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

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.

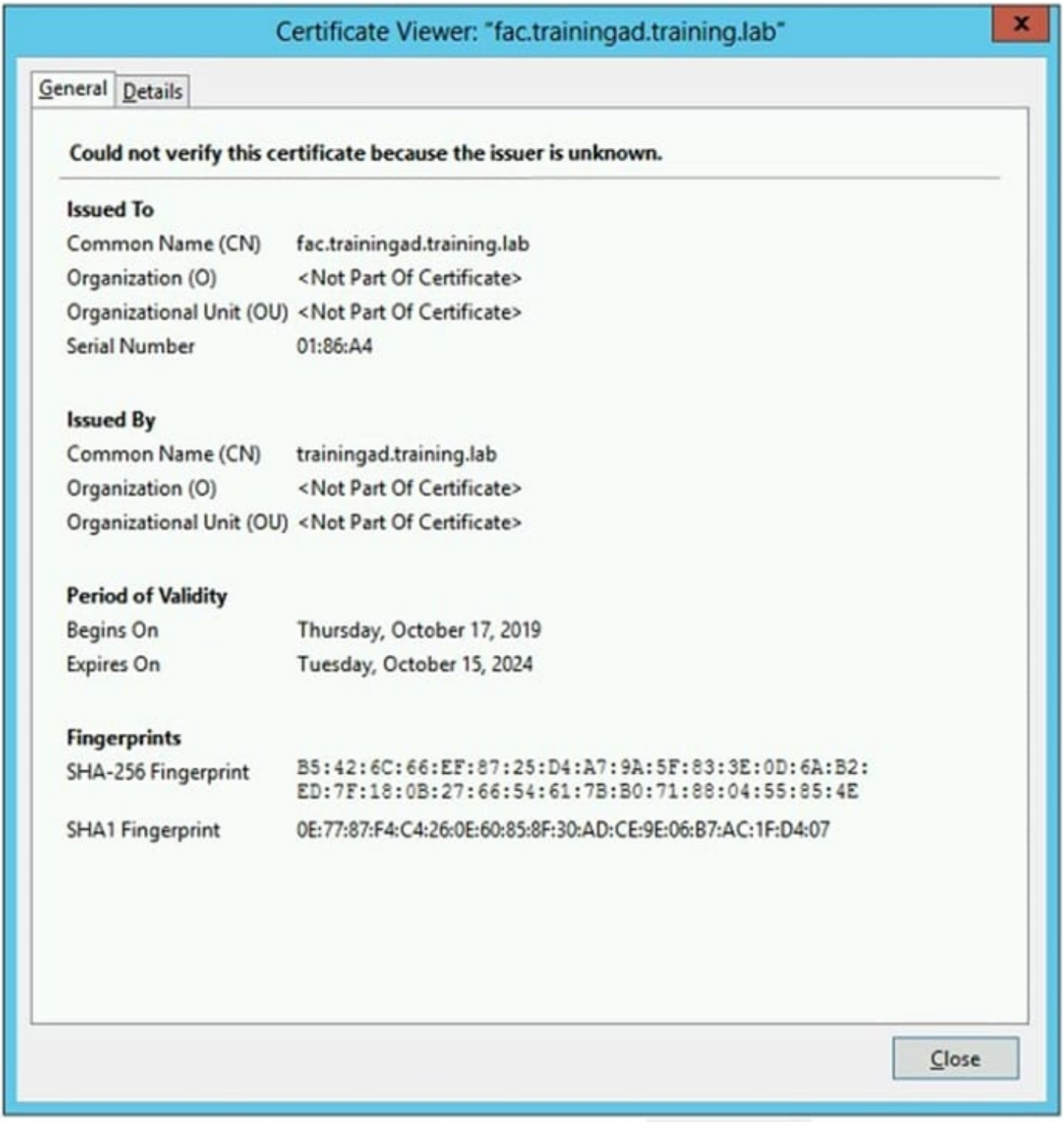
C. All guest accounts must be activated using SMS or email activation codes.

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

Correct Answer: A

QUESTION 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

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.

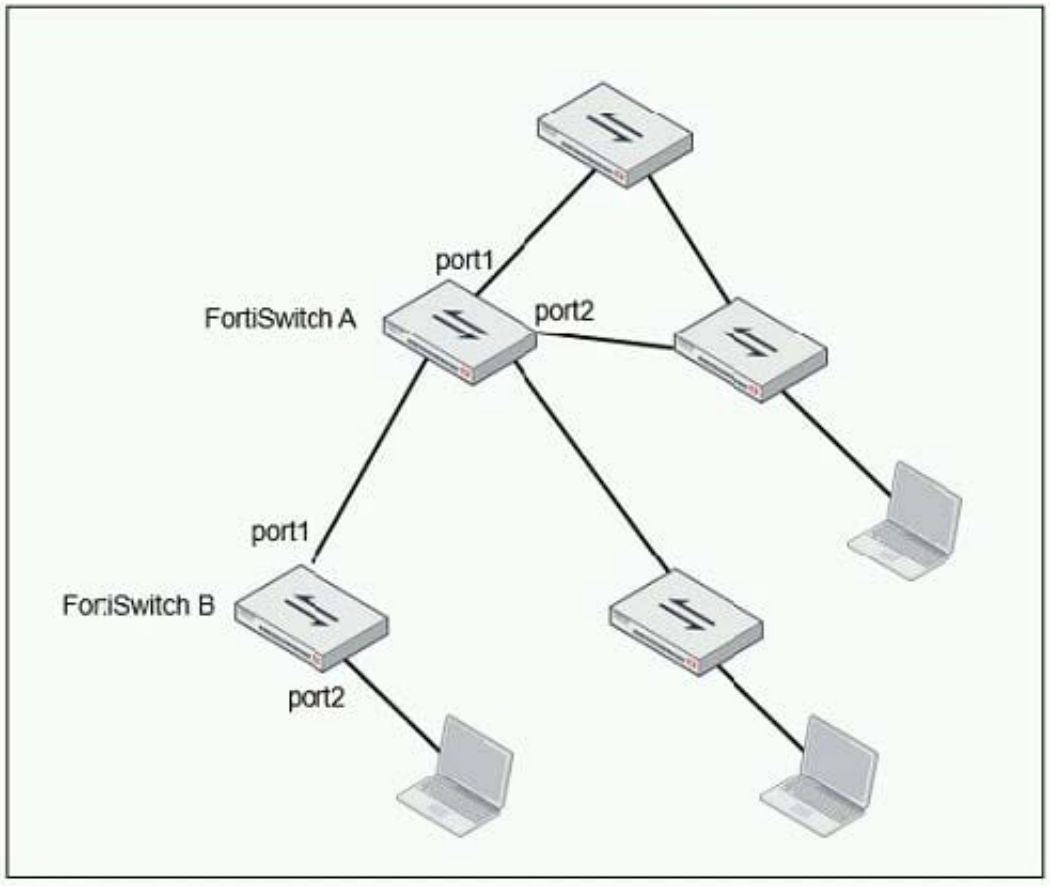
D. Assign a custom AP profile for the remote APs with the set mpls-connectionoption enabled.

Correct Answer: B

QUESTION 4

Refer to the exhibit.

Examine the network topology shown in the exhibit.



Which port should have root guard enabled?

A. FortiSwitch A, port2

B. FortiSwitch A, port1

C. FortiSwitch B, port1

D. FortiSwitch B, port2

Correct Answer: A

Reference: https://docs.fortinet.com/document/fortiswitch/6.4.2/administration-guide/364614/spanningtree-protocol

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

Correct Answer: BC