

# **Fortinet**

## **FCP\_FMG\_AD-7.4**

### **FCP - FortiManager 7.4 Administrator**



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

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

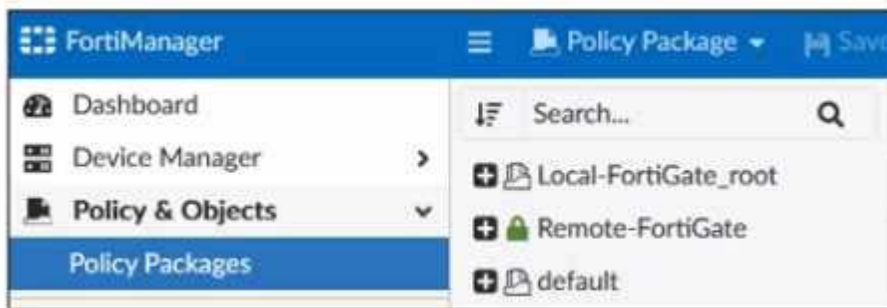
### **Product Version**

- ✓ Up to Date products, reliable and verified.
- ✓ Questions and Answers in PDF Format.

# Latest Version: 7.0

## Question: 1

Exhibit.



Given the configuration shown in the exhibit, which two statements are true? (Choose two.)

- A. An administrator can also lock the Local-FortiGate\_root policy package.
- B. FortiManager is in workflow mode.
- C. The FortiManager ADOM is locked by the administrator.
- D. The FortiManager ADOM workspace mode is set to Normal

**Answer: A, D**

## Question: 2

An administrator enabled workspace mode and now wants to delete an address object that is currently referenced in a firewall policy. Which two results can the administrator expect? (Choose two.)

- A. FortiManager will temporarily change the status of the referenced firewall policy to disabled.
- B. FortiManager will disable the status of the address object until the changes are installed.
- C. FortiManager will not allow the administrator to delete a referenced address object until they lock the ADOM.
- D. FortiManager will replace the deleted address object with the none address object in the referenced firewall policy.

**Answer: C, D**

Explanation:

When operating in workspace mode on FortiManager 7.4, the administrator must understand how object references and deletions work:

Option C - "FortiManager will not allow the administrator to delete a referenced address object until they lock the ADOM":

In workspace mode, all changes are managed within an Administrative Domain (ADOM) scope. When an

object (like an address object) is referenced in a policy, FortiManager prevents its deletion to maintain configuration integrity. The ADOM must be locked by the administrator to make changes to any referenced objects. This locking mechanism ensures that no unintended deletions or changes occur that could disrupt the policies or configuration.

FortiManager Reference: "In workspace mode, changes to objects or policies require the ADOM to be locked. If an object is referenced, you must lock the ADOM before deleting or modifying the object."

(FortiManager 7.4 Administration Guide, Section on Workspace Mode and ADOM Management)

Option D - "FortiManager will replace the deleted address object with the none address object in the referenced firewall policy":

If the administrator attempts to delete an address object that is currently referenced by a firewall policy, FortiManager will replace the deleted object with the 'none' address object. This is done to maintain the policy structure and avoid policy corruption due to a missing reference. This behavior ensures that the firewall policy remains syntactically correct, even though the specific address object is no longer in use.

FortiManager Reference: "When a referenced object is deleted, FortiManager will replace it with a 'none'

object in the policy. This behavior is to ensure the integrity and continuity of the policy configurations."

(FortiManager 7.4 Administration Guide, Object Management and Policy Handling in Workspace Mode)

### Question: 3

What is the purpose of ADOM revisions?

- A. To save the current state of the whole ADOM
- B. To save the current state of all policy packages and objects for an ADOM
- C. To revert individual policy packages and device-level settings for a managed FortiGate
- D. To save the FortiManager configuration in the System Checkpoints

**Answer: B**

Explanation:

Option B: To save the current state of all policy packages and objects for an ADOM is the correct answer. ADOM (Administrative Domain) revisions in FortiManager are used to create a snapshot of the current state of all policy packages and objects associated with an ADOM. This allows administrators to save a specific configuration state and revert to it if necessary. It helps in managing changes and recovering from configuration errors or unintended changes.

Explanation of Incorrect Options:

Option A: To save the current state of the whole ADOM is incorrect because ADOM revisions specifically save only the policy packages and object configurations, not the entire state of the ADOM, which may include logs, reports, and other non-policy data.

Option C: To revert individual policy packages and device-level settings for a managed FortiGate is incorrect as ADOM revisions are not meant for reverting individual policy packages or device settings; they are designed to handle the entire set of policy packages and objects within an ADOM.

Option D: To save the FortiManager configuration in the System Checkpoints is incorrect because ADOM revisions do not function as system checkpoints for FortiManager itself; they are specific to ADOM policy packages and objects.

FortiManager Reference:

Refer to the FortiManager 7.4 Administration Guide, "ADOM Management" section, which describes the purpose and usage of ADOM revisions for configuration management and restoration.

## Question: 4

Refer to the exhibit.

The screenshot shows the 'Edit Address' configuration window in FortiManager. The 'IP/Netmask' field is set to '192.168.1.0/255.255.255.0'. The 'Interface' is set to 'any'. The 'Static Route Configuration' is disabled. The 'Add To Groups' section is empty. The 'Per-Device Mapping' section shows a table with one entry: 'Local-FortiGate [root]' with 'IP/Netmask: 192.168.1.0,255.255.255.240'.

An administrator has created a firewall address object that is used in multiple policy packages for multiple FortiGate devices in an ADOM.

After the installation operation is performed, which IP/netmask is shown on FortiManager for this firewall address object for devices without a Per-Device Mapping set?

- A. FortiManager generates an error for each FortiGate without a per-device mapping defined for that object.
- B. 192.168.1.0/24
- C. 192.168.1.0/28
- D. FortiManager replaces the address object to none.

**Answer: B**

Explanation:

Option B: 192.168.1.0/24 is the correct answer. In FortiManager, when a firewall address object is defined and used across multiple policy packages without any Per-Device Mapping, the default value configured in the object definition (192.168.1.0/255.255.255.0) is applied to all devices. The exhibit shows that the address object LOCAL\_SUBNET has a default IP/netmask of 192.168.1.0/24. Therefore, FortiManager will use this default value for any FortiGate device that does not have a specific Per-Device Mapping configured.

Explanation of Incorrect Options:

Option A: FortiManager generates an error for each FortiGate without a per-device mapping defined for that object is incorrect because FortiManager does not generate an error when a Per-Device Mapping is not set. Instead, it uses the default value provided in the object definition.

Option C: 192.168.1.0/28 is incorrect because the default value is 192.168.1.0/24, as seen in the exhibit, not /28.

Option D: FortiManager replaces the address object to none is incorrect because FortiManager does not replace address objects to "none" when a Per-Device Mapping is missing; it uses the default value instead.

FortiManager Reference:

Refer to the FortiManager 7.4 Administration Guide, specifically in sections related to "Address Object Management" and "Per-Device Mapping," which detail the behavior of address objects without specific device mappings.

## Question: 5

Exhibit.

```
FortiManager # diagnose dvm device list
--- There are currently 1 devices/vdoms managed ---
--- There are currently 1 devices/vdoms count for license ---

TYPE          OID    SN              HA    IP          NAME          ADOM    IPS          FIRMWARE
fmgfaz-managed 325    FGVH010000077646 -    10.0.1.200  ISFW          ADOM2      6.00741 (regular) 7.0 MR4 (2463)
|- STATUS: dev-db: modified; conf: in sync; cond: pending; dm: retrieved; conn: up
|- vdom:[3]root flags:1 adom:ADOM2 pkg: [imported]ISFW
```

Which two statements about the output are true? (Choose two.)

- A. The latest revision history for the managed FortiGate does not match the device-level database.
- B. Configuration changes have been installed on FortiGate, which means the FortiGate configuration has been changed.
- C. Configuration changes directly made on FortiGate have been automatically updated to the devicelevel database.
- D. The latest revision history for the managed FortiGate does match the FortiGate running configuration.

**Answer: A, 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/fcp-fmg-ad-7-4>