

# Fortinet

## Exam Questions FCP\_FMG\_AD-7.6

FCP - FortiManager 7.6 Administrator



**NEW QUESTION 1**

Refer to the exhibit.

```
FortiManager # diagnose dvm device list
--- There are currently 6 devices/vdoms managed ---
--- There are currently 6 devices/vdoms count for license ---

TYPE          OID    SN          HA    IP          NAME          ADOM    IPS          FIRMWARE    HW_GenX
fmgfaz-managed 188    FGVM02TM24013504 -    100.65.1.111 BR1-FGT-1    My_ADOM  7.0 MR6 (3401) N/A
|- STATUS: dev-db: not modified; conf: in sync; cond: pending; dm: installed; conn: up; template:[modified]default
|- vdom:[3]root flags:0 adom:My_ADOM pkg:[imported]BR1-FGT-1
```

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, updating policy and device-level database.
- C. The latest revision history for the managed FortiGate does match the FortiManager policy database.
- D. The system template default will override device-level database configurations.

**Answer:** AD

**Explanation:**

The status "pending" indicates the latest revision history does not match the device-level database, meaning there are unapplied changes. The template is marked as [modified], so the system template default will override device-level database configurations when installed.

**NEW QUESTION 2**

You want to let multiple administrators work in the same ADOM without creating configuration conflicts. What is the best and the most effective solution to apply?

- A. Configure RADIUS authentication to assign ADOM roles to each user.
- B. Enable workflow mode, which is the only way to prevent concurrent configuration conflicts.
- C. Assign administrators with JSON API access to the FortiManager.
- D. Activate workspace mode in the ADOM settings.

**Answer:** D

**Explanation:**

Activating workspace mode in the ADOM settings allows multiple administrators to work concurrently in the same ADOM by isolating their configuration changes in separate workspaces, preventing conflicts and enabling effective collaboration.

**NEW QUESTION 3**

Refer to the exhibits.

**FortiManager device database**

The screenshot shows the FortiManager device database interface. On the left is a navigation tree with 'Managed FortiGate (4)' selected, listing devices: BR1-FGT-1, HQ-NGFW-1, Local-Firewall, and Remote-Firewall. The main area contains two donut charts: 'Connectivity' (2 green, 2 grey) and 'Device Conf' (2 green, 2 orange). Below the charts is a table with columns: Device Name, Config Status, Provisioning Templates, and Policy Package Status.

Device Name	Config Status	Provisioning Templates	Policy Package Status
BR1-FGT-1	✓ Synchronized	✓ default	⊙ BR1-FGT-1
HQ-NGFW-1	⚠ Modified	⚠ default	✓ HQ-NGFW-1
Local-Firewall	⚠ Modified	⚠ default	⚠ Central
Remote-Firewall	⚠ Modified	⚠ default	⚠ Central

**Installation Targets Central policy package**

Installation Target	Config Status	Policy Package Status
<input type="checkbox"/> Installation Target		
<input type="checkbox"/> BR1-FGT-1	✓ Synchronized	● BR1-FGT-1
<input type="checkbox"/> Local-Firewall	⊙ Unknown	▲ Central
<input type="checkbox"/> Remote-Firewall	⊙ Unknown	▲ Central

An administrator has been asked to install the same policies from a central policy package onto the BR1-FGT- 1 firewall. The administrator added BR1-FGT-1 as a target in the central policy package installation. What should the administrator do when reinstalling the central policy package on the BR1-FGT-1 firewall?

- A. Assign only one policy package to the firewall because FortiManager does not allow more than one policy package assigned per device at the same time.
- B. Import the policy package to change the unknown status and synchronize the policy package.
- C. Use the install wizard to install the central policy package on the BR1-FGT-1 firewall.
- D. First resolve the modified status in the configuration and provisioning templates to allow a smooth installation.

**Answer: C**

**Explanation:**

Using the Install Wizard is the recommended method to reinstall the central policy package on the BR1-FGT- 1 firewall, ensuring all settings, installation targets, and dependencies are correctly processed during installation.

**NEW QUESTION 4**

What is the purpose of ADOM revisions?

- A. ADOM revisions find unused, duplicate, and unnecessary firewall policies and objects.
- B. ADOM revisions show specific changes in a policy package when it is installed.
- C. ADOM revisions compare previous snapshots of the Policy Package and ADOM-level objects with the device-level database.
- D. ADOM revisions save the current state of all policy packages and objects for an ADOM.

**Answer: D**

**Explanation:**

ADOM revisions save the current state of all policy packages and objects within an ADOM, allowing administrators to track changes over time and revert to previous configurations if needed.

**NEW QUESTION 5**

Refer to the exhibit.

Workspace	Mail Server	Syslog Server	Meta Fields	Misc Settings
<input type="button" value="+ Create New"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Collapse All"/> <input type="button" value="Expand All"/>				
<input type="checkbox"/>	Meta Fields			
Firewall Address (2)				
<input type="checkbox"/>	ExternalSubnet			
<input type="checkbox"/>	InternalSubnet			

An administrator created two new meta fields in FortiManager. Which operation can you perform with these parameters?

- A. You can add them to objects as custom attributes.
- B. You can export them to be used in other ADOMs.
- C. You can use them as variables in scripts.
- D. You can invoke them using the \$ character.

**Answer: A**

**Explanation:**

Meta fields in FortiManager can be added to objects as custom attributes, allowing administrators to categorize and add additional information to firewall objects for

easier management and identification.

#### NEW QUESTION 6

Refer to the exhibit.

```
FortiManager # config system global
(global)# set workspace-mode normal
(global)# end
FortiManager #
```

What are two results from the configuration shown in the exhibit? (Choose two.)

- A. Ungraceful closed sessions will keep the ADOM in a locked state until the administrator session times out.
- B. The administrator can lock policy blocks and FortiManager global ADOM.
- C. The same administrator can lock more than one ADOM at the same time.
- D. The administrator must have access to the ADOM to approve changes.

**Answer:** AB

**Explanation:**

In normal workspace mode, ungraceful session closures will keep the ADOM locked until the session times out, preventing other administrators from editing. Normal workspace mode allows administrators to lock policy blocks and the global ADOM, providing granular locking control.

#### NEW QUESTION 7

An administrator is copying a system template profile between ADOMs by running the following command:

```
execute fmpfile export-profile ADOM 3547 /tmp/Backup_File
```

```
output dump to file: [/tmp/Backup_File]
```

Where does this command export the system template profile from?

- A. FortiManager /tmp/Backup\_File folder
- B. FortiManager ADOM policy database
- C. ADOM device database
- D. FortiManager configuration backup file

**Answer:** B

**Explanation:**

The command exports the system template profile from the FortiManager ADOM policy database, which stores the configuration templates for devices within that ADOM.

#### NEW QUESTION 8

Refer to the exhibit.

## FortiManager script

Create New Script
0/225

Type: CLI Script

Run script on: Device Database

Validate on change:

Validation device platform: FortiGate-VM64

Script details: Search...

```

1 config router prefix-list
2 edit public
3 config rule
4 edit 1
5 set prefix 0.0.0.0/0
6 set action permit
7 next
8 edit 2
9 set prefix 8.8.8.8/32
10 set action deny
11 end
                
```

Advanced Device Filters >

Which two results occur if you run the script using the Device Database option? (Choose two.)

- A. The device Config Status is tagged as Modified.
- B. The script history shows the successful installation of the script on the remote FortiGate.
- C. The successful execution of a script on the Device Database creates a new revision history.
- D. The administrator must install these changes on a managed device using the Install Wizard.

**Answer:** AD

**Explanation:**

Running a script on the Device Database marks the configuration as modified but does not immediately apply changes to the device. The administrator must use the Install Wizard to push and install these changes from the Device Database onto the managed device.

**NEW QUESTION 10**

.....

## **Thank You for Trying Our Product**

### **We offer two products:**

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### **FCP\_FMG\_AD-7.6 Practice Exam Features:**

- \* FCP\_FMG\_AD-7.6 Questions and Answers Updated Frequently
- \* FCP\_FMG\_AD-7.6 Practice Questions Verified by Expert Senior Certified Staff
- \* FCP\_FMG\_AD-7.6 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* FCP\_FMG\_AD-7.6 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The FCP\\_FMG\\_AD-7.6 Practice Test Here](#)**