

Fortinet

FCSS_LED_AR-7.6

Fortinet FCSS - LAN Edge 7.6 Architect



For More Information – Visit link below:

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

Product Version

- ✓ Up to Date products, reliable and verified.
- ✓ 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) | | | | | |
|--------------------------|---|-------------------------------------|--------------------|-----------|------------------------------|
| <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

0/63

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.)

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)

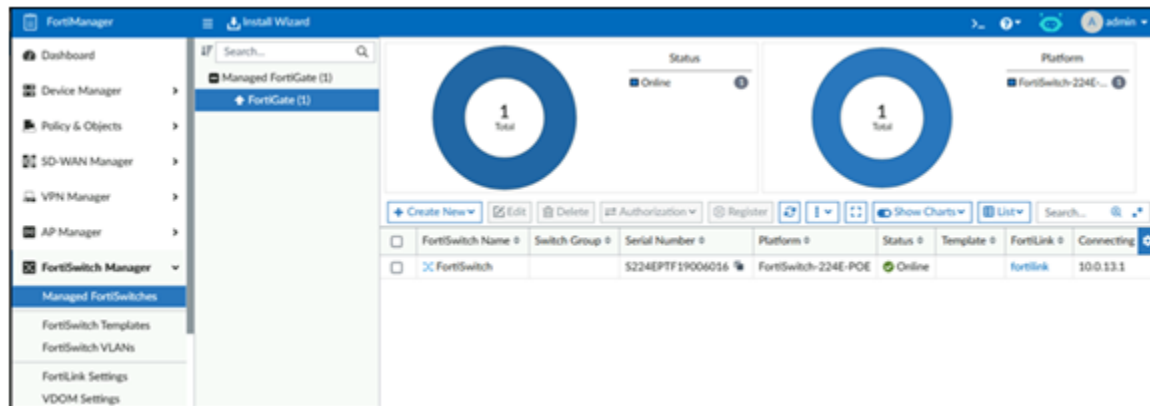
Response:

- 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:

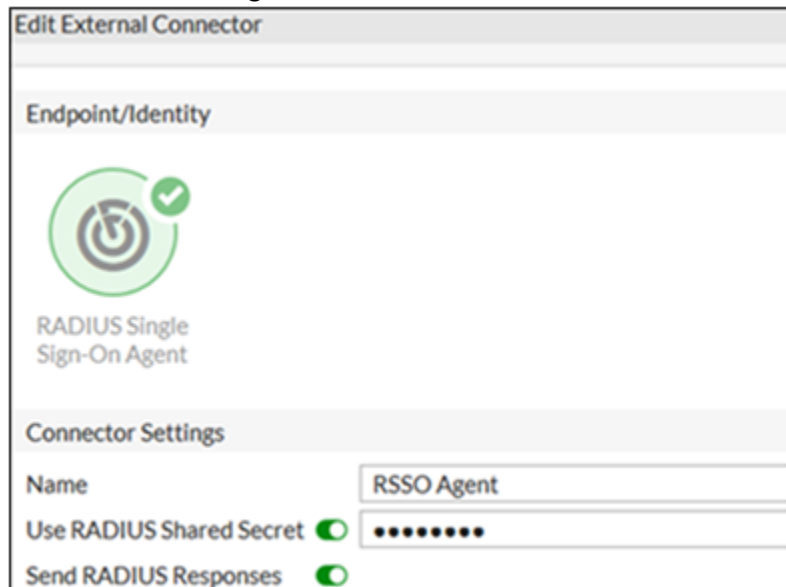
- A. Define RADIUS clients with shared secrets
- B. Enable RSSO on the FortiGate
- C. Configure LDAP query in FortiGate
- D. Create local user groups or remote user groups

Answer: A,D

Question: 10


Refer to the exhibits.

FortiGate RSSO configuration



Edit External Connector

Endpoint/Identity


RADIUS Single Sign-On Agent


Connector Settings

Name: RSSO Agent

Use RADIUS Shared Secret: ☒ ••••••••

Send RADIUS Responses: ☒

FortiGate RSSO Group



Edit User Group

Name: RSSO Group

Type: RADIUS Single Sign-On (RSSO)

RADIUS Attribute Value:  Users

FortiGate interface configuration

Edit Interface

Name
port3

Alias

Type
Physical Interface

VRF ID
0

Role
Undefined

Address

Addressing mode
Manual
DHCP
Auto-managed by IPAM

IP/Netmask
10.0.1.254/255.255.255.0

Secondary IP address

Administrative Access

IPv4

☒ HTTPS
☐ FMG-Access
☐ FTM
☐ Speed Test

☒ HTTP
☒ SSH
☒ RADIUS Accounting

☒ PING
☐ SNMP
☐ Security Fabric Connection

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

For More Information – **Visit link below:**

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

15 USD Discount Coupon Code:

G74JA8UF

FEATURES

- ✓ **90 Days Free Updates**
- ✓ **Money Back Pass Guarantee**
- ✓ **Instant Download or Email Attachment**
- ✓ **24/7 Live Chat Support**
- ✓ **PDF file could be used at any Platform**
- ✓ **50,000 Happy Customer**



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