DUMPSBOSS.

Fortinet NSE 6 - FortiManager 7.6 Administrator

Fortinet NSE6_FMG_AD-7.6

Version Demo

Total Demo Questions: 7

Total Premium Questions: 79

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

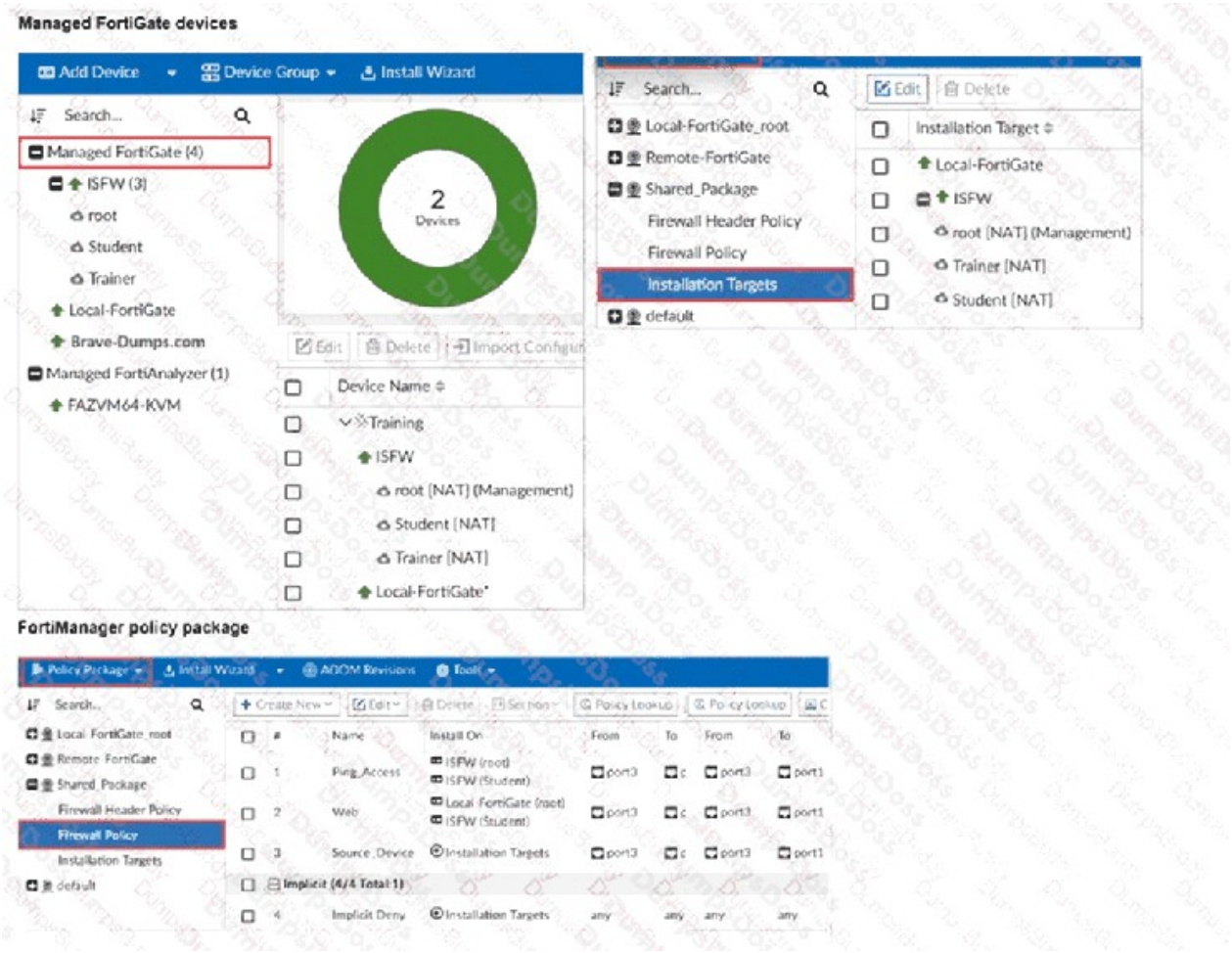
support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Administration	21
Topic 2, Device Manager	14
Topic 3, Policy and Objects	23
Topic 4, Scripts	10
Topic 5, FortiGuard Services	4
Topic 6, Troubleshooting	6
Topic 7, Mix Questions	1
Total	79

QUESTION NO: 1

Refer to the exhibits.



What can you conclude, based on the configuration shown in the exhibit? Choose one answer

A. The administrator needs to retrieve the Local-FortiGate configuration to sync with the Security Fabric group, Training.

B. Policy sequence #1 will be installed on the internal segmentation firewall ISFW device root NAT and Trainer NAT VDOMs.

C. Policy sequence #3 must have devices or VDOMs listed in the Install On column; otherwise, it will cause errors.

D. The global policy package will be added to the top of the ISFW policy package.

ANSWER: A

Explanation:

The administrator needs to retrieve the Local-FortiGate configuration to sync with the Security Fabric group, Training. The exhibit indicates that the Training Security Fabric group has configuration state that must be retrieved from its managed FortiGate members. In FortiManager, a retrieve operation imports the current device-side, or local FortiGate, configuration into FortiManager's device database. This is necessary when the local configuration is newer than the FortiManager revision, such as after changes have been made directly on a FortiGate, so FortiManager can accurately represent and manage the group's current settings. Retrieving is therefore the appropriate synchronization action before making further centralized changes or performing installations. It preserves the discovered FortiGate configuration as the working FortiManager configuration and resolves the indicated mismatch for the Training group. Fortinet documents device configuration retrieval as part of normal managed-device synchronization and revision management; administrators should review the retrieved changes and then use the resulting configuration as the basis for subsequent policy or device-level management. See the FortiManager 7.6 Administration Guide and Fortinet's device-configuration retrieval documentation.

QUESTION NO: 2

An administrator has completed a set of policy and object changes in an ADOM. Before installing the changes, the administrator must retain a recoverable snapshot of the current ADOM configuration and review the exact commands that FortiManager will send to the target FortiGate devices.

Which two actions meet these requirements? Choose two answers.

A. Retrieve configuration from each target FortiGate before installation.

B. Create an ADOM revision after completing the changes.

C. Enable auto-update for all target FortiGate devices.

D. Install device settings only on the target FortiGate devices.

E. Run an install preview for the intended policy package installation.

ANSWER: B E

Explanation:

Creating an ADOM revision saves a point-in-time snapshot of the ADOM policy packages and ADOM-level objects. This provides a recoverable record of the configuration state that is about to be installed. Running an install preview allows the administrator to review the calculated configuration changes and CLI commands before deployment.

Retrieving configuration collects the current configuration from FortiGate and does not create an ADOM recovery point or preview an installation. Enabling auto-update controls how FortiManager handles changes made directly on a managed device. Installing device settings is not an appropriate substitute because the required changes are in policy packages and ADOM-level objects.

QUESTION NO: 3

An administrator receives the import report after importing policies into the policy package layer.

```
Start to import config from device(BR1-FGT-1) vdom(root) to adom(My_ADOM), package(BR1-FGT-1)
"firewall address",SKIPPED,"(name=all, oid=2490, DUPLICATE)"
"firewall policy",SUCCESS,"(name=1, oid=3632, new object)"
"firewall profile-protocol-options",SKIPPED,"(name=default, oid=3491, DUPLICATE)"
"firewall schedule recurring",SKIPPED,"(name=always, oid=3479, DUPLICATE)"
"firewall service category",SKIPPED,"(name=General, oid=2537, DUPLICATE)"
"firewall service custom",SKIPPED,"(name=ALL, oid=2547, DUPLICATE)"
"firewall ssh local-ca",SKIPPED"(name=Fortinet_SSH_CA, oid=3488, reason=manually)"
"firewall ssh local-ca",SKIPPED"(name=Fortinet_SSH_CA_Untrusted, oid=3489, reason=manually)"
"firewall ssl-ssh-profile",SKIPPED,"(name=no-inspection, oid=3585, DUPLICATE)"
```

Based on the import report, how did FortiManager handle the profile-protocol-options object named default?

A. FortiManager deleted the duplicate value from its database.

B. FortiManager created a new service category in its database.

C. FortiManager did not update its database with the value.

D. FortiManager updated the duplicate value in the FortiGate database.

ANSWER: C

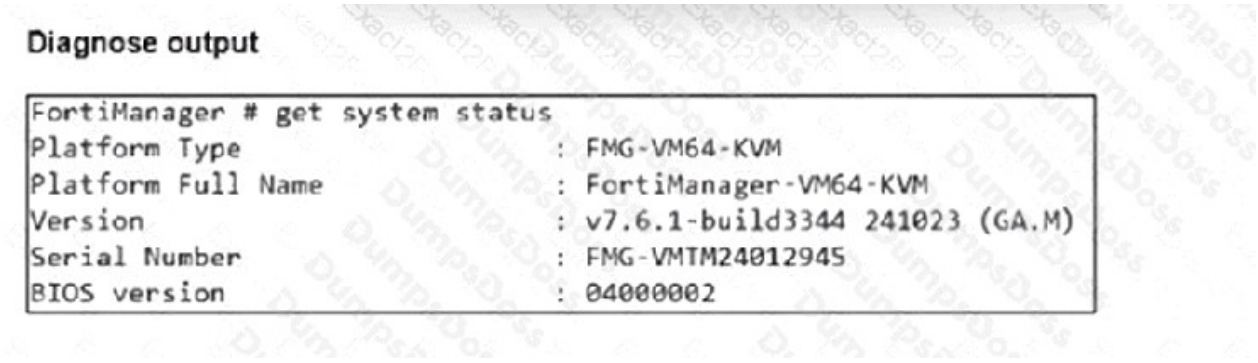
Explanation:

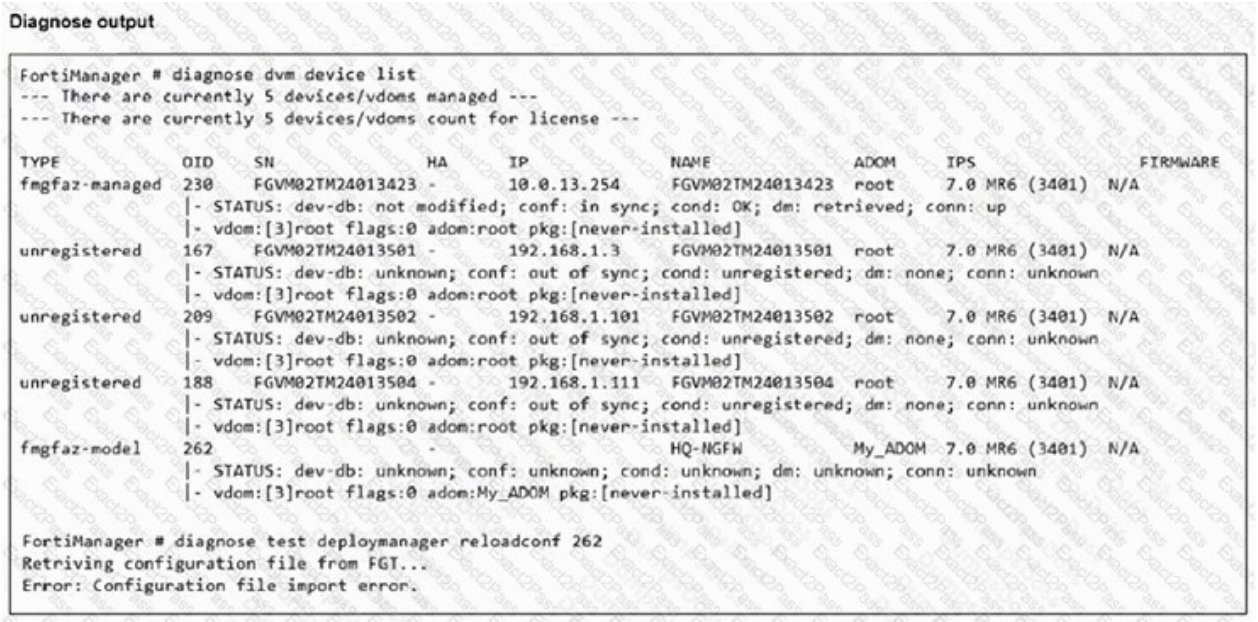
FortiManager did not update its database with the value. The import report identifies the `firewall profile-protocol-options` object named `default` as `SKIPPED` and marks it as a `DUPLICATE`. This result means FortiManager detected that the object already existed in the ADOM database and did not import the received object definition as a replacement or update. Therefore, the existing FortiManager database entry remains unchanged for this import operation.

This behavior is important when importing configuration from a FortiGate into a policy package or ADOM that already contains shared objects. FortiManager maintains its object database and evaluates imported entries for identity and conflicts. A duplicate object reported as skipped does not become a newly imported revision of that object; the import report is specifically confirming that no database update was applied for that entry. Administrators can use such report details to identify objects requiring review or reconciliation before making subsequent installation or synchronization decisions. FortiManager's administrative documentation covers device import, ADOM databases, and policy-package workflows in the FortiManager 7.6 Administration Guide. Additional FortiManager documentation and version-specific guidance are available through the FortiManager Documentation Library.

QUESTION NO: 4

Refer to the exhibits.





An administrator runs the reload failure command diagnose test deploymanager reloadconf 262 on FortiManager.

Why does the administrator receive an error message?

A. The administrator must use the FortiGate name instead of the ID number.

B. The administrator just recently added FortiGate HQ-NGFW as a model device.

C. FortiManager requires the FortiGate serial number instead of the ID number.

D. FortiManager does not support FortiOS version 7.0.

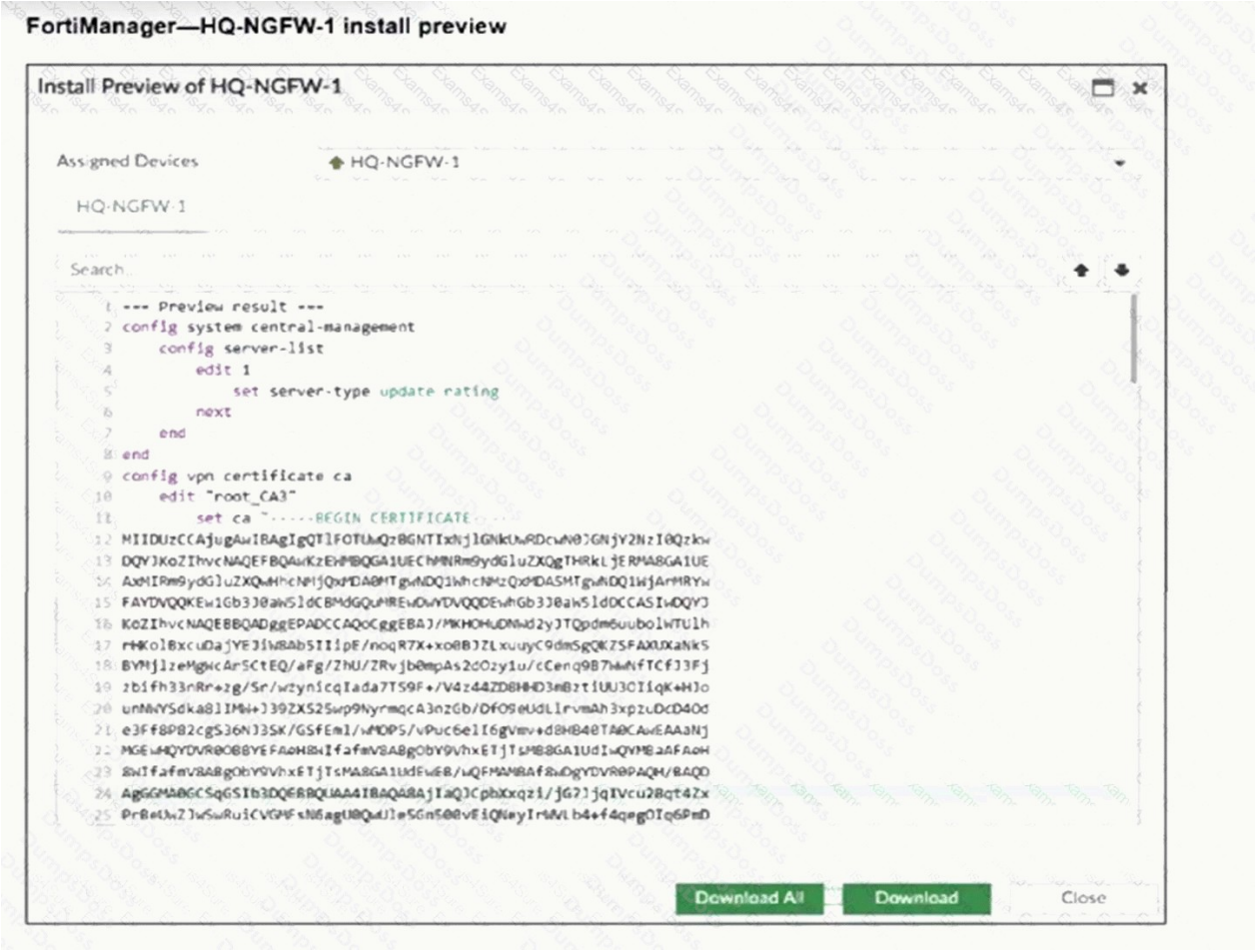
ANSWER: B

Explanation:

The correct answer is **The administrator just recently added FortiGate HQ-NGFW as a model device.** The `diagnose test deploymanager reloadconf <device-id>` command reloads the deployment manager's configuration data for a managed FortiGate. The device ID shown in the command identifies HQ-NGFW, but the exhibit indicates that this unit was added as a model device. A model device is an offline, placeholder representation used to prepare policy packages, objects, and provisioning configuration before a physical FortiGate is available and authorized. Because it has no active FortiGate management connection and no retrieved device configuration to reload, Deploy Manager cannot perform the reload operation for that ID and returns an error. This behavior is expected until the model device is replaced or associated with an actual managed FortiGate and relevant configuration data is available. FortiManager documentation describes model devices as devices created for preconfiguration and later deployment, while deployment and device-configuration operations depend on managed-device data. See the FortiManager 7.6 Administration Guide and Fortinet's model devices documentation.

QUESTION NO: 5

Refer to the exhibit.



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: B D

Explanation:

FortiGate HQ-NGFW-1 can contact the FortiManager acting as FortiGuard Distribution Server (FDS) to download FortiGuard updates because the installation preview contains a FortiGuard server list entry whose server type is configured for rating updates. FortiManager can operate as an on-premises FDS, allowing managed FortiGates to obtain FortiGuard packages and rating information from FortiManager rather than contacting the public FortiGuard distribution network directly. This is particularly useful where direct Internet access is restricted or where update traffic needs to be centralized.

FortiManager will install the CA certificate named root_CA3 to authenticate FortiGate-to-FortiManager communication protocol (FGFM) tunnel connections with FortiGate HQ- NGFW-1 because the certificate shown in the generated installation configuration is part of the trust material required for the managed device's secure connection to FortiManager. Installing the CA certificate enables FortiGate to validate the relevant certificate chain during FGFM communication, maintaining authenticated encrypted management connectivity. These entries can be automatically included when FortiManager prepares device configuration associated with its management and FortiGuard-distribution functions. See Fortinet's FortiManager Administration Guide and FortiGate Administration Guide.

QUESTION NO: 6

An administrator assigns a global policy package containing both header and footer policies to a local policy package in an ADOM.

Which two statements correctly describe the resulting policy structure? Choose two answers.

A. Global header policies are installed before the local policy-package policies.

B. Global footer policies are installed after the local policy-package policies.

C. The global policy package is automatically assigned to every policy package created later in the ADOM.

D. Local policies always replace global header and footer policies during installation.

E. Global policies can be installed only when the target ADOM is in backup mode.

ANSWER: A B

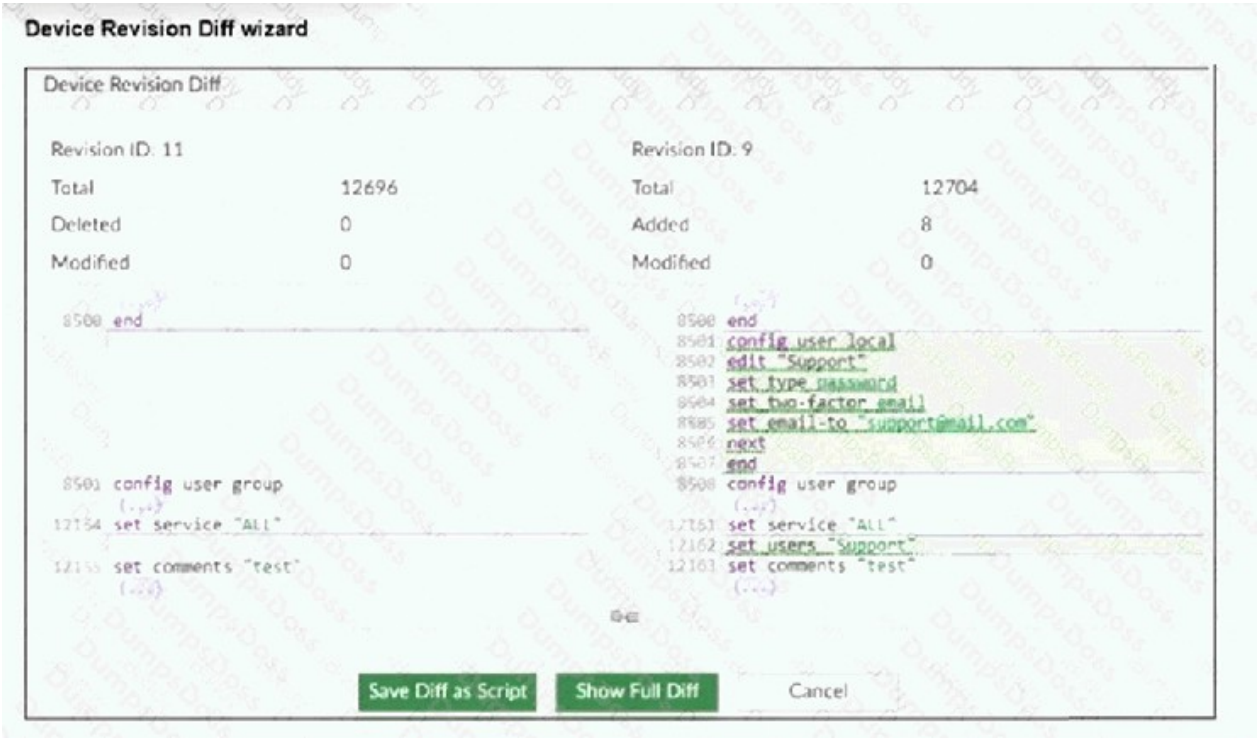
Explanation:

Global header policies are placed before the local policies in the assigned policy package, while global footer policies are placed after the local policies. This allows centrally managed rules to be enforced before or after the ADOM-specific policy rules as designed.

Global policy packages are assigned explicitly to policy packages. The administrator can choose which local policy packages receive the global policy package; creating another local policy package does not automatically assign the global package to it.

QUESTION NO: 7

Refer to the exhibits.



CLI output

```
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: OK; dm: installed; conn: up; template:[installed]default
                |- vdom:[3]root flags:0 adom:My_ADOM pkg:[unknown]BR1-FGT-1
```

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 the Configuration Revision History window 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: D

Explanation:

The administrator installed only the device-level configuration. A configuration revision revert in FortiManager restores the managed device's device database to the selected historical revision. This includes device-specific settings that FortiManager tracks, such as system and interface-related configuration, but it does not restore the policy package and associated policy/object database as part of the revert operation.

The CLI status shown after the action is consistent with this behavior: the device-manager portion is installed and synchronized, indicating that the device-level revision was applied, while the policy-package state does not show a corresponding installed and synchronized policy deployment. Consequently, reverting revision ID 9 and then installing performs a device-level installation only. To recover policy and object information from the relevant configuration state, the administrator must subsequently use the appropriate import or policy/object synchronization workflow, rather than expecting the revision revert itself to reinstall the policy package.

Fortinet documents configuration revision operations and their scope in the FortiManager 7.6 Administration Guide. See also Fortinet's Configuration Revision History documentation for the revision-management workflow.