



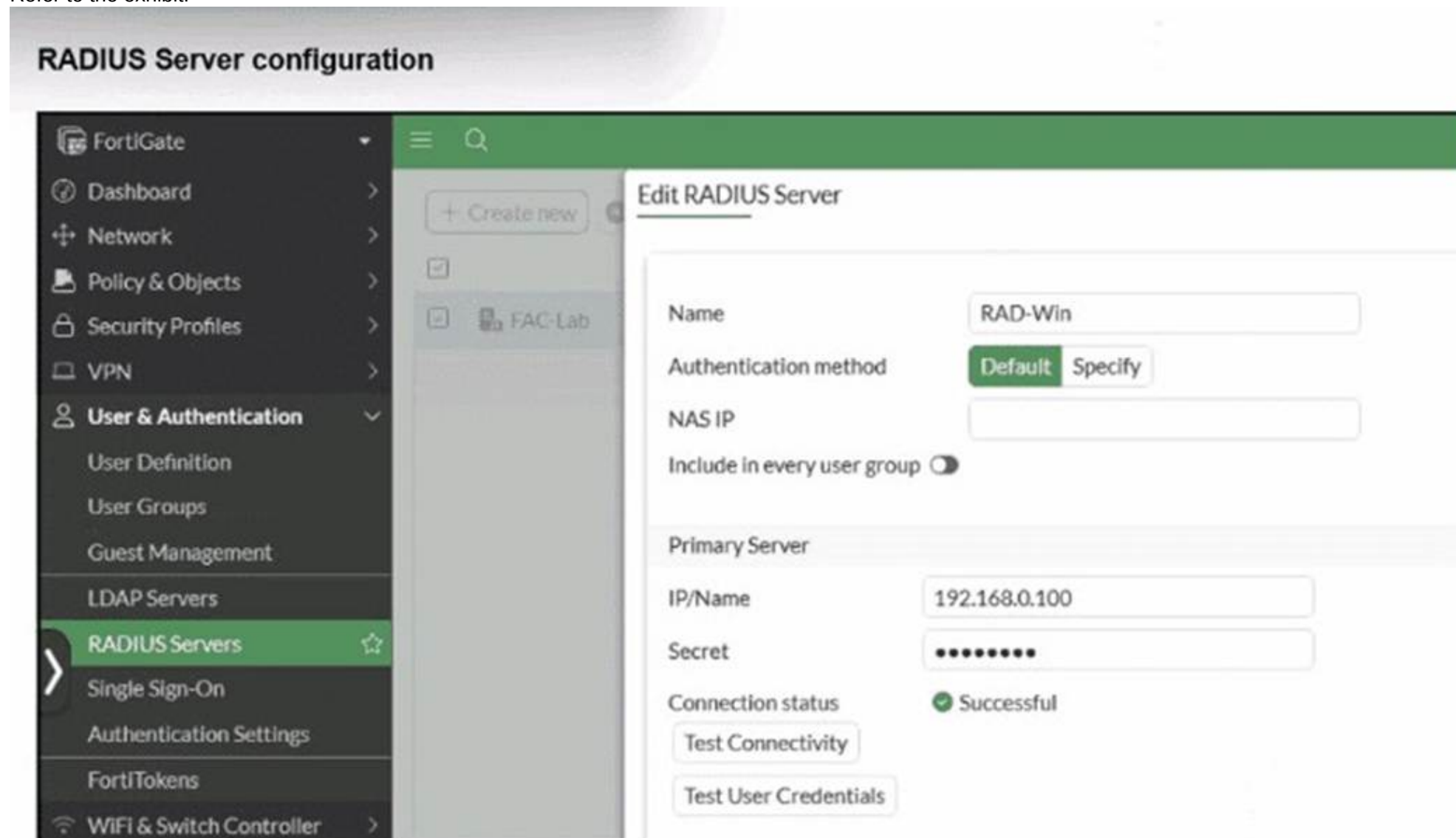
**Fortinet**

## **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-CHAPV2.

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

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. Choose Manual in the SSIDs setting and select the SSIDs to broadcast.
- D. Set the Transmit Power Mode to Auto.

**Answer: C**

#### NEW QUESTION 5

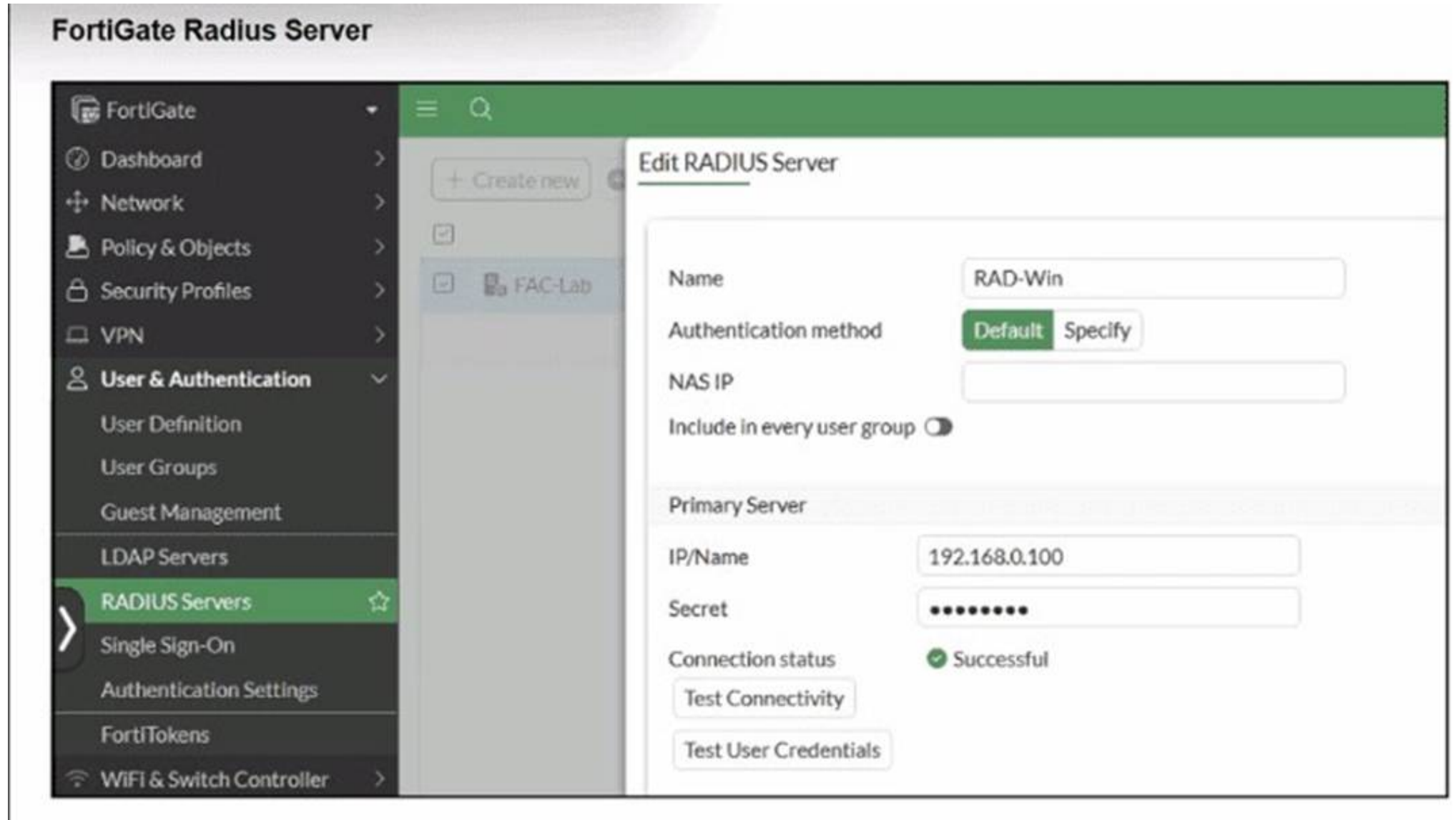
You are troubleshooting a Syslog-based single sign-on (SSO) issue on FortiAuthenticator, where user authentication is not being correctly mapped from the syslog messages. You need a tool to diagnose the issue and understand the logs to resolve it quickly. Which tool in FortiAuthenticator can you use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

Refer to the exhibit.



The screenshot shows the FortiGate Radius Server configuration page. The left sidebar contains the navigation menu with 'RADIUS Servers' highlighted. The main panel is titled 'Edit RADIUS Server' and shows the configuration for a server named 'RAD-Win'. The configuration includes:

- Name: RAD-Win
- Authentication method: Default (selected), Specify
- NAS IP: (empty field)
- Include in every user group: (unchecked)
- Primary Server: (checked)
- IP/Name: 192.168.0.100
- Secret: (masked with dots)
- Connection status: Successful (with a green checkmark)
- Buttons: Test Connectivity, Test User Credentials

#### FortuiGate CLI RADIUS server test

```
FortiGate #
FortiGate # diagnose test authserver radius FAC-Lab pap wifil01 password
authenticate 'wifil01' 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 wifil01 password
authenticate 'wifil01' against 'mschap2' failed, assigned_rad_session_id=19718280638474 session_timeout=0 secs idle_timeout=0 secs!
```

## FortiAuthenticator - Remote LDAP server configuration

Edit LDAP Server

Name:

WindowsAD

Primary server name/IP:

10.0.1.10

Port:

389

☐ Use Zero Trust tunnel

[ Please Select ]

☐ Use secondary server

Base distinguished name:

DC=trainingAD,DC=training,DC=lab

Q Browse

Bind type:

Simple

Regular

Username:

CN=Administrator,CN=Users,DC=trainingAC

Password:

\*\*\*\*\*

Server type:

Microsoft Active Directory

OpenLDAP/GSuite

Novell eDirectory/Others

Apply template

☐ Add supported domain names (used only if this is not a Windows Active Directory server)

Query Elements

User object class:

person

Username attribute:

sAMAccountName

Group object class:

group

Obtain group memberships from:

User attribute

Group attribute

Group membership attribute:

memberOf

☐ Force use of administrator account for group membership lookups

Secure Connection

☐ Enable

Windows Active Directory Domain Authentication

☐ Enable

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

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 8

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 9

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

A conference center wireless network provides guest access through a captive portal, allowing unregistered users to self-register and connect to the network. The IT team has been tasked with updating the existing configuration to enforce captive portal authentication over a secure HTTPS connection. Which two steps should the administrator take to implement this change? (Choose two.)

- A. Enable HTTP redirect in the user authentication settings.
- B. Create a new SSID with the HTTPS captive portal URL.
- C. Disable HTTP administrative access on the guest SSID to enforce HTTPS connection.
- D. Update the captive portal URL to use HTTPS on FortiGate and FortiAuthenticator.

**Answer: AD**

#### 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?

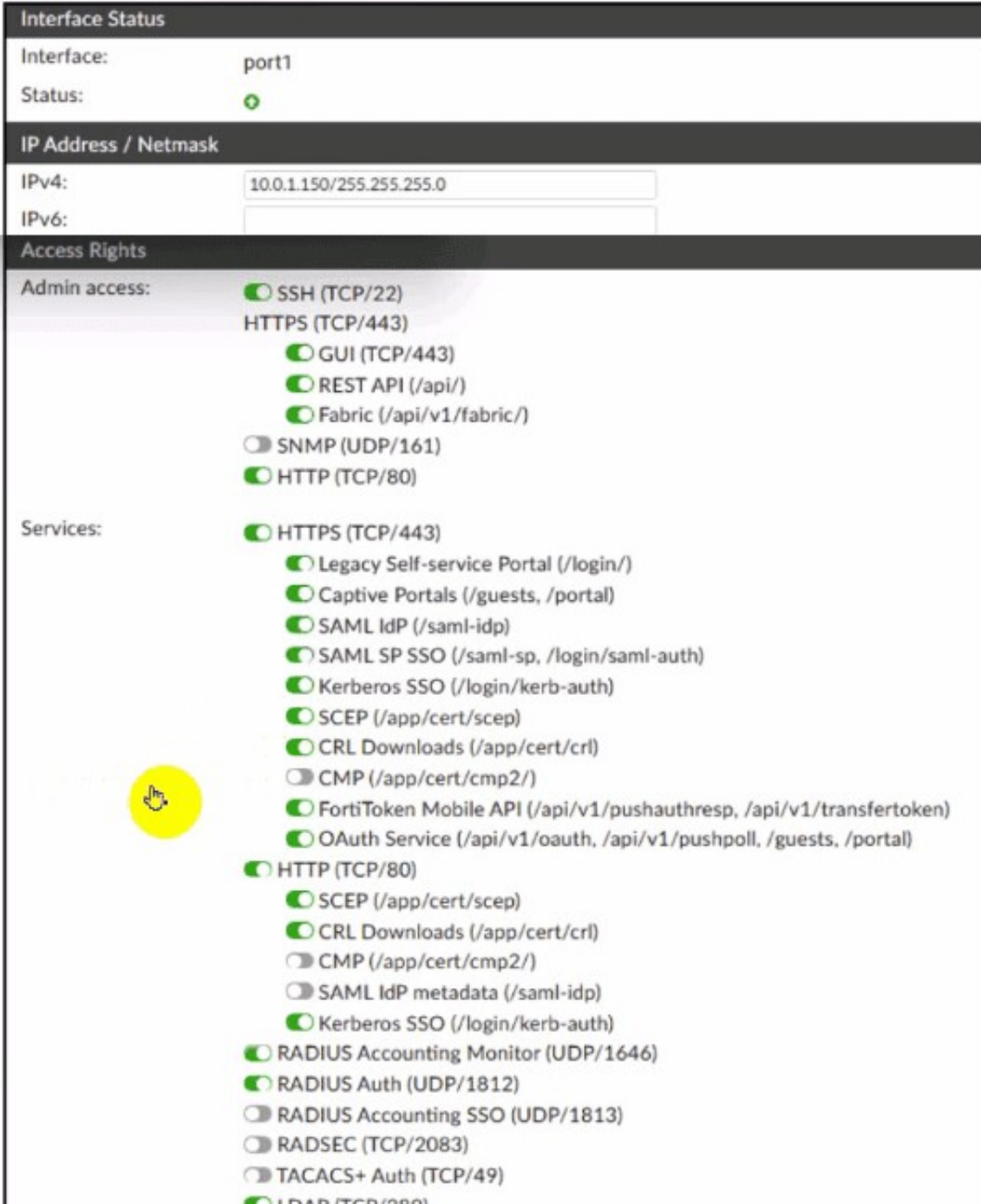
- A. Configure a static route on FortiGate to reach the APs over the IPsec tunnel.
- B. Assign a custom AP profile for the remote APs with the set mpls-connection option enabled.
- C. Decrease the CAPWAP tunnel MTU size for APs to prevent fragmentation.
- D. Upgrade the FortiAP firmware image to ensure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

**Answer: B**

#### NEW QUESTION 11

Refer to the exhibits.

**FortiAuthenticator**



The screenshot displays the FortiAuthenticator configuration interface. The 'Interface Status' section shows 'port1' is up. The 'IP Address / Netmask' section shows IPv4 as 10.0.1.150/255.255.255.0. The 'Access Rights' section is expanded, showing 'Admin access' and 'Services'. A yellow circle highlights the 'Services' section, which lists various protocols and their status (enabled/disabled).

| Section                          | Item                                                                | Status   |
|----------------------------------|---------------------------------------------------------------------|----------|
| Admin access:                    | SSH (TCP/22)                                                        | Enabled  |
|                                  | HTTPS (TCP/443)                                                     | Enabled  |
|                                  | GUI (TCP/443)                                                       | Enabled  |
|                                  | REST API (/api/)                                                    | Enabled  |
|                                  | Fabric (/api/v1/fabric/)                                            | Enabled  |
|                                  | SNMP (UDP/161)                                                      | Disabled |
| Services:                        | HTTP (TCP/80)                                                       | Enabled  |
|                                  | Legacy Self-service Portal (/login/)                                | Enabled  |
|                                  | Captive Portals (/guests, /portal)                                  | Enabled  |
|                                  | SAML IdP (/saml-idp)                                                | Enabled  |
|                                  | SAML SP SSO (/saml-sp, /login/saml-auth)                            | Enabled  |
|                                  | Kerberos SSO (/login/kerb-auth)                                     | Enabled  |
|                                  | SCEP (/app/cert/scep)                                               | Enabled  |
|                                  | CRL Downloads (/app/cert/crl)                                       | Enabled  |
|                                  | CMP (/app/cert/cmp2/)                                               | Disabled |
|                                  | FortiToken Mobile API (/api/v1/pushauthresp, /api/v1/transfertoken) | Enabled  |
|                                  | OAuth Service (/api/v1/oauth, /api/v1/pushpoll, /guests, /portal)   | Enabled  |
|                                  | HTTP (TCP/80)                                                       | Enabled  |
|                                  | SCEP (/app/cert/scep)                                               | Enabled  |
|                                  | CRL Downloads (/app/cert/crl)                                       | Enabled  |
|                                  | CMP (/app/cert/cmp2/)                                               | Disabled |
|                                  | SAML IdP metadata (/saml-idp)                                       | Disabled |
|                                  | Kerberos SSO (/login/kerb-auth)                                     | Enabled  |
|                                  | RADIUS Accounting Monitor (UDP/1646)                                | Enabled  |
| RADIUS Auth (UDP/1812)           | Enabled                                                             |          |
| RADIUS Accounting SSO (UDP/1813) | Disabled                                                            |          |
| RADSEC (TCP/2083)                | Disabled                                                            |          |
| TACACS+ Auth (TCP/49)            | Disabled                                                            |          |
| LDAP (TCP/389)                   | Enabled                                                             |          |

FortiAuthenticator SSO Methods

Edit Fortinet Single Sign-On Methods

Maximum concurrent user sessions:

0

Fine-grained control

☒ Windows event log polling (e.g. domain controllers/Exchange servers)

Configure Events

☒ DNS lookup to get IP from workstation name

☐ Directly use domain DNS suffix in lookup

☒ Reverse DNS lookup to get workstation name from IP

☐ Do one more DNS lookup to get full list of IPs after reverse lookup of workstation name

☐ Include account name ending with \$ (usually computer account)

☐ FortiNAC SSO

FortiNAC sources

☒ RADIUS Accounting SSO clients

☒ Syslog SSO

Syslog sources

☐ Allow TLS encryption

☐ FortiClient SSO Mobility Agent Service

☐ Hierarchical FSSO tiering

☐ DC/TS Agent Clients

FortiAuthenticator RADIUS Accounting SS Client

Edit RADIUS Accounting SSO Client

Name:

RADIUS-SSO

Client name/IP:

10.0.1.10

Secret:

\*\*\*\*\*

Description:

SSO user type:

☐ External ⓘ

☐ Local users ⓘ

☒ Remote users ⓘ

WindowsAD (10.0.1.10) ▾

☒ Strip off prefix or suffix from username if any

☐ Use a different attribute to search for the user in the remote LDAP server (instead of the username attribute specified in the remote LDAP server settings)

☐ Use the prefix or suffix supplied in the username as the domain (instead of the domain specified in the remote LDAP server settings)

RADIUS Attributes

Username attribute:

User-Name

Browse

Default

Client IPv4 attribute:

Framed-IP-Address

Browse

Default

Client IPv6 attribute:

Framed-IPv6-Address

Browse

Default

User group attribute:

Fortinet-Group-Name

Browse

Default

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 16

How can FortiAI Ops 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 AI-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 18**

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 19**

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              |                          |                        |           |                         |
|--------------------------|--------------------------|------------------------|-----------|-------------------------|
| <input type="checkbox"/> | <input type="checkbox"/> | (i-i) Corp (Corporate) | WiFi SSID | 0.0.0.0/0.0.0.0         |
| <input type="checkbox"/> | <input type="checkbox"/> | Corp.101               | VLAN      | 0.0.0.0/0.0.0.0         |
| <input type="checkbox"/> | <input type="checkbox"/> | Corp.102               | VLAN      | 10.0.20.1/255.255.255.0 |
| <input type="checkbox"/> | <input type="checkbox"/> | wqtn.5.Corporat        | VLAN      | 0.0.0.0/0.0.0.0         |
| <input type="checkbox"/> | <input type="checkbox"/> | (i-i) Guest (Guest)    | WiFi SSID | 0.0.0.0/0.0.0.0         |
| <input type="checkbox"/> | <input type="checkbox"/> | Student01 (Student01)  | WiFi SSID | 0.0.0.0/0.0.0.0         |
| Zone 1                   |                          |                        |           |                         |
| <input type="checkbox"/> | <input type="checkbox"/> | Corp.zone              | Zone      | Corp.101<br>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 20

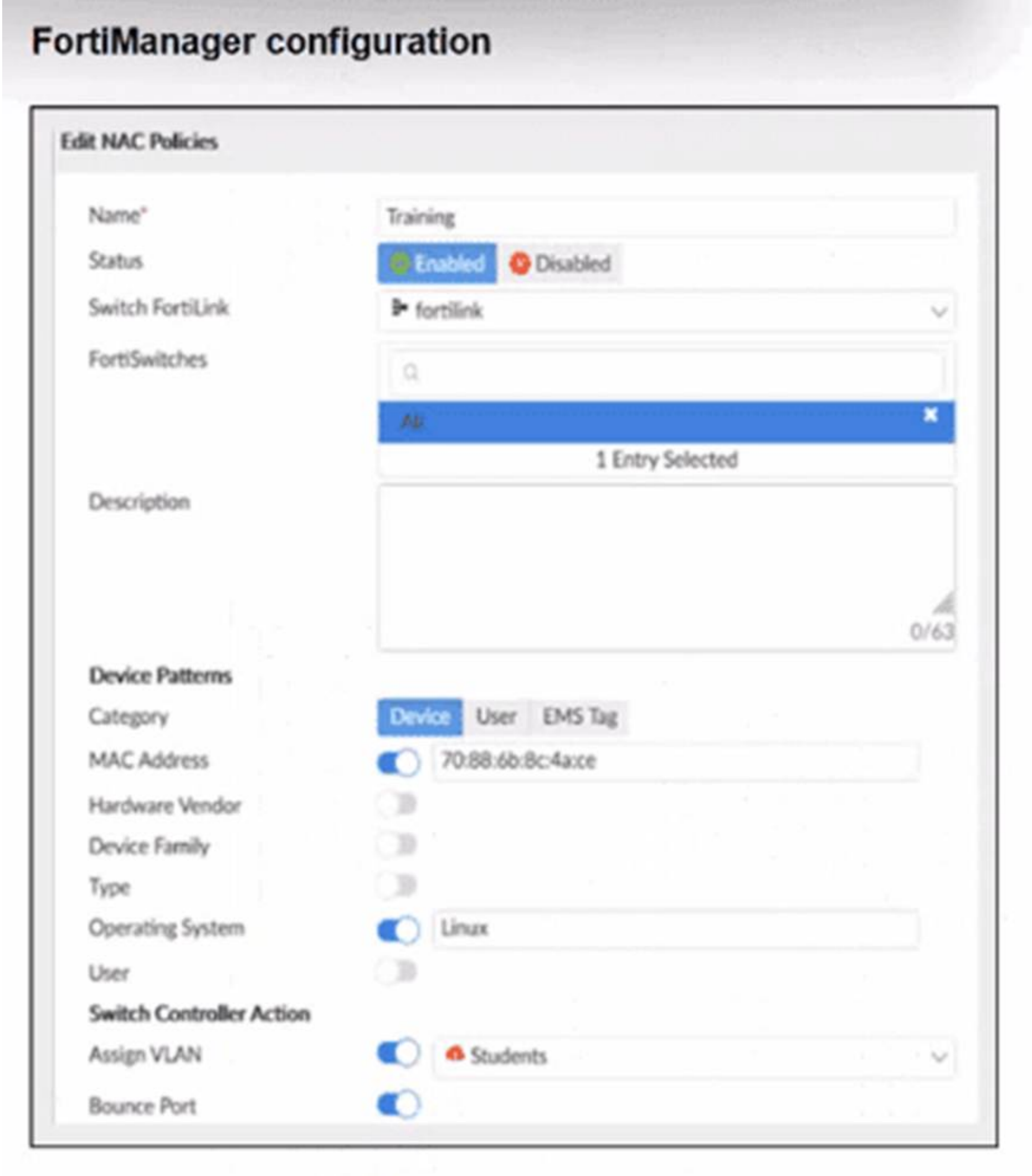
When troubleshooting a captive portal issue, which POST parameter in the redirected HTTPS request can be used to track the user's session and ensure that the request is valid?

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

Answer: C

NEW QUESTION 23

Refer to the exhibits.



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: GVM1V00000141680(trunk-id 0)
  Flags: 0x000104c1 ( hit trunk dynamic src-hit native )

MAC: 00:0c:29:e6:ea:d2 VLAN: 1 Trunk: GVM1V00000141680(trunk-id 0)
  Flags: 0x000104c1 ( hit trunk dynamic src-hit native I

MAC: 00:0c:29:e6:ea:d2 VLAN: 4093 Trunk: GVM1V00000141680(trunk-id 0)
  Flags: 0x000104c1 ( hit trunk dynamic src-hit native )

MAC: 00:0c:29:e6:ea:d2 VLAN: 4094 Trunk: GVM1V00000141680(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: GVM1V00000141680(trunk-id 0)
  Flags: 0x000104c1 ( hit trunk dynamic src-hit native )

MAC: 00:0c:29:e6:ea:d2 VLAN: 10 Trunk: GVM1V00000141680(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 28

.....

## 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

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The FCSS\\_LED\\_AR-7.6 Practice Test Here](#)**