Fortinet

FCSS_LED-AR-7.6

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.**

Latest Version: 6.0

Question: 1

Which CLI command enables FortiLink on port1 of a FortiGate for FortiSwitch management?
Response:

A. config system interface
B. edit port1
C. set fortilink enable
D. All of the above

Answer: D

Question: 2

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?
Response:

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: 3

To manually quarantine a MAC address in FortiGate CLI, which command is correct?
Response:

A. diagnose quarantine mac add <mac-address>
B. config user quarantine → set mac <mac-address>
C. config system quarantine → edit <mac>
D. diagnose firewall mac blacklist <mac-address>

Answer: A

Question: 4

Which three conditions can FortiLink NAC use to enforce network access control?
(Choose three)
Response:

A. MAC address
B. User identity
C. Switch stack priority
D. Device type
E. Interface MTU

Answer: A,B,D

Question: 5

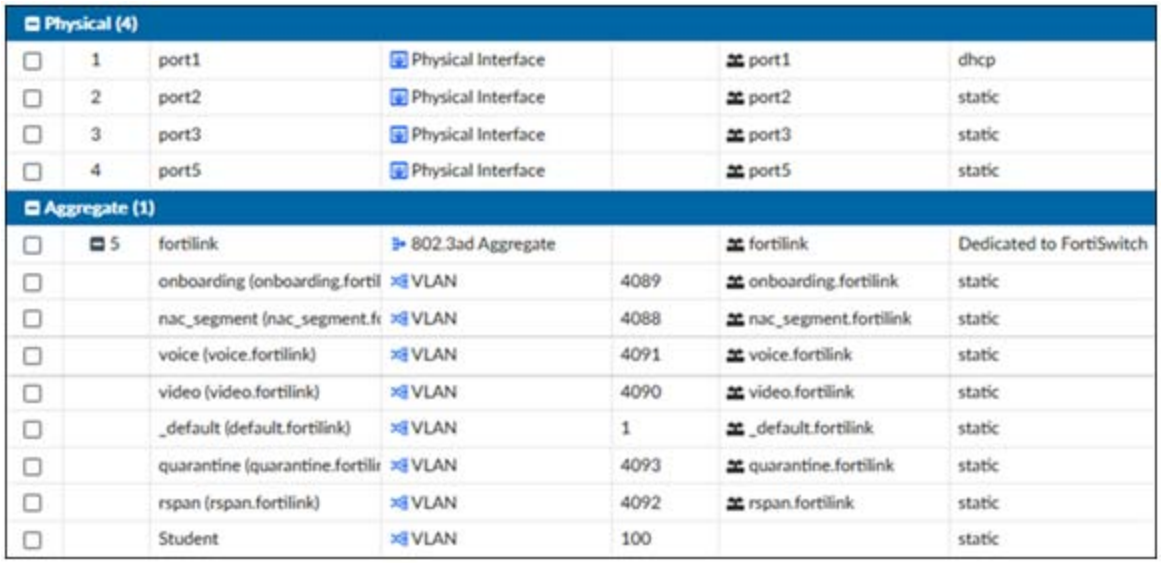
Which log category must be selected to capture authentication logs in FortiAuthenticator's syslog settings?
Response:

A. System Events
B. Authentication
C. Policy
D. Debug

Answer: B

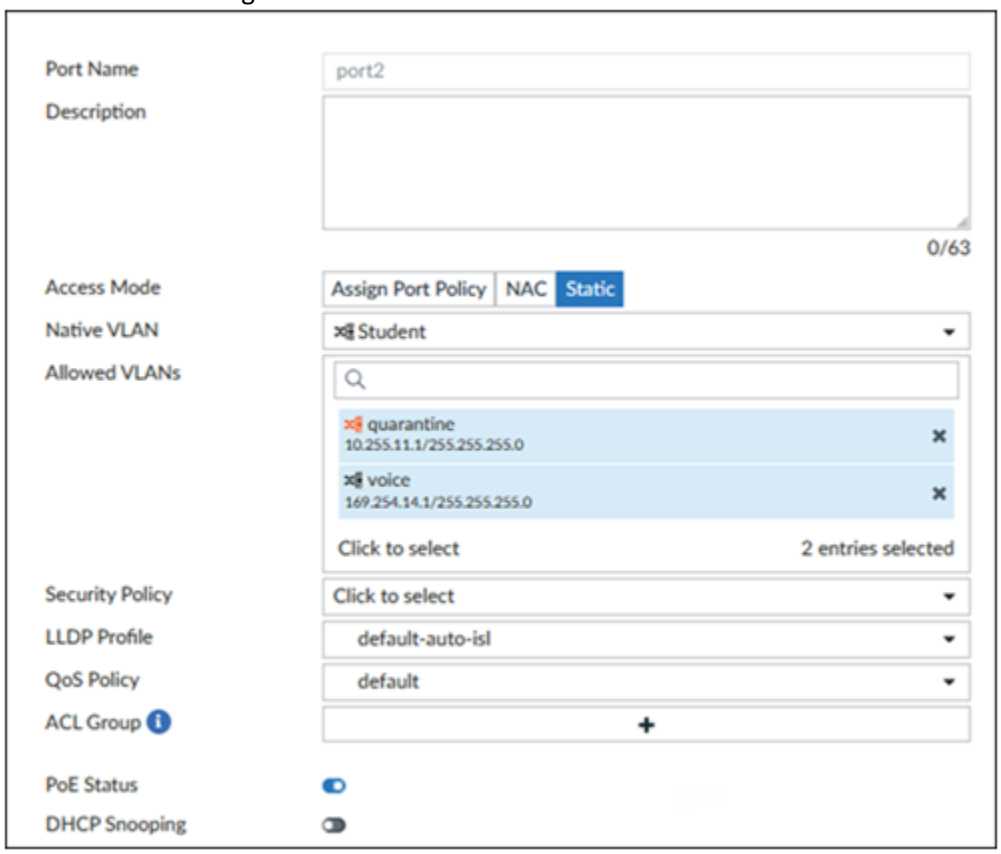
Question: 6

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



Physical (4)						
	1	port1	Physical Interface		port1	dhcp
	2	port2	Physical Interface		port2	static
	3	port3	Physical Interface		port3	static
	4	port5	Physical Interface		port5	static
Aggregate (1)						
	5	fortilink	802.3ad Aggregate		fortilink	Dedicated to FortiSwitch
		onboarding (onboarding.fortil	VLAN	4089	onboarding.fortilink	static
		nac_segment (nac_segment.fo	VLAN	4088	nac_segment.fortilink	static
		voice (voice.fortilink)	VLAN	4091	voice.fortilink	static
		video (video.fortilink)	VLAN	4090	video.fortilink	static
		_default (default.fortilink)	VLAN	1	_default.fortilink	static
		quarantine (quarantine.fortili	VLAN	4093	quarantine.fortilink	static
		rspan (rspan.fortilink)	VLAN	4092	rspan.fortilink	static
		Student	VLAN	100		static

Port2 interface configuration



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

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: 7

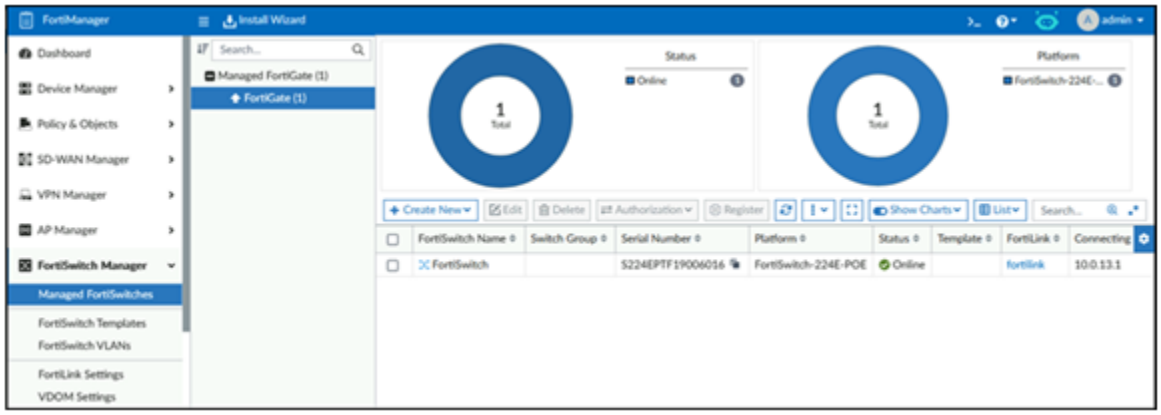
When configuring FortiLink in FortiManager to manage FortiSwitch, which of the following steps are mandatory?
(Choose two)
Response:

A. Enable FortiLink interface on FortiGate
B. Import FortiSwitch configuration template into FortiManager
C. Apply provisioning template to FortiAP
D. Configure switch controller in FortiGate policies

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?
Response:

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

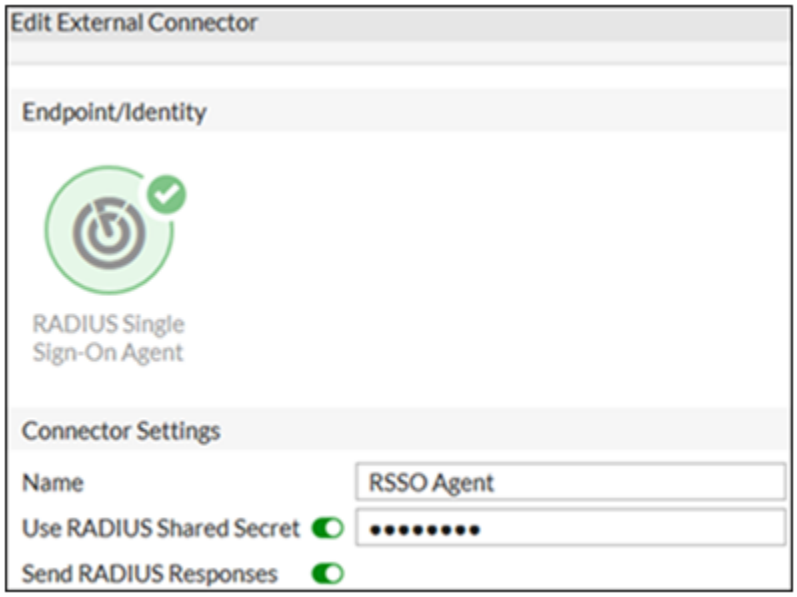
Which of the following are required steps to configure FortiAuthenticator as a RADIUS server for user authentication?
(Choose two)
Response:

A. Define RADIUS clients with shared secrets
B. Enable RSSO on the FortiGate
C. Configure LDAP query in FortiGate
D. Create local user groups or remote user groups

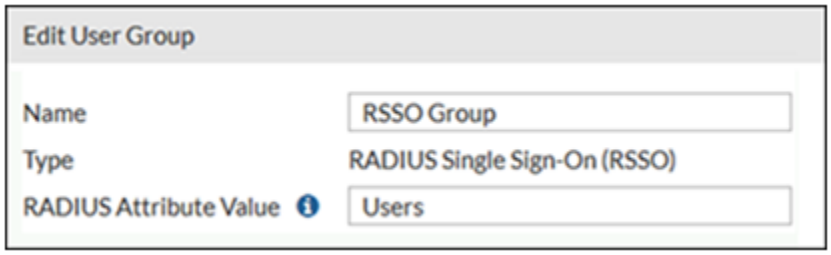
Answer: A,D

Question: 10

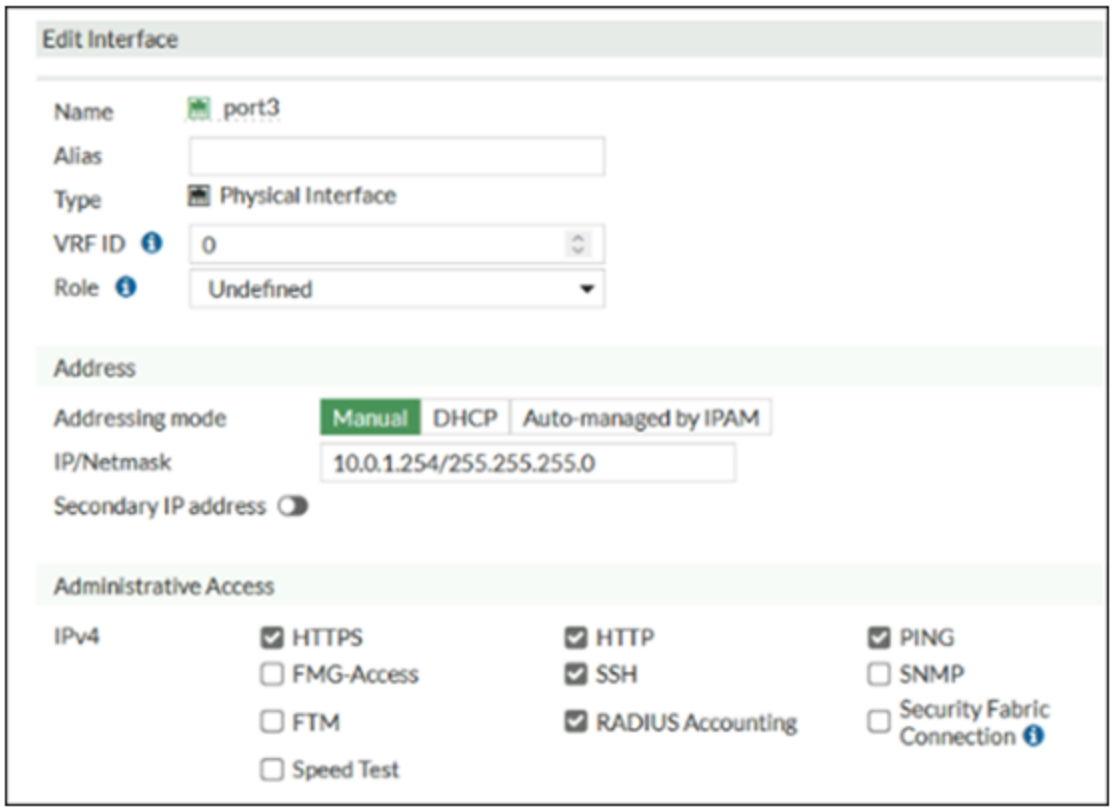
Refer to the exhibits.
FortiGate RSSO configuration



FortiGate RSSO Group



FortiGate interface configuration



RSSO authentication has been configured on FortiGate. Port3 has been enabled to receive RADIUS accounting messages. Internet access is available through port1.
FortiGate is successfully handling incoming RADIUS accounting messages, ensuring that RSSO users are correctly mapped to the RSSO Group user group. The administrator realized that internet access is open to all users and aims to enforce access restrictions, ensuring that only RSSO users are permitted to have internet access.
Which configuration change should the administrator apply to address this issue?
Response:

A. Change the RADIUS attribute value setting to match the name of the RADIUS attribute containing the group membership information of the RSSO users.
B. Create a second firewall policy from port3 to port1, and select the target destination subnets.
C. Configure a local user group and manually add users to enforce authentication-based restrictions.
D. Modify the firewall policy and add RSSO Group as a Source.

Answer: 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/