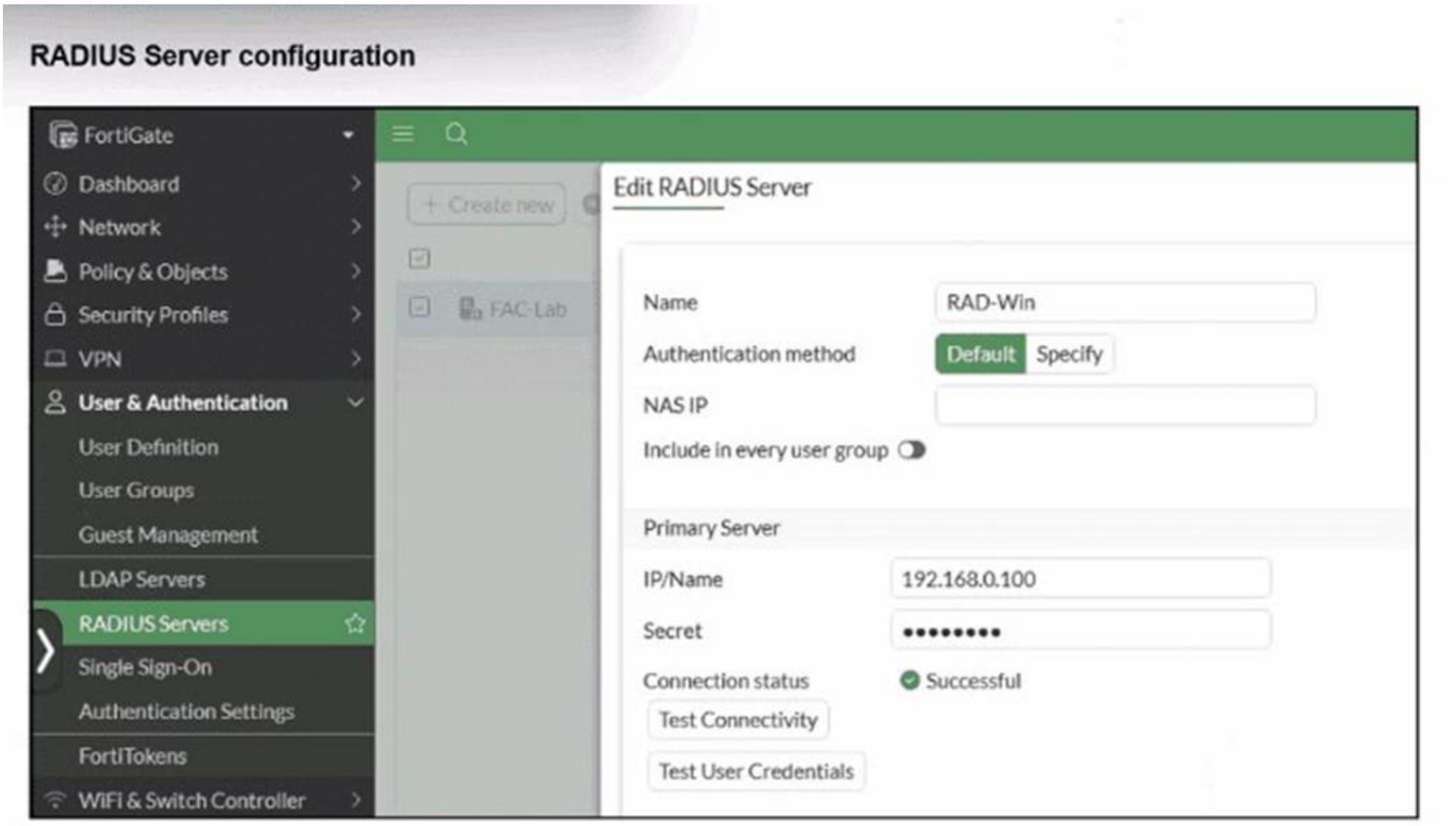
Fortinet

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

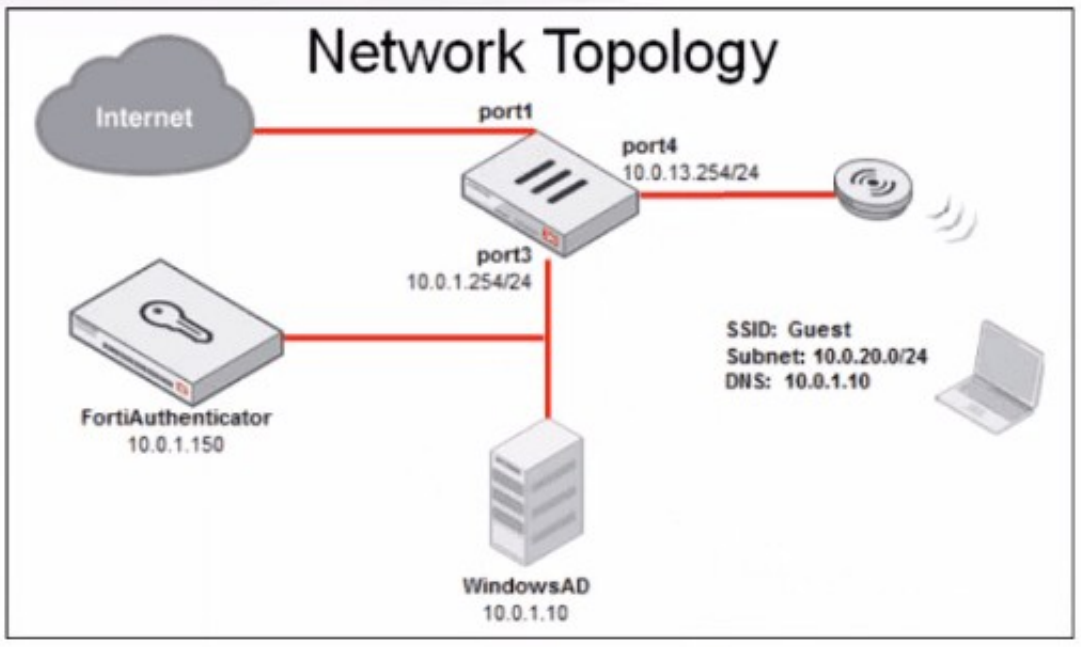
NEW QUESTION 2
You are configuring FortiAuthenticator to integrate with FSSO for user identification. To enable FortiAuthenticator to extract user information from syslog messages and inject it into FSSO, you have configured syslog matching rules.
What is the role of syslog matching rules in the process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

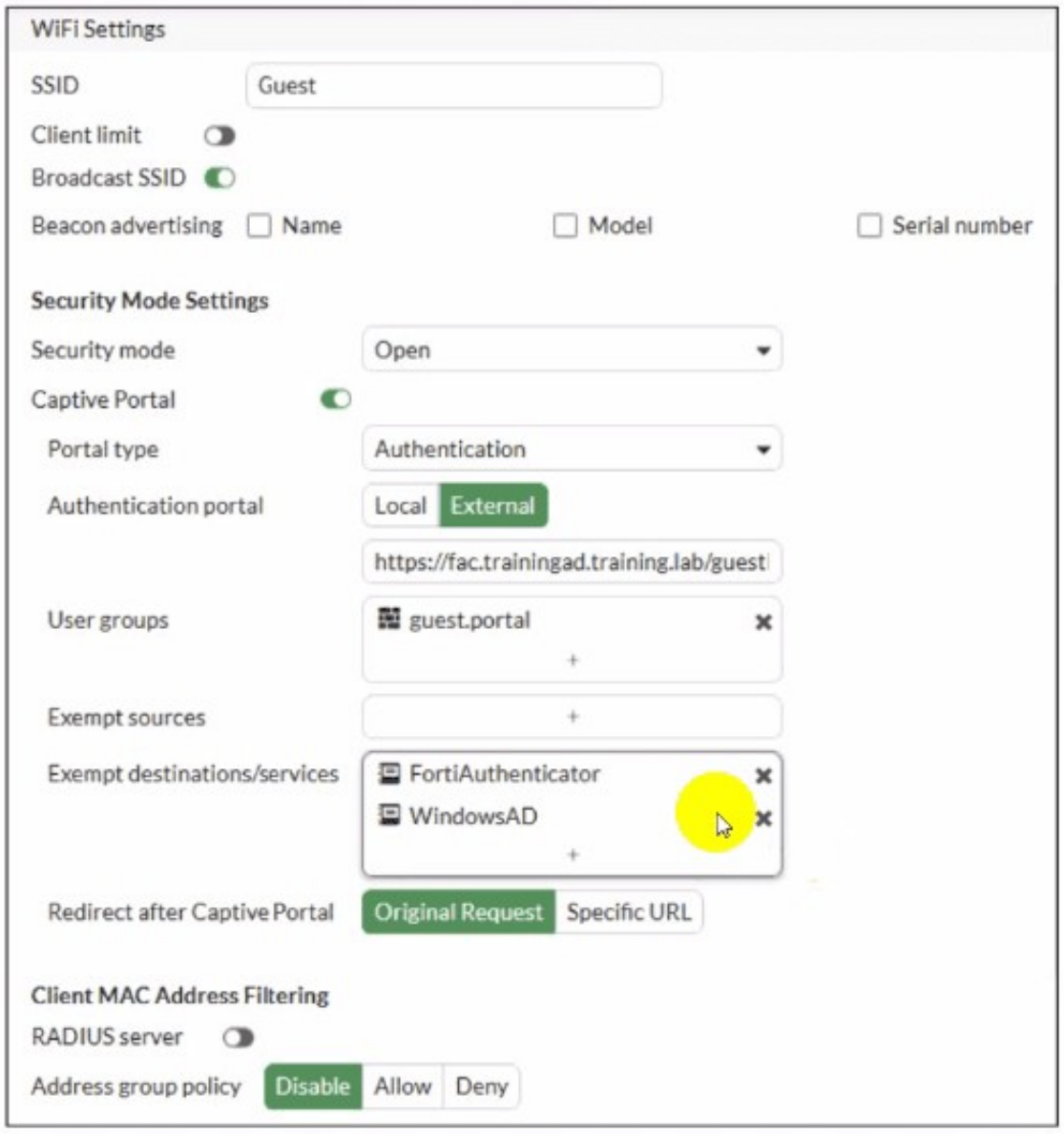
Answer: C

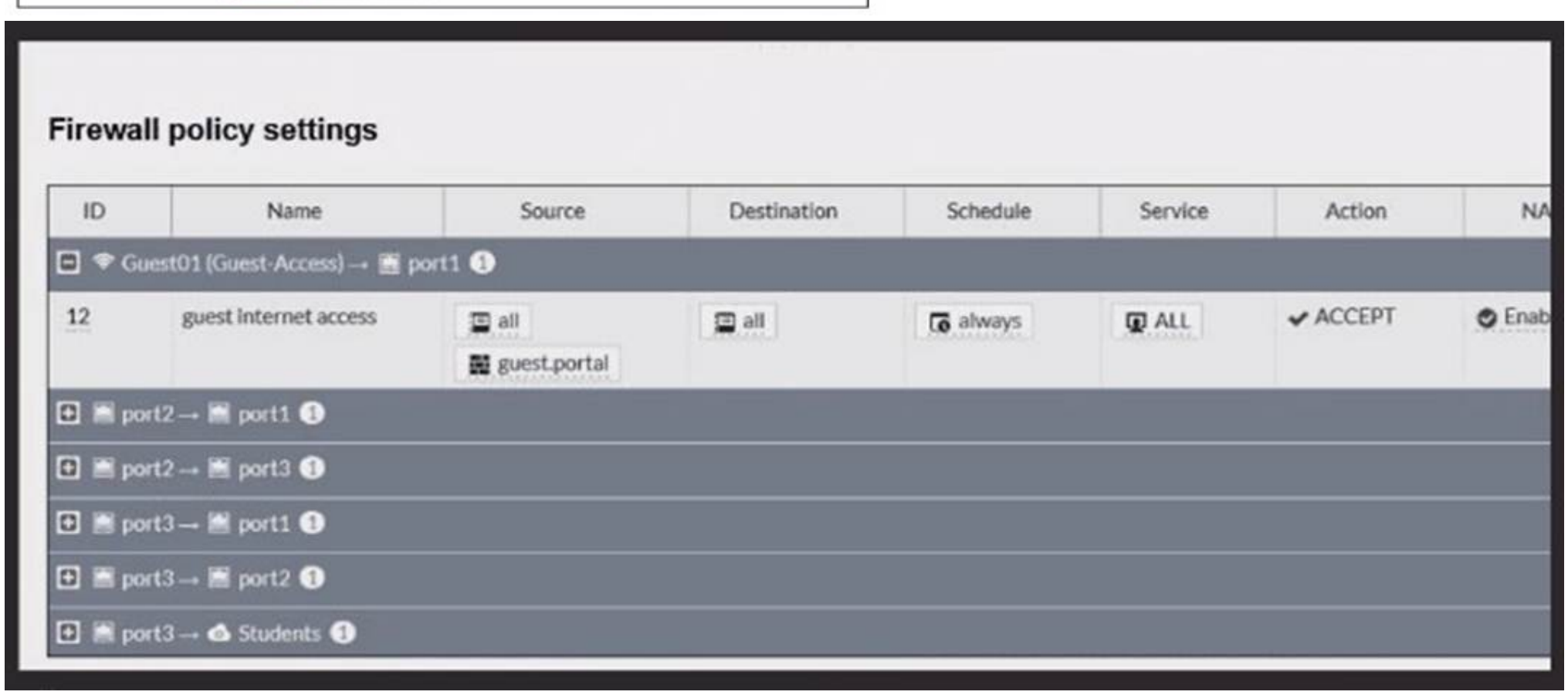
NEW QUESTION 3
Refer to the exhibit.

Network Topology



WiFi settings





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

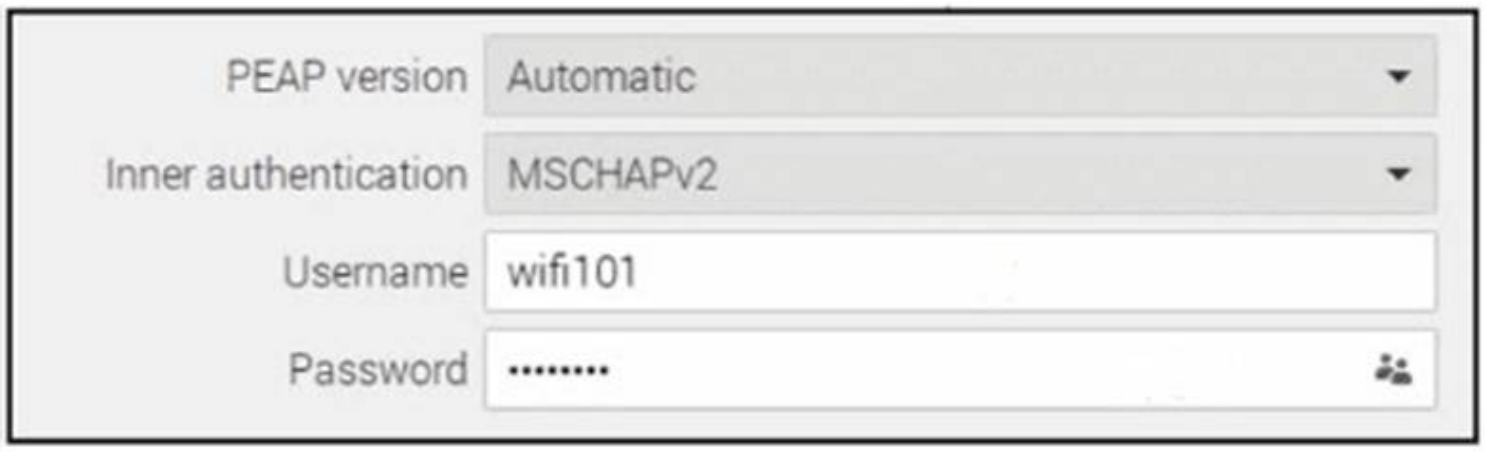
NEW QUESTION 4
Refer to the exhibits.

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
Refer to the exhibits.

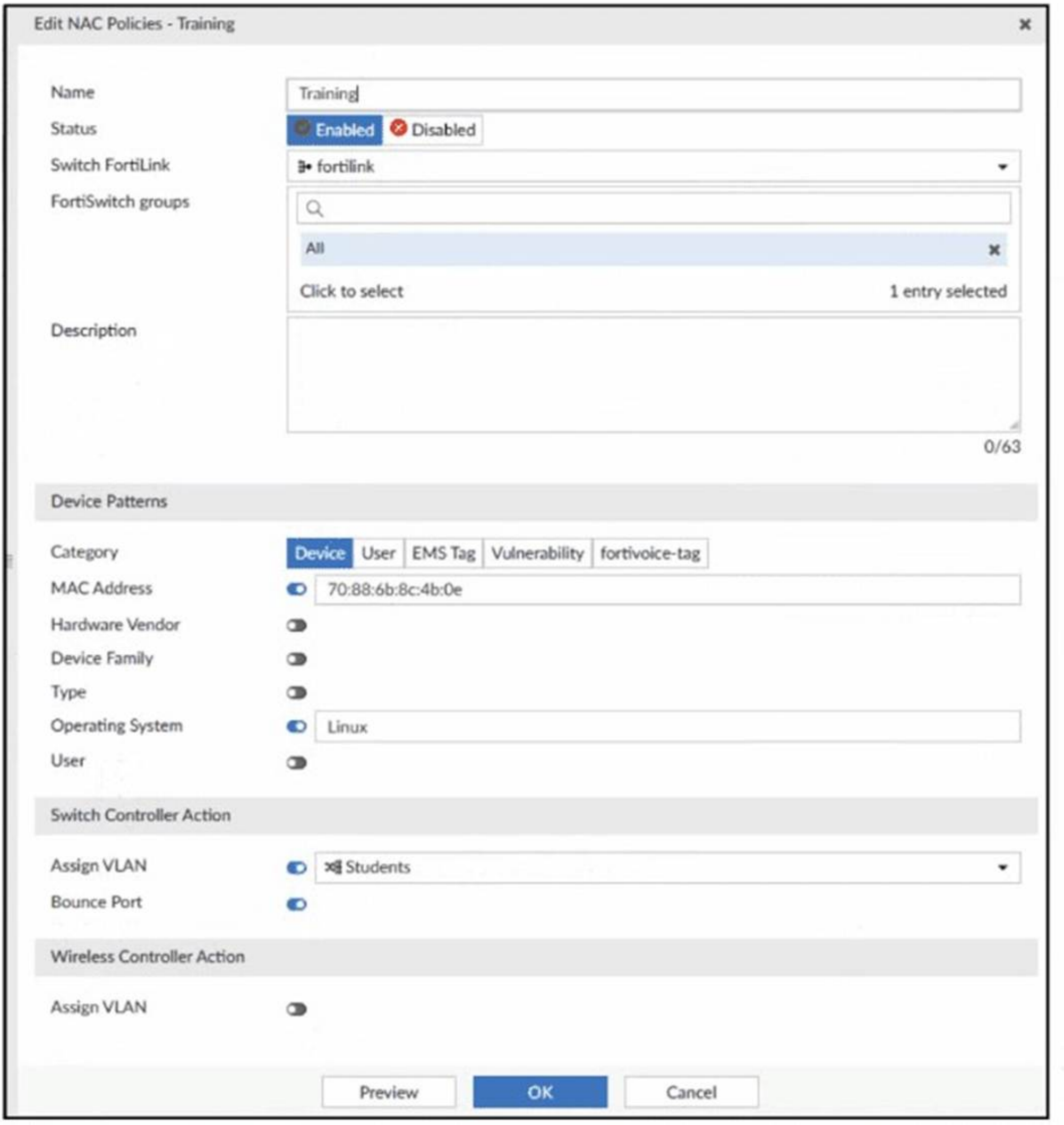
FortiSwitch Ports

FortiSwitch Ports - FortiSwitch

+ Create New | Edit | Delete | Refresh

	Port	Description	Mode	Port Policy	Enabled Features	Native VLAN	Allowed VLANs
☐	port1		Static		Edge Port Spanning Tree Protocol	AP Management (APs)	HR (VLAN102) IT (VLAN101) quarantine.fortilink (quarantine)
☐	port2		Static		Edge Port Spanning Tree Protocol	Students	quarantine.fortilink (quarantine)
☐	port3		Static		Edge Port Spanning Tree Protocol	default.fortilink (_default)	quarantine.fortilink (quarantine)

NAC policy

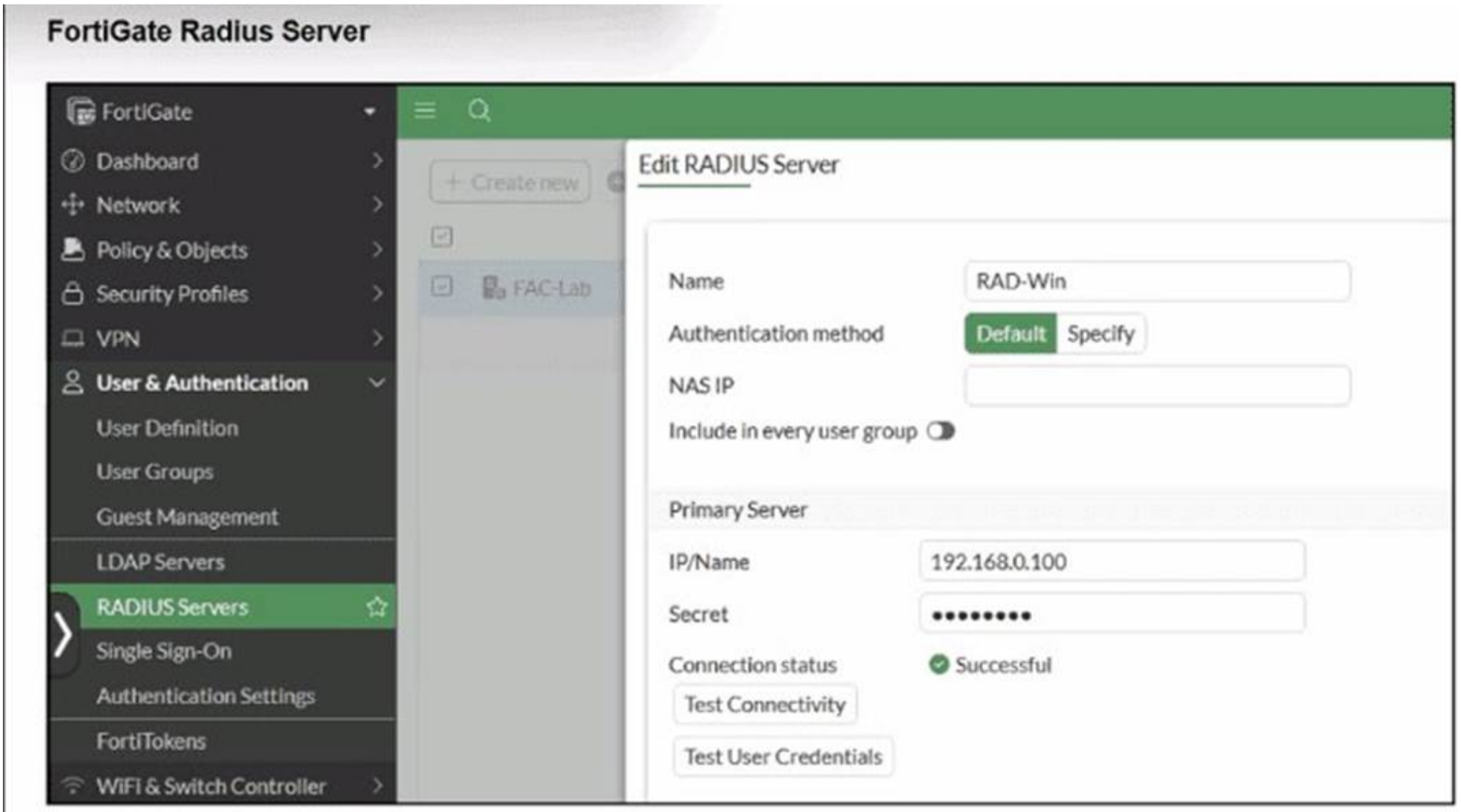


A NAC policy has been configured to apply traffic that flows through FortiSwitch port 2. Traffic that meets the NAC policy criteria will be assigned to the Students VLAN. However, the NAC policy does not seem to be taking effect.
Which configuration is missing?

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

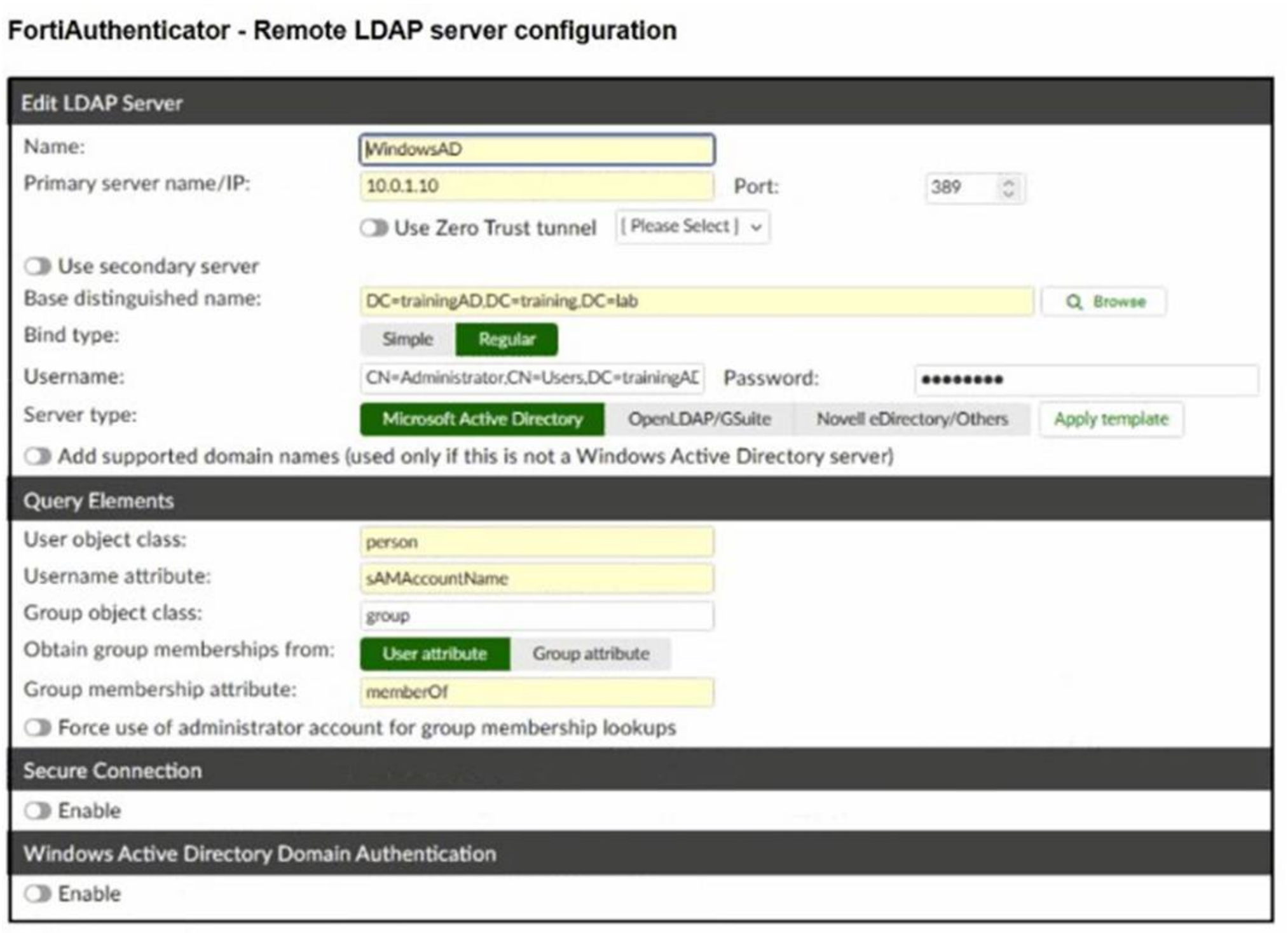
NEW QUESTION 6
Refer to the exhibit.



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

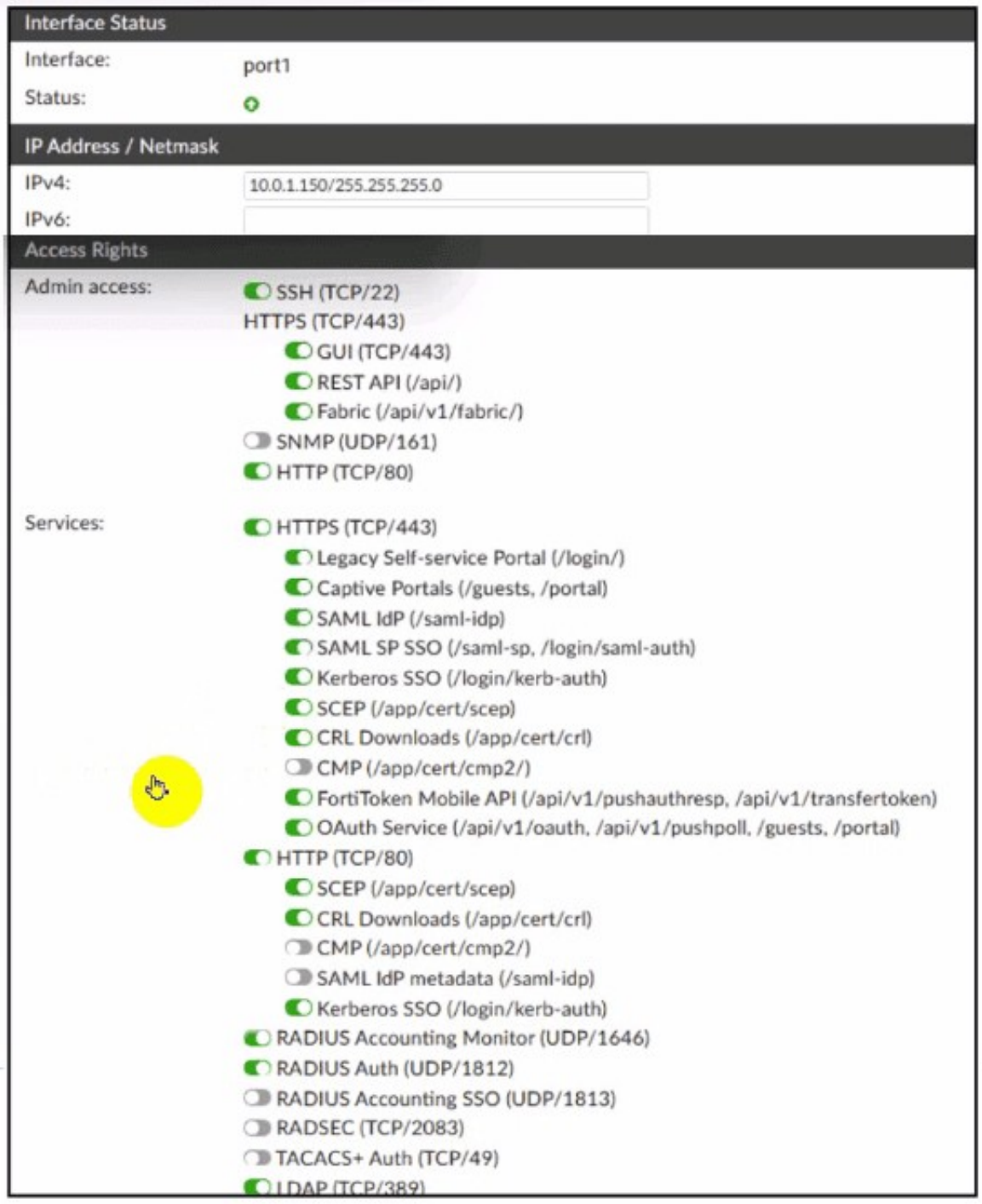
NEW QUESTION 7
In a Windows environment using AD machine authentication, how does FortiAuthenticator ensure that a previously authenticated device is maintaining its network access once the device resumes operating after sleep or hibernation?

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.

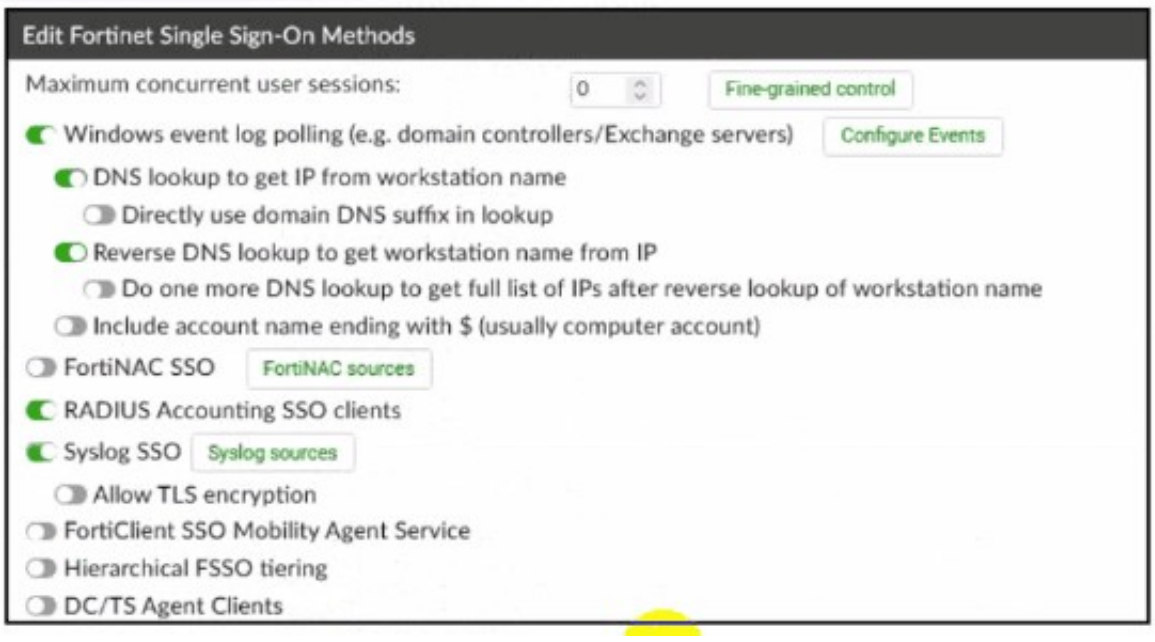
Answer: D

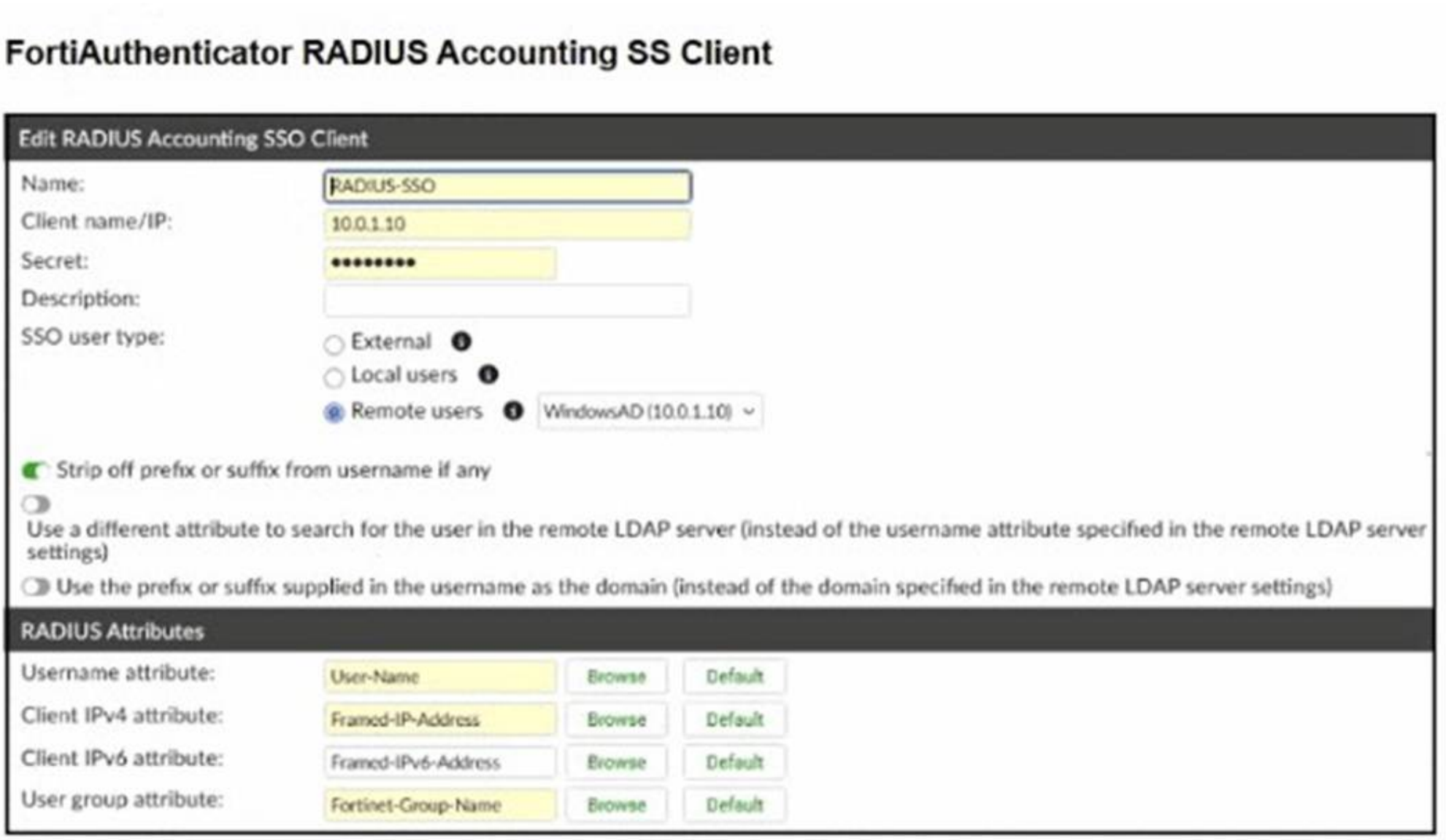
NEW QUESTION 8
Refer to the exhibits.

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

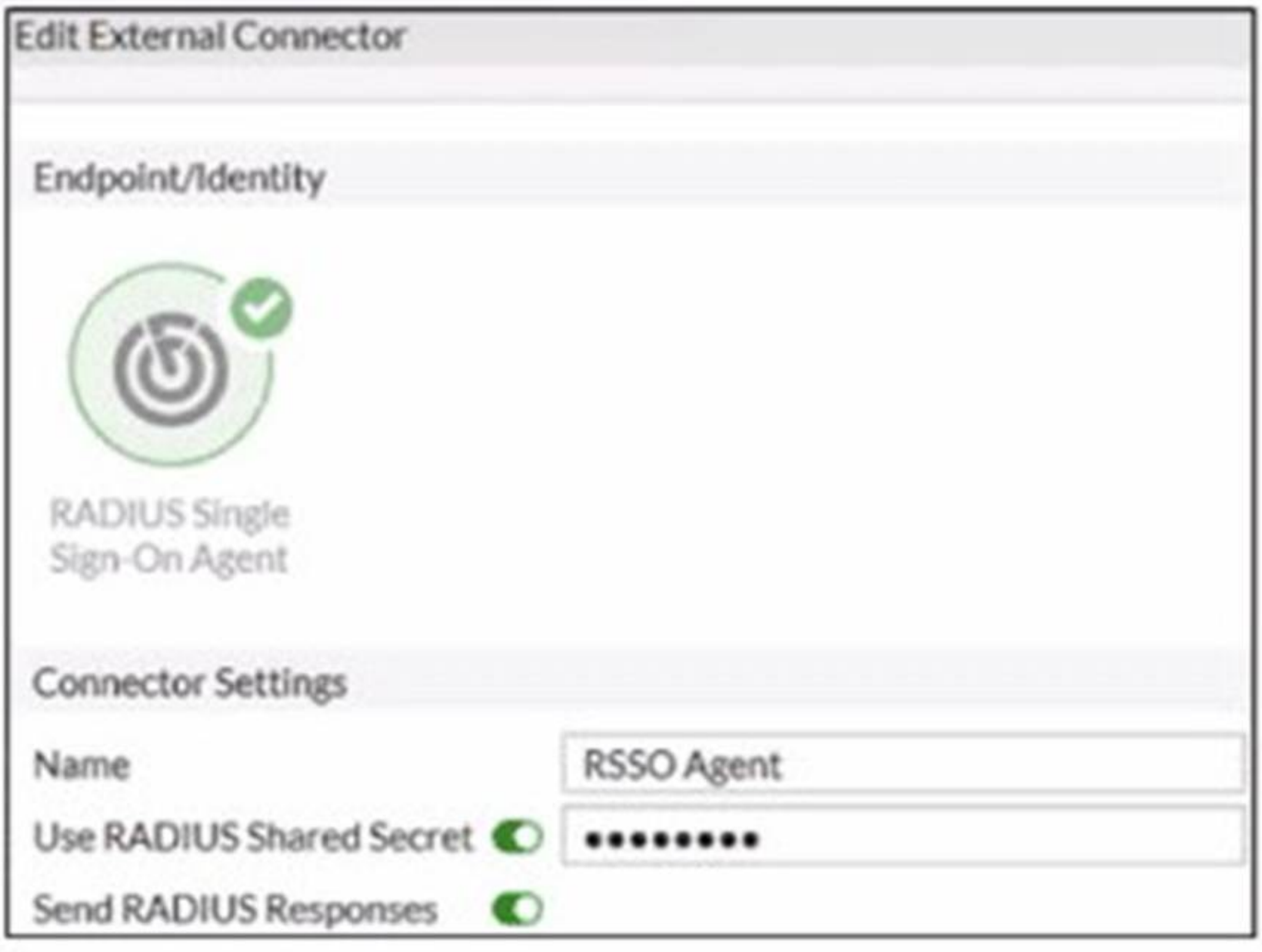
NEW QUESTION 9
You are setting up a captive portal to provide Wi-Fi access for visitors. To simplify the process, your team wants visitors to authenticate using their existing social media accounts instead of creating new accounts or entering credentials manually.
Which two actions are required to enable this functionality? (Choose two.)

A. Set up a remote open authorization (OAuth) server for each selected social media platform.
B. Configure only the email login option because a social media login cannot be used with captive portals.
C. Enable Account Login as the authentication type and configure a remote LDAP server.
D. Set up the FortiAuthenticator internal database as the primary source for user credentials
E. Configure the social login profiles for the supported platforms.

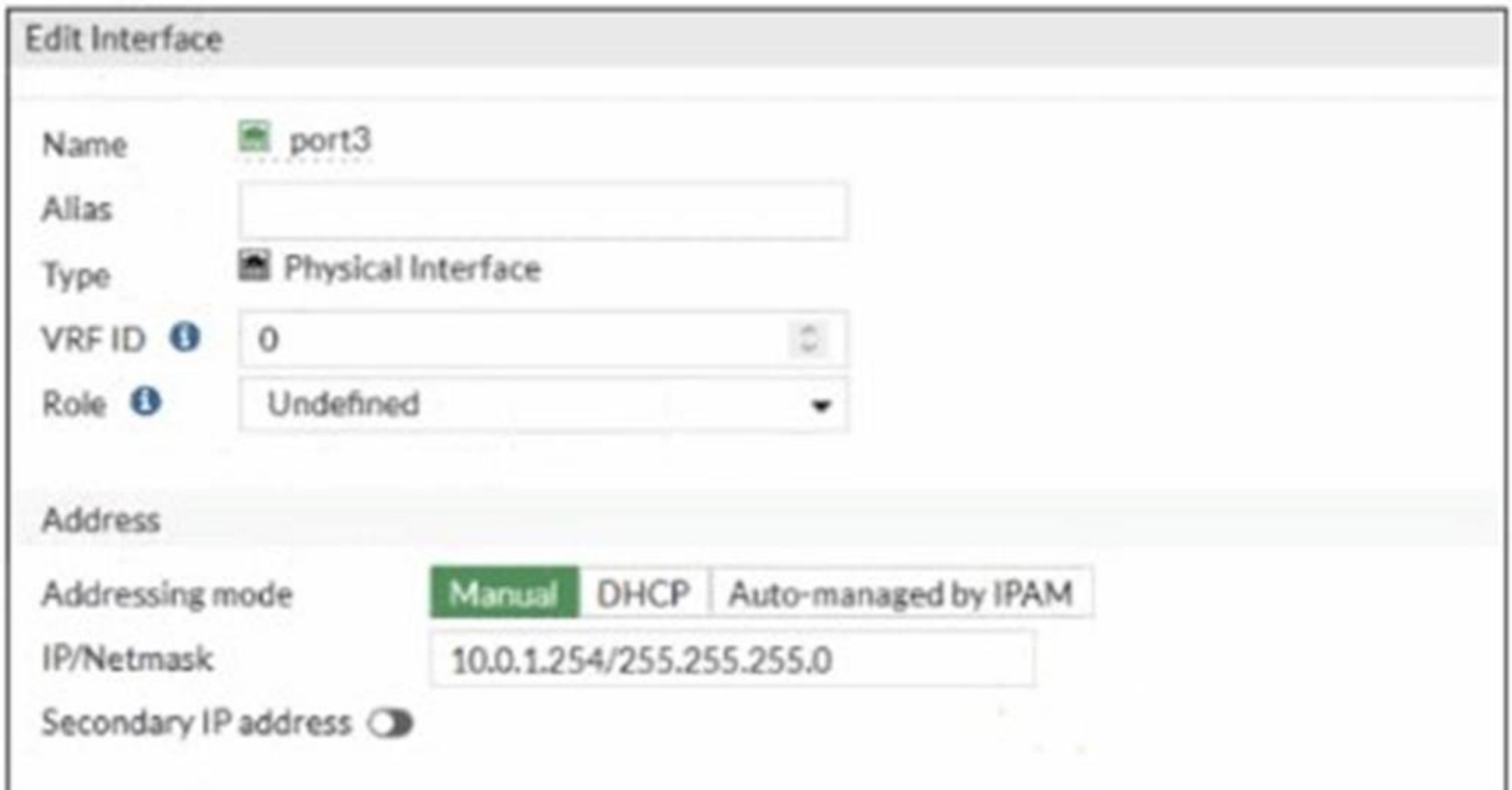
Answer: AD

NEW QUESTION 10
Refer to the exhibits.

FortiGate RSSO configuration



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 10

.....

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