

## NSE5\_FMG-7.0 Dumps

### Fortinet NSE 5 - FortiManager 7.0

[https://www.certleader.com/NSE5\\_FMG-7.0-dumps.html](https://www.certleader.com/NSE5_FMG-7.0-dumps.html)



### NEW QUESTION 1

- (Exam Topic 1)

An administrator would like to create an SD-WAN using central management in the Training ADOM.

To create an SD-WAN using central management, which two steps must be completed? (Choose two.)

- A. Specify a gateway address when you create a default SD-WAN static route
- B. Enable SD-WAN central management in the Training ADOM
- C. Configure and install the SD-WAN firewall policy and SD-WAN static route before installing the SD-WAN template settings
- D. Remove all the interface references such as routes or policies that will be a part of SD-WAN member interfaces

**Answer:** BD

#### Explanation:

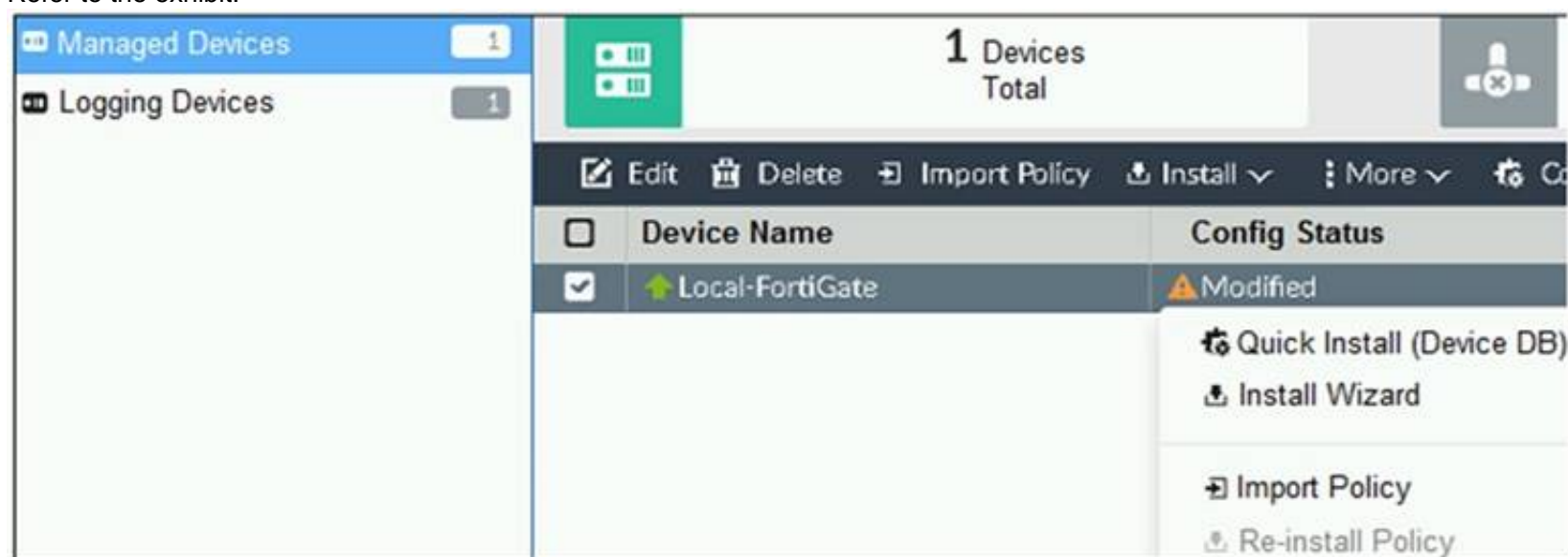
Reference:

<https://docs.fortinet.com/document/fortigate/6.0.0/cookbook/676493/removing-existing-configuration-reference>

### NEW QUESTION 2

- (Exam Topic 1)

Refer to the exhibit.



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 will not create a new revision in the revision history
- B. It installs device-level changes to FortiGate without launching the Install Wizard
- C. It cannot be canceled once initiated and changes will be installed on the managed device
- D. It provides the option to preview configuration changes prior to installing them

**Answer:** BC

#### Explanation:

FortiManager\_6.4\_Study\_Guide-Online – page 164

The Install Config option allows you to perform a quick installation of device-level settings without launching the Install Wizard. When you use this option, you cannot preview the changes prior to committing. Administrator should be certain of the changes before using this install option, because the install can't be cancelled after the process is initiated.

### NEW QUESTION 3

- (Exam Topic 1)

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

- A. To find and provide recommendation to combine multiple separate policy packages into one common policy package
- B. To find and merge duplicate policies in the policy package
- C. To find and provide recommendation for optimizing policies in a policy package
- D. To find and delete disabled firewall policies in the policy package

**Answer:** C

#### Explanation:

Reference:

[https://help.fortinet.com/fmgr/50hlp/56/5-6-2/FortiManager\\_Admin\\_Guide/1200\\_Policy%20and%20Objects/08](https://help.fortinet.com/fmgr/50hlp/56/5-6-2/FortiManager_Admin_Guide/1200_Policy%20and%20Objects/08)

### NEW QUESTION 4

- (Exam Topic 1)

View the following exhibit.

The screenshot displays the FortiGate GUI configuration interface. The top navigation bar includes 'Device Manager', 'Device & Groups', 'Firmware', and 'License'. The 'Device Manager' tab is active, showing a list of managed devices. A red box labeled 'Managed FortiGate devices' highlights the list of devices: Local-FortiGate, Remote-FortiGate, root [NAT] (Management), Student[NAT], and Trainer [NAT].

The 'Policy Packages' tab is also visible, showing a list of policy packages. A red box labeled 'Installation targets' highlights the list of targets: Installation Target, Remote-FortiGate, root [NAT][Management], Student[NAT], and Local-PortiGate.

The 'Interface Pair View' tab is selected, showing a table of policy packages. A red box labeled 'Policy Package' highlights the table.

Seq.#	Install On	Name	From	To
1	Remote-FortiGate(Student) Local-FortiGate(root)	Ping_Access	port3	port1
2	Remote-FortiGate(Student)	Web	port3	port1
3	Installation Targets	Source_Device	port3	port1

Given the configurations shown in the exhibit, what can you conclude from the installation targets in the Install On column?

- A. The Install On column value represents successful installation on the managed devices
- B. Policy seq#3 will be installed on all managed devices and VDOMs that are listed under Installation Targets
- C. Policy seq#3 will be installed on the Trainer[NAT] VDOM only
- D. Policy seq#3 will be not installed on any managed device

Answer: B

#### NEW QUESTION 5

- (Exam Topic 1)

View the following exhibit:

## Create New CLI Script

[\[View Sample Script\]](#)

Script Name	<input type="text" value="Config"/>	
Comments	<input type="text" value="Write a comment"/>	0/255
Type	<input type="text" value="CLI Script"/>	
Run Script on	<input type="text" value="Remote FortiGate Directly(via CLI)"/>	

### Script Detail

```
config vpn ipsec phase1-interface
edit "H25_0"
set auto-discovery-sender enable
next
end
config system interface
edit "H25_0"
set vdom "root"
set ip 172.16.1.1 255.255.255.255
set remote-ip 172.16.1.254
next
end
config router bgp
set as 65100
set router-id 172.16.1.1
config neighbor-group
```

### Advanced Device Filters

Which two statements are true if the script is executed using the Remote FortiGate Directly (via CLI) option? (Choose two.)

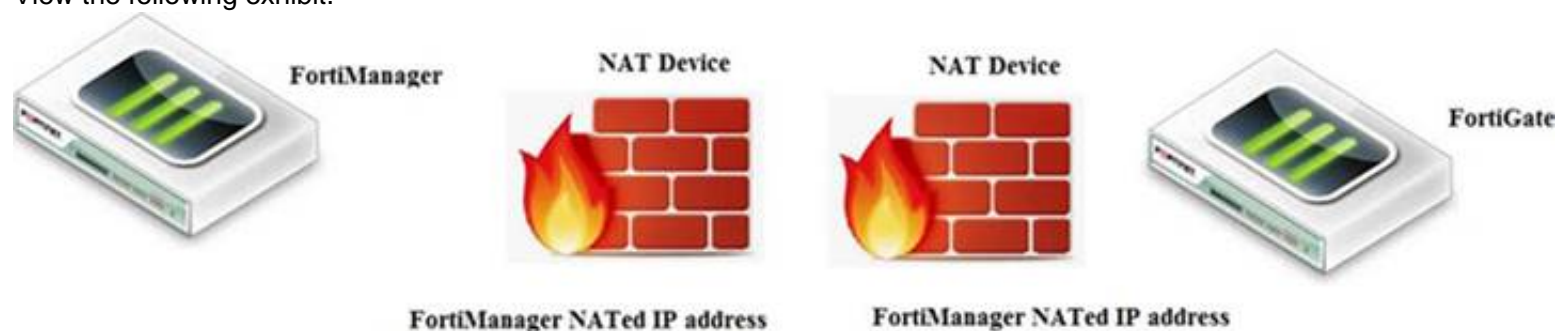
- A. You must install these changes using Install Wizard
- B. FortiGate will auto-update the FortiManager's device-level database.
- C. FortiManager will create a new revision history.
- D. FortiManager provides a preview of CLI commands before executing this script on a managed FortiGate.

**Answer:** BC

### NEW QUESTION 6

- (Exam Topic 1)

View the following exhibit.



If both FortiManager and FortiGate are behind the NAT devices, what are the two expected results? (Choose two.)

- A. FortiGate is discovered by FortiManager through the FortiGate NATed IP address.
- B. FortiGate can announce itself to FortiManager only if the FortiManager IP address is configured on FortiGate under central management.
- C. During discovery, the FortiManager NATed IP address is not set by default on FortiGate.
- D. If the FCFM tunnel is torn down, FortiManager will try to re-establish the FGFM tunnel.

**Answer:** AC

### Explanation:

FortiManager can discover FortiGate through a NATed FortiGate IP address. If a FortiManager NATed IP address is configured on FortiGate, then FortiGate can announce itself to FortiManager. FortiManager will not attempt to re-establish the FGFM tunnel to the FortiGate NATed IP address, if the FGFM tunnel is interrupted. Just like it was in the NATed FortiManager scenario, the FortiManager NATed IP address in this scenario is not configured under FortiGate central management configuration.

### NEW QUESTION 7

- (Exam Topic 1)

Refer to the exhibit.



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

TYPE          OID   SN      HA   IP          NAME          ADOM      IPS          FIRMWARE
fmq/faz enabled 157  FGVM01.. -   10.200.1.1   Local-FortiGate  My_ADOM   14.00641 (regular) 6.0 MR2 (866)
|- 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 match with the FortiGate running configuration
- B. Configuration changes have been installed to FortiGate and represents FortiGate configuration has been changed
- C. The latest history for the managed FortiGate does not match with the device-level database
- D. Configuration changes directly made on the FortiGate have been automatically updated to device-level database

**Answer:** AC

**Explanation:**

STATUS: dev-db: modified; conf: in sync; cond: pending; dm: retrieved; conn: up – dev-db: modified –

This is the device setting status which indicates that configuration changes were made on FortiManager.

– conf: in sync – This is the sync status which shows that the latest revision history is in sync with Fortigate's configuration. – cond: pending – This is the configuration status which says that configuration changes need to be installed.

Most probably a retrieve was done in the past (dm: retrieved) updating the revision history DB (conf: in sync) and FortiManager device level DB, now there is a new modification on FortiManager device level DB (dev-db: modified) which wasn't installed to FortiGate (cond: pending), hence; revision history DB is not aware of that modification and doesn't match device DB.

Conclusion:– Revision DB does match FortiGate.– No changes were installed to FortiGate yet.– Device DB doesn't match Revision DB.– No changes were done on FortiGate (auto-update) but configuration was retrieved instead

After an Auto-Update or Retrieve:device database = latest revision = FGT

Then after a manual change on FMG end (but no install yet):latest revision = FGT (still) but now device database has been modified (is different).

After reverting to a previous revision in revision history:device database = reverted revision != FGT

**NEW QUESTION 8**

- (Exam Topic 1)

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)"
```

Which statement about the object named ALL is true?

- A. FortiManager updated the object ALL using the FortiGate value in its database.
- B. FortiManager installed the object ALL with the updated value.
- C. FortiManager created the object ALL as a unique entity in its database, which can be only used by this managed FortiGate.
- D. FortiManager updated the object ALL using the FortiManager value in its database.

**Answer:** A

**NEW QUESTION 9**

- (Exam Topic 1)

View the following exhibit, which shows the Download Import Report:

```
Start to import config from devices(Remote-FortiGate) vdom (root)to adom (MyADOM),
```

```
Package(Remote-FortiGate)
```

```
"firewall address", SUCCESS,"(name=REMOTE_SUBNET,oid=580, new object)"
```

```
"firewall policy",SUCCESS,"(name=1, oid=990,new object)"
```

```
"firewall policy",FAIL,"(name=ID:2(#2), oid=991, reason=interface(interface binding
```

```
Contradiction.detail:any<-port6)binding fail)"
```

Why it is failing to import firewall policy ID 2?

- A. The address object used in policy ID 2 already exist in ADON database with any as interface association and conflicts with address object interface association locally on the FortiGate
- B. Policy ID 2 is configured from interface any to port6 FortiManager rejects to import this policy because any interface does not exist on FortiManager
- C. Policy ID 2 does not have ADOM Interface mapping configured on FortiManager
- D. Policy ID 2 for this managed FortiGate already exists on FortiManager in policy package named Remote-FortiGate.

**Answer:** A

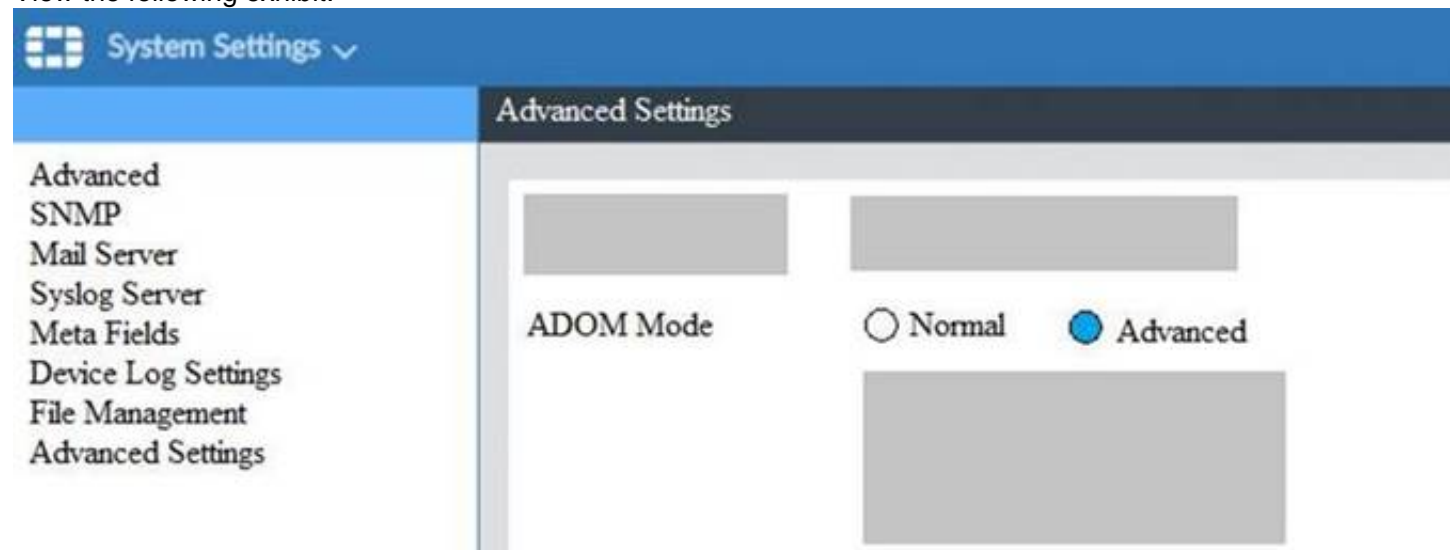
**Explanation:**

FortiManager\_6.4\_Study\_Guide-Online – page 331 & 332

**NEW QUESTION 10**

- (Exam 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 10**

- (Exam 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%20s](https://help.fortinet.com/fmgr/50hlp/56/5-6-1/FMG-FAZ/0800_ADOMs/1800_Workflow/0600_Workflow%20s)

**NEW QUESTION 15**

- (Exam Topic 1)

View the following exhibit.

**Starting Log (Run the device)****Start installing**

```
Local-FortiGate $ config user device
Local-FortiGate (device) $ edit "mydevice"
new entry 'mydevice' added
Local-FortiGate (mydevice) $ next
MAC address can not be 0
Node_check_object fail!for mac 00:00:00:00:00:00
Attribute 'mac' value '00:00:00:00:00:00' checkingfail -33
Command fail. Return code 1
Local-FortiGate (device) $ end
...
Local-FortiGate $ config firewall policy
Local-FortiGate (policy) $ edit 2
New entry '2' added
Local-FortiGate (2) $ set name "Device_policy"
Local-FortiGate (2) $ set uuid 64...
Local-FortiGate (2) $ set srcintf "port3"
Local-FortiGate (2) $ set dstintf "port1"
Local-FortiGate (2) $ set srcaddr "all"
Local-FortiGate (2) $ set dstaddr "all"
Local-FortiGate (2) $ set action accept
Local-FortiGate (2) $ set schedule "always"
Local-FortiGate (2) $ set service "ALL"
Local-FortiGate (2) $ set devices "mydevice"
Entry not found in datasource
Value parse error before 'mydevice'
Command fail. Return code -3
Local-FortiGate (2) $ set nat enable
Local-FortiGate (2) $ next
Local-FortiGate (policy) $ end
...
```

Which statement is true regarding this failed installation log?

- A. Policy ID 2 is installed without a source address
- B. Policy ID 2 will not be installed
- C. Policy ID 2 is installed in disabled state
- D. Policy ID 2 is installed without a source device

**Answer: D**

**NEW QUESTION 20**

- (Exam Topic 1)

In addition to the default ADOMs, an administrator has created a new ADOM named Training for FortiGate devices. The administrator sent a device registration to FortiManager from a remote FortiGate. Which one of the following statements is true?

- A. The FortiGate will be added automatically to the default ADOM named FortiGate.
- B. The FortiGate will be automatically added to the Training ADOM.
- C. By default, the unregistered FortiGate will appear in the root ADOM.
- D. The FortiManager administrator must add the unregistered device manually to the unregistered device manually to the Training ADOM using the Add Device wizard

**Answer: C**

**Explanation:**

Reference: <https://docs.fortinet.com/document/fortimanager/7.0.0/administration-guide/718923/root-adom>

**NEW QUESTION 24**

- (Exam Topic 1)

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

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

**Answer: BC**



**Explanation:**

Reference:

[https://help.fortinet.com/fmgr/50hlp/56/5-6-1/FortiManager\\_Admin\\_Guide/1000\\_Device%20Manager/1500\\_M](https://help.fortinet.com/fmgr/50hlp/56/5-6-1/FortiManager_Admin_Guide/1000_Device%20Manager/1500_M)**NEW QUESTION 28**

- (Exam Topic 1)

An administrator would like to review, approve, or reject all the firewall policy changes made by the junior administrators. How should the Workspace mode be configured on FortiManager?

- A. Set to workflow and use the ADOM locking feature
- B. Set to read/write and use the policy locking feature
- C. Set to normal and use the policy locking feature
- D. Set to disable and use the policy locking feature

**Answer:** A**Explanation:**

Reference:

[https://help.fortinet.com/fmgr/50hlp/52/5-2-0/FMG\\_520\\_Online\\_Help/200\\_What's-New.03.03.html](https://help.fortinet.com/fmgr/50hlp/52/5-2-0/FMG_520_Online_Help/200_What's-New.03.03.html)**NEW QUESTION 33**

- (Exam Topic 1)

An administrator wants to delete an address object that is currently referenced in a firewall policy. What can the administrator expect to happen?

- A. FortiManager will not allow the administrator to delete a referenced address object
- B. FortiManager will disable the status of the referenced firewall policy
- C. FortiManager will replace the deleted address object with the none address object in the referenced firewall policy
- D. FortiManager will replace the deleted address object with all address object in the referenced firewall policy

**Answer:** C**Explanation:**

Reference:

[https://help.fortinet.com/fmgr/50hlp/56/5-6-2/FortiManager\\_Admin\\_Guide/1200\\_Policy%20and%20Objects/12](https://help.fortinet.com/fmgr/50hlp/56/5-6-2/FortiManager_Admin_Guide/1200_Policy%20and%20Objects/12)**NEW QUESTION 34**

- (Exam Topic 1)

When an installation is performed from FortiManager, what is the recovery logic used between FortiManager and FortiGate for an FGFM tunnel?

- A. After 15 minutes, FortiGate will unset all CLI commands that were part of the installation that caused the tunnel to go down.
- B. FortiManager will revert and install a previous configuration revision on the managed FortiGate.
- C. FortiGate will reject the CLI commands that will cause the tunnel to go down.
- D. FortiManager will not push the CLI commands as a part of the installation that will cause the tunnel to go down.

**Answer:** A**Explanation:**

The configuration change will break the fgfm connection, causing the FortiGate unit to attempt to reconnect for 900 seconds. If the FortiGate cannot reconnect, it will rollback to its previous configuration.

**NEW QUESTION 39**

- (Exam Topic 1)

Which two settings must be configured for SD-WAN Central Management? (Choose two.)

- A. SD-WAN must be enabled on per-ADOM basis
- B. You can create multiple SD-WAN interfaces per VDOM
- C. When you configure an SD-WAN, you must specify at least two member interfaces.
- D. The first step in creating an SD-WAN using FortiManager is to create two SD-WAN firewall policies.

**Answer:** AC**NEW QUESTION 42**

- (Exam Topic 2)

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

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

**Answer:** C**Explanation:**<https://kb.fortinet.com/kb/documentLink.do?externalID=FD47942>



**NEW QUESTION 43**

- (Exam Topic 2)

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

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

**Answer:** CD

**NEW QUESTION 45**

- (Exam Topic 2)

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

- A. FortiGuard database
- B. Global database
- C. Logs
- D. All devices

**Answer:** BD

**Explanation:**

Reference: <https://kb.fortinet.com/kb/viewContent.do?externalId=FD34549>

**NEW QUESTION 46**

- (Exam 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 47**

- (Exam Topic 2)

Refer to the exhibit.

```
config system global
set workspace-mode normal
end
```

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 52**

- (Exam Topic 2)

Refer to the exhibit.



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

**Answer:** BD

#### NEW QUESTION 56

- (Exam Topic 2)

Refer to the exhibit.

```
config system dm
set rollback-allow-reboot enable
end
```

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

**Answer:** B

#### Explanation:

Reference:

<https://docs.fortinet.com/document/fortimanager/6.2.0/fortigate-fortimanager-communicationsprotocol-guide/14>

#### NEW QUESTION 57

- (Exam Topic 2)

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

**Answer:** D

#### NEW QUESTION 61

- (Exam Topic 3)

An administrator would like to create an SD-WAN using central management. What steps does the administrator need to perform to create an SD-WAN using central management?

- A. First create an SD-WAN firewall policy, add member interfaces to the SD-WAN template and create a static route
- B. You must specify a gateway address when you create a default static route
- C. Remove all the interface references such as routes or policies
- D. Enable SD-WAN central management in the ADOM, add member interfaces, create a static route and SDWAN firewall policies.

**Answer:** D

#### NEW QUESTION 64

- (Exam Topic 3)

An administrator has added all the devices in a Security Fabric group to FortiManager. How does the administrator identify the root FortiGate?

- A. By a dollar symbol (\$) at the end of the device name
- B. By an at symbol (@) at the end of the device name
- C. By a QUESTION NO: mark(?) at the end of the device name
- D. By an Asterisk (\*) at the end of the device name

**Answer:** D

#### NEW QUESTION 67

- (Exam Topic 3)

What does the diagnose dvm check-integrity command do? (Choose two.)

- A. Internally upgrades existing ADOMs to the same ADON version in order to clean up and correct the ADOM syntax
- B. Verifies and corrects unregistered, registered, and deleted device states
- C. Verifies and corrects database schemas in all object tables
- D. Verifies and corrects duplicate VDOM entries

**Answer:** BD

**Explanation:**

\* 6.2 Study Guide page 305 verify and correct parts of the device manager databases, including:– inconsistent device-to-group and group-to-ADOM memberships– unregistered, registered, and deleted device states– device lock statuses– duplicate VDOM entries

**NEW QUESTION 71**

- (Exam Topic 3)

An administrator would like to create an SD-WAN default static route for a newly created SD-WAN using the FortiManager GUI. Both port1 and port2 are part of the SD-WAN member interfaces.

Which interface must the administrator select in the static route device drop-down list?

- A. port2
- B. virtual-wan-link
- C. port1
- D. auto-discovery

**Answer: B**

**NEW QUESTION 73**

- (Exam Topic 3)

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

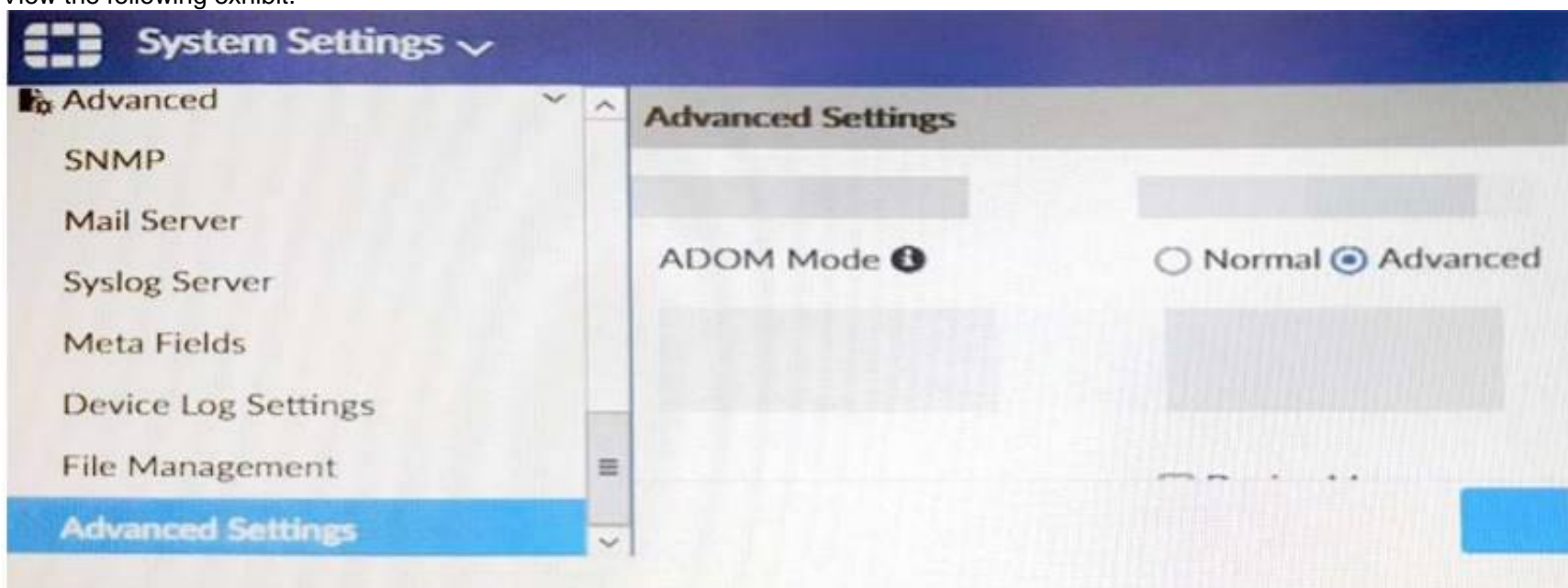
- A. When you configure MEA, you must open TCP or UDP port 540.
- B. You must open the ports to the Fortinet registry
- C. You must create a MEA special policy on FortiManager using the super user profile
- D. The administrator must have the super user profile.

**Answer: CD**

**NEW QUESTION 75**

- (Exam Topic 3)

View the following exhibit.



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

- 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: BC**

**NEW QUESTION 77**

- (Exam 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 82**

.....

## Thank You for Trying Our Product

\* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

\* One year free update

You can enjoy free update one year. 24x7 online support.

\* Trusted by Millions

We currently serve more than 30,000,000 customers.

\* Shop Securely

All transactions are protected by VeriSign!

**100% Pass Your NSE5\_FMG-7.0 Exam with Our Prep Materials Via below:**

[https://www.certleader.com/NSE5\\_FMG-7.0-dumps.html](https://www.certleader.com/NSE5_FMG-7.0-dumps.html)