



**Free Questions for [NSE5\\_FMG-7.2](#) by [braindumpscollection](#)**

**Shared by [Cross](#) on [22-07-2024](#)**

**For More Free Questions and Preparation Resources**

**[Check the Links on Last Page](#)**

## Question 1

---

**Question Type:** MultipleChoice

---

Which two conditions trigger FortiManager to create a new revision history? (Choose two.)

### Options:

---

- A- When FortiManager is auto-updated with configuration changes made directly on a managed device
- B- When changes to the device-level database are made on FortiManager
- C- When FortiManager installs device-level changes on a managed device
- D- When a configuration revision is reverted to a previous revision in the revision history

### Answer:

---

B, C

## Question 2

---

**Question Type:** MultipleChoice

---

Which three settings are the factory default settings on FortiManager? (Choose three.)

**Options:**

---

- A- The administrative domain is disabled.
- B- The Port1 interface IP address is 192.168.1.99/24.
- C- Management Extension applications are enabled.
- D- The FortiManager setup wizard is disabled.
- E- FortiAnalyzer features are disabled.

**Answer:**

---

A, B, E

## Question 3

---

**Question Type:** MultipleChoice

---

Which two settings are required for FortiManager Management Extension Applications (MEA)? (Choose two.)

**Options:**

---

- A- When you configure MEA, you must open TCP or UDP port 540.
- B- You must open the ports to the Fortinet registry
- C- You must create a MEA special policy on FortiManager using the super user profile
- D- The administrator must have the super user profile.

**Answer:**

---

C, D

## Question 4

---

**Question Type: MultipleChoice**

---

What will happen if FortiAnalyzer features are enabled on FortiManager?

**Options:**

---

- A- FortiManager will keep all the logs and reports on the FortiManager.

- B-** FortiManager will enable ADOMs to collect logs automatically from non-FortiGate devices.
- C-** FortiManager will install the logging configuration to the managed devices
- D-** FortiManager can be used only as a logging device.

**Answer:**

---

C

## Question 5

---

**Question Type:** MultipleChoice

---

Which configuration setting for FortiGate is part of an ADOM-level database on FortiManager?

**Options:**

---

- A-** NSX-T Service Template
- B-** Security profiles
- C-** SNMP
- D-** Routing

**Answer:**

---

B

## Question 6

---

**Question Type:** MultipleChoice

---

Refer to the exhibit.

```
Start to import config from device(Local-FortiGate) vdom(root) to
adom(My_ADOM), package(Local-FortiGate_root)

"firewall service category",SKIPPED,"(name=General, oid=697, DUPLICATE)"

"firewall address",SUCCESS,"(name=LOCAL_SUBNET, oid=684, new object)"

"firewall service custom",SUCCESS,"(name=ALL, oid=863, update previous
object)"

"firewall policy",SUCCESS,"(name=1, oid=1090, new object)"
```

Given the configuration shown in the exhibit, how did FortiManager handle the service category named General?

**Options:**

---

- A-** FortiManager ignored the firewall service category General but created a new service category in its database.
- B-** FortiManager ignored the firewall service category general and deleted the duplicate value In Its database
- C-** FortiManager ignored the firewall service category General and updated the FortiGate duplicate value in the FortiGate database.
- D-** FortiManager ignored the firewall service category General and did not update Its database with the value

**Answer:**

---

D

## Question 7

---

**Question Type: MultipleChoice**

---

Which of the following statements are true regarding VPN Gateway configuration in VPN Manager? (Choose two.)

**Options:**

---

- A-** Managed gateways are devices managed by FortiManager in the same ADOM
- B-** External gateways are third-party VPN gateway devices only
- C-** Protected subnets are the subnets behind the device that you don't want to allow access to over the IPsec VPN
- D-** Managed devices in other ADOMs must be treated as external gateways

**Answer:**

---

A, D

## Question 8

---

**Question Type: MultipleChoice**

---

Which of the following statements are true regarding reverting to previous revision version from the revision history? (Choose two.)

**Options:**

---

- A-** To push these changes to a managed device, it required an install operation to the managed FortiGate.
- B-** Reverting to a previous revision history will generate a new version ID and remove all other history



**C-** Reverting to a previous revision history will tag the device settings status as Auto-Update.

**D-** It will modify device-level database

**Answer:**

---

A, D

## **Question 9**

---

**Question Type: MultipleChoice**

---

View the following exhibit:

### Import Device - Local-FortiGate [root]

When importing configuration from this device, all enabled interfaces require a mapping to an ADOM Level interface. Note, the same ADOM Level interface can map to different interfaces on the each device.

Device Interface	ADOM Interface
port1	WAN
port3	LAN

Add mappings for all unused device interfaces

Next >

Cancel

An administrator used the value shown in the exhibit when importing a Local-FortiGate into FortiManager. What name will be used to display the firewall policy for port1?

#### Options:

---

- A- port1 on FortiGate and WAN on FortiManager
- B- port1 on both FortiGate and FortiManager
- C- WAN zone on FortiGate and WAN zone on FortiManager
- D- WAN zone on FortiGate and WAN interface on FortiManager

**Answer:**

---

A

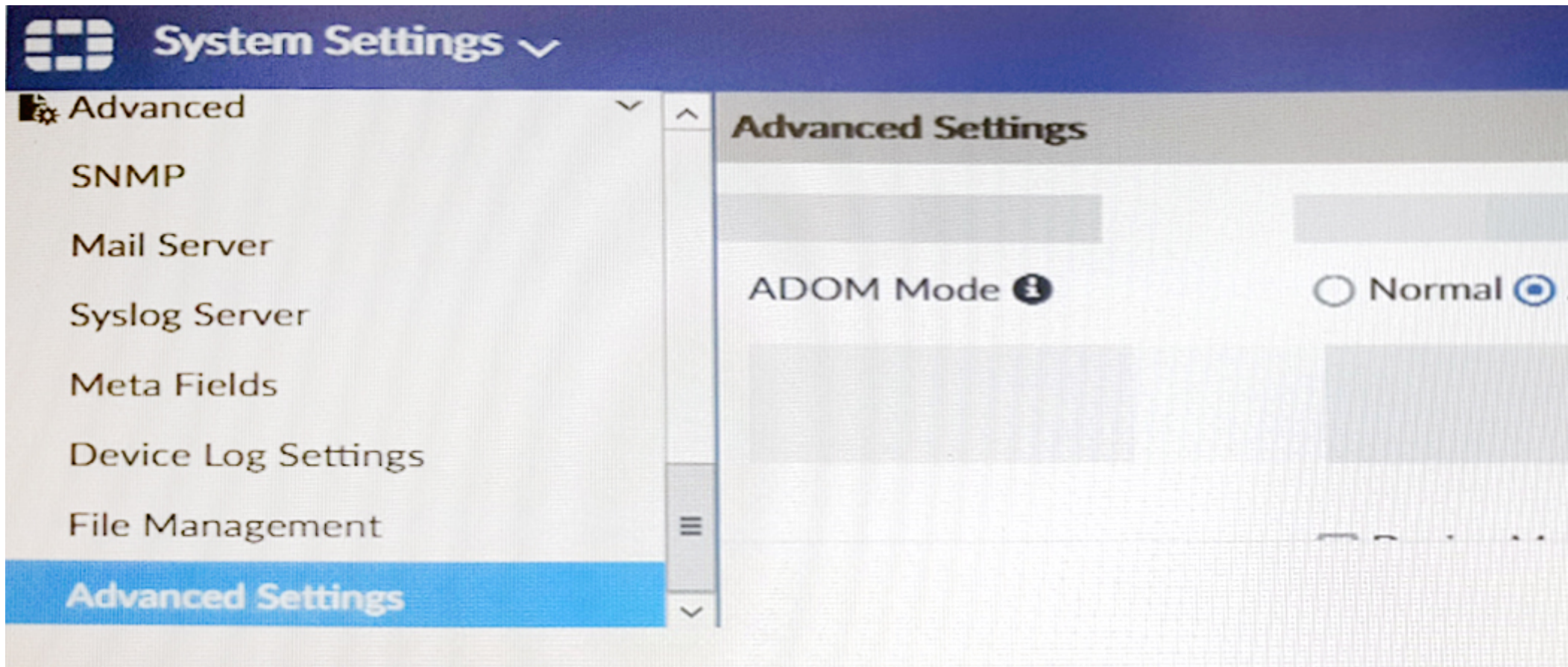
## **Question 10**

---

**Question Type: MultipleChoice**

---

View the following exhibit.



Which of the following statements are true based on this configuration setting? (Choose two.)

**Options:**

---

**A-** This setting will enable the ADOMs feature on FortiManager.

- B-** This setting is applied globally to all ADOMs.
- C-** This setting will allow assigning different VDOMs from the same FortiGate to different ADOMs.
- D-** This setting will allow automatic updates to the policy package configuration for a managed device.

**Answer:**

---

B, C

## Question 11

---

**Question Type: MultipleChoice**

---

An administrator would like to authorize a newly-installed AP using AP Manager. What steps does the administrator need to perform to authorize an AP?

**Options:**

---

- A-** Authorize the new AP using AP Manager and wait until the change is updated on the FortiAP. Changes to the AP's state do not require installation.
- B-** Changes to the AP's state must be performed directly on the managed FortiGate.

- C-** Authorize the new AP using AP Manager and install the policy package changes on the managed FortiGate.
- D-** Authorize the new AP using AP Manager and install the device level settings on the managed FortiGate.

**Answer:**

---

D

**To Get Premium Files for NSE5\_FMG-7.2 Visit**

[https://www.p2pexams.com/products/nse5\\_fmg-7.2](https://www.p2pexams.com/products/nse5_fmg-7.2)

**For More Free Questions Visit**

<https://www.p2pexams.com/fortinet/pdf/nse5-fmg-7.2>

