Exam Questions FCSS_LED_AR-7.6

FCSS - LAN Edge 7.6 Architect

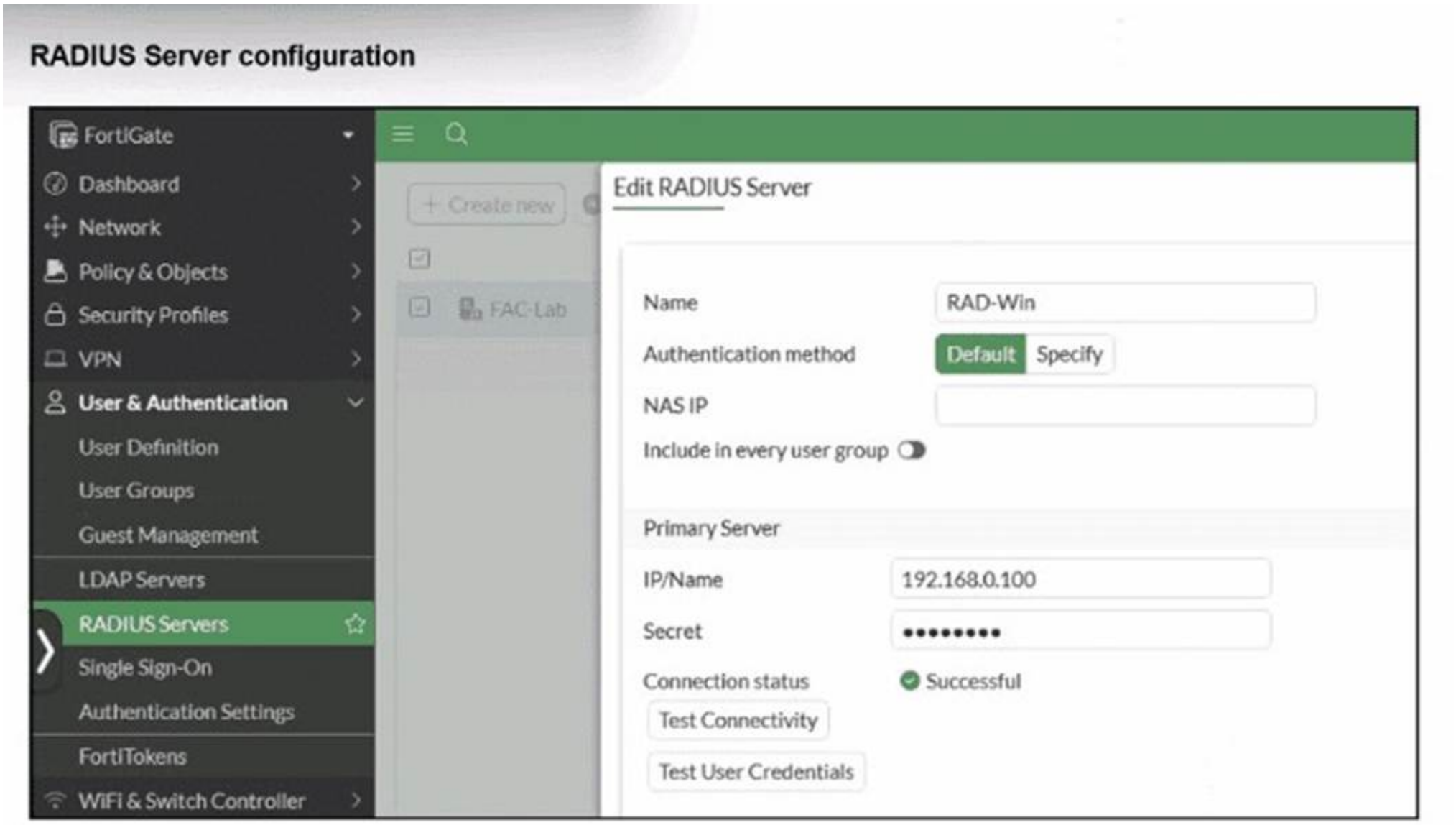
https://www.2passeasy.com/dumps/FCSS_LED_AR-7.6/

NEW QUESTION 1
Which FortiGuard licenses are required for FortiLink device detection to enable device identification and vulnerability detection?

A. FortiGuard Vulnerability Management and FortiGuard Endpoit Protection
B. FortiGuard Threat Intelligence and FortiGuard loT Detection
C. FortiGuard Threat Intelligence and FortiGuard Endpoint Protection
D. FortiGuard Attack Surface Security and FortiGuard loT Detection

Answer: D

NEW QUESTION 2
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 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

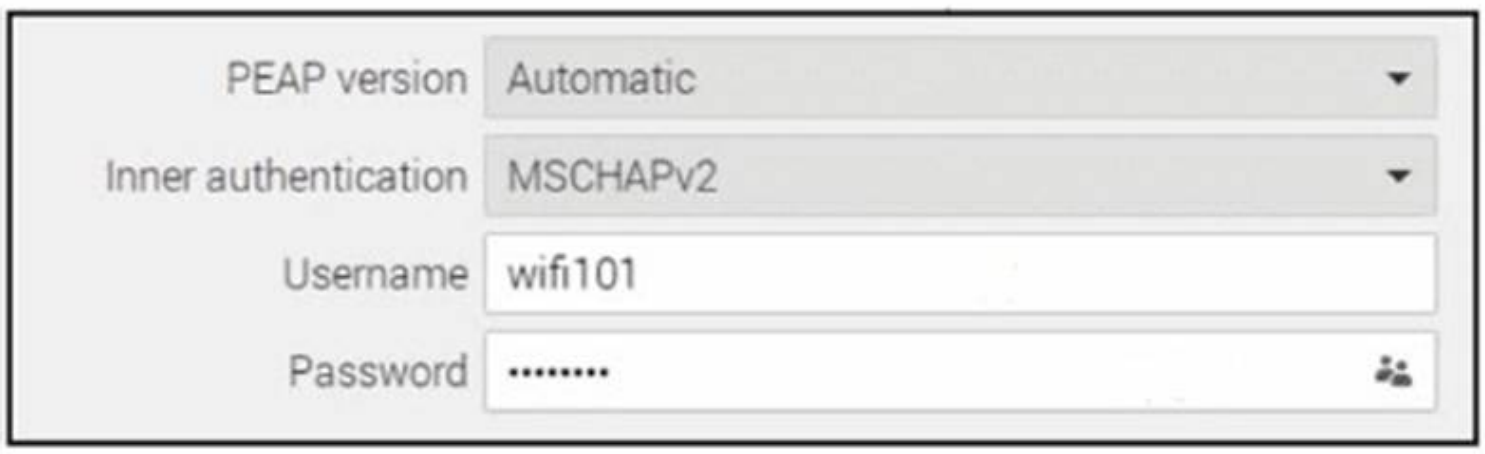
NEW QUESTION 4
Refer to the exhibits.

FortiGate LDAP server configuration and diagnostics

```
config user ldap
    edit "FAC-LDAP"
        set server "10.0.1.10"
        set cnid "sAMAccountName"
        set dn "DC=trainingAD,DC=training,DC=lab"
        set type regular
        set username "CN=Administrator,CN=Users,DC=trainingAD,DC=training,DC=lab"
        set password ENC MTAwNE2iciyoaiRa20HnjmgtQbCRYdI+OJtfO7y9+uW5V8ZxQ/Vj+mW4zPijgtCgrnAA
    next
end

FortiGate # diagnose test authserver ldap FAC-LDAP wifi101 password
authenticate 'wifi101' against 'FAC-LDAP' succeeded!
Group membership(s) - CN=Domain Users,CN=Users,DC=trainingad,DC=training,DC=lab
Domain of user is trainingad.training.lab
```

Wi-Fi Authentication

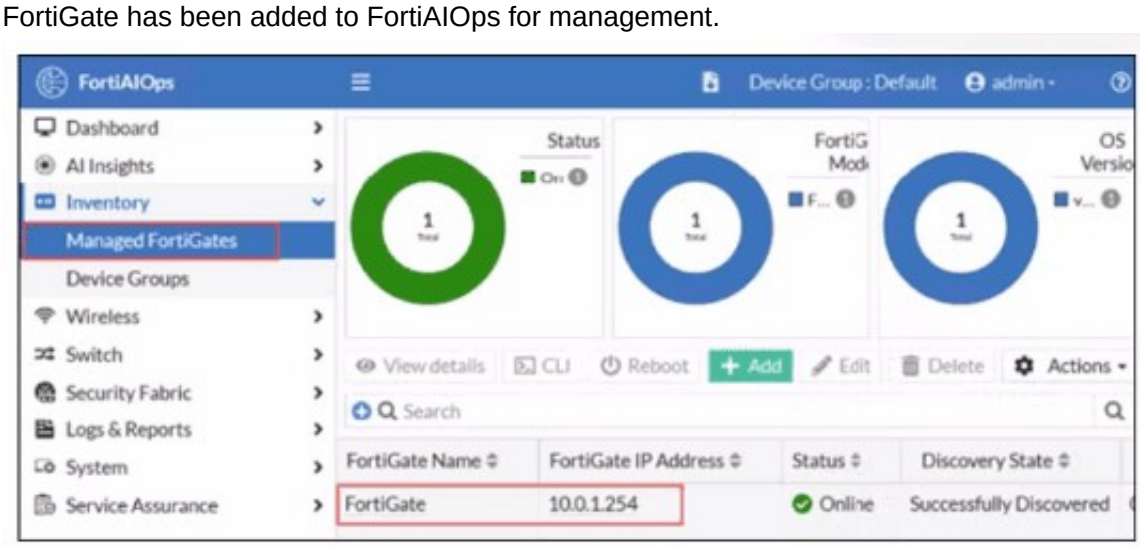


An LDAP server has been successfully configured on FortiGate. which forwards LDAP authentication requests to a Windows Active Directory (AD) server. Wireless users report that they are unable to authenticate. Upon troubleshooting, you find that authentication fails when using MSCHAPv2.
What is the most likely reason for this issue?

A. A firewall policy is missing an LDAP authentication rule.
B. The Windows AD server requires LDAPS (LDAP over SSL) for authentication.
C. The FortiGate LDAP configuration is missing the correct Bind DN.
D. FortiGate does not support MSCHAPv2 for LDAP authentication.

Answer: D

NEW QUESTION 5
FortiGate has been added to FortiAIOps for management.



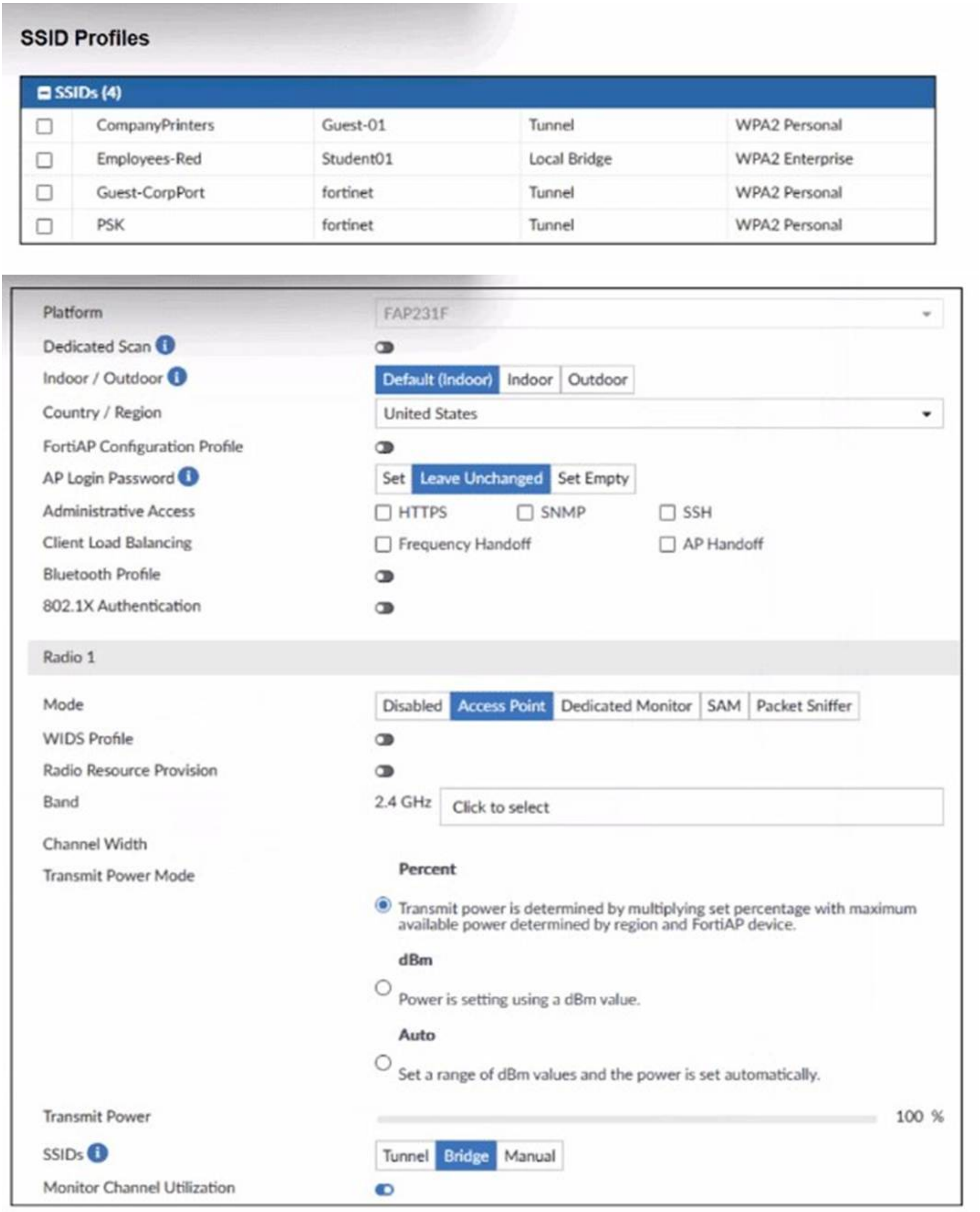
Which step must be performed on FortiAIOps to add a FortiSwitch device connected to the recently added FortiGate?

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 6
Refer to the exhibits.

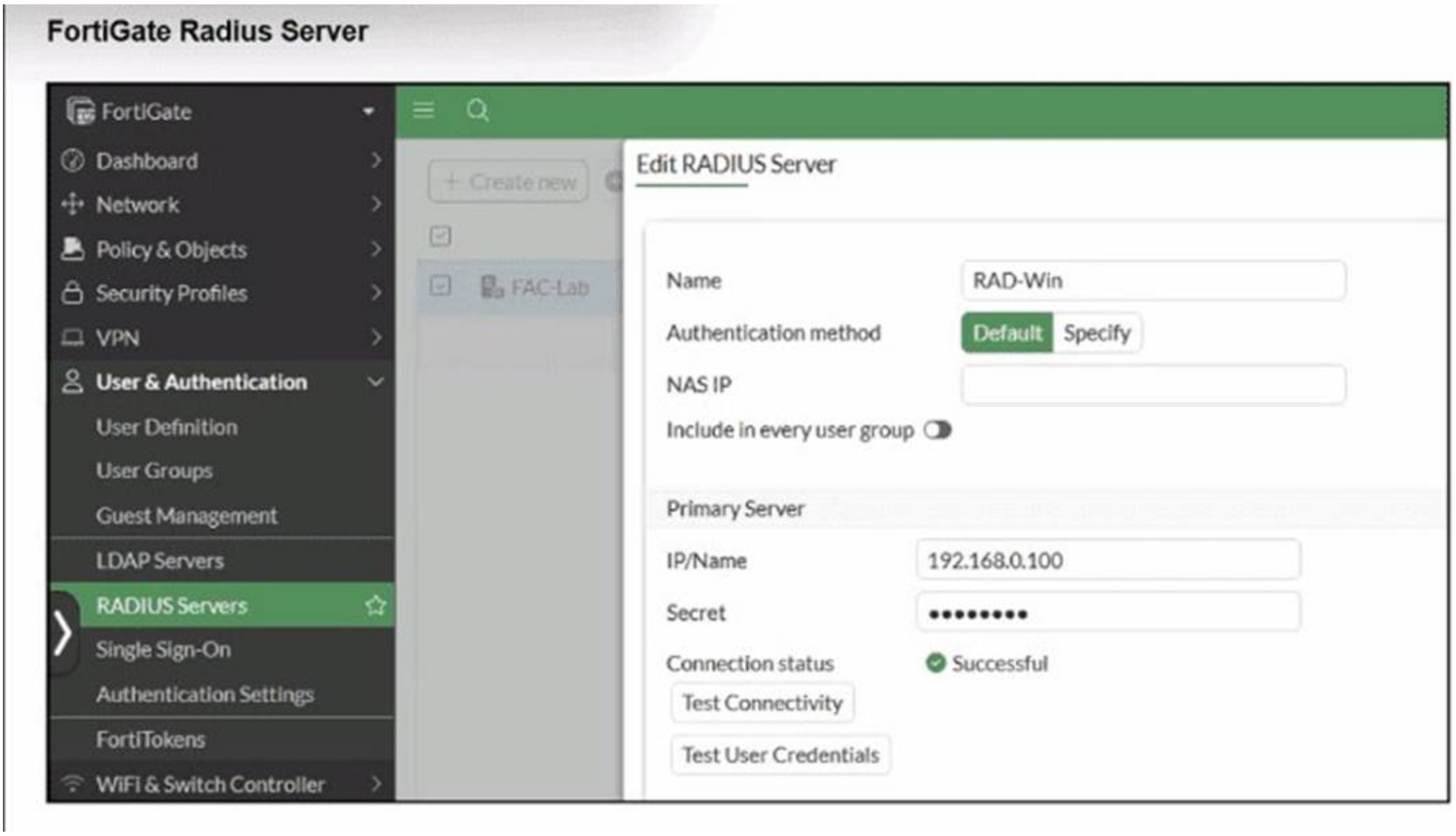


A set of SSID profiles has been configured on FortiManager, and an AP profile has been assigned to a group of AP managed by FortiGate. However, none of the designated SSIDs are being broadcast by these APs.
Which configuration change is required to make the APs broadcast these SSIDs as intended?

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

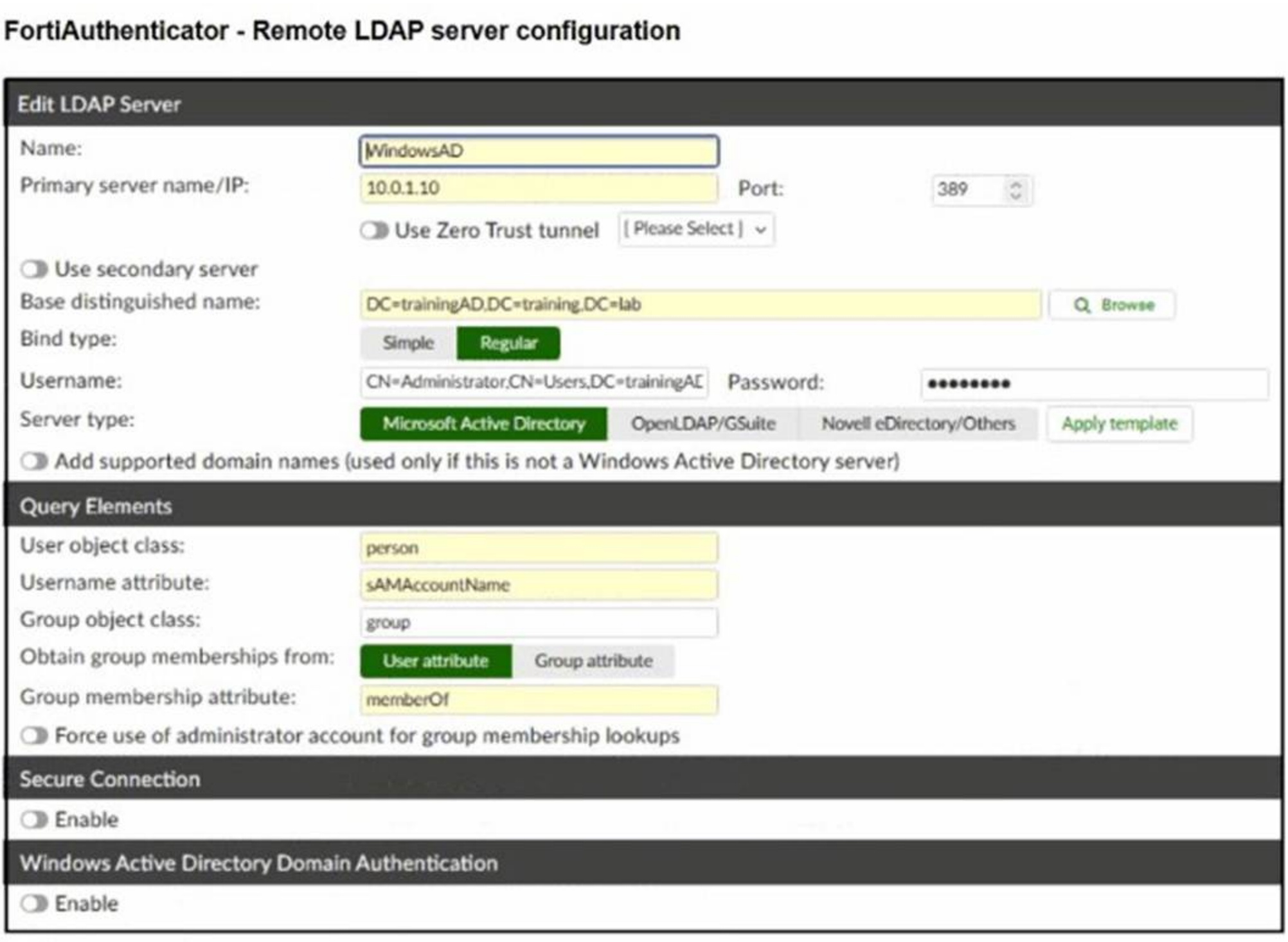
NEW QUESTION 7
Refer to the exhibit.



FortuiGate CLI RADIUS server test

```
FortiGate #
FortiGate # diagnose test authserver radius FAC-Lab pap wifi101 password
authenticate 'wifi101' against 'pap' succeeded, server=primary assigned_rad_session_id=19718280638473 session_timeout=0 secs idle_timeout=0 secs!

FortiGate # diagnose test authserver radius FAC-Lab mschap2 wifi101 password
authenticate 'wifi101' against 'mschap2' failed, assigned_rad_session_id=19718280638474 session_timeout=0 secs idle_timeout=0 secs!
```



A RADIUS server has been successfully configured on FortiGate, which sends RADIUS authentication requests to FortiAuthenticator. FortiAuthenticator, in turn, relays the authentication using LDAP to a Windows Active Directory server.
It was reported that wireless users are unable to authenticate successfully.
The FortiGate configuration confirms that it can connect to the RADIUS server without issues.
While testing authentication on FortiGate using the command diagnose test authserver radius, it was observed that authentication succeeds with PAP but fails with MSCHAPv2.
Additionally, the Remote LDAP Server configuration on FortiAuthenticator was reviewed. Which configuration change might resolve this issue?

A. Change the RADIUS authentication protocol to CHAP
B. Enable Windows Active Directory Domain Authentication.
C. Manually add user credentials to the FortiAuthenticator local database
D. Use RADIUS attributes under the FortiGate configuration.

Answer: B

NEW QUESTION 8
In addition to requiring a FortiAnalyzer device to configure the Security Fabric, which license must be added to FortiAnalyzer to use Indicators of Compromise (IOC) rules?

A. loT Security Add-on license
B. IOC Subscription license
C. IOC detection is included on FAZ-Basic license
D. Threat Detection Service license

Answer: D

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

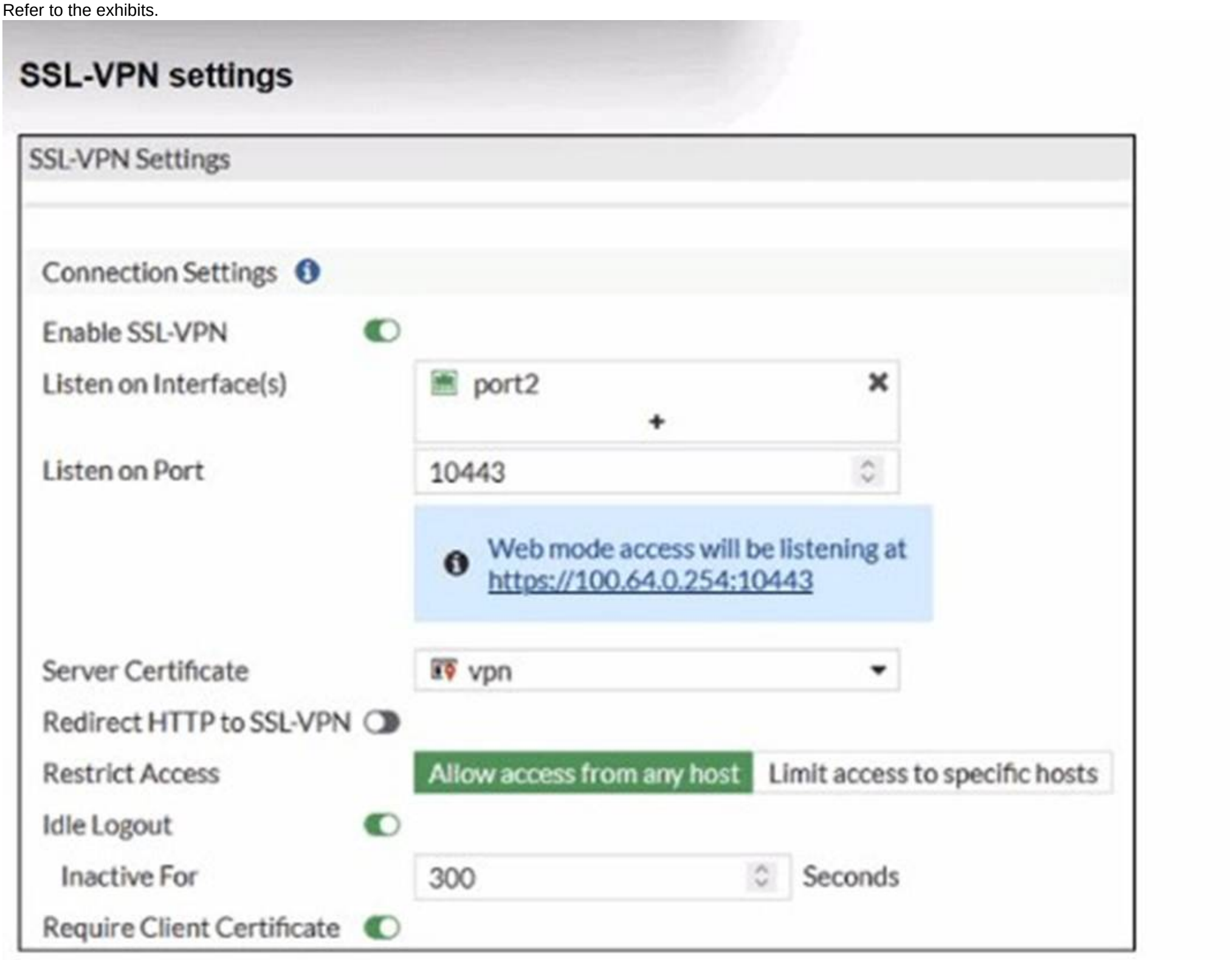
Answer: AE

NEW QUESTION 10
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 10
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.

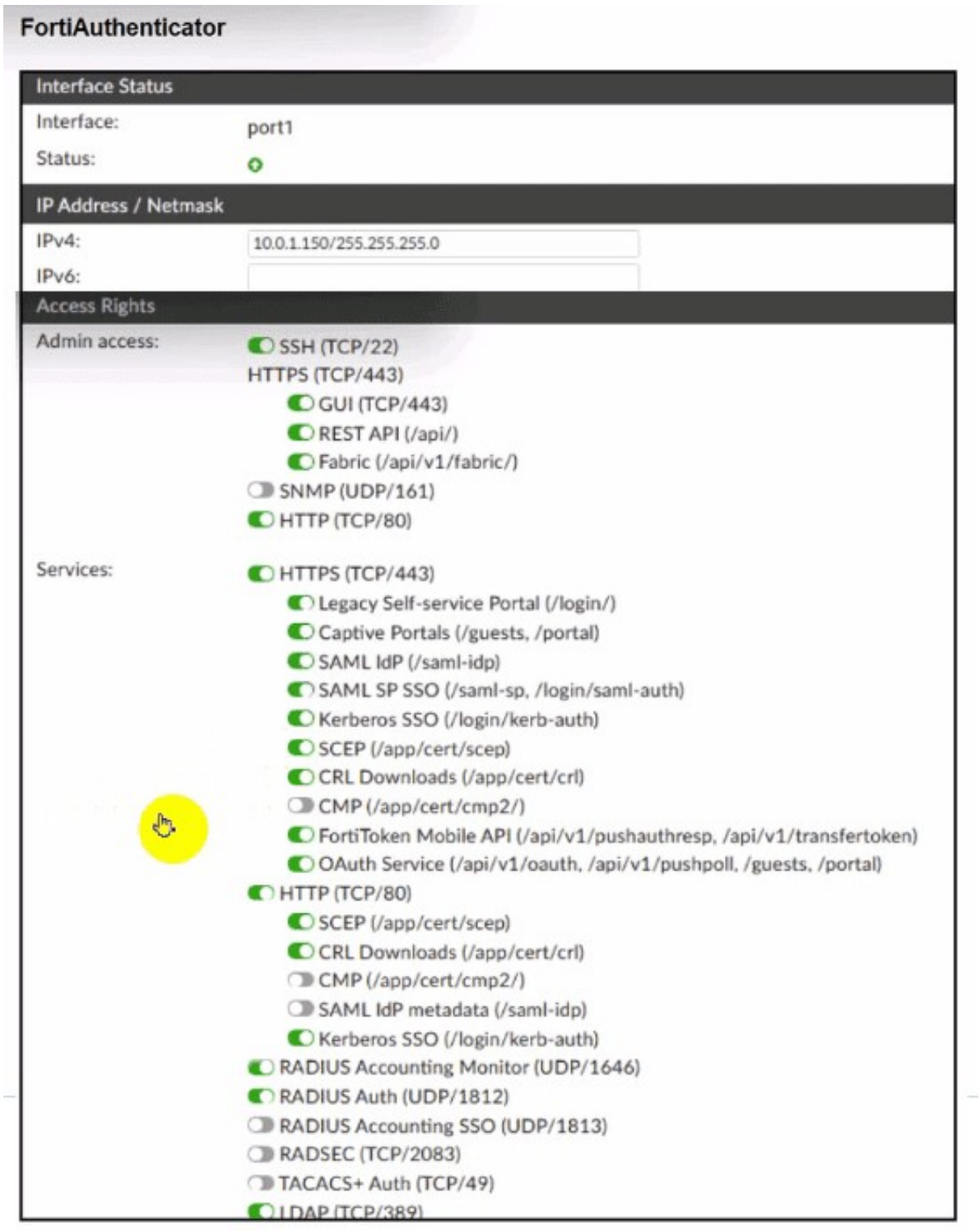
Answer: D

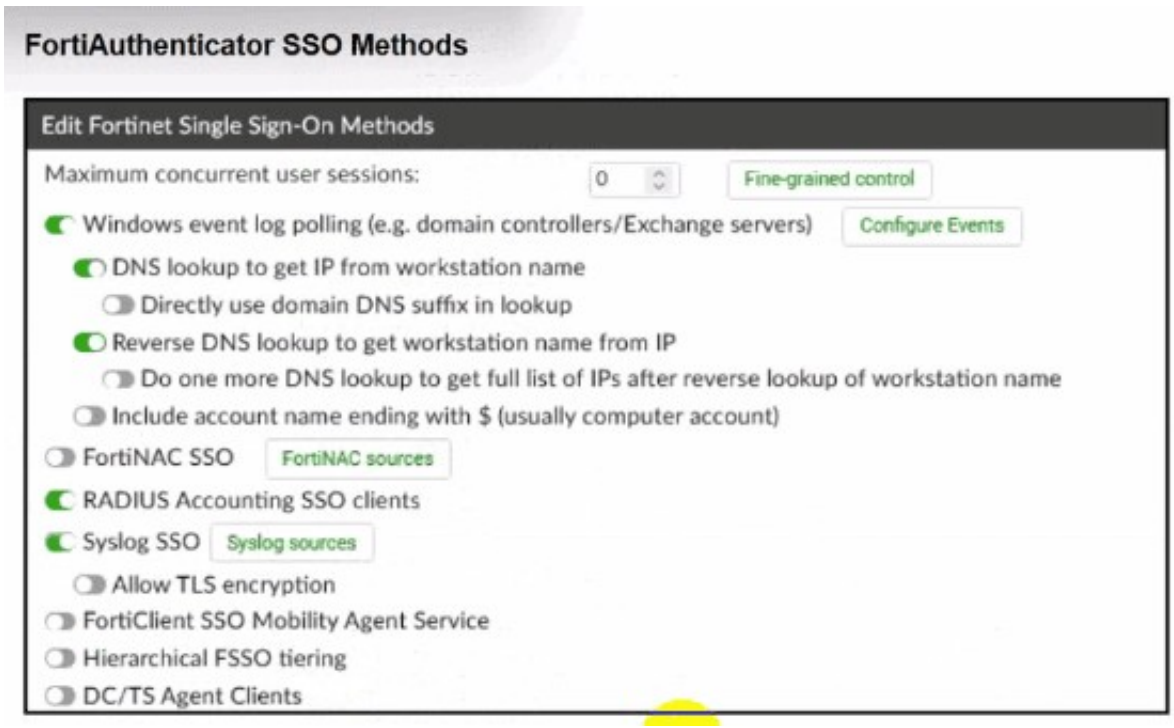
NEW QUESTION 13
APs have been manually configured to connect to FortiGate over an IPsec network, and FortiGate successfully detects and authorizes them. However, the APs remain unmanaged because FortiGate is unable to establish a CAPWAP tunnel with them.
What configuration change can resolve this issue and enable FortiGate to establish the CAPWAP tunnel over the IPsec connection?

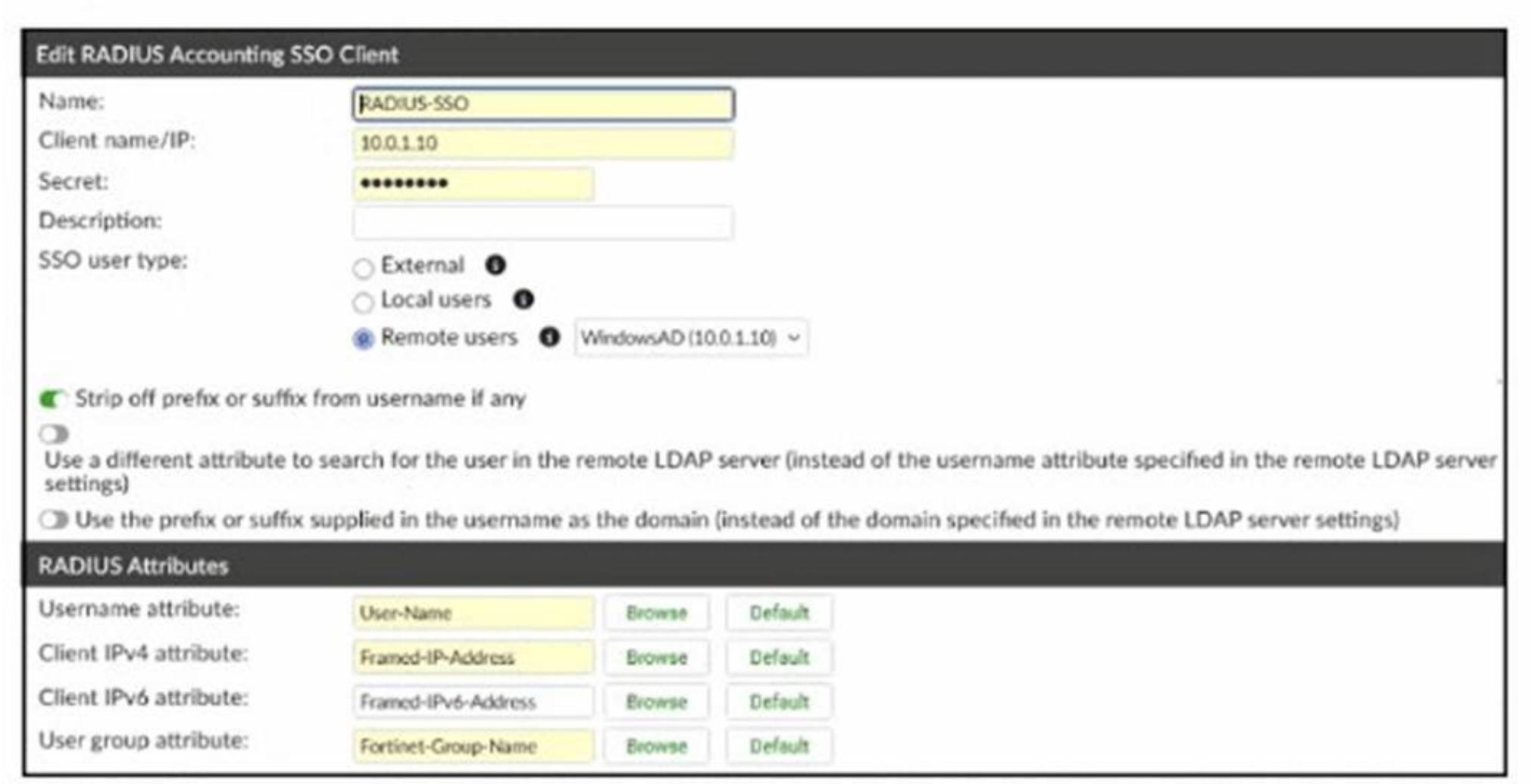
A. Configure a static route on FortiGate to reach the APs over the IPsec tunnel.
B. Assign a custom AP profile for the remote APs with the set mpls-connection option enabled.
C. Decrease the CAPWAP tunnel MTU size for APs to prevent fragmentation.
D. Upgrade the FortiAP firmware image to ensure compatibility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

Answer: B

NEW QUESTION 16
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 21
In each user certificate, you can define the subject field, expiration date. User Principal Name (UPN), URL for CRL download, and the OCSP URL. How does the detailed configuration of these attributes impact the certificate?

A. It makes the certificate easier to revoke manually because it reduces the need for automatic checks.
B. It limits the validity of the certificate to specific devices and applications, reducing its general usability.
C. It enables precise identification of the user and ensures timely certificate revocation checks.
D. It makes the certificate compatible with a wide range of applications and services by ensuring universal validity

Answer: C

NEW QUESTION 25

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual FCSS_LED_AR-7.6 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the FCSS_LED_AR-7.6 Product From:

https://www.2passeasy.com/dumps/FCSS_LED_AR-7.6/

Money Back Guarantee

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