

# Fortinet

## Exam Questions NSE5\_FMG-7.0

Fortinet NSE 5 - FortiManager 7.0



### NEW QUESTION 1

- (Topic 1)

An administrator, Trainer, who is assigned the Super\_User profile, is trying to approve a workflow session that was submitted by another administrator, Student. However, Trainer is unable to approve the workflow session.

What can prevent an admin account that has Super\_User rights over the device from approving a workflow session?

Session List

| View Diff                           |    |              |         |                 |                |                   |
|-------------------------------------|----|--------------|---------|-----------------|----------------|-------------------|
| <input type="checkbox"/>            | ID | Name         | User    | Date Submitt... | Approved/To... | Comments          |
| <input checked="" type="checkbox"/> | 1  | Firewall p.. | Student | 2017-06-01...   | 0/1            | firewall policies |

+ Add Comment

[Student] - 2017-06-01 13:31:35  
 firewall policies  
 [Student] - 2017-06-01 16:29:27

- A. Trainer is not a part of workflow approval group
- B. Trainer does not have full rights over this ADOM
- C. Trainer must close Student's workflow session before approving the request
- D. Student, who submitted the workflow session, must first self-approve the request

**Answer: A**

**Explanation:**

Reference: [https://help.fortinet.com/fmgr/50hlp/56/5-6-1/FMG-FAZ/0800\\_ADOMs/1800\\_Workflow/0600\\_Workflow%20sessions.htm](https://help.fortinet.com/fmgr/50hlp/56/5-6-1/FMG-FAZ/0800_ADOMs/1800_Workflow/0600_Workflow%20sessions.htm)

### NEW QUESTION 2

- (Topic 1)

An administrator with the Super\_User profile is unable to log in to FortiManager because of an authentication failure message.

Which troubleshooting step should you take to resolve the issue?

- A. Make sure FortiManager Access is enabled in the administrator profile
- B. Make sure Offline Mode is disabled
- C. Make sure the administrator IP address is part of the trusted hosts.
- D. Make sure ADOMs are enabled and the administrator has access to the Global ADOM

**Answer: C**

**Explanation:**

Even if a user entered the correct userid/password, the FMG denies access if a user is logging in from an untrusted source IP subnets.

Reference: <https://docs.fortinet.com/document/fortimanager/6.0.3/administration-guide/107347/trusted-hosts>

### NEW QUESTION 3

- (Topic 1)

An administrator has assigned a global policy package to a new ADOM called ADOM1. What will happen if the administrator tries to create a new policy package in ADOM1?

- A. When creating a new policy package, the administrator can select the option to assign the global policy package to the new policy package
- B. When a new policy package is created, the administrator needs to reapply the global policy package to ADOM1.
- C. When a new policy package is created, the administrator must assign the global policy package from the global ADOM.
- D. When the new policy package is created, FortiManager automatically assigns the global policy package to the new policy package.

**Answer: D**

**Explanation:**

Reference: [https://help.fortinet.com/fmgr/50hlp/56/5-6-2/FortiManager\\_Admin\\_Guide/1200\\_Policy%20and%20Objects/0800\\_Managing%20policy%20packages/1200\\_Assign%20a%20global%20policy%20package.htm](https://help.fortinet.com/fmgr/50hlp/56/5-6-2/FortiManager_Admin_Guide/1200_Policy%20and%20Objects/0800_Managing%20policy%20packages/1200_Assign%20a%20global%20policy%20package.htm)

### NEW QUESTION 4

- (Topic 1)

Which configuration setting for FortiGate is part of a device-level database on FortiManager?

- A. VIP and IP Pools
- B. Firewall policies
- C. Security profiles
- D. Routing

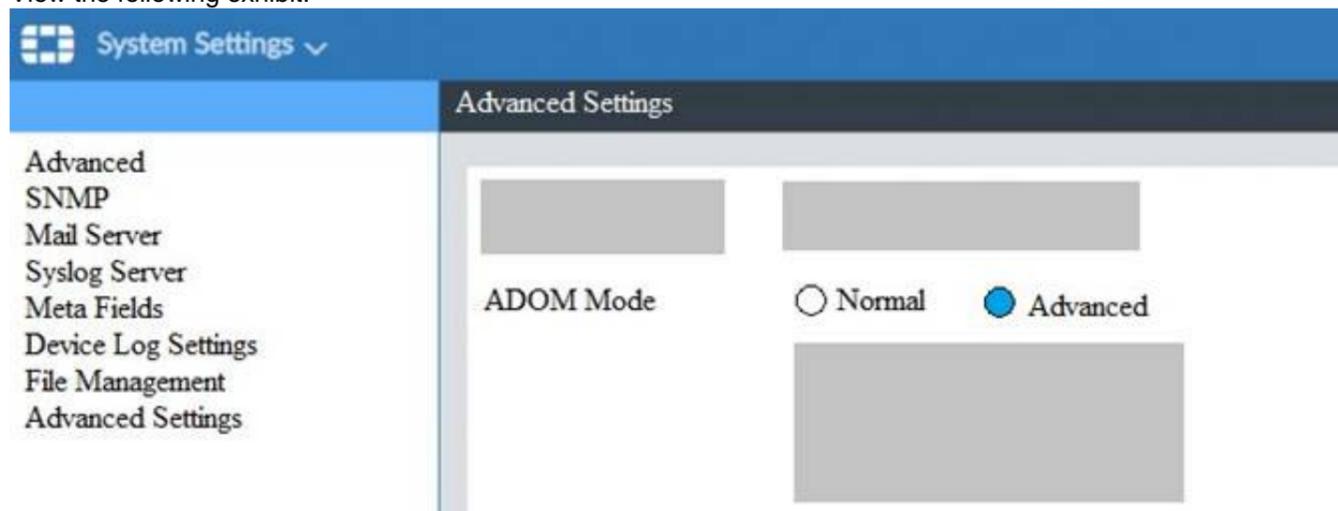
**Answer: D**

**Explanation:**

The FortiManager stores the FortiGate configuration details in two distinct databases. The device-level database includes configuration details related to device-level settings, such as interfaces, DNS, routing, and more. The ADOM-level database includes configuration details related to firewall policies, objects, and security profiles.

**NEW QUESTION 5**

- (Topic 1)  
 View the following exhibit.



What is the purpose of setting ADOM Mode to Advanced?

- A. The setting allows automatic updates to the policy package configuration for a managed device
- B. The setting enables the ADOMs feature on FortiManager
- C. This setting allows you to assign different VDOMs from the same FortiGate to different ADOMs.
- D. The setting disables concurrent ADOM access and adds ADOM locking

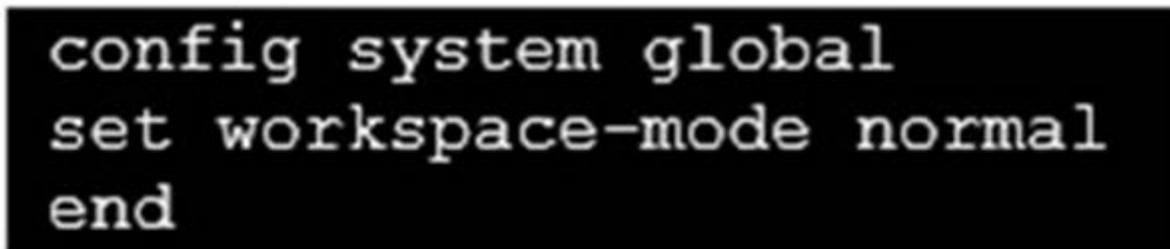
**Answer: C**

**Explanation:**

Reference: <https://docs.fortinet.com/document/fortianalyzer/7.0.0/administration-guide/66530/adom-device-modes>

**NEW QUESTION 6**

- (Topic 2)  
 Refer to the exhibit.



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

- A. It allows two or more administrators to make configuration changes at the same time, in the same ADOM.
- B. It disables concurrent read-write access to an ADOM.
- C. It allows the same administrator to lock more than one ADOM at the same time.
- D. It is used to validate administrator login attempts through external servers.

**Answer: BC**

**Explanation:**

Reference: <https://docs.fortinet.com/document/fortimanager/6.0.4/administration-guide/86456/concurrentadom-access>

**NEW QUESTION 7**

- (Topic 2)  
 Which two statements regarding device management on FortiManager are true? (Choose two.)

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

**Answer: AC**

**NEW QUESTION 8**

- (Topic 2)  
 What does a policy package status of Conflict indicate?

- A. The policy package reports inconsistencies and conflicts during a Policy Consistency Check.
- B. The policy package does not have a FortiGate as the installation target.
- C. The policy package configuration has been changed on both FortiManager and the managed device independently.
- D. The policy configuration has never been imported after a device was registered on FortiManager.

**Answer: C**

**NEW QUESTION 9**

- (Topic 2)

An administrator has assigned a global policy package to custom ADOM1. Then the administrator creates a new policy package, Fortinet, in the custom ADOM1. Which statement about the global policy package assignment to the newly-created policy package Fortinet is true?

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

**Answer:** A

**Explanation:**

Global Policy Package is applied at the ADOM level and you have the option to choose which ADOM policy packages you want to exclude (there is no option to choose Policy Packages to include).

**NEW QUESTION 10**

- (Topic 3)

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

- 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 historyversions.
- C. Reverting to a previous revision history will tag the device settings status as Auto- Update.
- D. It will modify device-level database

**Answer:** AD

**NEW QUESTION 10**

- (Topic 3)

View the following exhibit.

**Edit Address**

Address Name

Type

IP/Network

Interface

Static Route Configuration  
 OFF

Comments  
 0/255

Add to Groups

Advanced Options >

Per-Device Mapping  
 ON

+ Add Edit Delete

| <input type="checkbox"/> | Name                 | VDOM       | Details               |
|--------------------------|----------------------|------------|-----------------------|
| <input type="checkbox"/> | Local-FortiGate root | IP/Netmask | 10.0.10/255.255.255.0 |

An administrator has created a firewall address object, Training, which is used in the Local- FortiGate policy package. When the install operation is performed, which IP Netmask will be installed on the Local-FortiGate, for the Training firewall address object?

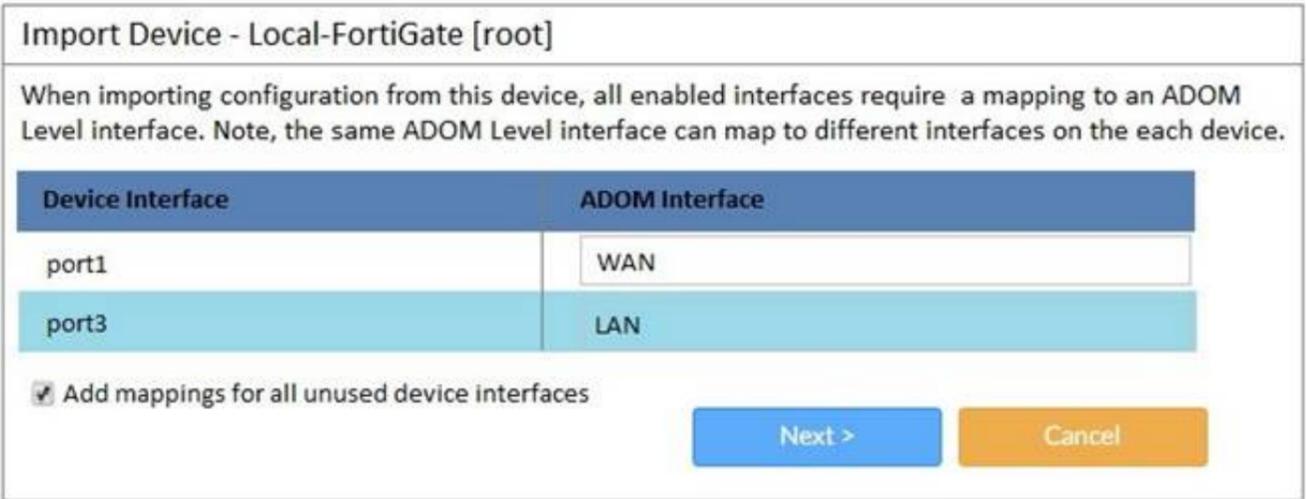
- A. 10.0.1.0/24
- B. It will create firewall address group on Local-FortiGate with 192.168.0.1/24 and 10.0.1.0/24 object values
- C. 192.168.0.1/24
- D. Local-FortiGate will automatically choose an IP Network based on its network interface settings.

**Answer:** A

**NEW QUESTION 15**

- (Topic 3)

View the following exhibit:



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?

- 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**

**NEW QUESTION 19**

- (Topic 3)  
 Refer to the exhibit.



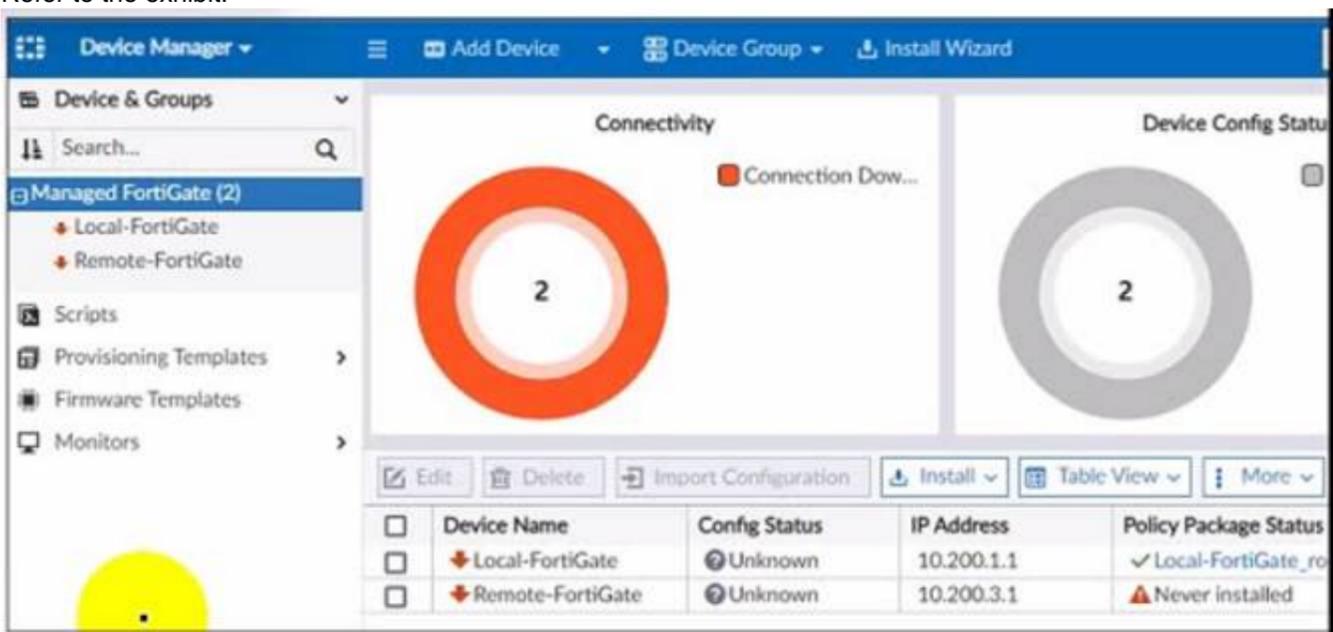
An administrator is about to add the FortiGate device to FortiManager using the discovery process FortiManager is operating behind a NAT device, and the administrator configured the FortiManager NATed IP address under the FortiManager system administration settings. What is the expected result?

- A. During discovery FortiManager sets the FortiManager NATed IP address on FortiGate
- B. During discovery FortiManager sets both the FortiManager NATed IP address and NAT device IP address on FortiGate
- C. During discovery FortiManager sets the NATed device IP address on FortiGate
- D. During discovery FortiManager uses only the FortiGate serial number to establish the connection

**Answer: C**

**NEW QUESTION 23**

- (Topic 3)  
 Refer to the exhibit.



A junior administrator is troubleshooting a FortiManager connectivity issue that is occurring with managed FortiGate devices. Given the FortiManager device manager settings shown in the exhibit, what can you conclude from the exhibit?

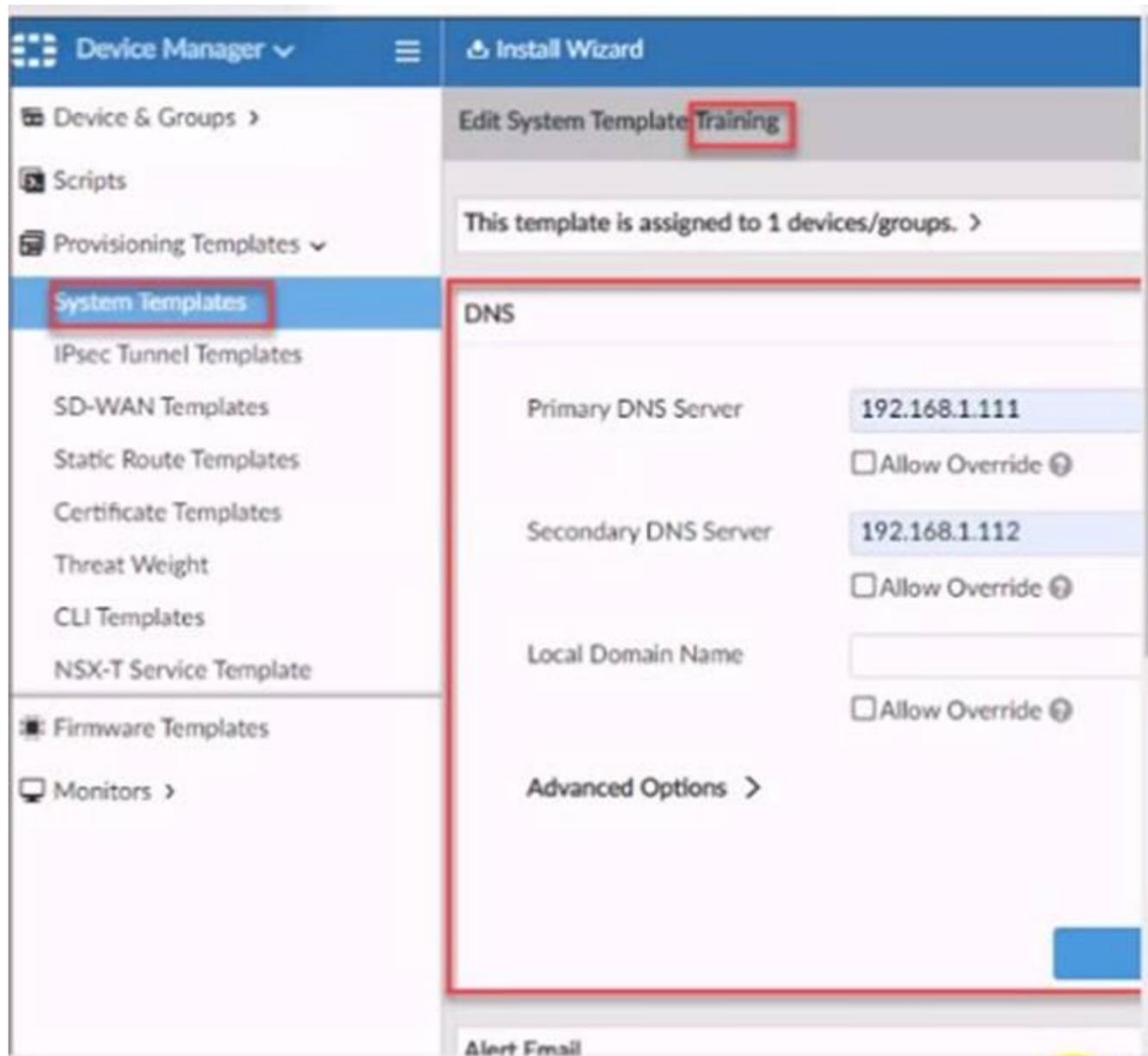
- A. The administrator had restored the FortiManager configuration file
- B. The administrator must refresh both devices to restore connectivity
- C. FortiManager test internet connectivity therefore, both devices appear to be down
- D. The administrator can reclaim the FGFM tunnel to get both devices online

Answer: C

**NEW QUESTION 28**

- (Topic 3)

Refer to the exhibit.



According to the error message why is FortiManager failing to add the FortiAnalyzer device?

- A. The administrator must turn off the Use Legacy Device login and add the FortiAnalyzer device to the same network as Forti-Manager
- B. The administrator must select the Forti-Manager administrative access checkbox on the FortiAnalyzer management interface
- C. The administrator must use the Add Model Device section and discover the FortiAnalyzer device
- D. The administrator must use the correct user name and password of the FortiAnalyzer device

Answer: C

**NEW QUESTION 33**

.....

## **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

### **NSE5\_FMG-7.0 Practice Exam Features:**

- \* NSE5\_FMG-7.0 Questions and Answers Updated Frequently
- \* NSE5\_FMG-7.0 Practice Questions Verified by Expert Senior Certified Staff
- \* NSE5\_FMG-7.0 Most Realistic Questions that Guarantee you a Pass on Your First Try
- \* NSE5\_FMG-7.0 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The NSE5\\_FMG-7.0 Practice Test Here](#)**