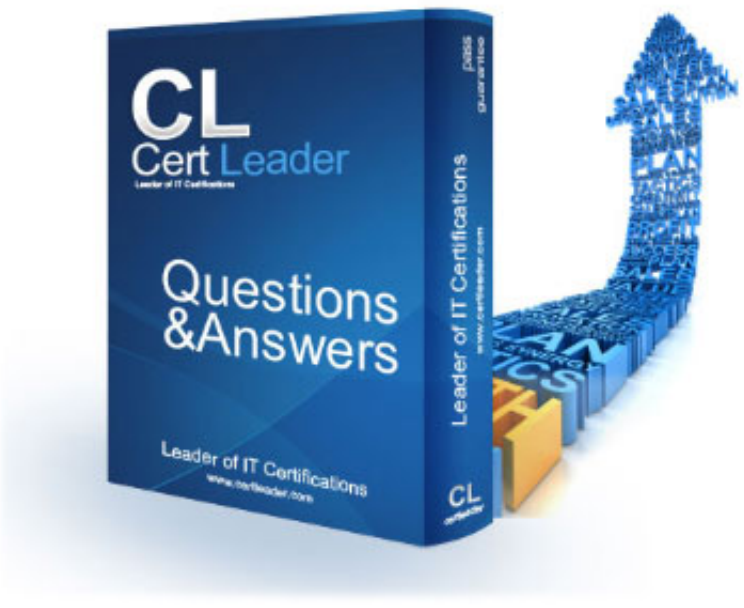
FCSS_LED_AR-7.6 Dumps

FCSS - LAN Edge 7.6 Architect

https://www.certleader.com/FCSS_LED_AR-7.6-dumps.html



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?

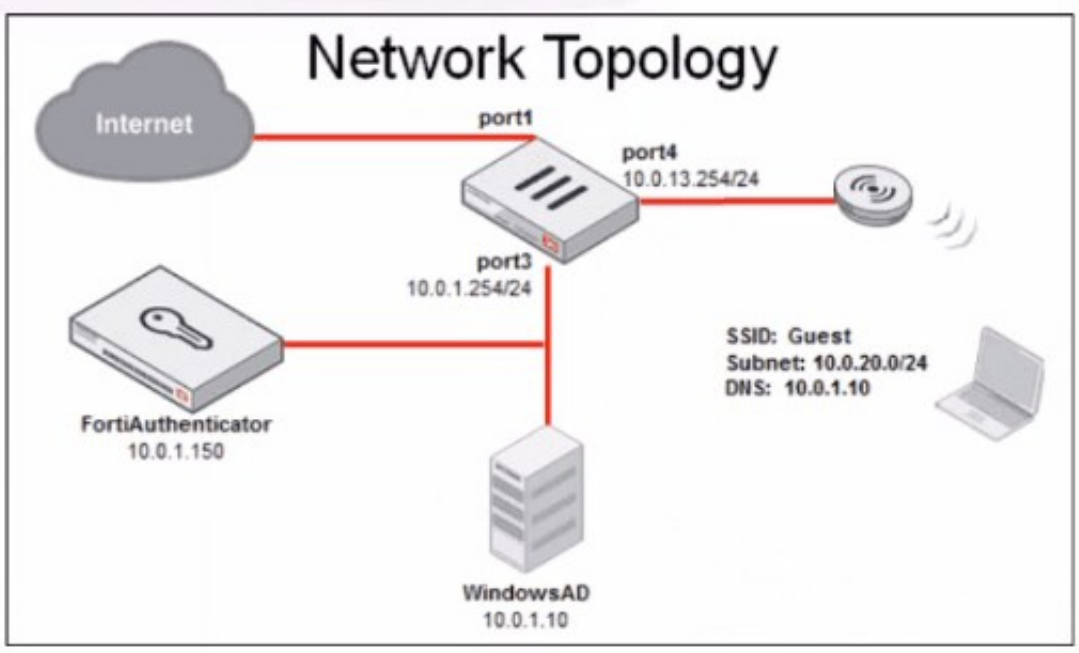
A. Traffic is sent to an access VLAN.

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

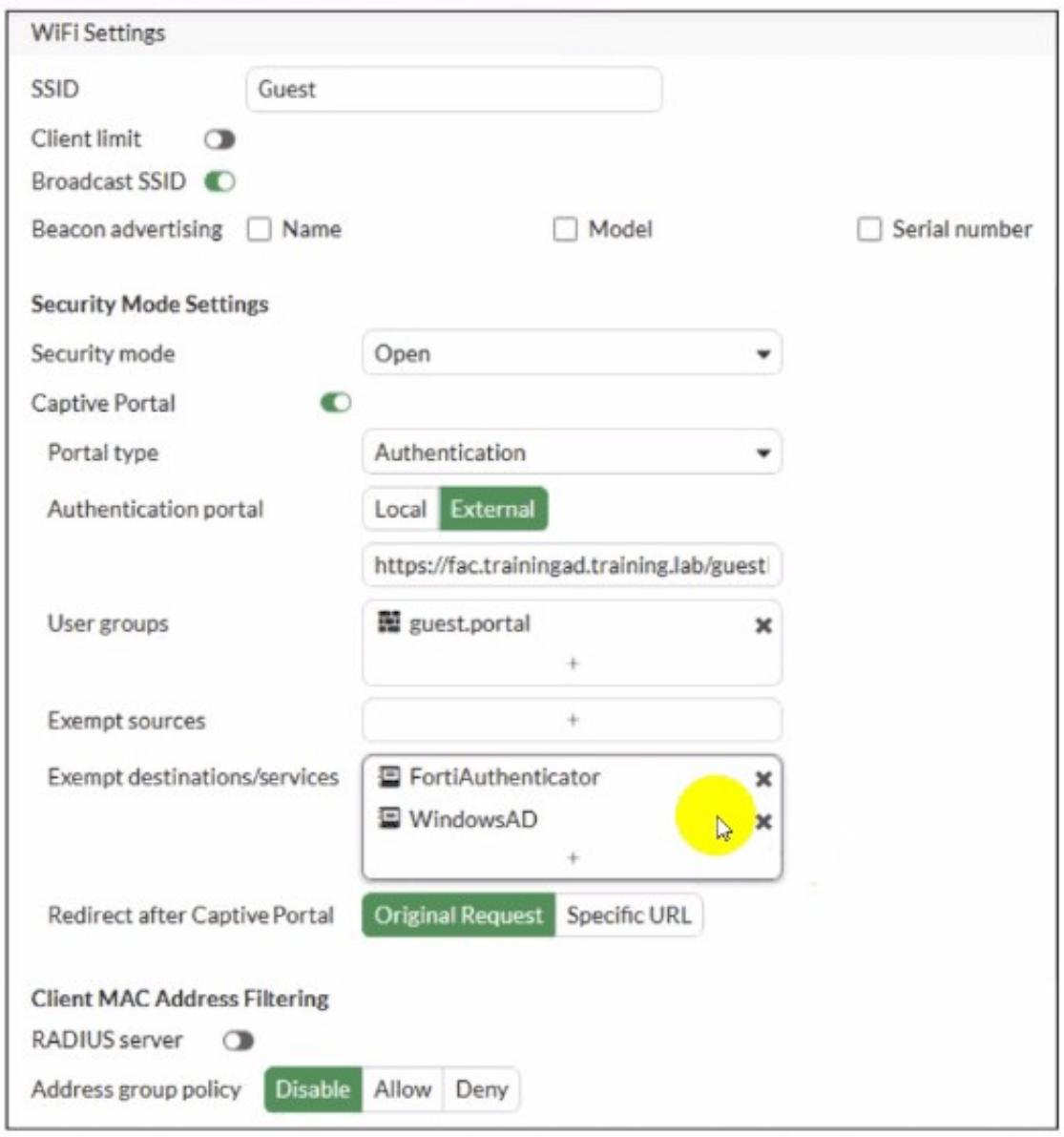
Answer: A

NEW QUESTION 3
Refer to the exhibit.

Network Topology



WiFi settings

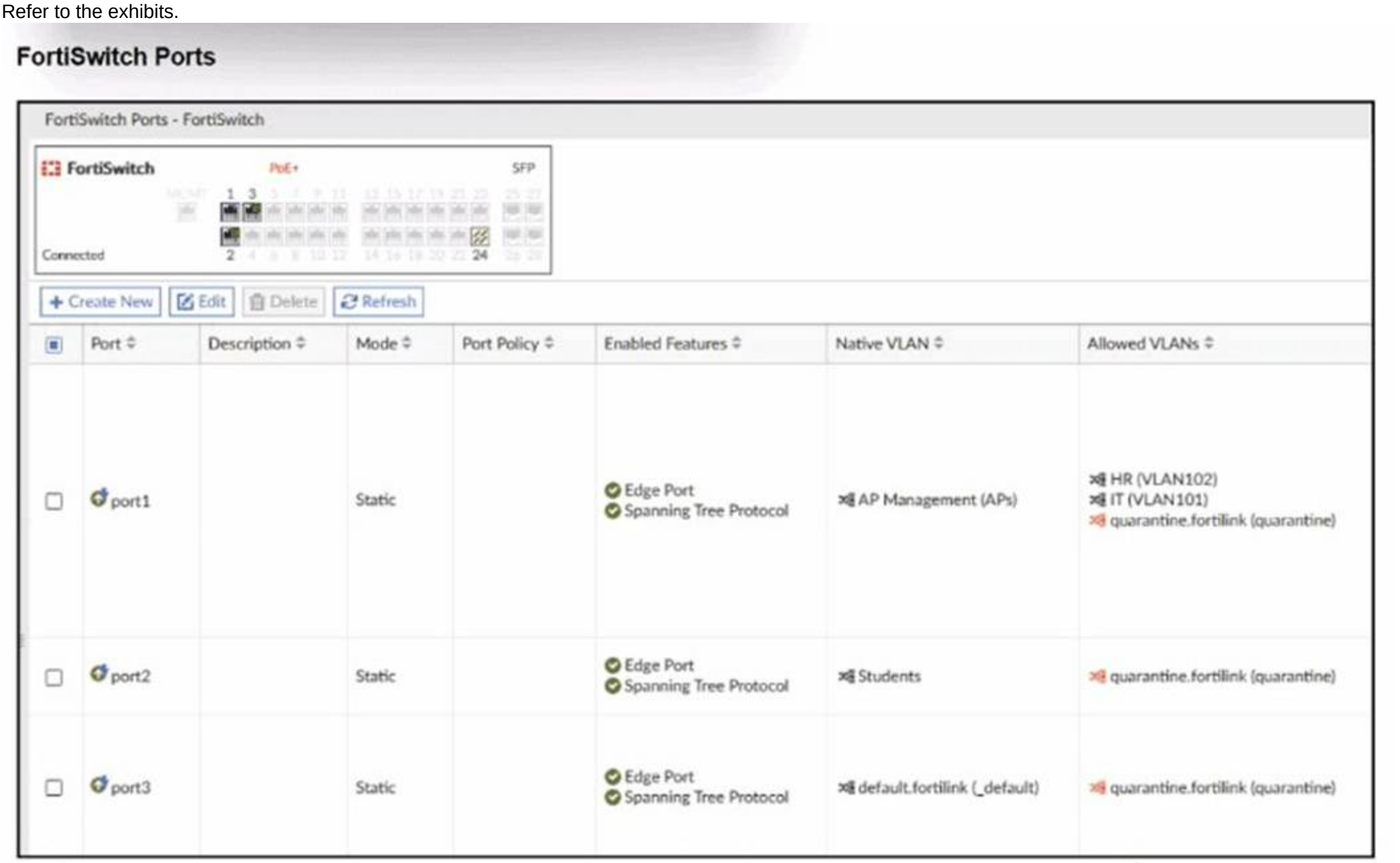


Review the exhibits to analyze the network topology, SSID settings, and firewall policies.
FortiGate is configured to use an external captive portal for authentication to grant access to a wireless network. During testing, it was found that users attempting to connect to the SSID cannot access the captive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

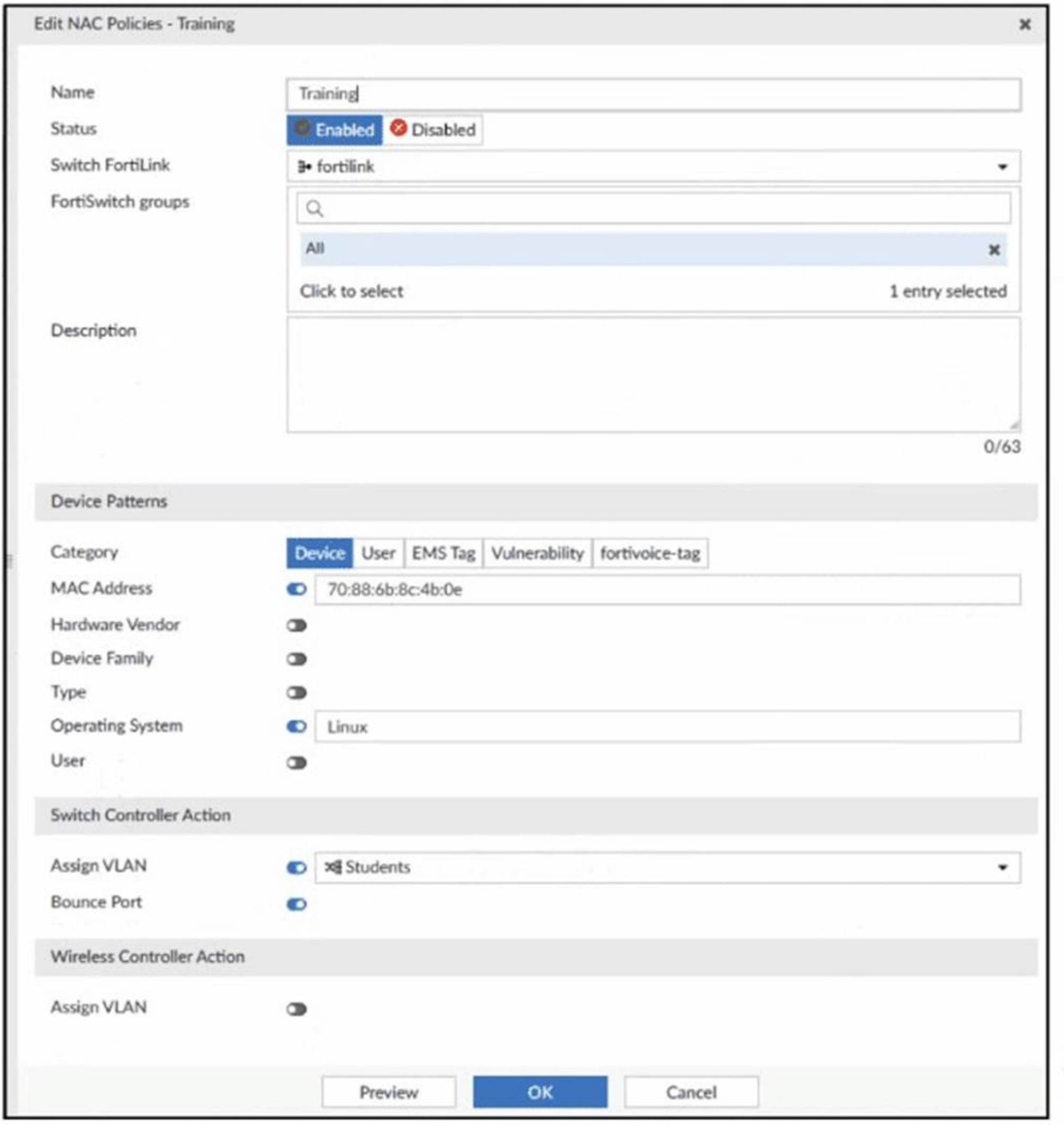
A. Change the SSID security mode to WPA2-Enterprise for authentication.
B. Disable HTTPS redirection for the captive portal authentication page.
C. Exclude FortiAuthenticator and Windows AD address objects from filtering.
D. A firewall policy allowing Guest SSID traffic to reach FortiAuthenticator and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

Answer: D

NEW QUESTION 4
Refer to the exhibits.



NAC policy

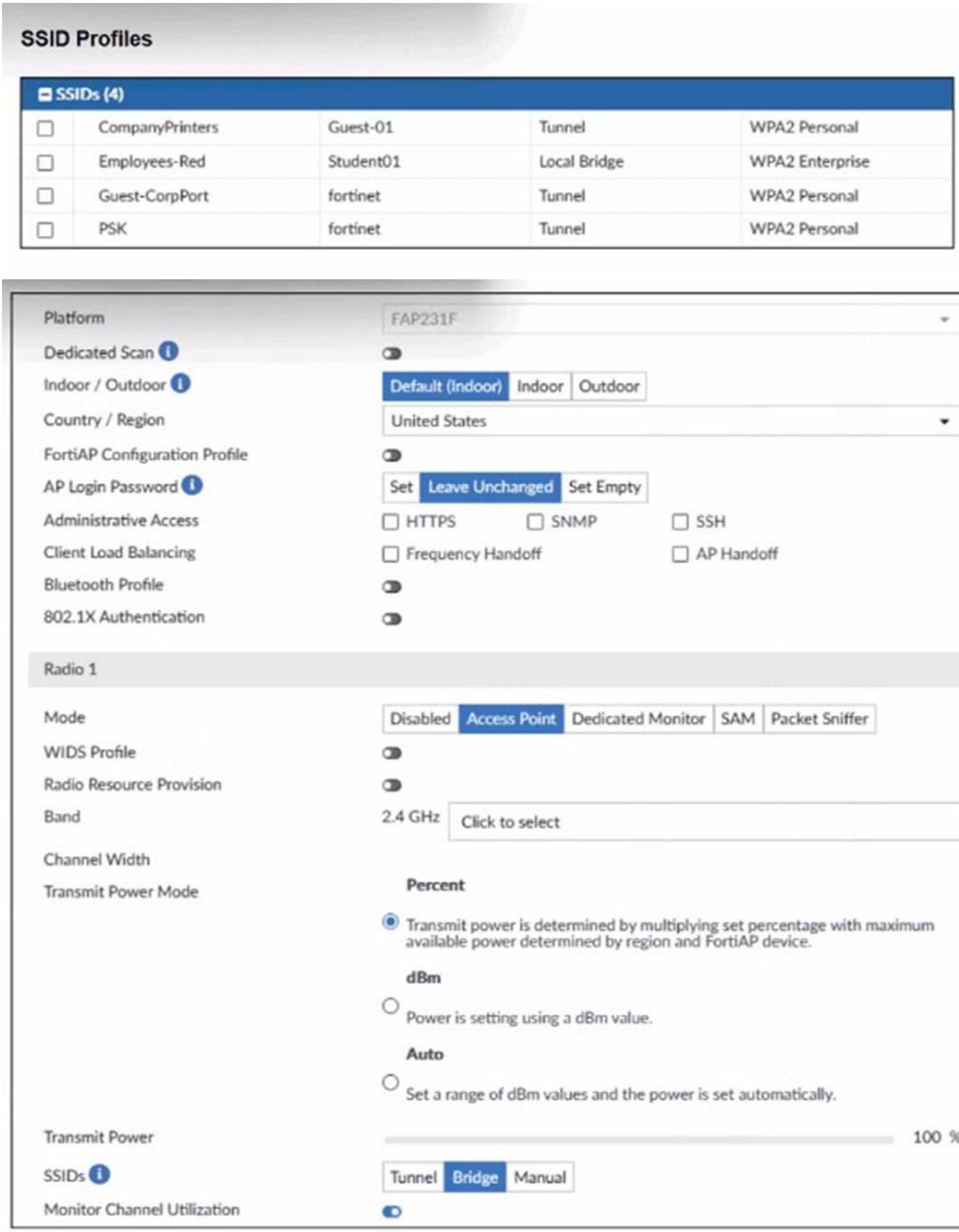


A NAC policy has been configured to apply traffic that flows through FortiSwitch port 2. Traffic that meets the NAC policy criteria will be assigned to the Students VLAN. However, the NAC policy does not seem to be taking effect.
Which configuration is missing?

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 5
Refer to the exhibits.

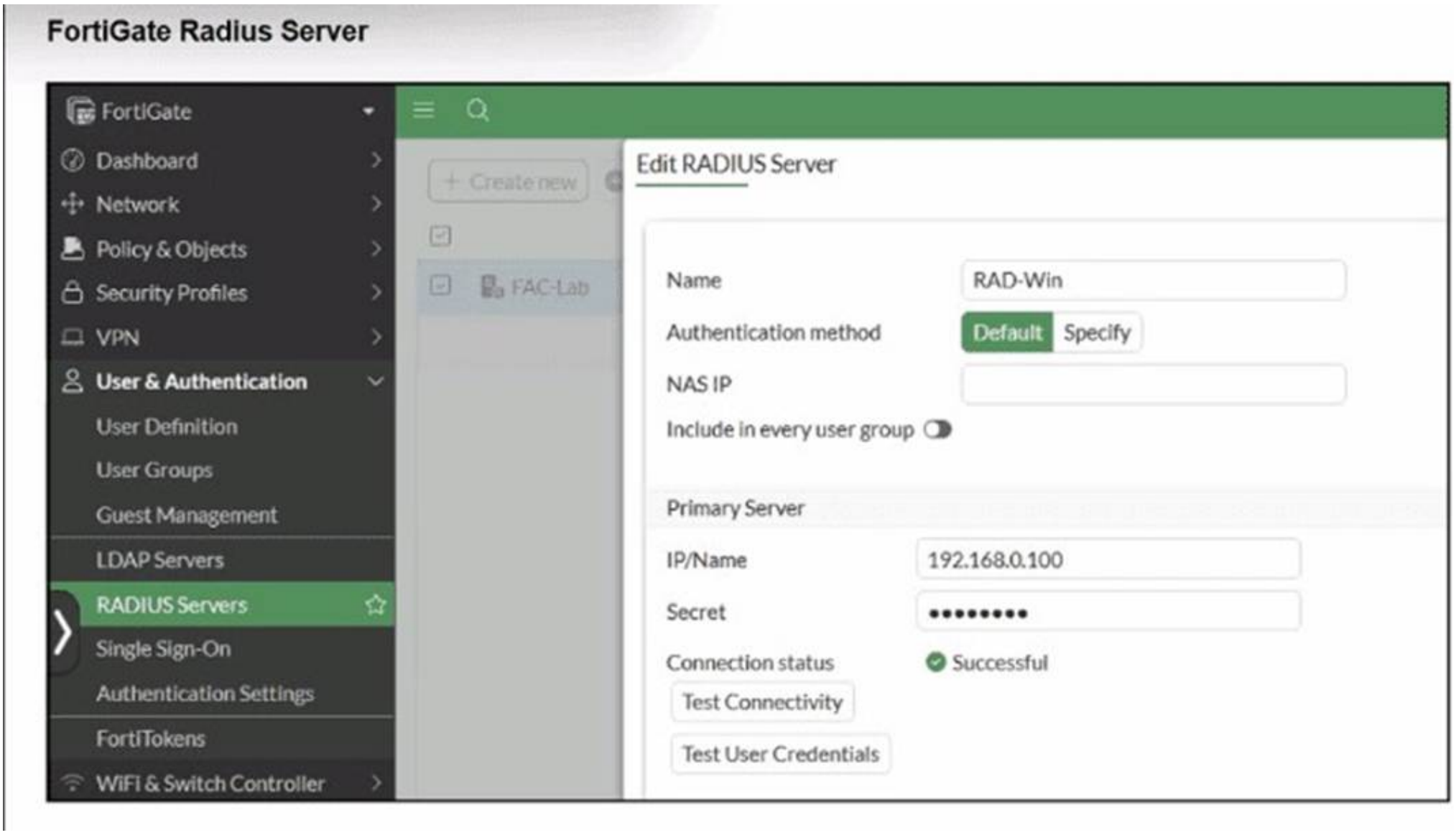


A set of SSID profiles has been configured on FortiManager, and an AP profile has been assigned to a group of AP managed by FortiGate. However, none of the designated SSIDs are being broadcast by these APs.
Which configuration change is required to make the APs broadcast these SSIDs as intended?

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

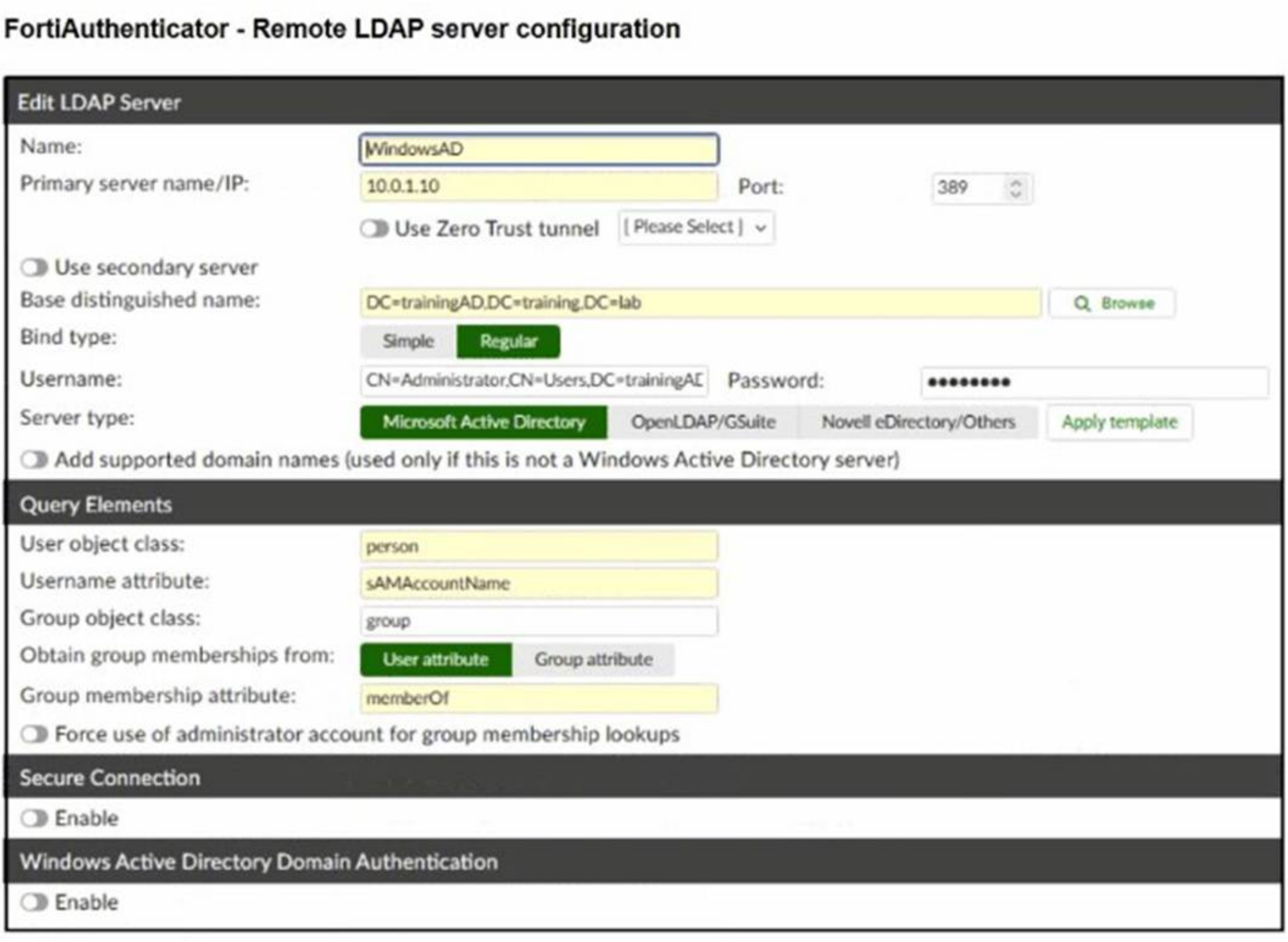
NEW QUESTION 6
Refer to the exhibit.



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
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 0x00000000000000001551027757ddfff7
        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 8
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 9
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 10
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 10
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 13
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 18
What is the primary function of FortiLink NAC in a LAN environment?

A. To extend security policies across FortiGate firewalls only
B. To automate device onboarding and verify security posture
C. To manage FortiSwitch devices and apply manual firewall rules
D. To ensure devices are manually placed in VLANs based on their user roles

Answer: B

NEW QUESTION 23
A network administrator connects a new FortiGate to the network, allowing it to automatically discover andI register with FortiManager.
What occurs after FortiGate retrieves the FortiManager address?

A. FortiGate establishes a secure tunnel to FortiManager over TCP port 541.
B. The device needs to be manually authorized on FortiManager.
C. FortiGate configures its interface settings based on a DHCP response from FortiManager.
D. FortiGate sends a discovery request to all devices on the local network using UDP port 1068.

Answer: A

NEW QUESTION 27
How can FortiAIOps help optimize network performance in an SD-Branch deployment with FortiGate, FortiSwitch, and FortiAP?

A. It disables low-performing APs and switches automatically.
B. It uses Al-driven analytics to identify network issues and provide optimization recommendations.
C. It removes the need for SD-WAN configuration by automating all routing decisions.
D. It predicts and resolves all network issues without any human intervention.

Answer: B

NEW QUESTION 31
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 35
Refer to the exhibits.

VAP configuration

```
config wireless-controller vap
    edit "Corporate"
        set ssid "Corp"
        set security wpa2-only-enterprise
        set auth radius
        set radius-server "FAC-Lab"
        set intra-vap-privacy enable
        set schedule "always"
        set vlan-pooling wtp-group
        config vlan-pool
            edit 101
                set wtp-group "Floor_1"
            next
            edit 102
                set wtp-group "Office"
            next
        end
    next
end
```

Wi-Fi zone table

WiFi SSID 7				
	Corp (Corporate)	WiFi SSID		0.0.0.0/0.0.0.0
	Corp.101	VLAN		0.0.0.0/0.0.0.0
	Corp.102	VLAN		10.0.20.1/255.255.255.0
	wqtn.5.Corporat	VLAN		0.0.0.0/0.0.0.0
	Guest (Guest)	WiFi SSID		0.0.0.0/0.0.0.0
	Student01 (Student01)	WiFi SSID		0.0.0.0/0.0.0.0
Zone 1				
	Corp.zone	Zone	Corp.101 Corp.102	

The exhibits show the VAP configuration. Wi-Fi SSIDs. and zone table.

Which two statements describe how FortiGate handles VLAN assignment for wireless clients? (Choose two.)

A. FortiGate will load balance clients using VLAN 101 and VLAN 102 and assign them an IP address from the 10.0.3.0/24 subnet.
B. All clients connecting to the Corp Zone will receive an IP address from the 10.0.20.0/24 subnet.
C. Clients connecting to APs in the Floor 1 group will not be able to receive an IP address.
D. Clients connecting to APs in the Office group will be assigned to VLAN 102.

Answer: CD

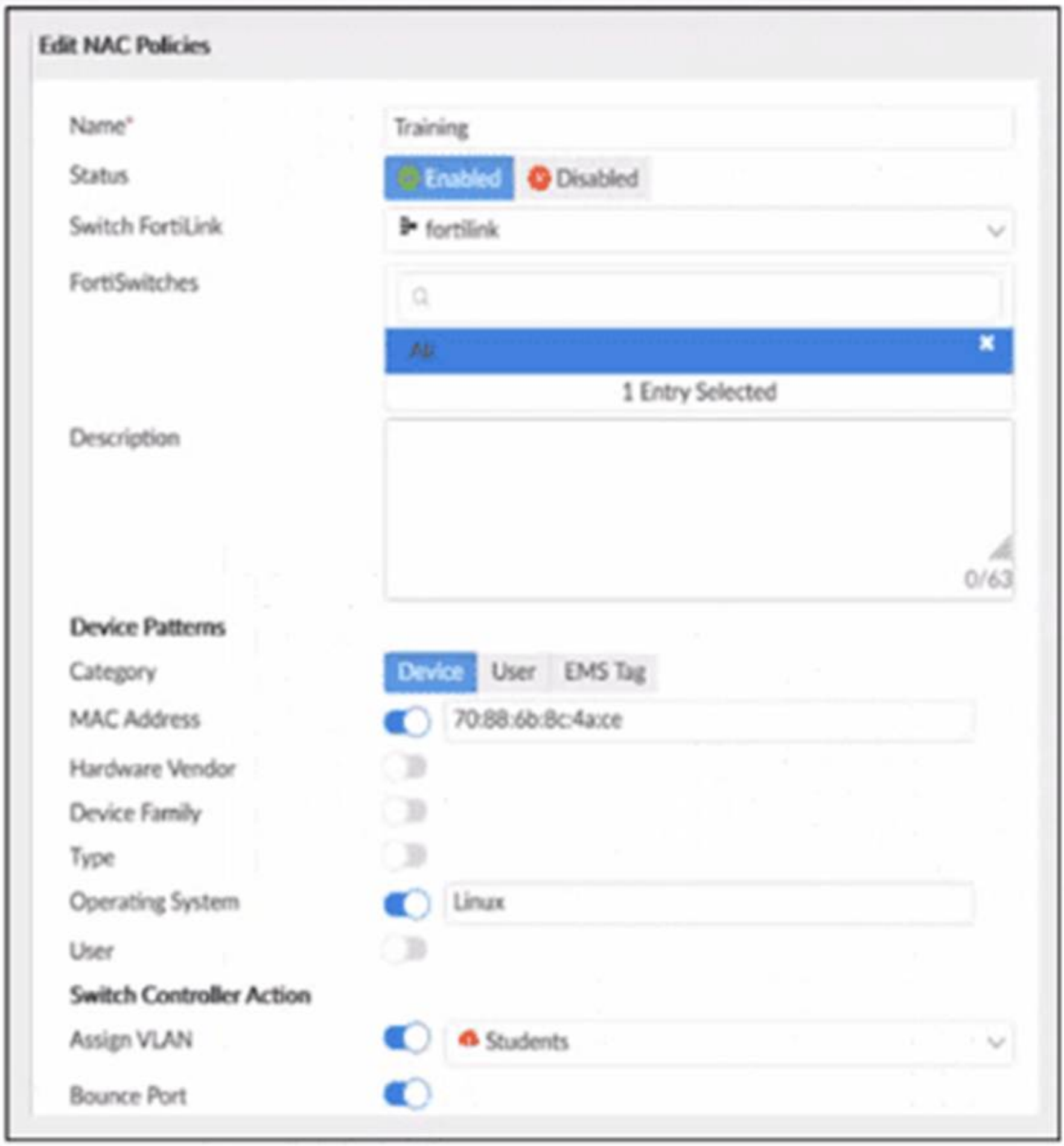
NEW QUESTION 37
When troubleshooting a captive portal issue, which POST parameter in the redirected HTTPS request can be used to track the user's session and ensure that the request is valid?

A. username
B. redir
C. magic
D. email

Answer: C

NEW QUESTION 40
Refer to the exhibits.

FortiManager configuration



FortiGate CLI output

```
FortiGate# diagnose switch-controller switch-info mac-table S224EPTF19005867
vdom: root

Managed Switch : S224EPTF19005867 0

MAC: 00:0c:29:e6:ea:d2 VLAN: 4089 Trunk: GVM1V0000141680(trunk-id 0)
   Flags: 0x000104c1 ( hit trunk dynamic src-hit native )

MAC: 00:0c:29:e6:ea:d2 VLAN: 1 Trunk: GVM1V0000141680(trunk-id 0)
   Flags: 0x000104c1 ( hit trunk dynamic src-hit native I

MAC: 00:0c:29:e6:ea:d2 VLAN: 4093 Trunk: GVM1V0000141680(trunk-id 0)
   Flags: 0x000104c1 ( hit trunk dynamic src-hit native )

MAC: 00:0c:29:e6:ea:d2 VLAN: 4094 Trunk: GVM1V0000141680(trunk-id 0)
   Flags: 0x000104c1 ( hit trunk dynamic src-hit native )

MAC: 70:88:6b:8c:4a:ce VLAN: 4089 Port: port2(port-id 2)
   Flags: 0x00010441 ( hit dynamic src-hit native )

MAC: 04:d5:90:3e:e7:80 VLAN: 1 Port: port1(port-id 1)
   Flags: 0x00010441 ( hit dynamic src-hit native )

MAC: 00:0c:29:06:ea:d2 VLAN: 4088 Trunk: GVM1V0000141680(trunk-id 0)
   Flags: 0x000104c1 ( hit trunk dynamic src-hit native )

MAC: 00:0c:29:e6:ea:d2 VLAN: 10 Trunk:  GVM1V0000141680(trunk-id 0)
   Flags: 0x000104c1 ( hit trunk dynamic src-hit native )

Total Displayed: 8

FortiGate# diagnose switch-controller mac-device nac onboarding
vdom: root
VLAN        MAC                 LAST-SEEN    TYPE    LOCATION
4089        70:88:6b:8c:4a:ce   4            SW      S224EPTF19005867      port2

FortiGate# diagnose switch-controller mac-device nac known
vdom: root
MAC        LAST-KNOWN-SWITCH     LAST-KNOWN-PORT       MATCHED-NAC-POLICY MAC-POLICY-ACTION   FSW-ID  COMMENTS
```

Examine the FortiManager configuration and FortiGate CLI output shown in the exhibit.
The NAC feature is being tested with a device connected to port2 on managed FortiSwitch S224SPTF19005867. The NAC policy has been applied to port2, and traffic was generated from the test device. However, the traffic from the test device does not match the NAC policy and remains in the onboarding VLAN.
What are two possible reasons why the test device is not being correctly classified by the NAC policy? (Choose two.)

A. Device detection is not enabled on VLAN 4089.
B. The device operating system detected by FortiGate is not Linux.
C. Management communication between FortiGate and FortiSwitch is down.
D. The MAC address configured on the NAC policy is incorrect.

Answer: AB

NEW QUESTION 43
Refer to the exhibits.

Network topology

FortiSwitch status

Name	Switch Group	Status	Model
FortiLink: fortilink 1			
FortiSwitch		Offline	FortiSwitch 224E-PO

Fortilink interface settings in FortiGate

```
FortiGate (fortilink) # show
config system interface
    edit "fortilink"
        set vdom "root"
        set fortilink enable
        set ip 10.0.13.254 255.255.255.0
        set allowaccess ping fabric
        set type aggregate
        set member "port4"
        set device-identification enable
        set lldp-reception enable
        set lldp-transmission enable
        set role lan
        set snmp-index 14
        set auto-auth-extension-device enable
        set ip-managed-by-fortiipam disable
        set switch-controller-nac "fortilink"
        set switch-controller-dynamic "fortilink"
        set swc-first-create 255
        set lacp-mode static
    next
end
```

DHCP server setting for fortilink

```
config system dhcp server
    edit 1
        set dns-service default
        set ntp-service local
        set default-gateway 10.0.13.254
        set netmask 255.255.255.0
        set interface "fortilink"
        config ip-range
            edit 1
                set start-ip 10.0.13.1
                set end-ip 10.0.13.253
            next
        end
        set vci-match enable
        set vci-string "FortiExtender"
    next
end
```

You are adding a new FortiSwitch to FortiGate for management. All necessary settings have been configured on FortiGate, but FortiSwitch remains offline. The cabling has been verified and is correctly connected.
Which misconfiguration might be preventing FortiGate from detecting FortiSwitch?

A. The Fortilink interface setting ip-managed-by-fortiipam must be enabled.
B. The Fortilink interface has the wrong interface member.
C. The Fortilink interface setting cype must be physical.
D. The DHCP server setting vci-string is misconfigured.

Answer: D

NEW QUESTION 48
.....

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 FCSS_LED_AR-7.6 Exam with Our Prep Materials Via below:

https://www.certleader.com/FCSS_LED_AR-7.6-dumps.html