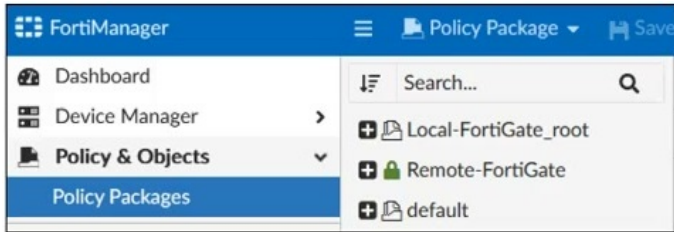




- Expert Verified, Online, **Free**.

Refer to the 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.

Suggested Answer: AD

Community vote distribution

AD (100%)

🗨️ **M3trk** 1 month ago

Selected Answer: AB

- A. Is correct because an administrator can also lock the "local-fortigate" policy package because you have enabled the "per policy option".
 - B. Is correct because you need to have workspace enable in this case is more tentative that "workflow" was enabled.
 - C. Is incorrect because if the ADOM was blocked you wouldnt see any locked policy packages. Study Guide p.57
 - D. Is incorrect because the correct ADOM "operation" mode is NORMAL, and the default setting of workspace mode is "disable". Study guide p.55
- upvoted 1 times

🗨️ **flamengo** 1 month, 2 weeks ago

Selected Answer: CD

The absence of a lock icon next to "Local-FortiGate_root" and "default" indicates that these policy packages are not locked and are available for editing. The answers correct is C and D.

upvoted 1 times

🗨️ **flamengo** 1 month, 2 weeks ago

The absence of a lock icon next to "Local-FortiGate_root" and "default" indicates that these policy packages are not locked and are available for editing. The answers correct is C and D.

upvoted 1 times

🗨️ **abirafiq** 1 month, 2 weeks ago

Selected Answer: AD

Policy lock

upvoted 1 times

🗨️ **eamstar** 1 month, 4 weeks ago

Selected Answer: AD

Answer is A & D

upvoted 1 times

🗨️ **LAFNELL** 1 month, 4 weeks ago

Selected Answer: AD

A&D

B false because there is no "sessions" tab on the toolbar before Policy package

C false because you can not have a policy package locked, in a locked ADOM

upvoted 1 times

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.

Suggested Answer: CD

Community vote distribution

CD (100%)

🗨️ 👤 **e7f2ce0** 1 month, 3 weeks ago

Selected Answer: CD

C & D is correct

upvoted 2 times

🗨️ 👤 **LAFNELL** 1 month, 3 weeks ago

Selected Answer: CD

A & B are false cause there is no disable status on FMG during configuration

upvoted 2 times

🗨️ 👤 **eamstar** 1 month, 4 weeks ago

Selected Answer: CD

Answer is C & D

upvoted 2 times


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

Suggested Answer: B

Community vote distribution

B (100%)

 **LAFNELL** 1 month, 3 weeks ago

Selected Answer: B

A is false because Revision does not permit to save the whole ADOM

C is false because ADOM Revision is related to all policy package in the ADOM, and does not concern device settings

D is false because ADOM Revision does not concern the save of all Fortimanager

Answer B

upvoted 1 times

 **MaDeInBe** 2 months ago

Selected Answer: B

B

upvoted 1 times

Refer to the exhibit.

FortiManager address object

The screenshot shows the 'Edit Address' configuration page in FortiManager. The object is named 'LOCAL_SUBNET' and is of type 'Subnet'. The IP/Netmask 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 'Advanced Options' section is expanded to show 'Per-Device Mapping'. Below this, there are buttons for '+ Create New', 'Edit', and 'Delete', along with a search bar. A table shows the mapping for the 'Local-FortiGate [root]' device, with the IP/Netmask set to '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.

Suggested Answer: B

Community vote distribution

B (100%)

Collins 1 month, 3 weeks ago

B. FortiManager installs the default value if there is no reference.

upvoted 2 times

Collins 1 month, 3 weeks ago

reference to mean per-device mapping

upvoted 1 times

LAFNELL 1 month, 3 weeks ago

Selected Answer: B

A is false

C is false, that s the value only for Local-Fortigate which has a per-device mapping

D is false because the none object is used in the case where Fortimanager installs on a device an object which has been previously deleted

answer is B

upvoted 2 times

Mahfoud_31 1 month, 4 weeks ago

in my opinion it's B

upvoted 2 times

  **Ygrec** 2 months ago

Anyone please to share ? I don't understand that one and the answer
upvoted 1 times

  **LAFNELL** 1 month, 3 weeks ago

look for my answer at the top
upvoted 1 times

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 325     FGM010000077646 -    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 device-level database.
- D. The latest revision history for the managed FortiGate does match the FortiGate running configuration.

Suggested Answer: AD

Community vote distribution

AD (60%)

AB (40%)

 **Imptcne** 1 month, 3 weeks ago

Selected Answer: AB


A,B

dev-db: modified - This status indicates that the device-level database in FortiManager has unsynchronized changes, meaning that the latest revision history stored in FortiManager does not match the configuration that was installed on the FortiGate.

conf: in sync - Since configuration changes have been installed successfully on the FortiGate from FortiManager, this status would show as "in sync." This status indicates that FortiGate's running configuration now aligns with the last installed configuration, even if the device-level database in FortiManager does not match the latest revision history.[^]

cond: pending - FortiManager knows the change was made directly on FortiGate


upvoted 1 times

 **LAFNELL** 1 month, 2 weeks ago

No

dev-db: modified, means modifications have been done on device level directly on Fortimanager, but not yet installed on managed device.

upvoted 1 times

 **Imptcne** 1 month, 2 weeks ago

you're right, after reading it again I realized that... A&D are correct!

upvoted 1 times

 **TigerL** 1 month, 3 weeks ago

Selected Answer: AD

Answer A and D

upvoted 2 times

 **LAFNELL** 1 month, 3 weeks ago

B is false cause dev-db is modified so configurations changes have not been installed

C is false cause dm is retrieved and not auto-updated

A&D are correct

upvoted 3 times

 **Radicalcactus** 1 month, 4 weeks ago

Selected Answer: AD

Correct answer is A & D

upvoted 2 times

 **eamstar** 1 month, 4 weeks ago

Selected Answer: AD

Answer is A & D

upvoted 2 times

  **MaDeInBe** 2 months ago

Selected Answer: AB

dm: retrieved is not dm: autoupdated which makes option C invalid

upvoted 2 times

  **Mahfoud_31** 2 months ago

A&D are correct

upvoted 2 times

  **Shashanka** 2 months, 1 week ago

A&D are correct.

- conf: in sync - This is the sync status which shows that the latest revision history is in sync with Fortigate's configuration.
 - There is a new modification on FortiManager device level DB (dev-db: modified) which wasn't installed to FortiGate (cond: pending)
- upvoted 4 times

Refer to the exhibit.

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

Given the configuration shown in the exhibit, what are two results from this configuration? (Choose two.)

- A. You can validate administrator login attempts through external servers.
- B. The same administrator can lock more than one ADOM at the same time.
- C. Two or more administrators can make configuration changes at the same time, in the same ADOM.
- D. Concurrent read-write access to an ADOM is disabled.

Suggested Answer: *BD*

Community vote distribution

BD (67%)

BC (33%)

🗨️ 👤 **Ispawnd_1989** 1 month, 3 weeks ago

Selected Answer: BC

B y C

B : one admin can lock multiples ADOMs same time

C : two admin can work whit diferent police package into same ADOM

D : "CHECK READ-WRITE "...Only concurrent WRITE is disable (into ADOM or policy package). read is permitted all ADOM
upvoted 2 times

🗨️ 👤 **LAFNELL** 1 month, 2 weeks ago

C is not correct

Referring the hexibit, For C, we should see the command

"set per-policy-lock enable"

There is two mode on FMG read-write, and read-only. D is definitely correct.

refer to FMG Administrator study guide page57

"Enabling Workspace mode allows you to lock different items in Fortimanager, effectively preventing concurrent read-write access to locked item."

upvoted 2 times

🗨️ 👤 **LAFNELL** 1 month, 3 weeks ago

Selected Answer: BD

B&D are correcto

upvoted 2 times

🗨️ 👤 **eamstar** 1 month, 4 weeks ago

Selected Answer: BD

Answer is B & D

upvoted 2 times

🗨️ 👤 **MaDeInBe** 2 months ago

Selected Answer: BD

Workspace mode for all adoms means that only a single admin can update an ADOM at the same time. However, nothing forbids an admin to lock several ADOMs...

<https://docs.fortinet.com/document/fortimanager/7.4.1/administration-guide/302496/workspace-mode>

<https://docs.fortinet.com/document/fortimanager/7.4.1/administration-guide/908521/enable-workspace-mode>

upvoted 3 times

Which statement about the policy lock feature on FortiManager is true?

- A. Policy locking is available in workspace normal mode.
- B. Locking a policy takes precedence over a locked ADOM.
- C. When a policy is locked, the ADOM that contains it is also locked.
- D. Administrators in the approval group can work concurrently on a locked policy.

Suggested Answer: A

Community vote distribution

A (100%)

🗨️ 👤 **LAFNELL** 1 month, 3 weeks ago

Selected Answer: A

A is correct

upvoted 3 times

🗨️ 👤 **MaDeInBe** 2 months ago

Selected Answer: A

If you want to modify a policy, you don't need to lock the entire policy package. Once you lock a policy, a padlock icon appears beside the policy. Others are now unable to modify your policy or lock the policy package where the locked policy is in, and unable to lock the ADOM.

upvoted 2 times

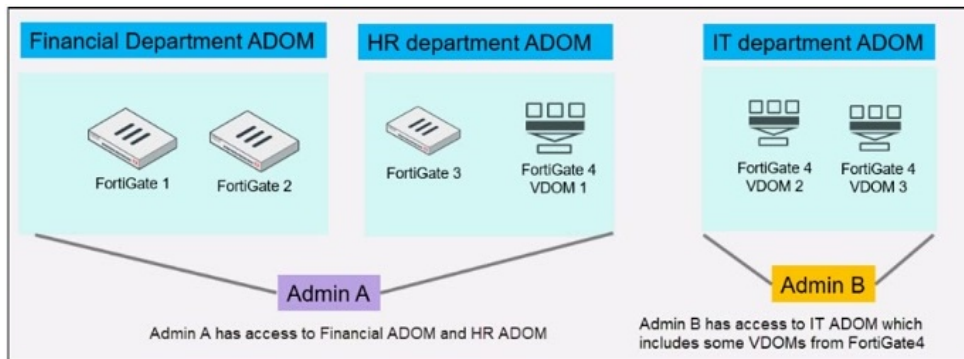
🗨️ 👤 **Shashanka** 2 months, 1 week ago

Option A is the correct answer.

Ref: FortiManager_7.4_Administrator_Study_Guide-Online - page-205

upvoted 3 times

Refer to the exhibit.



An administrator would like to create three ADOMs on FortiManager with different access levels based on departments. What two conclusions can you draw from the design shown in the exhibit? (Choose two.)

- A. The FortiManager administrator must set the ADOM device mode to Advanced.
- B. Policies and objects databases can be shared between the Financial and HR ADOMs.
- C. An administrator with the super user profile can access all the VDOMs.
- D. The administrator must configure FortiManager in workspace normal mode.

Suggested Answer: AC

Community vote distribution

AC (100%)

flamengo 1 month, 2 weeks ago

Answers A and C page 9 - FortiManager_7.4_Administrator_Study_Guide
upvoted 2 times

LAFNELL 1 month, 3 weeks ago

Selected Answer: AC

Correct answer A&C

A is mandatory

C is 100% true

D is not necessary for this question

B is false

upvoted 3 times

MaDeInBe 2 months ago

Selected Answer: AC

A is obviously required to split VDOMs over several ADOMs

B is not true

D is not asked (locking ADOM etc is not required)

so C is the other valid reply

upvoted 3 times

Which two items does an FGFM keepalive message include? (Choose two.)

- A. FortiGate IPS version
- B. FortiGate license information
- C. FortiGate configuration checksum
- D. FortiGate uptime

Suggested Answer: AC

Community vote distribution

AC (100%)

🗨️ 👤 **LAFNELL** 1 month, 3 weeks ago

Selected Answer: AC

A&C correct answers

FMG

Fortigates send keepalive messages, which content IPS version and checksum

upvoted 2 times

🗨️ 👤 **Nightwolf33** 1 month, 3 weeks ago

Selected Answer: AC

Answer is A & C

upvoted 2 times

🗨️ 👤 **eamstar** 1 month, 4 weeks ago

Selected Answer: AC

Answer is A & C

upvoted 2 times

🗨️ 👤 **MaDeInBe** 2 months ago

Selected Answer: AC

AC are the correct answers

upvoted 2 times

🗨️ 👤 **BIGFATNUTS** 2 months, 1 week ago

Selected Answer: AC

Wrong.

There is no uptime involved. Only IPS version and checksum.

upvoted 3 times

🗨️ 👤 **dadolphe** 2 months, 1 week ago

You are right !

"The keep-alive message contains information that assists the FortiManager in managing the FortiGate unit, such as

current OS version, platform, configuration checksum and versions of the unit's AV and IPS databases." - Communications Protocol Guide

FortiGate / FortiManager 7.4 page 6.

upvoted 2 times

Refer to the exhibit.

Managed FortiGate devices

| <input type="checkbox"/> | Device Name |
|--------------------------|-------------------------|
| <input type="checkbox"/> | Training |
| <input type="checkbox"/> | ISFW |
| <input type="checkbox"/> | root [NAT] (Management) |
| <input type="checkbox"/> | Student [NAT] |
| <input type="checkbox"/> | Trainer [NAT] |
| <input type="checkbox"/> | Local-FortiGate* |

FortiManager policy package

| <input type="checkbox"/> | Installation Target |
|--------------------------|-------------------------|
| <input type="checkbox"/> | Local-FortiGate |
| <input type="checkbox"/> | ISFW |
| <input type="checkbox"/> | root [NAT] (Management) |
| <input type="checkbox"/> | Trainer [NAT] |
| <input type="checkbox"/> | Student [NAT] |

FortiManager policy package

| <input type="checkbox"/> | # | Name | Install On | From | To |
|-------------------------------|---|---------------|--|-------|-------|
| <input type="checkbox"/> | 1 | Ping_Access | ISFW (root) ISFW (Student) | port3 | port1 |
| <input type="checkbox"/> | 2 | Web | Local-FortiGate (root) ISFW (Student) | port3 | port1 |
| <input type="checkbox"/> | 3 | Source_Device | Installation Targets | port3 | port1 |
| Implicit (4/4 Total:1) | | | | | |
| <input type="checkbox"/> | 4 | Implicit Deny | Installation Targets | any | any |

Given the configuration shown in the exhibit, which two conclusions can you draw from the installation targets in the Install On column? (Choose two.)

- A. Policy seq.# 3 will be installed on all managed devices and VDOMs that are listed under Installation Targets.
- B. Policy seq.# 3 will be skipped because no installation targets are specified.
- C. Policy seq.# 2 will not be installed on the Local-FortiGate root VDOM because there is no root VDOM in the Installation Target.
- D. Policy seq.# 1 will be installed on the ISFW device root[NAT] and Student[NAT] VDOMs only.

Suggested Answer: AD

Community vote distribution



☒ 👤 **LAFNELL** 1 month, 3 weeks ago

Selected Answer: AD

A&D are correct

upvoted 2 times

☒ 👤 **eamstar** 1 month, 4 weeks ago

Selected Answer: AD

Answer is A & D

upvoted 2 times

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

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

Suggested Answer: C

Community vote distribution

C (100%)

🗨️ 👤 **LAFNELL** 1 month, 3 weeks ago

Selected Answer: C

A is false cuz this is the install wizard or quick install purpose

B is false cuz auto-update is made by settings changed directly on managed device

D is definitely not correct

upvoted 2 times

🗨️ 👤 **eamstar** 1 month, 4 weeks ago

Selected Answer: C

Answer is C

upvoted 2 times

An administrator wants to create a policy on an ADOM that is in backup mode and install it on a FortiGate device in the same ADOM. How can the administrator perform this task?

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

Suggested Answer: B

Community vote distribution

B (100%)

🗨️ **LAFNELL** 1 month, 3 weeks ago

Selected Answer: B

A is false, as no conf changes possible using policy package panel when in backup mode
C is false, as there is no relationship between offline mode and this case
D is false as no relationship here too
upvoted 2 times

🗨️ **Nightwolf33** 1 month, 3 weeks ago

Selected Answer: B

Answer B is correct
upvoted 2 times

🗨️ **eamstar** 1 month, 4 weeks ago

Selected Answer: B

Correct answer is B
upvoted 2 times

🗨️ **Ygrec** 2 months ago

In my opinion. In backup mode. It is it possible to make change on the FMG? So the answer can't be A?
upvoted 1 times

🗨️ **Ygrec** 2 months ago

It's not possible to make change I mean
upvoted 1 times

🗨️ **Mahfoud_31** 2 months ago

B is correct
upvoted 2 times

🗨️ **BIGFATNUTS** 2 months, 1 week ago

Wrong.
Only scripts can be used in backup mode. Configuration changes are disabled.

upvoted 3 times

Refer to the exhibit.

FortiManager log

```

-----Executing time: -----

Starting log (Run on device)

Local-FortiGate $ config user local
Local-FortiGate (local) $ edit student
Local-FortiGate (student) $ set type ldap
Local-FortiGate (student) $ set status enable
Local-FortiGate (student) $ next
Attribute 'ldap-server' MUST be set.
Command fail. Return code 1
Local-FortiGate (local) $ end
Local-FortiGate $ config firewall policy
Local-FortiGate (policy) $ edit 2
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 users student
entry not found in datasource

value parse error before 'student'
Command fail. Return code -3
Local-FortiGate (2) $ set nat enable
Local-FortiGate (2) $ next
Local-FortiGate (policy) $ end
Local-FortiGate $

-----End of Log-----

```

What can you conclude from the failed installation log shown in the exhibit?

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

Suggested Answer: B

Community vote distribution

B (100%)

814d1c6 2 weeks, 3 days ago

Selected Answer: B

B for sure, also the policy is edited not new created since there is no message that the policy ID is new.

upvoted 2 times

0d6e481 1 month ago

Selected Answer: C

FortiManager_7.4_Administrator_Study_Guide, page 281

upvoted 2 times

LAFNELL 1 month, 3 weeks ago

Selected Answer: B

B is 100% correct

upvoted 2 times

dfd68e5 1 month, 3 weeks ago

Is B right?

upvoted 1 times

In the event that one of the secondary FortiManager devices fails, which action must be performed to return the FortiManager HA manual mode to a working state?

- A. The FortiManager HA state transition is transparent to administrators and does not require any reconfiguration.
- B. Reboot the failed device to remove its IP from the primary device.
- C. Manually promote one of the working secondary devices to the primary role, and reboot the old primary device to remove the peer IP of the failed device.
- D. Reconfigure the primary device to remove the peer IP of the failed device.

Suggested Answer: D

Community vote distribution

D (100%)

🗨️ 👤 **LAFNELL** 1 month, 3 weeks ago

Selected Answer: D

D correct for sure
upvoted 2 times

🗨️ 👤 **Nightwolf33** 1 month, 3 weeks ago

Selected Answer: D

Correct answer is D
upvoted 2 times

🗨️ 👤 **dfd68e5** 1 month, 3 weeks ago

Selected Answer: D

D the correct answer
upvoted 2 times

🗨️ 👤 **dfd68e5** 1 month, 3 weeks ago

D guys
upvoted 2 times

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 happens to the Fortinet policy package when it is created?

- A. You must assign the global policy package from the global ADOM.
- B. The global policy package is automatically assigned.
- C. You must reapply the global policy package to ADOM1.
- D. You can select the option to assign the global policies.

Suggested Answer: D

Community vote distribution

B (100%)

814d1c6 2 weeks, 4 days ago

Selected Answer: B

This is automatically done
upvoted 2 times

LAFNELL 1 month, 3 weeks ago

Selected Answer: B

B correct
upvoted 2 times

eamstar 1 month, 4 weeks ago

Selected Answer: B

Answer is B
upvoted 2 times

Atn 1 month, 4 weeks ago

Correct answer B
upvoted 2 times

Which output is displayed right after moving the ISFW device from one ADOM to another?

A.

B.

```
FortiManager # diagnose dvm device list ISFW
--- There are currently 4 devices/vdoms managed ---
--- There are currently 4 devices/vdoms count for license ---

TYPE          OID      SN              HA      IP          NAME          ADOM      IPS          FIRMWARE
fmgfaz-managed 325     FGVM010000077646 -      10.0.1.200  ISFW          ADOM74    6.00741 (regular) 7.0 MR4 (2463)
|- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: retrieved; conn: up
|- vdom:[3]root flags:0 adom:ADOM74 pkg:[unknown]ISFW
```

C.

```
FortiManager # diagnose dvm device list ISFW
--- There are currently 4 devices/vdoms managed ---
--- There are currently 4 devices/vdoms count for license ---

TYPE          OID      SN              HA      IP          NAME          ADOM      IPS          FIRMWARE
fmgfaz-managed 325     FGVM010000077646 -      10.0.1.200  ISFW          ADOM74    6.00741 (regular) 7.0 MR4 (2463)
|- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: autoupdated; conn: up
|- vdom:[3]root flags:1 adom:ADOM74 pkg:[out-of-sync]ISFW
```

D.

```
FortiManager # FortiManager # diagnose dvm device list ISFW
--- There are currently 4 devices/vdoms managed ---
--- There are currently 4 devices/vdoms count for license ---

TYPE          OID      SN              HA      IP          NAME          ADOM      IPS          FIRMWARE
fmgfaz-managed 325     FGVM010000077646 -      10.0.1.200  ISFW          ADOM74    6.00741 (regular) 7.0 MR4 (2463)
|- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: installed; conn: up
|- vdom:[3]root flags:0 adom:ADOM74 pkg:[never-installed]
```

```
FortiManager # diagnose dvm device list ISFW
--- There are currently 4 devices/vdoms managed ---
--- There are currently 4 devices/vdoms count for license ---

TYPE          OID      SN              HA      IP          NAME          ADOM      IPS          FIRMWARE
fmgfaz-managed 325     FGVM010000077646 -      10.0.1.200  ISFW          ADOM74    6.00741 (regular) 7.0 MR4 (2463)
|- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: installed; conn: up
|- vdom:[3]root flags:0 adom:ADOM74 pkg:[imported]ISFW
```

Suggested Answer: D

Community vote distribution

C (50%)

A (50%)

 Charly0710 2 weeks ago

Selected Answer: A


The output that is displayed immediately after moving the ISFW device from one ADOM to another is Option A, where the package status is still unknown (pkg: [unknown]) because FortiManager has not yet fully synchronized the device's configuration in the new ADOM.

upvoted 1 times

 flamengo 4 weeks ago

Answer D

upvoted 1 times

 Nitty1s 1 month, 2 weeks ago

Selected Answer: C

Tested it. Will show "never installed"

upvoted 4 times

 Sparo 1 month, 2 weeks ago

Unknown with policy package name:

Gray question mark

Configurations of the managed device are retrieved on FortiManager after being imported/installed.

For example, when you retrieve a policy package after upgrading FortiOS, the policy package status changes to Unknown.

upvoted 1 times

 Sparo 1 month, 2 weeks ago



Selected Answer: C

Out of Sync - Policies or objects are modified on the managed device.

Never Installed - The assigned policy package is not the result of an import for this device, and the package has not been installed since it has been assigned to this device.

I think its C


upvoted 2 times

  **Imptcne** 1 month, 3 weeks ago

Selected Answer: A


it should be A as the device is not currently linked to any policy package in the new ADOM

upvoted 1 times

  **LAFNELL** 1 month, 2 weeks ago

No the status unknown, just means FMG is unable to determine the pkg status. But here we are talking about after migrating device to another ADOM. the status after migration is "never installed"

upvoted 1 times

  **LAFNELL** 1 month, 3 weeks ago

Selected Answer: C

Correct Answer is the third one.

The policy Package will show never installed, once an import configuration is launched in the new ADOM

upvoted 2 times

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 third-party applications to gain read/write access to FortiManager.
- D. It allows FortiManager to determine the connection status of managed devices.

Suggested Answer: B

Community vote distribution

B (100%)

🗨️ 👤 **LAFNELL** 1 month, 3 weeks ago

Selected Answer: B

Answer B is correct
upvoted 2 times

🗨️ 👤 **dfd68e5** 1 month, 3 weeks ago

B correct
upvoted 2 times

Refer to the exhibit.

FortiManager Managed FortiGate devices

| Device Name | Config Status | Host Name | Policy Package Status | IP Address | Platform |
|-------------|---------------|-----------|-----------------------|------------|-----------|
| ISFW | Unknown | ISFW | Never Installed | 10.0.1.200 | FortiGate |

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

- A. The administrator must refresh the device to restore connectivity.
- B. FortiManager lost internet connectivity, therefore, the device appears to be down.
- C. The administrator can reclaim the FortiGate to FortiManager protocol (FGFM) tunnel to get the device online.
- D. The administrator recently restored a FortiManager configuration file.

Suggested Answer: C

Community vote distribution

D (100%)

terminatoritsec 1 month, 1 week ago

Selected Answer: D

D is the only possible match.
upvoted 2 times

Sparo 1 month, 2 weeks ago

Selected Answer: D

D is Correct
upvoted 2 times

LAFNELL 1 month, 3 weeks ago

Selected Answer: D

Answer is D
FMG is in offline mode, which is activated after restoring a configuration file
upvoted 2 times

79fad4e 1 month, 3 weeks ago

Selected Answer: D

By default, offline mode is enabled when a Fortimanager backup is restored.
upvoted 2 times

e7f2ce0 1 month, 3 weeks ago

off line mode, D is correct
upvoted 2 times

e7f2ce0 1 month, 3 weeks ago



Selected Answer: D

D is correct
upvoted 2 times

Atn 1 month, 3 weeks ago

Correct answer D

upvoted 2 times

  **dfd68e5** 1 month, 3 weeks ago

Any suggestions?

upvoted 1 times

Refer to the exhibit.

FortiManager managed devices

The screenshot displays the FortiManager interface for managed devices. On the left, a sidebar lists device groups: Managed FortiGate (3), ISFW, Local-FortiGate, Remote-FortiGate, Managed FortiAnalyzer (1), and FAZVM64-KVM. The main area features two donut charts: 'Connectivity' showing 3 devices connected, and 'Device Config Sta...' showing 3 devices with 2 auto-updated and 1 modified. Below the charts is a table of managed devices with columns for Device Name, Config Status, IP Address, Policy Package Status, and Platform. A context menu is open over the 'Remote-FortiGate' device, showing options: Install Wizard, Quick Install (Device DB) (highlighted), and Re-install Policy.

| Device Name | Config Status | IP Address | Policy Package Status | Platform |
|------------------|-------------------|------------|-----------------------|-------------|
| Remote-FortiGate | Modified (recent) | 10.200.3.1 | Remote-FortiGate | FortiGate-V |
| ISFW | Auto-update | 10.200.1.1 | Never Installed | FortiGate-V |
| Local-FortiGate* | Auto-update | 10.200.1.1 | Local-FortiGate_root | FortiGate-V |

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

Suggested Answer: CD

Community vote distribution

AD (100%)

SingSingHK 4 days, 18 hours ago

Selected Answer: CD

as per description in 7.4 admin guide, I think C & D are correct. <https://docs.fortinet.com/document/fortimanager/7.4.0/administration-guide/379044/quick-install-device-db>

upvoted 1 times

LAFNELL 1 month, 3 weeks ago

Selected Answer: AD

A&D are correct

B&C are false, With Quick install no preview before the installation of changes, nothing to do on the managed device

upvoted 2 times

eamstar 1 month, 4 weeks ago

Selected Answer: AD

Answer is A & D

upvoted 2 times

dadolphe 2 months, 1 week ago

Selected Answer: AD

I think it's AD, there is no need to reinstall after a quick install.

upvoted 2 times

Refer to the exhibit.

FortiManager CLI output

```
FortiManager # execute top
top - 13:08:23 up 1 day,  1:01,  0 users,  load average: 2.40, 3.19, 3.34

Tasks: 188 total,  2 running, 186 sleeping,  0 stopped,  0 zombie

%Cpu(s): 15.4 us,  7.7 sy,  0.0 ni, 76.9 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st

MiB Mem : 7955.5 total,  2235.6 free,  2895.6 used,  2824.1 buff/cache

MiB Swap: 2048.0 total,  2048.0 free,  0.0 used.  4011.0 avail Mem

  PID USER      PR  NI   VIRT   RES  %CPU  %MEM     TIME+ S COMMAND
 1163 root       20   0   17.6m   2.1m   7.1   0.1   0:00.05 R top
    1 root       20   0  602.2m  14.9m   0.0   0.7   0:11.67 S /bin/initXXXXXXXXXX
    2 root       20   0    0.0m   0.0m   0.0   0.0   0:00.00 S [kthreadd]
 1462 root       20   0  303.2m 248.0m   0.0   3.1   0:14.72 S fwmsvrd
 1463 root       20   0  288.2m 232.3m   0.0   2.9   0:16.47 S fgdlinkd
 1465 root       20   0  383.7m 328.0m   0.0   4.1   0:15.26 S fgdsvr
 1467 root       20   0   84.0m  23.6m   0.0   0.3   0:00.06 S /bin/fgdhttpd
 1468 root       20   0   63.9m  13.1m   0.0   0.2   0:13.00 S fgdupd
 1469 root       20   0   63.5m  12.6m   0.0   0.2   0:00.07 S fmtr_svrd
 1470 root       20   0    6.3m   3.5m   0.0   0.0   0:00.09 S /bin/webconsoled
 1471 root       20   0  996.4m 850.6m   0.0  10.7   0:00.01 S srchd
 1475 root       20   0  996.4m 120.6m   0.0   1.5   0:00.00 S fclinkd
```

What percent of the available RAM is being used by the process in charge of downloading the web and email filter databases from the public FortiGuard servers?

- A. 2.9
- B. 3.1
- C. 1.5
- D. 4.1

Suggested Answer: A


Community vote distribution

A (100%)

 **LAFNELL** 1 month, 3 weeks ago

Selected Answer: A

fgdlinkd is the process responsible for downloading wf and email filter db
upvoted 3 times

 **e7f2ce0** 1 month, 3 weeks ago

Selected Answer: A

The fgdlinkd process on FortiManager is responsible for downloading web-filter and email-filter databases from public FortiGuard servers, providing up-to-date security threat protection
upvoted 3 times

 **dfd68e5** 1 month, 3 weeks ago

Is this correct?

upvoted 2 times

Refer to the exhibit.

FortiManager script

Create New Script

Script Name:

Comments:

Type:

Run script on:

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

```

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

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

Suggested Answer: AD

Community vote distribution

AD (100%)

LAFNELL 1 month, 3 weeks ago

Selected Answer: AD

A is correct, as the script is installed on device db, and not directly on the fortigate CLI

D is correct, the device config will show status modified like whenever you do some changes using fortimanager and you don't install them.

upvoted 3 times

Collins 1 month, 2 weeks ago

Once scripts are run on the device database, you can then install the changes on a managed device using the installation wizard.

Since the script changed the device settings in FortiManager, the Config Status shows "Modified" and needs to be installed with Installation Wizard.

upvoted 2 times

dfd68e5 1 month, 3 weeks ago

Someone help!

upvoted 1 times

Push updates are failing on a FortiGate device that is located behind a NAT device.

Which two settings should the administrator check? (Choose two.)

- A. That the override server IP address is set on FortiManager and the NAT device
- B. That the external IP address on the NAT device is set to DHCP and configured with the virtual IP
- C. That the NAT device IP address and correct ports are configured on FortiManager
- D. That the virtual IP address and correct ports are set on the NAT device

Suggested Answer: CD

Community vote distribution

CD (83%)

AC (17%)

🗨️ 👤 **LAFNELL** 1 month, 3 weeks ago

Selected Answer: CD

C and D are correct

FMG should contact NAT ip address and NAT device should have VIP correctly configured
upvoted 4 times

🗨️ 👤 **Alessiocre** 1 month, 3 weeks ago

Selected Answer: CD

I think C and D

upvoted 3 times

🗨️ 👤 **dfd68e5** 1 month, 3 weeks ago

Selected Answer: AC

A and C

upvoted 1 times

🗨️ 👤 **dfd68e5** 1 month, 3 weeks ago

Sorry I mean C and D

upvoted 2 times

Refer to the exhibit.

| Metadata Variables | | CLI Configurations | |
|----------------------------------|-------------|--------------------|--|
| + Create New Edit Delete ⋮ | | | |
| <input type="checkbox"/> | Name | ↕ | |
| <input type="checkbox"/> | DMZ_SUBNET | | |
| <input type="checkbox"/> | ISP1_SUBNET | | |
| <input type="checkbox"/> | LAN_SUBNET | | |

What is true about the objects highlighted in the image?

- A. They can be set to optional or required.
- B. They are available across all ADOMs by default.
- C. They can be used as variables in scripts.
- D. They cannot be created in the global database ADOM.

Suggested Answer: C

Community vote distribution

C (100%)

🗨️ **Miznasty** 1 month, 2 weeks ago

A is correct, FMG 7.4 admin guide
upvoted 1 times

🗨️ **Miznasty** 1 month, 2 weeks ago

nevermind, i was looking at Meta, not Metadata
upvoted 1 times

🗨️ **LAFNELL** 1 month, 3 weeks ago

Selected Answer: C

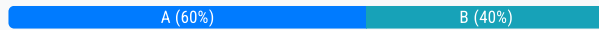
C is correct
Check FMG 7.4 Administrator study guide
upvoted 1 times

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

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

Suggested Answer: A

Community vote distribution



🗨️ **Sparo** 1 month, 3 weeks ago

Selected Answer: B

B is correct

upvoted 1 times

🗨️ **TigerL** 1 month, 3 weeks ago

Selected Answer: A

OSPF configurations are made on device-level database. Be sure to activate the feature visibility in device & groups menu.

upvoted 2 times

🗨️ **LAFNELL** 1 month, 3 weeks ago

Selected Answer: A

OSPF configurations are made on device-level database. Be sure to activate the feature visibility in device & groups menu.

A is the correct answer

upvoted 3 times

🗨️ **LAFNELL** 1 month, 3 weeks ago

Selected Answer: B

B is correct

upvoted 1 times

🗨️ **LAFNELL** 1 month, 3 weeks ago

Moderator, don't approve this answer sorry it's not correct. A is the correct one

upvoted 3 times

Which statement about the upgrade of ADOMs on FortiManager is true?

- A. To ensure database consistency, you must upgrade an ADOM before you upgrade the devices in it.
- B. Upgrading the FortiManager version upgrades all existing ADOMs automatically.
- C. You cannot import policies from a device until its FortiOS version matches the ADOM version.
- D. ADOMs using global objects can be upgraded before or after upgrading the global database ADOM.

Suggested Answer: C

Community vote distribution

C (100%)

 **rigonet** 1 week, 3 days ago

Selected Answer: C

Correct answer: C. You cannot import policies from a device until its FortiOS version matches the ADOM version.

Explanation: A. Incorrect. Devices should first be upgraded to the desired firmware, then the ADOM version. Reference: Study Guide, p. 65.

B. Incorrect. ADOM upgrades are manual after a FortiManager firmware upgrade. Reference: FortiManager Administration Guide, p. 60-62.

C. Correct in earlier versions. Policy imports required matching FortiOS and ADOM versions. This restriction was removed in later versions. Reference: FortiManager Administration Guide, earlier versions (7.4.1 behavior) and newer versions (7.4.6 behavior).

D. Incorrect. The global database ADOM must be upgraded after all dependent ADOMs. Reference: FortiManager Administration Guide, p. 883.
upvoted 1 times

 **Tweefo** 2 weeks, 3 days ago

Selected Answer: A

I'd say A.

C is not fully accurate because there is some flexibility depending on compatibility. This makes A the most correct answer because upgrading the ADOM first ensures consistency and prevents potential issues.

upvoted 2 times

 **LAFNELL** 1 month, 3 weeks ago

Selected Answer: C

C is correct

upvoted 2 times

 **aa0v1snjr9** 1 month, 3 weeks ago

i'm not sure because if i have ADOM 7.2 i can import policy from Fortios 7.4

upvoted 1 times

 **LAFNELL** 1 month, 2 weeks ago

Exactly mister. the "match" is the key word. ADOM in 7.0 is ok with devices in 7.2, ADOM in 7.2 is ok with devices in 7.0,7.2 and 7.4. But my interrogation was about answer D. I think D is not correct as well, that s why i chose C (A & B are not correct for sure). Little doubt between C and D in fact

upvoted 1 times

 **dfd68e5** 1 month, 3 weeks ago

Selected Answer: C

True C

upvoted 1 times

An administrator created a new global policy package that includes header and footer policies and then assigned it to an ADOM. What are two outcomes of this action? (Choose two.)

- A. To assign another global policy package later to the same ADOM, you must unassign this policy first.
- B. After you assign the global policy package to an ADOM, the impacted policy packages become hidden in that ADOM.
- C. You can editor delete all the global objects in the global ADOM.
- D. You must manually move the header and footer policies after the policy assignment.

Suggested Answer: AB

Community vote distribution

AC (100%)

🗨️ **LAFNELL** 1 month, 3 weeks ago

Selected Answer: AC

i go for A and C because i am sure B and D are false.
but there is something weird

on FMG you can assign two differents global policy package to the same ADOM at same time but on different policy package in that ADOM. No need to unassign one of them first.

But you cannot assign a new global policy package to the "same policy" in an ADOM without unassign first the other one already assigned.
upvoted 2 times

🗨️ **79fad4e** 1 month, 3 weeks ago

Selected Answer: AC

A AND C IS CORRECT
upvoted 2 times

🗨️ **dfd68e5** 1 month, 3 weeks ago

Selected Answer: AC

A and C
upvoted 2 times

Which configuration setting for FortiGate is part of an ADOM-level database on FortiManager?

- A. NSX-T Service Template
- B. Routing
- C. SNMP
- D. Security profiles

Suggested Answer: D

Community vote distribution

D (100%)

 **rigonet** 1 week, 5 days ago

Selected Answer: D

correct answer is:

D. Security profiles.

Explanation:

Security profiles are part of the ADOM-level database in FortiManager. These configurations allow for centralized management of security settings like antivirus, web filtering, application control, and intrusion prevention. Security profiles are created and managed under the Policy & Objects section, which operates at the ADOM level.

Incorrect Options:

- A. NSX-T Service Template: This is not directly related to ADOM-level databases but rather specific to integration with VMware NSX-T.
- B. Routing: Routing configurations are managed at the device level, not at the ADOM database level.
- C. SNMP: SNMP is configured at the device or system level, not part of the ADOM database.

upvoted 1 times

 **LAFNELL** 1 month, 3 weeks ago

Selected Answer: D

Answer D is correct

upvoted 3 times

Refer to the exhibit which shows the Download Import Report.

```
Start to import config from device(Remote-FortiGate) vdom(root) to
adam(root), package(Remote-FortiGate_root)
```

```
"firewall address",SKIPPED,"(name=all, oid=2309, DUPLICATE)"
```

```
"firewall address",FAIL,"(name=REMOTE_SUBNET, oid=2311,
reason=interface((firewall address:REMOTE_SUBNET) any<-port6) binding
fail)"
```

```
"firewall policy",FAIL,"(name=1, oid=3070, reason=interface(interface binding
contradiction. detail: (firewall address:REMOTE_SUBNET) any<-port6) binding
fail)"
```

Why is FortiManager failing to import firewall policy ID 1?

- A. Policy ID 1 is configured from the interface any to port6. FortiManager rejects the request to import this policy because the any interface does not exist on FortiManager.
- B. Policy ID 1 for this managed FortiGate already exists on FortiManager in the policy package named Remote-FortiGate.
- C. Policy ID 1 has an address object that already exists in the ADOM database with any as the interface association, and conflicts with the address object interface association locally on FortiGate.
- D. Policy ID 1 does not have the ADOM interface mapping configured on FortiManager.

Suggested Answer: C

Community vote distribution

C (100%)

🗨️ 👤 **LAFNELL** 1 month, 3 weeks ago

Selected Answer: C

C is correct

upvoted 3 times

🗨️ 👤 **dfd68e5** 1 month, 3 weeks ago

C is true

upvoted 2 times

What must you consider before deciding to use FortiManager to manage a FortiAnalyzer device?

- A. Confirm that FortiManager has enough storage capacity for the expected logs.
- B. Ensure that FortiAnalyzer features are installed in advance.
- C. Check whether FortiManager is part of a high availability (HA) cluster.
- D. Determine whether the VDOMs of the same FortiGate will be assigned to different ADOMs.

Suggested Answer: A

Community vote distribution

D (100%)

 **rigonet** 1 week, 3 days ago

Selected Answer: C

Correct answer: C. Check whether FortiManager is part of a high availability (HA) cluster.

Correct. Enabling FortiAnalyzer features is not possible if FortiManager is already in HA mode. HA must be disabled before enabling FortiAnalyzer features.

Reference: FortiManager Administration Guide, p. 38.

Explanation:

A. Incorrect. Logs are stored on FortiAnalyzer, not FortiManager, so storage capacity on FortiManager is not relevant.

Reference: FortiManager Administration Guide, p. 123.


B. Incorrect. FortiAnalyzer features must be enabled on FortiManager, but the critical point is that this cannot be done if FortiManager is already part of an HA cluster.

Reference: FortiManager Administration Guide, p. 38.

D. Incorrect. This applies to FortiGate devices managed in FortiManager and does not directly concern FortiAnalyzer management.

Reference: FortiManager Administration Guide, p. 113.

upvoted 1 times

 **LAFNELL** 1 month, 3 weeks ago

Selected Answer: D

D is correct. When FMG is managing a FAZ, you cannot switch to advanced mode. And it s only in advanced mode Vdoms of the same Fortigate can be assigned to differents ADOM

upvoted 4 times

 **aa0v1snjr9** 1 month, 3 weeks ago

I don't found any correct response.

A Wrong because the logs kept on the FAZ

B Wrong because if FMG manage FAZ is not need enable FAZ feature

C should be wrong because i don't find anything about it

D wrong because it's not relevant about question

upvoted 1 times

 **LAFNELL** 1 month, 2 weeks ago

D is completely relevant, PAY ATTENTION.

if different VDOMs of the same Fortigate will be managed in different ADOM, FMG should be configure in advanced mode. But if you manage a Fortianalyzer, you cannot configure FMG in Advanced Mode.

upvoted 1 times

 **dfd68e5** 1 month, 3 weeks ago

Any suggestions?

upvoted 1 times