



# NSE7\_SAC-6.2<sup>Q&As</sup>

Fortinet NSE 7 - Secure Access 6.2

## Pass Fortinet NSE7\_SAC-6.2 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

[https://www.passapply.com/nse7\\_sac-6-2.html](https://www.passapply.com/nse7_sac-6-2.html)

100% Passing Guarantee  
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet  
Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers





### QUESTION 1

Examine the sections of the configuration shown in the following output:

```
config vpn certificate setting
  set oosp-status enable
  set oosp-default-server "FAC"
  set strict-oosp-check disable
end
config vpn certificate oosp-server
  edit "FAC"
    set url "http://10.0.1.150:2560"
    set unavail-action revoke
  next
end
config vpn ssl settings
  set ssl-oosp-option certificate
end
```

What action will the FortiGate take when using OCSP certificate validation?

- A. FortiGate will reject the certificate if the OCSP server replies that the certificate is unknown.
- B. FortiGate will use the OCSP server 10.0.1.150 even when the OCSP URL field in the user certificate contains a different OCSP server IP address.
- C. FortiGate will use the OCSP server 10.0.1.150 even when there is a different OCSP IP address in the oosp-override-serveroption under config user peer.
- D. FortiGate will invalidate the certificate if the OSCP server is unavailable.

Correct Answer: D

---

### QUESTION 2

Refer to the exhibit.



```
FortiGate # diagnose switch-controller switch-info 802.1X
Managed Switch : S224EPTF18001736
```

```
port2 : Mode: port-based (mac-by-pass disable)
Link: Link up
Port State: unauthorized: ( )
Dynamic Authorized Vlan : 0
EAP pass-through mode : Enable
Quarantine VLAN (4093) detection : Enable
Native Vlan : 10
Allowed Vlan list: 10,4093
Untagged Vlan list: 4093
Guest VLAN :
Auth-Fail Vlan :

Sessions info:
00:09:0f:02:02:02      Type=802.1x,,state=AUTHENTICATING,etime=0,eap_cnt=0 params:reAuth=3600
```

A host machine connected to port2 on FortiSwitch cannot connect to the network. All ports on FortiSwitch are assigned a security policy to enforce 802.1X port authentication. While troubleshooting the issue, the administrator runs the debug command and obtains the output shown in the exhibit.

Which two scenarios are the likely cause of this issue? (Choose two.)

- A. The host machine is not configured for 802.1X port authentication.
- B. The host machine does not support 802.1X authentication.
- C. The host machine is quarantined due to a security incident.
- D. The host machine is configured with wrong VLAN ID.

Correct Answer: AB

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD46428>

### QUESTION 3

What does DHCP snooping MAC verification do?

- A. Drops DHCP release packets on untrusted ports
- B. Drops DHCP packets with no relay agent information (option 82) on untrusted ports
- C. Drops DHCP offer packets on untrusted ports
- D. Drops DHCP packets on untrusted ports when the client hardware address does not match the source MAC address

Correct Answer: D

Reference: <https://docs.fortinet.com/document/fortiswitch/6.4.2/administration-guide/335964/dhcpsnooping> (note)

### QUESTION 4

Default VLANs are created on FortiGate when the FortiLink interface is created. By default, which VLAN is set as



Allowed VLANs on all FortiSwitch ports?

- A. Sniffer VLAN
- B. Camera VLAN
- C. Quarantine VLAN
- D. Voice VLAN

Correct Answer: A

---

#### QUESTION 5

An administrator is deploying APs that are connecting over an IPsec network. All APs have been configured to connect to FortiGate manually. FortiGate can discover the APs and authorize them. However, FortiGate is unable to establish CAPWAP tunnels to manage the APs.

Which configuration setting can the administrator perform to resolve the problem?

- A. Decrease the CAPWAP tunnel MTU size for APs to prevent fragmentation.
- B. Enable CAPWAP administrative access on the IPsec interface.
- C. Upgrade the FortiAP firmware image to ensure compatibility with the FortiOS version.
- D. Assign a custom AP profile for the remote APs with the set mpls-connectionoption enabled.

Correct Answer: B

[NSE7\\_SAC-6.2 VCE Dumps](#)

[NSE7\\_SAC-6.2 Study Guide](#)

[NSE7\\_SAC-6.2 Exam Questions](#)