# Fortinet

## Exam Questions FCSS_LED_AR-7.6

FCSS - LAN Edge 7.6 Architect

# About Exambible

***Your Partner of IT Exam***

# Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

# Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

**NEW QUESTION 1**
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

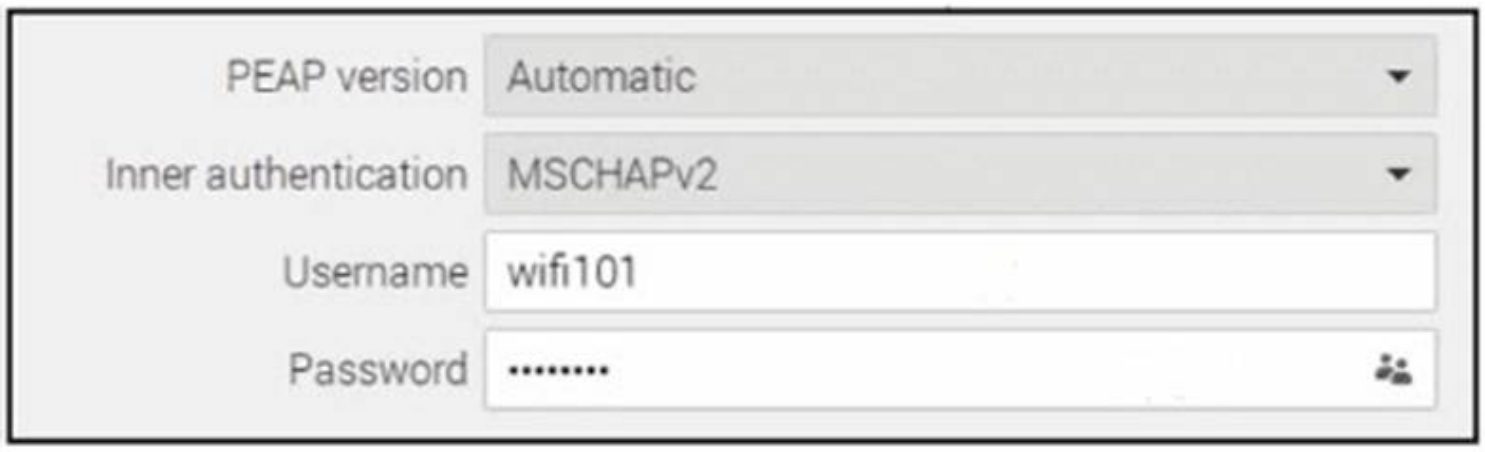
**NEW QUESTION 2**
Refer to the exhibits.

**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 3**
A network engineer is deploying FortiGate devices using zero-touch provisioning (ZTP). The devices must automatically connect to FortiManager and receive their configurations upon first boot. However, after powering on the devices, they fail to register with FortiManager.
What could be a possible cause of this issue?

A. The FortiGate device requires manual intervention to accept the FortiManager connection.
B. In this scenario, the ZTP process works only when devices are connected using a console cable.
C. The FortiGate device must be preloaded with a configuration file before ZTP can function.
D. The FortiManager IP address is not reachable over TCP port 541.

**Answer:** D

**NEW QUESTION 4**
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. IoT 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 5**
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 6**
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 7**
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<br>Corp.102 | |

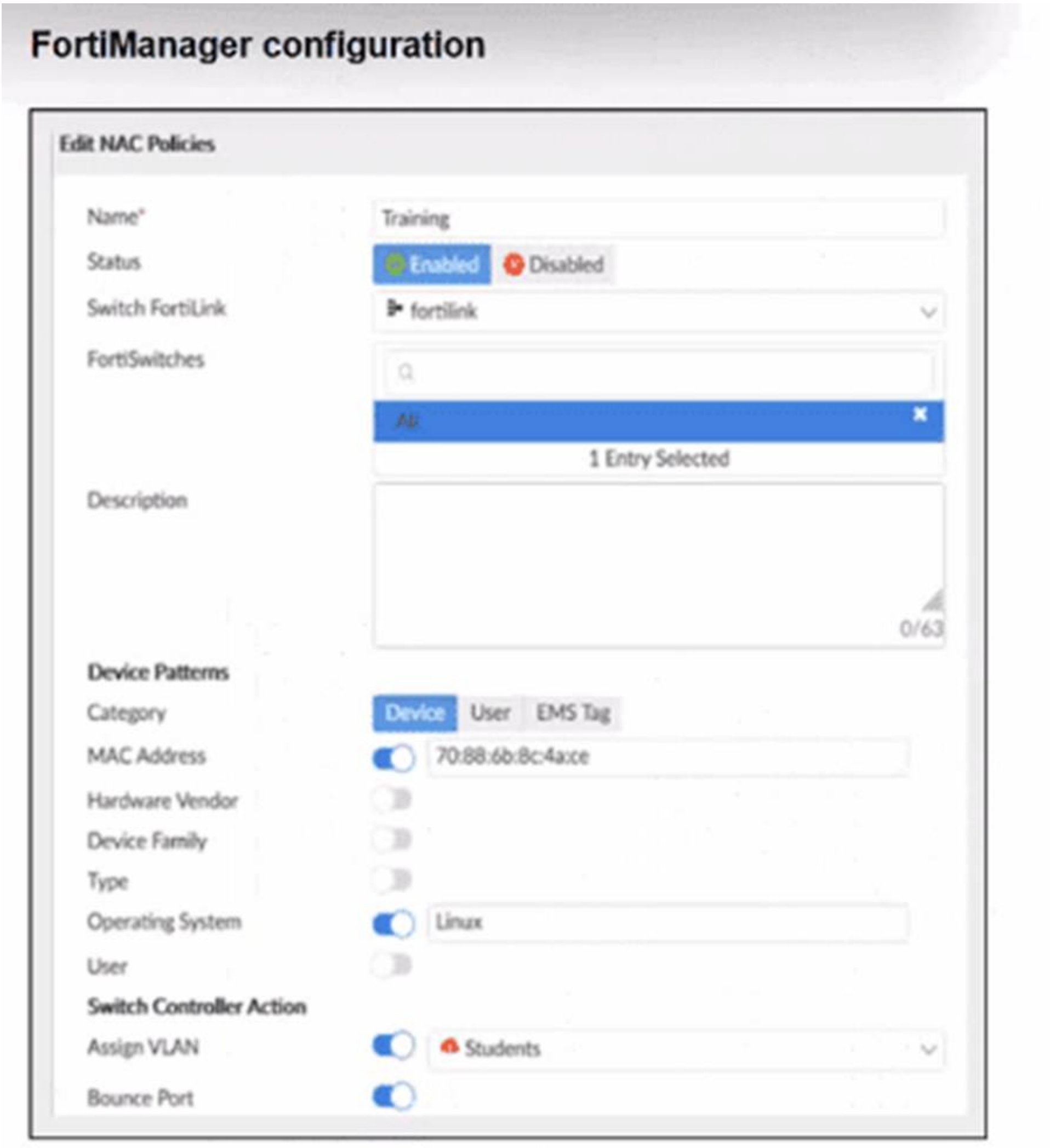
The exhibits show the VAP configuration. Wi-Fi SSIDs. and zone table.
Which two statements describe how FortiGate handles VLAN assignment for wireless clients? (Choose two.)

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 8**
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: 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 9**
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?

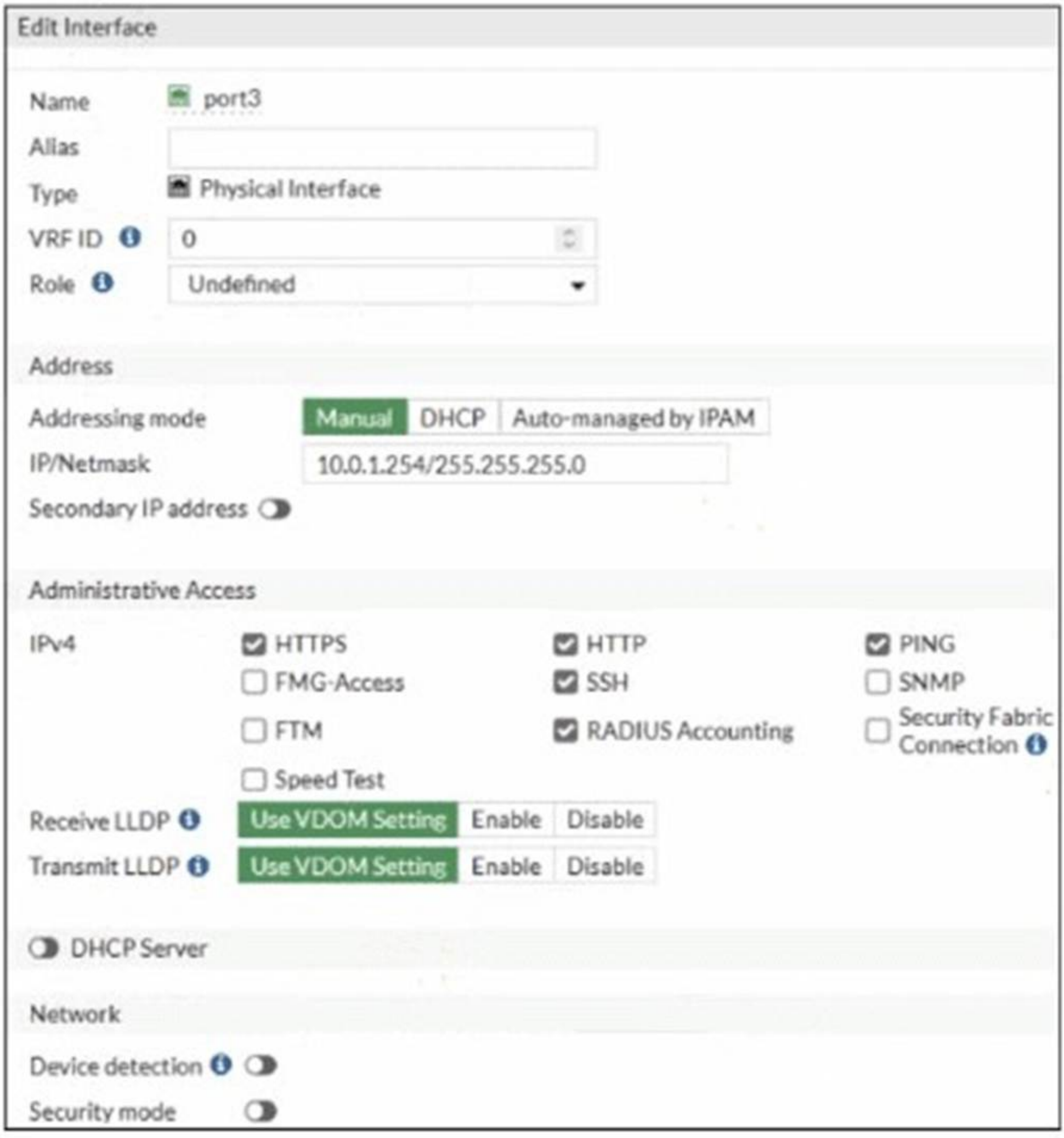
A. The Fortilink interface setting ip-managed-by-fortiipam must be enabled.
B. The Fortilink interface has the wrong interface member.
C. The Fortilink interface setting cype must be physical.
D. The DHCP server setting vci-string is misconfigured.

**Answer:** D

**NEW QUESTION 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**

.....

# Relate Links

**100% Pass Your FCSS_LED_AR-7.6 Exam with Exambible Prep Materials**

https://www.exambible.com/FCSS_LED_AR-7.6-exam/

# Contact us

**We are proud of our high-quality customer service, which serves you around the clock 24/7.**

**Viste -** https://www.exambible.com/