

Fortinet

FCSS_LED_AR-7.6

Fortinet FCSS - LAN Edge 7.6 Architect

For More Information – Visit link below:

<https://www.examsempire.com/>

Product Version

1. Up to Date products, reliable and verified.
2. Questions and Answers in PDF Format.



<https://examsempire.com/>

Visit us at: <https://www.examsempire.com/fcss-led-ar-7-6>

Latest Version: 6.0

Question: 1

Which encryption protocols can CAPWAP use to secure the data channel when communicating between a FortiGate wireless controller and FortiAP?

- A. WPA3 and TLS
- B. SSH and SSL
- C. DTLS and IPsec
- D. SSL/TLS and IPsec

Answer: C

Question: 2

An LDAP server has been successfully configured on FortiGate, which forwards authentication requests to a Windows Active Directory (AD) server. Users can authenticate using PAP, but authentication fails with MSCHAPv2. Why is it not recommended to use PAP for authentication?

- A. PAP sends passwords in cleartext.
- B. PAP requires the use of an insecure port that is easily blocked by firewalls.
- C. PAP does not support domain-based authentication for Active Directory.
- D. PAP is only supported for local user accounts, not external authentication sources.

Answer: A

Question: 3

You are configuring a new wireless network for your organization. The network requires users to authenticate through a RADIUS server for secure access. Which two security modes should you select when creating the SSID to ensure compatibility with the RADIUS server?
(Choose two.)

- A. WEP
- B. WPA-Personal
- C. WPA3-Enterprise
- D. WPA/WPA2 Mixed Mode
- E. WPA2-Enterprise

Answer: C,D

Question: 4

Refer to the exhibits which show the FortiSwitch and FortiGate interface configurations.

FortiSwitch VLAN configuration

Physical (4)						
<input type="checkbox"/>	1	port1	Physical Interface		port1	dhcp
<input type="checkbox"/>	2	port2	Physical Interface		port2	static
<input type="checkbox"/>	3	port3	Physical Interface		port3	static
<input type="checkbox"/>	4	port5	Physical Interface		port5	static
Aggregate (1)						
<input type="checkbox"/>	5	fortilink	802.3ad Aggregate		fortilink	Dedicated to FortiSwitch
<input type="checkbox"/>		onboarding (onboarding.fortilink)	VLAN	4089	onboarding.fortilink	static
<input type="checkbox"/>		nac_segment (nac_segment.fortilink)	VLAN	4088	nac_segment.fortilink	static
<input type="checkbox"/>		voice (voice.fortilink)	VLAN	4091	voice.fortilink	static
<input type="checkbox"/>		video (video.fortilink)	VLAN	4090	video.fortilink	static
<input type="checkbox"/>		_default (default.fortilink)	VLAN	1	_default.fortilink	static
<input type="checkbox"/>		quarantine (quarantine.fortilink)	VLAN	4093	quarantine.fortilink	static
<input type="checkbox"/>		rspan (rspan.fortilink)	VLAN	4092	rspan.fortilink	static
<input type="checkbox"/>		Student	VLAN	100		static

Port2 interface configuration

Port Name

port2

Description

Access Mode

Assign Port Policy NAC Static

Native VLAN

Student

Allowed VLANs

quarantine 10.255.11.1/255.255.255.0

voice 169.254.14.1/255.255.255.0

Click to select 2 entries selected

Security Policy

Click to select

LLDP Profile

default-auto-isl

QoS Policy

default

ACL Group

PoE Status

DHCP Snooping

Which two statements describe how port2 handles tagged and untagged traffic?
(Choose two.)

- A. Port2 accepts ingress tagged traffic for VLAN IDs 4091 and 4093 only.
- B. Port2 assigns ingress untagged traffic to VLAN 100.
- C. Port2 accepts ingress untagged traffic for VLAN IDs 100, 4091, and 4093 only.
- D. Port2 tags egress traffic for VLAN 100.

Answer: A,B

Question: 5

A network administrator wants a newly deployed FortiGate to automatically discover its FortiManager without manual configuration. Which of the following must be correctly configured for this process to work?

- A. FortiGate interface administrative access must have enabled Security Fabric Connection.
- B. The FortiGate interface must be set to receive an IP address over DHCP.
- C. The DHCP server must provide a valid default gateway to reach FortiManager.
- D. The DHCP server must include Option 240 or Option 241 in its lease offers.

Answer: D

Question: 6

Which features does FortiAuthenticator support when acting as a certificate authority (CA)?

- A. It can issue and revoke digital certificates but cannot act as an OCSP server.
- B. It can integrate with third-party certificate authorities to validate external certificates.
- C. It functions solely as a CRL repository and does not support certificate signing requests (CSR).
- D. It can act as a self-signer for issuing and revoking digital certificates.

Answer: D

Question: 7

You want to configure Syslog-based single sign-on (SSO) on FortiAuthenticator to enhance user authentication across your network. You have to ensure that the system correctly extracts the user information from syslog messages and links it to the correct authentication events. Which two steps must you perform to successfully configure Syslog SSO on FortiAuthenticator? (Choose two.)

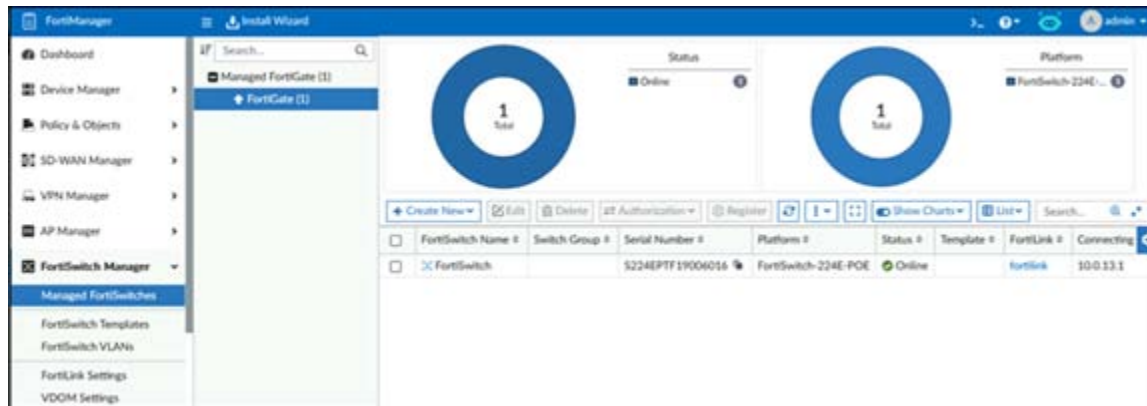
- A. Specify the devices that will send syslog messages to FortiAuthenticator.
- B. Configure parsing rules to extract the relevant information from syslog messages.

- C. Configure the syslog messages that FortiAuthenticator sends to authentication devices.
- D. Set up user authentication policies in FortiAuthenticator.
- E. Enable syslog forwarding on source devices.

Answer: A,B

Question: 8

Refer to the exhibit.



The FortiManager device is set to central management mode for FortiSwitch devices. How are configuration changes applied to multiple FortiSwitch devices?

- A. Configuration changes require manually updating each device.
- B. Changes are applied only to switches that share the same model number.
- C. Changes are made through a template.
- D. Configuration changes are made on individual switches.

Answer: D

Question: 9

You need to deploy a security policy on a FortiSwitch port connected to legacy printers that do not support 802.1X authentication. How can you configure the network to ensure these printers have access while maintaining security?

- A. Enable MAC Authentication Bypass (MAB) on the FortiSwitch port.
- B. Configure the FortiSwitch port to operate in promiscuous mode.
- C. Assign the printers to a high-priority VLAN that bypasses security policies.
- D. Use port mirroring to copy traffic from the printer to another secured port for authentication.

Answer: A

Question: 10

Your team is planning to configure a FortiGate wireless network that automatically quarantines devices using automation stitches. Which two configurations must be in place for a wireless client to be successfully quarantined upon detecting IOC events?
(Choose two.)

- A. Enable Device Detection at the interface level.
- B. FortiAnalyzer must have a valid threat detection services license.
- C. SSIDs must be configured in Bridge mode.
- D. Configure FortiGate as a member of a Security Fabric group.

Answer: B,D

Thank You for Trying Our Product

Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

**Check our Customer Testimonials and ratings
available on every product page.**

Visit our website.

<https://examsempire.com/>