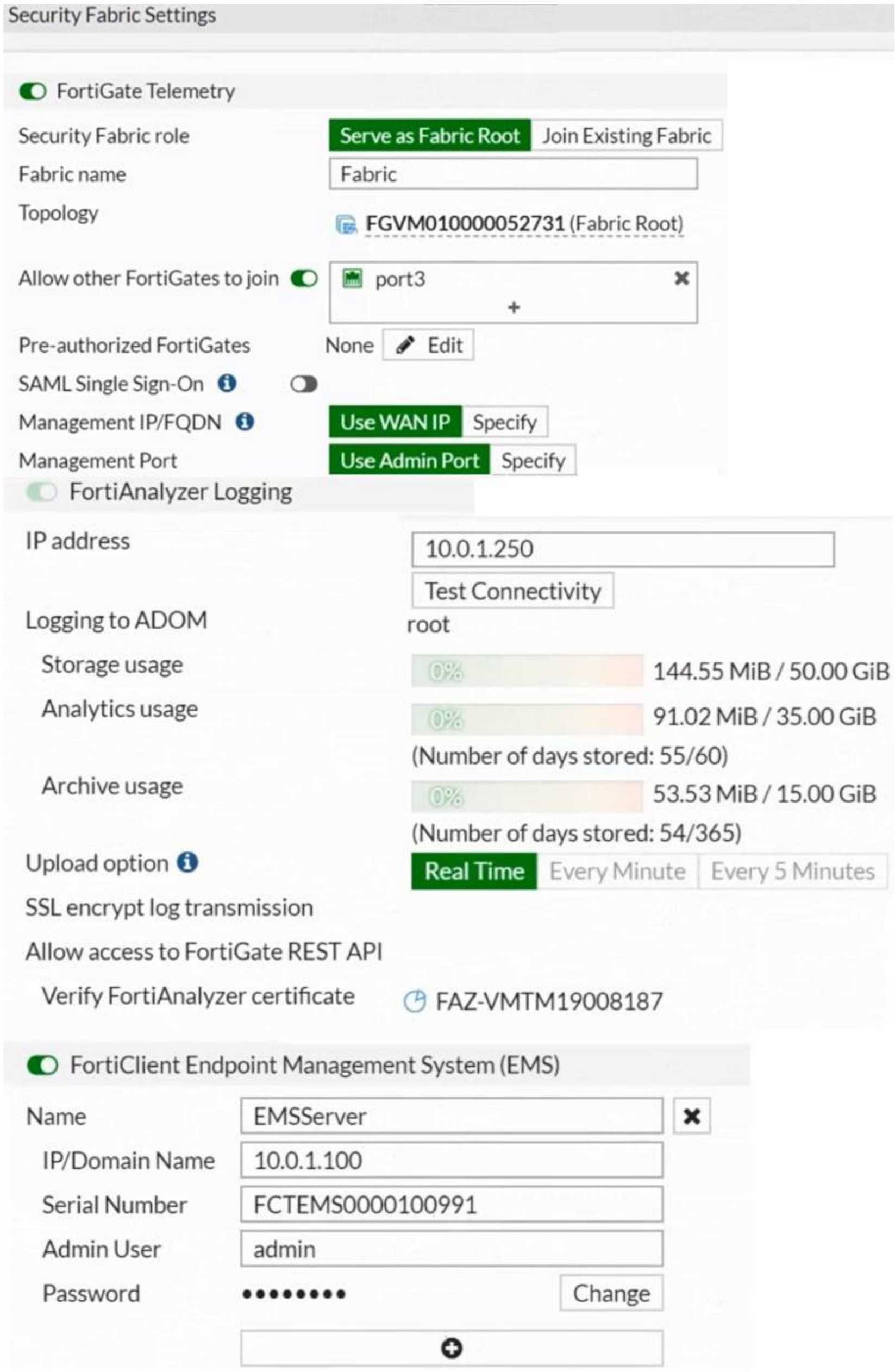
Answer: BD

NEW QUESTION 21
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 22
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 23
Which two VPNtypes can a FortiClientendpoint user inmate from the Windows command prompt? (Choose two)

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

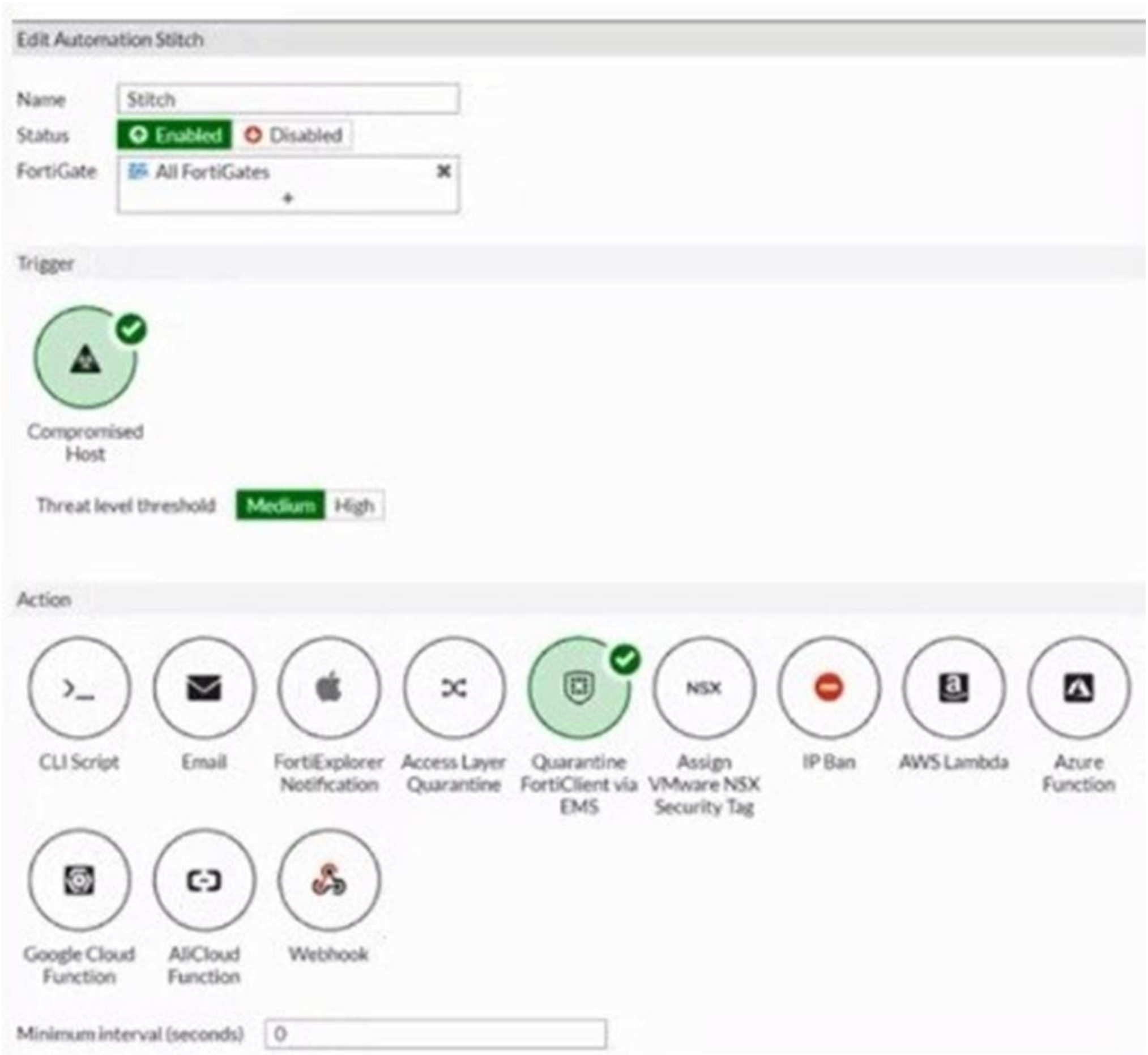
Answer: CD

NEW QUESTION 28
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 32
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 36
Refer to the exhibit.

FortiClient logs

```
20250226 05:50:24.563 TZ=+0100 [DEBUG] proxy:381 ConnID 1557243034: now rate bbc.com /
20250226 05:50:24.563 TZ=+0100 [DEBUG] accessors:127 url comparing https://www.twitter.com https://bbc.com
20250226 05:50:24.563 TZ=+0100 [DEBUG] fgdahandle:346 Category request: host bbc.com path /
20250226 05:50:24.564 TZ=+0100 [ERROR] rating_db:97 Category query failure: failed to UrlRequestSendReceive
receiveResponse error: FortiGuard server down, task dropped, https bbc.com / Brave-Dumps.com /
20250226 05:50:24.564 TZ=+0100 [INFO ] proxy:383 ConnID 1557243034: bbc.com / rating: -1 action: WF_ACTION_BLOCK
20250226 05:50:24.564 TZ=+0100 [INFO ] accessors:352 inserting violation: {bbc.com / Unknown 2025-02-26 05:50:24.564598172
+0100 CET m=+4561.038040408 admin 368039 /opt/google/chrome/chrome}
20250226 05:50:24.601 TZ=+0100 [DEBUG] http2_handler:312 set table size to 65536
20250226 05:50:24.820 TZ=+0100 [DEBUG] proxy:381 ConnID 1557243034: now rate bbc.com /favicon.ico
20250226 05:50:24.820 TZ=+0100 [DEBUG] accessors:127 url comparing https://www.twitter.com https://bbc.com/favicon.ico
20250226 05:50:24.820 TZ=+0100 [DEBUG] fgdahandle:346 Category request: host bbc.com path /favicon.ico
20250226 05:50:24.821 TZ=+0100 [ERROR] rating_db:97 Category query failure: failed to UrlRequestSendReceive
receiveResponse error: FortiGuard server down, task dropped, https bbc.com /favicon.ico Brave-Dumps.com
20250226 05:50:24.821 TZ=+0100 [INFO ] proxy:383 ConnID 1557243034: bbc.com /favicon.ico rating: -1 action: WF_ACTION_BLOCK
20250226 05:50:24.821 TZ=+0100 [INFO ] accessors:352 inserting violation: {bbc.com /favicon.ico Unknown 2025-02-26 05:50:24.8212253
+0100 CET m=+4561.294667764 admin 368039 /opt/google/chrome
```

Why is the user not able to access bbc.com? (Choose one answer)

A. The URL is blocked by the web filter endpoint profile.
B. The endpoint cannot resolve the URL FQDN.
C. FortiGuard servers are not reachable from the endpoint.
D. The application firewall is blocking Google Chrome.

Answer: C

NEW QUESTION 37
Which component or device shares ZTNA tag information through Security Fabric integration?

A. FortiGate
B. FortiGate Access Proxy
C. FortiClient

Answer: A

NEW QUESTION 40
.....

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