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.geekcert.com/nse7_sac-6-2.html

100% Passing Guarantee
100% Money Back Assurance

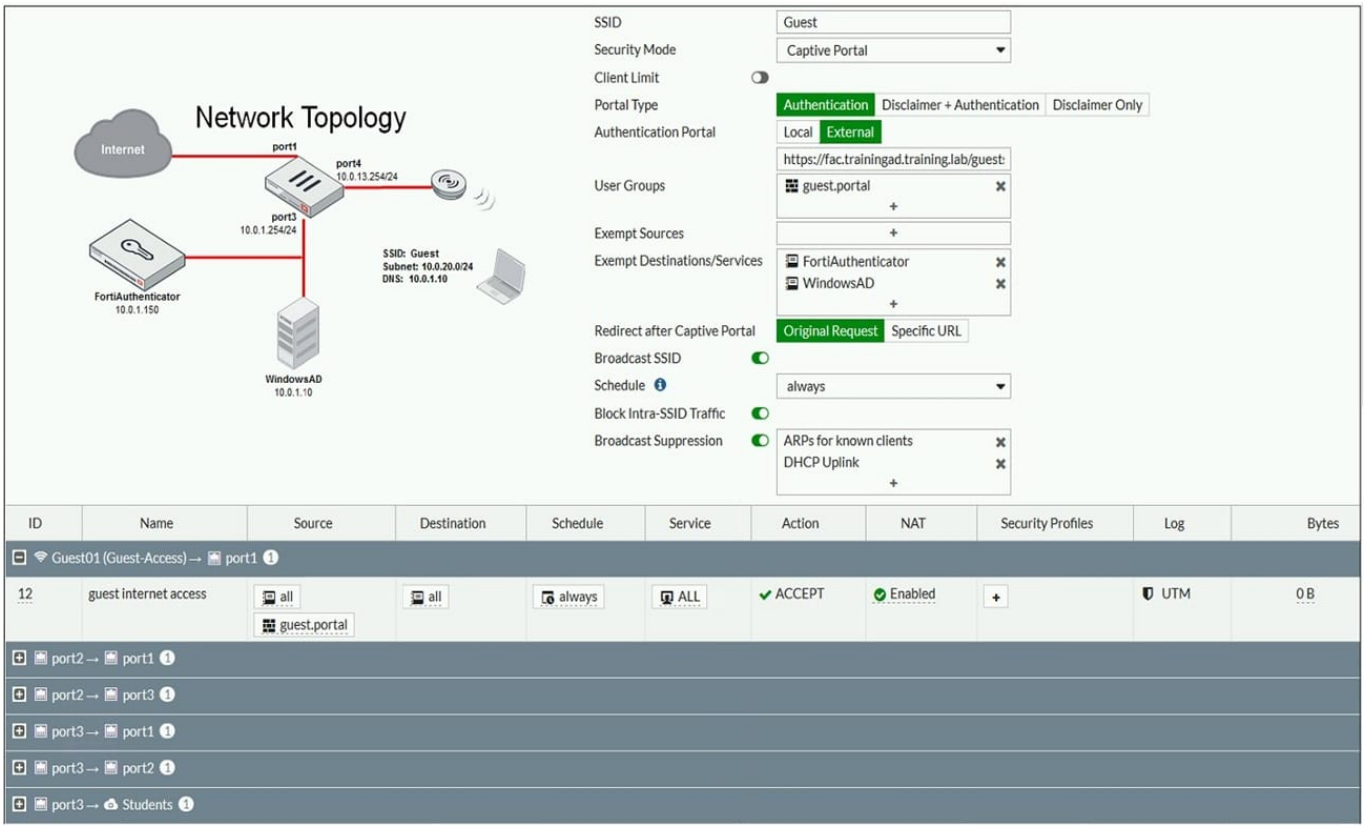
Following Questions and Answers are all new published by Fortinet Official Exam Center

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

QUESTION 1

Refer to the exhibit.

The exhibit shows a network topology and SSID settings.



FortiGate is configured to use an external captive portal. However, wireless users are not able to see the captive portal login page.

Which configuration change should the administrator make to fix the problem?

A. Create a firewall policy to allow traffic from the Guest SSID to FortiAuthenticator and Windows AD devices.

B. Enable the captive-portal-exemptoption in the firewall policy with the ID 10.

C. Remove guest.portal user group in the firewall policy.

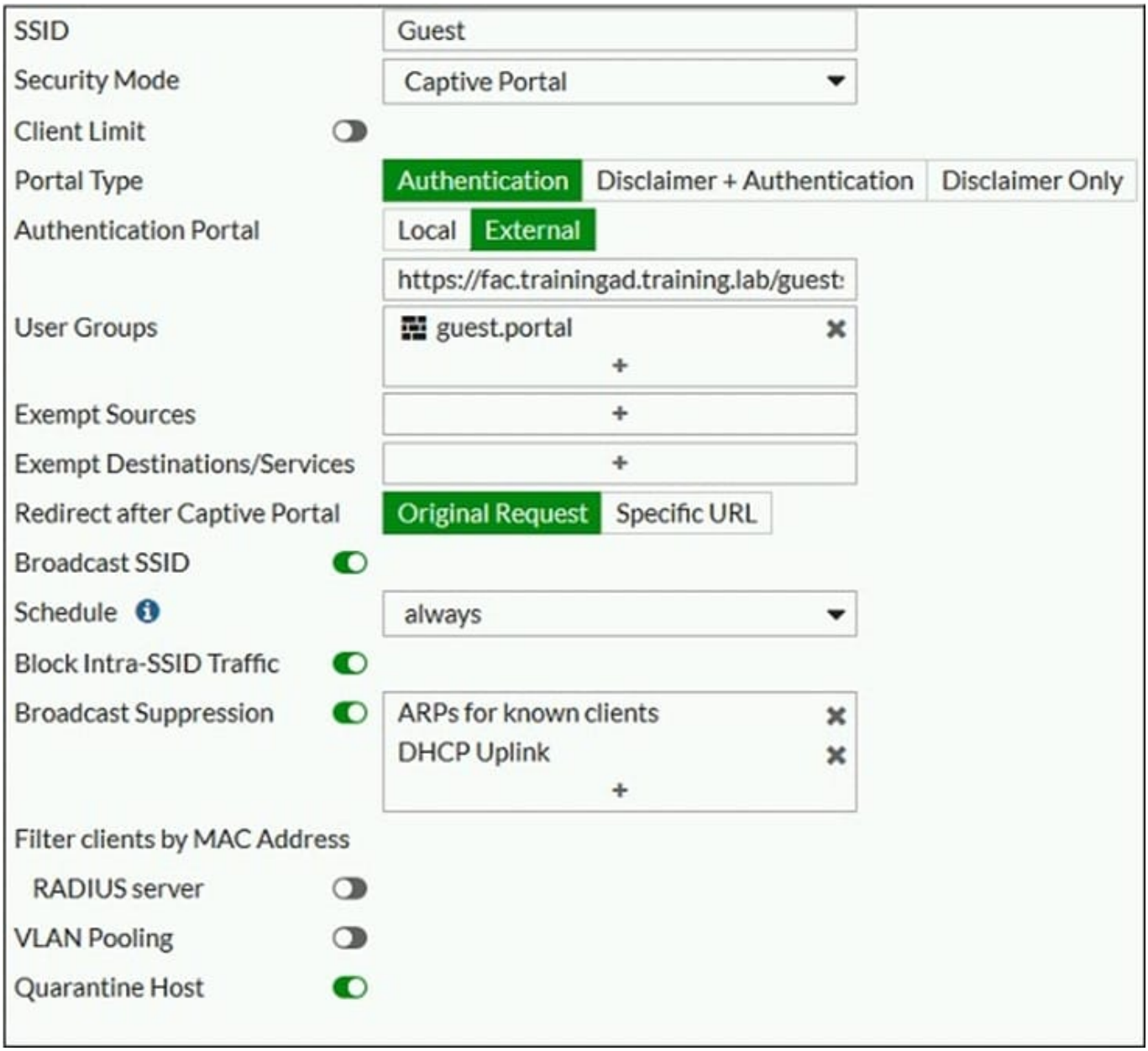
D. FortiAuthenticator and WindowsAD address objects should be added as exempt sources.

Correct Answer: B

Reference: https://docs.fortinet.com/document/fortigate/6.0.0/handbook/868644/captive-portals

QUESTION 2

Refer to the exhibits.



Examine the firewall policy configuration and SSID settings.

```
config firewall policy
   edit 11
      set name "Guest to Internal"
      set uuid c5e45130-aada-51e8-ee0c-bc1204f9f163
      set srcintf "guest"
      set dstintf "port3"
      set srcaddr "all"
      set dstaddr: "FortiAuthenticator" "WindowsAD"
      set action accept
      set schedule "always"
      set service "ALL"
   next
end
```

An administrator has configured a guest wireless network on FortiGate using the external captive portal. The administrator has verified that the external captive portal URL is correct. However, wireless users are not able to see the captive portal login page.

Given the configuration shown in the exhibit and the SSID settings, which configuration change should the administrator make to fix the problem?

A. Enable the captive-portal-exemptoption in the firewall policy with the ID 11.

B. Apply a guest.portal user group in the firewall policy with the ID 11.

C. Disable the user group from the SSID configuration.

D. Include the wireless client subnet range in the Exempt Source section.

Correct Answer: C

QUESTION 3

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.

Correct Answer: BD

QUESTION 4

Which statement correctly describes the quest portal behavior on FortiAuthenticator?

A. Sponsored accounts cannot authenticate using guest portals.

B. FortiAuthenticator uses POST parameters and a RADIUS client configuration to map the request to a guest portal for authentication.

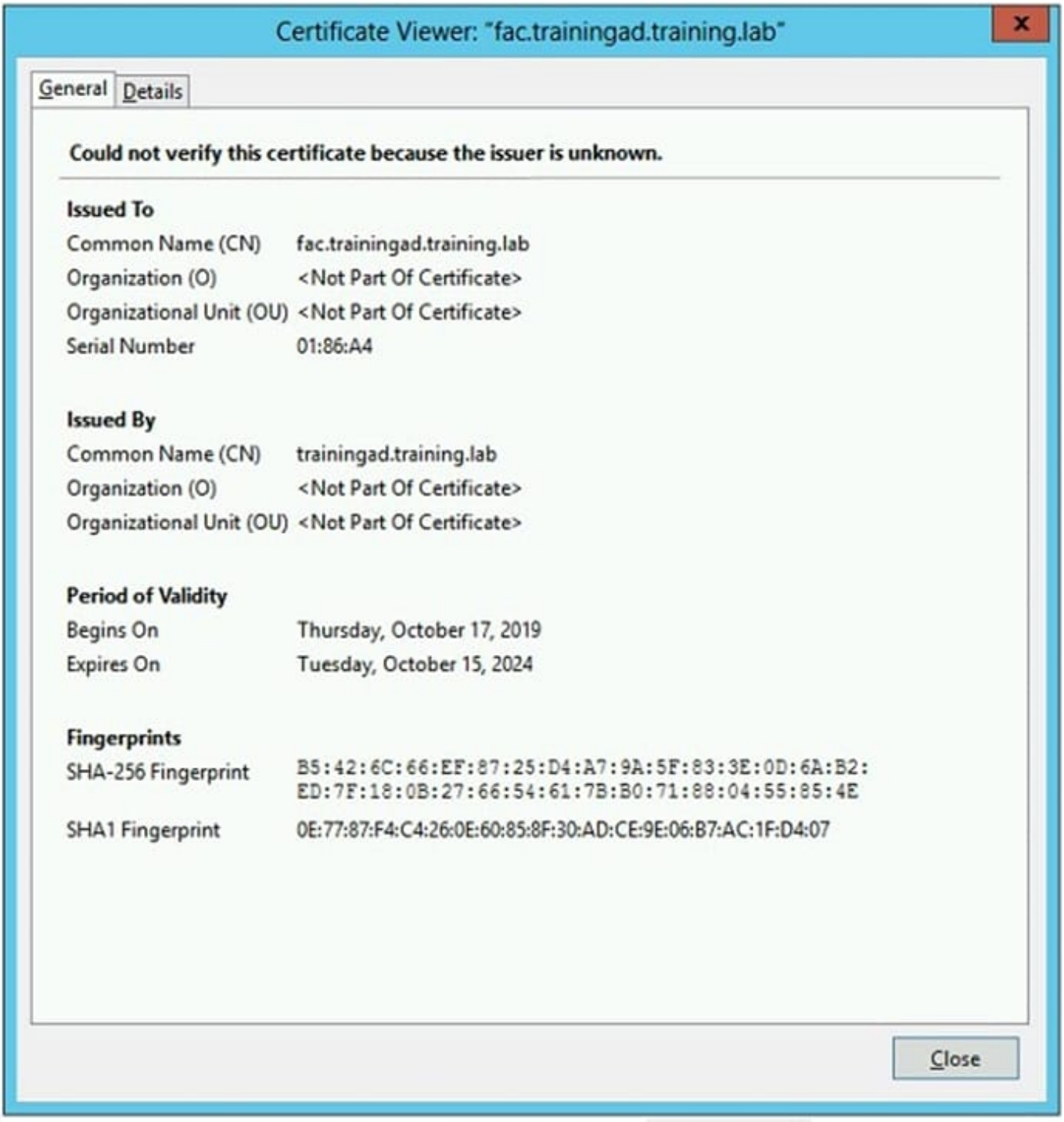
C. All guest accounts must be activated using SMS or email activation codes.

D. All self-registered and sponsored accounts are listed on the local Users GUI page on FortiAuthenticator.

Correct Answer: A

QUESTION 5

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