



NSE7_SAC-6.2^{Q&As}

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

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

Refer to the exhibits.

```
config wireless-controller vap
  edit "Corp"
    set vdom "root"
    set ssid "Corp"
    set security wpa2-only-enterprise
    set auth radius
    set radius-server "FAC-Lab"
    set intra-vap-privacy enabled
    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
```

Examine the VAP configuration and the WiFi zones table shown in the exhibits.

WiFi (1)					
		Corp ((W)) SSID: Corp)	10.0.3.1 255.255.255.0	WiFi SSID	3
Zone (3)					
		Corp.zone		Zone	0
		Corp.101	0.0.0.0 0.0.0.0	VLAN	1 101
		Corp.102	10.0.20.1 255.255.255.0	VLAN	2 102

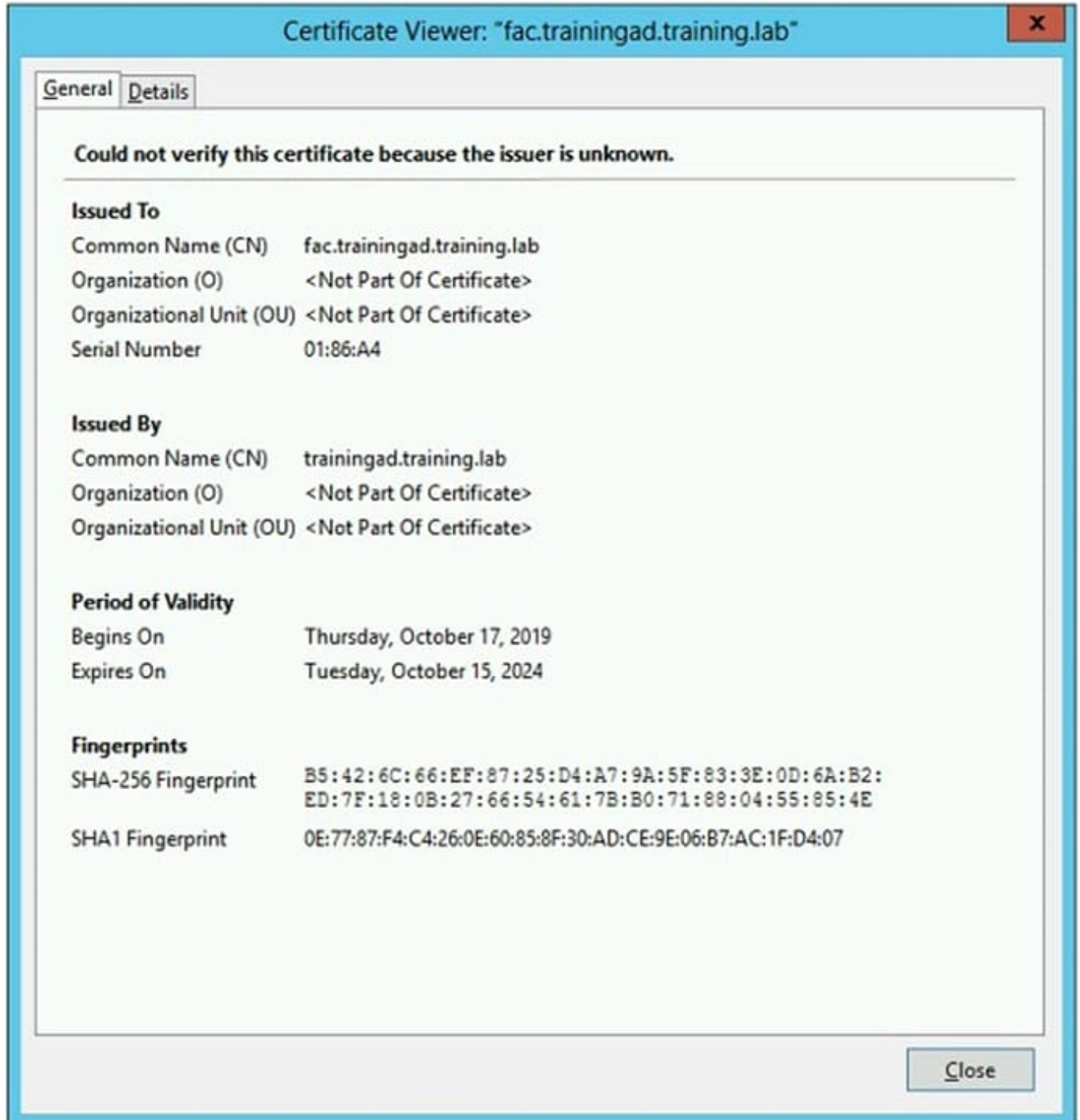
Which two statements describe FortiGate behavior regarding assignment of VLANs to wireless clients? (Choose two.)

- 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. Clients connecting to APs in the Floor 1 group will not be able to receive an IP address.
- C. All clients connecting to the Corp SSID will receive an IP address from the 10.0.3.1/24 subnet.
- D. Clients connecting to APs in the Office group will be assigned an IP address from the 10.0.20.1/24 subnet.

Correct Answer: BD

**QUESTION 2**

Refer to the exhibit showing certificate values.



Wireless guest users are unable to authenticate because they are getting a certificate error while loading the captive portal login page. This URL string is the HTTPS POST URL guest wireless users see when attempting to access the network using the web browser:

<https://fac.trainingad.training.com/guests/login/?loginandpost=https://auth.trainingad.training.1ab:1003/fgtauthandmagic>



=000a038293d1f411andusermac=b8:27:eb:d8:50:02andapmac=70:4c:a5:9d:0d:28andapip=10.10.100.2anduserip=10.0.3.1andssid=Guest03andapname=PS221ETF18000148andbssid=70:4c:a5:9d:0d:30

Which two settings are the likely causes of the issue? (Choose two.)

- A. The external server FQDN is incorrect.
- B. The FortiGate authentication interface address is using HTTPS.
- C. The wireless user's browser is missing a CA certificate.
- D. The user address is not in DDNS form.

Correct Answer: AC

QUESTION 3

What action does FortiSwitch take when it receives a loop guard data packet (LGDP) that was sent by itself?

- A. The receiving port is shut down.
- B. The sending port is shut down
- C. The receiving port is moved to the STP blocking state.
- D. The sending port is moved to the STP blocking state

Correct Answer: B

Reference: <https://www.scribd.com/document/468940309/Secure-Access-6-0-Study-Guide-Online-pdf>

QUESTION 4

An administrator has deployed dual band-capable wireless APs in a wireless network. Multiple 2.4 GHz wireless clients are connecting to the network, and subsequent monitoring shows that individual AP

2.4GHz interfaces are being overloaded with wireless connections. Which configuration change would best resolve the overloading issue?

- A. Configure load balancing AP handoff on both the AP interfaces on all APs.
- B. Configure load balancing AP handoff on only the 2.4GHz interfaces of all Aps.
- C. Configure load balancing frequency handoff on both the AP interfaces.
- D. Configure a client limit on the all AP 2.4GHz interfaces.

Correct Answer: C



QUESTION 5

Examine the following RADIUS configuration:

```
config user radius
  edit "FAC-Lab"
    set server "10.0.1.150"
    set secret ENC XXX
    set nas-ip 10.1.0.254
  next
```

An administrator has configured a RADIUS server on FortiGate that points to FortiAuthenticator. FortiAuthenticator is acting as an authentication proxy and is configured to relay all authentication requests to a remote Windows AD server using LDAP.

While testing the configuration, the administrator notices that the diagnose test authservercommand works with PAP, however, authentication requests fail when using MSCHAPv2.

Which two changes should the administrator make to get MSCHAPv2 to work? (Choose two.)

- A. Force FortiGate to use the PAP authentication method in the RADIUS server configuration.
- B. Change the remote authentication server from LDAP to RADIUS on FortiAuthenticator.
- C. Use MSCHAP instead of using MSCHAPv2
- D. Enable Windows Active Directory Domain Authentication on FortiAuthenticator to add FortiAuthenticator to the Windows domain.

Correct Answer: BD

Reference: <https://docs.fortinet.com/document/fortiauthenticator/6.0.0/administration-guide/641286/remote-authentication-servers>

[NSE7_SAC-6.2 VCE Dumps](#)

[NSE7_SAC-6.2 Study Guide](#)

[NSE7_SAC-6.2 Exam Questions](#)