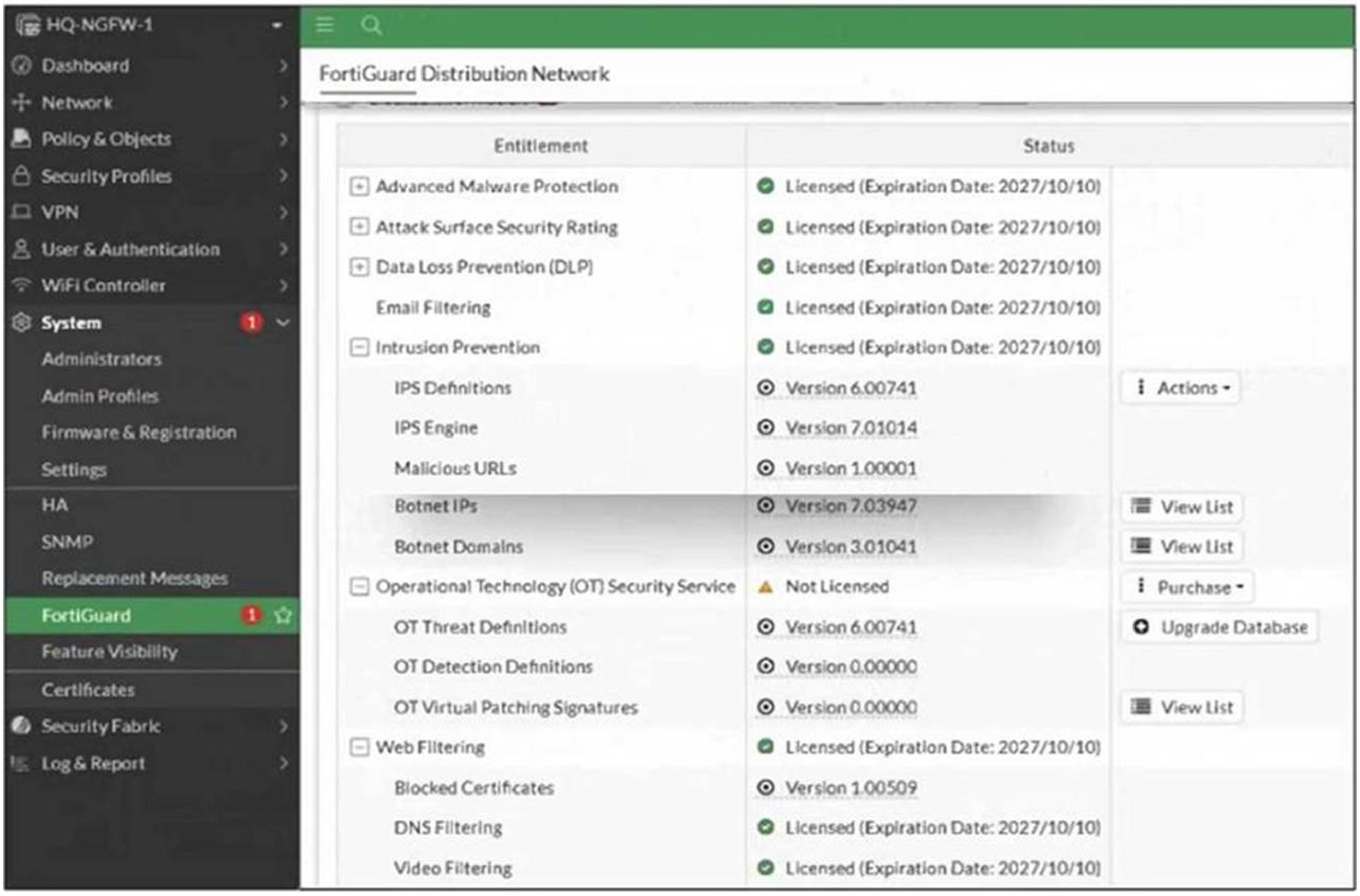
Exam Questions FCP_FMG_AD-7.6

FCP - FortiManager 7.6 Administrator

https://www.2passeasy.com/dumps/FCP_FMG_AD-7.6/

NEW QUESTION 1
Refer to the exhibits

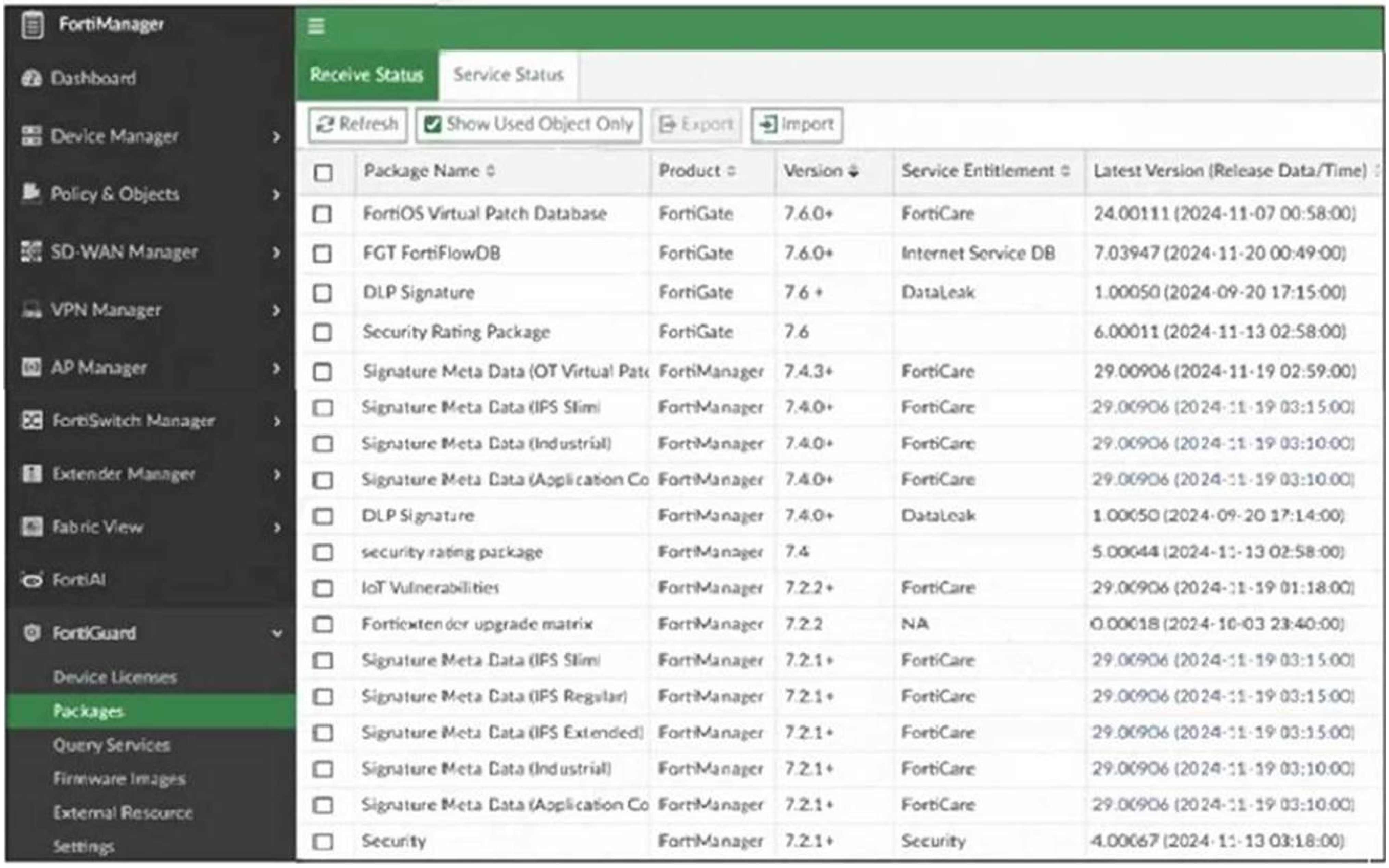
FortiGate GUI—FortiGuard



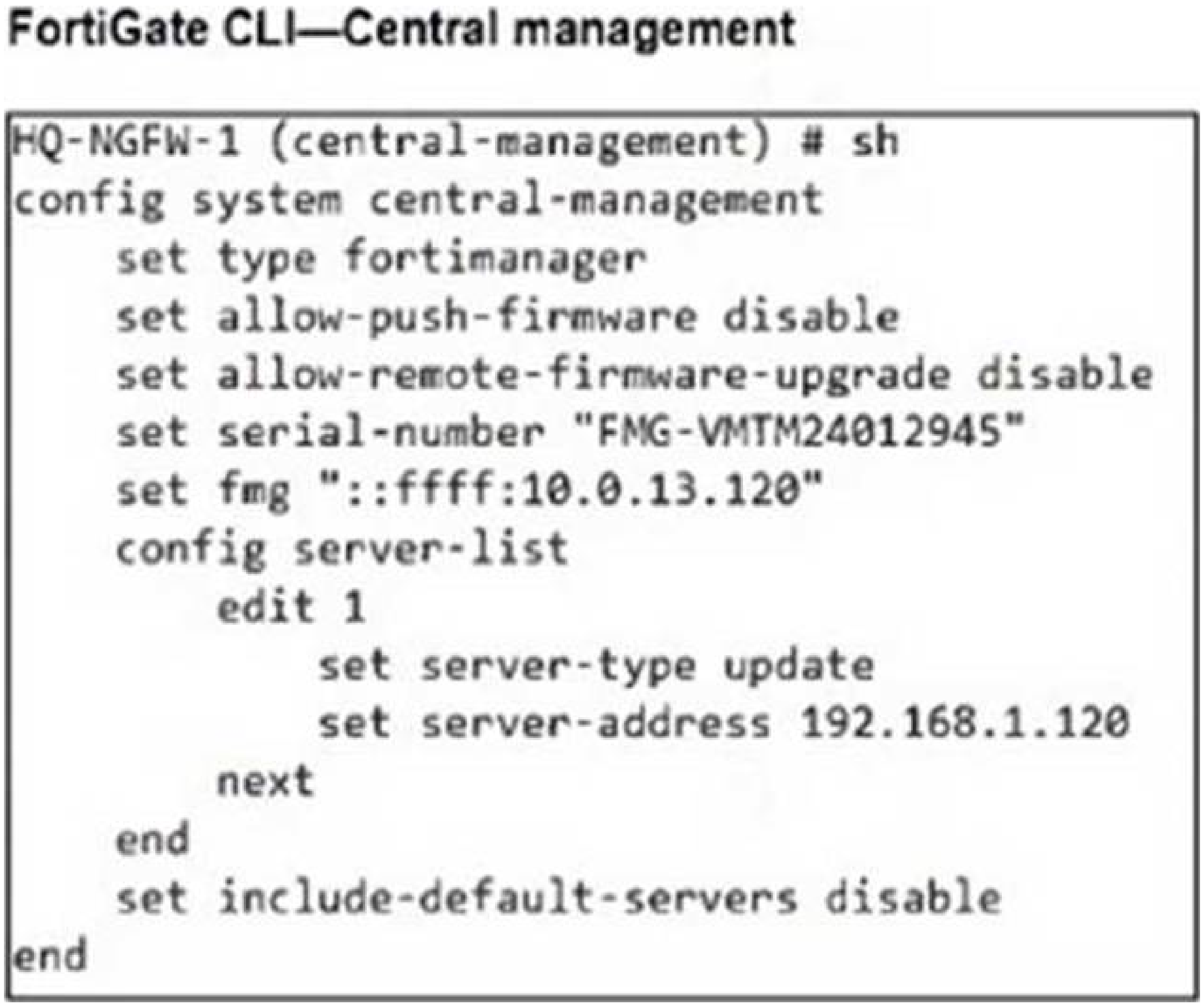
FortiGuard Distribution Network

Entitlement	Status	
⊞ Advanced Malware Protection	● Licensed (Expiration Date: 2027/10/10)	
⊞ Attack Surface Security Rating	● Licensed (Expiration Date: 2027/10/10)	
⊞ Data Loss Prevention (DLP)	● Licensed (Expiration Date: 2027/10/10)	
Email Filtering	● Licensed (Expiration Date: 2027/10/10)	
⊟ Intrusion Prevention	● Licensed (Expiration Date: 2027/10/10)	
IPS Definitions	⊙ Version 6.00741	Actions ▾
IPS Engine	⊙ Version 7.01014	
Malicious URLs	⊙ Version 1.00001	
Botnet IPs	⊙ Version 7.03947	View List
Botnet Domains	⊙ Version 3.01041	View List
⊟ Operational Technology (OT) Security Service	▲ Not Licensed	Purchase ▾
OT Threat Definitions	⊙ Version 6.00741	Upgrade Database
OT Detection Definitions	⊙ Version 0.00000	
OT Virtual Patching Signatures	⊙ Version 0.00000	View List
⊟ Web Filtering	● Licensed (Expiration Date: 2027/10/10)	
Blocked Certificates	⊙ Version 1.00509	
DNS Filtering	● Licensed (Expiration Date: 2027/10/10)	
Video Filtering	● Licensed (Expiration Date: 2027/10/10)	

FortiManager GUI—FortiGuard



□	Package Name	Product	Version	Service Entitlement	Latest Version (Release Data/Time)
□	FortiOS Virtual Patch Database	FortiGate	7.6.0+	FortiCare	24.00111 (2024-11-07 00:58:00)
□	FGT FortiFlowDB	FortiGate	7.6.0+	Internet Service DB	7.03947 (2024-11-20 00:49:00)
□	DLP Signature	FortiGate	7.6 +	DataLeak	1.00050 (2024-09-20 17:15:00)
□	Security Rating Package	FortiGate	7.6		6.00011 (2024-11-13 02:58:00)
□	Signature Meta Data (OT Virtual Patc	FortiManager	7.4.3+	FortiCare	29.00906 (2024-11-19 02:59:00)
□	Signature Meta Data (IPS Slim)	FortiManager	7.4.0+	FortiCare	29.00906 (2024-11-19 03:15:00)
□	Signature Meta Data (Industrial)	FortiManager	7.4.0+	FortiCare	29.00906 (2024-11-19 03:10:00)
□	Signature Meta Data (Application Co	FortiManager	7.4.0+	FortiCare	29.00906 (2024-11-19 03:10:00)
□	DLP Signature	FortiManager	7.4.0+	DataLeak	1.00050 (2024-09-20 17:14:00)
□	security rating package	FortiManager	7.4		5.00044 (2024-11-13 02:58:00)
□	IoT Vulnerabilities	FortiManager	7.2.2+	FortiCare	29.00906 (2024-11-19 01:18:00)
□	Fortiextender upgrade matrix	FortiManager	7.2.2	NA	0.00018 (2024-10-03 23:40:00)
□	Signature Meta Data (IPS Slim)	FortiManager	7.2.1+	FortiCare	29.00906 (2024-11-19 03:15:00)
□	Signature Meta Data (IPS Regular)	FortiManager	7.2.1+	FortiCare	29.00906 (2024-11-19 03:15:00)
□	Signature Meta Data (IPS Extended)	FortiManager	7.2.1+	FortiCare	29.00906 (2024-11-19 03:15:00)
□	Signature Meta Data (Industrial)	FortiManager	7.2.1+	FortiCare	29.00906 (2024-11-19 03:10:00)
□	Signature Meta Data (Application Co	FortiManager	7.2.1+	FortiCare	29.00906 (2024-11-19 03:10:00)
□	Security	FortiManager	7.2.1+	Security	4.00067 (2024-11-13 03:18:00)



FortiGate CLI—Central management

```
HQ-NGFW-1 (central-management) # sh
config system central-management
    set type fortimanager
    set allow-push-firmware disable
    set allow-remote-firmware-upgrade disable
    set serial-number "FMG-VMTM24012945"
    set fmg "::ffff:10.0.13.120"
    config server-list
        edit 1
            set server-type update
            set server-address 192.168.1.120
        next
    end
    set include-default-servers disable
end
```

FortiGate HQ-NGFW-1 downloads and validates FortiGuard databases from FortiManager which acts as a local FortiGuard Distribution Server (FDS) in a closed network. An administrator pushes a new firewall policy with an intrusion prevention system (IPS) profile from FortiManager to FortiGate HQ- NGFW-1 However, FortiGate does not recognize the new IPS signature from FortiManager.
What is the most likely reason why FortiGate HQ-NGFW-1 does not recognize the new IPS signature?

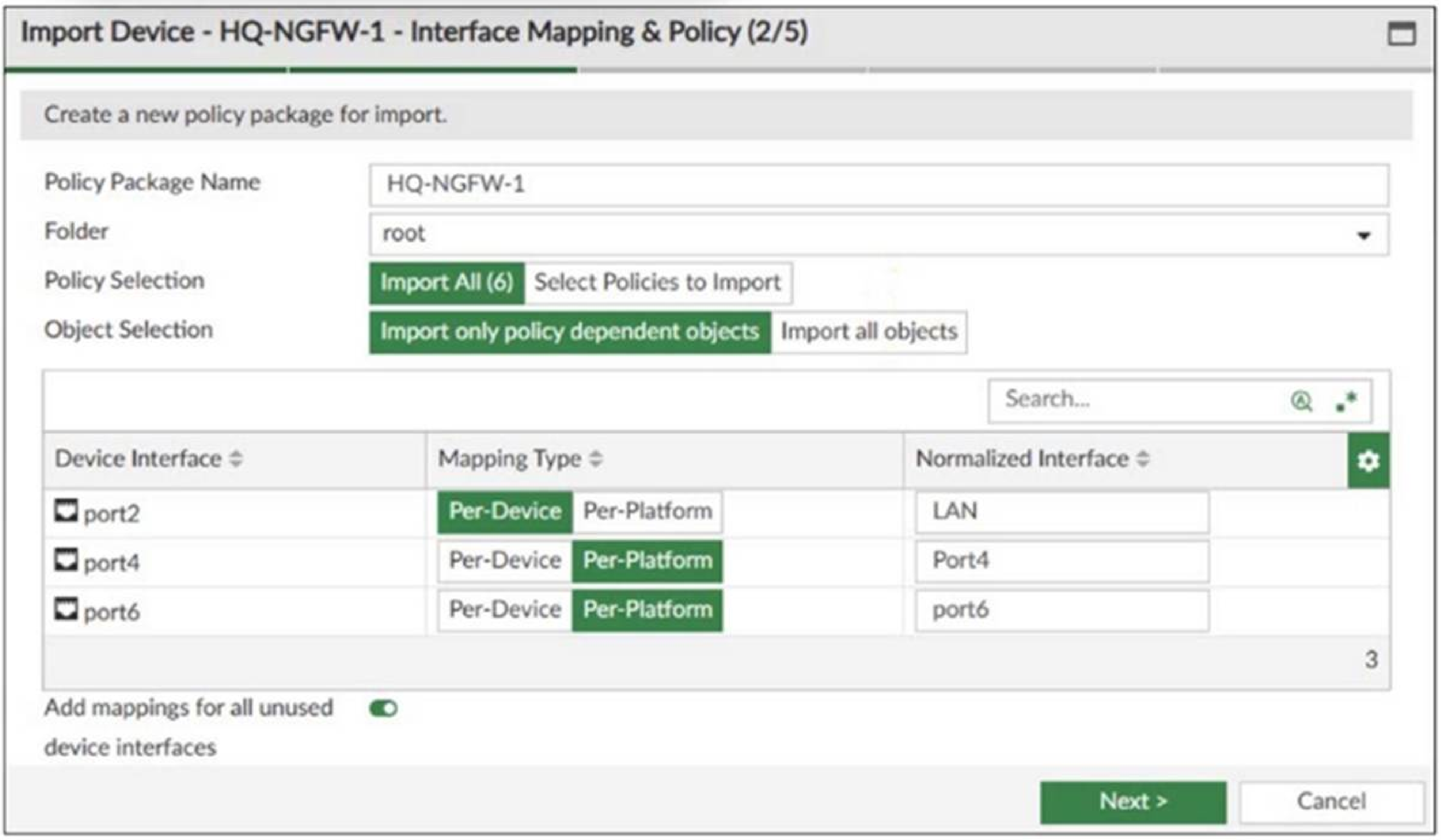
A. FortiGate must enable rating for the FortiManager IP address, 192.168.1.120, in server list 1.
B. FortiManager and FortiGate have different IPS database versions.
C. The administrator must enable IPv6 connections for FortiGuard services on FortiManager.
D. The administrator must enable the fortiguard-anycast option to correctly download all signatures from the local FDS.

Answer: B

Explanation:
The most likely reason FortiGate HQ-NGFW-1 does not recognize the new IPS signature is that FortiManager and FortiGate have different IPS database versions. The FortiManager may have pushed a signature update that FortiGate has not yet synchronized or validated locally, causing the signature to be unrecognized.

NEW QUESTION 2
Refer to the exhibit.

FortiManager policy package



Import Device - HQ-NGFW-1 - Interface Mapping & Policy (2/5)

Create a new policy package for import.

Policy Package Name	HQ-NGFW-1
Folder	root
Policy Selection	[✓ Import All (6)] Select Policies to Import
Object Selection	[✓ Import only policy dependent objects] Import all objects

Device Interface	Mapping Type	Normalized Interface
port2	[✓ Per-Device] Per-Platform	LAN
port4	Per-Device [✓ Per-Platform]	Port4
port6	Per-Device [✓ Per-Platform]	port6

3

Add mappings for all unused device interfaces: enabled

An administrator added a FortiGate device to FortiManager with the default object settings at the ADOM layer.
What can you conclude from the import policy package process of the HQ-NGFW- 1 device?

A. The administrator must select Per Platform for all interfaces to correctly detect all interfaces from HQ- NGFW-1.
B. The administrator must manually create the port4 interface on the ADOM layer to avoid import policy errors.
C. FortiManager will create LAN, port4, and port6 as normalized interfaces at the ADOM layer.
D. FortiGate may not work as expected when the administrator does not import all objects.

Answer: C

Explanation:
The import process shows that FortiManager will create normalized interfaces named LAN, port4, and port6 at the ADOM layer, mapping them to the corresponding device interfaces based on the import settings.

NEW QUESTION 3
An administrator must create a policy and install it on a FortiGate device within an ADOM in backup mode. How can the administrator perform this task?

A. Use the Install Wizard located on the device manager.
B. Enable workflow mode to allow policy creation and approval.
C. Make sure the ADOM and FortiGate firmware versions match and use the ADOM policy package.
D. Use a FortiManager script to apply the configuration changes.

Answer: D

Explanation:
In backup mode, FortiManager does not directly manage policy installation via the usual ADOM policy packages; instead, administrators use FortiManager scripts to push configuration changes, including policies, to FortiGate devices.

NEW QUESTION 4
An administrator has assigned a global policy package to a new ADOM named ADOM1.
What will happen if the administrator tries to create a new policy package in ADOM1?

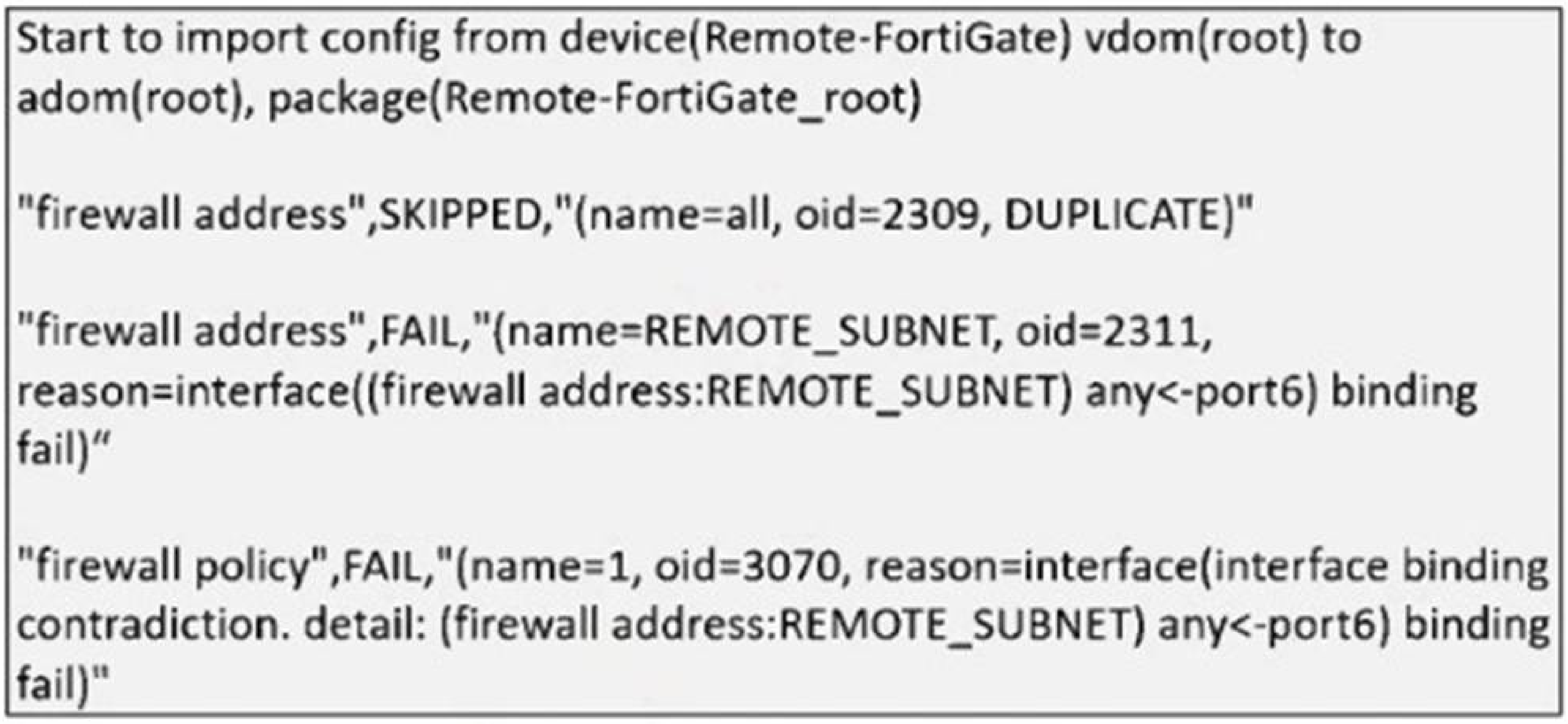
A. The administrator will be able to select the option to assign the global policy package to the new policy package.
B. FortiManager will automatically assign the global policy package to the new policy package.
C. FortiManager will automatically install policies on the policy package in ADOM1.
D. The administrator will have to assign the global policy package from the global ADOM.

Answer: A

Explanation:
When a global policy package is assigned to an ADOM, administrators creating new policy packages within that ADOM have the option to select and assign the global policy package to the new policy package if desired.

NEW QUESTION 5

Refer to the exhibit.



```
Start to import config from device(Remote-FortiGate) vdom(root) to
adom(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)"
```

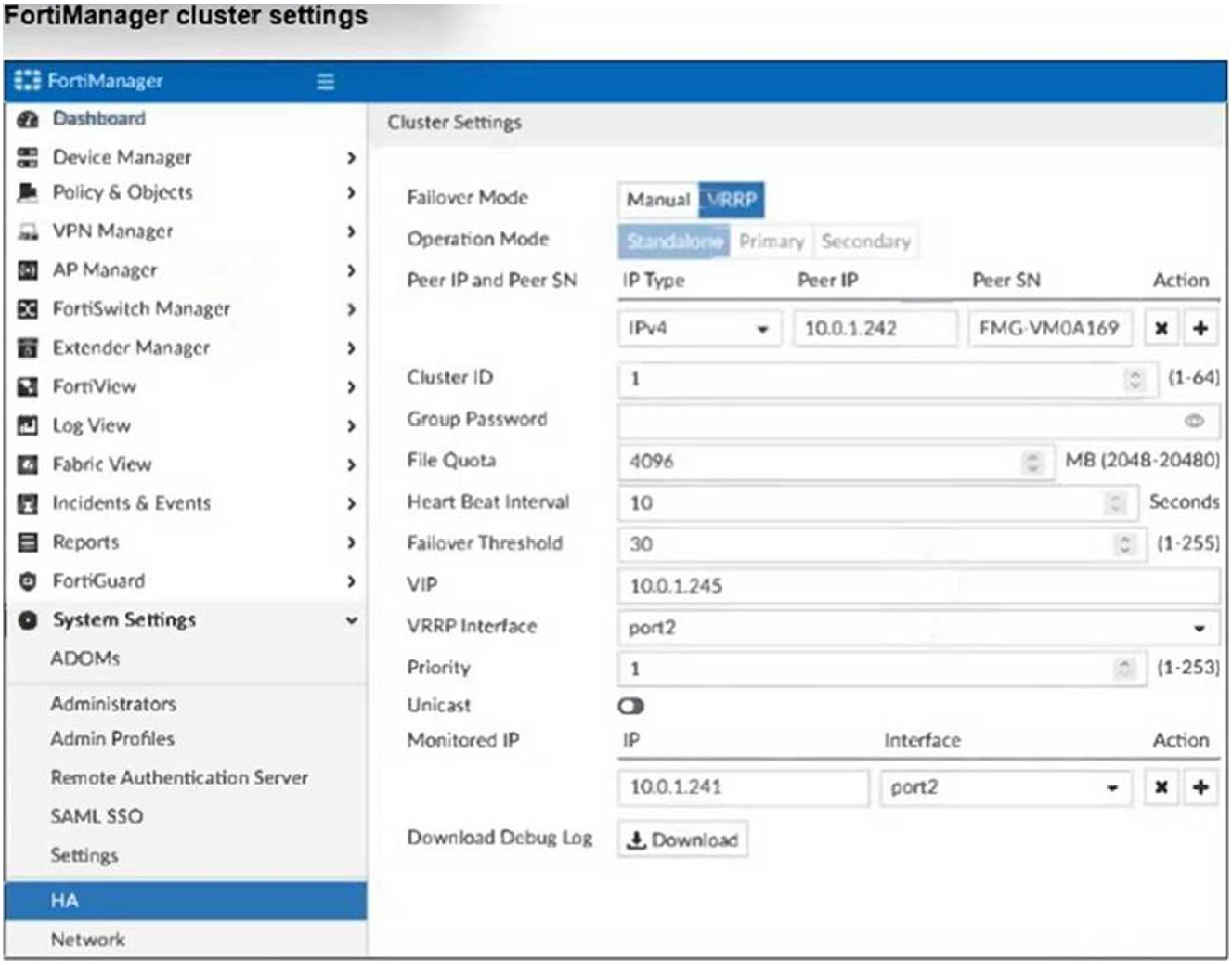
What can you conclude from the downloaded import report?

A. FortiManager does not support per-device mapping for firewall addresses.
B. The administrator will see a new policy package named Remote-FortiGate_root in the FortiManager ADOM database.
C. FortiManager will change the configuration of REMOTE_SUBNET to match the interface mapping coming in from Remote-FortiGate.
D. As a result of this policy import process, FortiManager will create a new firewall address called REMOTE_SUBNET in the ADOM database.

Answer: B

Explanation:
The import report shows that a new policy package named Remote-FortiGate_root will be created in the FortiManager ADOM database, but some firewall addresses and policies failed to import due to interface binding conflicts.

NEW QUESTION 6
Refer to the exhibit.



Failover Mode: Manual [✓ VRRP]
Operation Mode: [✓ Standalone] Primary Secondary
Peer IP and Peer SN:

IP Type	Peer IP	Peer SN	Action
IPv4	10.0.1.242	FMG-VM0A169	✖ ✚

Cluster ID: 1 (1-64)
Group Password:
File Quota: 4096 MB (2048-20480)
Heart Beat Interval: 10 Seconds
Failover Threshold: 30 (1-255)
VIP: 10.0.1.245
VRRP Interface: port2
Priority: 1 (1-253)
Unicast: ○
Monitored IP:

IP	Interface	Action
10.0.1.241	port2	✖ ✚

Download Debug Log: Download

If the monitored interface for the primary FortiManager device fails, what must you do to maintain high availability (HA)?

A. The FortiManager HAfailover is transparent to administrators and does not require any additional action.
B. Manually promote one of the working secondary devices to the primary role: and reboot the original primary device to remove the peer IP address of the failed device.
C. Reconfigure the primary device to remove the peer IP address of the failed device from its configuration.
D. Check the integrity database of the primary device to force a secondary device to become the new primary with all active interfaces.

Answer: A

Explanation:
In a FortiManager HA cluster configured with VRRP failover, the failover process is automatic and transparent to administrators. If the monitored interface on the primary device fails, the secondary device takes over without requiring manual intervention to maintain HA.

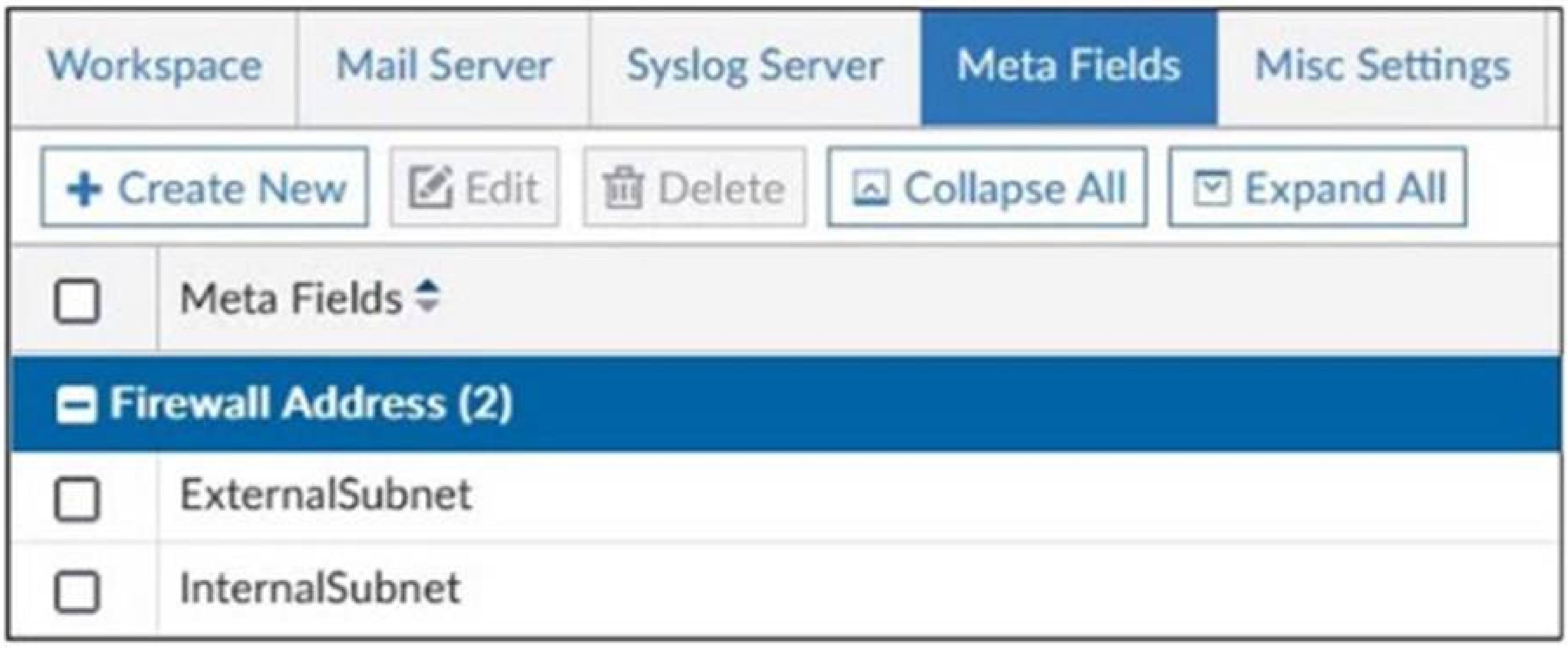
NEW QUESTION 7
What is the purpose of ADOM revisions?

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

Answer: D

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

NEW QUESTION 8
Refer to the exhibit.



Workspace | Mail Server | Syslog Server | Meta Fields | Misc Settings

+ Create New | Edit | Delete | Collapse All | Expand All

□	Meta Fields
Firewall Address (2)	
□	ExternalSubnet
□	InternalSubnet

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

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

Answer: A

Explanation:
Meta fields in FortiManager can be added to objects as custom attributes, allowing administrators to categorize and add additional information to firewall objects for easier management and identification.

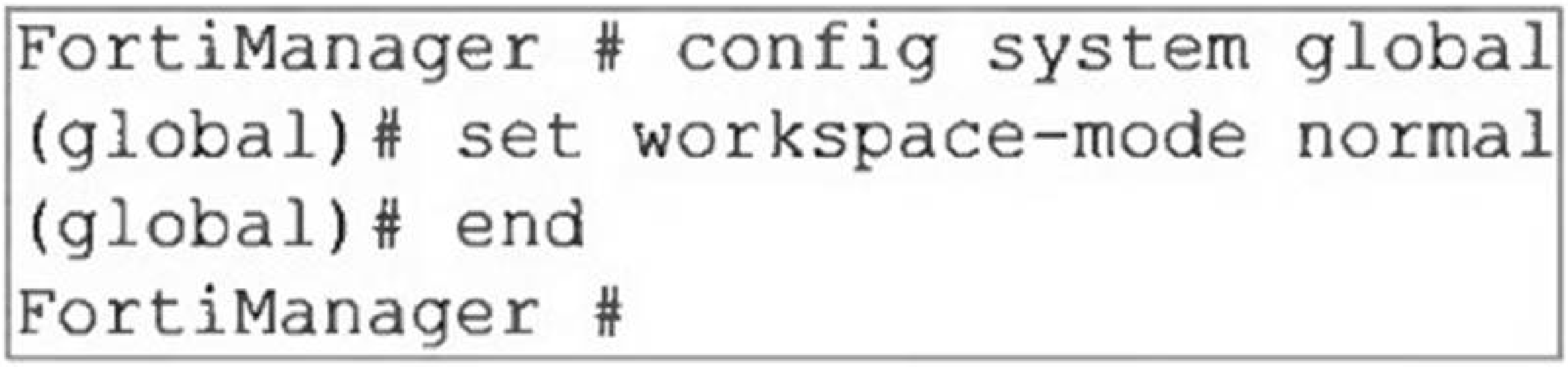
NEW QUESTION 9
Which two conditions trigger FortiManager to create a new revision history? (Choose two.)

A. When FortiManager installs device-level changes on a managed device
B. When changes to the device-level database are made on FortiManager
C. When FortiManager is auto-updated with configuration changes made directly on a managed device
D. When a provisioning template is assigned to a managed device on the device-level database

Answer: BC

Explanation:
FortiManager creates a new revision history entry whenever changes are made to the device-level database on FortiManager.
FortiManager also creates a new revision when it auto-updates its database with configuration changes detected directly on a managed device.

NEW QUESTION 10
Refer to the exhibit.



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

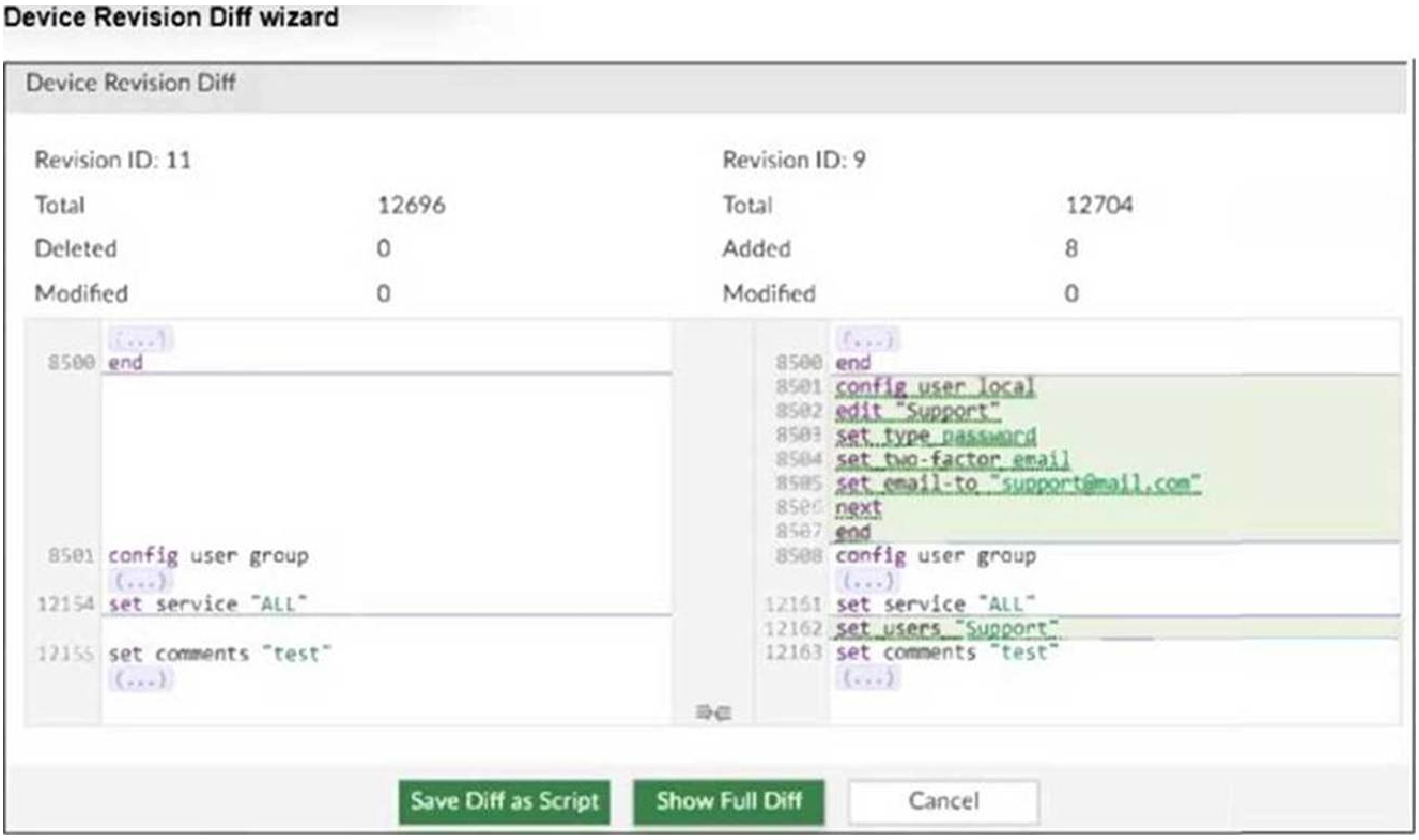
What are two results from the configuration shown in the exhibit? (Choose two.)

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

Answer: AB

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

NEW QUESTION 10
Refer to the exhibits.



Device Revision Diff wizard

Device Revision Diff

Revision ID: 11		Revision ID: 9	
Total	12696	Total	12704
Deleted	0	Added	8
Modified	0	Modified	0

```
      (...)
 8500 end




 8501 config user group
      (...)
12154 set service "ALL"

12155 set comments "test"
      (...)
```

```
      (...)
 8500 end
 8501 config user local
 8502 edit "Support"
 8503 set type password
 8504 set two-factor email
 8505 set email-to "support@mail.com"
 8506 next
 8507 end
 8508 config user group
      (...)
12161 set service "ALL"
12162 set users "Support"
12163 set comments "test"
      (...)
```

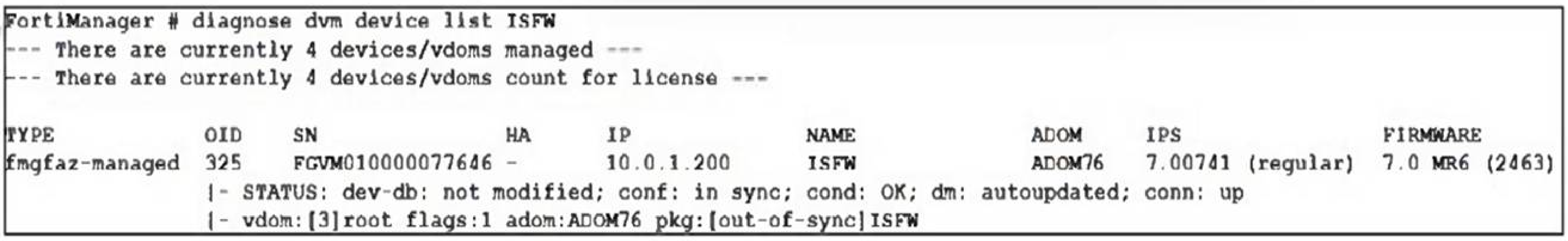
An administrator needed to recover all the configurations related to the user, Support. The configurations were saved in configuration revision ID 9.
The administrator reverted the configuration using theConfiguration Revision Historywindow and received the CLI output shown in the exhibit.
What can you conclude from the CLI output?

A. The administrator set the flag to 0 to prevent configuration overrides.
B. The administrator reinstalled the policy package.
C. The administrator needs to retrieve the device to correctly detect the FortiGate firmware version.
D. The administrator installed only the device-level configuration.

Answer: C

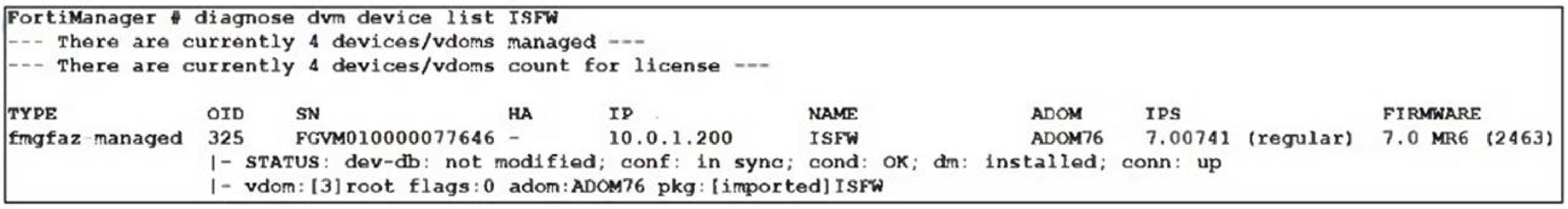
Explanation:
The CLI output shows the status "dev-db: not modified; conf: in sync; cond: OK; dm: installed," but the firmware version for the device is listed as "[unknown]." This indicates that FortiManager has not properly detected the FortiGate firmware version, likely because the device needs to be retrieved to update its information.

NEW QUESTION 14
Which output is displayed right after moving the ISFW device from one ADOM to another?
A)



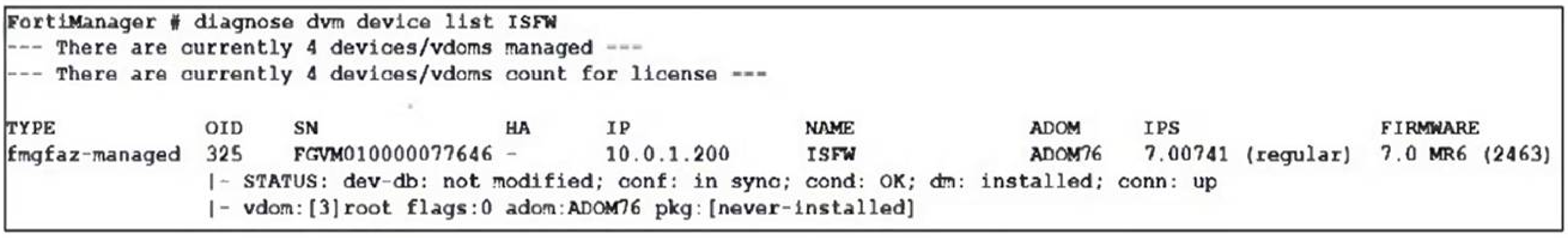
```
FortiManager # diagnose dvm device list ISFW
--- There are currently 4 devices/vdoms managed ---
--- There are currently 4 devices/vdoms count for license ---

TYPE            OID    SN                HA     IP              NAME          ADOM     IPS                  FIRMWARE
fmgfaz-managed  325    FGVM010000077646  -      10.0.1.200      ISFW          ADOM76   7.00741 (regular)    7.0 MR6 (2463)
                       |- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: autoupdated; conn: up
                       |- vdom:[3]root flags:1 adom:ADOM76 pkg:[out-of-sync]ISFW
```

B)



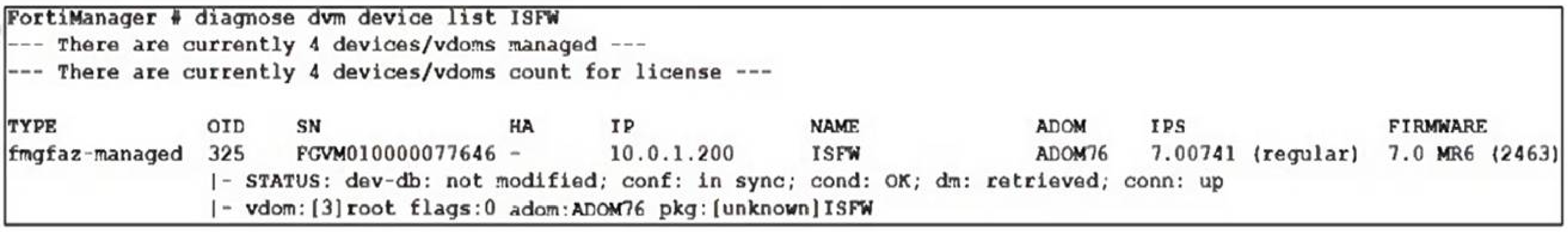
```
FortiManager # diagnose dvm device list ISFW
--- There are currently 4 devices/vdoms managed ---
--- There are currently 4 devices/vdoms count for license ---

TYPE            OID    SN                HA     IP              NAME          ADOM     IPS                  FIRMWARE
fmgfaz-managed  325    FGVM010000077646  -      10.0.1.200      ISFW          ADOM76   7.00741 (regular)    7.0 MR6 (2463)
                       |- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: installed; conn: up
                       |- vdom:[3]root flags:0 adom:ADOM76 pkg:[imported]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          ADOM76   7.00741 (regular)    7.0 MR6 (2463)
                       |- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: installed; conn: up
                       |- vdom:[3]root flags:0 adom:ADOM76 pkg:[never-installed]
```

D)



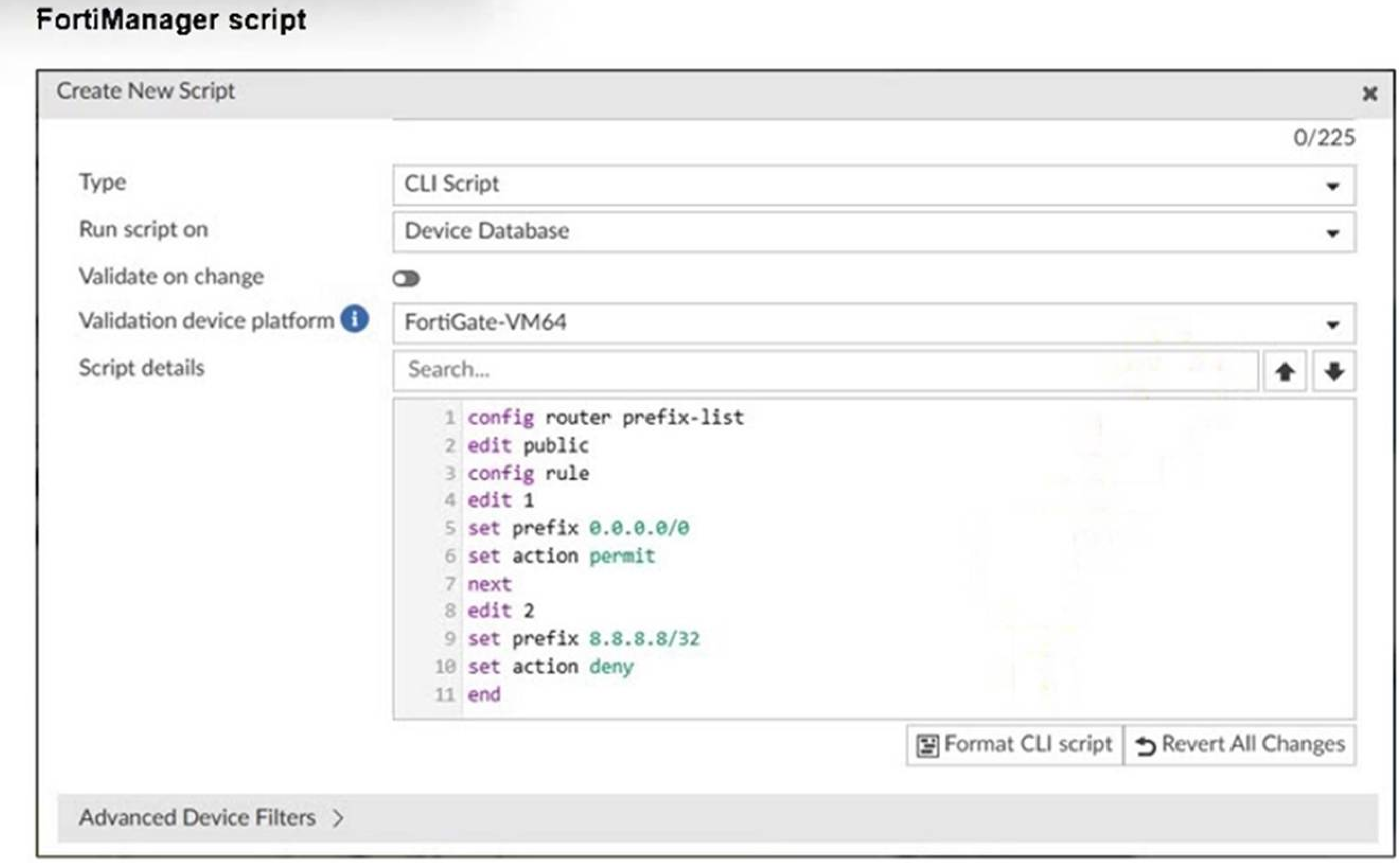
```
FortiManager # diagnose dvm device list ISFW
--- There are currently 4 devices/vdoms managed ---
--- There are currently 4 devices/vdoms count for license ---

TYPE            OID    SN                HA     IP              NAME              ADOM     IPS                 FIRMWARE
fmgfaz-managed  325    FGVM010000077646  -      10.0.1.200      ISFW              ADOM76   7.00741 (regular)   7.0 MR6 (2463)
                |- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: retrieved; conn: up
                |- vdom:[3]root flags:0 adom:ADOM76 pkg:[unknown]ISFW
```

A. Option A
B. Option B
C. Option C
D. Option D

Answer: C

Explanation:
Right after moving the ISFW device to a new ADOM, the status typically shows the policy package as never-installed, indicating that the device has been assigned to the new ADOM but no policy package has yet been installed in that ADOM.

NEW QUESTION 16
Refer to the exhibit.



FortiManager script

Create New Script

0/225

Type: CLI Script
Run script on: Device Database
Validate on change
Validation device platform: FortiGate-VM64
Script details

```
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
```

Which two results occur if you run the script using theDevice Databaseoption? (Choose two.)

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

Answer: AD

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

NEW QUESTION 21
......