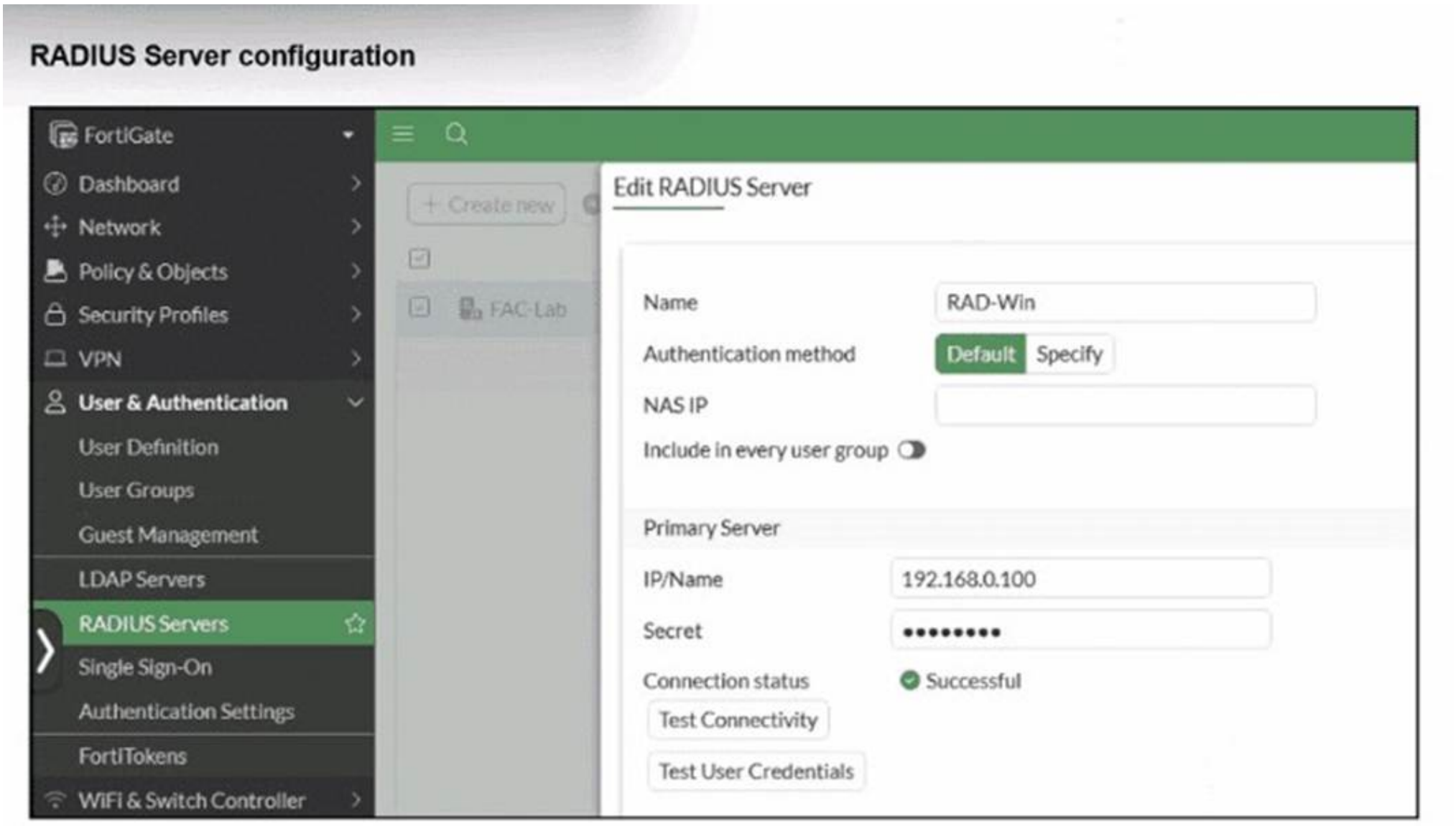
Fortinet

Exam Questions FCSS_LED_AR-7.6

FCSS - LAN Edge 7.6 Architect

NEW QUESTION 1
Refer to the exhibit.



On FortiGate, a RADIUS server is configured to forward authentication requests to FortiAuthenticator, which acts as a RADIUS proxy. FortiAuthenticator then relays these authentication requests to a remote Windows AD server using LDAP.
While testing authentication using the CLI command diagnose test authserver. the administrator observed that authentication succeeded with PAP but failed when using MS- CHAFV2.
Which two solutions can the administrator implement to enable MS-CHAPv2 authentication? (Choose two.)

A. Change the FortiGate authentication method to CHAP instead of MS-CHAPv2.
B. Enable Windows Active Directory domain authentication on FortiAuthenticator.
C. Enable RADIUS attribute filtering on FortiAuthenticator.
D. Configure FortiAuthenticator to use RADIUS instead of LDAP as the back-end authentication server

Answer: AD

NEW QUESTION 2
You are configuring FortiAuthenticator to integrate with FSSO for user identification. To enable FortiAuthenticator to extract user information from syslog messages and inject it into FSSO, you have configured syslog matching rules.
What is the role of syslog matching rules in the process of injecting user information into FSSO?

A. To automatically update user group memberships in FSSO based on syslog events
B. To enforce user authentication policies based on syslog message contents
C. To define how syslog messages are parsed and extract user information, such as usernames and IP addresses
D. To filter and block irrelevant syslog messages from being processed by the FortiAuthenticator

Answer: C

NEW QUESTION 3
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.

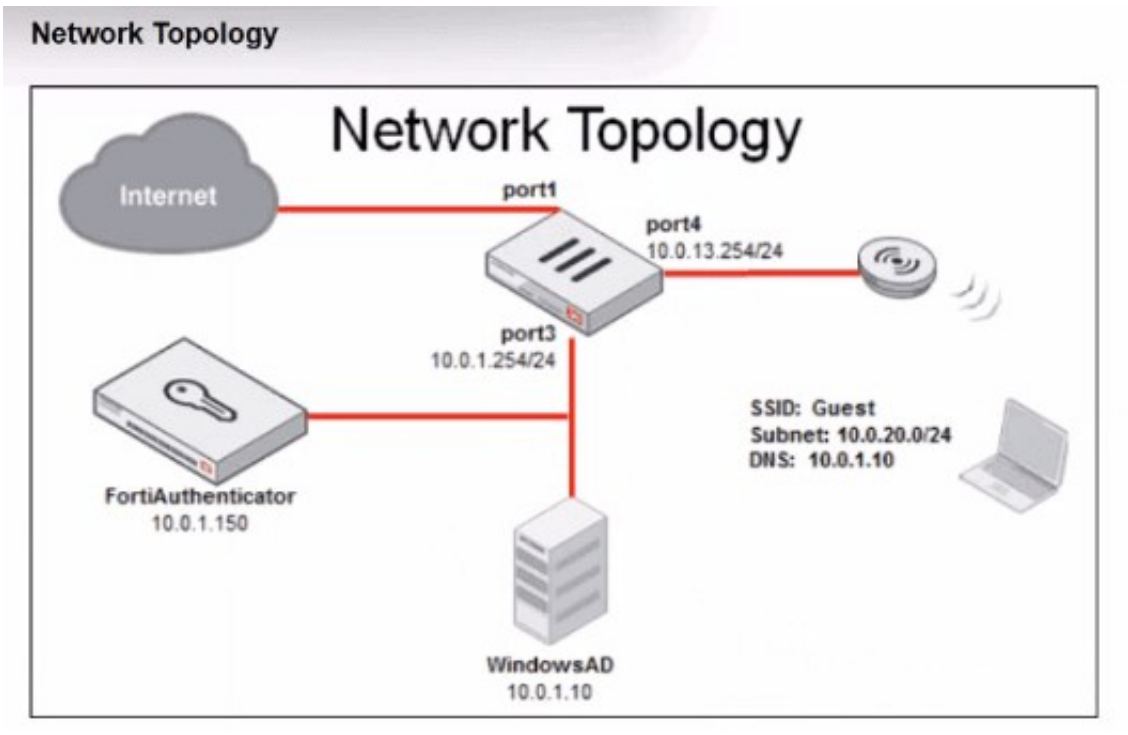
Answer: C

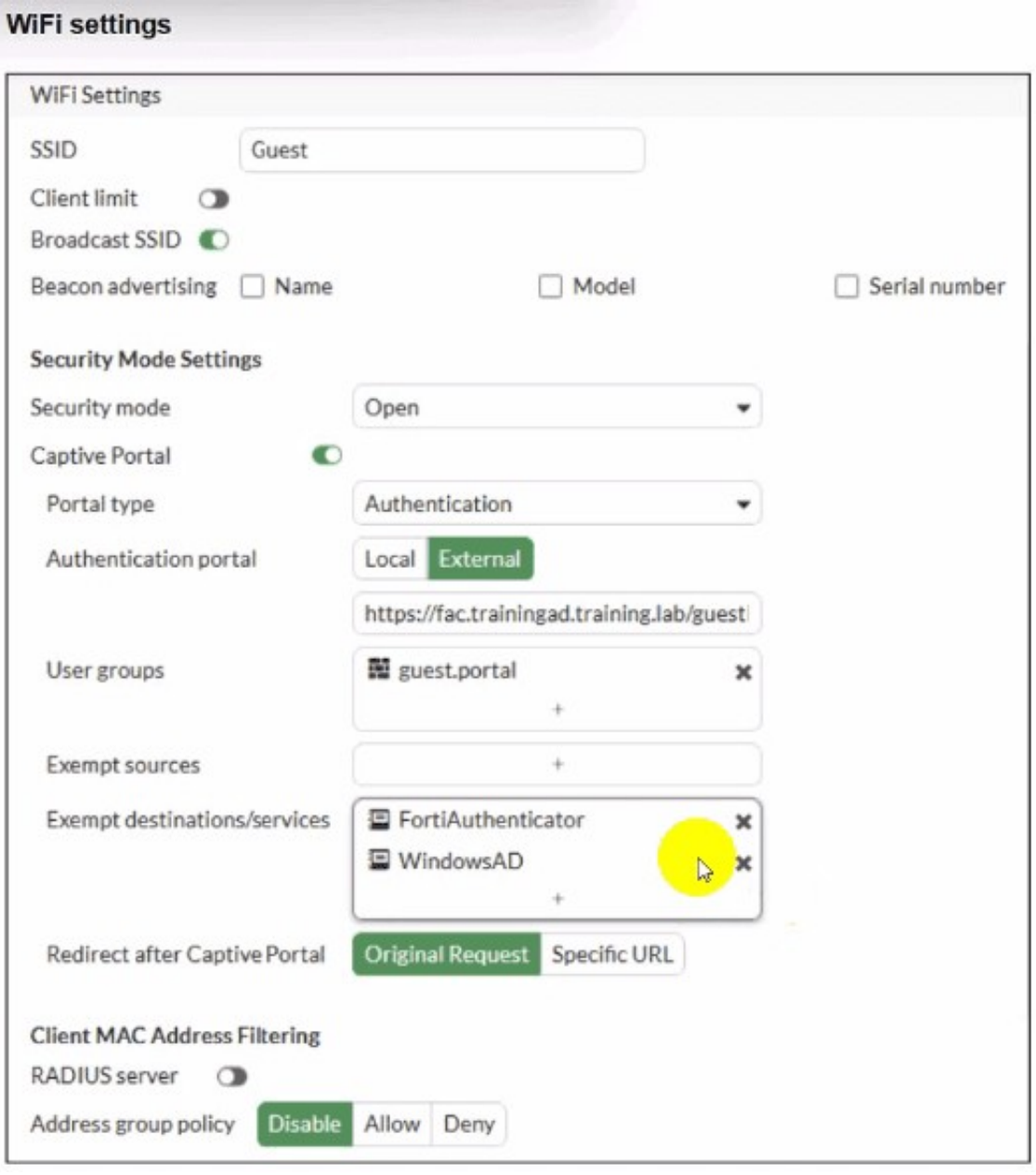
NEW QUESTION 4
When the MAC address of a device is placed in quarantine on FortiSwitch, what happens to its egress traffic?

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 5
Refer to the exhibit.





Review the exhibits to analyze the network topology, SSID settings, and firewall policies.
FortiGate is configured to use an external captive portal for authentication to grant access to a wireless network. During testing, it was found that users attempting to connect to the SSID cannot access the captive portal login page.
What configuration change should be made to resolve this issue to allow users to access the captive portal?

A. Change the SSID security mode to WPA2-Enterprise for authentication.
B. Disable HTTPS redirection for the captive portal authentication page.
C. Exclude FortiAuthenticator and Windows AD address objects from filtering.
D. A firewall policy allowing Guest SSID traffic to reach FortiAuthenticator and Windows AD.

Answer: D

NEW QUESTION 6
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

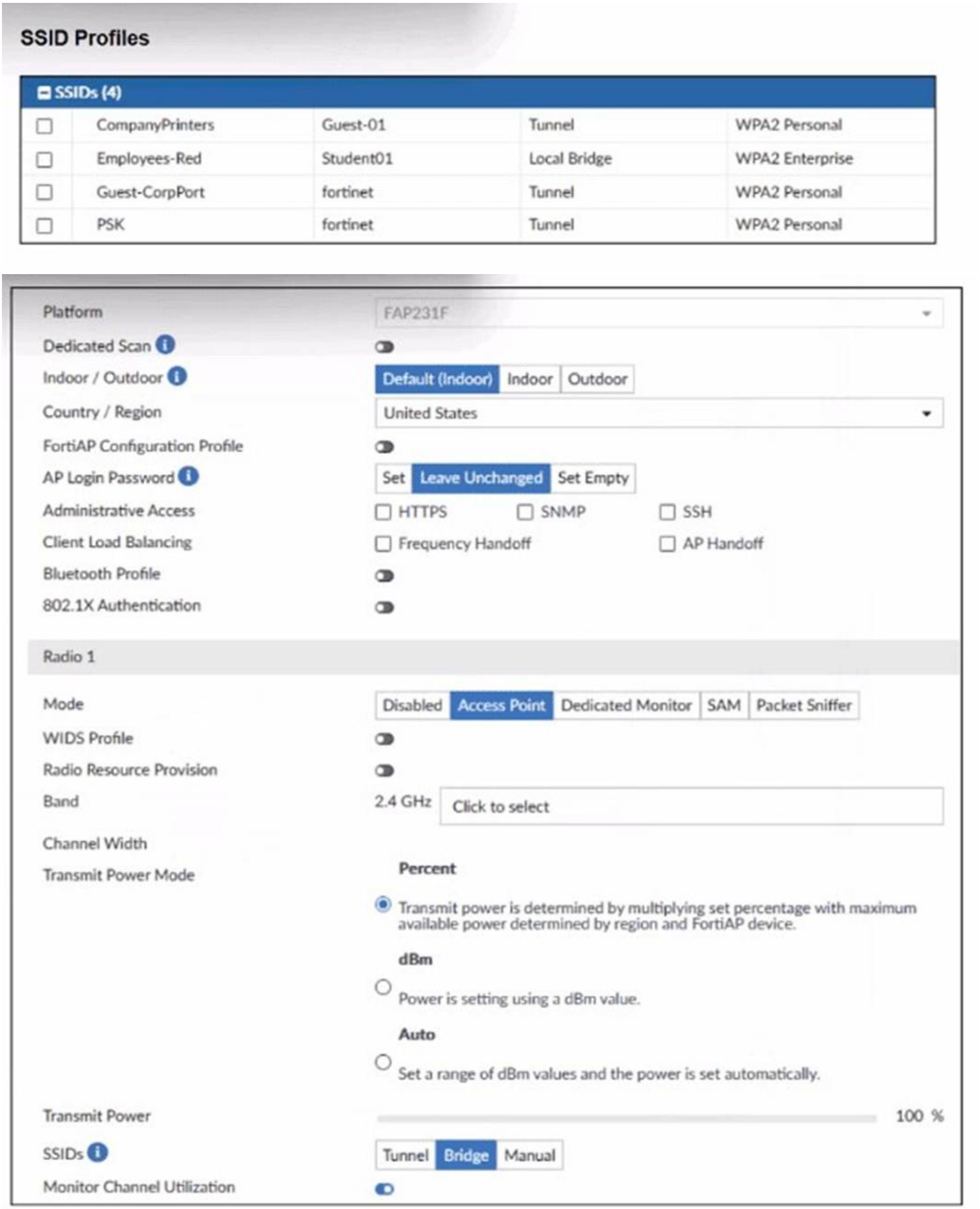
NEW QUESTION 7
FortiGate has been added to FortiAIOps for management.

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 8
Refer to the exhibits.



A set of SSID profiles has been configured on FortiManager, and an AP profile has been assigned to a group of AP managed by FortiGate. However, none of the designated SSIDs are being broadcast by these APs.
Which configuration change is required to make the APs broadcast these SSIDs as intended?

A. Adjust the AP profile to ensure all SSIDs are configured in a supported mode, either bridge or tunnel, but not a mix of both.
B. Change the AP profile to use a platform that supports the configured mix of SSIDs.
C. Choose Manual in the SSIDs setting and select the SSIDs to broadcast.
D. Set the Transmit Power Mode to Auto.

Answer: C

NEW QUESTION 9
Refer to the exhibits.

FortiGate VLAN AP settings

```
config system interface
    edit "APs"
        set vdom "root"
        set ip 10.10.100.254 255.255.255.0
        set allowaccess ping
        set alias "AP Management"
        set device-identification enable
        set role lan
        set snmp-index 118
        set ip-managed-by-fortiipam disable
        set interface "fortilink"
        set vlanid 100
    next
end
```

DHCP configuration

```
config system dhcp server
    edit 7
        set dns-service default
        set default-gateway 10.10.100.254
        set netmask 255.255.255.0
        set interface "APs"
        config ip-range
            edit 1
                set start-ip 10.10.100.1
                set end-ip 10.10.100.253
            next
        end
    next
end
```

FortiSwitch port1 VLAN AP assignment

```
config switch-controller managed-switch
    edit "FortiSwitch"
        set sn "S224EPTF19006016"
        set fsw-wan1-peer "fortilink"
        set fsw-wan1-admin enable
        set poe-detection-type 2
        set version 1
        set max-allowed-trunk-members 8
        set pre-provisioned 1
        set dynamic-capability 0x0000000000000001551027757dddfff7
        config ports
            edit "port1"
                set poe-capable 1
                set vlan "APs"
                set allowed-vlans "VLAN102" "VLAN101" "quarantine"
                set untagged-vlans "quarantine"
                set export-to "root"
                set mac-addr 04:d5:90:39:7d:8e
            next
```

A FortiSwitch is successfully managed by a FortiGate. FortiAP is connected to port1 of the managed FortiSwitch. On FortiGate, the VLAN AP is configured to detect and manage FortiAP, along with a DHCP server for the VLAN AP. Additionally, the VLAN AP is assigned to port1 of FortiSwitch. However. FortiGate is unable to detect or manage FortiAP.
Which FortiGate misconfiguration is preventing the detection of FortiAP?

A. Security Fabric is disabled in the administrative access options of the VLAN.
B. The FortiAP firmware is incompatible with the FortiGate firmware version.
C. The VLAN is not tagged correctly on the FortiSwitch uplink port.
D. The CAPWAP ports (UDP 5246 and 5247) are not open on FortiGate.

Answer: A

NEW QUESTION 10
Which VLAN is used by FortiGate to place devices that fail to match any configured NAC policies? CRSPAN

A. NAC
B. segment
C. Quarantine
D. Onboarding

Answer: D

NEW QUESTION 10
In a Windows environment using AD machine authentication, how does FortiAuthenticator ensure that a previously authenticated device is maintaining its network access once the device resumes operating after sleep or hibernation?

A. It temporarily assigns the device to a guest VLAN until full reauthentication is completed.
B. It sends a wake-on-LAN packet to trigger reauthentication.
C. It uses machine authentication based on the device IP address.
D. It caches the MAC address of authenticated devices for a configurable period of time.

Answer: D

NEW QUESTION 11
Connectivity tests are being performed on a newly configured VLAN. The VLAN is configured on a FortiSwitch device that is managed by FortiGate. During testing, it is observed that devices within the VLAN can successfully ping FortiGate. and FortiGate can also ping these devices.
Inter-VLAN communication is working as expected. However, devices within the same VLAN are unable to communicate with each other.
What could be causing this issue?

A. Access VLAN is enabled on the VLAN.
B. The FortiSwitch MAC address table is missing entries.
C. The FortiGate ARP table is missing entries.
D. The native VLAN configured on the ports is incorrect.

Answer: A

NEW QUESTION 16
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.

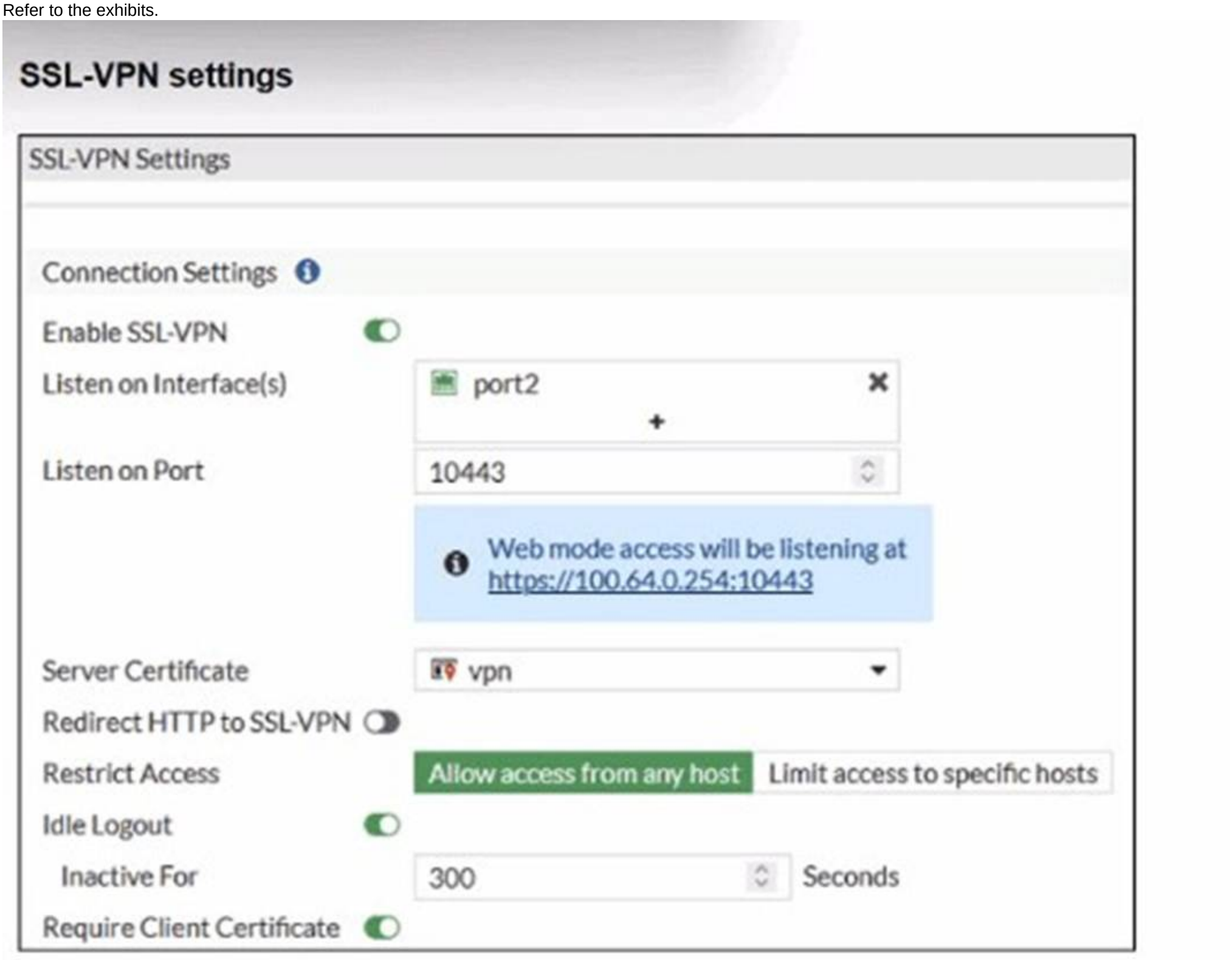
Answer: C

NEW QUESTION 18
Which statement about generating a certificate signing request (CSR) for a CER certificate is true?

A. Inaccurate or missing fields in the CSR will prevent the CA from validating the request, leading to the rejection of the certificate and possible delays in the deployment process.
B. If key fields like the common name (CN) and organization (O) are incorrect, the certification authority (CA) will still issue the certificate, but it may not be trusted by certain applications or systems that rely on accurate field information for validation.
C. CSR fields are primarily used for internal recordkeeping by the requesting organization, and only the public key in the CSR must be accurate for successful certificate signing.
D. The fields in the CSR are primarily for documentation purposes; any missing or incorrect information will be automatically corrected by the CA during the signing process.

Answer: A

NEW QUESTION 21
Refer to the exhibits.



Real-Time debug output

```
FortiGate # diagnose debug application fnbamd -1
Debug messages will be on for 30 minutes.

FortiGate # diagnose debug enable

FortiGate # [2341] handle_req-Rcvd auth_cert req id=1288058918, len=1104, opt=0
[948] __cert_auth_ctx_init-req_id=1288058918, opt=0
[103] __cert_chg_st- 'Init'
[140] fnbamd_cert_load_certs_from_req-1 cert(s) in req.
[99] __cert_chg_st- 'Init' -> 'Chain-Build'
[683] __cert_build_chain-req_id=1288058918
[200] fnbamd_chain_build-Chain discovery, opt 0x17, cur total 1
[216] fnbamd_chain_build-Following depth 0
[271] fnbamd_chain_build-Extend chain by system trust store. (no luck)
[283] fnbamd_chain_build-Extend chain by remote CA cache. (no luck)
[99] __cert_chg_st- 'Chain-Build' -> 'CA-Query'
[777] __cert_ca_query-req_id=1288058918
[769] fnbamd_need_CA_query-Do CA query?0
[793] __cert_ca_query_do_next-req_id=1288058918
[99] __cert_chg_st- 'CA-Query' -> 'Validation'
[804] __cert_verify-req_id=1288058918
[805] __cert_verify-Chain is not complete.
[200] fnbamd_chain_build-Chain discovery, opt 0x7, cur total 1
[216] fnbamd_chain_build-Following depth 0
[271] fnbamd_chain_build-Extend chain by system trust store. (no luck)
[283] fnbamd chain build-Extend chain by remote CA cache. (no luck)
```

Real-Time debug output

```
[396] fnbamd_cert_verify-Chain number:1
[410] fnbamd_cert_verify-Following cert chain depth 0
[676] fnbamd_cert_check_group_list-checking group with name 'SSLVPN'
[490] __check_add_peer-check 'student'
[460] __quick_check_peer-CA does not match.
[498] __check_add_peer-'student' check ret:bad
[193] __get_default_ocsp_ctx-def_ocsp_ctx=(nil), no_ocsp_query=0, ocsp_enabled=0
[841] __cert_verify_do_next-req_id=1288058918
[99] __cert_chg_st- 'Validation' -> 'Done'
[886] __cert_done-req_id=1288058918
[1652] fnbamd_auth_session_done-Session done, id=1288058918
[931] __fnbamd_cert_auth_run-Exit, req_id=1288058918
[1689] create_auth_cert_session-fnbamd_cert_auth_init returns 0, id=1288058918
[1608] auth_cert_success-id=1288058918
[1031] fnbamd_cert_auth_copy_cert_status-req_id=1288058918
[833] fnbamd_cert_check_matched_groups-checking group with name 'SSLVPN'
[903] fnbamd_cert_check_matched_groups-not matched
[1070] fnbamd_cert_auth_copy_cert_status-Leaf cert status is unchecked.
[1087] fnbamd_cert_auth_copy_cert_status-Issuer of cert depth 0 is not deteced in CMDB.
[1158] fnbamd_cert_auth_copy_cert_status-Cert st 2040, req_id=1288058918
[217] fnbamd_comm_send_result-Sending result 0 (nid 672) for req 1288058918, len=2144
[1553] destroy_auth_cert_session-id=1288058918
[1004] fnbamd_cert_auth_uninit-req_id=1288058918
```

Which include debug output and SSL VPN configuration details.
An SSL VPN has been configured on FortiGate. To enhance security, the administrator enabled Required Client Certificate in the SSL VPN settings. However, when a user attempts to connect, authentication fails.
Which configuration change is needed to fix the issue and allow the user to connect?

A. Enable Redirect HTTP to SSL-VPN on the SSL VPN configuration page.

B. Import the CA that signed the SSL VPN Server Certificate to FortiGate.
C. Set the user certificate as the Server Certificate on the SSL VPN configuration page.
D. Import the CA that signed the user certificate to FortiGate.

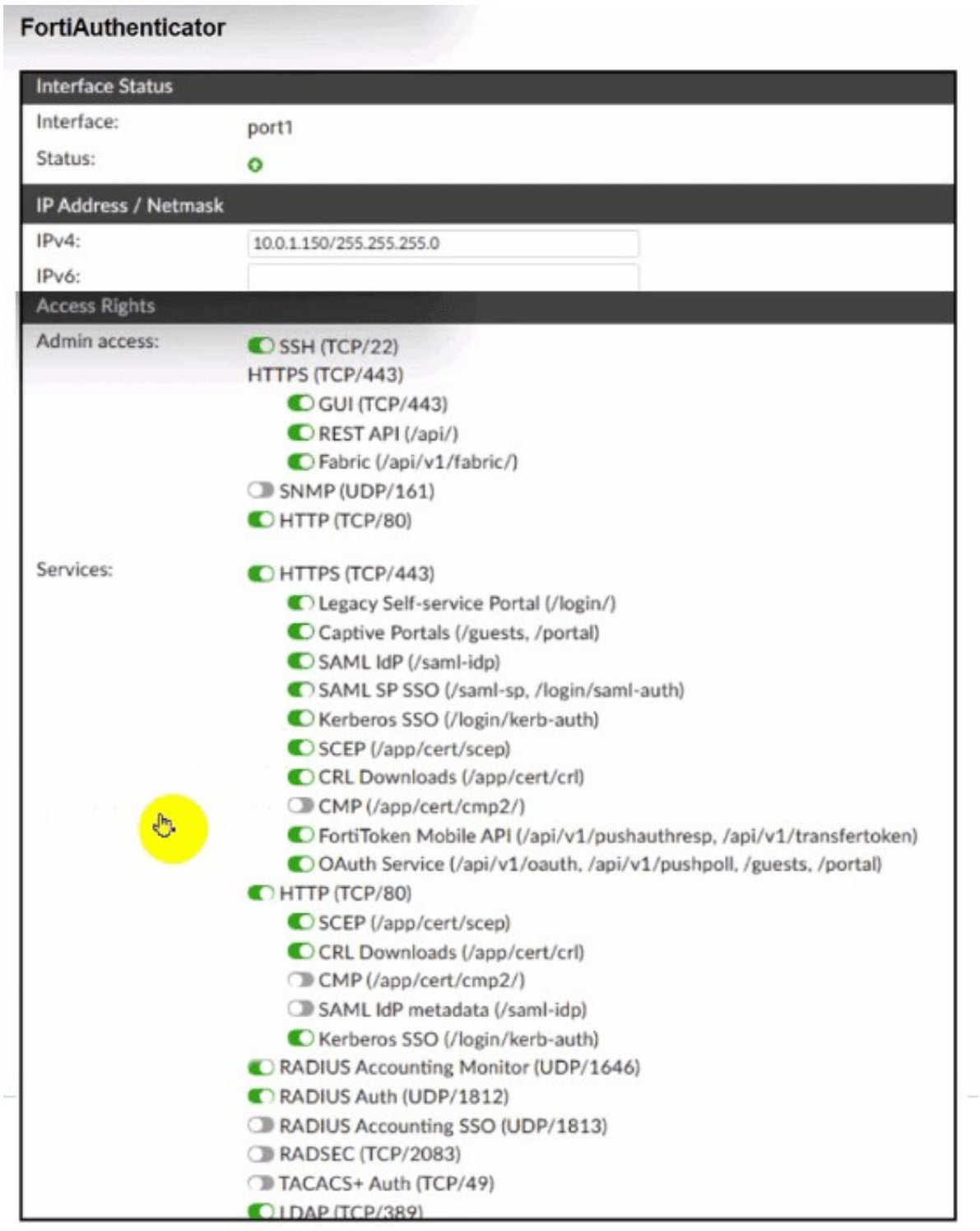
Answer: D

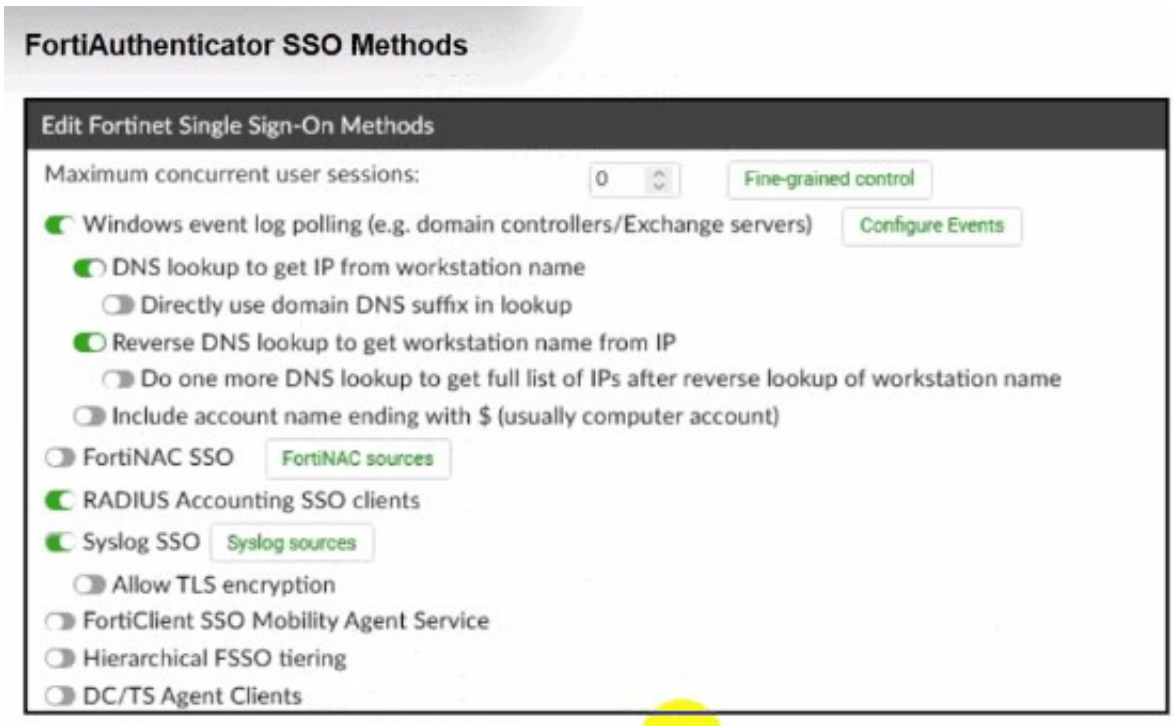
NEW QUESTION 23
APs have been manually configured to connect to FortiGate over an IPsec network, and FortiGate successfully detects and authorizes them. However, the APs remain unmanaged because FortiGate is unable to establish a CAPWAP tunnel with them.
What configuration change can resolve this issue and enable FortiGate to establish the CAPWAP tunnel over the IPsec connection?

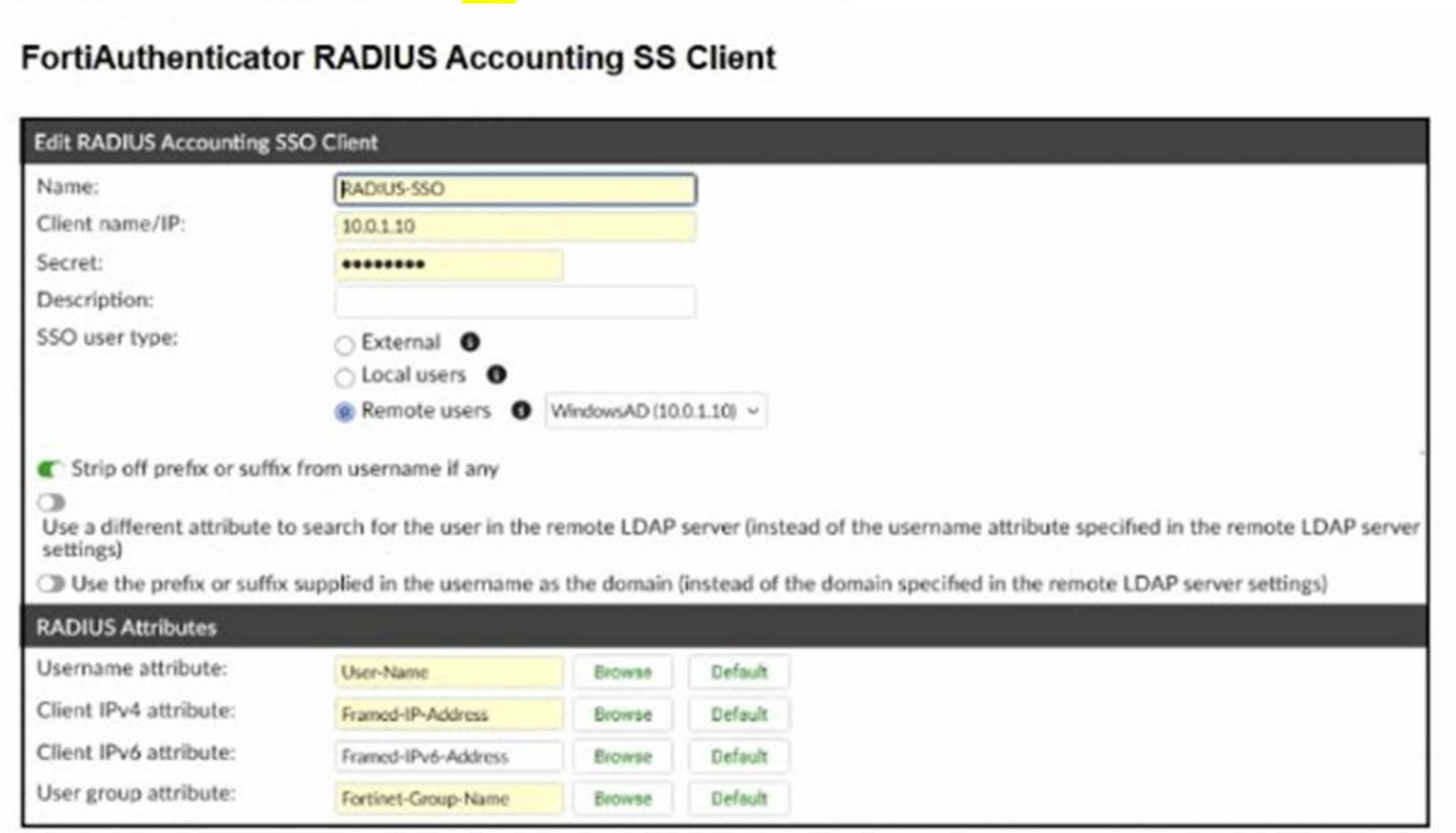
A. Configure a static route on FortiGate to reach the APs over the IPsec tunnel.
B. Assign a custom AP profile for the remote APs with the set mpls-connection option enabled.
C. Decrease the CAPWAP tunnel MTU size for APs to prevent fragmentation.
D. Upgrade the FortiAP firmware image to ensure compatibility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

Answer: B

NEW QUESTION 28
Refer to the exhibits.







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 29
You've configured the FortiLink interface, and the DHCP server is enabled by default.

```
config system dhcp server
    edit 1
        set ntp-service local
        set default-gateway 169.254.1.1
        set netmask 255.255.255.0
        set interface "fortilink"
        config ip-range
            edit 1
                set start-ip 169.254.1.2
                set end-ip 169.254.1.254
            next
        end
        set vci-match enable
        set vci-string "FortiSwitch" "FortiExtender"
    next
end
```

The resulting DHCP server settings are shown in the exhibit. What is the role of the vci-string setting in this configuration?

A. To ignore DHCP requests coming from FortiSwitch and FortiExtender devices.
B. To restrict the IP address assignment to devices that have FortiSwitch or FortiExtender as their hostname.
C. To connect, devices must match the VCI string; otherwise, they will not receive an IP address.
D. To reserve IP addresses for FortiSwitch and FortiExtender devices.

Answer: C

NEW QUESTION 32
.....

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