Fortinet

Exam Questions FCP_FMG_AD-7.6

FCP - FortiManager 7.6 Administrator

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
An administrator has a FortiGate-HQ device with VDOMs—root, HR and Facilities, currently managed under the FortiManager ADOM—Site1. They try to move VDOM HR to the FortiManager ADOM—Site2, but it does not work.
Why is the administrator not able to move FortiGate-HQ VDOM HR to FortiManager ADOM—Site2?

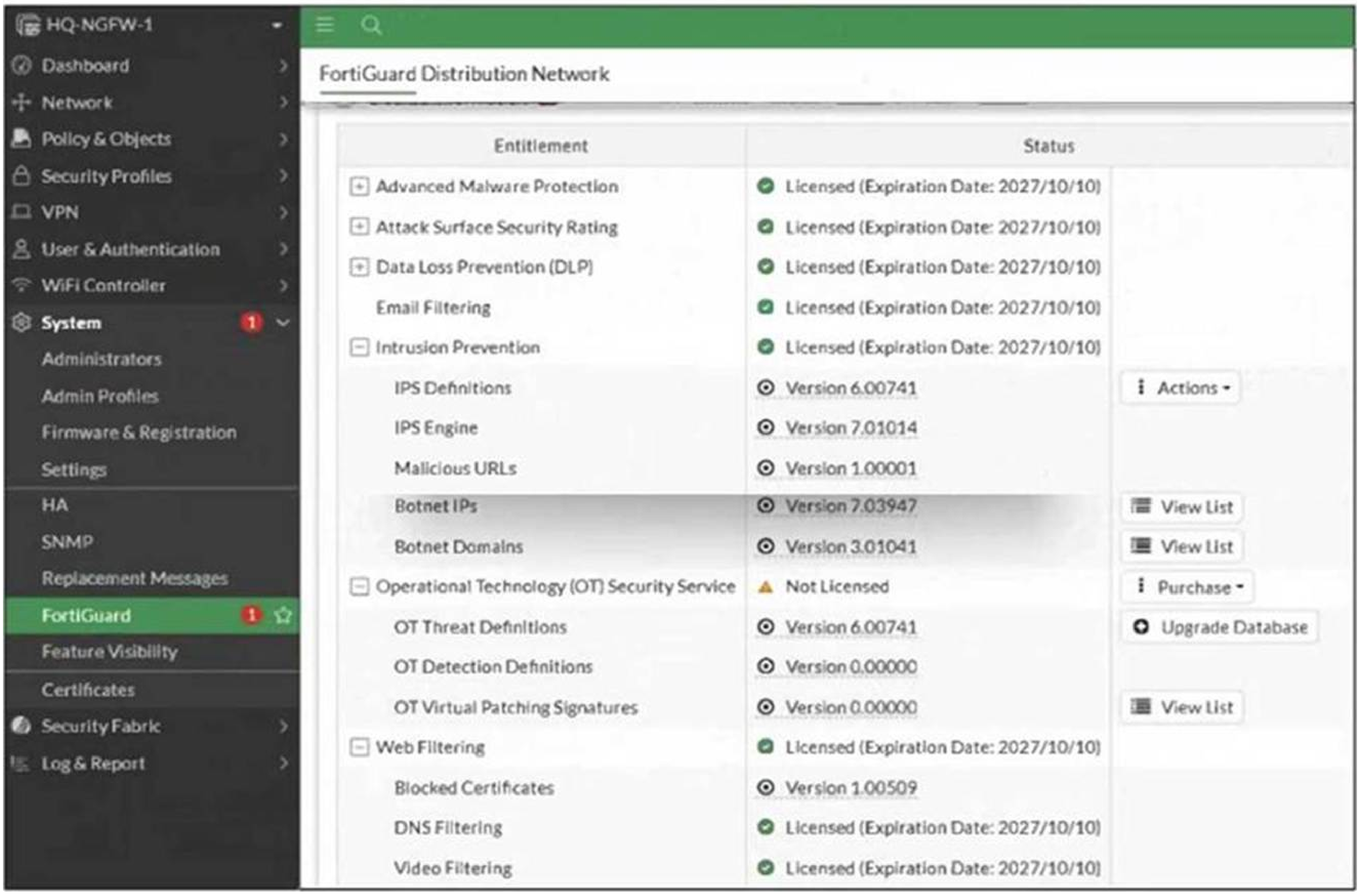
A. The FortiGate-HQ must be managed under the FortiManager ADOM—root to allow moving its VDOMs to different ADOMs.
B. The administrator must have full access in the device layer of FortiGate-HQ VDOM-root before they can VDOMs to different ADOMs.
C. FortiManager must be in ADOM normal mode, which does not allow VDOMs to be managed separately.
D. The administrator must delete the FortiGate-HQ device from FortiManager and add it again using the Add Device wizard before moving the VDOM.

Answer: A

Explanation:
FortiGate devices must be managed under the FortiManager ADOM corresponding to the root VDOM to allow their individual VDOMs to be moved and managed in different ADOMs. Managing the root VDOM in a different ADOM prevents moving subordinate VDOMs across ADOMs.

NEW QUESTION 2
Refer to the exhibits

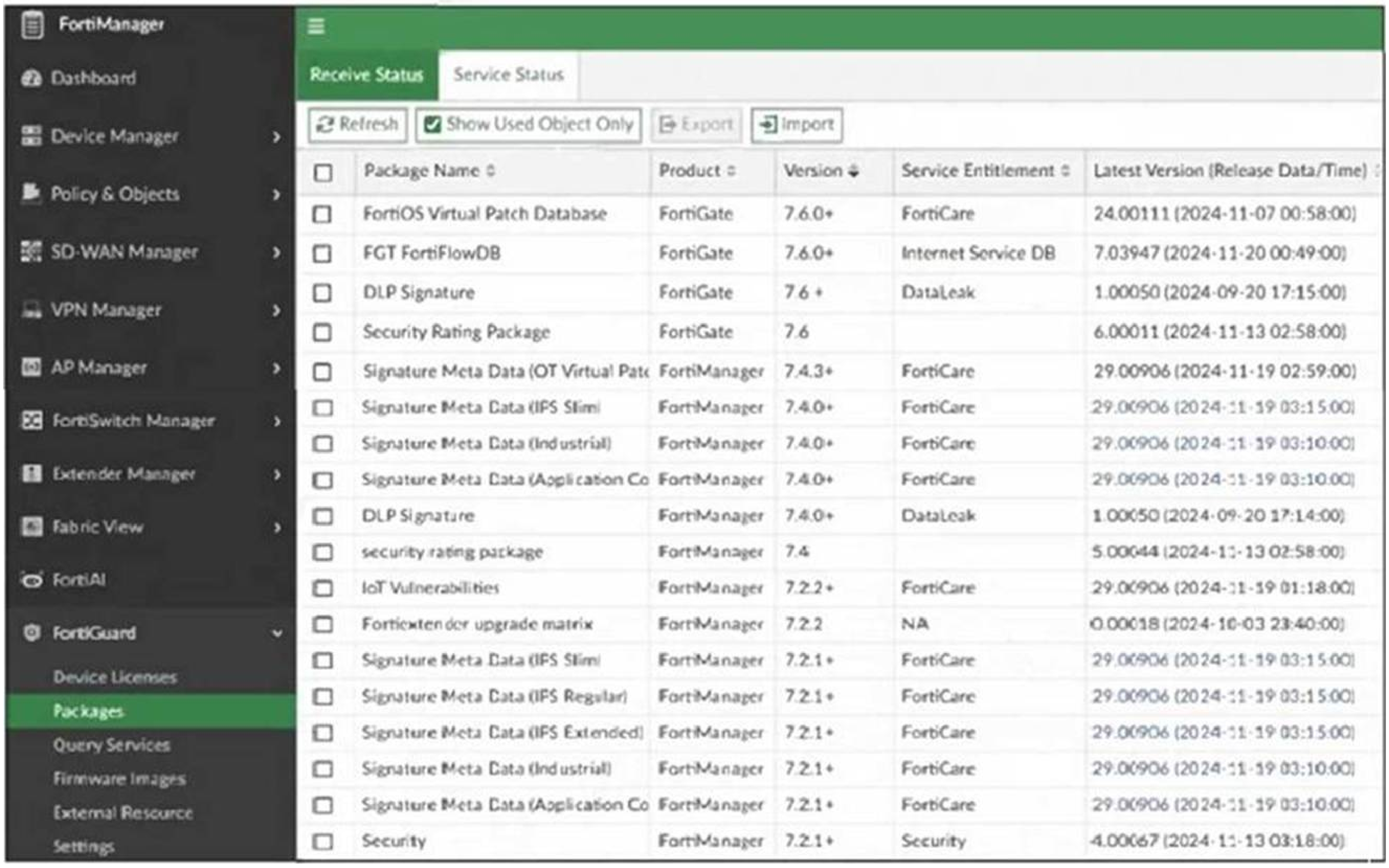
FortiGate GUI—FortiGuard



FortiGuard Distribution Network

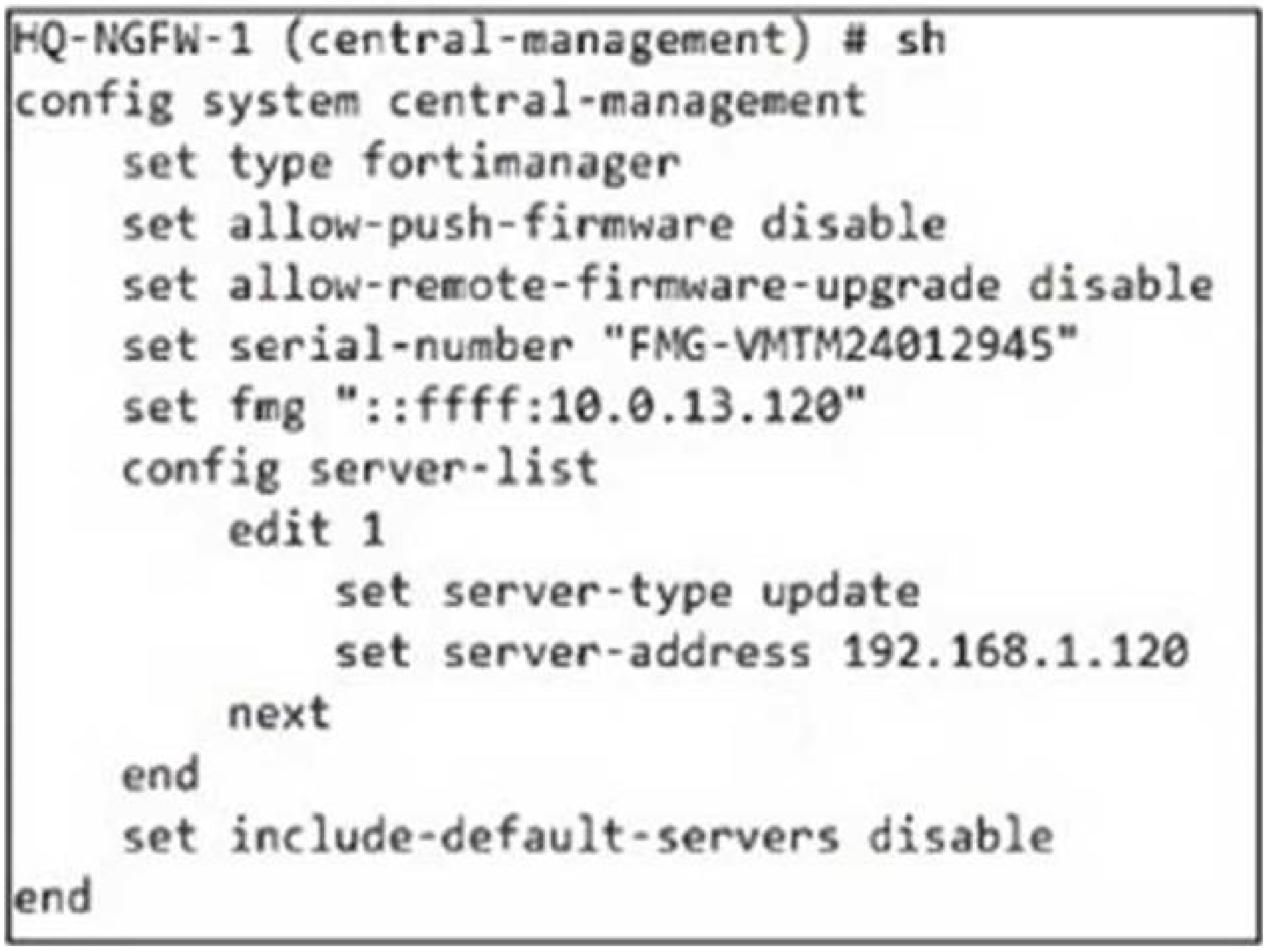
Entitlement	Status	
⊞ Advanced Malware Protection	Licensed (Expiration Date: 2027/10/10)	
⊞ Attack Surface Security Rating	Licensed (Expiration Date: 2027/10/10)	
⊞ Data Loss Prevention (DLP)	Licensed (Expiration Date: 2027/10/10)	
Email Filtering	Licensed (Expiration Date: 2027/10/10)	
⊟ Intrusion Prevention	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.

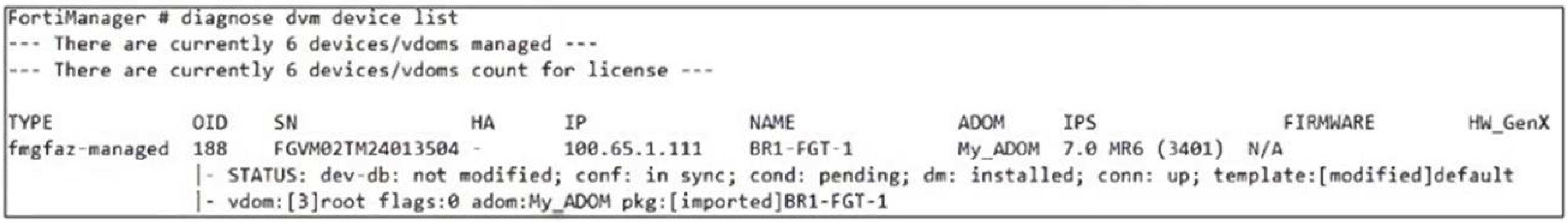
NEW QUESTION 3
Which is recommended when you are managing a high volume of logs in your network?

A. Store logs on FortiManager and use FortiView.
B. Add and manage FortiAnalyzer from FortiManager.
C. Enable advanced ADOM mode on FortiManager.
D. Forward logs from FortiAnalyzer to FortiManager daily.

Answer: B

Explanation:
Adding and managing FortiAnalyzer from FortiManager is recommended for handling a high volume of logs, as FortiAnalyzer is designed specifically for centralized log management, analysis, and reporting, which offloads this workload from FortiManager.

NEW QUESTION 4
Refer to the exhibit.



```
FortiManager # diagnose dvm device list
--- There are currently 6 devices/vdoms managed ---
--- There are currently 6 devices/vdoms count for license ---

TYPE            OID    SN                HA      IP              NAME            ADOM     IPS               FIRMWARE        HW_GenX
fmgfaz-managed  188    FGVM02TM24013504  -       100.65.1.111    BR1-FGT-1       My_ADOM  7.0 MR6 (3401)  N/A
                |- STATUS: dev-db: not modified; conf: in sync; cond: pending; dm: installed; conn: up; template:[modified]default
                |- vdom:[3]root flags:0 adom:My_ADOM pkg:[imported]BR1-FGT-1
```

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, updating policy and device-level database.
C. The latest revision history for the managed FortiGate does match the FortiManager policy database.
D. The system template default will override device-level database configurations.

Answer: AD

Explanation:
The status "pending" indicates the latest revision history does not match the device-level database, meaning there are unapplied changes.
The template is marked as [modified], so the system template default will override device-level database configurations when installed.

NEW QUESTION 5
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?

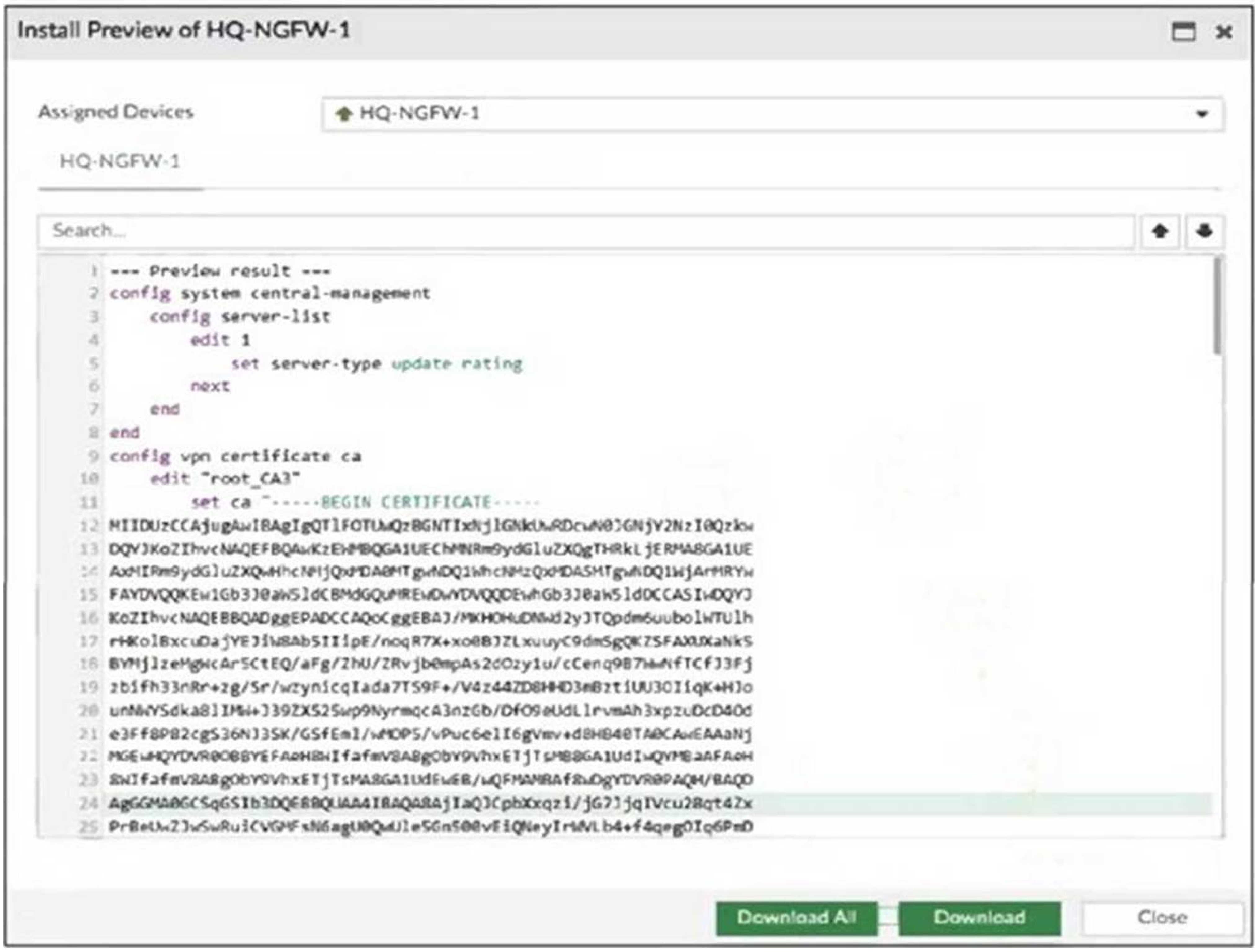
A. Use the Install Wizard located on the device manager.
B. Enable workflow mode to allow policy creation and approval.
C. Make sure the ADOM and FortiGate firmware versions match and use the ADOM policy package.
D. Use a FortiManager script to apply the configuration changes.

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 6
Refer to the exhibit.

FortiManager—HQ-NGFW-1 install preview



```
--- Preview result ---
config system central-management
    config server-list
        edit 1
            set server-type update rating
        next
    end
end
config vpn certificate ca
    edit "root_CA3"
        set ca "-----BEGIN CERTIFICATE-----
MIIDUzCCAjugAwIBAgIgQTlFOTUwQzBGNTIxNjlGNkUwRDcwN0JGNjY2NzI0Qzkw
DQYJKoZIhvcNAQEFBQAwKzEhMBQGA1UEChMNRm9ydGluZXQgTHRkLjERMA8GA1UE
AxMIRm9ydGluZXQwHhcNMjQxMDA0MTgwNDQ1WhcNMzQxMDA5MTgwNDQ1WjArMRYw
FAYDVQQKEw1Gb3J0aW5ldCBMdGQuMREwDwYDVQQDEwhGb3J0aW5ldDCCASIwDQYJ
KoZIhvcNAQEBBQADggEPADCCAQoCggEBAJ/MKHOHuDNWd2yJTQpdm6uubolWTUlh
rHKolBxcuDajYEJiW8Ab5III1pE/noqR7X+xo0BJZLxuuyC9dmSgQKZ5FAXUXaNkS
BYMjlzeMgWcAr5CtEQ/aFg/ZhU/ZRvjb0mpAs2dOzy1u/cCenq9B7wWNfTCfJ3Fj
zb1fh33nRr+zg/Sr/wzynicqIada7TS9F+/V4z44ZD8HHD3mBztiUU3OIiqK+HJo
unNWYSdka8lIMW+J39ZX52Swp9NyrmqcA3nzGb/DfO9eUdLlrvmAh3xpzuDcD4Od
e3Ff8PB2cgS36NJ3SK/GSfEml/wMOP5/vPuc6elI6gVmv+d8HB40TA0CAwEAAaNj
MGEwHQYDVR0OBBYEFAoHBwIfafmV8ABgObY9VhxETjTsMB8GA1UdIwQYMBaAFAoH
BwIfafmV8ABgObY9VhxETjTsMA8GA1UdEwEB/wQFMAMBAf8wDgYDVR0PAQH/BAQD
AgGGMA0GCSqGSIb3DQEBBQUAA4IBAQA8AjIaQJCpbXxqzi/jG7JjqIVcu28qt4Zx
PrBeUwZJwSwRuiCVGMFsN6agU0QwUleSGn500vEiQNeyIrWVLb4+f4qeg0Iq6PmD
```

An administrator assigned a new policy package to FortiGate HQ-NGFW-1. In the installation preview, they noticed some settings they did not modify and are unsure about the changes.
Based on the exhibit, which two things will happen if they continue with the installation? (Choose two.)

A. FortiGate HQ-NGFW-1 can use FortiManager firmware templates to upgrade firmware and ratings.
B. FortiGate HQ-NGFW-1 can contact the FortiManager acting as FortiGuard Distribution Server (FDS) to download FortiGuard updates.
C. FortiGate HQ-NGFW-1 will use the root_CA3 certificate in firewall address objects or policies.
D. FortiManager will install the CA certificate named root_CA3 to authenticate FortiGate-to-FortiManager communication protocol (FGFM) tunnel connections with FortiGate HQ- NGFW-1.

Answer: BD

Explanation:
The configuration includes a server-list with server-type set to "update rating," which enables FortiGate HQ- NGFW-1 to contact FortiManager as a FortiGuard Distribution Server (FDS) for FortiGuard updates.
The installation includes a root_CA3 certificate, which FortiManager will install on FortiGate HQ-NGFW-1 to authenticate FGFM tunnel connections between the devices.

NEW QUESTION 7
An administrator wants to configure and manage multiple objects in the FortiManager database and give access to other users who work in the same database.
To stay in control of the changes made to firewall policies by other team members, the administrator needs a setup where all modifications go through a central check before they can be installed.
How can the administrator create this setup?

A. Enable the prompt asking the administrator to accept firewall policies changes before saving.
B. Enable the workspace (for all ADOMs) to control all changes made by any administrator.
C. Enable device lock and the advanced mode feature in the ADOM.
D. Enable workflow mode and the ADOM lock feature.

Answer: D

Explanation:
Enabling workflow mode along with the ADOM lock feature ensures that all configuration changes go through a centralized review and approval process before installation, allowing controlled and coordinated management of firewall policies by multiple administrators.

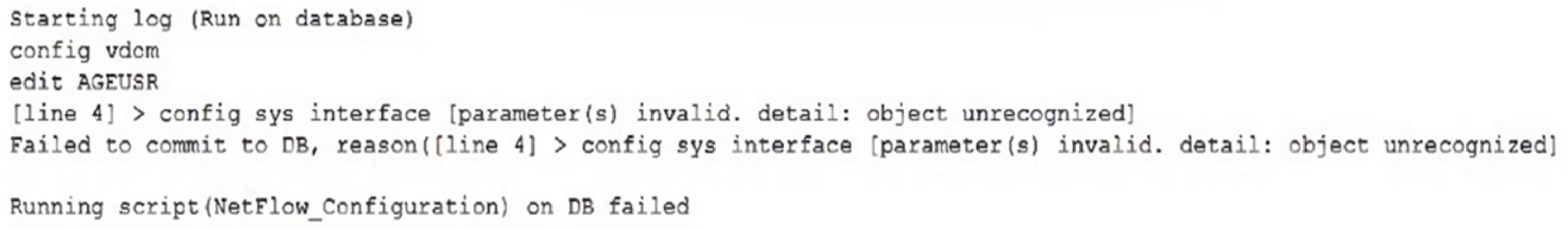
NEW QUESTION 8
You want to let multiple administrators work in the same ADOM without creating configuration conflicts.
What is the best and the most effective solution to apply?

A. Configure RADIUS authentication to assign ADOM roles to each user.
B. Enable workflow mode, which is the only way to prevent concurrent configuration conflicts.
C. Assign administrators with JSON API access to the FortiManager.
D. Activate workspace mode in the ADOM settings.

Answer: D

Explanation:
Activating workspace mode in the ADOM settings allows multiple administrators to work concurrently in the same ADOM by isolating their configuration changes in separate workspaces, preventing conflicts and enabling effective collaboration.

NEW QUESTION 9
While attempting to push a NetFlow configuration script through the FortiManager policy package: an administrator encounters an error stating that an object is unrecognized in line 4.



```
Starting log (Run on database)
config vdom
edit AGEUSR
[line 4] > config sys interface [parameter(s) invalid. detail: object unrecognized]
Failed to commit to DB, reason([line 4] > config sys interface [parameter(s) invalid. detail: object unrecognized]

Running script(NetFlow_Configuration) on DB failed
```

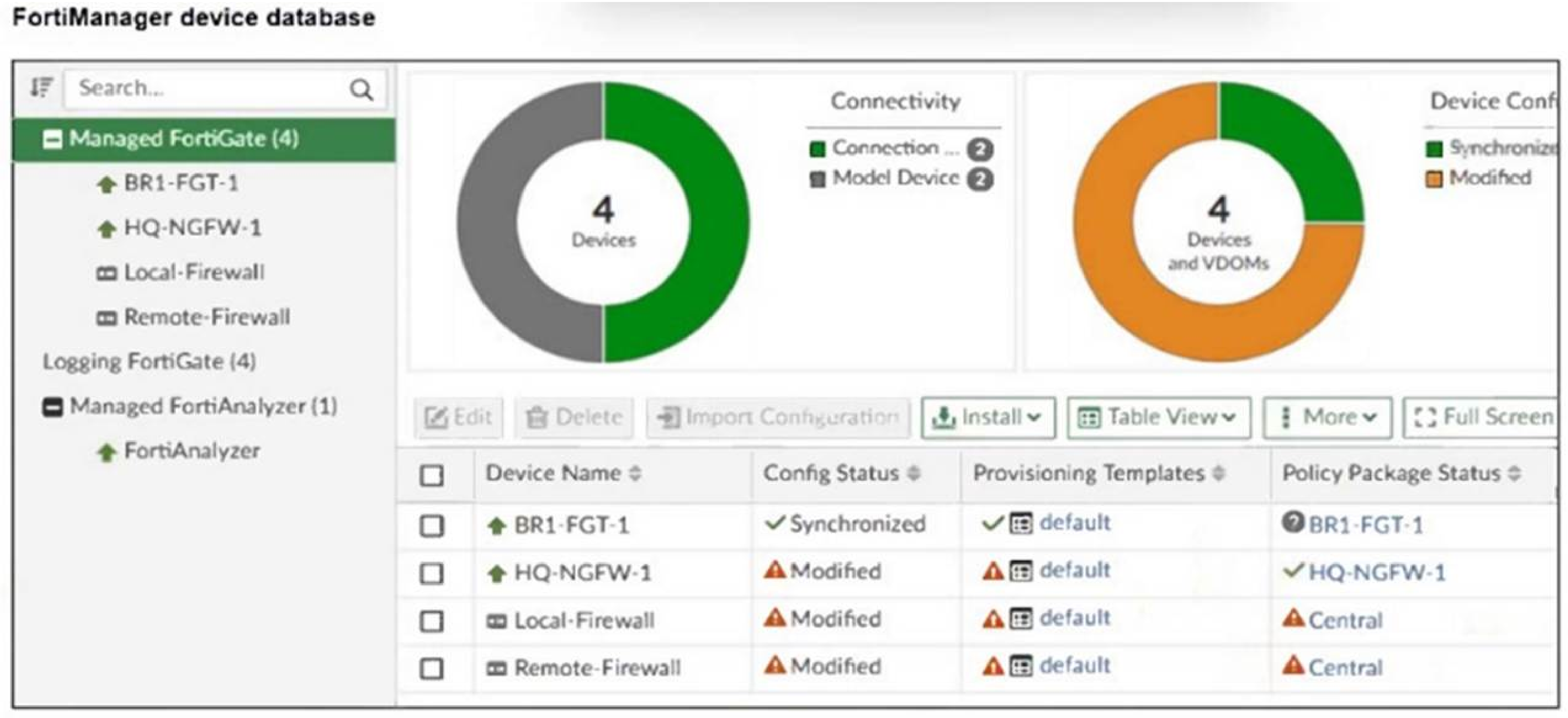
What must the administrator do to successfully apply the NetFlow configuration script and avoid the object unrecognized error?

A. Make sure the user running the script has full access to the VDOM—AGEUSR.
B. Run the script on the device database.
C. Use metadata variables if they use VDOMs in the script.
D. Create a normalized interface on the policy layer before running the script.

Answer: C

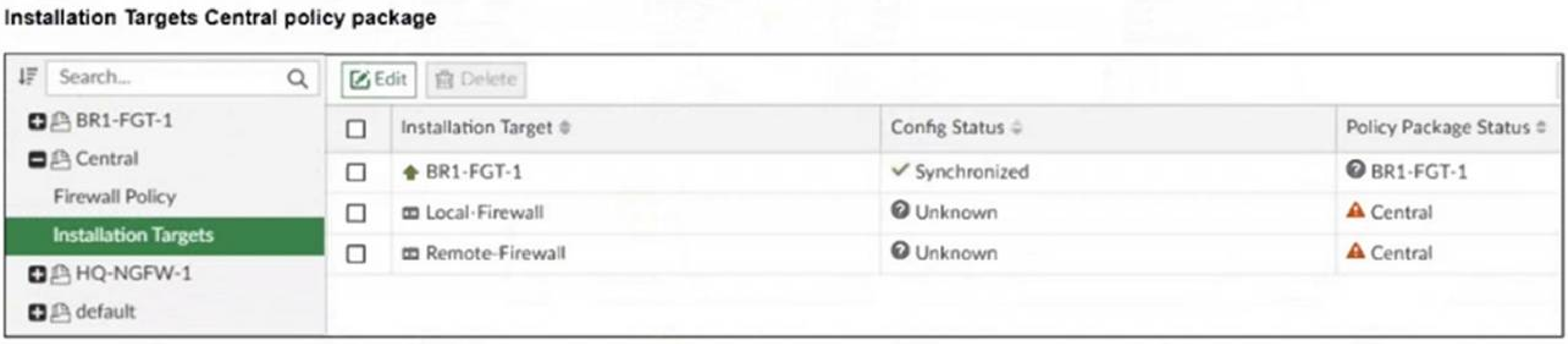
Explanation:
When using scripts that reference VDOM-specific objects, such as interfaces, in FortiManager, metadata variables must be used to correctly map those objects per VDOM. This prevents "object unrecognized" errors during script execution.

NEW QUESTION 10
Refer to the exhibits.



FortiManager device database

☐	Device Name	Config Status	Provisioning Templates	Policy Package Status
☐	BR1-FGT-1	✓ Synchronized	✓ default	BR1-FGT-1
☐	HQ-NGFW-1	⚠ Modified	⚠ default	✓ HQ-NGFW-1
☐	Local-Firewall	⚠ Modified	⚠ default	⚠ Central
☐	Remote-Firewall	⚠ Modified	⚠ default	⚠ Central



Installation Targets Central policy package

□	Installation Target	Config Status	Policy Package Status
□	BR1-FGT-1	✓ Synchronized	BR1-FGT-1
□	Local-Firewall	Unknown	Central
□	Remote-Firewall	Unknown	Central

An administrator has been asked to install the same policies from a central policy package onto the BR1-FGT- 1 firewall.
The administrator added BR1-FGT-1 as a target in the central policy package installation.
What should the administrator do when reinstalling the central policy package on the BR1-FGT-1 firewall?

A. Assign only one policy package to the firewall because FortiManager does not allow more than one policy package assigned per device at the same time.
B. Import the policy package to change the unknown status and synchronize the policy package.
C. Use the install wizard to install the central policy package on the BR1-FGT-1 firewall.
D. First resolve the modified status in the configuration and provisioning templates to allow a smooth installation.

Answer: C

Explanation:
Using the Install Wizard is the recommended method to reinstall the central policy package on the BR1-FGT- 1 firewall, ensuring all settings, installation targets, and dependencies are correctly processed during installation.

NEW QUESTION 10
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 13
Push updates are failing on a FortiGate device located behind a network address translation (NAT) device? Which two settings should the administrator check to correct this problem? (Choose two.)

A. Make sure the NAT device IP address and the correct ports are configured on FortiManager.
B. Make sure FortiGuard updates and web service are enabled on the FortiGuard service interface.
C. Make sure the virtual IP address and the correct ports are configured on the NAT device.
D. Make sure the Bind to IP address option on the FortiGuard service interface is set to the virtual IP address from the NAT device.

Answer: AC

Explanation:
FortiManager must have the NAT device's IP address and correct ports configured to communicate properly with the FortiGate behind NAT.
The NAT device must have the correct virtual IP address and ports configured to allow push updates to reach the FortiGate device.

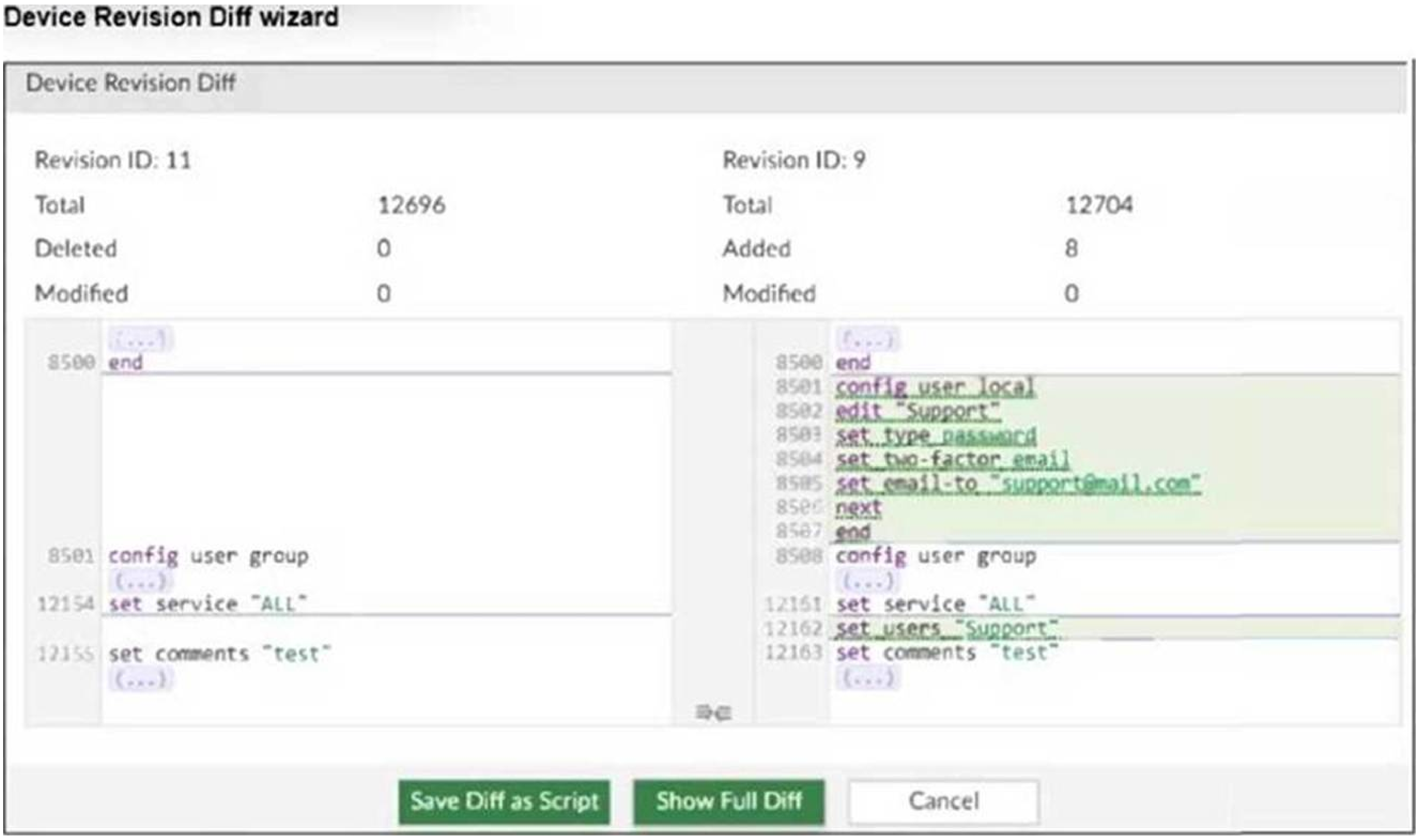
NEW QUESTION 14
An administrator is copying a system template profile between ADOMs by running the following command:
execute fmprofile export-profile ADOM 3547 /tmp/Backup_File
output dump to file: [/tmp/Backup_File]
Where does this command export the system template profile from?

A. FortiManager /tmp/Backup_File folder
B. FortiManager ADOM policy database
C. ADOM device database
D. FortiManager configuration backup file

Answer: B

Explanation:
The command exports the system template profile from the FortiManager ADOM policy database, which stores the configuration templates for devices within that ADOM.

NEW QUESTION 18
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

```
(...)
end




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

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

```
(...)
end
config user local
edit "Support"
set type password
set two-factor email
set email-to "support@mail.com"
next
end
config user group
(...)
set service "ALL"
set users "Support"
set comments "test"
(...)
```

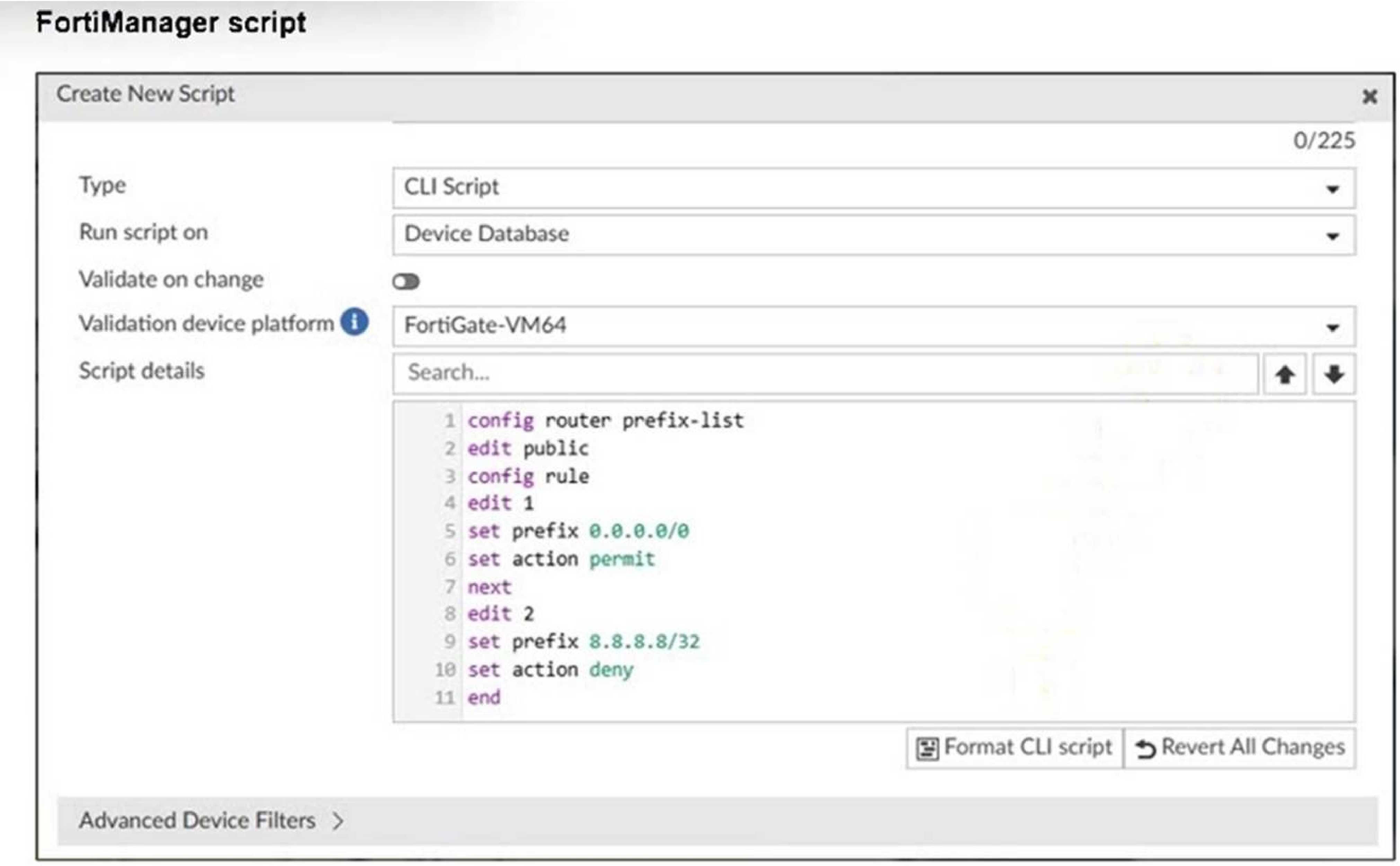
An administrator needed to recover all the configurations related to the user, Support. The configurations were saved in configuration revision ID 9.
The administrator reverted the configuration using theConfiguration Revision Historywindow and received the CLI output shown in the exhibit.
What can you 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 21
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 26
An administrator configures a new BGP peer in the FortiManager device-level database of FortiGate. They reinstall the policy package to the managed FortiGate device without any errors. However, when the administrator logs in to FortiGate, they do not see the BGP configuration changes.
What is the most likely reason why FortiManager did not push the BGP peer changes to FortiGate?

A. The administrator must run a sanity check on FortiManager to make sure the database is not corrupted.
B. Fortigate has a BGP template assigned on the FortiManager database.
C. The administrator must use the Install Wizard and select Install device settings only to push BGP settings
D. The FortiGate firmware version is different from the FortiManager ADOM version.

Answer: B

Explanation:
If a BGP template is assigned to the FortiGate device on FortiManager, device-level BGP configurations made directly in the device-level database are overridden by the template settings, so the changes do not get pushed to the device.

NEW QUESTION 31
......