

➤ **Vendor: Fortinet**

➤ **Exam Code: NSE7\_SAC-6.2**

➤ **Exam Name: Fortinet NSE 7 - Secure Access 6.2**

➤ **New Updated Questions from [Braindump2go](#) (Updated in [September/2020](#))**

[Visit Braindump2go and Download Full Version NSE7\\_SAC-6.2 Exam Dumps](#)

**QUESTION 1**

Refer to the exhibit.

```

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 ((*) SSID: Corp)	10.0.3.1 255.255.255.0	WiFi SSID	3	
Zone (3)					
	Corp.zone		<input type="checkbox"/> Zone	0	
	Corp.101	0.0.0.0.0.0.0	<input checked="" type="checkbox"/> VLAN	1	101
	Corp.102	10.0.20.1 255.255.255.0	<input checked="" type="checkbox"/> VLAN	2	102

Which two statements describe FortiGate behavior regarding assignment of?

- 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 I 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.

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

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

<https://www.braindump2go.com/nse7-sac-6-2.html>

**Answer:** AC

**QUESTION 2**

What is the purpose of configuring the Windows Active Directory Domain Authentication feature?

- A. Allows FortiAuthenticator to register itself as a Windows trusted device to proxy CHAP authentication using Kerberos.
- B. Allows FortiAuthenticator to use Windows administrator credentials to perform an LDAP lookup for a user search.
- C. Allows FortiAuthenticator to use a Windows CA certificate when authenticating RADIUS users.
- D. Allows FortiAuthenticator to authenticate users listed on Windows AD. Enables single sign-on services for VPN and wireless users.

**Answer:** B

**QUESTION 3**

Which two EAP methods can use MSCHAP2 for client authentication? (Choose two.)

- A. GPEAP
- B. EAP-TTLS
- C. EAP-TLS
- D. EAP-GTC

**Answer:** CD

**Explanation:**

<https://docs.fortinet.com/document/fortiauthenticator/6.0.0/administration-guide/125951/extensible-authentication-protocol>

**QUESTION 4**

Which two statements about the use of digital certificates are true? (Choose two.)

- A. An intermediate CA can sign server certificates.
- B. An intermediate CA can sign another intermediate CA certificate.
- C. The end entity's certificate can only be created by an intermediate CA.
- D. An intermediate CA can validate the end entity certificate signed by another intermediate CA

**Answer:** AC

**QUESTION 5**

802.1X port authentication is enabled on only those ports that the FortiSwitch security policy is assigned to. Which configurable items are available when you configure the security policy on FortiSwitch? (Choose two.)

- A. FSSO groups
- B. Security mode
- C. User groups
- D. Default guest group

**Answer:** CD

**QUESTION 6**

A wireless network in a school provides guest access using a captive portal to allow unregistered users to self-register

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

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

**<https://www.braindump2go.com/nse7-sac-6-2.html>**

and access the network. The administrator is requested to update the existing configuration to provide captive portal authentication through a secure connection (HTTPS) to protect and encrypt guest user credentials after they receive the login information when registered for the first time.

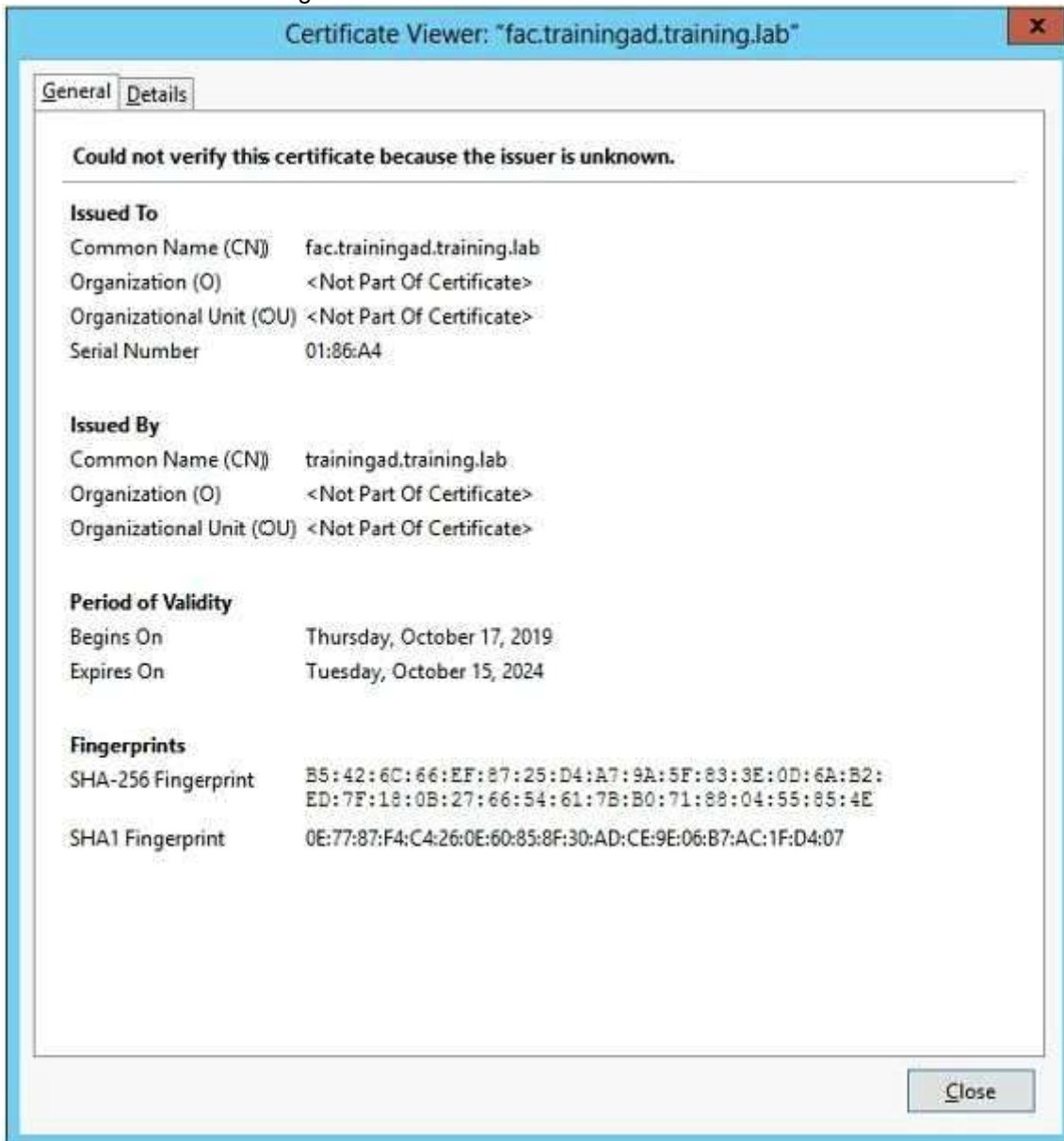
Which two changes must the administrator make to enforce HTTPS authentication? (Choose two.)

- A. Provide instructions to users to use HTTPS to access the network
- B. Create a new SSID with the HTTPS captive portal URL
- C. Enable Redirect HTTP Challenge to a Secure Channel (HTTPS) in the user authentication settings
- D. Update the captive portal URL to use HTTPS on FortiGate and FortiAuthenticator

**Answer:** AC

**QUESTION 7**

Refer to the exhibit showing certificate values.



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

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

<https://www.braindump2go.com/nse7-sac-6-2.html>

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/?
login&post=https://auth.trainingad.training.lab:100
3/fgtauth&magic=000a038293d1f411&usermac=b8:27:eb:d
8:50:02&apmac=70:4c:a5:9d:0d:28&apip=10.10.100.2&us
erip=10.0.3.1&ssid=Guest03&apname=PS221ETF18000148&
bssid=70:4c:a5:9d:0d:30
```

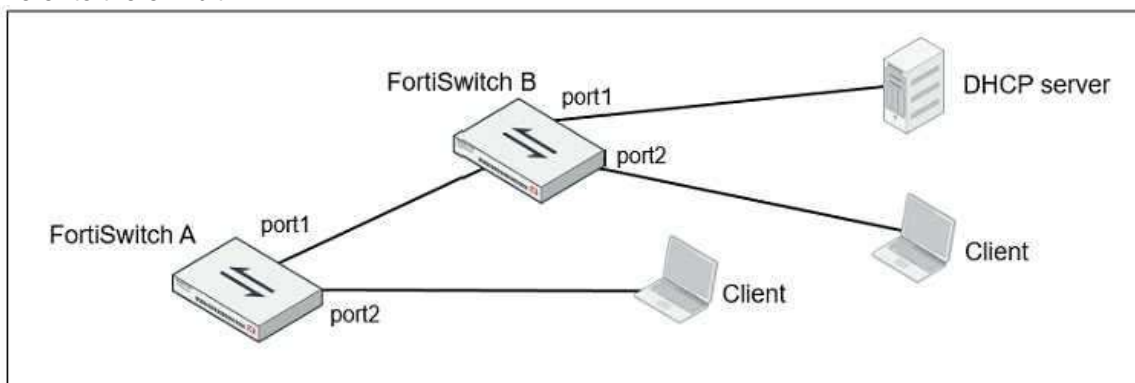
Which two settings are the likely causes of the issue? (Choose two.)

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

**Answer: BC**

### QUESTION 8

Refer to the exhibit.



Given the network topology shown in the exhibit, which two ports should be configured as untrusted DHCP ports? (Choose two.)

- A. FortiSwitch B, port1
- B. FortiSwitch A, port2
- C. FortiSwitch B, port2
- D. FortiSwitch A, port1

**Answer: D**

### QUESTION 9

Examine the following output from the FortiLink real-time debug.:

```
FortiGate# diagnose debug application fortilinkd 3
fl_node_apply_switch_port_fgt_properties_update_with_portname[977]:port properties are different for
port(port9) in switch(F8108D3W17002387) old(0x1) new(0x1)o-peer-port() n-peer-port(port2) o-peer-device() n-
peer-device(FGVMEVBB6ITDA01B)
... flp_event_handler[605]:node: port2 received event 110 state FL_STATE_READY switchname flags 0x26a
... flp_event_handler[605]:node: port2 received event 111 state FL_STATE_READY switchname flags 0x26a
... flp_send_pkt[339]:pkt-sent (type(5) flag=0xe2 node(port2) sw(port2) len(26) smac: 0: c:29:51:dd:a0
dmac:70:4c:a5:24:ba:4f
```

Based on the output, what is the status of the communication between FortiGate and FortiSwitch?

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

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

<https://www.braindump2go.com/nse7-sac-6-2.html>

- A. FortiGate is unable to authorize the FortiSwitch.
- B. FortiGate is unable to establish FortiLmk tunnel to manage the FortiSwitch.
- C. FortiGate is unable to located a previously managed FortiSwitch.
- D. The FortiLink heartbeat is up.

**Answer:** A

**QUESTION 10**

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.

**Answer:** C

**QUESTION 11**

A FotliGate has the following LDAP configuration

```
config user ldap
  edit "Training-Lab"
    set server "10.0.1.10"
    set onid "cn"
    set dn "cn=users,dc=trainingad,dc=training,dc=lab"
    set type regular
    set username "CN=Administrator,DC=trainingAD,DC=training,DC=lab"
    set password ENC XXX
  next
```

On the Windows LDAP server 10.0.1.10, the administrator used dsqueryT which returned the following output:  
>dsquery user -samid admin\* "CN=AdministratorrCN=UsersiDC=trainingAD;DC=trainingiDC=lab" According to the output, which FortiGate LDAP setting is configured incorrectly?

- A. Odn
- B. OsAMAccountName
- C. username
- D. Ocnid

**Answer:** D

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

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

<https://www.braindump2go.com/nse7-sac-6-2.html>