



Actual exam question from Fortinet's NSE5\_FMG-7.0

Question #: 1

Topic #: 1

[\[All NSE5\\_FMG-7.0 Questions\]](#)

---

Which two statements about Security Fabric integration with FortiManager are true? (Choose two.)

- A. The Fabric View module enables you to view the Security Fabric ratings for Security Fabric devices.
- B. The Security Fabric license, group name, and password are required for the FortiManager Security Fabric integration.
- C. The Security Fabric settings are part of the device-level settings.
- D. The Fabric View module enables you to generate the Security Fabric ratings for Security Fabric devices.

Show Suggested Answer



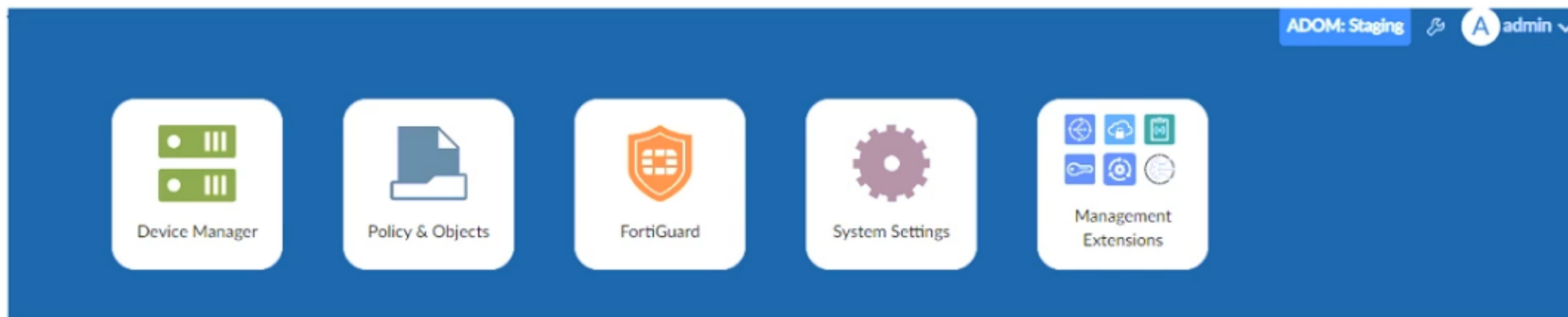
Actual exam question from Fortinet's NSE5\_FMG-7.0

Question #: 2

Topic #: 1

[\[All NSE5\\_FMG-7.0 Questions\]](#)

Refer to the exhibit.



An administrator would like to create a policy on the Staging ADOM in backup mode, and install it on the FortiGate device in the same ADOM.

How can the administrator perform this task?

- A. The administrator must change the ADOM mode to Advanced to bring the FortiManager online.
- B. The administrator must disable the FortiManager offline mode first.
- C. The administrator must use the Policy & Objects section to create a policy first.

Show Suggested Answer





Actual exam question from Fortinet's NSE5\_FMG-7.0

Question #: 3

Topic #: 1

[\[All NSE5\\_FMG-7.0 Questions\]](#)

---

What is the purpose of the Policy Check feature on FortiManager?

- A. It provides recommendations for optimizing policies in a policy package.
- B. It provides recommendations to combine similar policy packages within an ADOM into one single policy package.
- C. It compares the policy packages with the revision history, and updates policy packages in the ADOM database.
- D. It merges and creates dynamic mappings for duplicate objects used in a policy package.

Show Suggested Answer





Actual exam question from Fortinet's NSE5\_FMG-7.0

Question #: 4

Topic #: 1

[\[All NSE5\\_FMG-7.0 Questions\]](#)

---

An administrator's PC crashes before the administrator can submit a workflow session for approval. After the PC is restarted, the administrator notices that the ADOM was locked from the session before the crash.

How can the administrator unlock the ADOM?

- A. Log in using the same administrator account to unlock the ADOM.
- B. Log in as Super\_User in order to unlock the ADOM.
- C. Delete the previous admin session manually through the FortiManager GUI or CLI.
- D. Restore the configuration from a previous backup.

Show Suggested Answer



Actual exam question from Fortinet's NSE5\_FMG-7.0

Question #: 5

Topic #: 1

[\[All NSE5\\_FMG-7.0 Questions\]](#)

Refer to the exhibit.

#### Create ADOM

Name

Type  6.2 6.4 **7.0**

Description

Devices

Select Device  Column Settings

<input type="checkbox"/>	Name	IP Address	Platform
No record found.			

Mode  Normal  Backup

Central Management  VPN  FortiAP  FortiSwitch

Which two statements about an ADOM set in Normal mode on Fortitvnanager are true? (Choose two.)

- A. It supports the FortiManager script feature.
- B. You cannot assign the same ADOM to multiple administrators.
- C. FortiManager automatically installs the configuration difference in revisions on the managed FortiGate.
- D. It allows making configuration changes for managed devices on FortiManager panes.

Show Suggested Answer

Actual exam question from Fortinet's NSE5\_FMG-7.0

Question #: 6

Topic #: 1

[\[All NSE5\\_FMG-7.0 Questions\]](#)

Refer to the exhibit.

The screenshot shows the Fortinet Device Manager interface. The top navigation bar includes 'Device Manager', 'Add Device', 'Device Group', and 'Install Wizard'. Below this, there are statistics for '2 Devices Total', '0 Devices Connection Down', and '1 Device Device Config N'. A table of managed FortiGate devices is displayed with columns for Device Name, Config Status, Policy Package Status, Provisioning Templates, and Firmware Template. The 'Local-FortiGate' row is selected, and the 'Quick Install (Device DB)' option is highlighted in a red box.

Device Name	Config Status	Policy Package Status	Provisioning Templates	Firmware Template
Local-FortiGate	Modified	Local-FortiGate_root	default	default
Remote-FortiGate	Modified	Never installed	default	default

You are using the Quick Install option to install configuration changes on the managed FortiGate.

Which two statements correctly describe the result? (Choose two.)

- A. It installs all the changes in the device database first and the administrator must reinstall the changes on the FortiGate device.
- B. It provides the option to preview only the policy package changes before installing them.
- C. It installs provisioning templates changes on the FortiGate device.
- D. It installs device-level changes on the FortiGate device without launching the Install Wizard.

Show Suggested Answer

Actual exam question from Fortinet's NSE5\_FMG-7.0

Question #: 7

Topic #: 1

[\[All NSE5\\_FMG-7.0 Questions\]](#)

Refer to the exhibit.

```
FortiManager # config system dm
(dm) # set rollback-allow-reboot enable
(dm) # end
FortiManager #
```

An administrator has configured the command shown in the exhibit on FortiManager. A configuration change has been installed from FortiManager to the managed FortiGate that causes the FGFM tunnel to go down for more than 15 minutes.

What is the purpose of this command?

- A. It allows FortiGate to unset central management settings.
- B. It allows FortiGate to reboot and restore a previously working firmware image.
- C. It allows FortiManager to revert and install a previous configuration revision on the managed FortiGate.
- D. It allows FortiGate to reboot and recover the previous configuration from its configuration file.

Show Suggested Answer



Actual exam question from Fortinet's NSE5\_FMG-7.0

Question #: 8

Topic #: 1

[\[All NSE5\\_FMG-7.0 Questions\]](#)

---

An administrator would like to review, approve, or reject all the firewall policy changes made by the junior administrators.

How should the workspace mode settings be configured on FortiManager?

- A. Set to read/write and using the policy locking feature
- B. Set to normal and using the approval group feature
- C. Set to workflow and using the ADOM locking feature
- D. Set to workspace and using the policy locking feature

Show Suggested Answer







Actual exam question from Fortinet's NSE5\_FMG-7.0

Question #: 9

Topic #: 1

[\[All NSE5\\_FMG-7.0 Questions\]](#)

---

What is the purpose of ADOM revisions?

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

Show Suggested Answer





Actual exam question from Fortinet's NSE5\_FMG-7.0

Question #: 10

Topic #: 1

[\[All NSE5\\_FMG-7.0 Questions\]](#)

---

An administrator configures a new OSPF route on FortiManager and has not yet pushed the changes to the managed FortiGate device. In which database will the configuration be saved?

- A. ADOM-level database
- B. Configuration-level database
- C. Revision history database
- D. Device-level database

[Show Suggested Answer](#)



Actual exam question from Fortinet's NSE5\_FMG-7.0

Question #: 11

Topic #: 1

[\[All NSE5\\_FMG-7.0 Questions\]](#)

Refer to the exhibit.

#### Create New CLI Script

Script Name	<input type="text" value="Routing"/>
Comments	<input type="text" value="Write a comment"/> 0/255
Type	<input type="text" value="CLI Script"/>
Run Script on	<input type="text" value="Device Database"/>
Script Detail	<pre>config router prefix-list edit public config rule edit 1 set prefix 0.0.0.0/0 set action permit next edit 2 set prefix 8.8.8.8/32 set action deny end</pre>

#### Advanced Device Filters

What will happen if the script is executed using the Device Database option? (Choose two.)

- A. You must install these changes using the Install Wizard to a managed device.
- B. The successful execution of a script on the Device Database will create a new revision history.
- C. The script history will show successful installation of the script on the remote FortiGate.
- D. The Device Settings Status will be tagged as Modified.

Show Suggested Answer

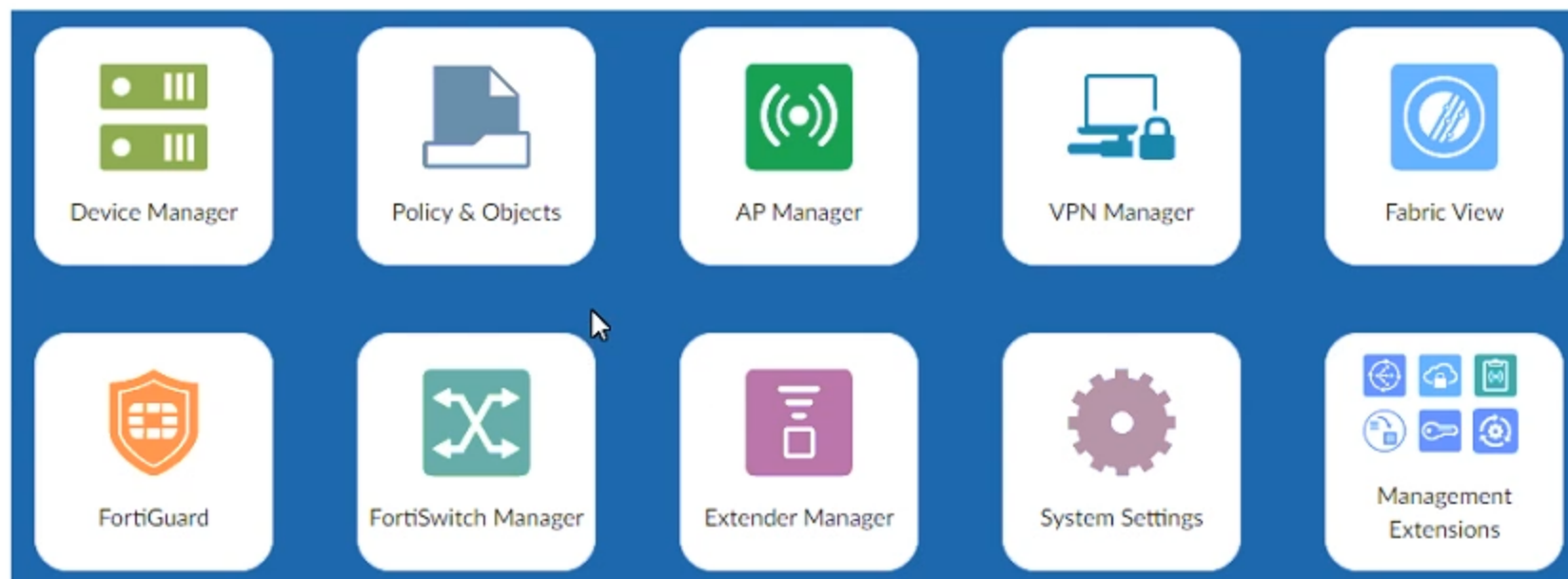
Actual exam question from Fortinet's NSE5\_FMG-7.0

Question #: 12

Topic #: 1

[\[All NSE5\\_FMG-7.0 Questions\]](#)

Refer to the exhibit.



An administrator logs in to the FortiManager GUI and sees the panes shown in the exhibit.

Which two reasons can explain why the FortiAnalyzer feature panes do not appear? (Choose two.)

- A. The administrator profile does not have full access privileges like the Super\_User profile.
- B. The administrator IP address is not a part of the trusted hosts configured on FortiManager interfaces.
- C. The administrator logged in using the unsecure protocol HTTP, so the view is restricted.
- D. FortiAnalyzer features are not enabled on FortiManager.

Show Suggested Answer

Actual exam question from Fortinet's NSE5\_FMG-7.0

Question #: 13

Topic #: 1

[\[All NSE5\\_FMG-7.0 Questions\]](#)

Refer to the exhibit.

#	Name	From	To	Source	Destination	Schedule	Service	Users	Action	Security Profiles	Log
1	Deny ping	any	any	gall	gall	galways	gALL_ICMP		Deny		Log Violation Traffic

A service provider administrator has assigned a global policy package to a managed customer ADOM named My\_ADOM, which has four policy packages. The customer administrator has access only to My\_ADOM.

How can customer or service provider administrators remove both global header and footer policies from the policy package named Shared\_Package?

- A. The service provider administrator can unassign both global policies from My\_ADOM.
- B. The service provider administrator can unassign both policies from the global ADOM.
- C. The customer administrator can unassign both global policies from My\_ADOM.
- D. The customer administrator can unassign both policies by locking My\_ADOM.

Show Suggested Answer

Actual exam question from Fortinet's NSE5\_FMG-7.0

Question #: 14

Topic #: 1

[\[All NSE5\\_FMG-7.0 Questions\]](#)

Refer to the 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 161    FGVM010000064692 -    10.200.1.1  Local-FortiGate  My_ADOM    18.00171 (extended) 7.0 MR0 (157)
|- STATUS: dev-db: modified; conf: in sync; cond: pending; dm: retrieved; conn: up
|- vdom:[3]root flags:0 adom:My_ADOM pkg:[imported]Local-FortiGate
```

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 device-level database.
- D. The latest revision history for the managed FortiGate does match the FortiGate running configuration.

Show Suggested Answer



Actual exam question from Fortinet's NSE5\_FMG-7.0

Question #: 15

Topic #: 1

[\[All NSE5\\_FMG-7.0 Questions\]](#)

---

What will be the result of reverting to a previous revision version in the revision history?

- A. It will generate a new version ID and remove all other revision history versions.
- B. It will install configuration changes to managed device automatically.
- C. It will tag the device settings status as Auto-Update.
- D. It will modify the device-level database.

Show Suggested Answer





Actual exam question from Fortinet's NSE5\_FMG-7.0

Question #: 16

Topic #: 1

[\[All NSE5\\_FMG-7.0 Questions\]](#)

---

An administrator has assigned a global policy package to custom ADOM1. Then the administrator creates a new policy package, Fortinet, in the custom ADOM1. What will happen to the Fortinet policy package?

- A. When the Fortinet policy package is created, it automatically assigns the global policies.
- B. When the Fortinet policy package is created, you can select the option to assign the global policies.
- C. When the Fortinet policy package is created, you need to reapply the global policy package to the ADOM.
- D. When the Fortinet policy package is created, you need to assign the global policy package from the global ADOM.

Show Suggested Answer







Actual exam question from Fortinet's NSE5\_FMG-7.0

Question #: 17

Topic #: 1

[\[All NSE5\\_FMG-7.0 Questions\]](#)

---

What is the advantage of using FortiManager to manage FortiAnalyzer?

- A. It allows FortiManager to act as a collector and FortiAnalyzer device.
- B. It allows FortiManager to manage all FortiGate devices.
- C. It allows FortiManager to run reports based on FortiAnalyzer.
- D. It allows FortiManager to store all managed FortiGate device logs.

Show Suggested Answer





Actual exam question from Fortinet's NSE5\_FMG-7.0

Question #: 18

Topic #: 1

[\[All NSE5\\_FMG-7.0 Questions\]](#)

---

Which two items are included in the FortiManager backup? (Choose two.)

- A. FortiGuard database
- B. Firmware images
- C. Flash configuration
- D. All devices

Show Suggested Answer





Actual exam question from Fortinet's NSE5\_FMG-7.0

Question #: 19

Topic #: 1

[\[All NSE5\\_FMG-7.0 Questions\]](#)

---

An administrator has enabled Service Access on FortiManager.

What is the purpose of Service Access on the FortiManager interface?

- A. It allows administrative access to FortiManager.
- B. It allows FortiManager to respond to requests for FortiGuard services from FortiGate devices.
- C. It allows FortiManager to determine the connection status of managed devices.
- D. It allows third-party applications to gain read/write access to FortiManager.

Show Suggested Answer



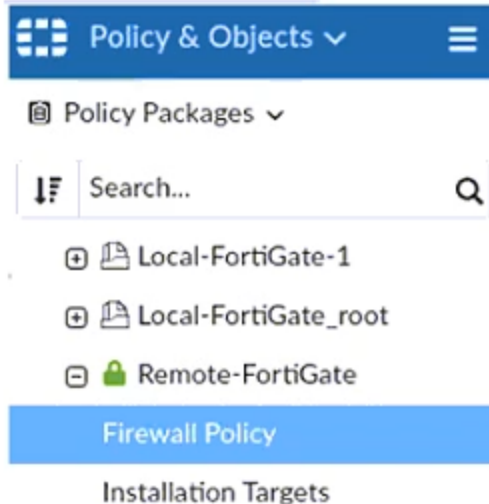
Actual exam question from Fortinet's NSE5\_FMG-7.0

Question #: 20

Topic #: 1

[\[All NSE5\\_FMG-7.0 Questions\]](#)

Refer to the exhibit.



The screenshot shows the FortiManager 'Policy & Objects' configuration page. The 'Policy Packages' section is expanded, showing three packages: 'Local-FortiGate-1' (locked), 'Local-FortiGate\_root' (locked), and 'Remote-FortiGate' (unlocked). The 'Firewall Policy' section is highlighted in blue, and the 'Installation Targets' section is visible below it.

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

- A. An administrator can also lock the Local-FortiGate-1 policy package.
- B. The FortiManager ADOM is locked by the administrator.
- C. The FortiManager ADOM mode is set to Normal.
- D. FortiManager is in workflow mode.

Show Suggested Answer



Actual exam question from Fortinet's NSE5\_FMG-7.0

Question #: 21

Topic #: 1

[\[All NSE5\\_FMG-7.0 Questions\]](#)

---

You are moving managed FortiGate devices from one ADOM to a new ADOM.

Which statement correctly describes the expected result?

- A. Policy packages will be imported into the new ADOM automatically.
- B. Any pending device settings will be installed automatically.
- C. The shared policy package will not be moved to the new ADOM.
- D. Any unused objects from a previous ADOM are moved to the new ADOM automatically.

Show Suggested Answer





Actual exam question from Fortinet's NSE5\_FMG-7.0

Question #: 22

Topic #: 1

[\[All NSE5\\_FMG-7.0 Questions\]](#)

---

Which two statements regarding device management on FortiManager are true? (Choose two.)

- A. FortiGate devices in an HA cluster are counted as a single device.
- B. FortiGate devices in transparent mode configurations are not counted toward the device count on FortiManager.
- C. The maximum number of managed devices for each ADOM is 500.
- D. FortiGate devices in an HA cluster that has five VDOMs are counted as five separate devices.

Show Suggested Answer





Actual exam question from Fortinet's NSE5\_FMG-7.0

Question #: 23

Topic #: 1

[\[All NSE5\\_FMG-7.0 Questions\]](#)

---

An administrator is replacing a failed device on FortiManager by running the following command: `execute device replace sn <devname> <serialnum>`.  
What device name and serial number must the administrator use?

- A. The device name of the new device and serial number of the failed device
- B. The device name and serial number of the new device
- C. The device name and serial number of the failed device
- D. The device name of the failed device and serial number of the new device

Show Suggested Answer

