Fortinet

Exam Questions FCSS_LED_AR-7.6

FCSS - LAN Edge 7.6 Architect

NEW QUESTION 1
Refer to the exhibit.

WTP profile configuration

```
config wireless-controller wtp-profile
    edit "S231F"
        config platform
            set type 231F
        end
        set handoff-rssi 30
        set handoff-sta-thresh 30
        set ap-country US
        config radio-1
            set band 802.11n-2G
            set wids-profile "default-wids-apscan-enabled"
            set vap-all manual
            set vaps "Student01"
            set channel "1" "6" "11"
        end
        config radio-2
            set band 802.11ac-5G
            set channel-bonding 40MHz
            set wids-profile "default-wids-apscan-enabled"
            set darrp enable
            set arrp-profile "arrp-default"
            set vap-all manual
            set vaps "Student01"
            set channel "36" "44" "52"
        end
        config radio-3
            set mode disabled
        end
    next
end
```

Which shows the WTP profile configuration.
The AP profile is assigned to two FAP-231F APs that are installed in an open plan area. The first AP has 32 clients associated with the 5 GHz radios and 22 clients associated with the 2.4 GHz radio. The second AP has 12 clients associated with the 5 GHz radios and 20 clients associated with the 2.4 GHz radio.
A dual-band-capable client enters the area near the first AP and the first AP measures the new client at - 3 3 dBm signal strength. The second AP measures the new client at -43 dBm signal strength.
If the new client attempts to conned to the student 01 wireless network, which AP radio will the client be associated with?

A. The first AP 2.4 GHz interface provides a stronger signal, which clients often prioritize.
B. The first AP 5 GHz interface because it has a stronger signal.
C. The second AP 5 GHz interface has fewer clients, which ensures better performance despite the weaker signal.
D. The second AP 2.4 GHz interface is preferred over 5 GHz for better speed and lower interference.

Answer: C

NEW QUESTION 2
When the MAC address of a device is placed in quarantine on FortiSwitch, what happens to its egress traffic?

A. Traffic is sent to an access VLAN.

B. Traffic is assigned to the native VLAN.
C. Traffic is sent as untagged traffic.
D. Traffic is sent to an allowed VLAN.

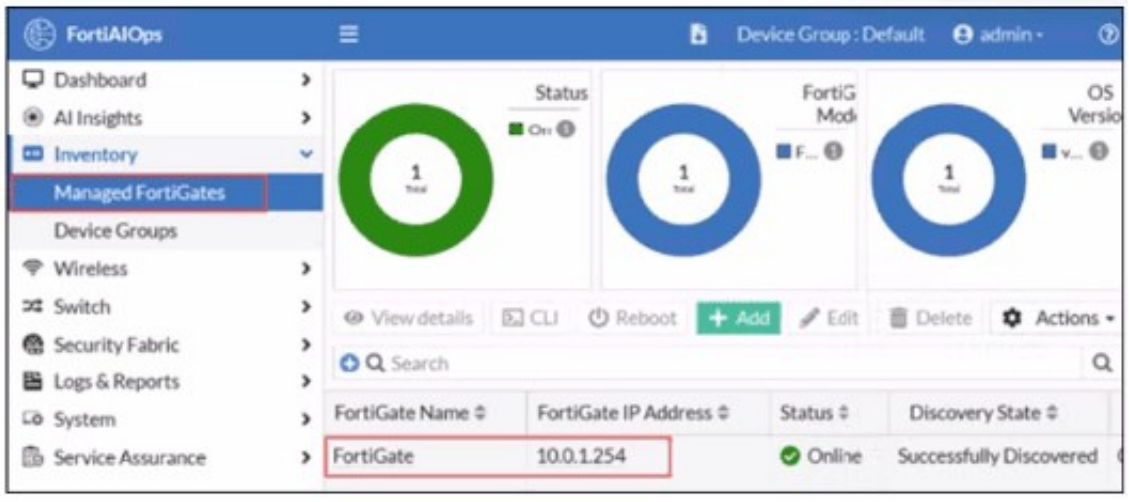
Answer: A

NEW QUESTION 3
What is the expected behavior when enabling auto TX power control on a FortiAP interface?

A. FortiGate monitors the signal strength of nearby AP interfaces and adjusts its own transmit power every 30 seconds to match the signal strength of the adjacent AP
B. FortiGate measures the signal strength of nearby FortiAP interfaces every 30 seconds and adjusts their transmit power to ensure they remain detectable at -70 dBm.
C. FortiGate periodically measures the signal strength of the weakest associated client and adjusts the AP radio power to align with the detected signal strength of that client.
D. The AP periodically evaluates the signal strength of its own transmission from the client perspective and adjusts its power to ensure the signal is detected at -70 dBm.

Answer: C

NEW QUESTION 4
FortiGate has been added to FortiAIOps for management.



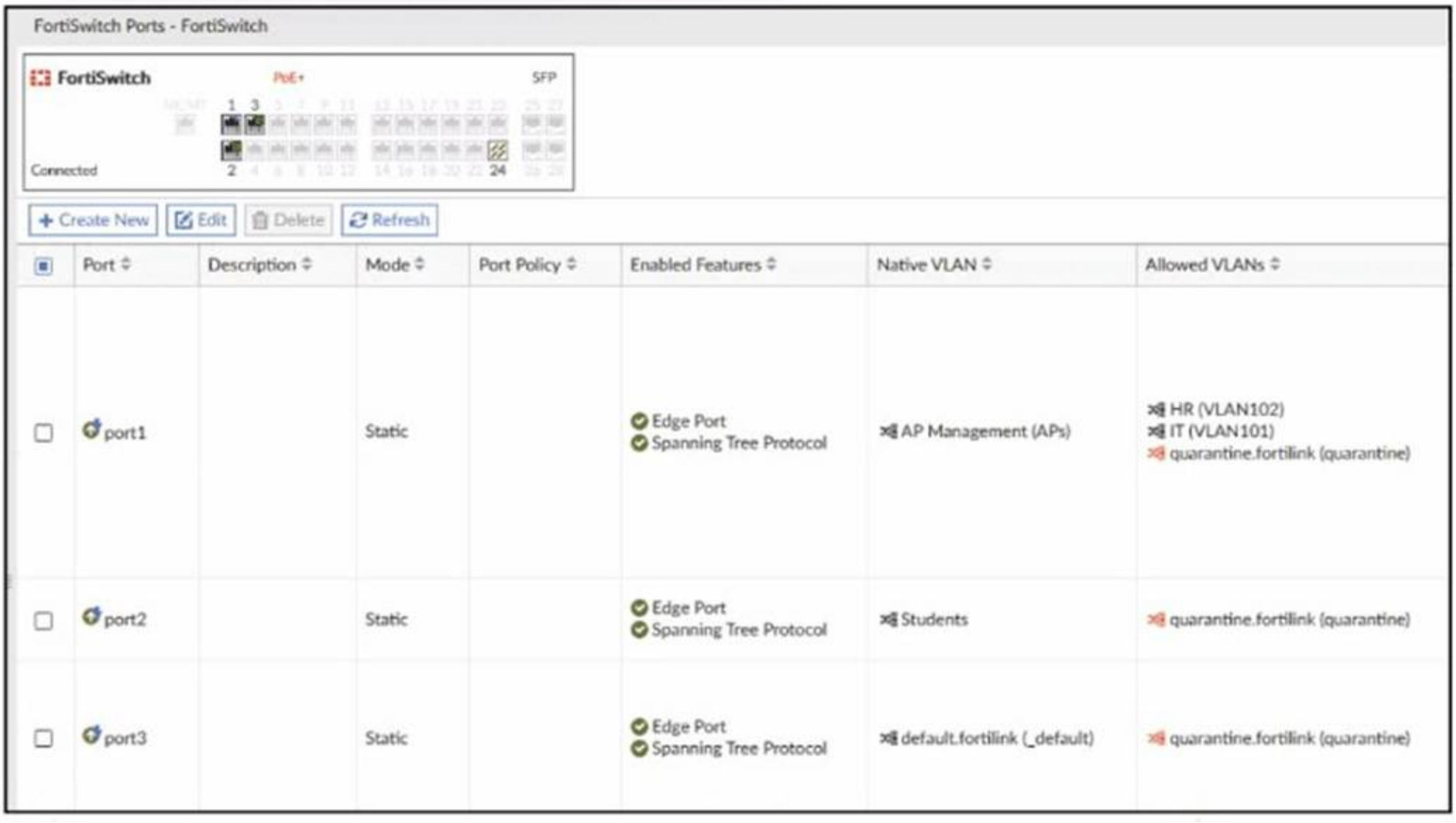
Which step must be performed on FortiAIOps to add a FortiSwitch device connected to the recently added FortiGate?

A. Add the FortiSwitch device by submitting its serial number.
B. FortiAIOps requires that the FortiSwitch IP address is submitted.
C. FortiSwitch is added automatically.
D. Configure the FortiSwitch IP address, user ID, and password

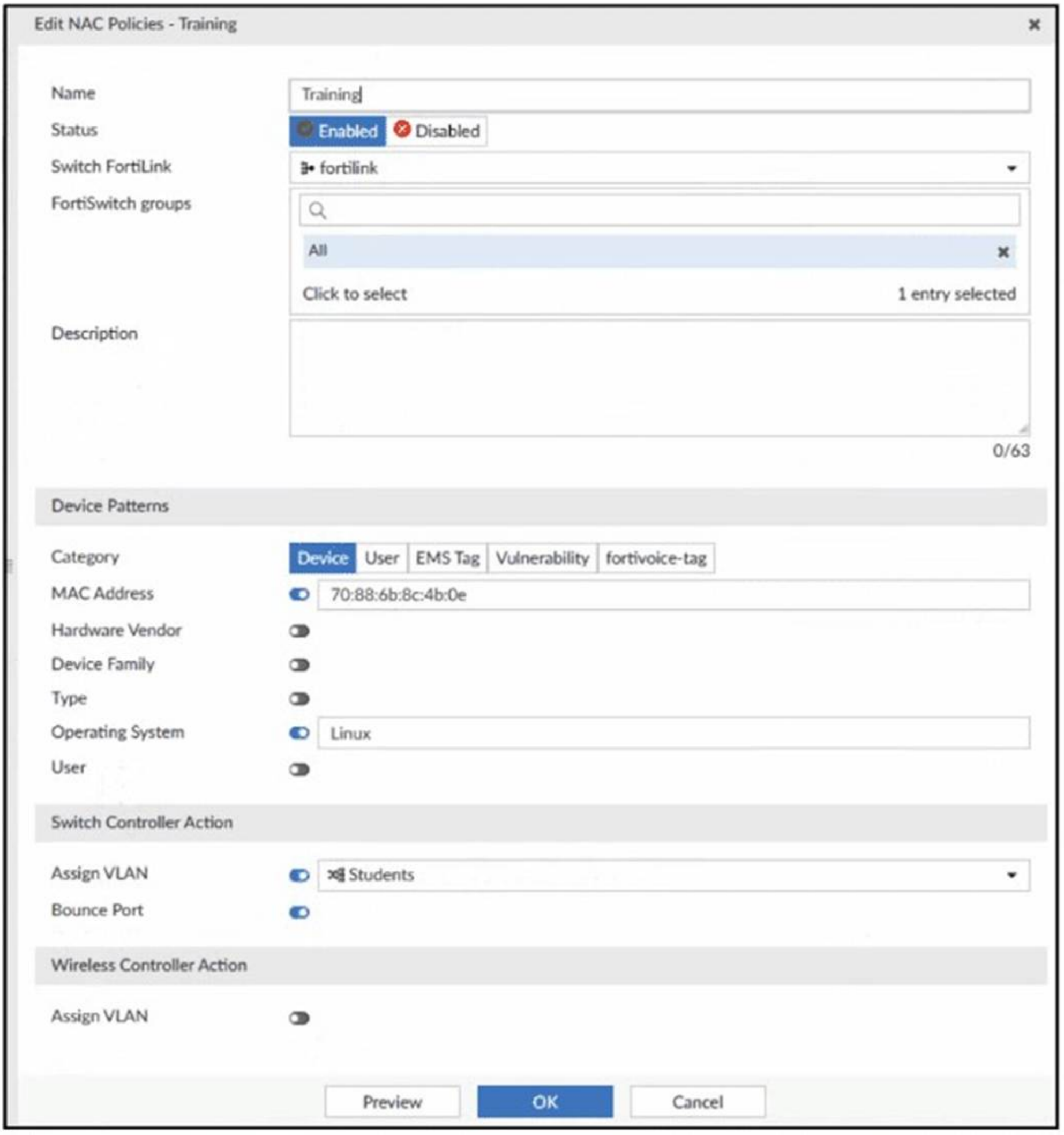
Answer: C

NEW QUESTION 5
Refer to the exhibits.

FortiSwitch Ports



NAC policy



A NAC policy has been configured to apply traffic that flows through FortiSwitch port 2. Traffic that meets the NAC policy criteria will be assigned to the Students VLAN. However, the NAC policy does not seem to be taking effect.
Which configuration is missing?

A. Port2 Access mode should be set to NAC mode.
B. The MAC address or OS might be misconfigured for the connected device.
C. Port2 Access mode should be set to Port Policy mode.
D. The Students VLAN should be set to Allowed VLANs instead of Native VLAN.

Answer: A

NEW QUESTION 6
You are troubleshooting a Syslog-based single sign-on (SSO) issue on FortiAuthenticator, where user authentication is not being correctly mapped from the syslog messages. You need a tool to diagnose the issue and understand the logs to resolve it quickly.
Which tool in FortiAuthenticator can you use to troubleshoot and diagnose a Syslog SSO issue?

A. Debug logs > Remote Servers > Syslog Viewer
B. Parsing Test Tool

C. Debug logs > SSO Sessions page
D. Debug logs > Single Sign-On > Syslog SSO

Answer: D

NEW QUESTION 7
A network engineer is deploying FortiGate devices using zero-touch provisioning (ZTP). The devices must automatically connect to FortiManager and receive their configurations upon first boot. However, after powering on the devices, they fail to register with FortiManager.
What could be a possible cause of this issue?

A. The FortiGate device requires manual intervention to accept the FortiManager connection.
B. In this scenario, the ZTP process works only when devices are connected using a console cable.
C. The FortiGate device must be preloaded with a configuration file before ZTP can function.
D. The FortiManager IP address is not reachable over TCP port 541.

Answer: D

NEW QUESTION 8
Why is it critical to maintain NTP synchronization between FortiGate and FortiSwitch when FortiLink is configured?

A. To facilitate synchronization of firmware updates across devices
B. To allow FortiSwitch to communicate with other FortiSwitche devices in the network.
C. To ensure accurate time for logs, authentication, and event correlation
D. To allow FortiSwitch to function in standalone mode if FortiGate becomes unavailable

Answer: C

NEW QUESTION 9
Your office wants to set up a Wi-Fi network for visitors. Your company would like to require them to log in for (racking purposes. Which two types of captive portals could be enabled on an interface? (Choose two.)

A. Terms Acknowledgment Without Authentication
B. Email Notification Only
C. Disclaimer + Authentication
D. Guest Pass Access
E. Authentication

Answer: AE

NEW QUESTION 10
A FortiSwitch is not appearing in the FortiGate management interface after being connected via FortiLink. What could be a first troubleshooting step?

A. Ensure that the FortiGate security policies allow traffic from the FortiSwitch.
B. Manually assign a static IP to the FortiSwitch.
C. Verify that FortiGate device DHCP server is assigning an IP to the FortiSwitch.
D. Ensure the FortiSwitch has internet access.

Answer: C

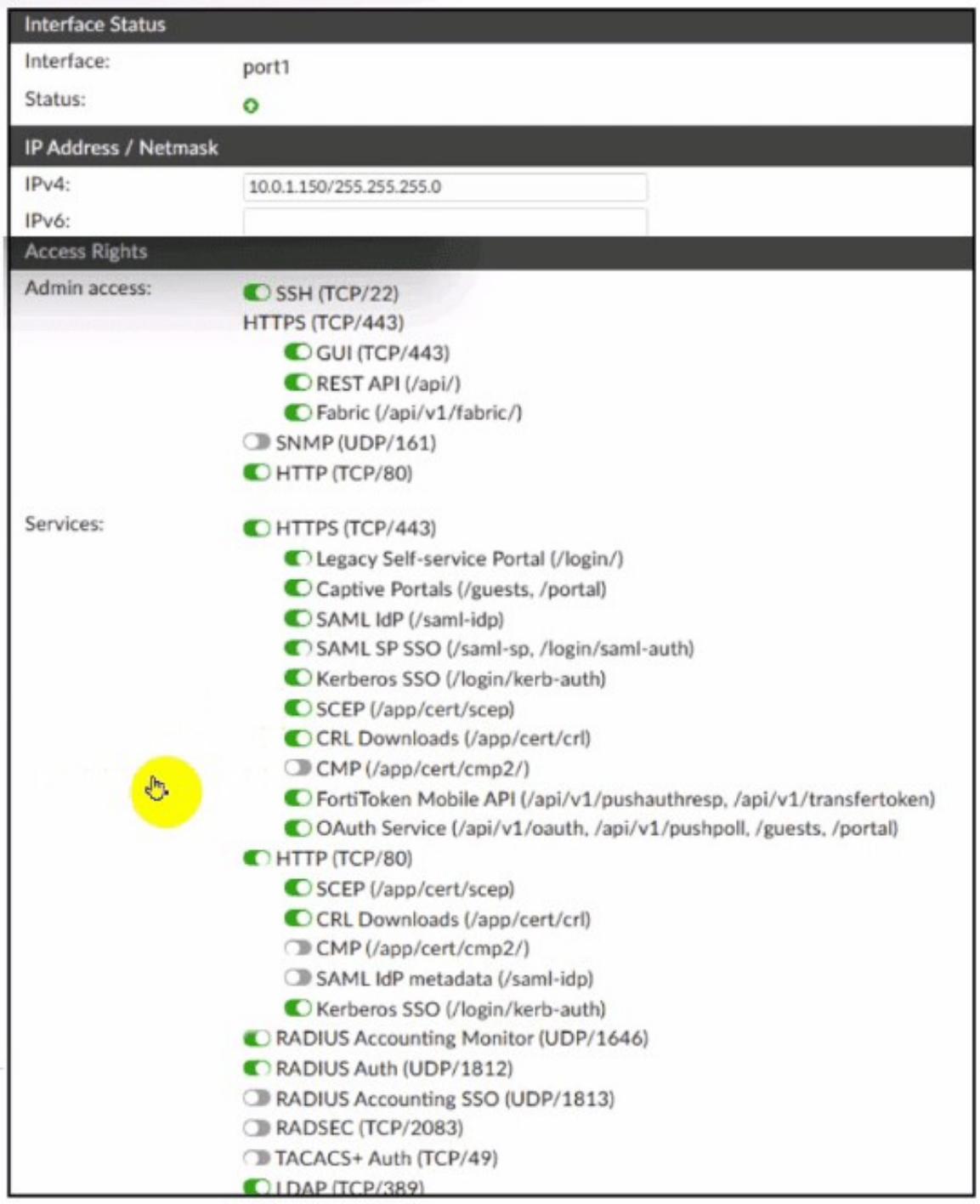
NEW QUESTION 10
APs have been manually configured to connect to FortiGate over an IPsec network, and FortiGate successfully detects and authorizes them. However, the APs remain unmanaged because FortiGate is unable to establish a CAPWAP tunnel with them.
What configuration change can resolve this issue and enable FortiGate to establish the CAPWAP tunnel over the IPsec connection?

A. Configure a static route on FortiGate to reach the APs over the IPsec tunnel.
B. Assign a custom AP profile for the remote APs with the set mpls-connection option enabled.
C. Decrease the CAPWAP tunnel MTU size for APs to prevent fragmentation.
D. Upgrade the FortiAP firmware image to ensure compatibility with the FortiOS version.

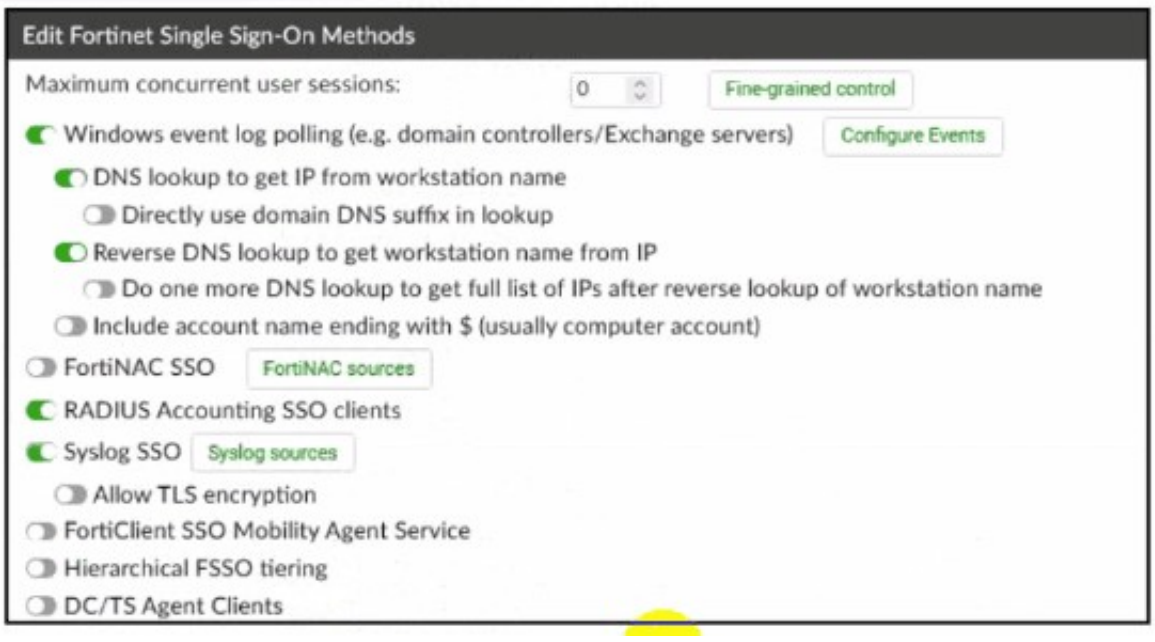
Answer: B

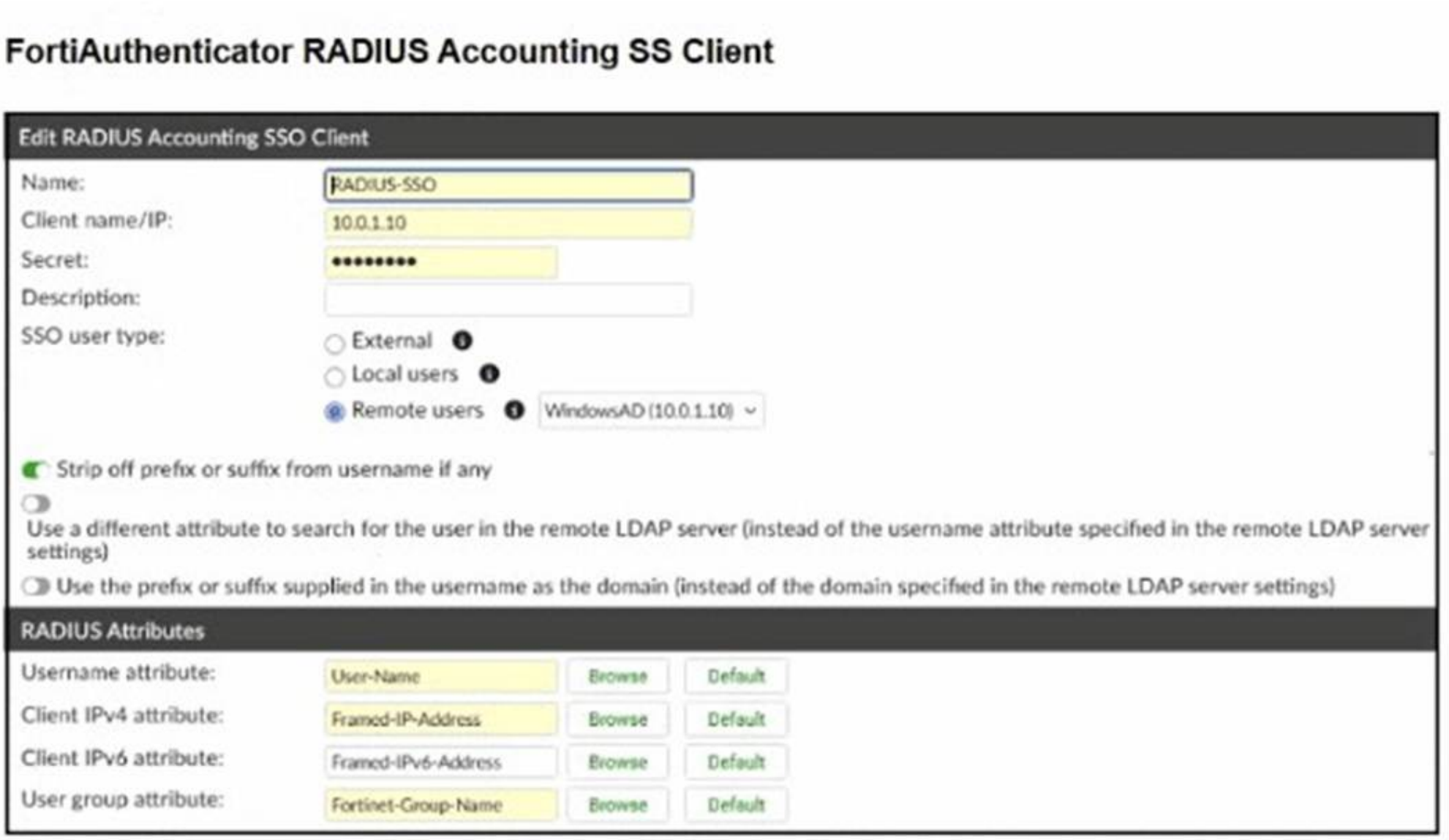
NEW QUESTION 13
Refer to the exhibits.

FortiAuthenticator



FortiAuthenticator SSO Methods





A company has multiple FortiGate devices deployed and wants to centralize user authentication and authorization. The administrator decides to use FortiAuthenticator to convert RSSO messages to FSSO, allowing all FortiGate devices to receive user authentication updates.
After configuring FortiAuthenticator to receive RADIUS accounting messages, users can authenticate, but FortiGate does not enforce the correct policies based on user groups. Upon investigation, the administrator discovers that FortiAuthenticator is receiving RADIUS accounting messages from the RADIUS server and successfully queries LDAP for user group information. But, FSSO updates are not being sent to FortiGate devices and FortiGate firewall policies based on FSSO user groups are not being applied.
What is the most likely reason FortiGate is not receiving FSSO updates?

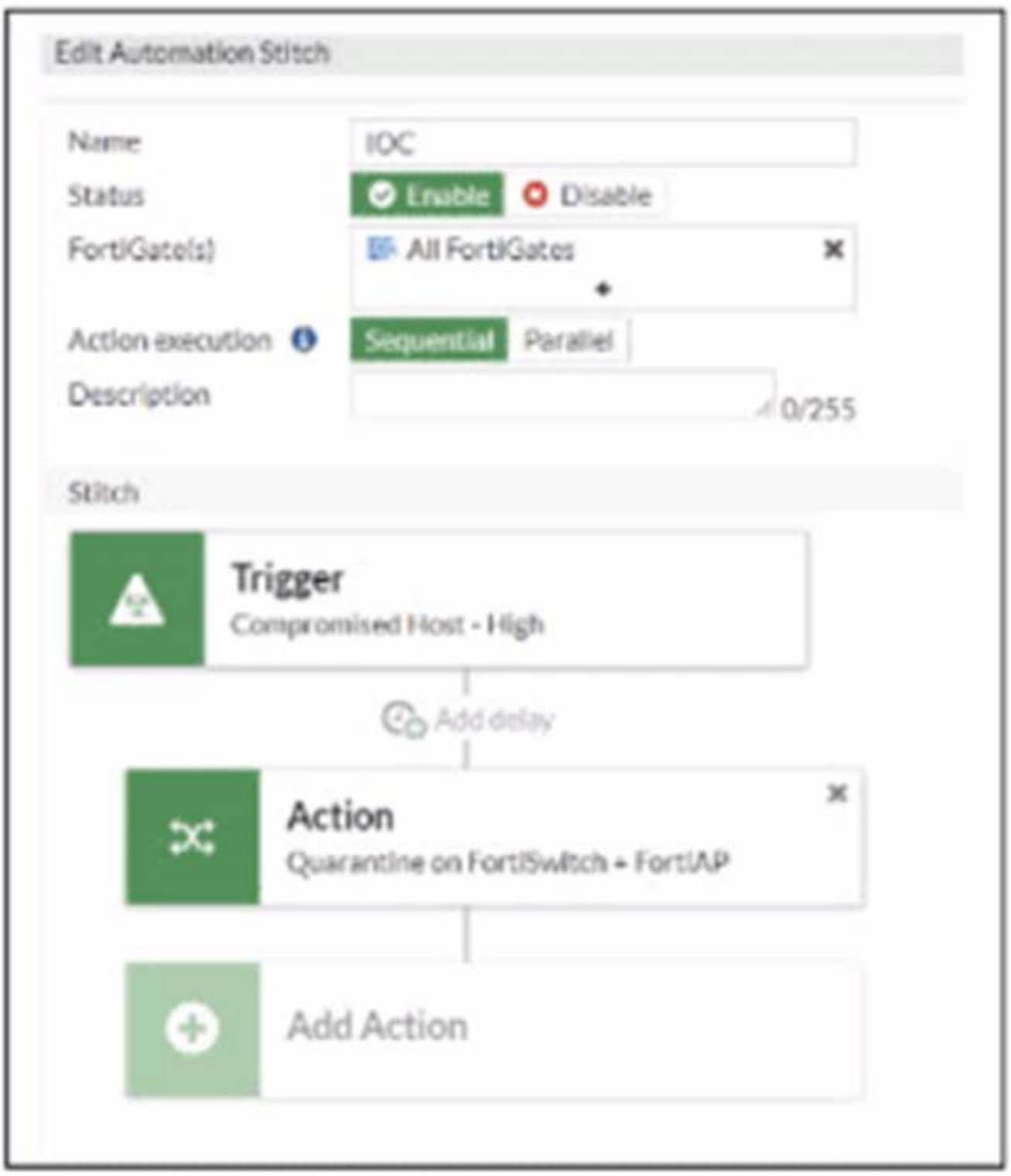
A. The RADIUS Username and Client IPv4 attributes are not defined on FortiAuthenticator.
B. The LDAP server is not configured to retrieve group memberships for RSSO users.
C. FortiAuthenticator is missing the FSSO user group attribute in the configuration.
D. The FortiAuthenticator interface is not enabled to receive RADIUS accounting messages.

Answer: A

NEW QUESTION 17
Refer to the exhibits.

FortiGate Security Fabric widget

Security Fabric Automation Stitch



Quarantine widget

FortiGate firewall policy

FortiAnalyzer log

Examine the FortiGate configuration, FortiAnalyzer logs, and FortiGate widget shown in the exhibits.
Security Fabhc quarantine automation has been configured to isolate compromised devices automatically. FortiAnalyzer has been added to the Security Fabric, and an automation stitch has been configured to quarantine compromised devices.
To test the setup, a device with the IP address 10.0.2.1 that is connected through a managed FortiSwitch attempts to access a malicious website. The logs on FortiAnalyzer confirm that the event was recorded, but the device does not appear in the FortiGate quarantine widget.
Which two reasons could explain why FortiGate is not quarantining the device? (Choose two.)

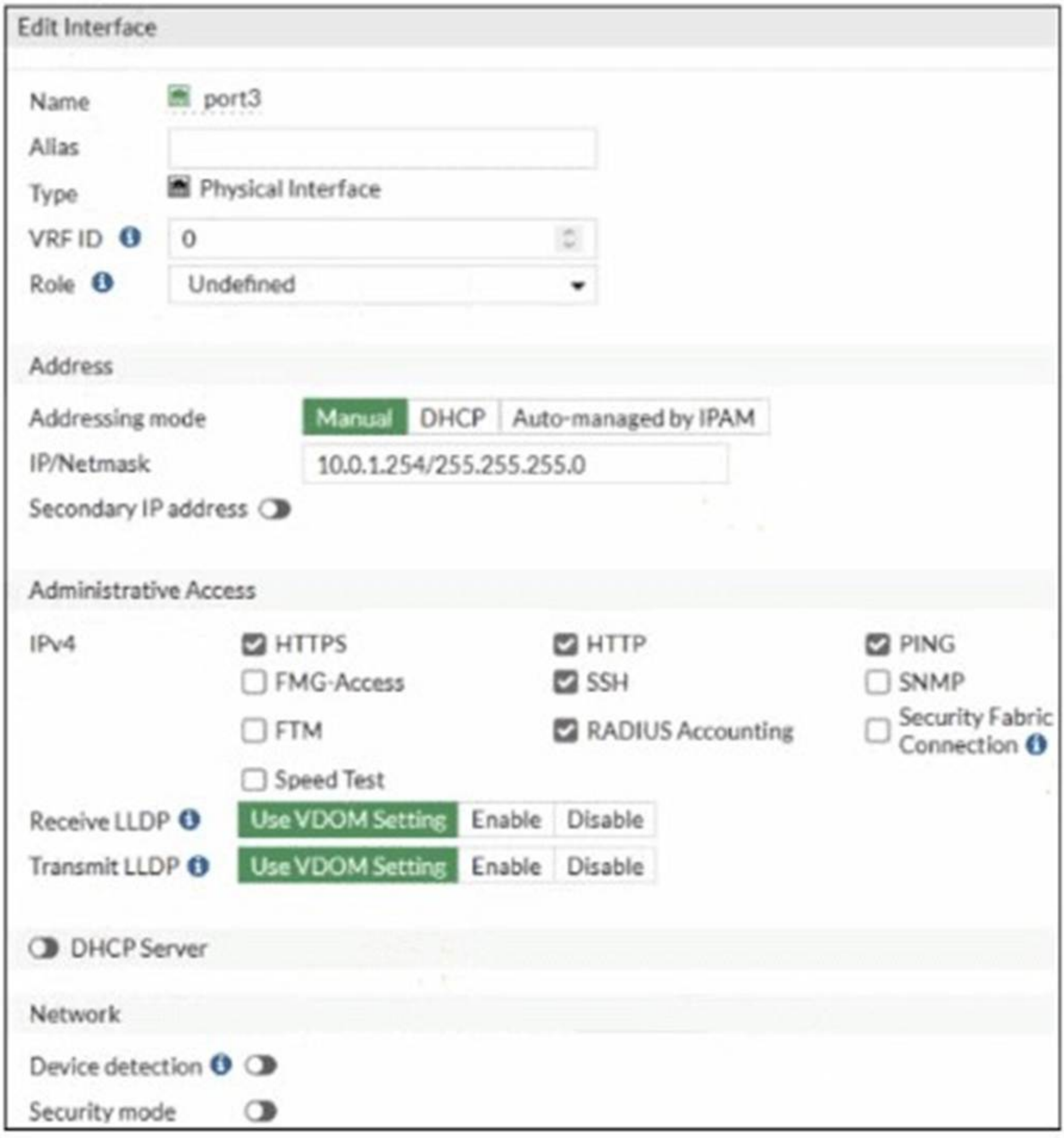
A. The IOC action should include only the FortiSwitch in the quarantine.
B. The SSL inspection should be set to deep-Inspection
C. The malicious website is not recognized as an indicator of compromise (IOC) byFortiAnalyzer.
D. The threat detection services license is missing or invalid under FortiAnalyzer.

Answer: CD

NEW QUESTION 21
Refer to the exhibits.


FortiGate RSSO configuration
Edit External Connector
Endpoint/Identity
RADIUS Single
Sign-On Agent
Connector Settings
Name
RSSO Agent
Use RADIUS Shared Secret
Send RADIUS Responses

FortiGate interface configuration



Examine the FortiGate RSSO configuration shown in the exhibit.
FortiGate is set up to use RSSO for user authentication. It is currently receiving RADIUS accounting messages through port3. The incoming RADIUS accounting messages contain the username in the User-Name attribute and group membership in the Class attribute. You must ensure that the users are authenticated through these RADIUS accounting messages and accurately mapped to their respective RSSO user groups.
Which three critical configurations must you implement on the FortiGate device? (Choose three.)

A. The RADIUS Attribute Value setting configured for an RSSO user group should match the class RADIUS attribute value in the RADIUS accounting message.
B. RSSO user groups should be assigned to all firewall policies.
C. Device detection and Security Fabric Connection should be enabled on port3
D. The sso-attribute CLI setting in the RSSO agent configuration should be set to Class.
E. The rsso-endpoint-attribute CLI setting in the RSSO agent configuration should be set toUser-Name.

Answer: ADE

NEW QUESTION 22

.....

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

FCSS_LED_AR-7.6 Practice Exam Features:

* FCSS_LED_AR-7.6 Questions and Answers Updated Frequently

* FCSS_LED_AR-7.6 Practice Questions Verified by Expert Senior Certified Staff

* FCSS_LED_AR-7.6 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* FCSS_LED_AR-7.6 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year