DO NOT REPRINT
© FORTINET
BrainDumps.com

FortiManager

Lab Guide

for FortiManager 7.2

FORTINET
Training Institute

Fortinet Vouchers & Dumps are Available on Braindumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

Fortinet Training Institute - Library

https://training.fortinet.com

Fortinet Product Documentation

https://docs.fortinet.com

Fortinet Knowledge Base

https://kb.fortinet.com

Fortinet Fuse User Community

https://fusecommunity.fortinet.com/home

Fortinet Forums

https://forum.fortinet.com

Fortinet Product Support

https://support.fortinet.com

FortiGuard Labs

https://www.fortiguard.com

Fortinet Training Program Information

https://www.fortinet.com/nse-training

Fortinet | Pearson VUE

https://home.pearsonvue.com/fortinet

Fortinet Training Institute Helpdesk (training questions, comments, feedback)

https://helpdesk.training.fortinet.com/support/home

1/10/2023

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

TABLE OF CONTENTS

Network Topology 6
Lab 1: Initial Configuration 7
Exercise 1: Examining the Initial Configuration 10
Examine the Initial Configuration Using the CLI 10
Examine the Initial Configuration Using the GUI 12
Exercise 2: Configuring ADOMs 16
Enable ADOMs 16
View ADOM Information 16
Configure ADOMs 18
Exercise 3: Adding FortiAnalyzer to FortiManager 21
Lab 2: Administration and Management 24
Exercise 1: Creating and Assigning Administrators 25
Test Administrator Privileges 26
Restrict Administrator Access Using a Trusted Host 27
Test the Restricted Administrator Access 28
Exercise 2: Enabling ADOM Locking (Workspace Mode) 30
Enable ADOM Locking (Workspace Mode) 30
Exercise 3: Backing Up and Restoring FortiManager 32
Back Up the FortiManager Configuration 32
Restore the FortiManager Configuration 33
Exercise 4: Monitoring Alerts and Event Logs 35
Disable Offline Mode 35
View Alerts and Event Logs 36
Lab 3: Device Registration 38
Exercise 1: Configuring System Templates 39
Configure System Templates 39
Disable ADOM Locking (Workspace Mode) 42
Exercise 2: Registering a Device on FortiManager 44
Review the Central Management Configuration on Local-FortiGate 44
Enable Real-Time Debug 45
Add Local-FortiGate Using the Add Device Wizard 45
View the Local-FortiGate Policy Package 50
Import System Template Settings From FortiGate 51

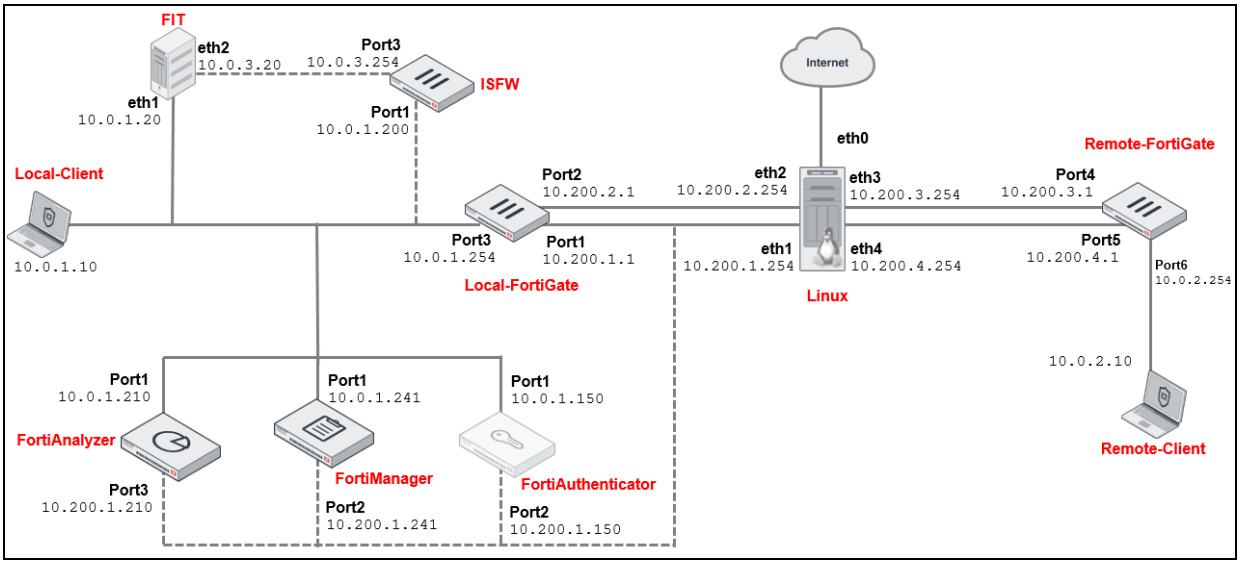
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET
Add Remote-FortiGate Using the Add Device Wizard 54
Assign the System Template to Local-FortiGate and Remote-FortiGate 55
Lab 4: Device-Level Configuration and Installation 58
Exercise 1: Understanding the Statuses of Managed Devices 59
Exercise 2: Installing System Template Changes on Managed Devices 62
Install System Templates 62
Check the Status of the Managed Device 64
View the Pushed Configuration on FortiGate 66
Exercise 3: Viewing the Auto Update Status and Revision History 68
Make Direct Changes on Local-FortiGate 68
Make Direct Changes on Remote-FortiGate 69
View the Auto Update Status and Revision History 69
View the Installation Log 71
View the Auto Update Status, Revision History, and Installation Log for Remote-FortiGate (Optional) 72
Check the Task Monitor 72
Exercise 4: Configuring Device-Level Changes 74
Change the Interface Settings of the Managed FortiGate 74
Filter Devices Based on Status 76
Configure the Administrator Account 76
Exercise 5: Installing Configuration Changes 80
Use the Install Wizard 80
View the Revision Differences 83
Exercise 6: Using Scripts 86
Configure Scripts 86
Run and Install Scripts 88
Generate Traffic With FIT 91
Lab 5: Policies and Objects 92
Exercise 1: Importing Policies 93
Import Policies 93
Create ADOM Revisions 96
Exercise 2: Enabling Workflow Mode 98
Exercise 3: Creating a Common Policy for Multiple Devices 109
Create Dynamic Mappings for Address Objects 109
Create Dynamic Mappings for Interfaces and Device Zones 112
Import and Install a CLI Script to Delete Policies 115
Run and Install the Scripts 116
Create a Common Policy Package, an Installation Target, and Use Install On 121
Exercise 4: Running a FortiAnalyzer Report 130
View Logs 130
Run a FortiAnalyzer Report 131
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET
Lab 6: Global ADOM Policy Configuration 134
Exercise 1: Creating and Assigning Header Policies in the Global ADOM 135
Lab 7: Diagnostics and Troubleshooting 140
Exercise 1: Diagnosing and Troubleshooting Installation Issues 143
View the Installation Preview 143
View the DNS Configuration 145
Install Device-Level Configuration Changes 147
Exercise 2: Troubleshooting Policy Import Issues 151
View the Policy Package and Objects 151
Review Policies and Objects Locally on Remote-FortiGate 152
Import a Policy Package 153
Check the Impact of a Partial Policy Import (Optional) 156
Fix a Partial Policy Import Issue 158
Retrieve the New Configuration From FortiManager 160
Lab 8: Additional Configuration 163
Exercise 1: Examining FortiGuard Management 164
Diagnose FortiGuard Issues 165
Exercise 2: Upgrading FortiGate Firmware Using FortiManager 167
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

Network Topology



Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

Lab 1: Initial Configuration

In this lab, you will examine network settings on the FortiManager CLI and GUI. You will also add FortiAnalyzer to FortiManager, for logging and reporting.

Objectives

- Examine initial system settings, including network and time settings
- Add FortiAnalyzer to FortiManager

Time to Complete

Estimated: 40 minutes

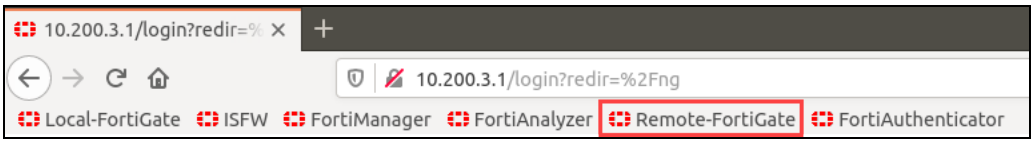
Prerequisites

This lab environment is also used for FortiGate Security 7.2 and FortiGate Infrastructure 7.2 training and initializes in a different state than is required for FortiManager 7.2.1 training.

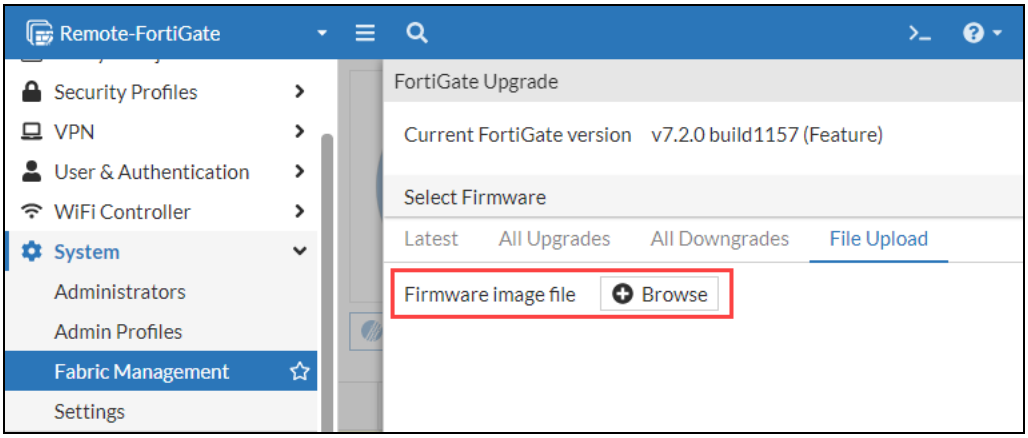
Before you begin this lab, you must update the firmware and initial configuration on the Local-FortiGate and Remote-FortiGate VMs.

To update the FortiGate firmware on FortiGate devices

1. On the Local-Client VM, open a browser, and then log in to the Remote-FortiGate GUI at `10.200.3.1` with the username `admin` and password `password`.



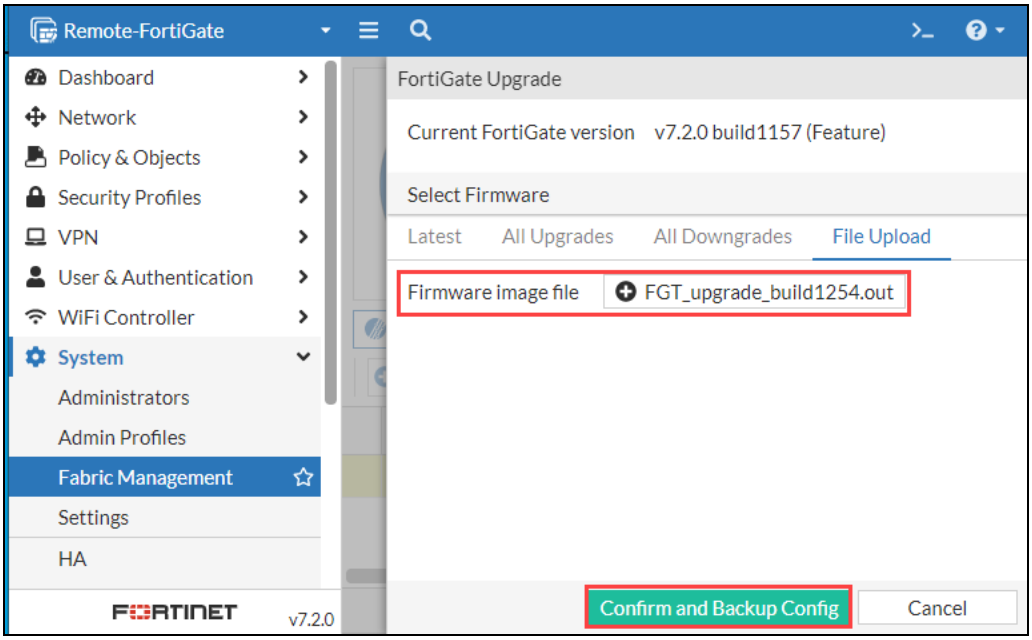
2. Click **System** > **Fabric Management**, select **Remote-FortiGate**, and then click **Upgrade**.
3. In the **Select Firmware** section, click the **File Upload** tab, and then click **Browse**.



Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

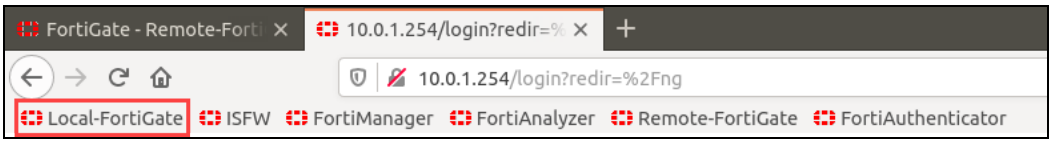
DO NOT REPRINT Brave-Dumps.com
© FORTINET

4. Browse to **Desktop** > **Resources** > **FortiManager** > **FGT-firmware**, select `FGT_upgrade_build1254.out`, and then click **Open** to load the file.
5. Click **Confirm and Backup Config**, and then in the warning window, click **Continue** to initiate the upgrade.



The system reboots. Click **Cancel** so that the configuration backup file is not saved.

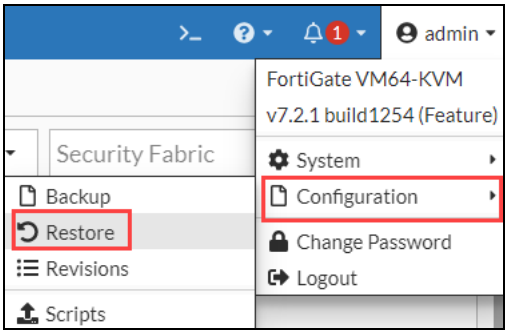
6. Open another browser tab, and then log in to the Local-FortiGate GUI at `10.0.1.254` with the username `admin` and password `password`.



7. Repeat the procedure to update the firmware for the Local-FortiGate VM.
   This procedure can take up to 10 minutes to upgrade.

To restore the Remote-FortiGate configuration file

1. On the Local-Client VM, open a browser, and then log in to the Remote-FortiGate GUI at `10.200.3.1` with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.



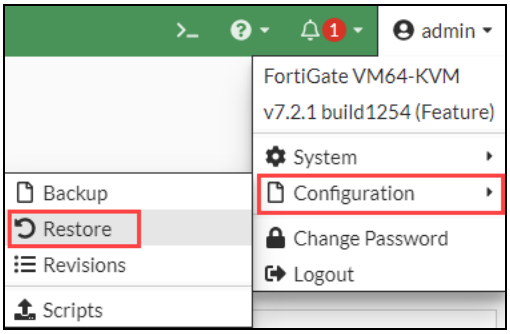
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop** > **Resources** > **FortiManager** > **Introduction**, select `remote-Initial.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

To restore the Local-FortiGate configuration file

1. On the Local-Client VM, open a browser, and then log in to the Local-FortiGate GUI at `10.0.1.254` with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.



3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop** > **Resources** > **FortiManager** > **Introduction**, select `local-Initial.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.
7. After the device restarts, close the browsers for both the Remote-FortiGate GUI and Local-FortiGate GUI.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

Exercise 1: Examining the Initial Configuration

FortiManager is preconfigured with initial network settings.

In this exercise, you will explore the basic configuration settings on the FortiManager CLI and GUI.

Examine the Initial Configuration Using the CLI

You will start by accessing FortiManager, using the CLI, to examine the initial configuration.

To examine the initial configuration using the CLI

1. Log in to the FortiManager CLI with the username `admin` and password `password`.
2. Enter the following command to display basic status information about FortiManager:

CLI command	Data	Result
`# get system status`	What is the firmware version? Knowing your FortiManager firmware version is important because it identifies which Fortinet products and firmware versions are supported.	
	What is the administrative domain (ADOM) configuration? By default, ADOMs are disabled.	
	What is the time zone? It is important that the system time on FortiManager and all registered devices is synchronized for tunnel negotiations and logging (if the FortiAnalyzer feature is used).	
	What is the license status? To ensure FortiManager continues to manage devices, a valid license is required.	

3. Enter the following command to display information about the configuration of the FortiManager interface:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

CLI command	Diagnostic	Result
`# show system interface`	What is the IP address for port1? port1 is the management port and has the IP address of FortiManager.	
	Which administrative access protocols are configured for port1? This helps troubleshoot any access issues you may experience. For example, this PuTTY session cannot connect without the SSH protocol enabled.	
	What is configured for the service access? If devices are configured to use FortiManager as the local FDS server, service access allows FortiManager to respond to FortiGuard queries that devices make.	
	What is the IP address for port2? According to the network topology diagram, port2 is where traffic is routed between Remote-FortiGate and FortiManager. Remote-FortiGate, therefore, connects to FortiManager with this port2 IP address.	
	Which administrative access protocols are configured for port2?	

4. Enter the following command to display DNS settings information:

CLI command	Diagnostic	Result
`# show system dns`	What are the primary and secondary DNS settings? By default, FortiManager uses FortiGuard DNS servers.	

5. Enter the following commands to display NTP settings information:

CLI command	Diagnostic	Result
`# get system ntp`	Is NTP enabled? NTP is recommended on FortiManager and all registered devices for correct tunnel establishment between FortiGate and FortiManager.	

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

CLI command	Diagnostic	Result
`# show system ntp`	Which server is configured for NTP? By default, Fortinet servers are configured for NTP.	

6. Enter the following command to display information about the FortiManager routing configuration:

CLI command	Diagnostic	Result
`# show system route`	What is the gateway route associated with port2? According to the network topology diagram, this IP address is the default route to the internet.	

7. To test basic network connectivity, and to ensure the default route to the internet is working, enter the following command to ping IP address `8.8.8.8` (a public IP address that is highly available):

```
execute ping 8.8.8.8
```

Packets should transmit successfully.

```
FMG-VM64 # execute ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: seq=0 ttl=115 time=6.279 ms
64 bytes from 8.8.8.8: seq=1 ttl=115 time=5.379 ms
64 bytes from 8.8.8.8: seq=2 ttl=115 time=4.856 ms
64 bytes from 8.8.8.8: seq=3 ttl=115 time=5.389 ms

--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 4.856/5.475/6.279 ms
```

8. Close the PuTTY session.

Examine the Initial Configuration Using the GUI

You will now log in to FortiManager, using the GUI, to examine the initial configuration.

To examine the initial configuration using the GUI

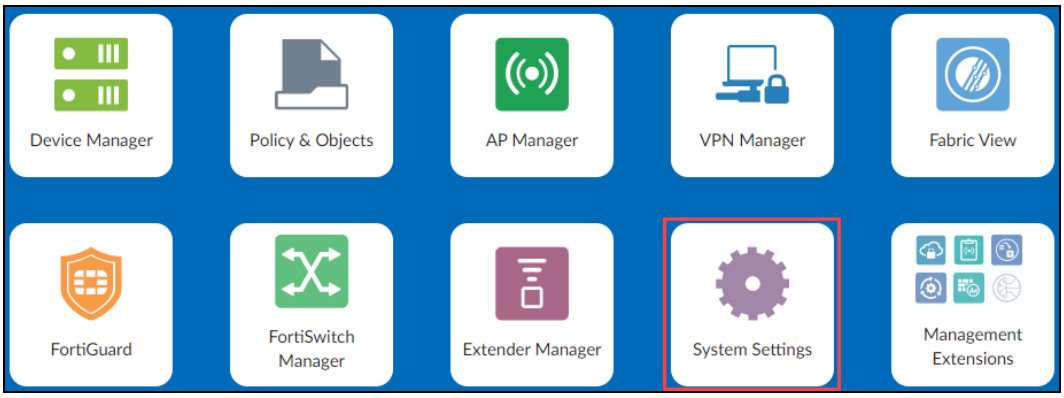
1. Log in to the FortiManager GUI with the username `admin` and password `password`.
   If a security alert appears, accept the self-signed certificate or security exemption.

All lab exercises were tested running Mozilla Firefox on the Local-Client VM and Remote-Client VM. To get consistent results, we recommend using Firefox in this virtual environment.

2. Click **System Settings**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET



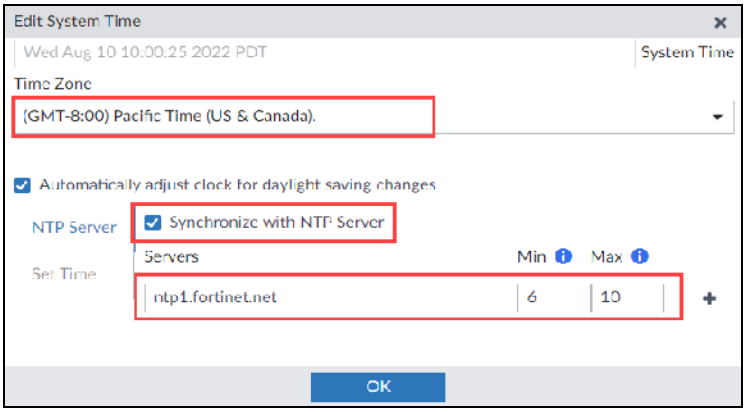
The dashboard shows the FortiManager widgets that display information, such as **System Information**, **License Information**, **System Resources**, and more.

3. In the **System Information** and **License Information** widgets, locate the following information:
   - Firmware version
   - Administrative domain status
   - System time and time zone
   - License status (VM)

   These widgets display the same information as the `get system status` CLI command.

4. In the **System Information** widget, in the **System Time** field, click the edit icon to view the NTP information.

This displays the same information as the `get system ntp` and `show system ntp` CLI commands.



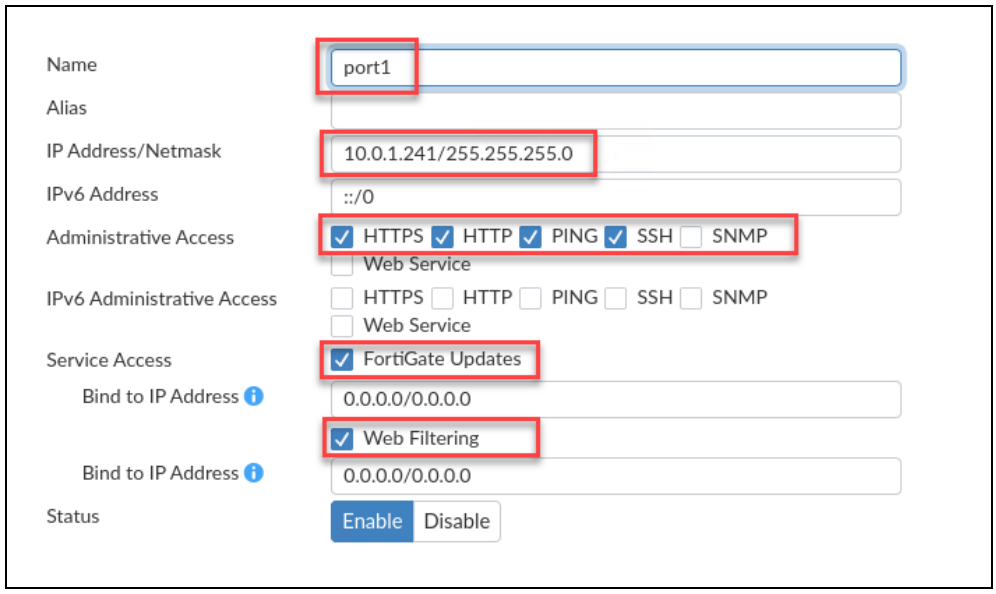
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

You will manage Local-FortiGate and Remote-FortiGate using FortiManager—they are configured with the same time zone and NTP server.

5. In the menu on the left, click **Network** > **port1**.
6. Edit **port1**.

   This section displays information about the port1 management interface, including the IP address, administrative access protocols, and service access. This displays the same information as the `show system interface` CLI command.



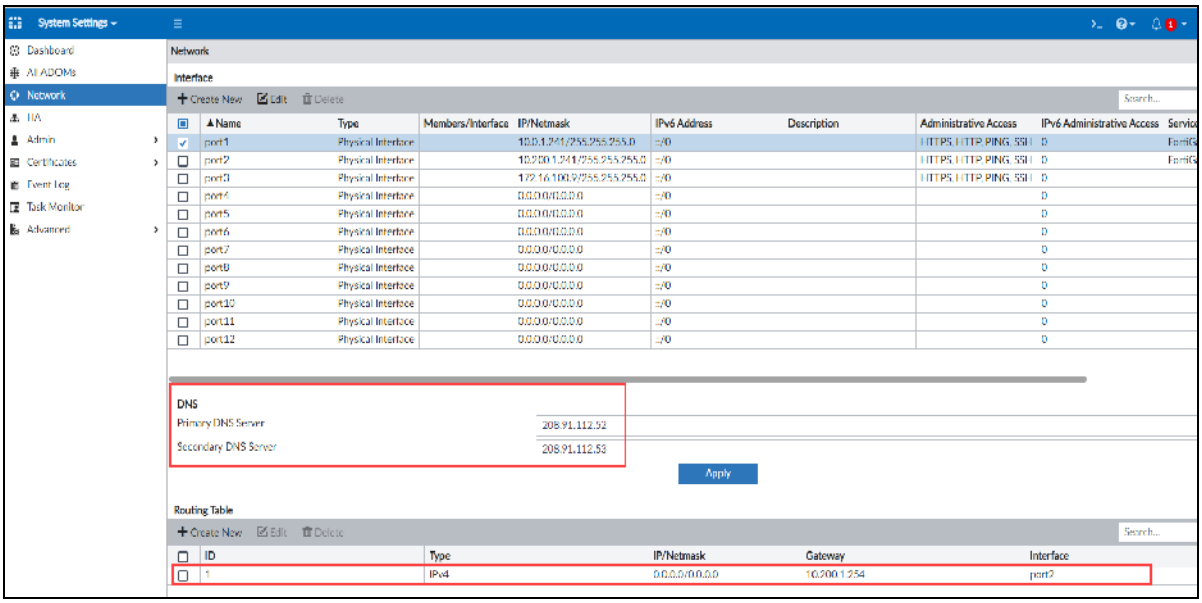
The `fgtupdates` and `fclupdates` CLI commands are equivalent to **FortiGate Updates** on the GUI. The `webfilter-antispam` CLI command is equivalent to **Web Filtering** on the GUI.

7. In the **port1** network interface window, click **Cancel**.

   The bottom of the **Network** page displays the **Routing Table**, **DNS** information, and all other interfaces. This displays the same information as the `show system route`, `show system dns`, and `show system interface` CLI commands.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET



Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

Exercise 2: Configuring ADOMs

Administrative domains (ADOMs) group devices for administrators to monitor and manage. The purpose of ADOMs is to divide the administration of devices and control (restrict) access.

In this exercise, you will enable and configure ADOMs.

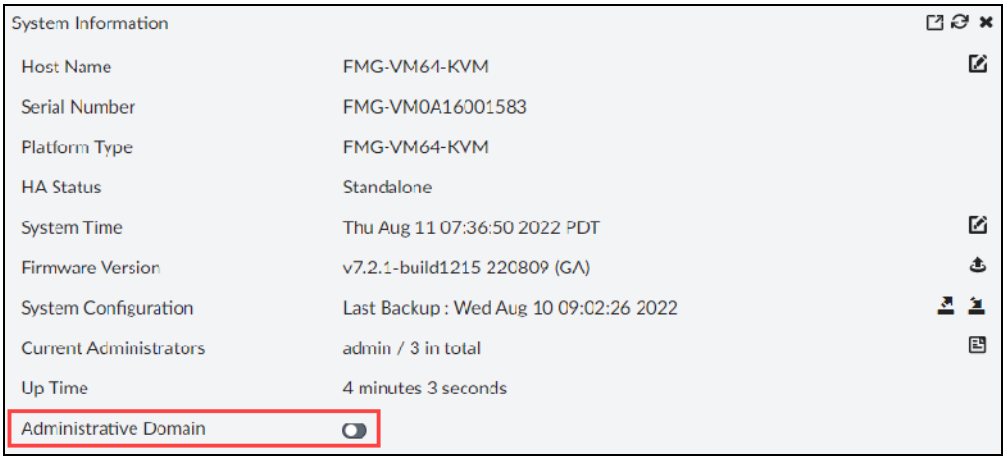
Enable ADOMs

ADOMs are not enabled by default, and can be enabled only by the **admin** administrator, or an administrator with the **Super_User** access profile.

You will enable ADOMs on FortiManager.

To enable ADOMs

1. Log in to the FortiManager GUI with the username `admin` and password `password`.
2. Click **System Settings**.
3. In the **System Information** widget, enable **Administrative Domain**.



4. Click **OK**.
   FortiManager logs you out.

View ADOM Information

Before you create new ADOMs, you should be aware of the types of ADOMs that are available to you. You will view ADOM information using both the GUI and CLI.

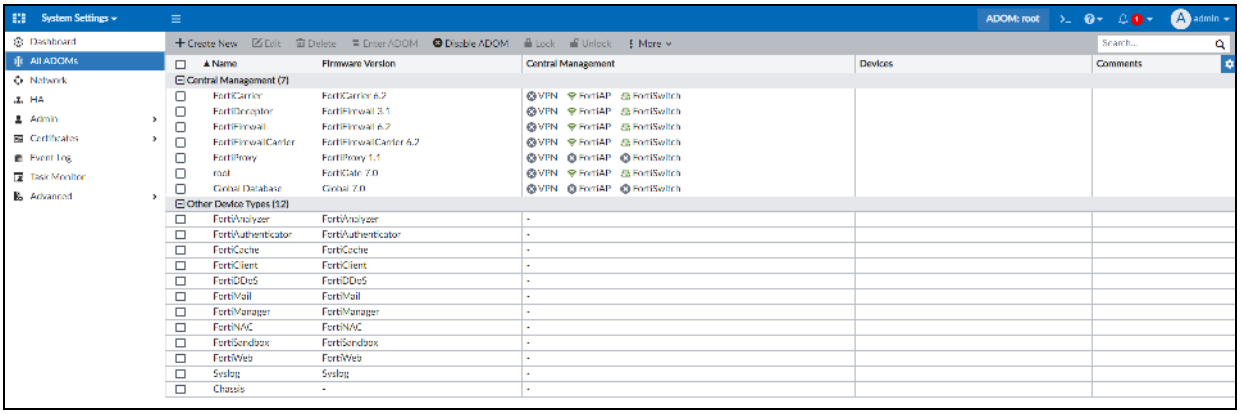
To view ADOM information

1. Log in to the FortiManager GUI with the username `admin` and password `password`.
2. Select the **root** ADOM.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

3. Click **System Settings**.
4. Click **All ADOMs**.



5. Log in to the FortiManager CLI with the username `admin` and password `password`.
6. Enter the following command to view the ADOMs that are currently enabled on FortiManager and the type of device you can register to each ADOM:

The CLI output formatting is easier to read if you maximize your PuTTY window. If you already executed the command, once the window is maximized, press the up arrow to show the last command that you entered, and then press `Enter` to run the command again.

```
# diagnose dvm adom list
```

```
FortiManager # diagnose dvm adom list
There are currently 19 ADOMs (count for license: 0/10):
OID     STATE    PRODUCT OSVER MR  LIC NAME                 MODE   VPN MANAGEMENT        IPS        ISDB
108     enabled  FAZ     7.0   0       FortiAnalyzer        Normal Policy & Device VPNs 21.336     7.2387
124     enabled  FAC     6.0   2       FortiAuthenticator   Normal Policy & Device VPNs 20.302     7.2361
112     enabled  FCH     4.0   2       FortiCache           Normal Policy & Device VPNs 0.0        0.0
104     enabled  FOC     7.0   0       FortiCarrier         Normal Policy & Device VPNs 21.336     7.2387
114     enabled  FCT     7.0   0       FortiClient          Normal Policy & Device VPNs 21.336     7.2387
122     enabled  FDD     6.0   1       FortiDDoS            Normal Policy & Device VPNs 20.302     7.2361
151     enabled  FDC     3.0   3       FortiDeceptor        Normal Policy & Device VPNs 0.0        0.0
149     enabled  FFW     6.0   2       FortiFirewall        Normal Policy & Device VPNs 20.302     7.2361
159     enabled  FWC     6.0   2       FortiFirewallCarrier Normal Policy & Device VPNs 20.302     7.2361
106     enabled  FML     6.0   4       FortiMail            Normal Policy & Device VPNs 20.302     7.2387
118     enabled  FMG     7.0   0       FortiManager         Normal Policy & Device VPNs 21.336     7.2387
126     enabled  FPX     2.0   0       FortiProxy           Normal Policy & Device VPNs 0.0        0.0
120     enabled  FSA     4.0   0       FortiSandbox         Normal Policy & Device VPNs 0.0        0.0
110     enabled  FWB     6.0   3       FortiWeb             Normal Policy & Device VPNs 20.302     7.2361
116     enabled  LOG     0.0   0       Syslog               Normal Policy & Device VPNs 0.0        0.0
128     enabled  FSF     7.0   0       Unmanaged Devices    Normal Policy & Device VPNs 21.336     7.2387
102     enabled  Chassis 6.0   0       Chassis              Normal Policy & Device VPNs 20.302     7.2361
3       enabled  FOS     7.0   0       root                 Normal Policy & Device VPNs 21.336     7.2387
10      enabled  FOS     7.0   0       Global               Normal Policy & Device VPNs 21.336     7.2387
   End ADOM list
```

As you can see, FortiManager supports 19 ADOMs, each associated with different devices. The CLI also displays the supported firmware versions.

7. Close the PuTTY session.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

Configure ADOMs

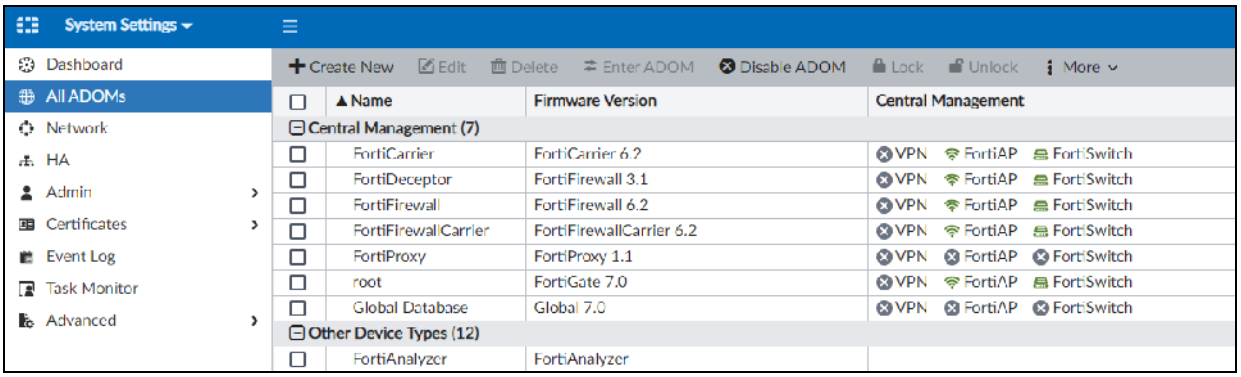
By default, when you enable ADOMs, FortiManager creates ADOMs based on supported device types. The **root** ADOM is based on the FortiGate ADOM type.

When you create a new ADOM, you must match the device type. For example, if you want to create an ADOM for FortiGate, you must select FortiGate as the ADOM type. With FortiGate ADOMs specifically, you must also select the firmware version of the FortiGate. Different firmware versions have different features, and therefore different CLI syntax. Your ADOM settings must match the device firmware.

You will create and configure a new ADOM.

To configure ADOMs

1. Continuing on the FortiManager GUI, click **System Settings** > **All ADOMs**.



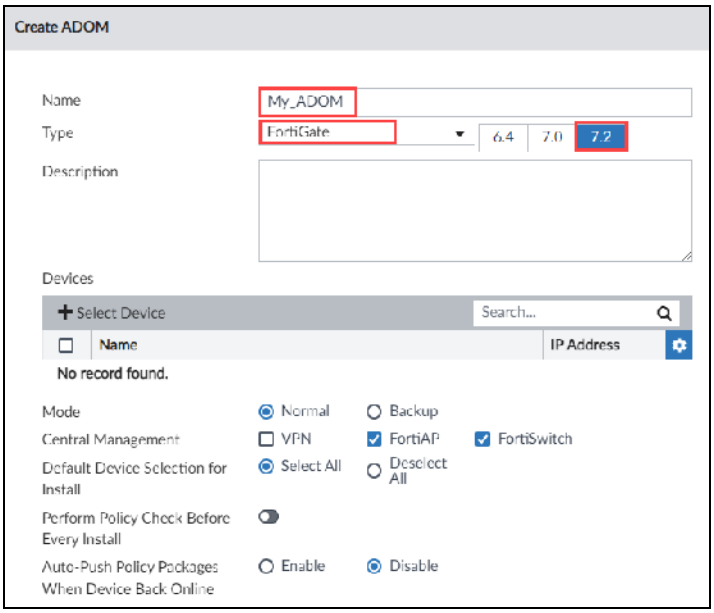
2. Click **Create New**.
3. Configure the following settings:

Field	Value
Name	My_ADOM
Type	FortiGate and 7.2

Your configuration should look like the following example:

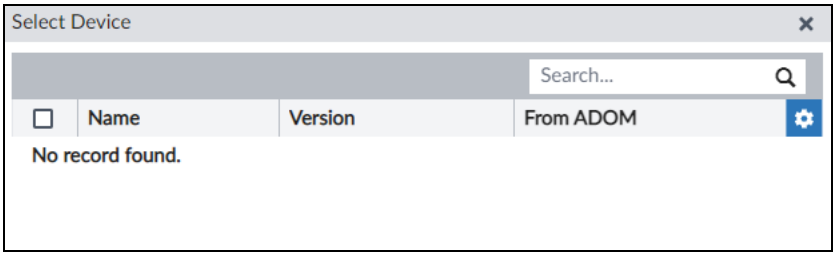
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET



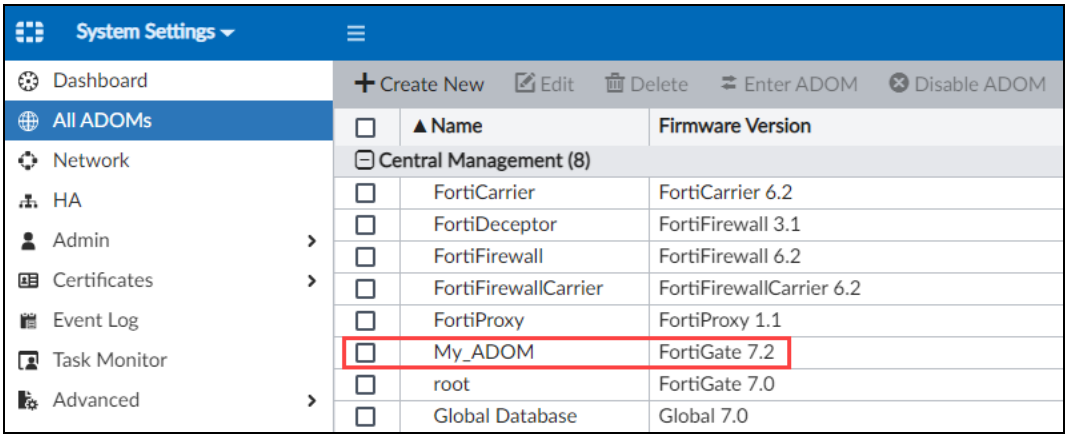
4. Click **Select Device**.

   If any devices were registered to FortiManager, you could select a device and add it to the ADOM. However, in this lab, the list is empty because no devices are registered.



5. Click **Cancel**.
6. Keep the default values for all other settings, and then click **OK**.

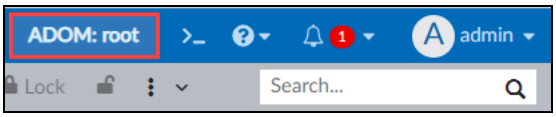
   You should see a list of predefined ADOMs, including your new ADOM.



Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

You can switch between ADOMs on the GUI. You do not have to log out and log back in. To switch between ADOMs on the GUI, in the upper-right corner, click **ADOM**. Your administrator privileges determine which ADOMs you can access.



Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

Exercise 3: Adding FortiAnalyzer to FortiManager

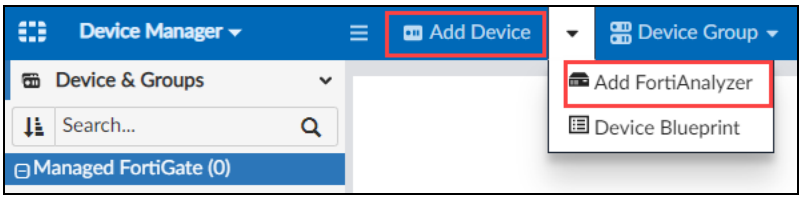
You can manage FortiAnalyzer from FortiManager. Adding a FortiAnalyzer to FortiManager gives FortiManager visibility into the logs on FortiAnalyzer, providing a single pane of glass on FortiManager. It also enables FortiAnalyzer features, such as FortiView and Log View.

You can also use FortiManager as a logging and reporting device by enabling FortiAnalyzer features on FortiManager. Remember that, unlike FortiAnalyzer, FortiManager has logging rate restrictions.

In this exercise, you will add FortiAnalyzer to FortiManager, so that you can manage FortiAnalyzer from FortiManager for logging and reporting.

To add FortiAnalyzer to FortiManager

1. Log in to the FortiAnalyzer GUI at `10.0.1.210` with the username `admin` and password `password`.
   Before you add FortiAnalyzer to FortiManager, you must enable the FortiManager **Administrative Access** checkbox on the FortiAnalyzer management interface.
2. Click **System Settings** > **Network**.
3. Select the **port1** checkbox, and then click **Edit**.
4. In the **Administrative Access** field, select the **FortiManager** checkbox.
5. Click **OK**.
6. Click **Dashboard**.
7. Enable **Administrative Domain**.
8. Click **OK**.
9. Log in to the FortiManager GUI at `10.0.1.241` with the username `admin` and password `password`.
10. Click **My_ADOM**.
11. Click **Device Manager**.
12. In the **Add Device** drop-down list, select **Add FortiAnalyzer**.



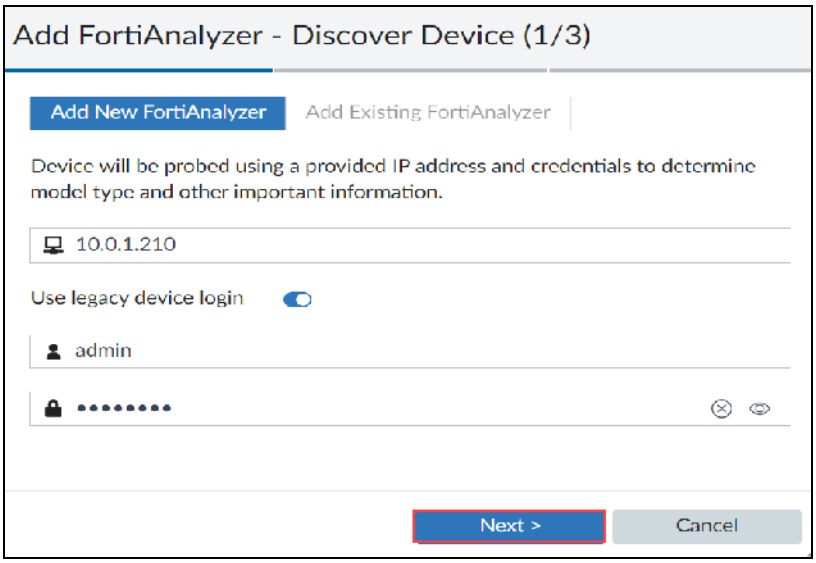
13. In the **Add FortiAnalyzer** wizard, configure the following settings:

Field	Value
IP Address	10.0.1.210
Use legacy device login	ON
Username	admin
Password	password

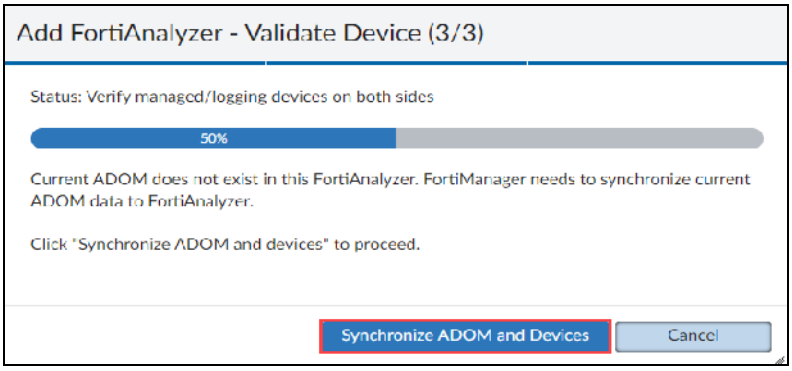
14. Click **Next**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET



15. Click **Next**.
16. Click **Synchronize ADOM and Devices**.

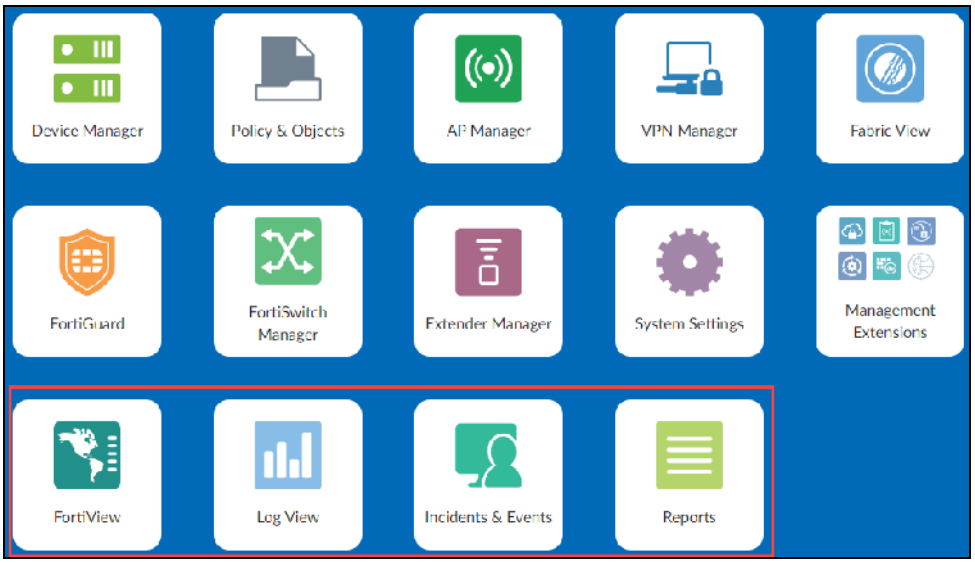


If the FortiManager ADOM does not exist on the FortiAnalyzer, a warning appears. You can add the ADOM and devices to FortiAnalyzer by clicking **Synchronize ADOM and Devices**.

17. Click **Finish**.
    You will configure logging on the FortiGate devices in a later lab.
18. Log out of FortiManager.
19. Log in to the FortiManager GUI at `10.0.1.241` with the username `admin` and password `password`.
20. Click **My_ADOM**.

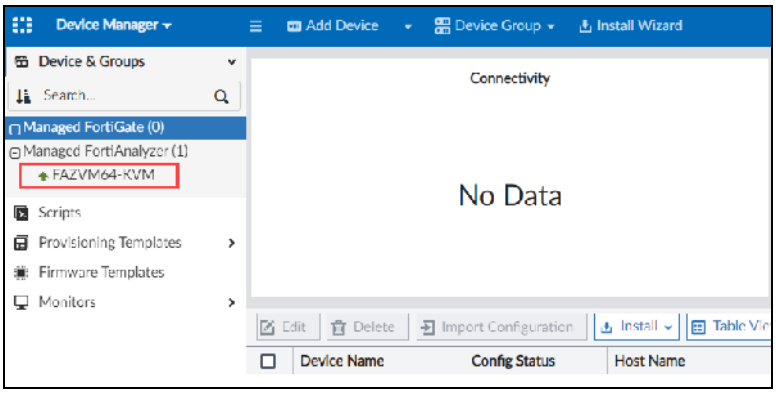
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET



Now that you have added FortiAnalyzer to FortiManager, you will notice that more panes related to logging and reporting appear—**FortiView**, **Log View**, **FortiSoC**, and **Reports**.

21. Click **Device Manager**.
22. Expand **Managed FortiAnalyzer** to see the FortiAnalyzer that you just added.



23. Log out of FortiManager.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

Lab 2: Administration and Management

In this lab, you will configure an administrator user. You will also restrict administrator access based on administrator profile, trusted hosts, and ADOMs. Then, you will enable ADOM locking, which disables concurrent access to the same ADOM.

Additionally, this lab will guide you through how to correctly back up and restore a FortiManager configuration, view alert messages in the **Alert Message Console**, and view event logs.

Objectives

- Configure an administrator and restrict access to a newly created ADOM
- Enable ADOM locking
- Back up FortiManager, restore the backup, and disable offline mode
- Read entries in the alert message console and view event logs

Time to Complete

Estimated: 45 minutes

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

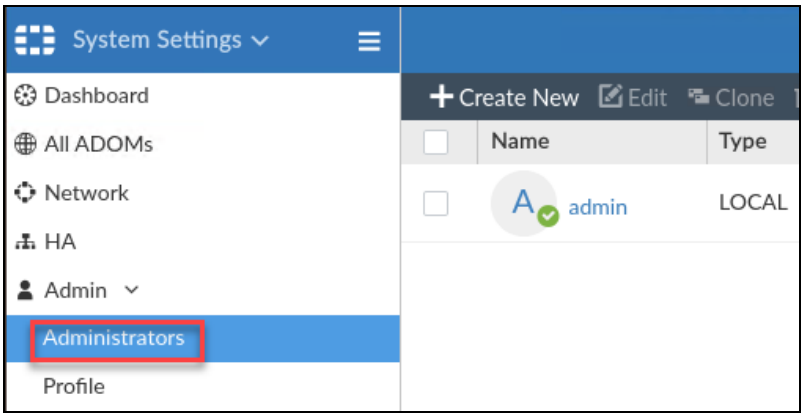
Exercise 1: Creating and Assigning Administrators

In this exercise, you will create an administrative user with restricted access permissions.

In an active deployment scenario, having more than one administrative user makes administering the network easier, especially if users are delegated specific administrative roles, or confined to specific areas within the network. In an environment with multiple administrators, you should ensure that every administrator has only the permissions necessary to do their specific job.

To create and assign administrators

1. Log in to the FortiManager GUI with the username `admin` and password `password`.
2. Click **root**.
3. Click **System Settings**.
4. Click **Admin** > **Administrators**.



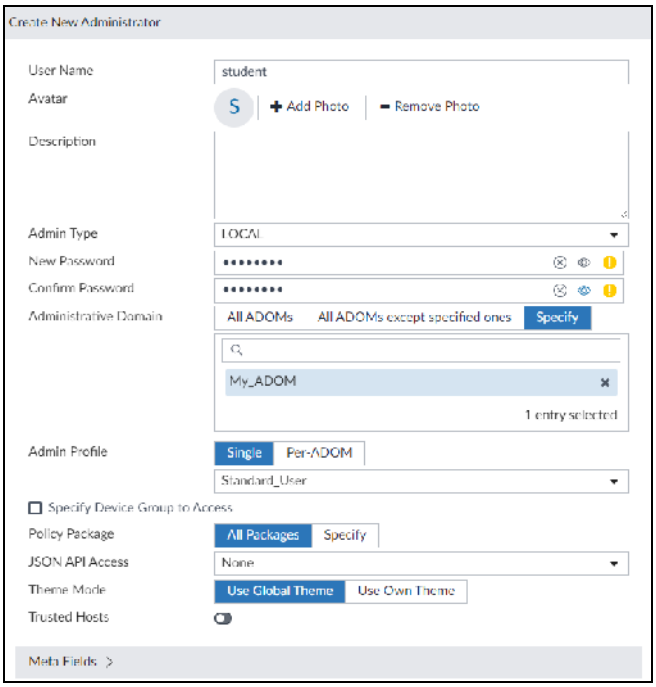
5. Click **Create New**.
6. Configure the following settings:

Field	Value
User Name	student
Admin Type	LOCAL
New Password	fortinet
Confirm Password	fortinet
Administrative Domain	Specify
Click here to select	My_ADOM
Admin Profile	Standard_User
Policy Package Access	All Packages

Your configuration should look like the following example:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

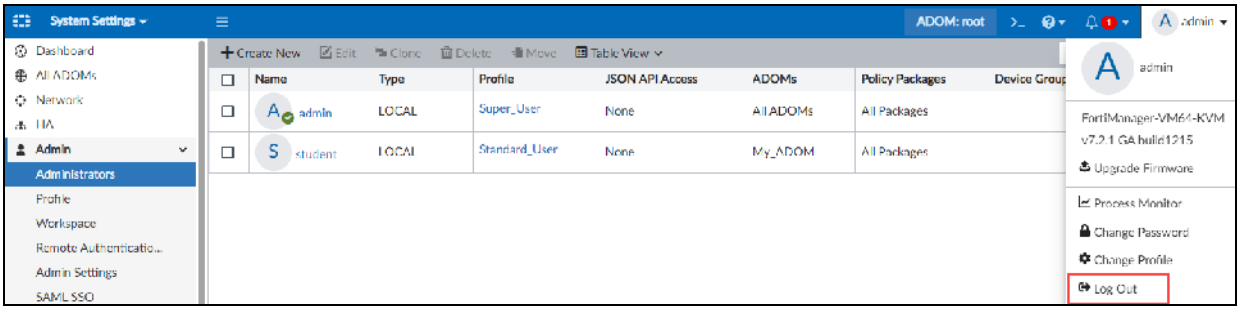
DO NOT REPRINT Brave-Dumps.com
© FORTINET



FortiManager comes with five default profiles preinstalled that you can assign to other administrative users. Alternatively, you can create your own custom profiles.

In this lab, we have assigned a preconfigured **Standard_User** profile to the newly created **student** administrator. The **Standard_User** profile provides read and write access for all device privileges, but not system privileges.

7. Keep the default values for all other settings, and then click **OK**.
8. In the upper-right corner, click **admin**.
9. Click **Log Out**.



Test Administrator Privileges

You will log in to FortiManager with the administrator account (**student**) that you just created, and then test the administrator privileges.

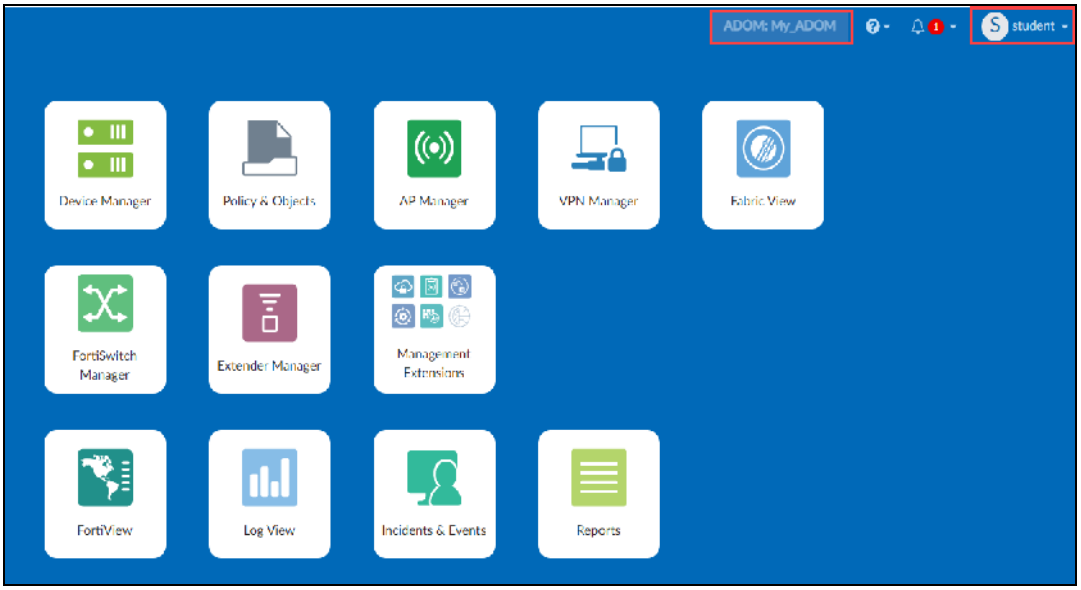
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

To test administrator privileges

1. Log in to the FortiManager GUI with the username `student` and password `fortinet`.
   You are limited to the **My_ADOM** administrative domain.

   Also, there are no **System Settings** and **FortiGuard** tabs.



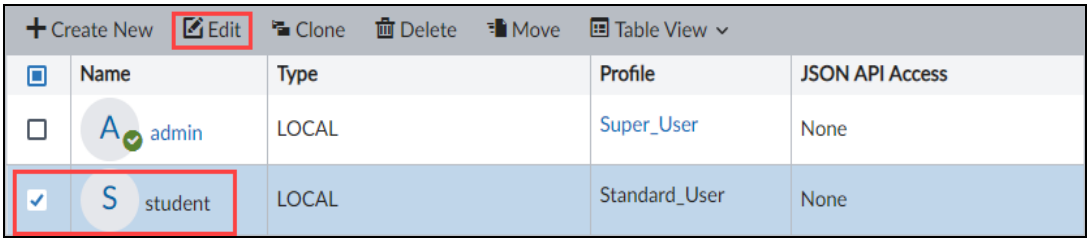
   The preceding image shows how you can control or restrict administrator access based on administrative profiles and ADOMs.

Restrict Administrator Access Using a Trusted Host

You will restrict access to FortiManager by configuring a trusted host for the administrator accounts. Only administrators connecting from a trusted subnet can access FortiManager.

To restrict administrator access

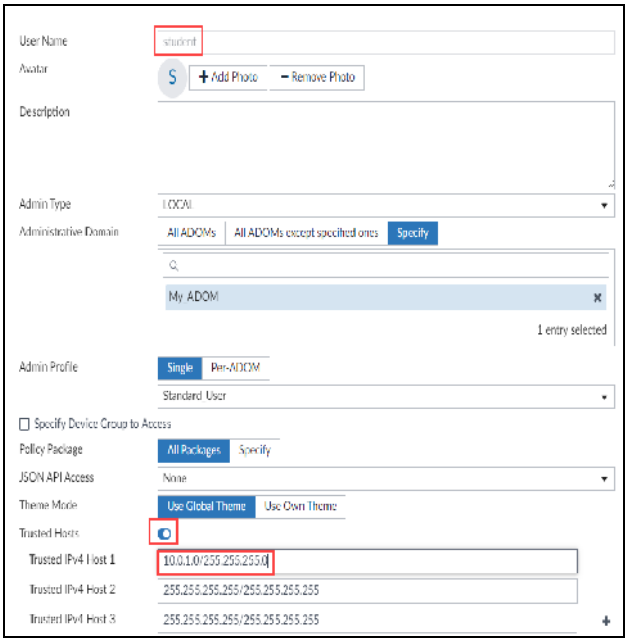
1. On the FortiManager GUI, log out of the GUI session for the **student** account.
2. Log in as the administrator with the username `admin` and password `password`.
3. Click **root**.
4. Click **System Settings**.
5. Click **Admin** > **Administrators**.
6. Edit the **student** account.



Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

7. Enable **Trusted Hosts**.
8. In the **Trusted IPv4 Host 1** field, type `10.0.1.0/24`.



9. Click **OK** to save the changes.

Test the Restricted Administrator Access

You will confirm that administrators outside the subnet 10.0.1.0/24 cannot access FortiManager.

To test the restricted administrator access

1. On the Remote-Client VM, open a browser, and then go to `https://10.200.1.241`.
2. Try to log in to the FortiManager GUI with the username `student` and password `fortinet`.
   What is the result?

   Because you are trying to connect from the 10.0.2.10 IP address, your login authentication fails. This is because you restricted logins to only the source IP addresses in the list of trusted hosts.

The IP address specified in the URL here is not the same as the one you used previously, because now FortiManager is being accessed from a device that is in a different part of the network (see Network Topology on page 6). Now, you are connecting to the port2 interface of the FortiManager device.

3. Return to the Local-Client VM.
4. Ensure that you are still logged in to the FortiManager GUI as `admin`, and then edit the **student** account.
5. Disable **Trusted Hosts**.
6. Click **OK**.
   Disabling **Trusted Hosts** allows the administrative user to log in from any IP address and subnet.

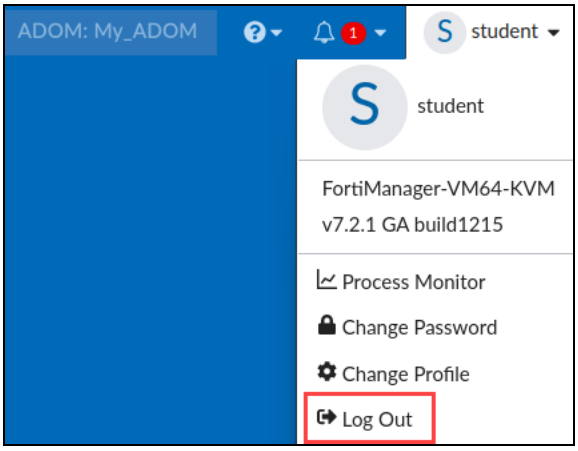
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

7. Return to the Remote-Client VM, and then try to log in to the FortiManager GUI again with the username `student` and password `fortinet`.

   This time, you should gain access because you just turned off the requirement to log in from a trusted host.

8. Log out of FortiManager.



Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

Exercise 2: Enabling ADOM Locking (Workspace Mode)

By default, multiple administrators can log in to the same ADOM at the same time, which allows concurrent access. This can cause conflicts, however, if two or more administrators try to make changes in the same ADOM at the same time.

You will enable ADOM locking, which includes the following:

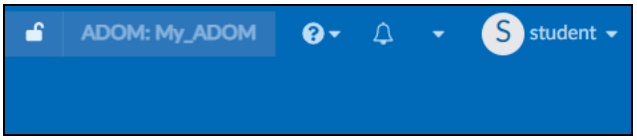
- Disabling concurrent ADOM access
- ADOM locking
- Single administrator access to the ADOM with read/write privileges
- Read-only access to the ADOM for all other administrators

Enable ADOM Locking (Workspace Mode)

Before you enable ADOM locking, ensure that all FortiManager administrators are notified and asked to save their work on FortiManager, because enabling ADOM locking terminates all management sessions.

To enable ADOM locking (workspace mode)

1. Log in to the FortiManager GUI with the username `admin` and password `password`.
2. Click **My_ADOM**.
3. Click **System Settings**.
4. Click **Admin** > **Workspace**.
5. Click **Workspace**, click **Apply**, and then click **OK**.
   FortiManager logs you out.
6. Log in to the FortiManager GUI with the username `student` and password `fortinet`.
7. At the top of the screen, click the lock icon.



   The lock icon changes from unlocked to locked and green.
8. On the Remote-Client VM, open a browser, and then go to `https://10.200.1.241`.
9. Log in to the FortiManager GUI with the username `admin` and password `password`.
   The lock icon is locked for **My_ADOM**.
10. Hover over the lock icon.
    The name of the administrator who locked the ADOM appears, along with the date and time it was locked.
11. Click **My_ADOM**.
12. Log out of the FortiManager **admin** account.
13. Return to the Local-Client VM, and then log out of the FortiManager **student** account.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

If an administrator locked one or more ADOMs, and then logged out of FortiManager, all of those ADOMs are unlocked.

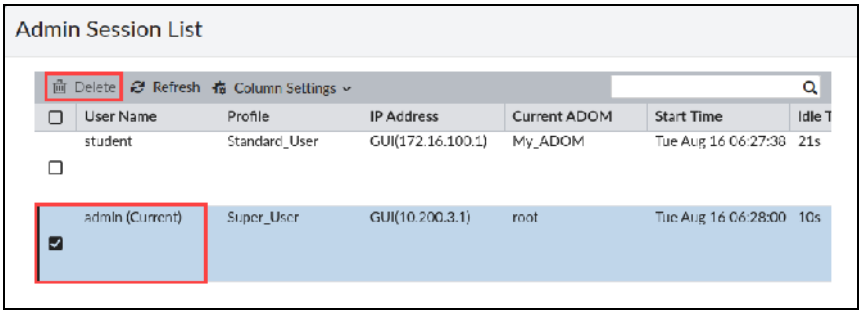
In this example, when the **student** administrator locked **My_ADOM**, and then logged out, FortiManager unlocked **My_ADOM**.

Always log out gracefully from FortiManager when ADOM locking is enabled.

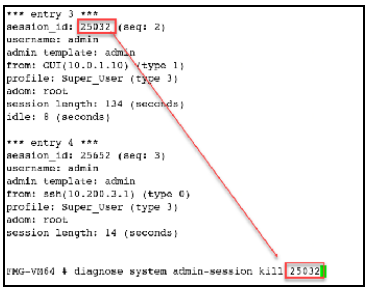
If a session is not closed gracefully (for example, because of a PC crash or closed browser window), FortiManager does not close the administrator session until it times out or the session is deleted. Until this time, the ADOM remains in a locked state.

If this situation arises and you cannot wait for the administrator session to time out, delete the session manually using the GUI or CLI.

On the GUI, on the **System Settings** pane, go to the **System Information** widget, and then click **Current Administrators** > **Current Session List**.



On the CLI, enter `diagnose system admin-session list`.



Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

Exercise 3: Backing Up and Restoring FortiManager

In this exercise, you will back up the FortiManager configuration.

In an active deployment scenario, it is a best practice to back up the device configuration before making any configuration changes. If the new configuration does not perform as expected, you can revert to the last working configuration. During these labs, it is beneficial for you to have a backup of the initial configuration, in case you must revert the configuration.

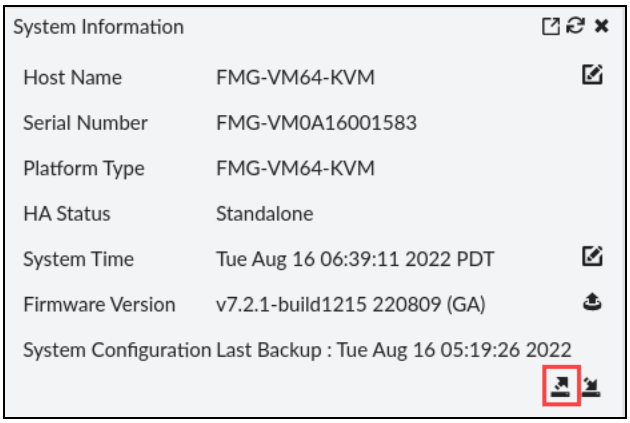
FortiManager configuration files are not stored in plaintext like FortiGate configuration files. They are stored as DAT files. You can uncompress them, and then view them offline using archive tools, such as WinRAR and tar.

Back Up the FortiManager Configuration

You will back up the FortiManager configuration using the GUI.

To back up FortiManager

1. On the Local-Client VM, open a browser, and then log in to the FortiManager GUI with the username `admin` and password `password`.
2. Select **root**.
3. At the top of the screen, click the lock icon to lock it.
4. Click **System Settings**.
5. In the **System Information** widget, click **System Configuration**, and then click the **backup** icon.



6. Clear the **Encryption** checkbox.
7. Click **OK**.
8. Select **Save File**.
9. Click **OK**.
10. Note the location of the backup file, and then rename this file to `lab2.dat`.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

11. Continuing on the FortiManager GUI, click **Admin** > **Administrators**.
12. Right-click **student**, and then click **Delete**.
13. Click **OK**.

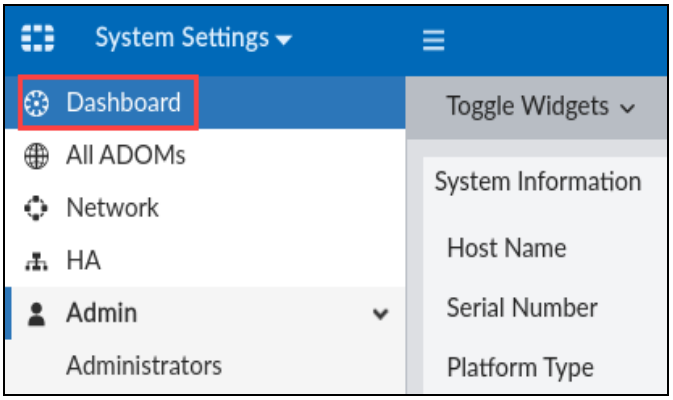
Restore the FortiManager Configuration

You can use the following options when you restore a FortiManager configuration:

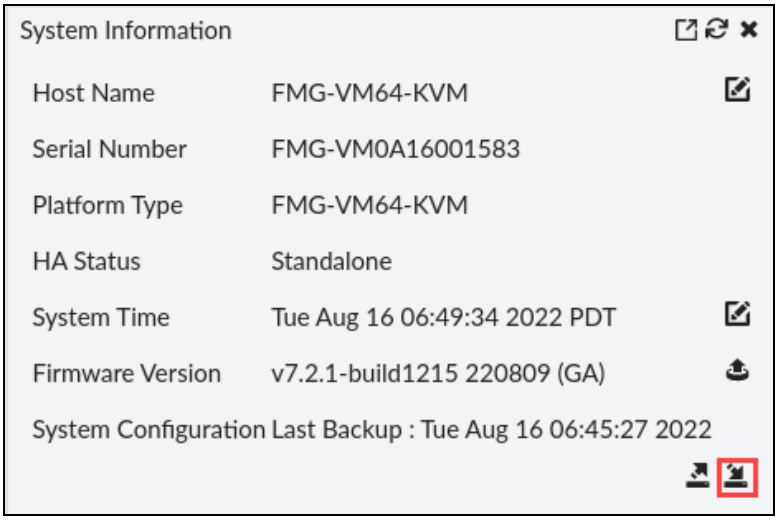
- **Overwrite current IP, routing and HA settings**: By default, this option is enabled. If FortiManager has an existing configuration, restoring a backup will overwrite everything, including the current IP address, routing, and HA settings. If you disable this option, FortiManager will still restore the configuration settings that are related to the device information and global database information, but it will preserve the basic HA and network settings.
- **Restore in Offline Mode**: By default, this option is enabled and grayed out–you cannot disable it. While restoring, FortiManager temporarily disables the communication channel between FortiManager and all managed devices. This is a safety measure in case any of the devices are being managed by another FortiManager device. To re-enable the communication, disable **Offline Mode**.

To restore FortiManager

1. Continuing on the FortiManager GUI, click **Dashboard**.



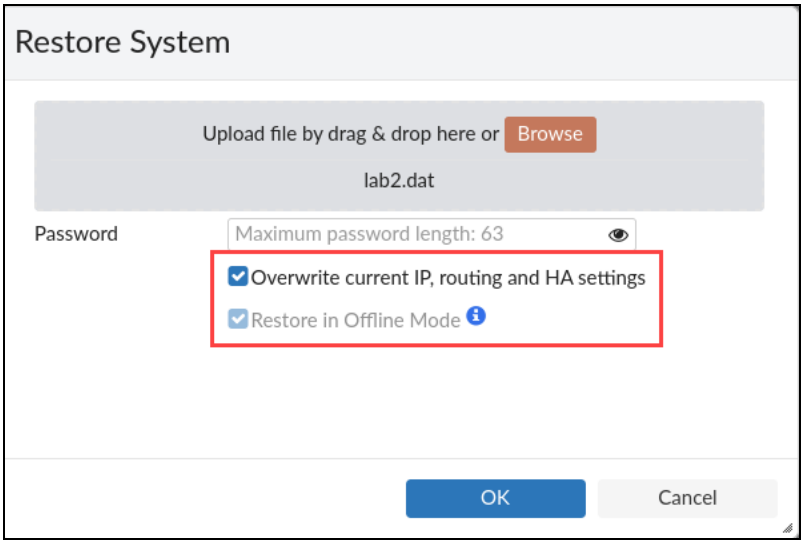
2. In the **System Information** widget, click **System Configuration**, and then click the **restore** icon.



Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

3. Click **Browse**.
4. Select the `lab2.dat` backup file.
   You do not have to enter a password because the file is not encrypted.
5. Leave **Overwrite current IP, routing and HA settings** enabled.



6. Click **OK**.
   FortiManager reboots.
7. Wait for FortiManager to reboot, and then log in to the FortiManager GUI with the username `admin` and password `password`.
8. Close the FortiManager setup page and then select **root**.
9. At the top of the screen, click the lock icon to lock it.
10. Click **System Settings**.
11. Click **Admin** > **Administrators**.
    The **student** administrator account was restored from the backup file.
12. Log out of the FortiManager **admin** account.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

Exercise 4: Monitoring Alerts and Event Logs

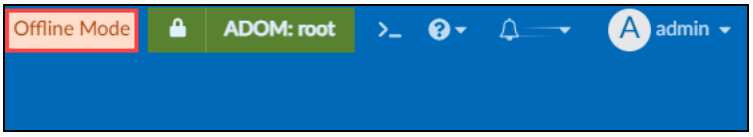
In this exercise, you will view the alerts in the alert console widget and view the event logs. You will also configure filter options to locate specific logs. First, you will disable offline mode, which is enabled by default when the FortiManager backup configuration is restored.

Disable Offline Mode

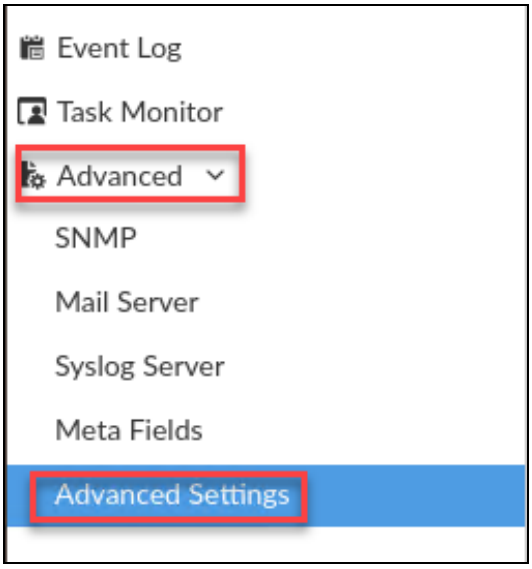
You will disable offline mode on FortiManager.

To disable offline mode

1. Log in to the FortiManager GUI with the username `admin` and password `password`.
2. Select **root**.
3. On the top bar, click the lock icon to lock it.
   You should see that FortiManager is in **Offline Mode**.



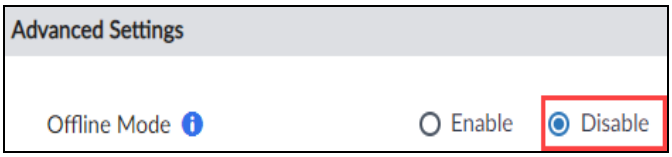
4. Click **System Settings**.
5. Click **Advanced** > **Advanced Settings**.



6. In the **Offline Mode** section, select **Disable**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET



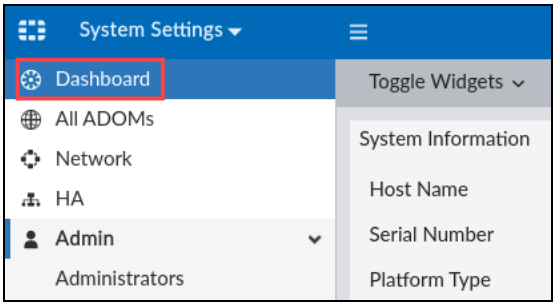
7. Click **Apply**.
   You will notice that the **Offline Mode** message disappears. At this point, FortiManager can establish a management connection with the managed devices.

View Alerts and Event Logs

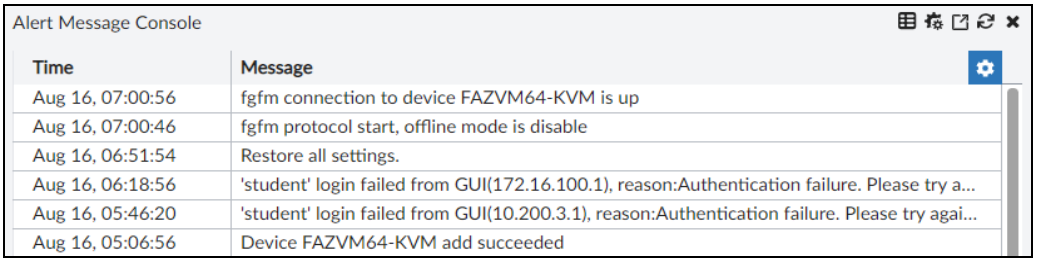
You will view the alerts on the **Alert Message Console** and logs under **Event Logs**.

To view alerts and event logs

1. Continuing on the FortiManager GUI, click **Dashboard**.



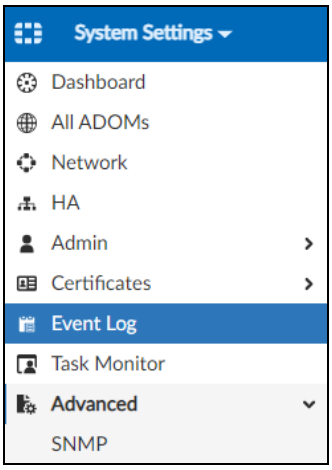
2. Go to the **Alert Message Console** widget.
   You should see **Restore all settings** messages, along with other alert messages.



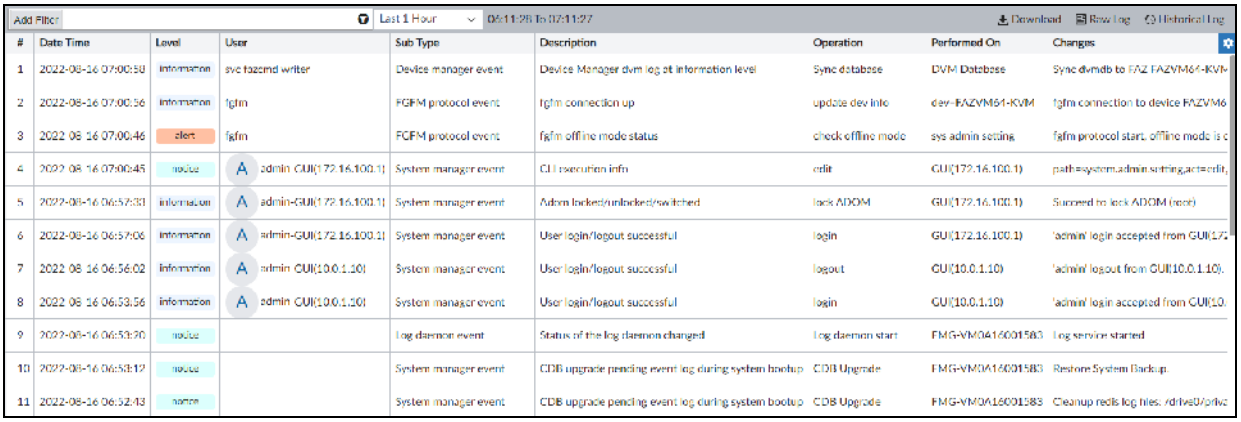
3. Click **Event Log**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET



4. Click **Download** to view the event log in raw format.



5. Log out of FortiManager.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

Lab 3: Device Registration

In this lab, you will explore the common operations performed using the device manager. You will use the **Device Manager** pane to add FortiGate devices.

Objectives

- Create and apply system templates to your managed devices
- Review central management settings on FortiGate
- Add a device using the **Add Device** wizard

Time to Complete

Estimated: 30 minutes

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

Exercise 1: Configuring System Templates

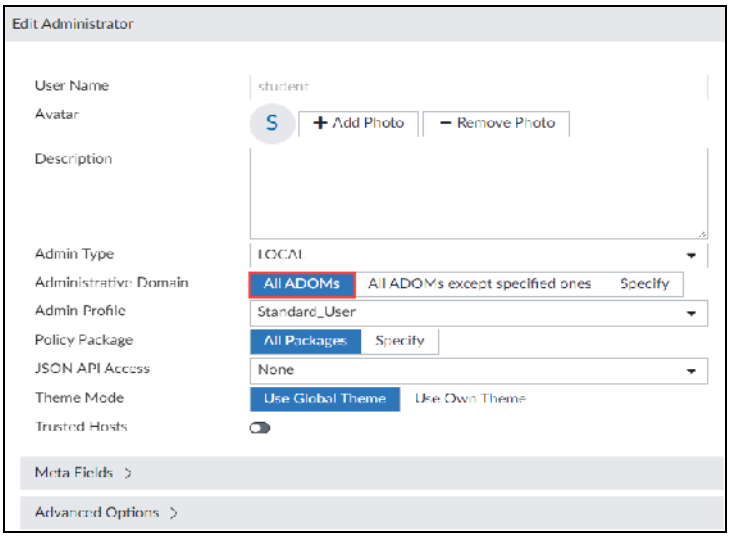
You can configure system templates on FortiManager to provision common system-level settings on FortiGate devices. You can configure the templates in advance, and then apply them either to FortiGate devices when they are first added to FortiManager or to FortiGate devices that FortiManager is currently managing.

Configure System Templates

You will configure and apply system templates to FortiGate.

To configure system templates

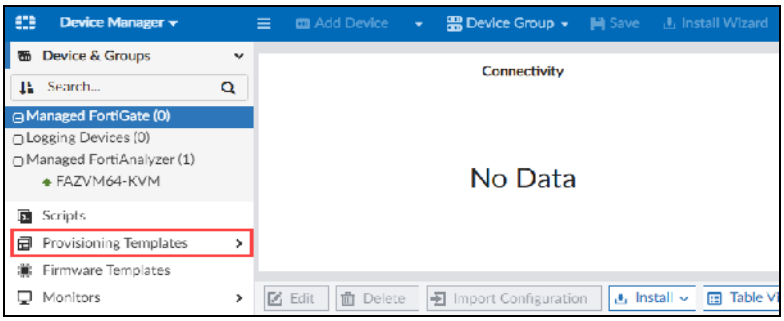
1. Log in to the FortiManager GUI with the username `admin` and password `password`.
2. Click **root**.
3. Click **System Settings**.
4. Click **Admin** > **Administrators**.
5. Select the **student** checkbox, click **Edit**, and then select **All ADOMs**.



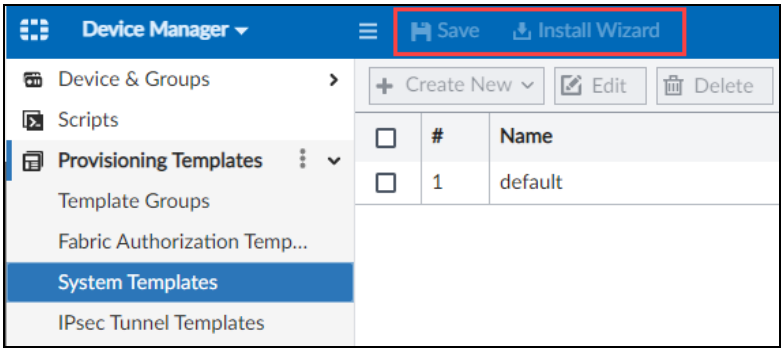
6. Click **OK**.
7. Log out of the FortiManager **admin** account.
8. Log in to the FortiManager GUI with the username `student` and password `fortinet`.
9. Click **My_ADOM**.
10. Click **Device Manager**.
11. Click **Provisioning Templates**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET



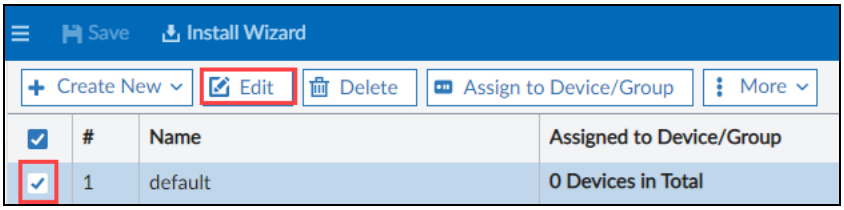
You will notice that you have read-only access.



This is because when ADOM locking is enabled, you must lock the ADOM before making configuration changes.

12. At the top of the screen, click the lock icon to lock **My_ADOM**.

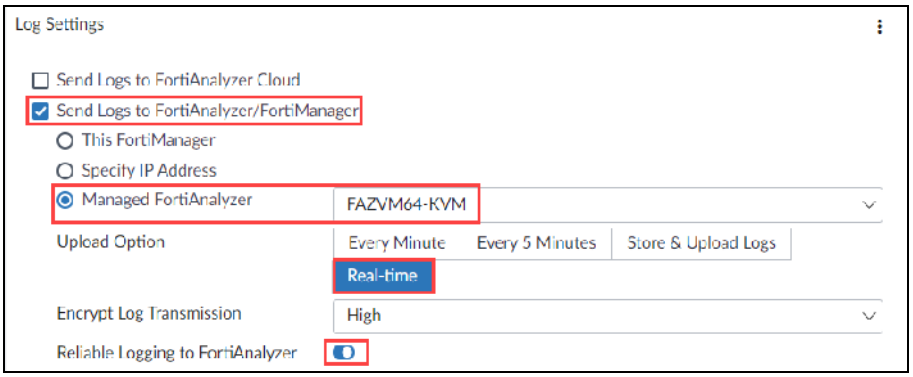
13. Under **System Templates**, select the **default** checkbox, and then click **Edit**.



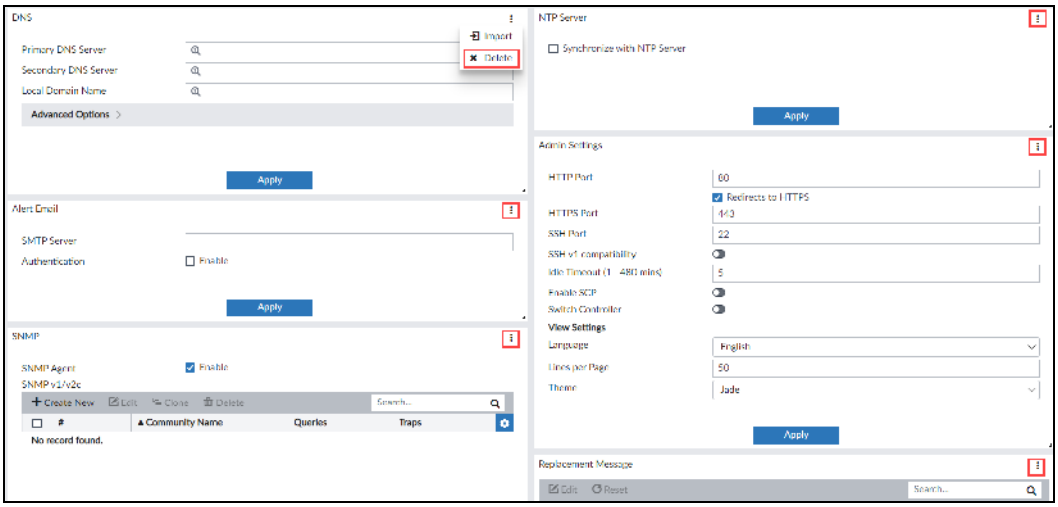
14. In the **Log Settings** widget, select the **Send Logs to FortiAnalyzer/FortiManager** checkbox.
15. Select **Managed FortiAnalyzer**, and then select the managed FortiAnalyzer in the drop-down list.
16. In the **Upload Option** field, select **Real-time**.
17. Enable **Reliable Logging to FortiAnalyzer**.
    Your configuration should look like the following example:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET



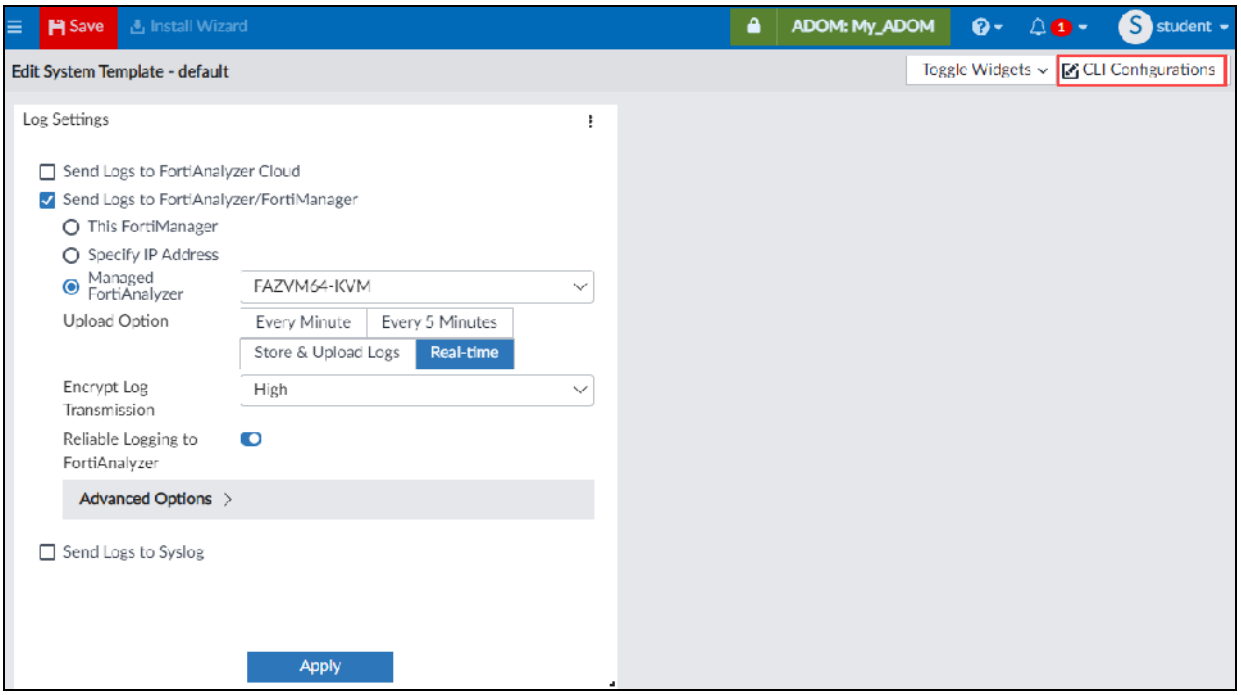
18. Click **Apply**.
19. Click **X** to delete all of the other widgets, and then click **OK**.



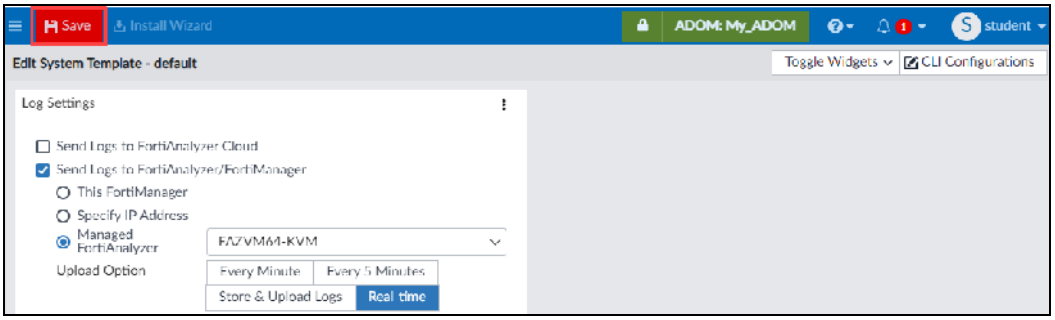
Your configuration should look like the following example:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET



20. Click **Save**.



When ADOM locking is enabled, you must save the changes to copy them to the FortiManager database.

21. At the top of the screen, click the lock icon to unlock **My_ADOM**.
22. Log out of the FortiManager **student** account.

Disable ADOM Locking (Workspace Mode)

You will disable ADOM locking because, in this lab, each student has a dedicated ADOM to work on.

Before disabling workspace mode, ensure that all the administrators logged in to FortiManager save their work.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

To disable ADOM locking (workspace mode)

1. Log in to the FortiManager GUI with the username `admin` and password `password`.
2. Click **root**.
3. Click **System Settings**.
4. Click **Admin** > **Workspace**.
5. Click **Disable**, click **Apply**, and then click **OK**.
   Disabling workspace mode logs administrators out of FortiManager and saves the changes.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

Exercise 2: Registering a Device on FortiManager

There are multiple ways to add FortiGate devices to FortiManager, including:

- Use the **Add Device** wizard.
- Send a request from FortiGate to FortiManager, and then accept the request from FortiManager.
- Add multiple devices using the **Device Manager**.

You will add FortiGate devices using the **Add Device** wizard.

FMG-Access on both FortiGate devices is enabled on the interface connected to FortiManager. **FMG-Access** is the communication protocol that is used between FortiManager and managed FortiGate devices.

Review the Central Management Configuration on Local-FortiGate

Before you add FortiGate to FortiManager, you will review the central management configuration on Local-FortiGate.

To review the central management configuration on Local-FortiGate

1. On the Local-Client VM, open PuTTY, and then connect over SSH to the **Local-FortiGate** saved session.
2. Log in with the username `admin` and password `password`.
3. Enter the following command:

```
get system central-management
```

You should observe the following output:

```
Local-FortiGate # get system central-management
mode                : normal
type                : fortimanager
schedule-config-restore: enable
schedule-script-restore: enable
allow-push-configuration: enable
allow-push-firmware : disable
allow-remote-firmware-upgrade: disable
allow-monitor       : enable
serial-number       :
fmg                 :
fmg-source-ip       : 0.0.0.0
```

The `serial-number` is the FortiManager serial number, which you cannot configure on FortiGate. FortiManager populates this setting, because it is managing this device. In this case, the `serial-number` field is blank because you have not yet added the device to FortiManager.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

4. Close the PuTTY session.

Enable Real-Time Debug

You will enable real-time debug on FortiManager to view the real-time status when you add FortiGate to FortiManager.

To enable real-time debug

1. On the Local-Client VM, open PuTTY, and then connect over SSH to the **FortiManager** saved session.
2. Log in with the username `admin` and password `password`.
3. Enter the following commands:

```
diagnose debug reset
diagnose debug disable
diagnose debug application depmanager 0
diagnose debug application depmanager 255
diagnose debug enable
```

You should place this PuTTY session and the FortiManager GUI side-by-side so that you can view the real-time debugs while you add FortiGate to the FortiManager GUI.

The output is verbose and you might have to scroll up or down to review the information. Alternatively, you can save the log file on your desktop, and then open it using a text editor, such as Notepad++.

Add Local-FortiGate Using the Add Device Wizard

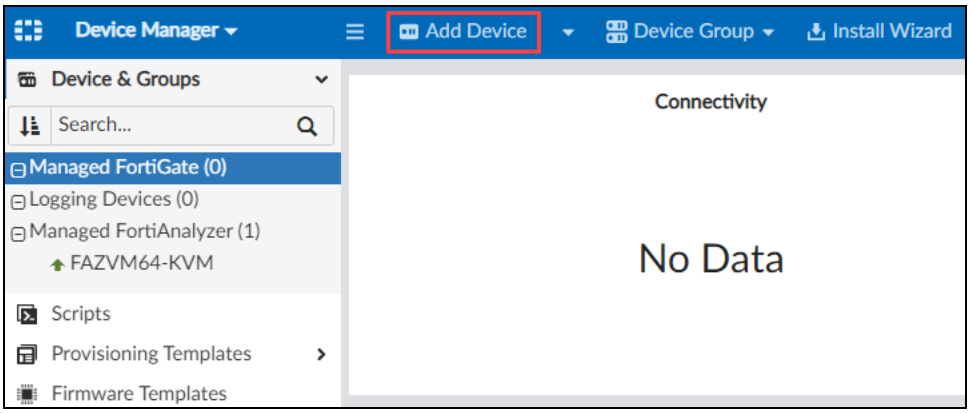
You will add Local-FortiGate to FortiManager in **My_ADOM** using the **Add Device** wizard, and then you will apply the **System Template** that you created earlier.

To add Local-FortiGate using the Add Device wizard

1. On the Local-Client VM, open a browser, and then log in to the FortiManager GUI at `10.0.1.241` with the username `student` and password `fortinet`.
2. Click **My_ADOM**.
3. Click **Device Manager**.
4. Click **Add Device**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET



5. In the **Add Device** wizard, select **Discover Device**, and then configure the following settings:

Field	Value
IP Address	10.200.1.1 (This is the IP address of port1 on FortiGate.)
Use legacy device login	Enable
Username	admin
Password	password

6. Click **Next**.
7. Review the discovered device information, and then compare it with the output from the FortiManager PuTTY session.
8. You should observe the following:

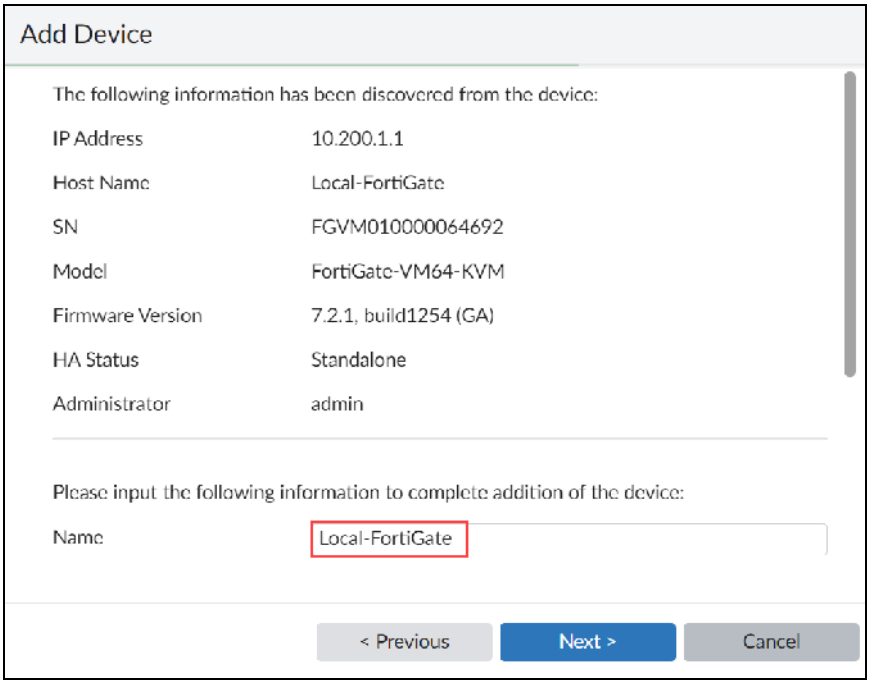
9. Press the up arrow on your keyboard, and then select the following commands to disable the debug—alternatively, you can enter these commands manually:

```
diagnose debug application depmanager 0
diagnose debug disable
diagnose debug reset
```

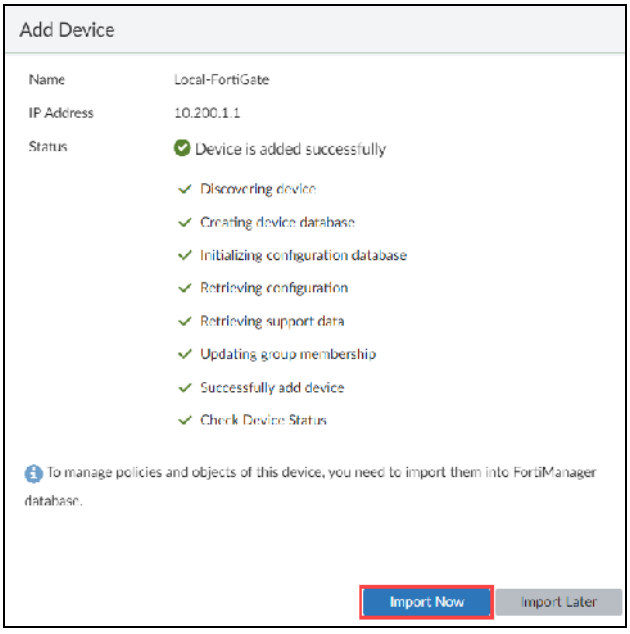

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

10. Close the PuTTY session.
11. Return to the FortiManager GUI.
12. Ensure that **Name** is set to **Local-FortiGate**.



13. Click **Next**.
14. Click **Import Now** to import the policies and objects.

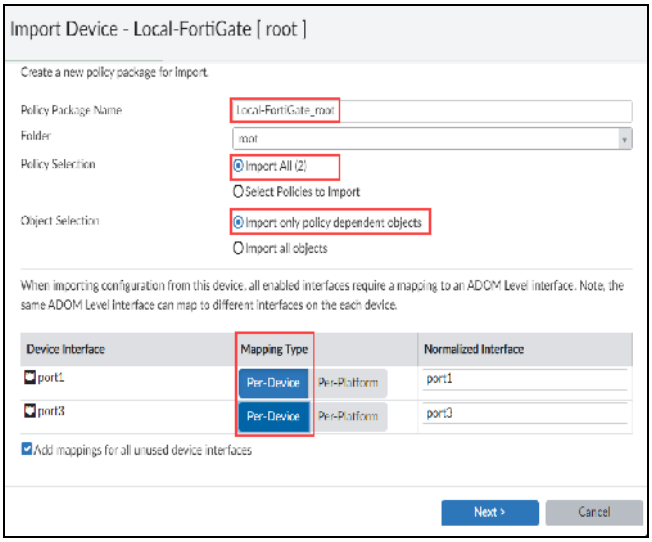


15. Select the **Import Policy Package** checkbox.
16. Click **Next**.
17. On the policy package import page, do the following:

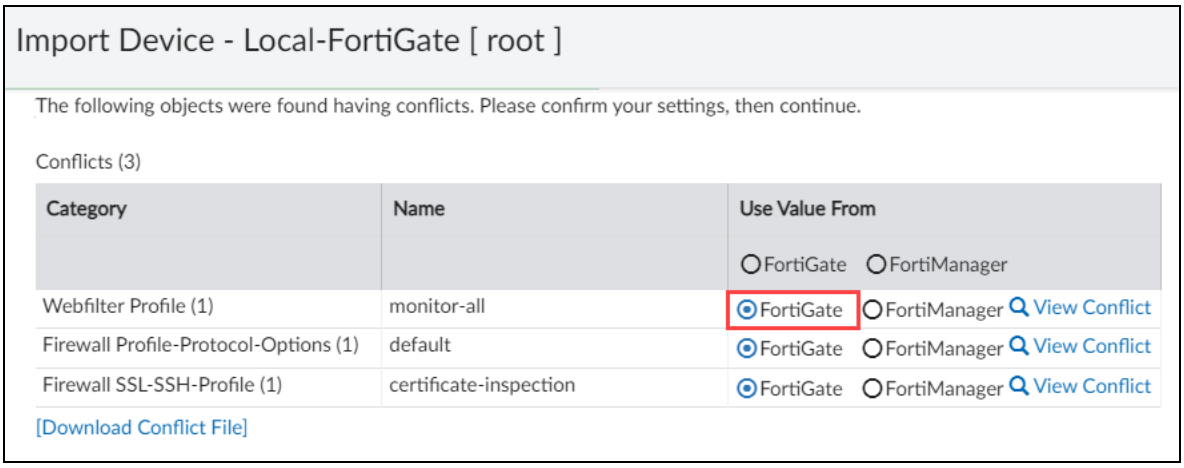
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

- Make sure the policy package name is configured as **Local-FortiGate_root**.
- Accept the policy and object import defaults.
- Change **Mapping Type** to **Per-Device**.



18. Click **Next**.
19. On the conflict page, click **View Conflict** on all of the entries.
    This shows you the details of the configuration differences between FortiGate and FortiManager.
20. In the **Use Value From** column, keep the default setting of **FortiGate**.



    You may see different output.

21. Click **Next**.
    Note the objects identified—these should be identified as duplicates, new, or updating existing FortiManager.
22. Click **Next**.
23. Click **Download Import Report**.
24. In a text editor, such as Notepad++, open the import report to review objects have been imported or skipped.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

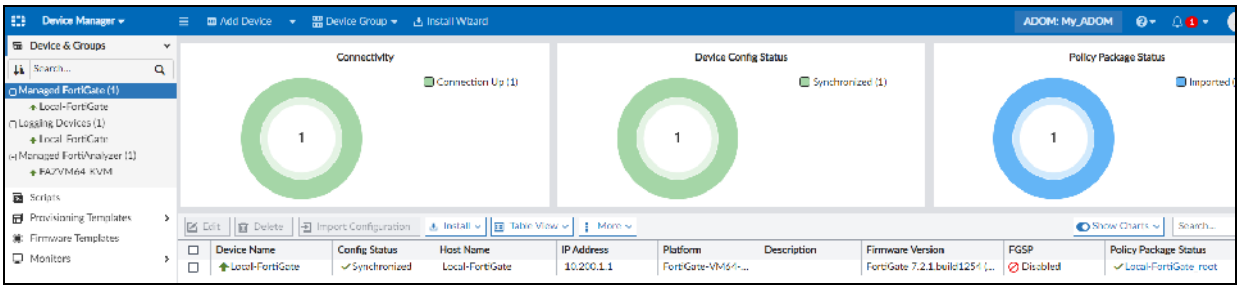
DO NOT REPRINT Brave-Dumps.com
© FORTINET

The option to download the import report is available only on this page. As a best practice, you should download the report and review the important information, such as which device is imported into which ADOM, as well as the name of the policy package created, along with the objects imported.

FortiManager imports new objects and updates existing objects based on the option that you choose on the conflict page. The duplicate objects are skipped because FortiManager does not import duplicate entries into the ADOM database.

25. Close the text editor.
26. Click **Finish**.

    The Local-FortiGate device should now be listed in **Device Manager**.



27. On the Local-Client VM, open PuTTY, and then connect over SSH to the **Local-FortiGate** saved session.
28. Log in with the username `admin` and password `password`.
29. Enter the following command:

```
get system central-management
```

    You should observe the following output:

```
Local-FortiGate # get system central-management
mode                : normal
type                : fortimanager
schedule-config-restore: enable
schedule-script-restore: enable
allow-push-configuration: enable
allow-push-firmware : disable
allow-remote-firmware-upgrade: disable
allow-monitor       : enable
serial-number       : "FMG-VM0A16001583"
fmg                 : "10.200.1.241"
fmg-source-ip       : 0.0.0.0
fmg-source-ip6      : ::
local-cert          :
ca-cert             :
vdom                : root
```

The `serial-number` is the serial number of FortiManager, which you cannot configure on FortiGate. This has been set by FortiManager, which is managing this device. Also, the FortiManager IP address is set.

30. Close the PuTTY session.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

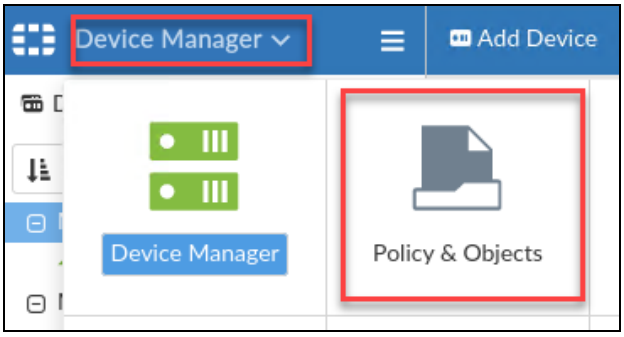
DO NOT REPRINT Brave-Dumps.com
© FORTINET

View the Local-FortiGate Policy Package

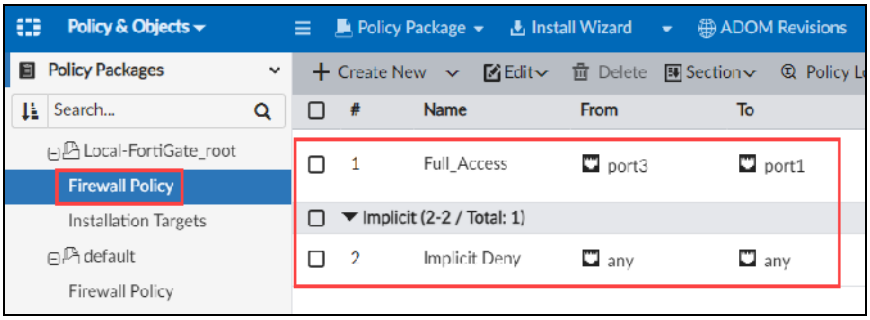
Now that you have imported policy and dependent objects for Local-FortiGate, you will view the policy package created for Local-FortiGate.

To view the Local-FortiGate policy package

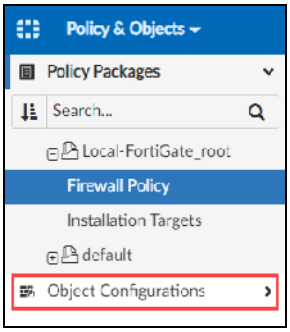
1. Continuing on the FortiManager GUI, click **Device Manager**, and then click **Policy & Objects**.



You will notice that a policy package named **Local-FortiGate_root** was created when you imported firewall policies from your Local-FortiGate.



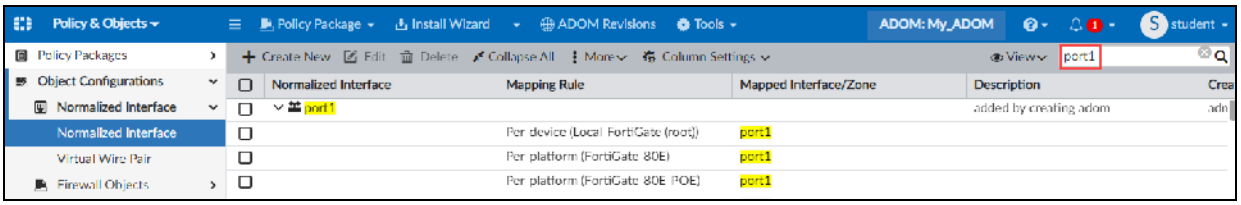
2. On the left, click **Object Configurations**.



3. Click **Normalized Interface**.
4. In the search field, type `port1`.

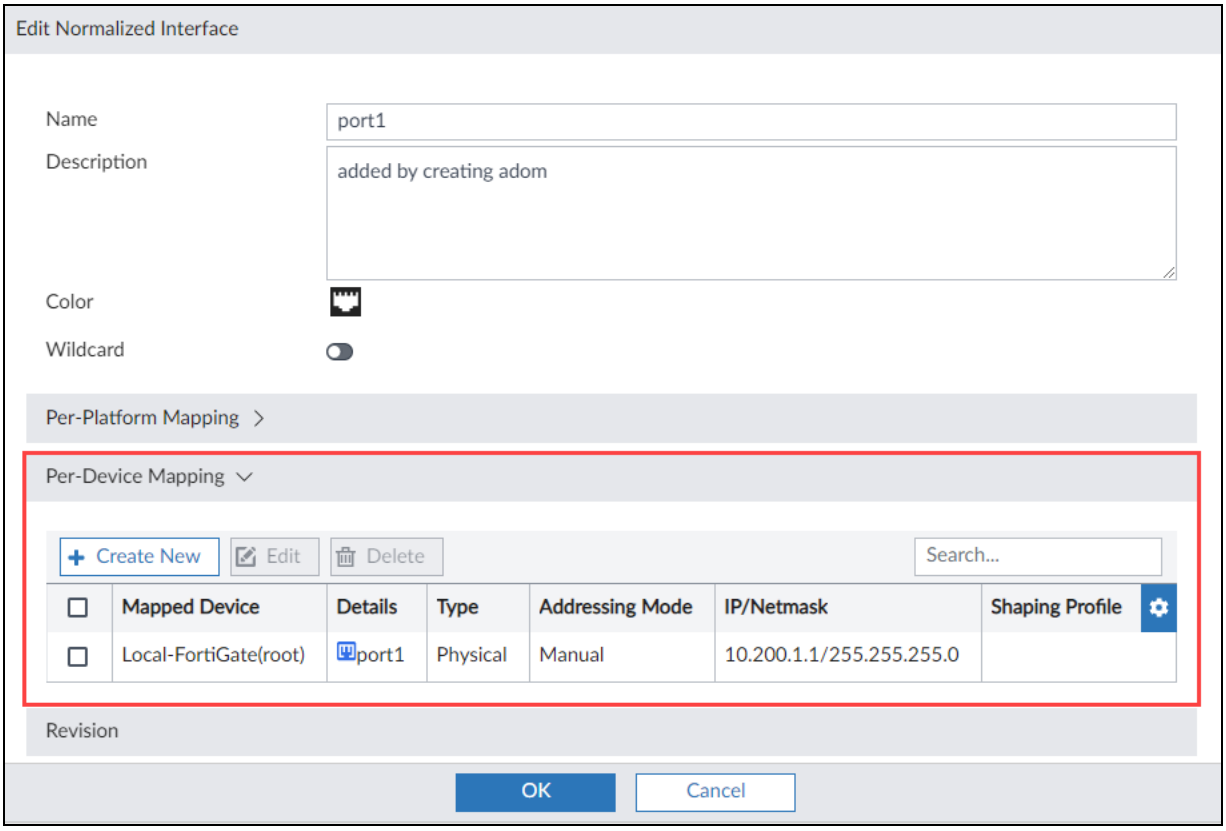
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET



5. Select **port1**, and then click **Edit**.
6. Scroll down to the **Per-Device Mapping** section to view the ADOM interface mapping to device-level mappings, which were created when the device was added.

   These interfaces are used in policy packages to map firewall policies to interfaces on the firewall.



7. Click **Cancel**.
8. Clear the **port1** from the search box.
9. Repeat the previous steps to view the **port3** interface mapping.

Import System Template Settings From FortiGate

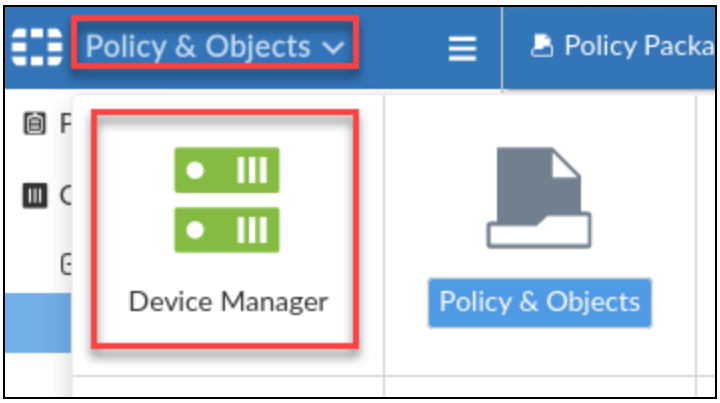
Now that you have added Local-FortiGate to FortiManager, you will import NTP server settings from Local-FortiGate. These server settings can be used by multiple FortiGate devices using this system template.

To import system template settings from FortiGate

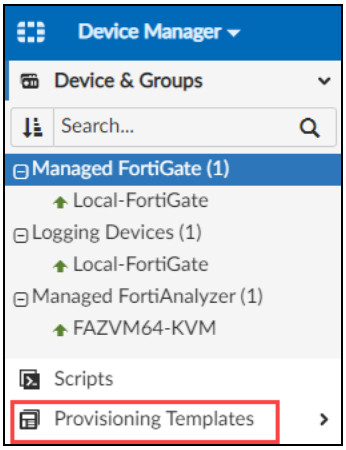
1. Continuing on the FortiManager GUI, click **Policy & Objects**, and then select **Device Manager**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

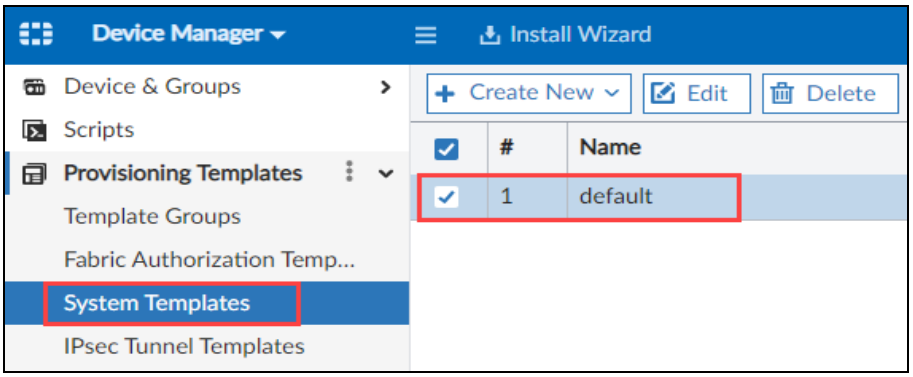
DO NOT REPRINT Brave-Dumps.com
© FORTINET



2. Click **Provisioning Templates**.



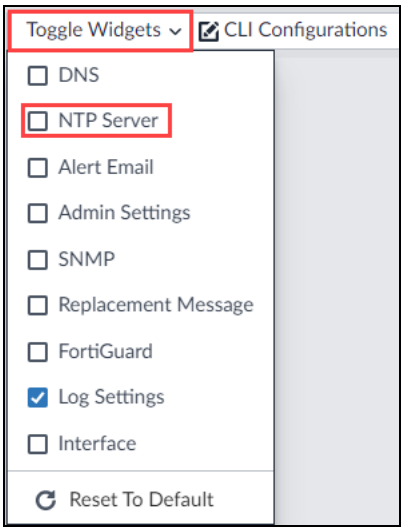
3. Click **System Templates**.
4. Select the **default** checkbox, and then click **Edit**.



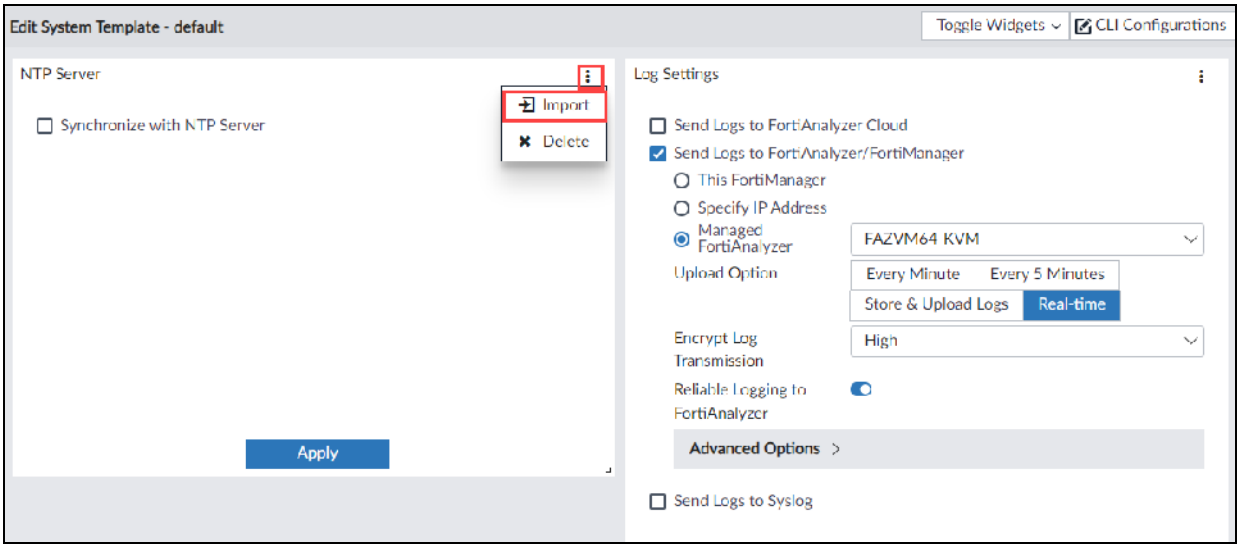
5. Click **Toggle Widgets**, and then select the **NTP Server** checkbox.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

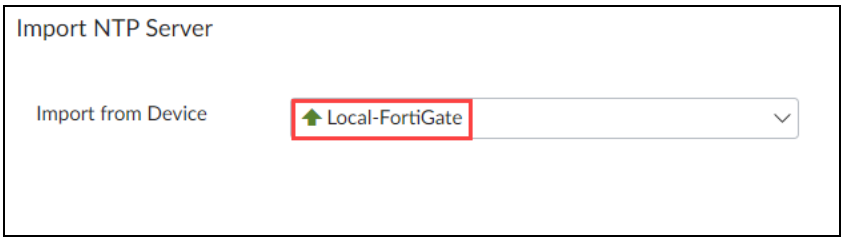
DO NOT REPRINT Brave-Dumps.com
© FORTINET



6. Click **Import**.



7. In the **Import from Device** field, select **Local-FortiGate**.



8. Click **OK**.
9. Click **Apply**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

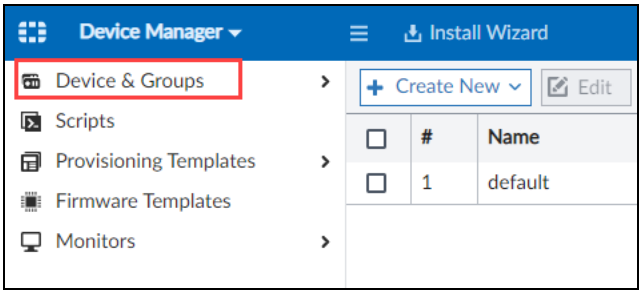
DO NOT REPRINT Brave-Dumps.com
© FORTINET

Add Remote-FortiGate Using the Add Device Wizard

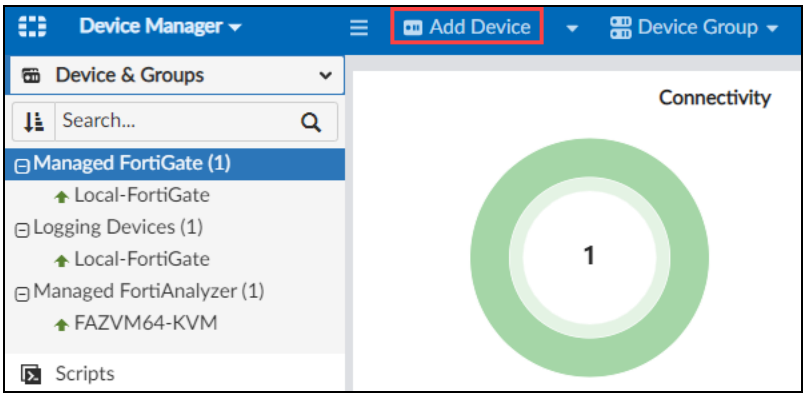
You will add Remote-FortiGate to FortiManager in **My_ADOM** using the **Add Device Wizard**. You will import the policies and objects for Remote-FortiGate later.

To add Remote-FortiGate using the Add Device wizard

1. Continuing on the FortiManager GUI, click **Device & Groups**.



2. Click **Add Device**.



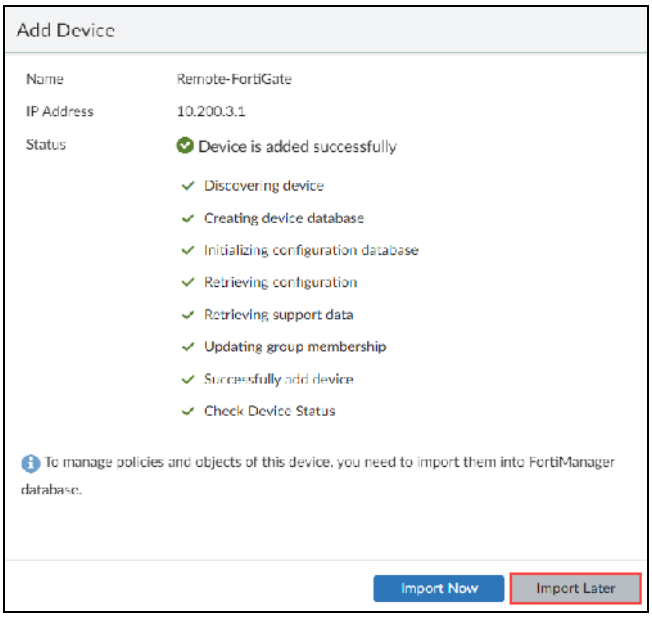
3. In the **Add Device** wizard, select **Discover Device**, and then configure the following settings:

Field	Value
IP Address	10.200.3.1 (This is the IP address of port4 on FortiGate.)
Use legacy device login	Enable
Username	admin
Password	password

4. Click **Next**.
5. Click **Next**.
6. Click **Import Later**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET



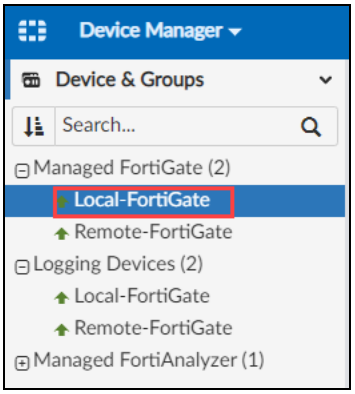
The **Remote-FortiGate** device should now be listed on the **Device Manager** page.

Assign the System Template to Local-FortiGate and Remote-FortiGate

You will assign the **default** system template to Local-FortiGate and Remote-FortiGate to apply system settings.

To assign the system template to Local-FortiGate and Remote-FortiGate

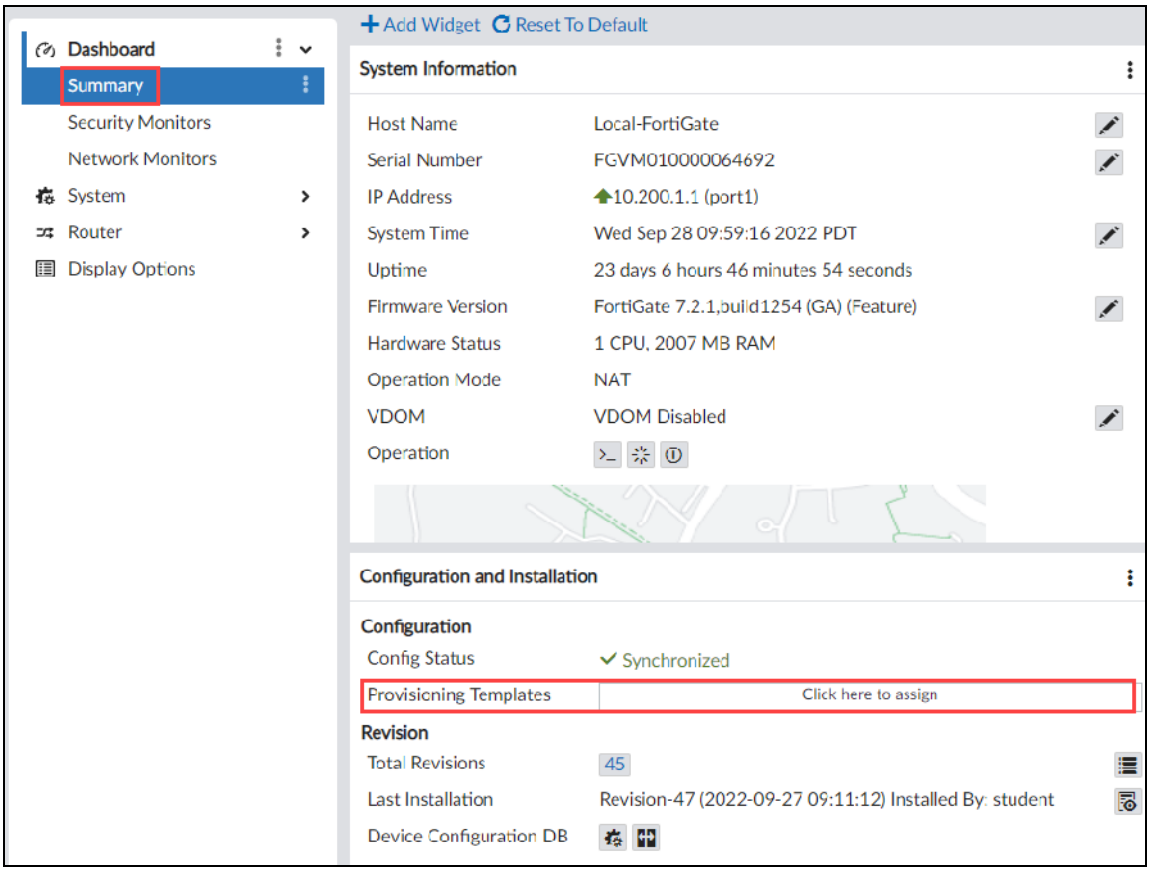
1. Continuing on the FortiManager GUI, click **Device & Groups**.
2. Click **Local-FortiGate**.



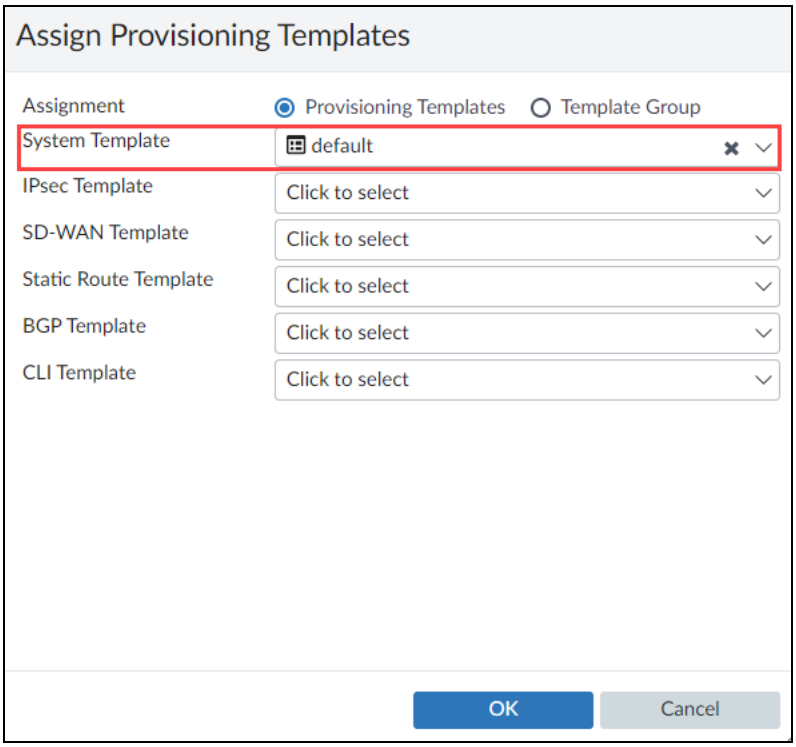
3. In the **Configuration and Installation** widget, click the **Provisioning Templates**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET



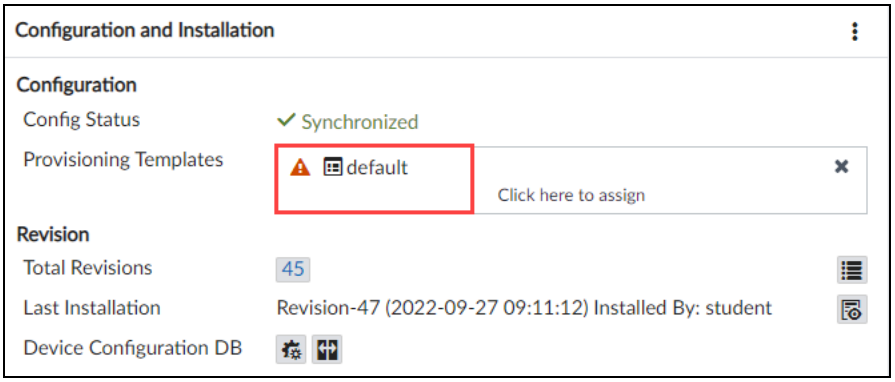
4. In the **Assign Provisioning Templates** window, in the **System Template** field, select **default**.



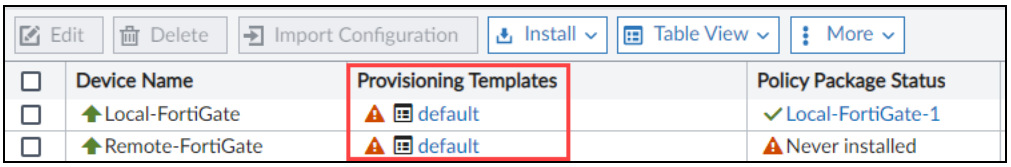
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

5. Click **OK**.
   You should see the following configuration:



6. Repeat steps 1 to 5 for Remote-FortiGate.
   The **Provisioning Templates** column displays **default** for both Local-FortiGate and Remote-FortiGate.



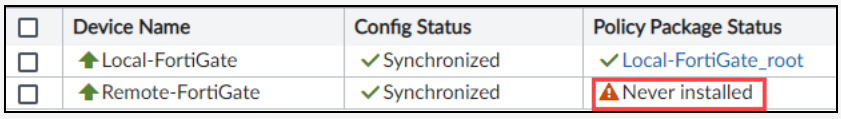
Stop and think!

Why is the **Policy Package Status** for Remote-FortiGate **Never Installed**?

When you select **Import Later** in the **Add Device** wizard, or add an unregistered device to FortiManager, the policy package status is **Never Installed** because there is still no policy package created for the newly added FortiGate.

You will run the **Import Policy** wizard later.

If you add an unregistered device, you must run the **Import Policy** wizard to import the device's firewall policy into a new policy package.



Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

Lab 4: Device-Level Configuration and Installation

In this lab, you will explore common operations that you can perform using the device manager, such as configuring device-level changes, checking the statuses of managed devices, installing configuration changes, and keeping the managed devices in sync with the device database on FortiManager.

Objectives

- Understand the statuses of managed devices on FortiManager
- Use the status information in the **Configuration and Installation Status** widget
- Make and install configuration changes using the device manager
- Make configuration changes locally on FortiGate, and then verify that FortiManager automatically retrieved the changes
- Identify entries in the revision history and the management actions that created the new revisions
- Install a large number of managed device changes using scripts

Time to Complete

Estimated: 70 minutes

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

Exercise 1: Understanding the Statuses of Managed Devices

In this exercise, you will check and learn about the statuses of FortiGate devices on FortiManager. Depending on the configuration changes, a FortiGate can have a different **Sync Status** and **Device Settings Status**.

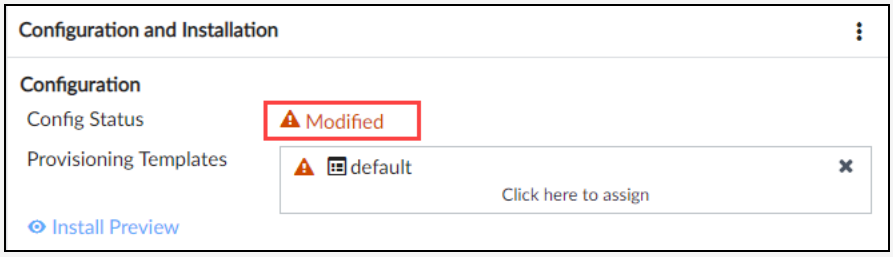
- The **Sync Status** indicates whether the FortiGate configuration matches the latest revision history.
- The **Device Settings Status** indicates whether the FortiGate configuration stored in the device-level database matches the latest running revision history.

To check the status of a managed device

1. Log in to the FortiManager GUI with the username `student` and password `fortinet`.
2. Click **My_ADOM**.
3. Click **Device Manager**.

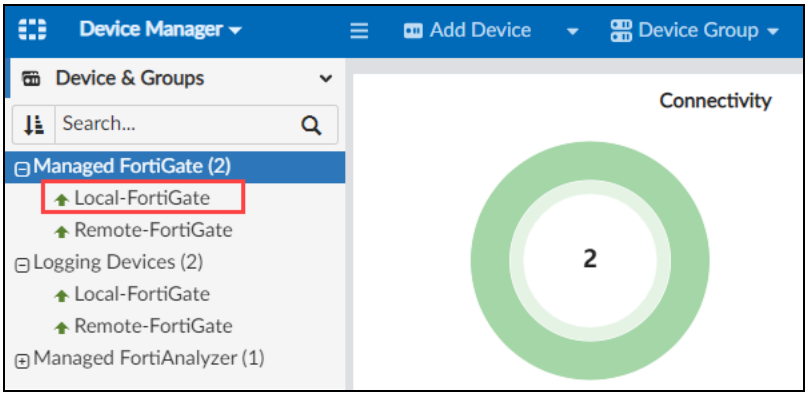
Stop and think!

Why does the **Config Status** field for the FortiGate devices show the status **Modified**?



In the previous exercise, you applied system templates to both FortiGate devices. The configuration running on the FortiManager device-level database is different from the latest revision history. This changes the **Config Status** to **Modified**. The provisioning template changes must be installed on the FortiGate devices to return the devices to the synchronized state.

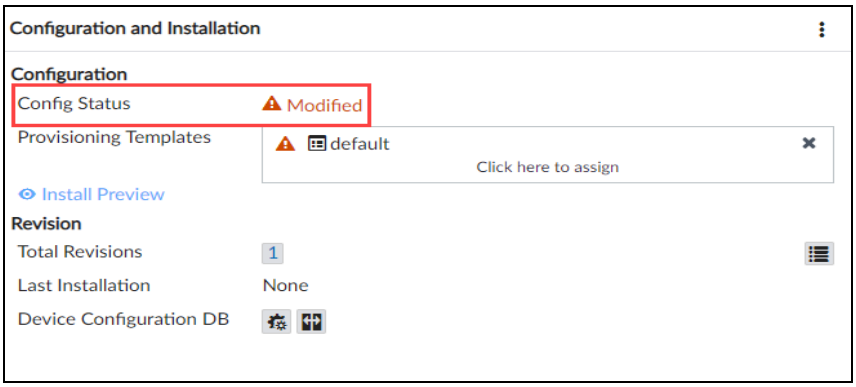
4. Click **Local-FortiGate**.



5. In the **Configuration and Installation** widget, check the **Config Status** field—it should be **Modified**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET



6. On the Local-Client VM, open PuTTY, and then connect over SSH to the **FortiManager** saved session.
7. Log in with the username `admin` and password `password`.
8. Enter the following command to display the device statuses on the CLI:

```
diagnose dvm device list
```

Stop and think!

If the **Config Status** is **Modified**, why is the FortiGate `conf` still showing as `in sync`?

```
FMG VM64 # diagnose dvm device list
--- There are currently 3 devices/vdoms managed ---
--- There are currently 3 devices/vdoms count for license ---

TYPE            OID    SN              HA      IP              NAME                                ADOM                            IPS
        FIRMWARE
fmgfaz-managed  239    FAZ-VM0000065043 -      10.0.1.210      FAZVM64                             MY_ADOM                         N/A
        7.0 MR0 (113)
        |- STATUS: conn: up
fmgfaz-managed  249    FGVM01000004a92 -       10.200.1.1      Local-FortiGate                     My_ADOM                         18.00
732 (extended) 7.0 MR0 (157)
        |- STATUS: dev-db: not modified; conf: in sync; cond: pending; dm: retrieved; conn: up; template:[modified]default
        |- vdom:[3]root flags:0 adom:My_ADOM pkg:[imported]Local-FortiGate_root
fmgfaz-managed  252    FGVM01000065036         10.200.3.1      Remote FortiGate                    My_ADOM                         6.007
41 (extended) 7.0 MR0 (157)
        |- STATUS: dev-db: not modified; conf: in sync; cond: pending; dm: retrieved; conn: up; template:[modified]default
        |- vdom:[3]root flags:0 adom:My_ADOM pkg:[never-installed]
```

The **Device Settings Status** is the status between the device-level database configuration and the latest revision history. Applying system templates changes the device-level database configuration, so it enters the **Modified** state. You can see these details when you run the `diagnose dvm device list` command.

The `conf` field on the CLI shows the status between the latest revision history and the actual FortiGate configuration. Because the latest revision history is the same as the FortiGate configuration, the `conf` field shows the `in sync` state.

The output also shows the serial number of the device, the connecting IP address of the device, the firmware version, the name of the device on FortiManager, and the ADOM that the device is added to.

```
FMG VM64 KVM # diagnose dvm  device list
--- There are currently 3 devices/vdoms managed ---
--- There are currently 3 devices/vdoms count for license ---

TYPE            OID    SN              HA      IP              NAME                                ADOM            IPS                 FIRMWARE
fmgfaz-managed  243    FAZ-VM0000065040 -      10.0.1.210      FAZVM64-KVM                         My_ADOM         N/A                 7.0 MR0 (1315)
                |  STATUS: conn: up
fmgfaz managed  253    FGVM01000064602         10.200.1.1      Local FortiGate                     My_ADOM         6.00741 (extended)  7.0 MR2 (1254)
                |- STATUS: dev-db: modified; conf: in sync; cond: pending; dm: installed; conn: up; template:[modified]default
                |- vdom:[3]root flags:0 adom:My_ADOM pkg:[installed]Local-FortiGate_root
fmgfaz managed  255    FGVM01000065036         10.200.3.1      Remote FortiGate                    My_ADOM         6.00741 (extended)  7.0 MR2 (1254)
                |- STATUS: dev-db: modified; conf: in sync; cond: pending; dm: retrieved; conn: up; template:[modified]default
                |- vdom:[3]root flags:0 adom:My_ADOM pkg:[never-installed]
```

9. Examine the `STATUS` row of the `diagnose dvm device list` output for Local-FortiGate and Remote-FortiGate.

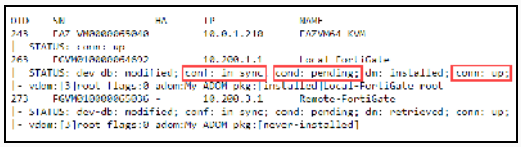
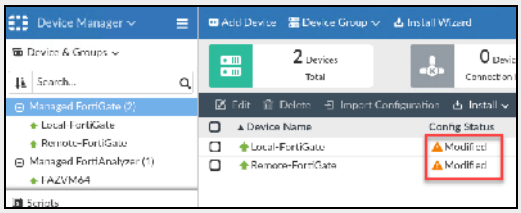
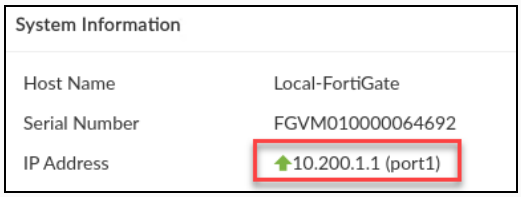
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET


```
TYPE           OID    SN              HA      IP             NAME                                        ADOM
fmgfaz-managed 243    FAZ-VM0000065040 -       10.0.1.210     FAZVM64-KVM                                 My_ADOM
               |- STATUS: conn: up
fmgfaz-managed 263    FGVM010000064692 -       10.200.1.1     Local-FortiGate                             My_ADOM
               |- STATUS: dev-db: modified; conf: in sync; cond: pending; dm: installed; conn: up; template:[modified]default
               |- vdom:[3]root flags:0 adom:My_ADOM pkg:[installed]Local-FortiGate_root
fmgfaz-managed 273    FGVM010000065036 -       10.200.3.1     Remote-FortiGate                            My_ADOM
               |- STATUS: dev-db: modified; conf: in sync; cond: pending; dm: retrieved; conn: up; template:[modified]default
               |- vdom:[3]root flags:0 adom:My_ADOM pkg:[never-installed]
```

Data	What it means	Actions to take

`dev-db: not modified`
 	
`template: [modified] default`
	Device-level configuration changes were made on FortiManager.
	
	Note: On the GUI, the **Config Status** appears as **Modified**. However, the CLI shows separate statuses for `dev-db` and `template`.
		The FortiManager administrator can install configuration changes to the managed device to return it to an unmodified state.

`conf: in sync`	The latest revision history is in sync with the FortiGate configuration. 	
`cond: pending`	Configuration changes must be installed. 	The FortiManager administrator can install configuration changes on the managed device to return it to an unmodified state.
`conn: up`	The FGFM tunnel between FortiManager and FortiGate is open. 	

10. Close the PuTTY session.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

Exercise 2: Installing System Template Changes on Managed Devices

In the previous lab, you added FortiGate devices to FortiManager and applied system templates.

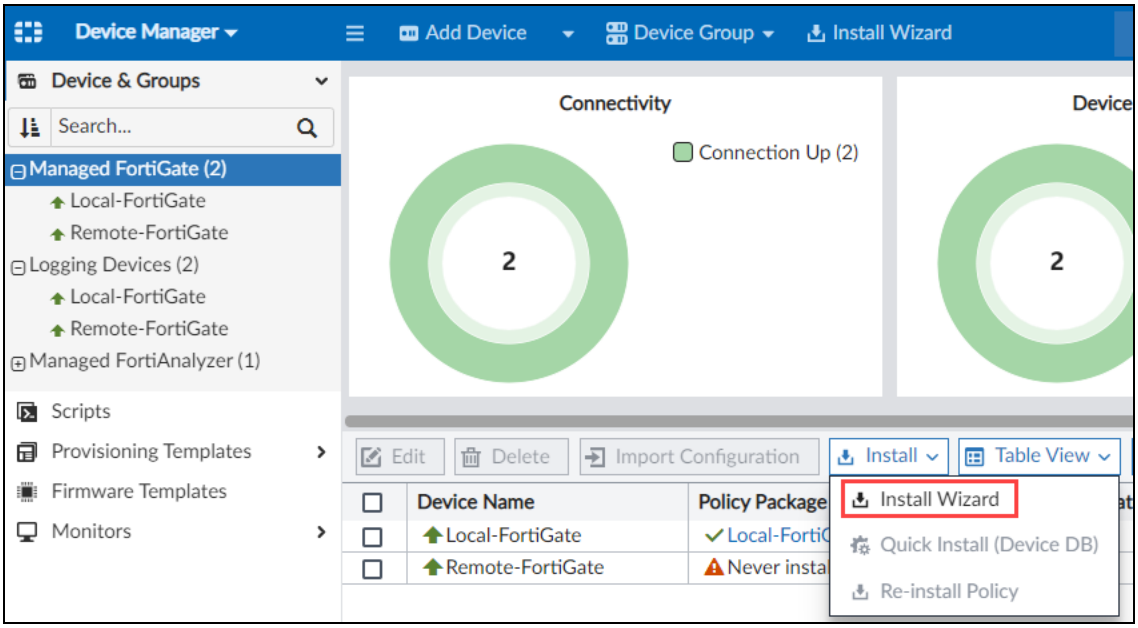
In this exercise, you will install system template changes on both FortiGate devices, and then view those changes locally, by logging in to each FortiGate.

Install System Templates

You will install the **default** system template changes to Local-FortiGate and Remote-FortiGate using the **Install Wizard**.

To install system templates

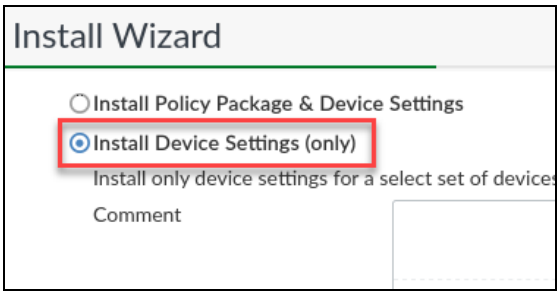
1. Log in to the FortiManager GUI with the username `student` and password `fortinet`.
2. Click **My_ADOM**.
3. Click **Device Manager** > **Managed FortiGate**.
4. Click **Install** > **Install Wizard**.



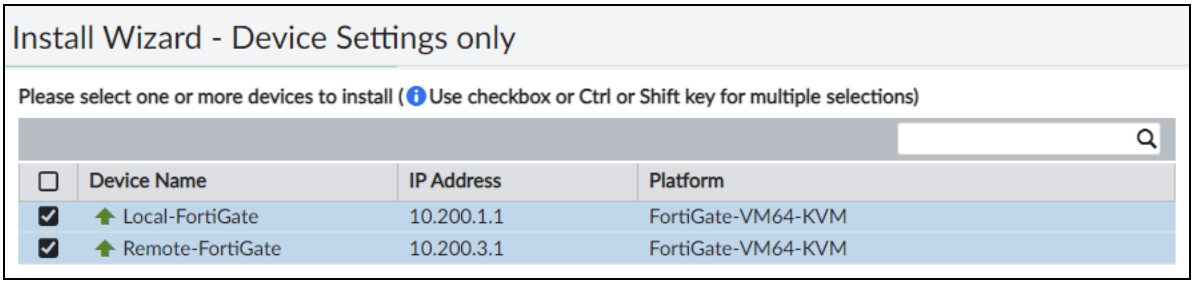
5. In the **Install Wizard**, make sure **Install Device Settings (only)** is selected, and then click **Next**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

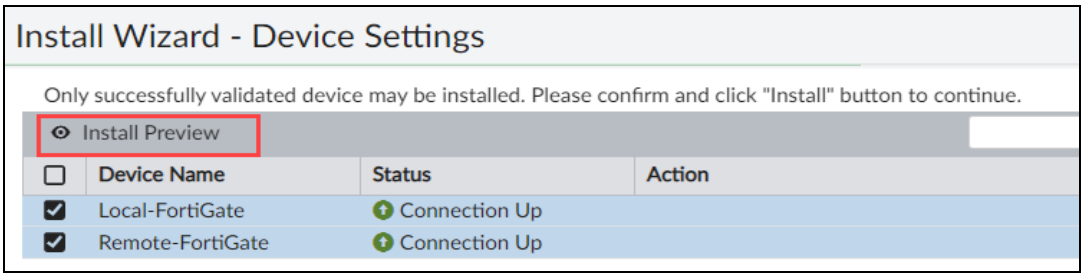
DO NOT REPRINT Brave-Dumps.com
© FORTINET



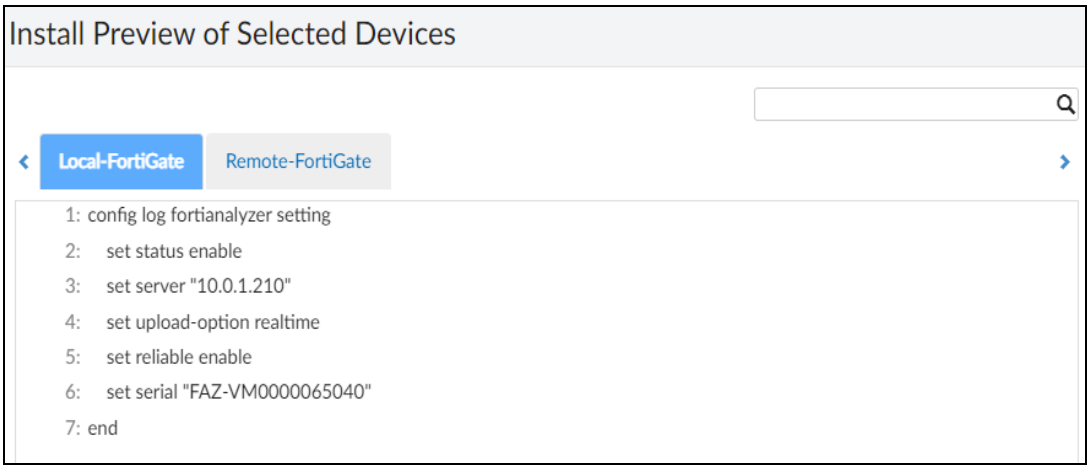
6. On the **Device Settings** page, ensure that both FortiGate devices are selected.



7. Click **Next**.
8. Click **Install Preview**.



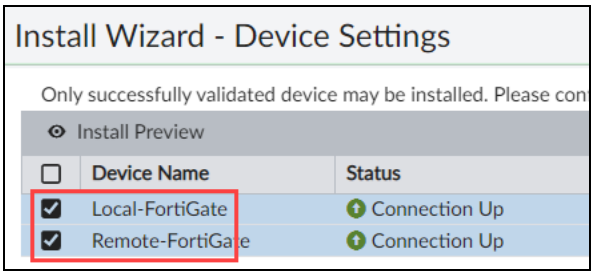
This shows you the changes that will be applied to all selected FortiGate devices.



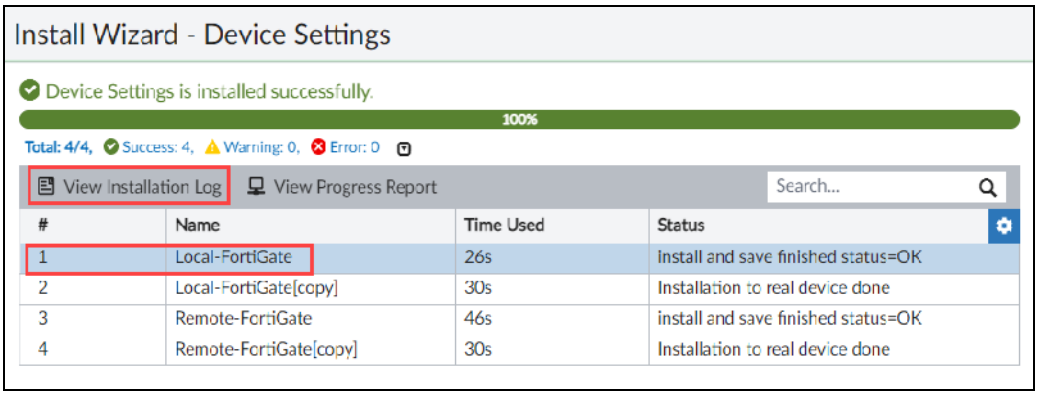
9. On the **Install Preview** page, click **Close**.
   Optionally, you can select **Install Preview** for Remote-FortiGate.
10. Make sure that both FortiGate devices are selected.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

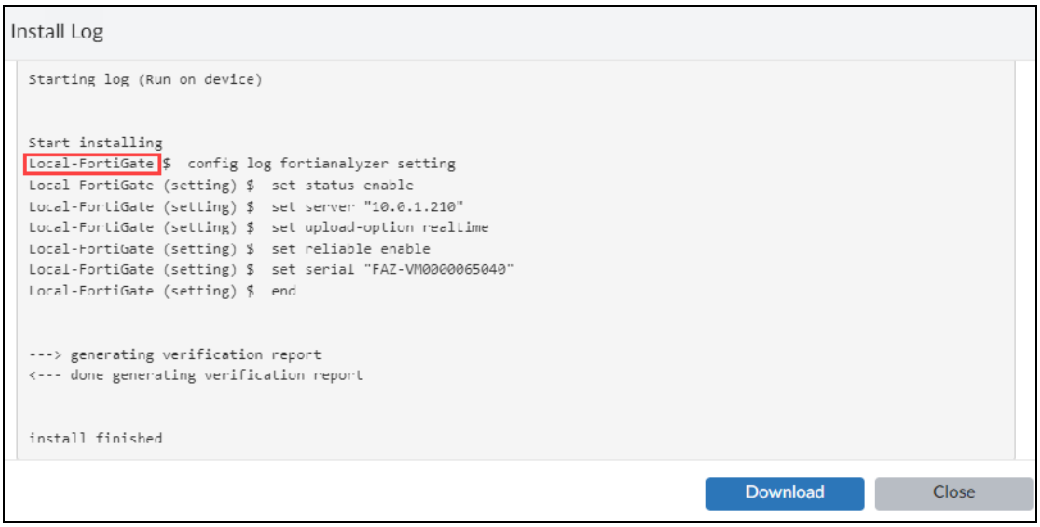


11. Click **Install**.
12. Once the installation is successful, select **Local-FortiGate**, and then click **View Installation Log**.



This is the installation log that shows exactly what is installed on the managed device.

The following image is an example log for Local-FortiGate:



13. Click **Close**.
14. Click **Finish**.

Check the Status of the Managed Device

You will check the status of the managed device after the installation.

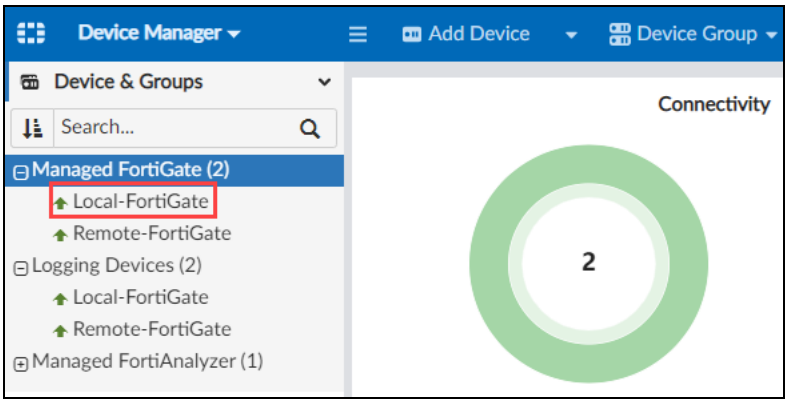
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

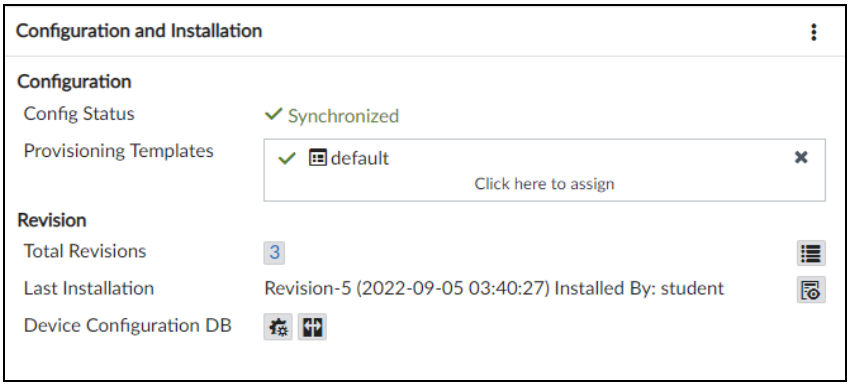
To check the status of the managed device

1. Continuing on the FortiManager GUI, review the **Config Status**.
   It should now appear as **Synchronized**.

2. Click **Local-FortiGate**.



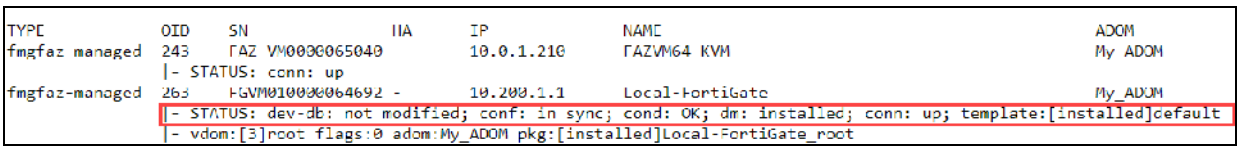
3. Under **Configuration and Installation** status, you should see that the **Config Status** is in the **Synchronized** state.



4. Open PuTTY, and then connect over SSH to the **FortiManager** saved session.
5. Log in with the username `admin` and password `password`.
6. Enter the following command to display device statuses on the CLI:

```
diagnose dvm device list
```

You should see the following in the output for Local-FortiGate and Remote-FortiGate:



Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

The `dev-db status` is `not modified`, which means that the FortiGate device-level database configuration matches the latest running revision history. The `dm: installed` field means that the installation was performed on FortiManager.

7. Enter the following command to display the FGFM tunnel statuses:

```
diagnose fgfm session-list
```

```
FMG-VM64-KVM # diagnose fgfm session-list
        FAZVM64-KVM(243) sn(FAZ-VM0000065040) ip(10.0.1.210)
                state(tunnel) tunnel(169.254.0.4) uptime:Mon Sep  5 03:00:09 2022
        Local-FortiGate(263) sn(FGVM010000064692) ip(10.200.1.1)
                state(tunnel) tunnel(169.254.0.7) uptime:Mon Sep  5 03:40:16 2022
        Remote-FortiGate(273) sn(FGVM010000065036) ip(10.200.3.1)
                state(tunnel) tunnel(169.254.0.8) uptime:Mon Sep  5 03:40:36 2022
        Session count = 3 (tunnel 3)
```

You can use this command to view the connecting IP address of managed devices, the link-level address that FortiManager assigns, and the uptime of the FGFM tunnel between FortiGate and FortiManager.

8. Close the PuTTY session.

View the Pushed Configuration on FortiGate

Using FortiManager, you installed the system template configuration on both FortiGate devices. Now, you will log in to the Local-FortiGate and Remote-FortiGate GUIs to view the configuration that was installed using FortiManager.

To view the pushed configuration on the Local-FortiGate GUI

1. Log in to the Local-FortiGate GUI with the username `admin` and password `password`.
2. Click **Login Read-Only**.

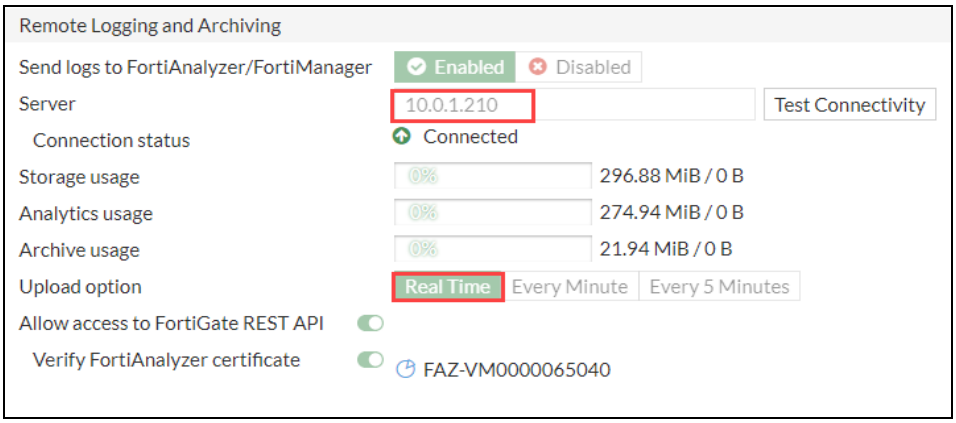
When you connect locally to a device that FortiManager is managing, a warning message appears because the device is centrally managed. *Do not use the read-write option locally on FortiGate unless it is absolutely necessary.* An example might be that a FortiManager administrator is unavailable to make configuration changes and installations to manage FortiGate devices.

3. Click **Log & Report** > **Log Settings**.

   You will notice that the **Remote Logging and Archiving** settings are the same as the **default** system template entries.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET



4. Log out of the Local-FortiGate GUI.

To view the pushed configuration on the Remote-FortiGate GUI

1. Log in to the Remote-FortiGate GUI with the username `admin` and password `password`.
2. Click **Login Read-Only**.
3. Click **Log & Report** > **Log Settings**.

   You will notice that the **Remote Logging and Archiving** settings are the same as the **default** system template entries. However, Remote-FortiGate logs are being queued because it has no connectivity to the FortiAnalyzer IP address `10.0.1.210`.
4. Log out of the Remote-FortiGate GUI.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

Exercise 3: Viewing the Auto Update Status and Revision History

By default, configuration changes made directly on FortiGate are automatically updated (retrieved) by FortiManager, and are reflected in the revision history. If required, you can disable the automatic update behavior on the FortiManager CLI under `config system admin settings`. This allows the FortiManager administrator to accept or reject the configuration changes.

In this exercise, you will make configuration changes directly on the FortiGate devices, and then verify that FortiManager automatically retrieved the configuration changes.

You will also review the configuration revision history of each FortiGate, which is created by auto update and other actions.

Make Direct Changes on Local-FortiGate

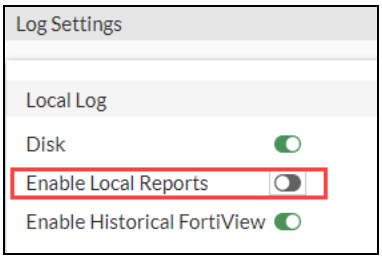
You will make direct changes on Local-FortiGate.

To make direct changes on Local-FortiGate

1. Log in to the Local-FortiGate GUI with the username `admin` and password `password`.
2. Click **Login Read-Write**.

When you connect locally to a device that FortiManager is managing, a warning message appears because the device is centrally managed. *Do not use the read-write option locally on FortiGate unless it is absolutely necessary.* An example might be that a FortiManager administrator is unavailable to make configuration changes and installations to manage FortiGate devices.

3. Click **Yes**.
4. Click **Log & Report** > **Log Settings**.
5. Disable **Enable Local Reports**.



6. Click **Apply**.
7. Log out of the Local-FortiGate GUI.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

Make Direct Changes on Remote-FortiGate

You will make direct changes on Remote-FortiGate. You will repeat the same steps for Remote-FortiGate that you did for Local-FortiGate.

To make direct changes on Remote-FortiGate

1. Log in to the Remote-FortiGate GUI with the username `admin` and password `password`.
2. Click **Login Read-Write**.
3. Click **Yes**.
4. Click **Log & Report** > **Log Settings**.
5. Disable **Enable Local Reports**.
6. Click **Apply**.
7. Log out of the Remote-FortiGate GUI.

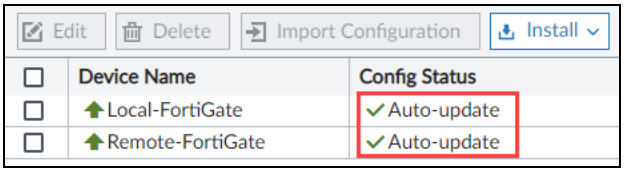
View the Auto Update Status and Revision History

Now that you have made the configuration changes locally on both FortiGate devices, you will view the auto update status on FortiManager, and view the configuration revision history entries that FortiManager created.

To view the auto update status

1. Log in to the FortiManager GUI with the username `student` and password `fortinet`.
2. Click **My_ADOM**.
3. Click **Device Manager**.
   You will notice that the **Config Status** is now in the **Auto-update** state for both FortiGate devices.

   This confirms that the changes you made locally were backed up to FortiManager.

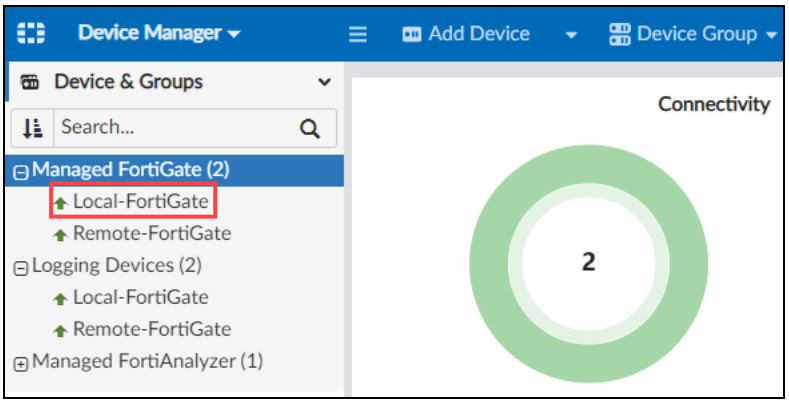


To view the revision history

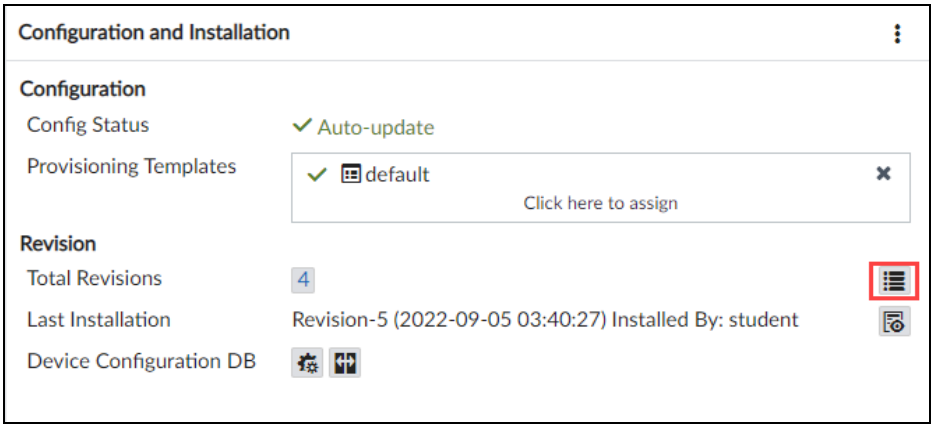
1. Click **Local-FortiGate**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET



2. In the **Configuration and Installation** widget, click the **Revision History** icon.

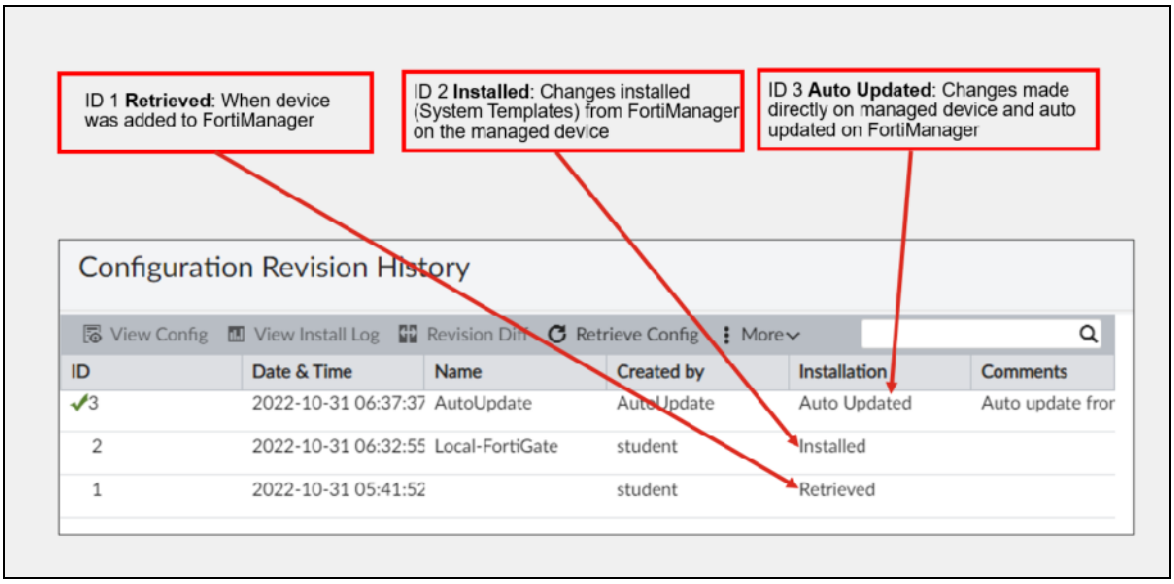


You should see three configurations (you may have more configurations if you made further changes):

- The first **Installation** status should be **Auto Updated**, indicating that these changes were made locally on FortiGate and were automatically updated on FortiManager.
- The second **Installation** status should be **Installed**, indicating that these changes were made by FortiManager on the managed device.
- The third **Installation** status should be **Retrieved**, indicating that this configuration was taken from the device running configuration, when it was added to FortiManager.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

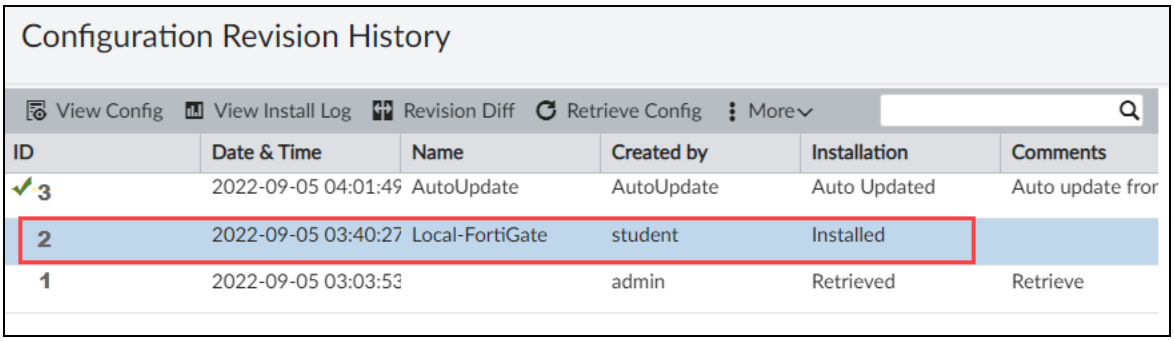


View the Installation Log

When the installation is done using FortiManager, the installation log shows the name of the administrator who made the changes, along with the commands that FortiManager sent. If an installation fails, the installation log is useful because it shows the commands that the managed device received and accepted, as well as the commands that the managed device did not accept.

To view the installation log

1. Continuing on the **Configuration Revision History** page, in the **ID** column, select **2**, and then click **View Install Log**.



You should see the CLI commands that FortiManager sent (which are identical to the installation that you previewed earlier) and the FortiGate response.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

2. Click **Close** to close the **View Installation Log of revision 2** window.
3. Click **Close** to close the **Configuration Revision History** window.

View the Auto Update Status, Revision History, and Installation Log for Remote-FortiGate (Optional)

Optionally, you can also view changes made to Remote-FortiGate.

To view the auto update status, revision history, and installation log for Remote-FortiGate (optional)

1. Continuing on the FortiManager GUI, click **Remote-FortiGate**, and then follow the steps in View the Auto Update Status and Revision History on page 69.

   For Remote-FortiGate, you will see the NTP settings that FortiManager pushed based on the imported NTP settings in the **default** system template from Local-FortiGate.

Check the Task Monitor

The task monitor provides the status of the task you performed. You can use it for troubleshooting various types of issues, such as adding, importing, and installing changes from FortiManager.

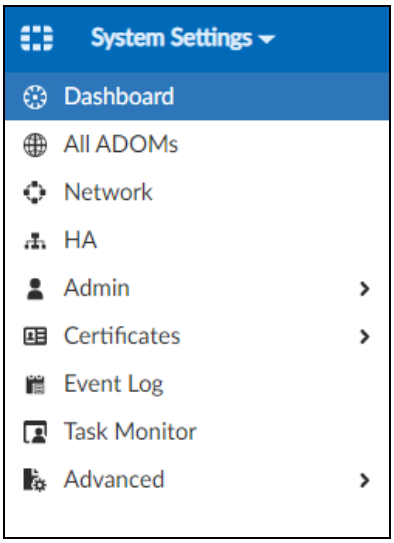
You will now check the entries in the task monitor.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

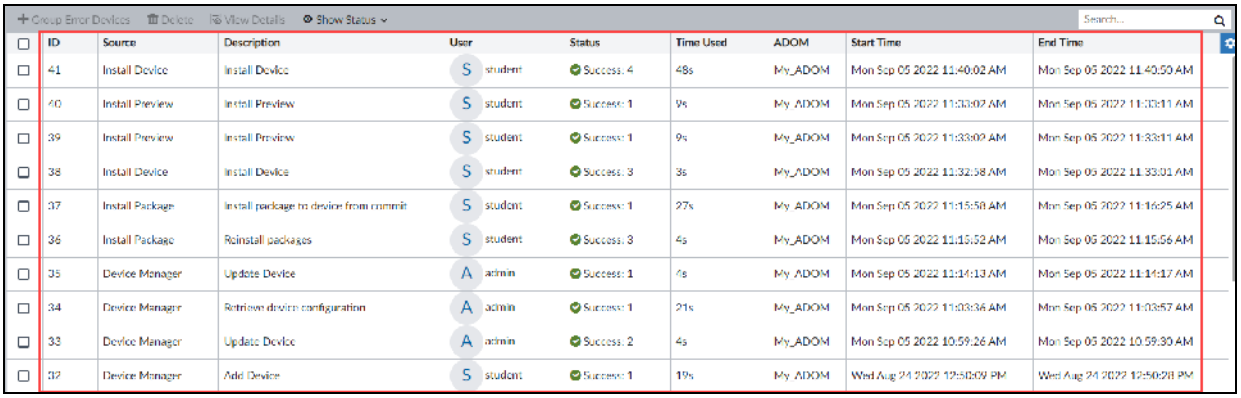
DO NOT REPRINT Brave-Dumps.com
© FORTINET

To check task monitor entries

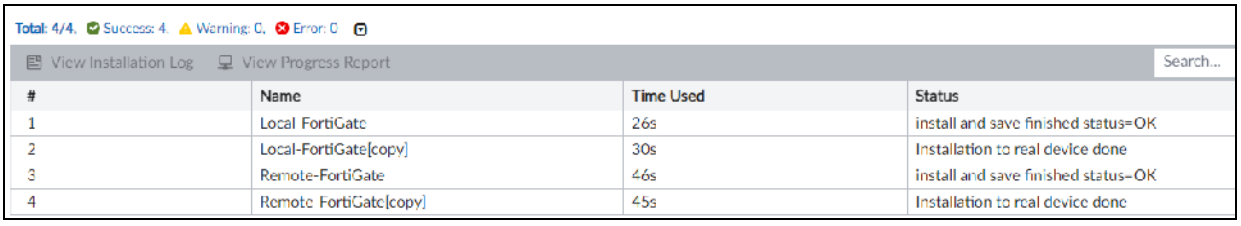
1. Log out of the FortiManager GUI, and then log back in to the FortiManager GUI with the username `admin` and password `password`.
2. Click **root**.
3. Click **System Settings**.
4. Click **Task Monitor**.



Task Monitor shows the tasks that all users performed.



5. Select **Install Device**, and then click **View Details**.



This shows the installation log that corresponds to the installation that you performed earlier.

6. Close the **Install Device** window.
7. Log out of the FortiManager GUI.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

Exercise 4: Configuring Device-Level Changes

You can view and configure the device-level settings of the managed FortiGate in the **Device Manager** pane. Most of these settings have a one-to-one correlation with the device configuration that you would see if you logged in locally on the GUI or CLI of each FortiGate.

In this exercise, you will make configuration changes for the managed FortiGate in the **Device Manager** pane.

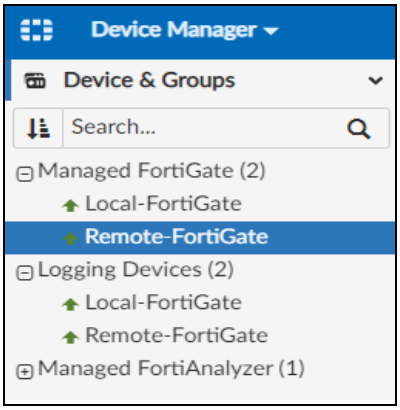
Change the Interface Settings of the Managed FortiGate

If you try to change the managed FortiGate interface that is used for communicating with FortiManager, you receive a warning that this may disrupt the communication between FortiManager and FortiGate. If there is a communication disruption between FortiManager and FortiGate during an installation, FortiManager attempts to recover the connection, but this reverts the installation changes.

You will change the **Administrative Access** setting of the Remote-FortiGate **port4** interface that is used by Remote-FortiGate to communicate with FortiManager.

To change the interface settings of the managed FortiGate

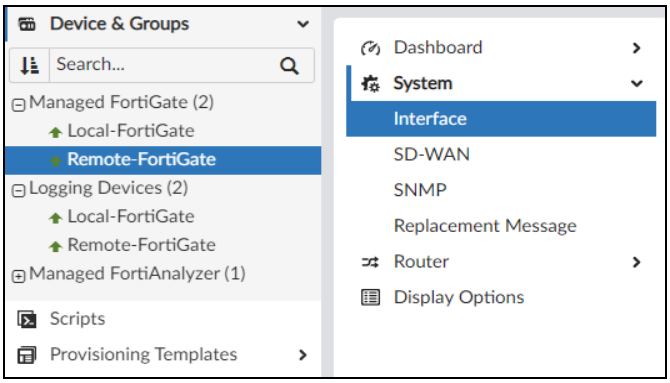
1. Log in to the FortiManager GUI with the username `student` and password `fortinet`.
2. Click **My_ADOM**.
3. Click **Device Manager**.
4. Click **Remote-FortiGate**.



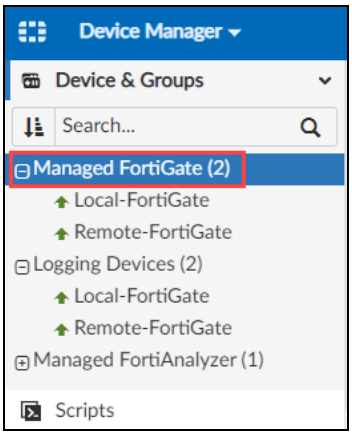
5. Click **System** > **Interface**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

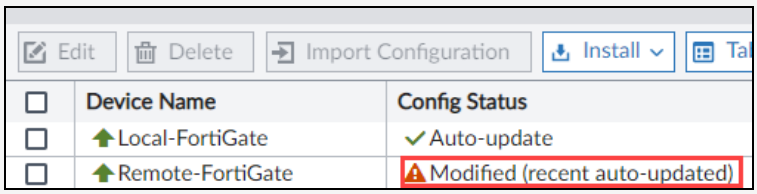


6. Right-click **port4**, and then click **Edit**.
7. In **Administrative Access** section, select the **Security Fabric Connection** checkbox.
8. Click **OK**.
9. Click **Managed FortiGate**.



Stop and think!

Why is the **Config Status** showing the **Modified (recent auto-updated)** status for Remote-FortiGate?



The **Modified** status means that the device-level database change was made to Remote-FortiGate. You changed the interface configuration.

The status **recent auto-updated** in parentheses means that the previous configuration changes were made locally on FortiGate, and then automatically updated on FortiManager. You made changes to logging settings locally in the previous lab.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

Filter Devices Based on Status

FortiManager allows you to filter devices based on their current status. This is very helpful when you are managing a large number of devices in the same ADOM. Based on the status, the FortiManager administrator can take appropriate action.

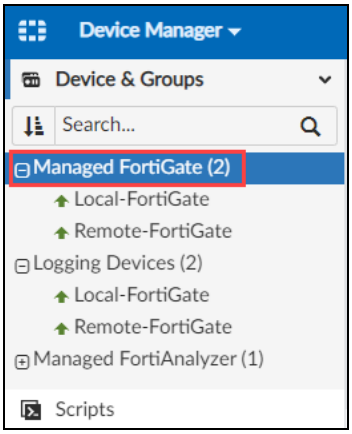
You can filter device statuses based on:

- Connection
- Device configuration (device database status)

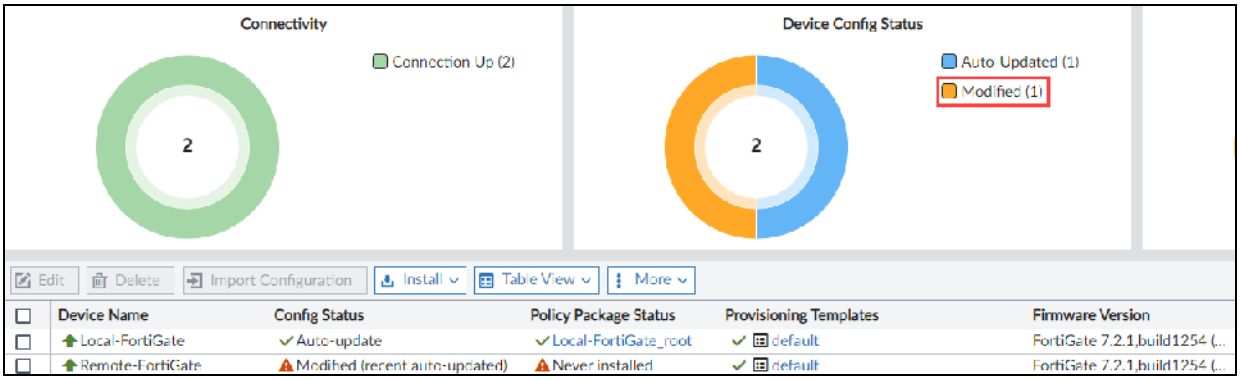
You will now filter devices based on their device configuration status.

To filter devices based on status

1. Continuing on the FortiManager GUI, click **Managed FortiGate**.



2. In the **Device Config Status** dashboard, click **Modified**.



Only **Remote-FortiGate** appears in the **Managed FortiGate** list.

Configure the Administrator Account

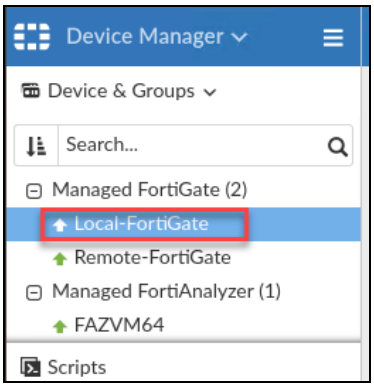
You will create a new administrator account for Local-FortiGate on FortiManager.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

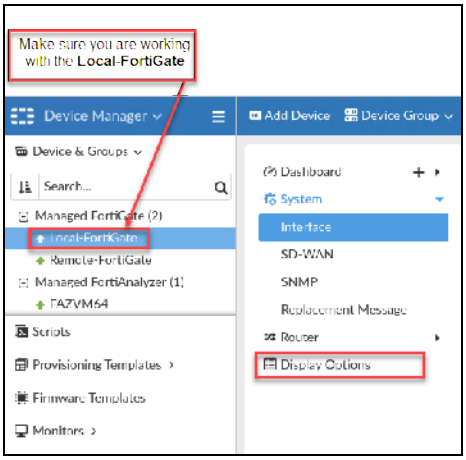
DO NOT REPRINT Brave-Dumps.com
© FORTINET

To configure the administrator account

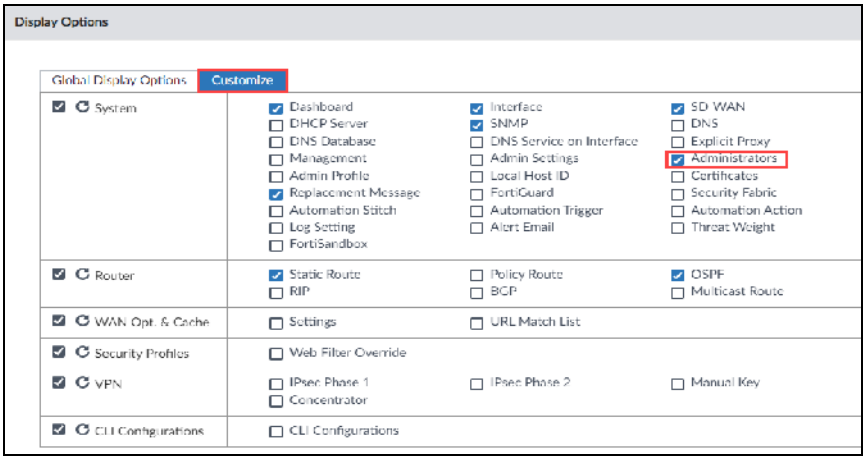
1. Continuing on the FortiManager GUI, click **Local-FortiGate**.



2. Click **Display Options**.



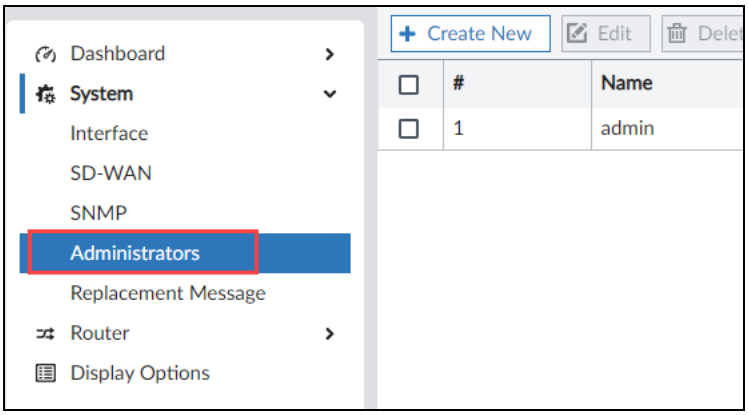
3. Click **Customize**.
4. In the **System** category, select the **Administrators** checkbox.



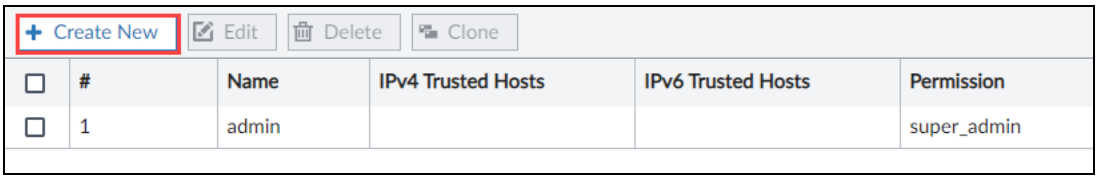
5. Click **OK**.
6. Click **System** > **Administrators**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET



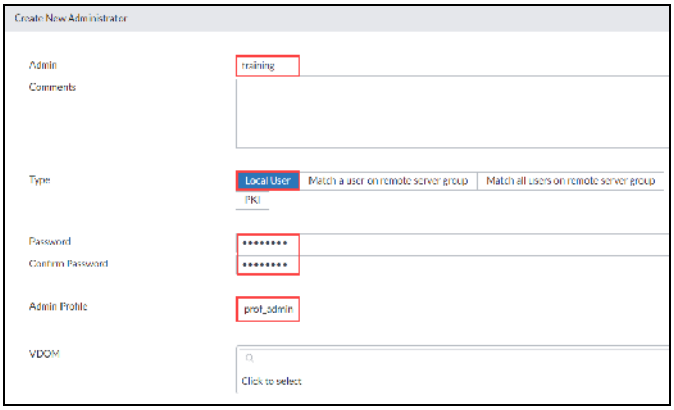
7. Click **Create New**.



8. Configure the following settings:

Field	Value
Admin	training
Type	Local User
Password	fortinet
Confirm Password	fortinet
Admin Profile	prof_admin

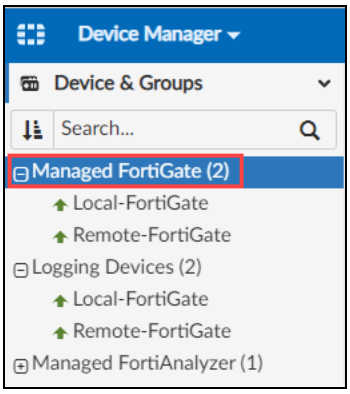
Your configuration should look like the following example:



9. Keep the default values for all other settings, and then click **OK**.
10. Click **Managed FortiGate**.

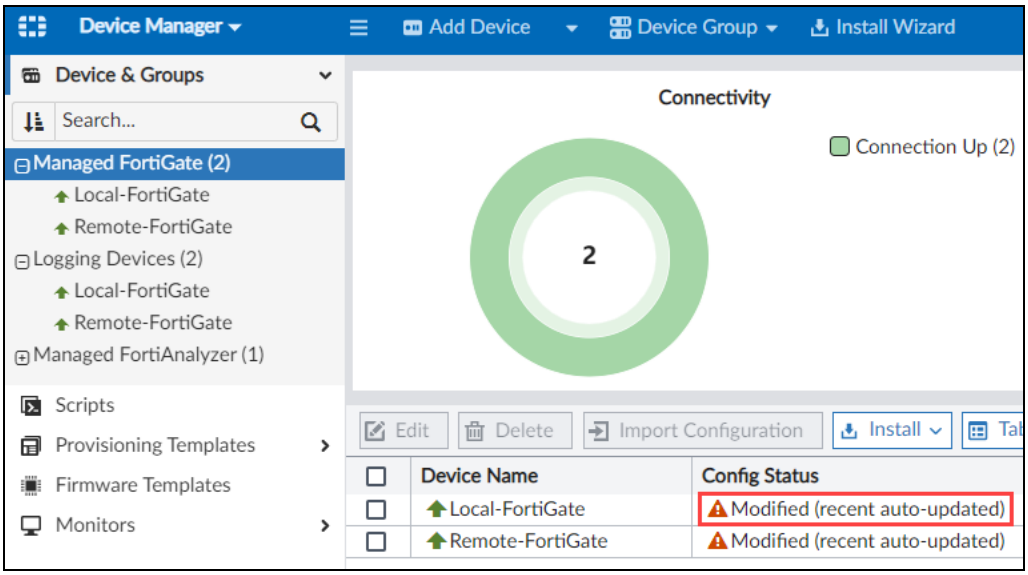
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET



You will notice that the **Config Status** for Local-FortiGate has changed to **Modified**.

This is because you made a device-level configuration change for Local-FortiGate by configuring the administrator account.



Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

Exercise 5: Installing Configuration Changes

You made configuration changes to the managed devices using FortiManager.

- For Remote-FortiGate, you enabled the Security Fabric connection service on port4.
- For Local-FortiGate, you configured a new administrator.

In this exercise, you will install these changes on the managed device using the **Install Wizard**, and then view the installation history. You will also compare the differences in the revision history configurations using the **Revision Diff** feature.

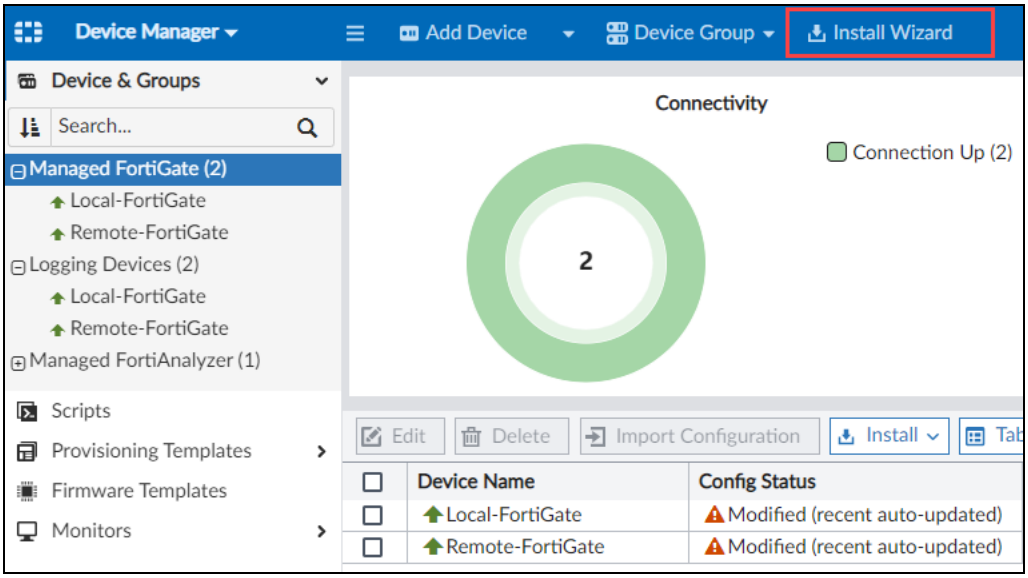
The **Install Preview** in the **Configuration and Installation Status** widget shows only the preview for the device-level changes, *not* the changes related to *policies and objects*.

Use the Install Wizard

You will install these changes on the managed devices using the **Install Wizard**.

To install configuration changes on FortiGate using the Install Wizard

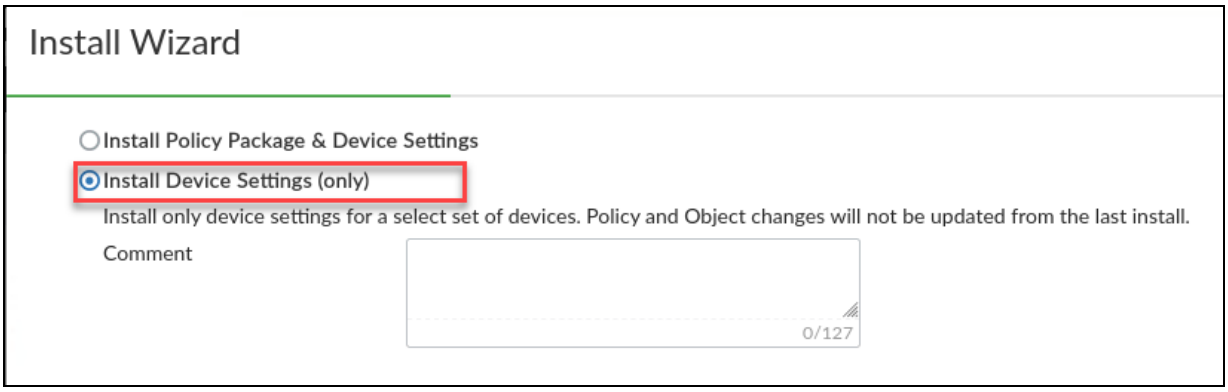
1. Continuing on the FortiManager GUI, click **Install Wizard**.



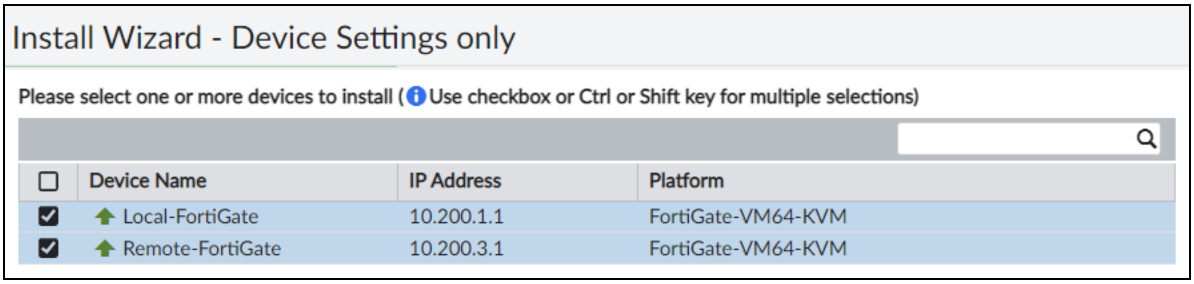
2. Select **Install Device Settings (only)**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

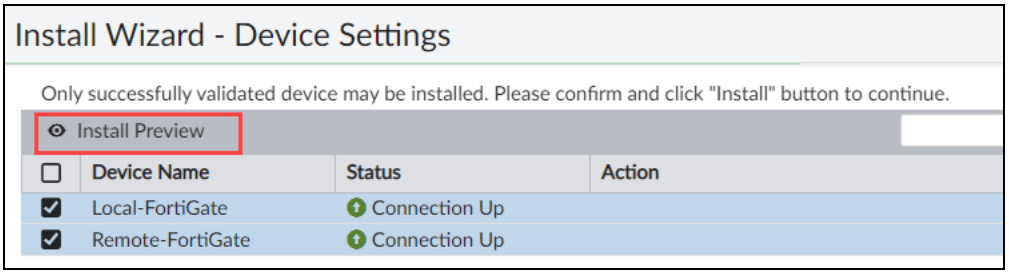
DO NOT REPRINT Brave-Dumps.com
© FORTINET



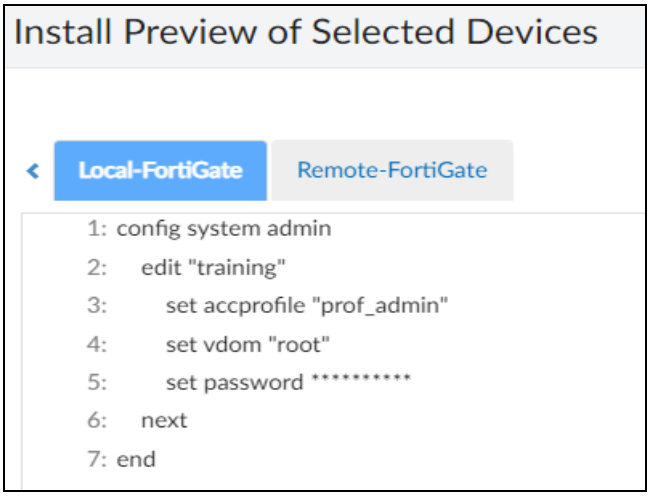
3. Click **Next**.
4. On the **Device Settings** page, make sure that both FortiGate devices are selected.



5. Click **Next**.
6. Click **Install Preview**.



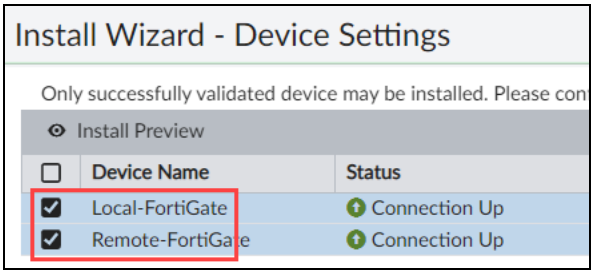
This shows you the changes that will be applied to the FortiGate devices.



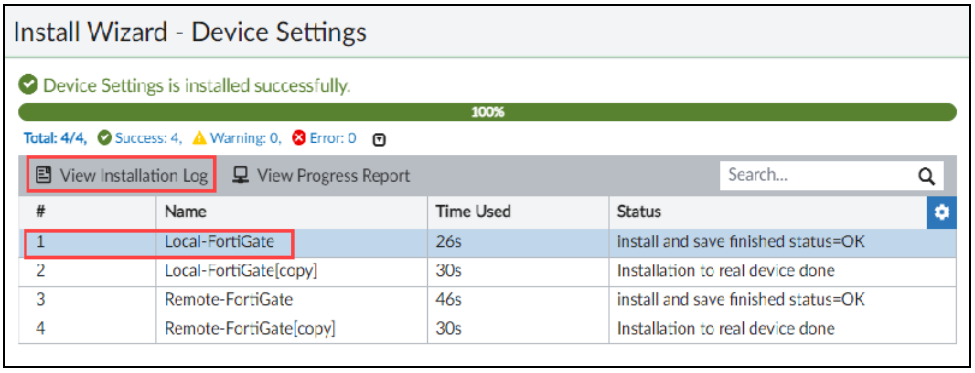
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

7. On the **Install Preview of Selected Devices** page, click **Close**.
   Optionally, you can also check the **Install Preview** for Remote-FortiGate.
8. Make sure that both FortiGate devices are selected.

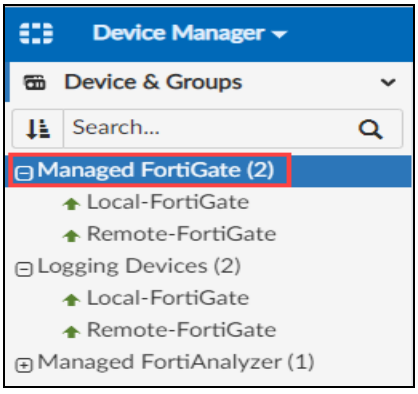


9. Click **Install**.
10. Once the installation has completed successfully, select **Local-FortiGate**, and then click **View Installation Log**.



This is the installation log that shows exactly what is installed on the managed device.

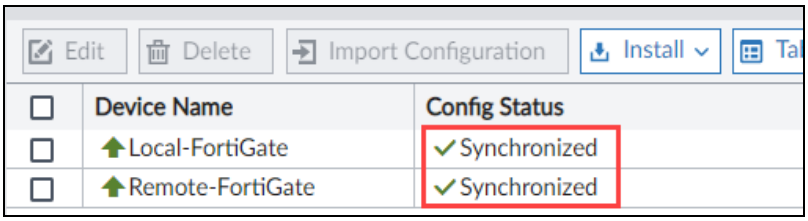
11. On the **Install Log** page, click **Close**.
12. Click **Finish**.
13. Click **Managed FortiGate**.



The **Config Status** should now be in the **Synchronized** state.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET



View the Revision Differences

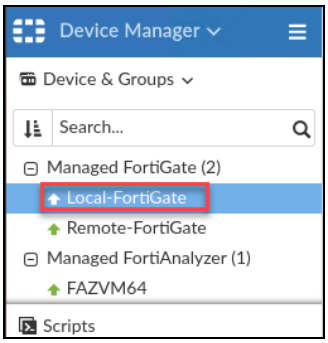
After every retrieve, auto update, and installation operation, FortiManager stores the FortiGate configuration checksum output with the revision history. This is how the out-of-sync condition is calculated.

The **Revision Diff** is a useful feature that you can use to compare the differences between previous revisions, a specific revision, or the factory default configuration. In terms of the output, you can choose to show full configuration with differences, only the differences, or you can capture the differences to a script.

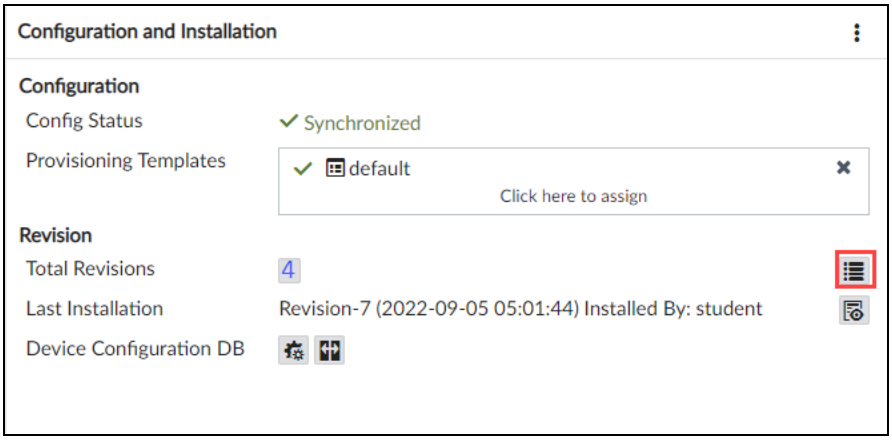
You will compare the differences between the latest revision and previous revision.

To view the revision differences

1. Continuing on the FortiManager GUI, click **Local-FortiGate** > **Dashboard** > **Summary**.



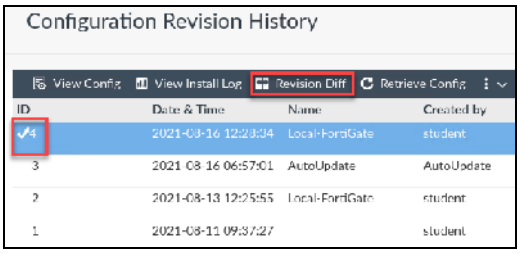
2. In the **Configuration and Installation** widget, click the **Revision History** icon.



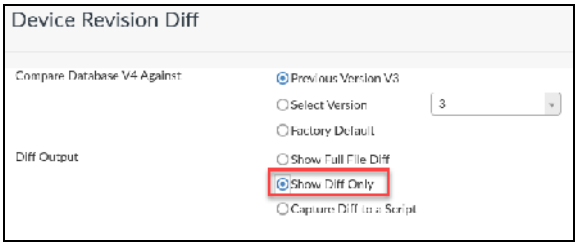
3. In the **ID** column, click **4**, and then click **Revision Diff**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

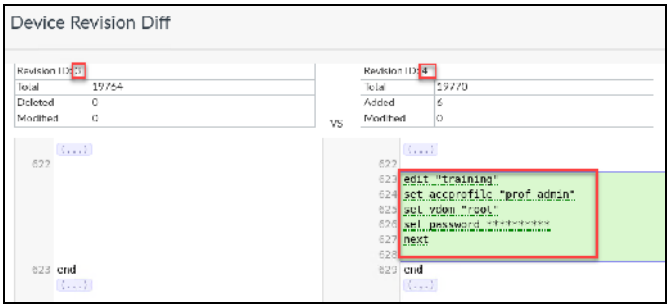
DO NOT REPRINT Brave-Dumps.com
© FORTINET



4. Select **Show Diff Only**.



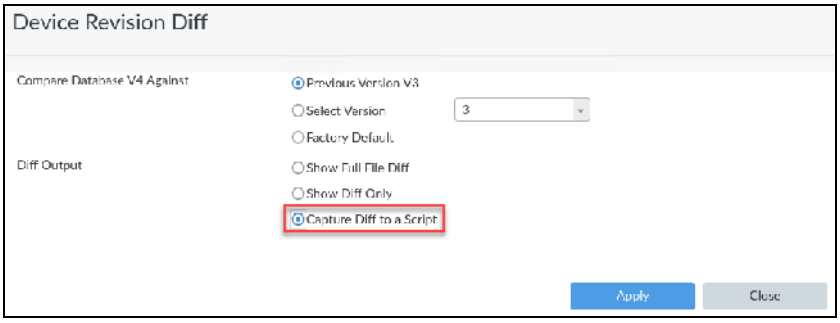
5. Click **Apply**.



This shows the difference in configuration between the previous version and the current running version.

Remember, you configured the FortiAnalyzer settings for both FortiGate devices.

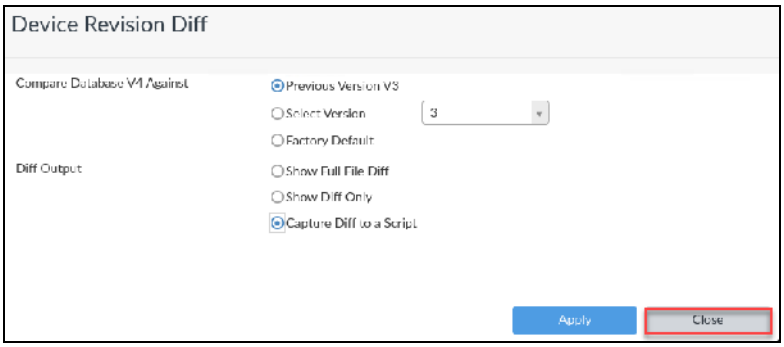
6. Click **Close**.
7. In the **ID** column, click **4** again, and then click **Revision Diff**.
8. Select **Capture Diff to a Script**.



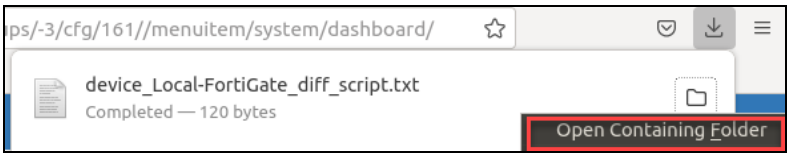
9. Click **Apply**.
10. Click **Close**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

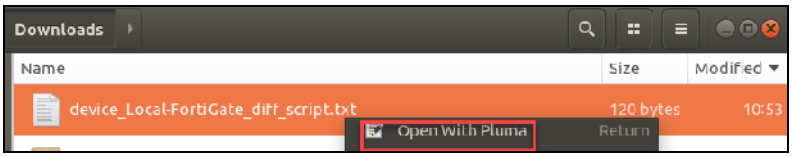
DO NOT REPRINT Brave-Dumps.com
© FORTINET



11. In the **Configuration Revision History** window, click **Close**.
12. In the Firefox window, click the download icon.
13. Right-click the filename, and then click **Open Containing Folder**.



14. Open the file using the default text editor.



This shows you the exact CLI syntax of the changes. You can use this script to configure other FortiGate devices if they require the same settings using the script feature on FortiManager.

15. Close the text editor and **Downloads** windows.

This demonstrates capturing differences in the form of scripts. Make sure that the script captured is valid for other FortiGate devices before using it for other FortiGate devices. If required, you can edit the script before applying it to other FortiGate devices.

For example, if you configured a static route along with the administrator setting, the static route settings might not be valid for other FortiGate devices.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

Exercise 6: Using Scripts

A script can make many changes to a managed device and is useful for making bulk configuration changes and ensuring consistency across multiple managed devices. You can configure and install scripts from FortiManager to managed devices.

Scripts can be run on:

- Device database (default)
- Policy package
- ADOM database
- Remote FortiGate directly (using the CLI)

You must perform an installation if you run a script on a device database, policy package, or ADOM database.

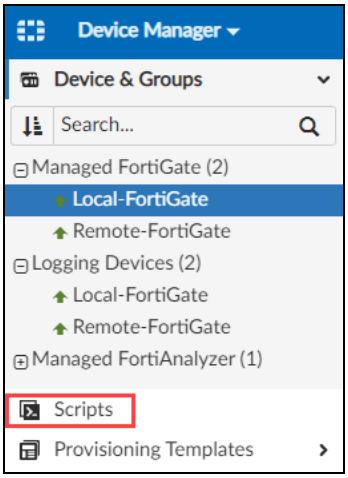
In this exercise, you will make configuration changes using the script feature, and then install the changes on the managed devices.

Configure Scripts

You will configure scripts for the managed devices.

To configure scripts

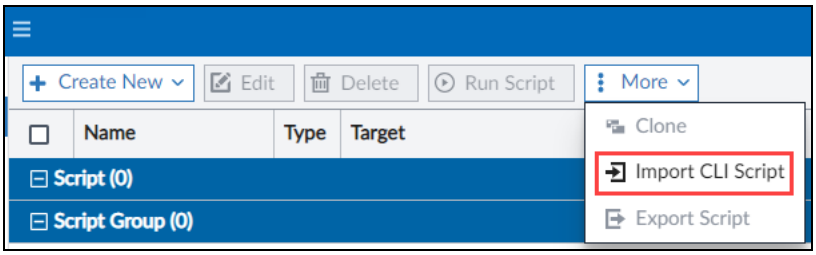
1. Log in to the FortiManager GUI with the username `student` and password `fortinet`.
2. Click **My_ADOM**.
3. Click **Device Manager**.
4. Click **Scripts**.



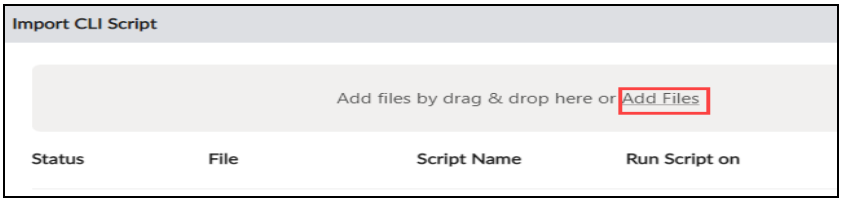
5. Click **More** , and then click **Import CLI Script**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

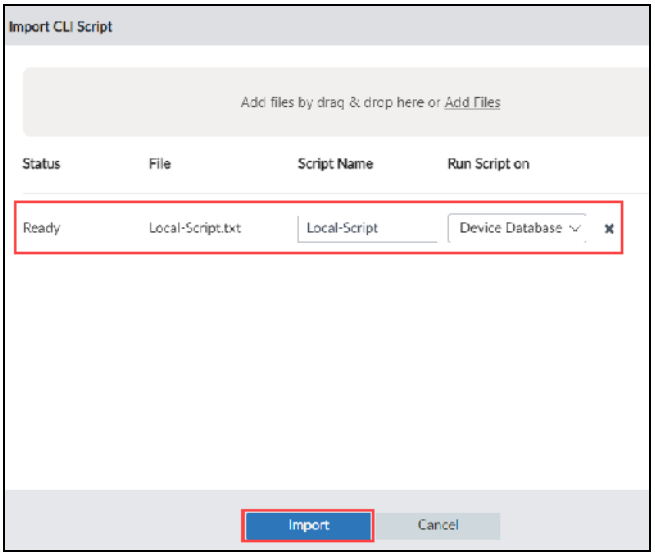
DO NOT REPRINT Brave-Dumps.com
© FORTINET



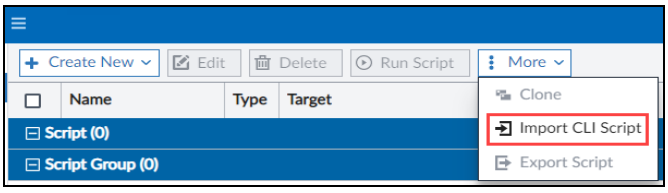
6. Click **Add Files**.



7. Click **Desktop** > **Resources** > **FortiManager** > **Device-Config**, and then select `Local-Script`.
8. Click **Open**, keep the default values for all other settings, and then click **Import**.



9. Click **Close**.
10. Click **Import CLI Script** again.



11. Click **Add Files**.
12. Click **Desktop** > **Resources** > **FortiManager** > **Device-Config**, and then select `Remote-Script`.
13. Click **Open**, keep the default values for all other settings, and then click **Import**.
14. Click **Close**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

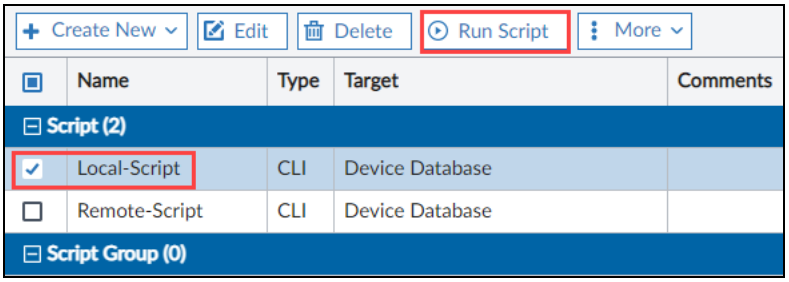
DO NOT REPRINT Brave-Dumps.com
© FORTINET

Run and Install Scripts

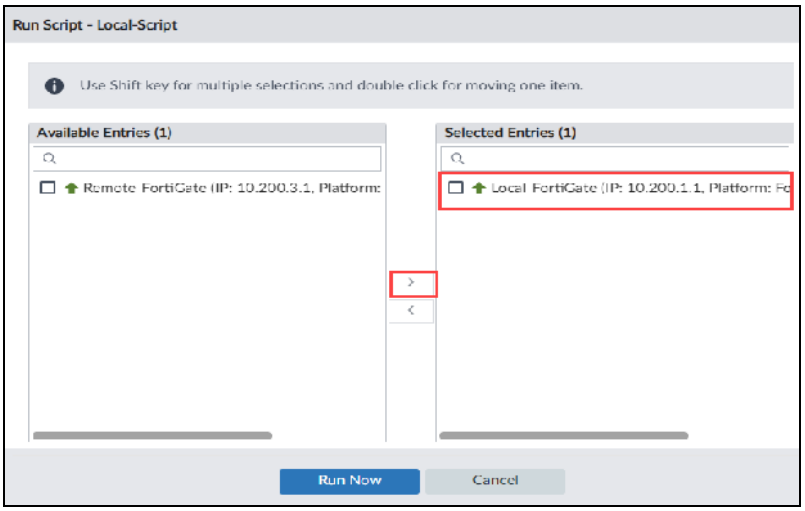
Because the scripts target the device database, you will first run the scripts against the device database, and then install the scripts on the managed devices.

To run scripts

1. Continuing on the FortiManager GUI, select the **Local-Script** checkbox, and then click **Run Script**.

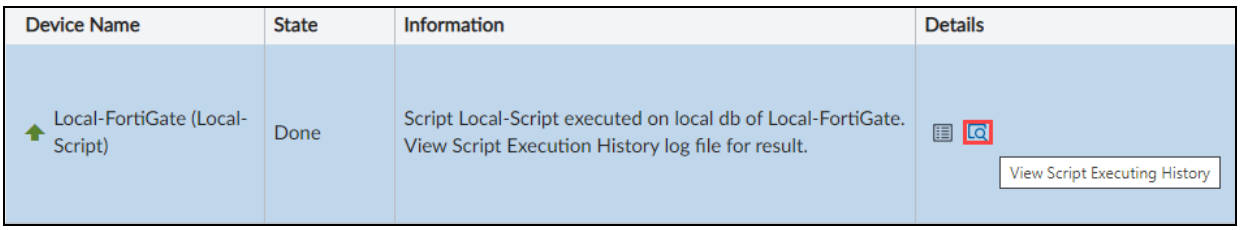


2. Select and add **Local-FortiGate** to the **Selected Entries** list.



3. Click **Run Now**.
4. Click **OK**.
5. Click **View Details**, and then click the **View Script Executing History** icon.

   Scroll to the bottom of the script execution window to check that the script ran successfully on the device database.



Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

View the log of script Local-Script: running on device Local-FortiGate (Local-Script)

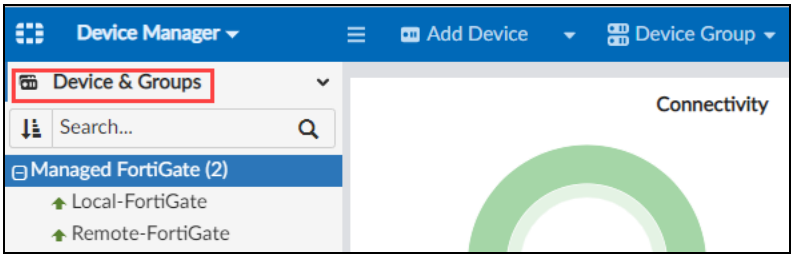
```
set gateway 10.200.2.254
set distance 20
set device "port2"
next
end
config system link-monitor
edit "1"
set srcintf "port1"
set server "10.200.3.1"
set gateway-ip 10.200.1.254
next
edit "2"
set srcintf "port2"
set server "10.200.4.1"
set gateway-ip 10.200.2.254
next
end
Running script(Local-Script) on DB success
----------------End of Log-------------------------
```

If required, you can also view the script execution history later in the **Configuration and Installation Status** widget or in the **Task Monitor**.

6. Click **Close**.
7. Click **Close**.
8. Clear the **Local-Script** checkbox, select the **Remote-Script** checkbox, and then click **Run Script**.
9. Select and add **Remote-FortiGate** to the **Selected Entries** list.
10. Click **Run Now**.
11. Click **OK**.
12. Click **Close**.

To install scripts

1. Continuing on the FortiManager GUI, click **Device & Groups** > **Managed FortiGate**.



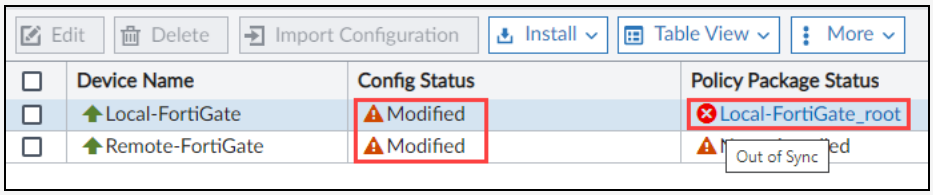
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

Stop and think!

Why is the **Config Status** showing **Modified** for both FortiGate devices? If you do not see the **Modified** status, refresh the page a few times.

Why is the **Policy Package Status** for Local-FortiGate showing **Out of Sync**, but the **Policy Package Status** for Remote-FortiGate remains unchanged as **Never Installed**?



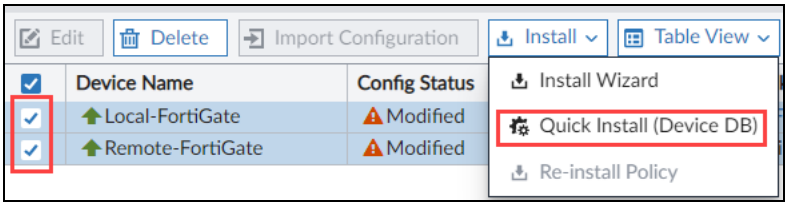
The scripts contain configuration changes related to device-level settings and policies.

The **Config Status** is **Modified** for both FortiGate devices because of device-level changes.

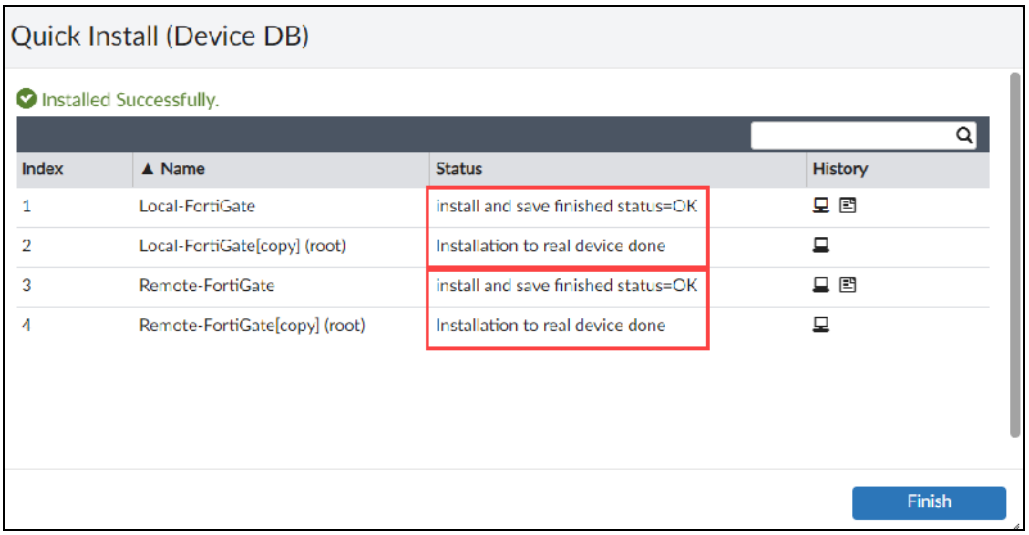
Because the Local-FortiGate policy package was imported when you added FortiGate, FortiManager detects policy-level changes, and marks the Local-FortiGate **Policy Package Status** as **Out of Sync**.

For Remote-FortiGate, the policy package was never imported, and therefore FortiManager cannot compare the differences in the policies.

2. Select **Local-FortiGate** and **Remote-FortiGate**, click **Install**, and then click **Quick Install**.



3. Click **OK**.
The installation is successful on both FortiGate devices.



Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

The **Quick Install** option does not provide an option for installation preview and installation log. You should use it only if you are absolutely sure about the changes you are trying to install.

4. Click **Finish**.

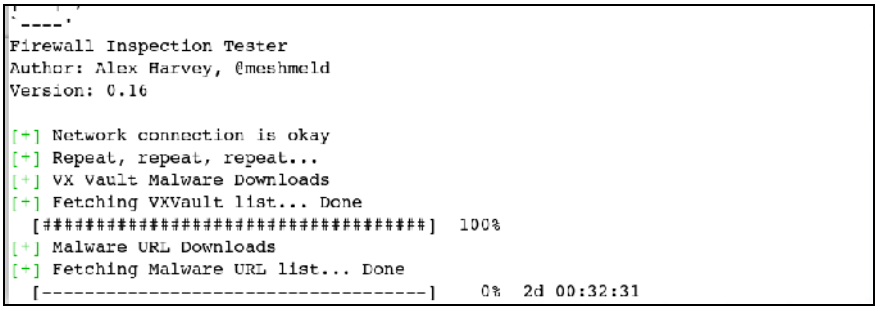
Generate Traffic With FIT

The firewall inspection tester (FIT) VM generates web browsing traffic, application control, botnet IP hits, malware URLs, and malware downloads.

You will direct FIT-generated traffic through the Local-FortiGate firewall policy. This traffic will be used to run FortiAnalyzer reports later in the labs.

To generate traffic with FIT

1. On the Local-Client VM, open PuTTY, and then connect over SSH to the FIT saved session.
2. Log in with the username `student` and password `password`.
3. Enter the following command to run a script to change the default route of FIT to send traffic through Local-FortiGate:
   `sudo ./default1`
4. When prompted, enter the password again.
5. Enter the following command to check the default route:
   `ip route`
   You should see the default route through `10.0.1.254`.
6. Enter the following commands:
   ```
   cd FIT
   ./fit.py all --repeat
   ```
   Traffic begins to generate and repeats the script each time it completes.



7. Leave the PuTTY session open (you can minimize it) so traffic continues to generate.
   This will run throughout the remainder of the labs.

Do not close the FIT PuTTY session or traffic will stop generating.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

Lab 5: Policies and Objects

In this lab, you will explore the common operations of the **Policy & Objects** pane, which you can use to centrally manage FortiGate firewall policies and manage shared and dynamic objects.

Objectives

- Import firewall policies and objects from a managed device, and then review the imported policy packages
- Create ADOM revisions
- Use workflow mode to configure and send changes for approval
- Find duplicate objects and merge them, and delete used objects
- Create a policy package that is shared across multiple devices
- Create shared objects and dynamic objects with mapping rules
- Identify the different policy and object interface mapping types, and configure zone mappings
- Install a policy package and device settings on the **Policy & Objects** pane
- Run a FortiAnalyzer report

Time to Complete

Estimated: 70 minutes

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

Exercise 1: Importing Policies

In the previous lab, you installed scripts that contained device-level and policy configuration changes. Because you ran the scripts on a device database that created the revision history containing these changes, the policy packages are not automatically updated, and you must import them manually.

In this exercise, you will import the policies using the **Import Policy** wizard, which will update the policy packages to reflect the configuration changes.

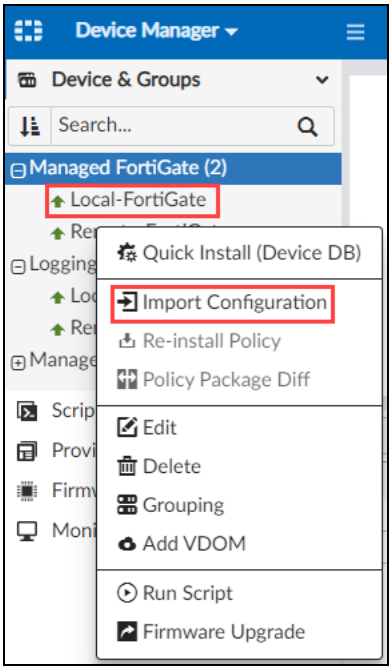
Additionally, you will create an ADOM revision, which is a snapshot of all the policy and object configurations for an ADOM.

Import Policies

You will import policies and objects for both of the managed FortiGate devices.

To import policies

1. Log in to the FortiManager GUI with the username `student` and password `fortinet`.
2. Click **My_ADOM**.
3. Click **Device Manager**.
4. Right-click **Local-FortiGate**, and then click **Import Configuration**.

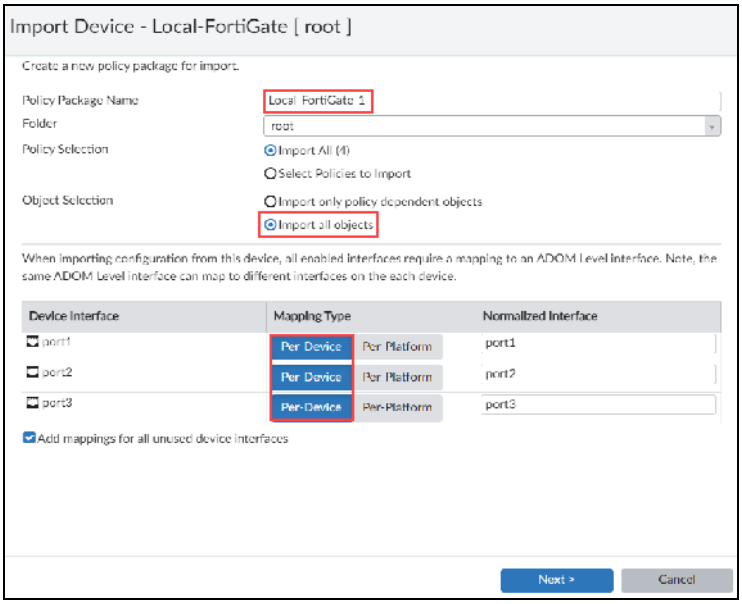


5. Select **Import Policy Package**.
6. Click **Next**.
7. In the **Policy Package Name** field, type `Local-FortiGate-1` to change the name.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

8. In the **Object Selection** field, select **Import all objects**.
9. In the **port2** row, select **Per-Device**, and then ensure that the other two ports are also set to **Per-Device**.



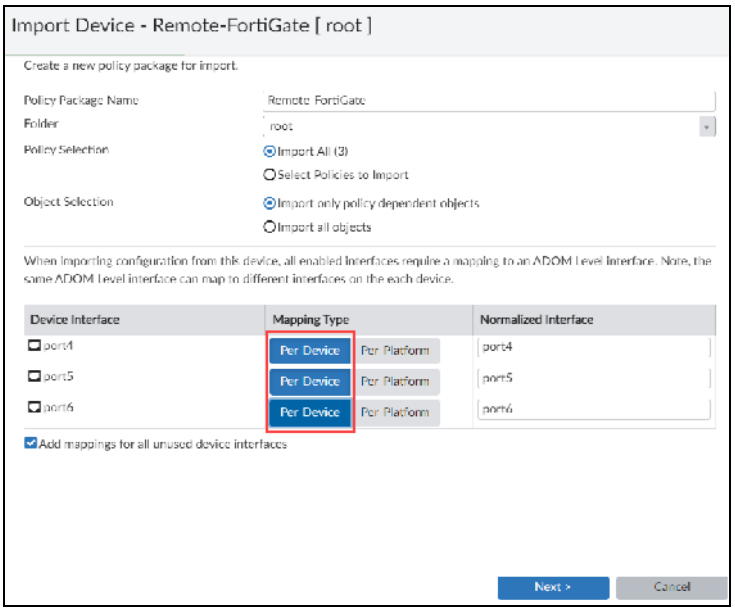
10. Click **Next**.
11. On the conflict page, click **Next**.
    Review the objects that will be imported.
12. Click **Next**.
13. Click **Download Import Report**.
14. In the **Downloads** folder, right-click the file, select **Open with**, select Notepad ++, and then click **OK**.
15. Review the download import report, and then close the Notepad++ file.
16. Click **Finish**.

Download Import Report is available only on this page—make sure that you download the import report before you click **Finish**.

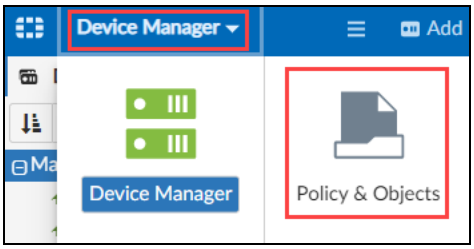
17. Right-click **Remote-FortiGate**, and then click **Import Configuration**.
18. Select **Import Policy Package**.
19. Click **Next**.
20. In the **Mapping Type** column, select **Per-Device** for all three ports.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

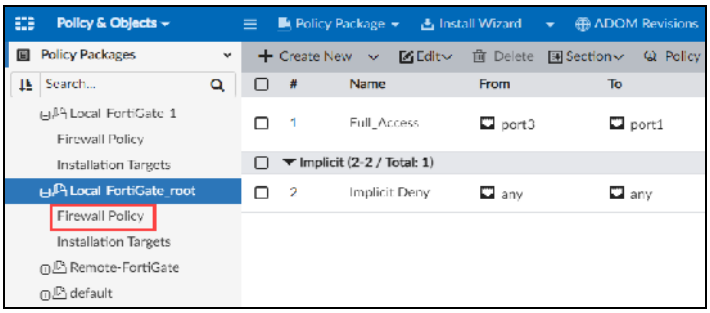


21. Click **Next**.
22. Click **Next** until you reach the **Finish** page.
23. Click **Finish**.
24. Click **Device Manager**, and then click **Policy & Objects**.



25. Click **Policy Packages**.
26. Click **Firewall Policy** for each policy package to compare the policies in the **Local-FortiGate_root** and **Local-FortiGate-1** policy packages.

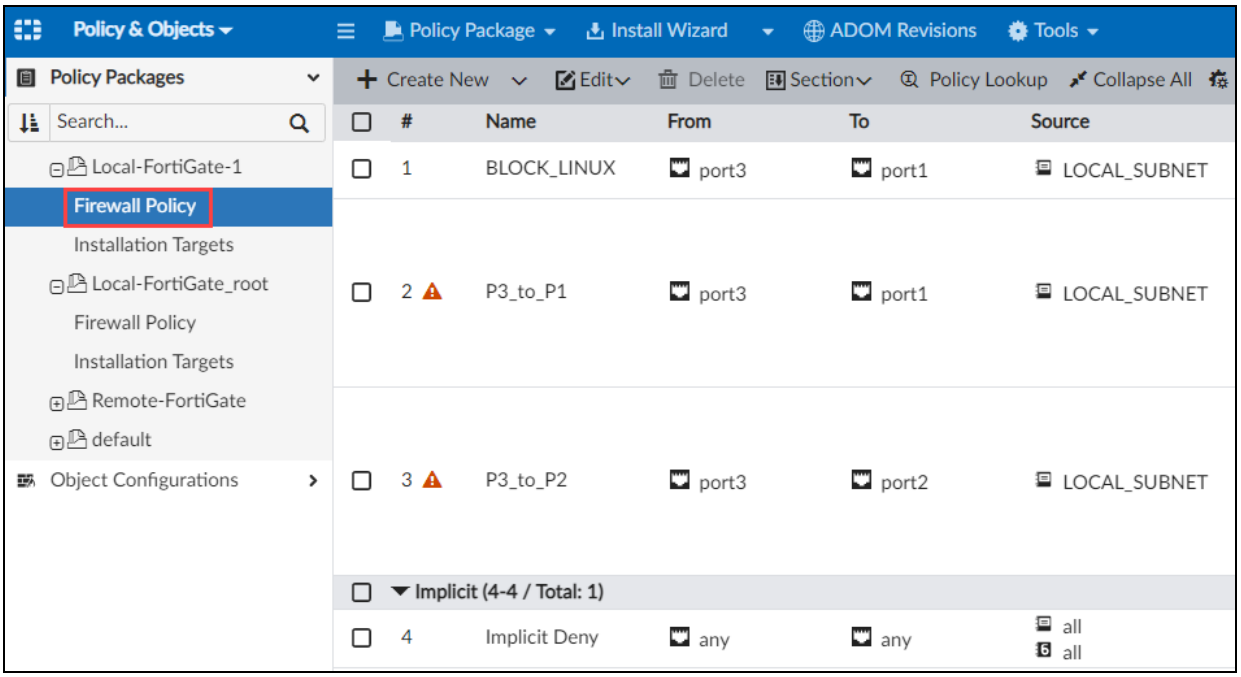
    The following image shows the policy package for **Local-FortiGate_root**:



    The following image shows the policy package for **Local-FortiGate-1**:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

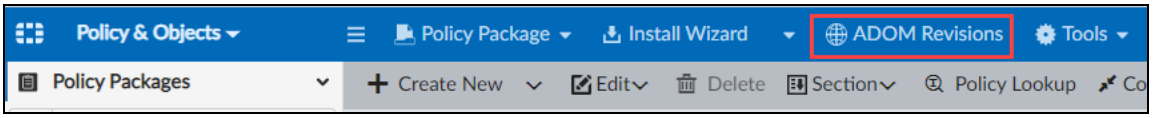


Create ADOM Revisions

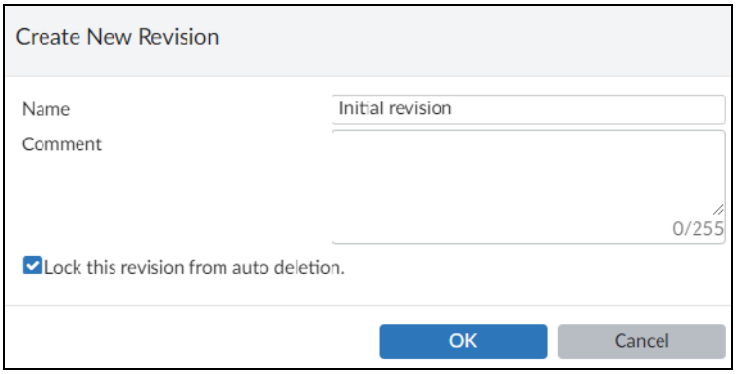
An ADOM revision creates a snapshot of the policy and object configuration for the ADOM. Now that you have imported policies and objects from both FortiGate devices, you will create ADOM revisions that are stored locally on FortiManager, and are useful for comparing the differences between two revisions or reverting to a previous revision.

To create an ADOM revision

1. Continuing on the FortiManager GUI, click **ADOM Revisions**.



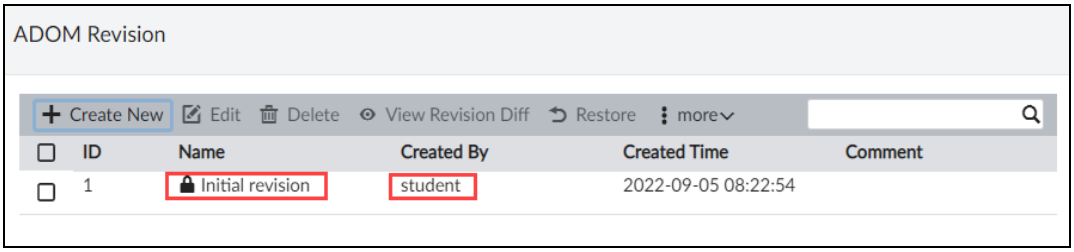
2. Click **Create New**, and then in the **Name** field, type `Initial revision`.
3. Select **Lock this revision from auto deletion**.



Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

4. Click **OK**.
   You can see the lock icon, the name of the administrator who created the revision, and the date and time.



5. Click **Close**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

Exercise 2: Enabling Workflow Mode

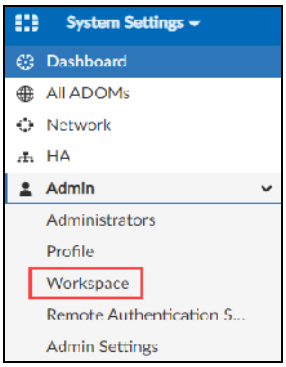
You can use workflow mode to control the creation, configuration, and installation of policies and objects. It helps to ensure that all changes are reviewed and approved before they are applied.

Workflow mode is similar to ADOM locking (workspace mode), but it also allows administrators to submit their configuration changes for approval. Configuration changes are not committed to the FortiManager database until the approval administrator approves the changes. Only approved configuration changes can be installed on the managed device.

In this exercise, you will enable workflow mode, and then make configuration changes related to policies and objects. You will send configuration changes for approval and, once they are approved, you will install the changes.

To enable workflow mode and configure approval permissions

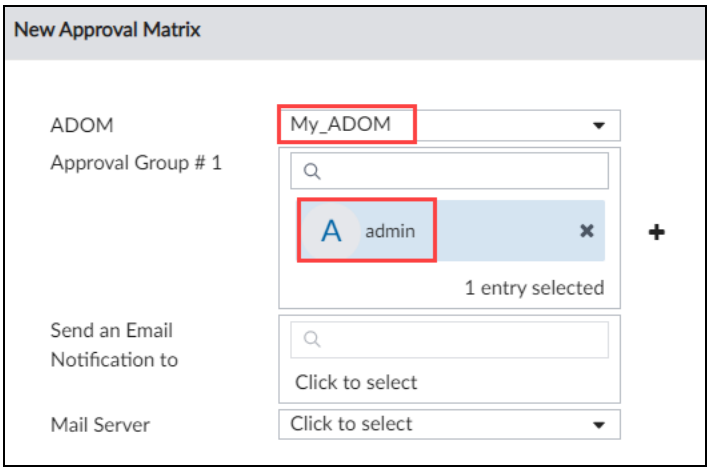
1. Log in to the FortiManager GUI with the username `admin` and password `password`.
2. Click **My_ADOM**.
3. Click **System Settings**.
4. Click **Admin** > **Workspace**.



5. Click **Workflow**.
6. Click **Create New**.
7. In the **ADOM** field, select **My_ADOM**.
8. In the **Approval Group # 1** field, select **admin**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET



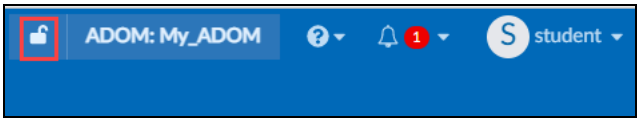
9. Click **OK**.
10. Click **OK**.
11. Click **Apply**.

Before you enable workflow mode, ensure that all FortiManager administrators are notified to save their work on FortiManager. This is because enabling workflow mode terminates all management sessions.

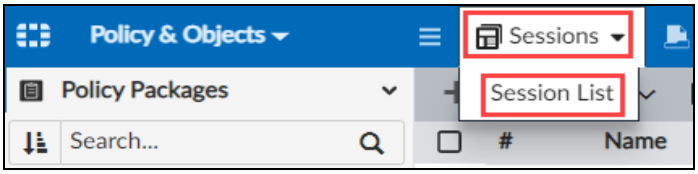
12. Click **OK**.

To configure policies and objects and send them for approval

1. Log in to the FortiManager GUI with the username `student` and password `fortinet`.
2. Click **My_ADOM**.
3. At the top of the page, click the lock icon to lock the ADOM.



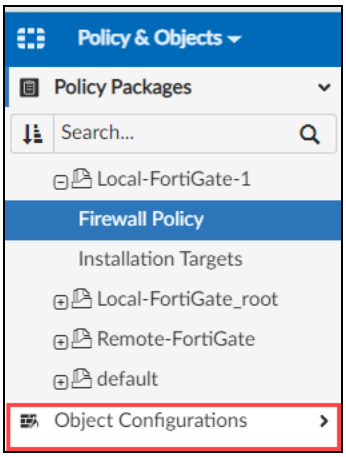
4. Click **Policy & Objects**.
5. Click **Sessions** > **Session List**.



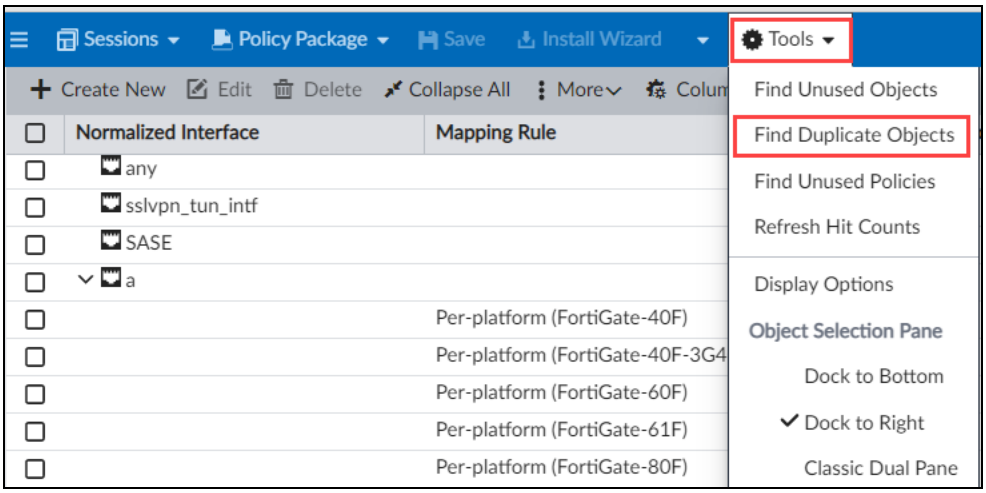
6. Click **Create New Session**.
7. In the **Session Name** field, type `Training`.
8. Click **OK**.
9. Click **Object Configurations**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

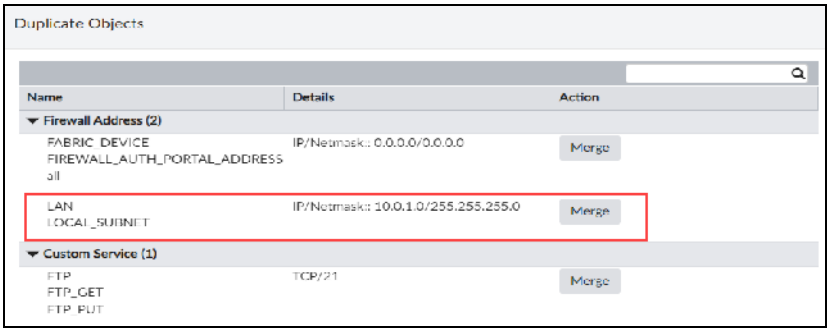
DO NOT REPRINT Brave-Dumps.com
© FORTINET



10. Click **Tools** > **Find Duplicate Objects**.

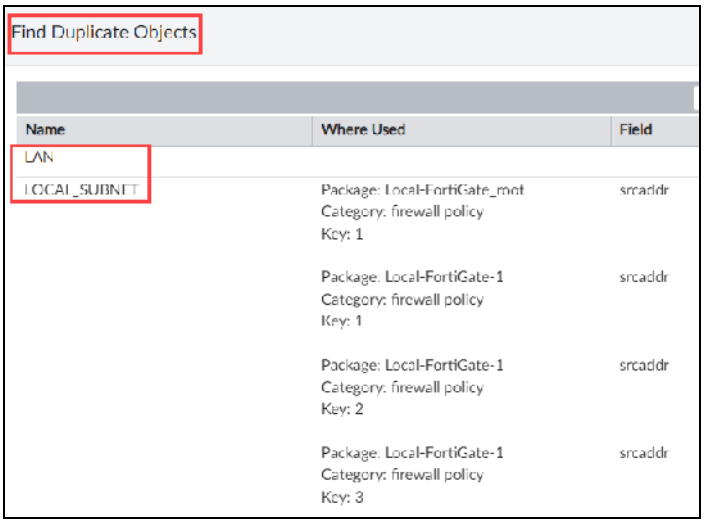


11. Expand **Firewall Address**, and then in the **LOCAL_SUBNET** row, click **Merge**.



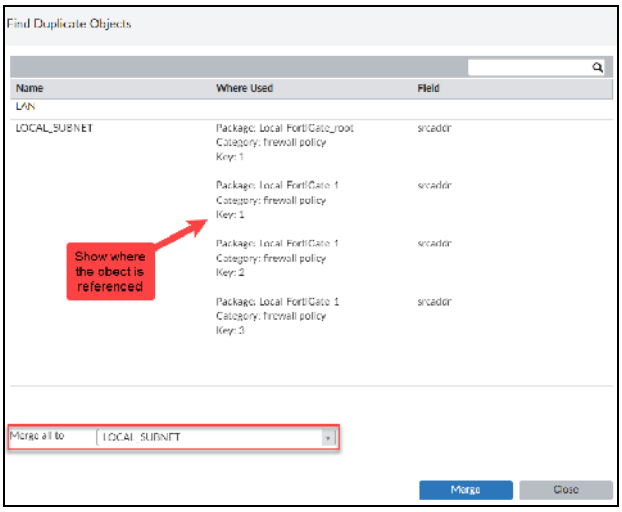
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET



You can see that both the **LAN** and **LOCAL_SUBNET** firewall addresses are displayed as duplicate objects because both have the same values. Other objects that have the same values are also displayed.

12. In the **Merge all to** field, select **LOCAL_SUBNET**.



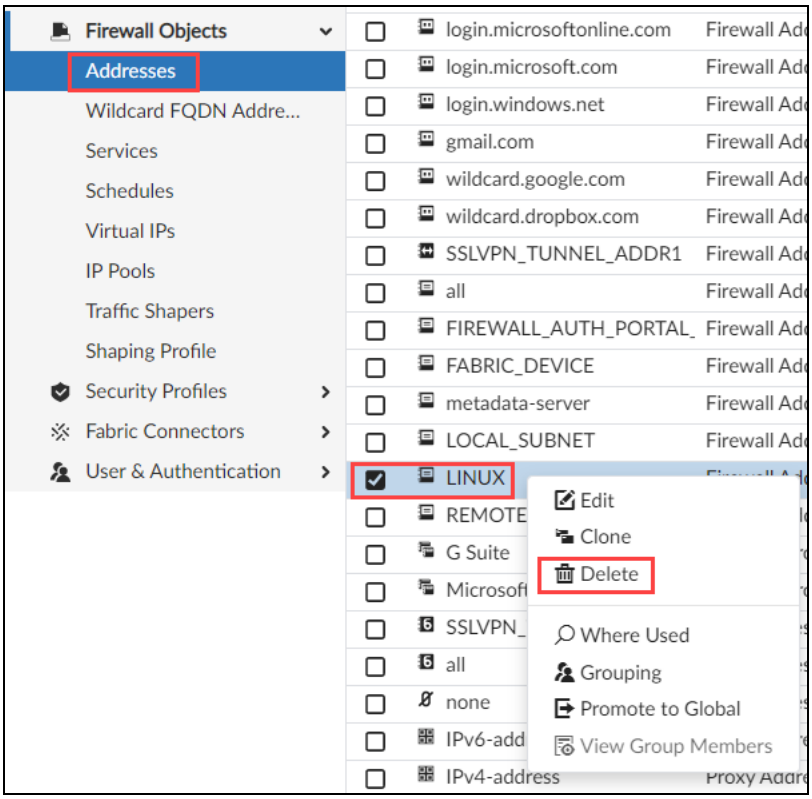
13. Click **Merge**.
14. Click **Close**.

By merging the duplicate objects, you can reduce the object database, which may help to avoid overwhelming the FortiManager administrator with a large number of objects from different FortiGate devices in the same ADOM. You can also delete the unused objects in the same **Tools** menu if they will not be used in the future.

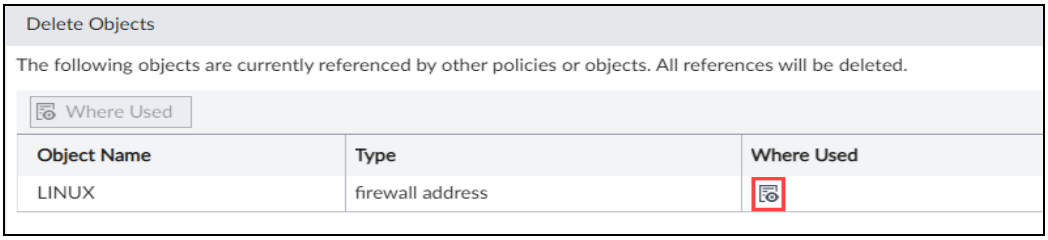
15. Expand **Firewall Objects**, and then click **Addresses**.
16. Right-click the **LINUX** address object, and then click **Delete**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET



17. Click **OK**.
18. Click the **Where Used** icon.
    This shows where the object is referenced.



    The object is referenced in the **Local-FortiGate-1** policy package in firewall policy **1** as the **destination address**.

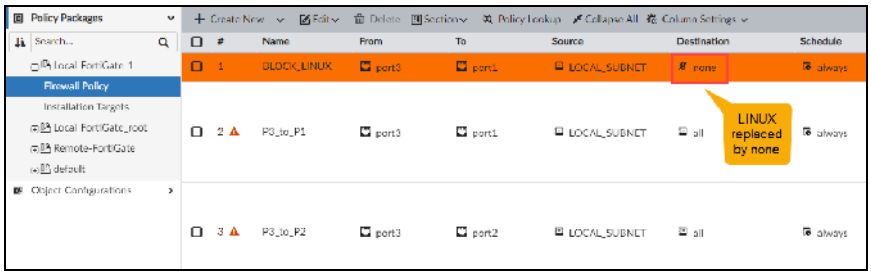
19. Click **Close**.
20. Click **Delete Anyway**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

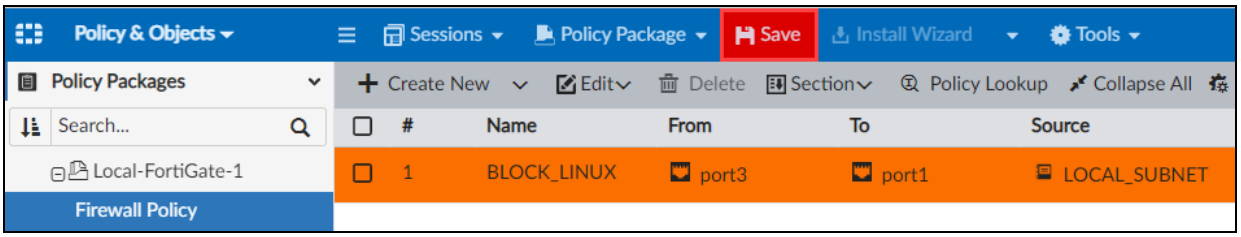
FortiManager allows you to delete a used object. Be careful about deleting a used object because it will be replaced by the none address 0.0.0.0/255.255.255.255.

This means that any traffic that meets this specific firewall policy is blocked if there is no catch all or shadowed policy below it. In this case, the **destination address** of firewall policy **1** in the **Local-FortiGate-1** policy package is replaced by **none** after the **LINUX** address object is deleted.

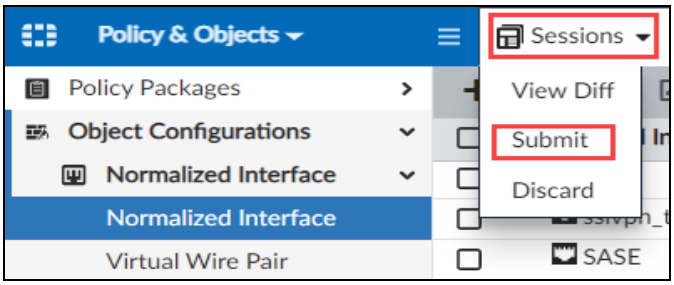


You will test this later in this exercise.

21. Click **Save**.



22. Click **Sessions**, and then click **Submit**.



23. Click **OK**.
    The ADOM unlocks itself after you submit the changes.

Your changes are still not saved in the FortiManager database because they must first be approved by the approval administrator.

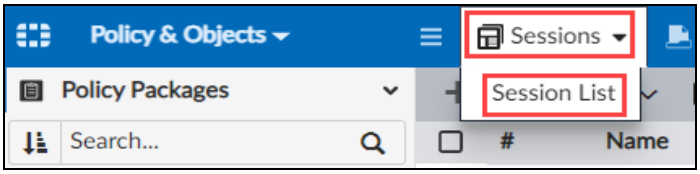
To approve the changes

1. Log out of the FortiManager GUI, and then log back in with the username `admin` and password `password`.
2. Click **My_ADOM**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

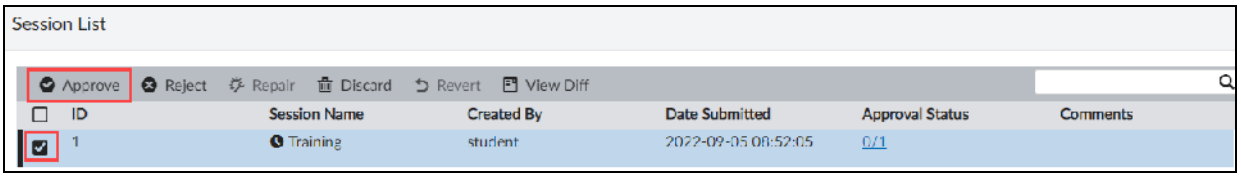
3. Click the lock icon to lock the ADOM.
4. Click **Policy & Objects**.
5. Click **Sessions** > **Session List**.



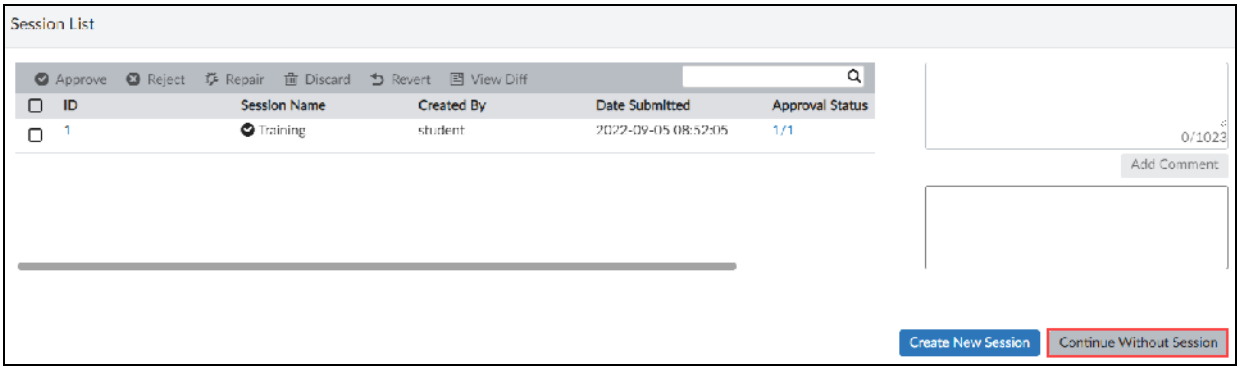
The session list shows you the name of the request made, user, date, and approval status.

The approval administrator can approve, reject, discard, or view the differences between two revisions. The approval administrator can also create a session that can be sent to a different approval administrator, or can self-approve based on the workflow approval matrix.

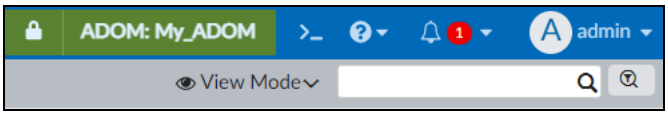
6. In the **ID** column, select **1**, and then click **Approve**.



7. Click **OK**.
8. Click **Continue Without Session**.



9. Click the **lock** icon to unlock the ADOM.



10. Log out of the FortiManager GUI.

If an administrator locks ADOMs, and then logs out of the FortiManager GUI, the locks release for all the ADOMs that the administrator locked.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

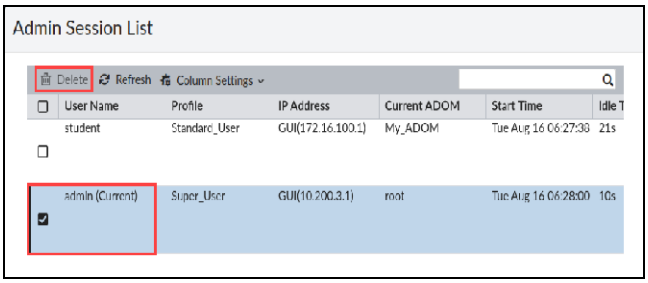
DO NOT REPRINT Brave-Dumps.com
© FORTINET

Always log out of the FortiManager GUI gracefully when ADOM locking (workspace or workflow) is enabled.

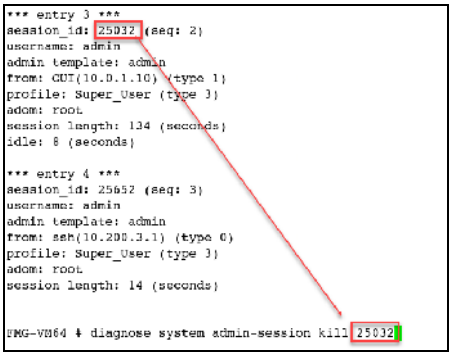
If a session is not closed gracefully (PC crash or closed browser window), FortiManager does not close the administrator session until the administrator session timeout is reached or the session is deleted. The locked ADOM remains locked.

You must delete the session manually on the GUI or CLI.

On the GUI (**System Settings** > **System Information** widget > **Current Administrators** > **Admin Session List**) :



On the CLI:



To install configuration changes after they are approved

1. Log in to the FortiManager GUI with the username `student` and password `fortinet`.
2. Click **My_ADOM**.
3. At the top of the page, click the lock icon to lock the ADOM.
4. Click **Policy & Objects**.
5. Click **Local-FortiGate-1** > **Firewall Policy**.
   You can see that **LINUX** is replaced by **none**.
6. On the Local-Client VM, open a terminal window, and then run a ping to the **LINUX** address object.
   ```
   ping 10.200.1.254
   ```
   You can see that the request timed out because the firewall policy has the destination set to **LINUX** and the action set to **DENY** locally on Local-FortiGate.

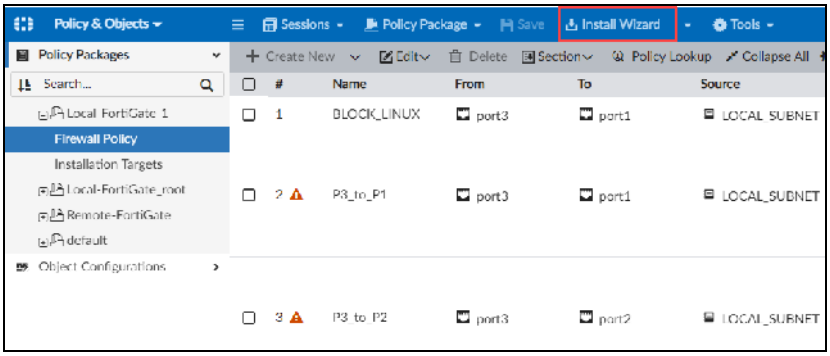
   The following image shows an example of Local-FortiGate:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

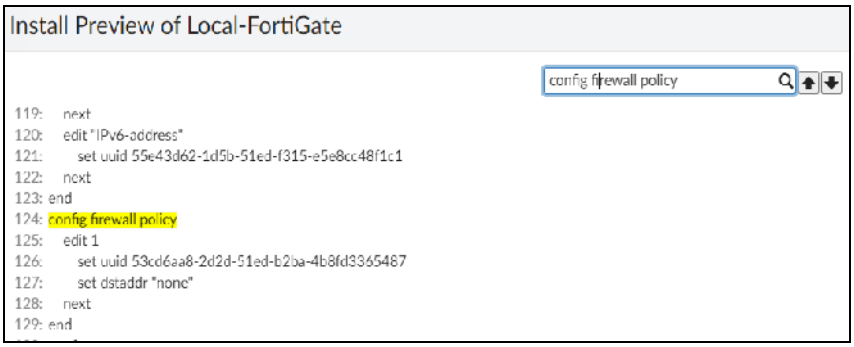
DO NOT REPRINT Brave-Dumps.com
© FORTINET

Name	Source	Destination	Schedule	Service	Action	NAT
port3 → port1 2						
BLOCK_LINUX	LOCAL_SUBNET	LINUX	always	ALL	DENY	
P3_to_P1	LOCAL_SUBNET	all	always	ALL	ACCEPT	Enabled
port3 → port2 1						
P3_to_P2	LOCAL_SUBNET	all	always	ALL	ACCEPT	Enabled

7. Return to the FortiManager GUI, and then click **Install Wizard**.



8. Make sure that the following settings are selected:
   - **Install Policy Package and Device Settings**
   - Policy Package: **Local-FortiGate-1**
9. Click **Next**.
10. Click **Next**.
11. Click **Install Preview**.
12. Using the search bar, search for the following:
    - config firewall policy
    - LINUX

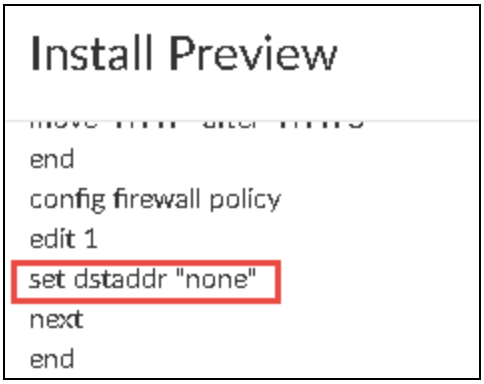


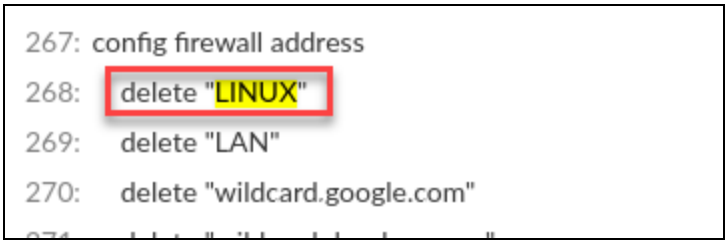
You can see that FortiManager is replacing the destination address of firewall policy **1** with **none**, and deleting the **LINUX** address object.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

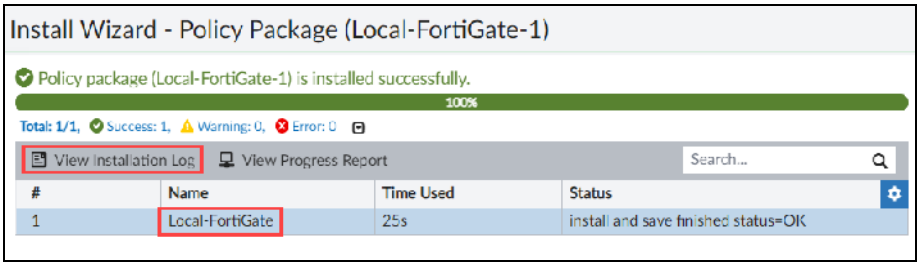
DO NOT REPRINT Brave-Dumps.com
© FORTINET

FortiManager also deletes any other unused objects. This is expected because when you install a policy package for the first time, FortiManager deletes all unused objects.





13. In the **Install Preview** window, click **Close**.
14. Click **Install**.
15. After the installation is successful, click **View Installation Log** to view the installation history.



16. Click **Close**.
17. Click **Finish**.
18. Return to the terminal window where you initiated the ping to **LINUX**.

    You will receive replies because there was a catch all policy below the **BLOCK_LINUX** policy. After installation, **LINUX** is replaced by **none**, and the **P3_to_P1** firewall policy starts processing the traffic.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

19. Close the terminal window.

To disable workflow mode on the CLI

1. Open a new PuTTY window, and then connect over SSH to the **FortiManager** saved session.
   Open a new window—do not close the FIT PuTTY session.
2. Log in with the username `admin` and password `password`.
3. Enter the following commands:

```
config system global
   set workspace-mode disabled
   y
end
```

All administrators are logged out of the FortiManager GUI so the changes can be saved. Therefore, before you disable workspace mode, inform all administrators logged in to the FortiManager GUI to save their work.

You can also disable workflow mode on the FortiManager GUI.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

Exercise 3: Creating a Common Policy for Multiple Devices

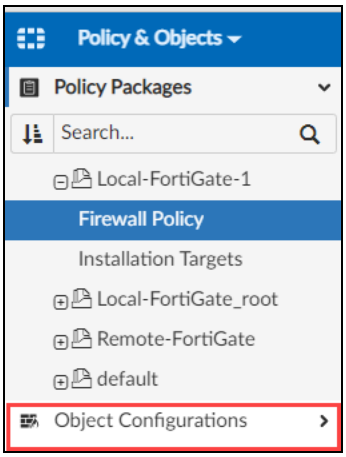
You will create a single policy package that can be shared by multiple devices, as opposed to having a policy package for each device, which is the current configuration. You will use the installation target setting in a firewall policy to target specific policies to specific FortiGate devices.

Create Dynamic Mappings for Address Objects

You will configure dynamic mappings for objects that are used to map a single logical object to a unique definition for each device.

To create dynamic mappings for address objects

1. Log in to the FortiManager GUI with the username `student` and password `fortinet`.
2. Click **My_ADOM**.
3. Click **Policy & Objects**.
4. Click **Object Configurations**.



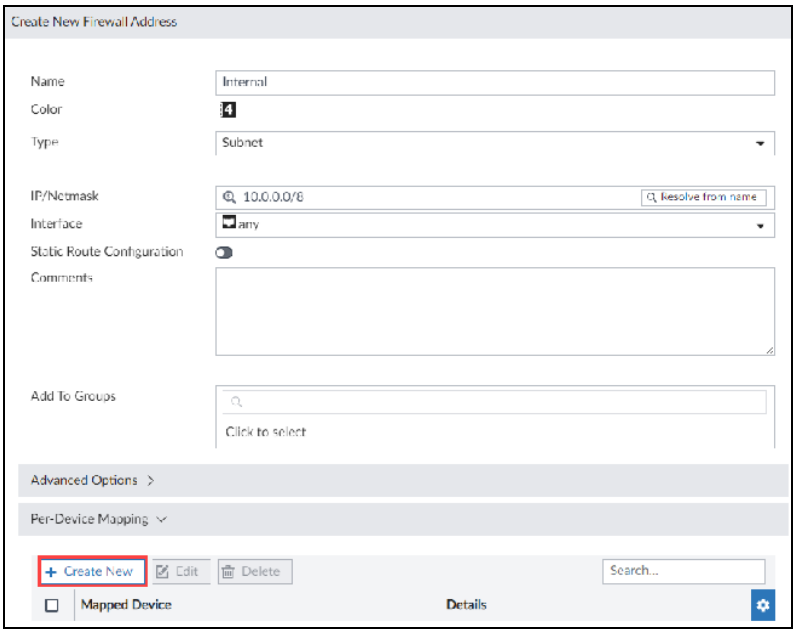
5. Click **Firewall Objects** > **Addresses**.
6. Click **Create New** > **Address**.
7. Configure the following settings:

Field	Value
Name	Internal
Type	Subnet
IP/Netmask	10.0.0.0/8

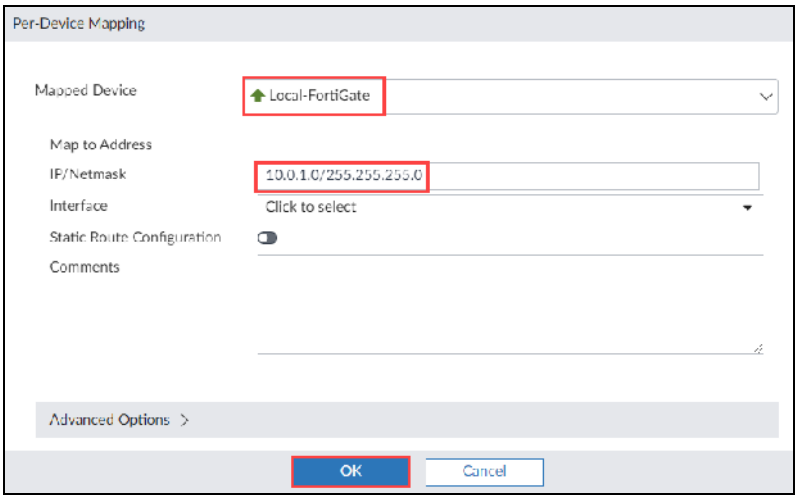
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

8. In the **Per-Device Mapping** section, configure the following settings:
   a. Expand **Per-Device Mapping**.
   b. Click **Create New**.



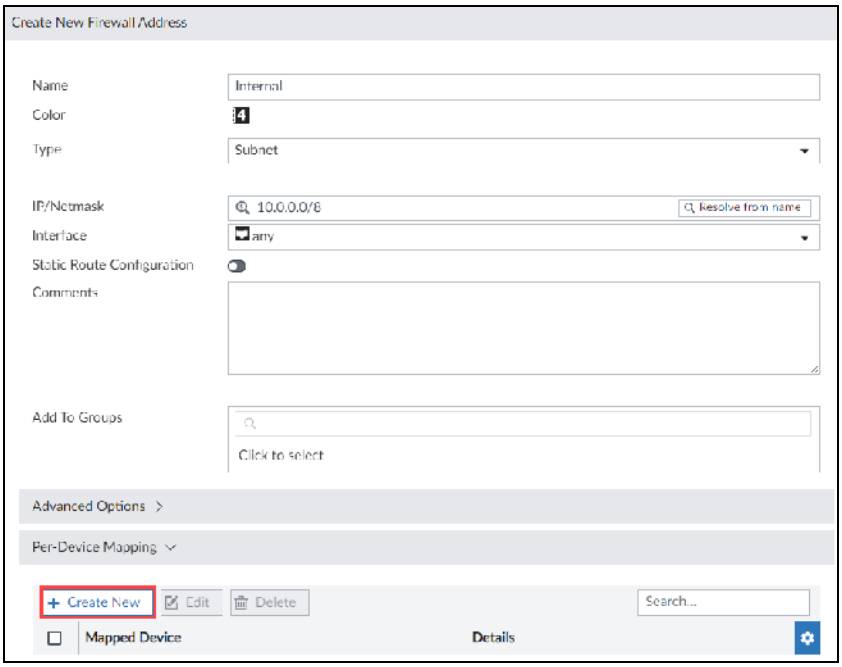
   c. In the **Mapped Device** field, select **Local-FortiGate**.
   d. In the **IP/NetMask** field, type `10.0.1.0/24`.
   e. Click **OK**.



   f. Click **Create New** again.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

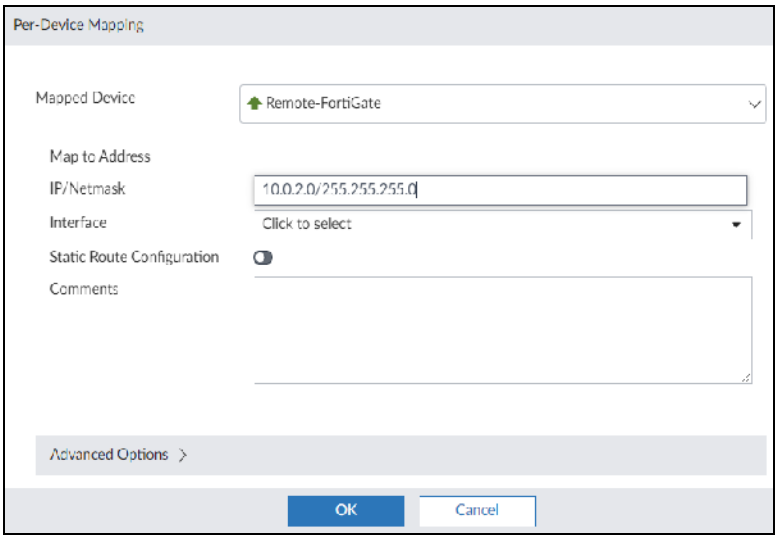
DO NOT REPRINT Brave-Dumps.com
© FORTINET



g. In the **Mapped Device** field, select **Remote-FortiGate**.

h. In the **IP/NetMask** field, type `10.0.2.0/24`.

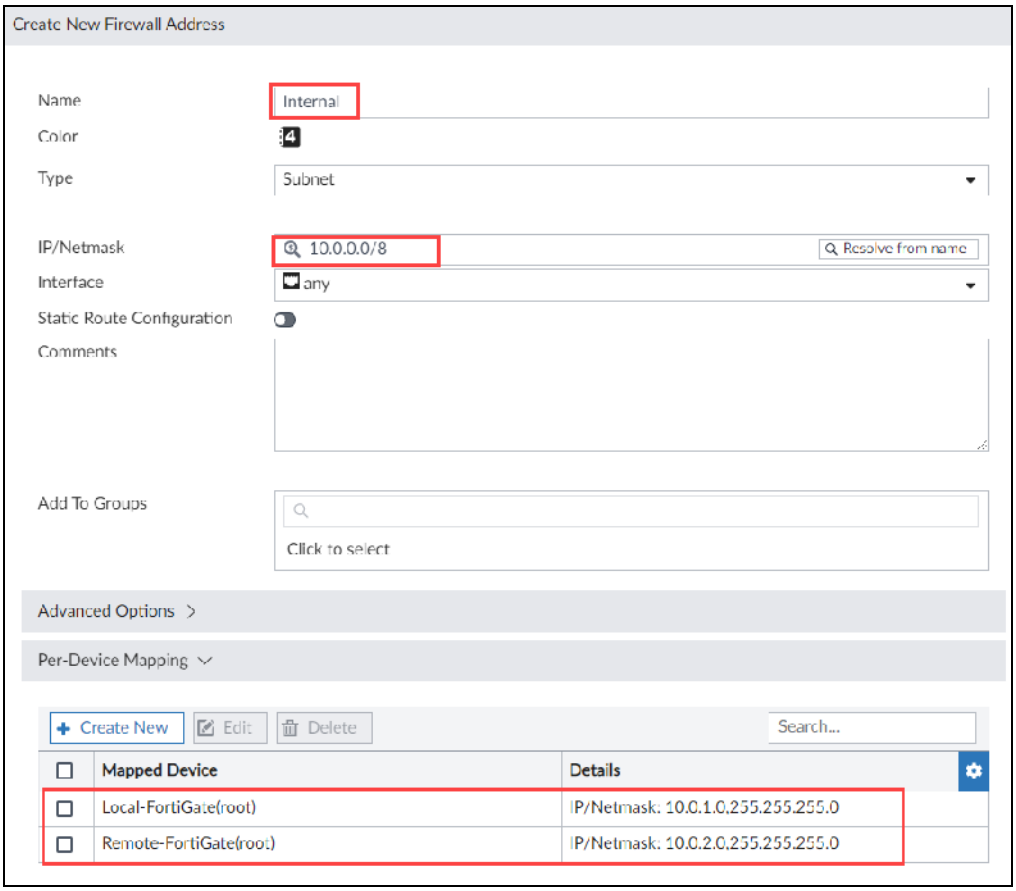
i. Click **OK**.



Your configuration should look like the following example:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com



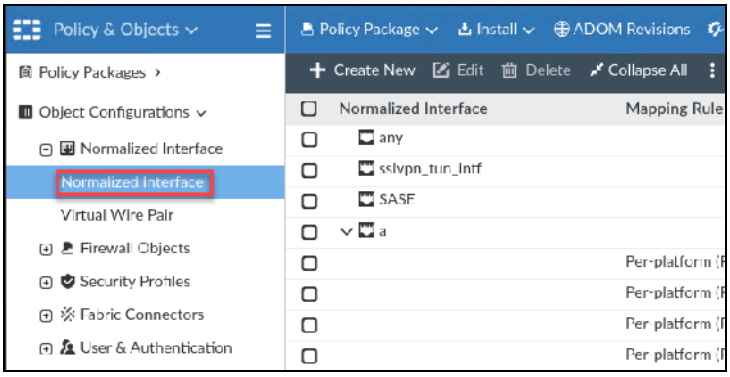
9. In the **Change Note** field, type some text.
10. Click **OK**.

Create Dynamic Mappings for Interfaces and Device Zones

You will create dynamic mappings for interfaces and device zones.

To create dynamic mappings for interfaces

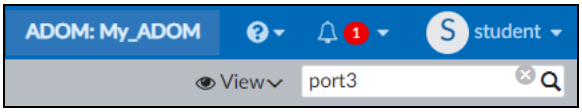
1. Continuing on the FortiManager GUI, click **Normalized Interface**.



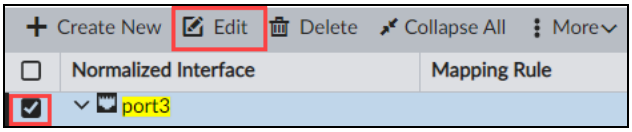
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

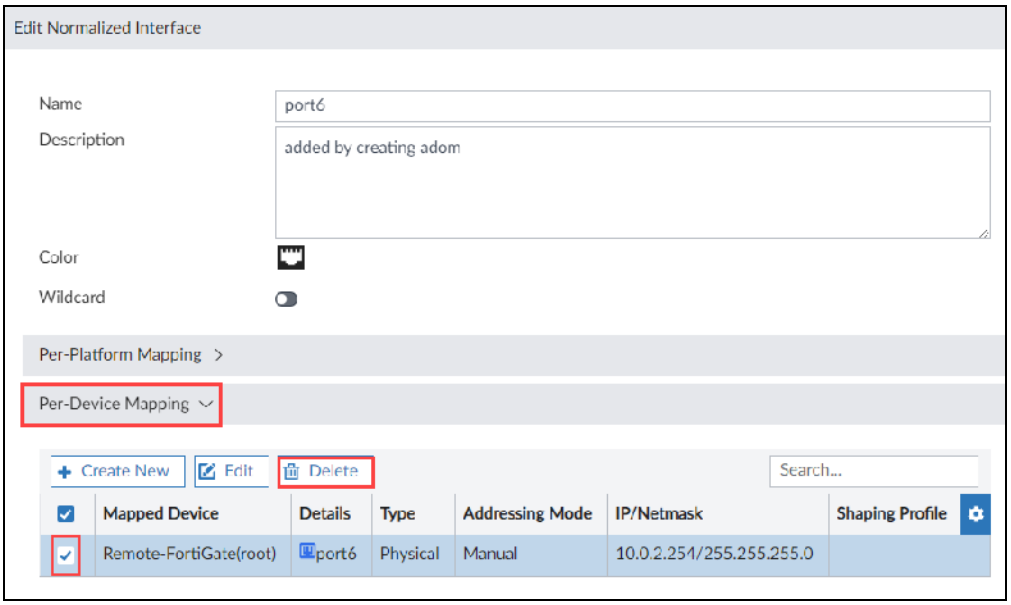
2. In the search field, type `port3`.



3. Right-click **port3**, and then select **Edit**.



4. In the **Per-Device Mapping** section, in the **Mapped Device** column, select **Local-FortiGate(root)**, and then click **Delete**.
5. In the **Change Note** field, type some text.
6. Click **OK**.
7. In the search field, type `port6`.
8. Right-click **port6**, and then select **Edit**.
9. In the **Per-Device Mapping** section, in the **Mapped Device** column, select **Remote-FortiGate(root)**, and then click **Delete**.



10. In the **Change Note** field, type some text.
11. Click **OK**.

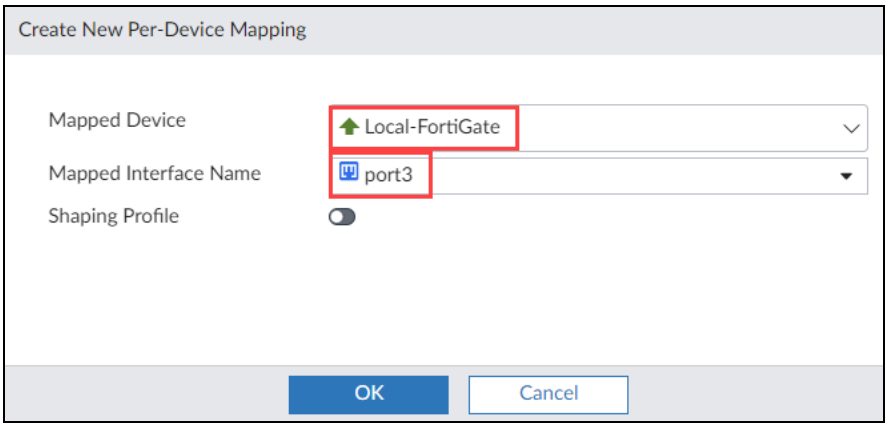
You must delete the **Per-Device Mapping**. This is because interfaces were dynamically mapped when the devices were added to FortiManager. After deleting the previous mapping, you can then add these interfaces to map to newly created normalized interfaces.

12. Click **Create New**.
13. In the **Name** field, type `Inside`.
14. In the **Per-Device Mapping** section, click **Create New**, and then configure the following settings:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

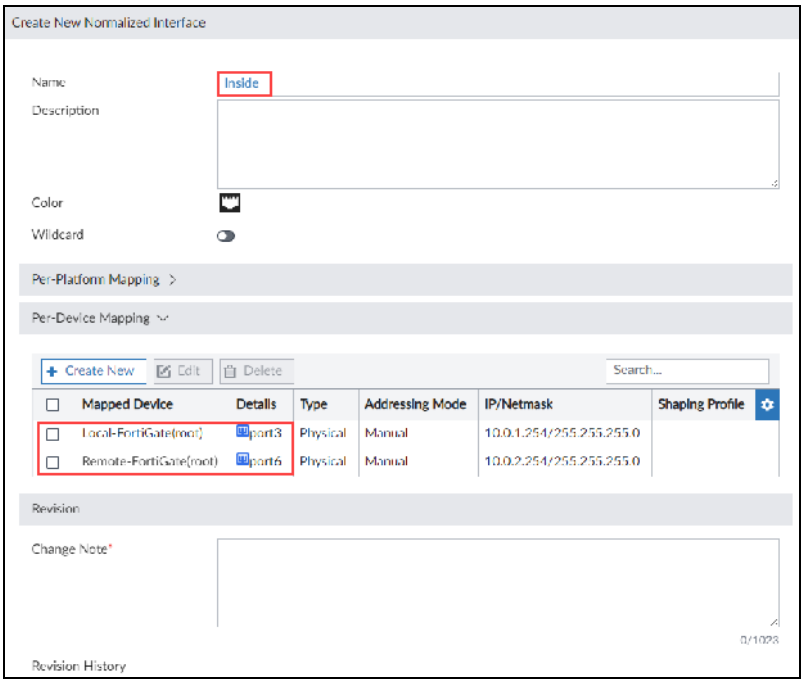
DO NOT REPRINT
© FORTINET
Brave-Dumps.com

a. In the **Mapped Device** field, select **Local-FortiGate**.
b. In the **Mapped Interface Name** field, select **port3**.
c. Click **OK**.



d. Click **Create New** again.
e. In the **Mapped Device** field, select **Remote-FortiGate**.
f. In the **Mapped Interface Name** field, select **port6**.
g. Click **OK**.

Your configuration should look like the following example:



15. In the **Change Note** field, type some text.
16. Click **OK**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

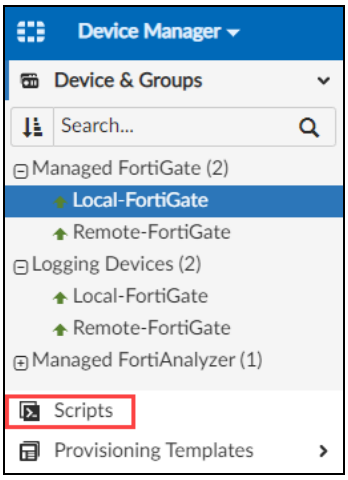
DO NOT REPRINT Brave-Dumps.com
© FORTINET

Import and Install a CLI Script to Delete Policies

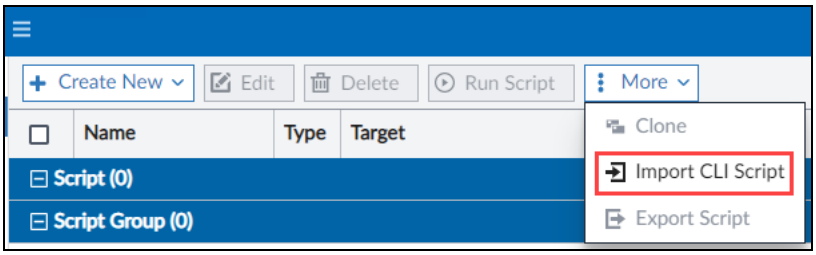
You will import and install a script on the policy package to delete policies.

To import and install a CLI script

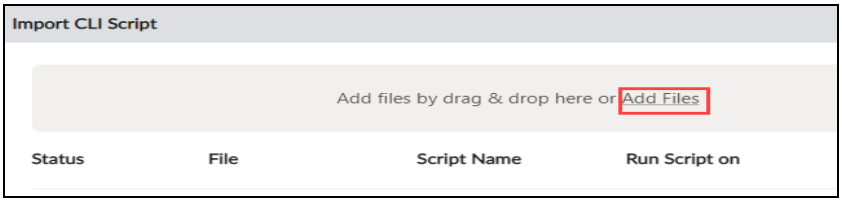
1. Continuing on the FortiManager GUI, click **Policy & Objects** > **Device Manager**.
2. Click **Scripts**.



3. Click **Import CLI Script**.



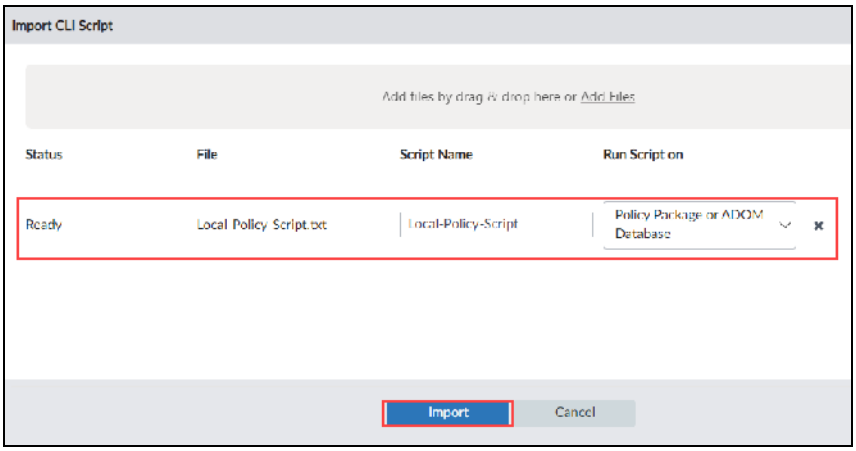
4. Click **Add Files**.



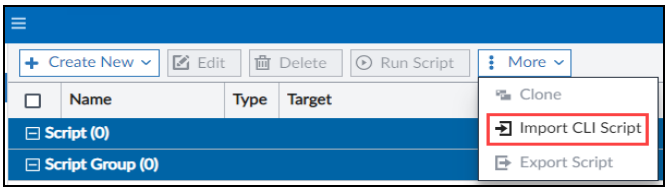
5. Click **Desktop** > **Resources** > **FortiManager** > **Policy**, and then select `Local-Policy-Script`.
6. Click **Open**, and then in the **Run Script on** field, select **Policy Package or ADOM Database**.
7. Click **Import**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET



8. Click **Close**.
9. Click **Import CLI Script** again.



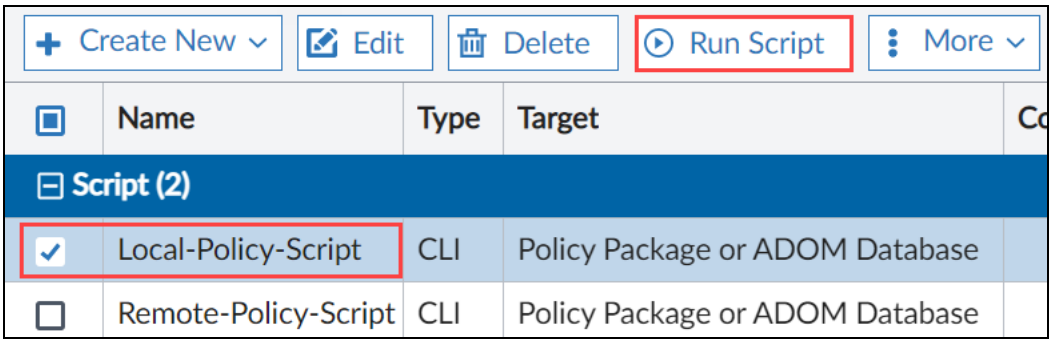
10. Click **Add Files**.
11. Click **Desktop** > **Resources** > **FortiManager** > **Policy**, and then select `Remote-Policy-Script`.
12. Click **Open**, and then in the **Run Script on** field, select **Policy Package or ADOM Database**.
13. Click **Import**.
14. Click **Close**.

Run and Install the Scripts

Because the scripts are targeting the policy package, you will first run the scripts against the policy package, and then install the scripts on the managed devices.

To run the scripts

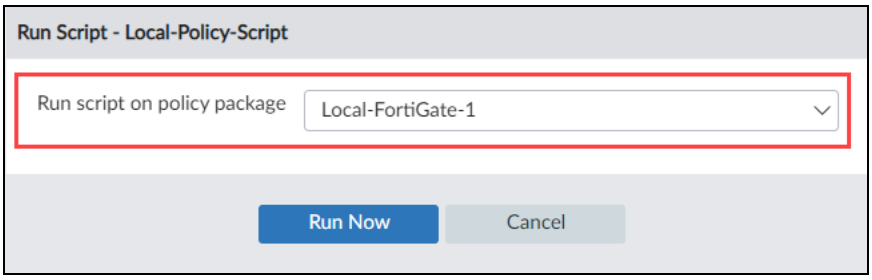
1. Continuing on the FortiManager GUI, select the **Local-Policy-Script** checkbox, and then click **Run Script**.



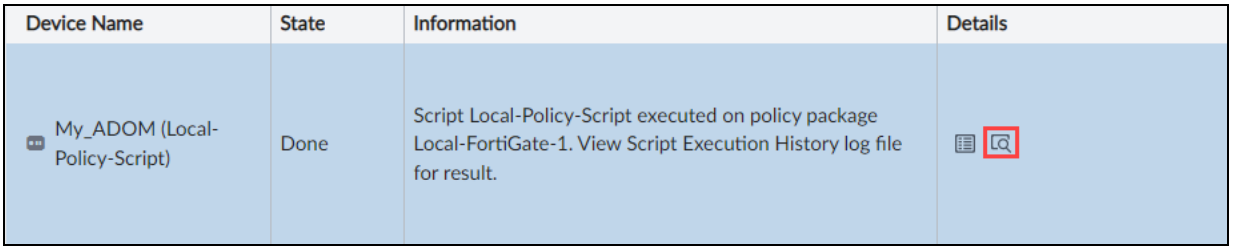
2. In the **Run script on policy package** field, select **Local-FortiGate-1**.

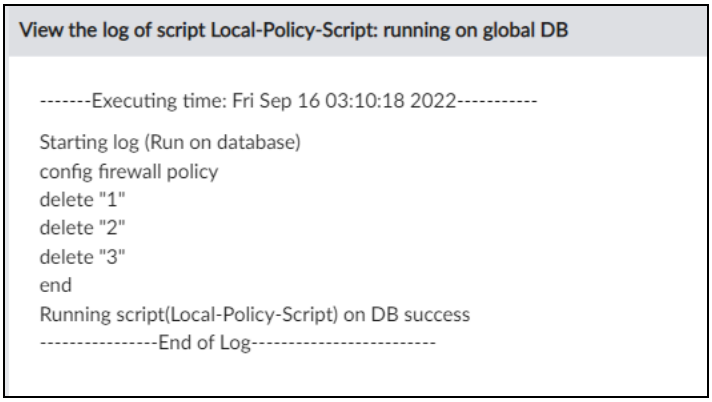
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET



3. Click **Run Now**.
4. Click **View Details**, and then click the **View Script Execution History** icon.
5. Scroll to the bottom of the script execution window to check that the script ran successfully on the policy package.



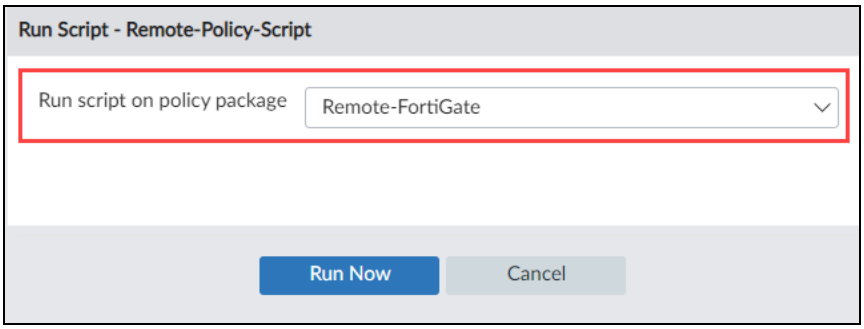


If needed, you can also view the script execution history later in the **Configuration and Installation Status** widget or in the **Task Monitor**.

6. Click **Close**.
7. Click **Close**.
8. Clear the **Local-Policy-Script** checkbox, select the **Remote-Policy-Script** checkbox, and then click **Run Script**.
9. In the **Run script on policy package** field, select **Remote-FortiGate**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

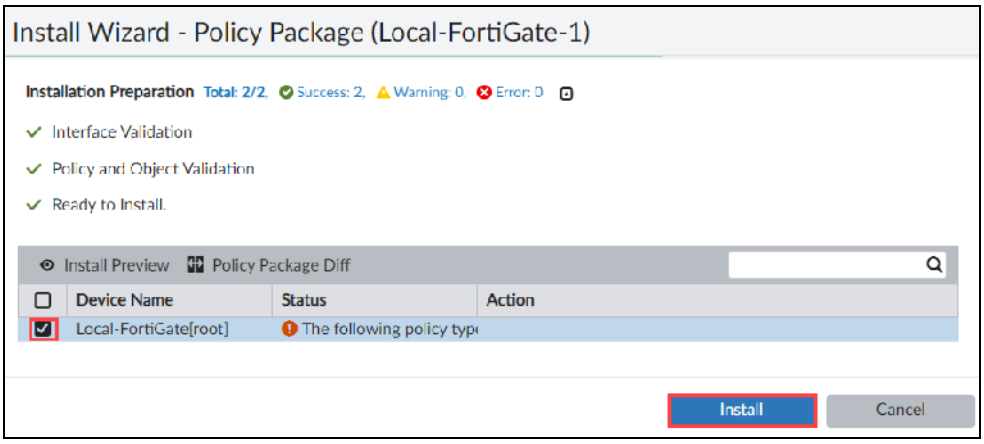
DO NOT REPRINT Brave-Dumps.com
© FORTINET



10. Click **Run Now**.
11. Click **Close**.

To install configuration

1. Continuing on the FortiManager GUI, click **Device & Groups** > **Managed FortiGate**.
2. Click **Install**, and then click **Install Wizard**.
3. Select **Install Policy Package & Device Settings**, and then in the **Policy Package** field, select **Local-FortiGate-1**.
4. Click **Next**.
5. Make sure that **Local-FortiGate** is selected, and then click **Next**.
6. Select **Local-FortiGate**, and then click **Install**.



7. Click **Finish**.
8. Click **Install**, and then click **Install Wizard**.
9. Select **Install Policy Package & Device Settings**, and then in the **Policy Package** field, select **Remote-FortiGate**.
10. Click **Next**.
11. Make sure that **Remote-FortiGate** is selected, and then click **Next**.
12. Select **Remote-FortiGate**, and then click **Install**.
13. Click **Finish**.

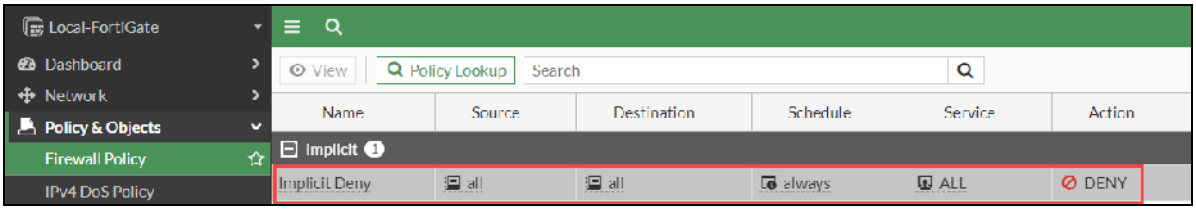
To view configuration changes locally on FortiGate

1. Log in to the Local-FortiGate GUI with the username `admin` and password `password`.
2. Click **Login Read-Only**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

3. Click **Policy & Objects** > **Firewall Policy**.
   You should see only the **Implicit Deny** policy.



4. Log out of the Local-FortiGate GUI.
5. Log in to the Remote-FortiGate GUI with the username `admin` and password `password`.
6. Click **Login read-only**.
7. Click **Policy & Objects** > **Firewall Policy**.
   You should see only the **Implicit Deny** policy.
8. Log out of the Remote-FortiGate GUI.

Stop and think!

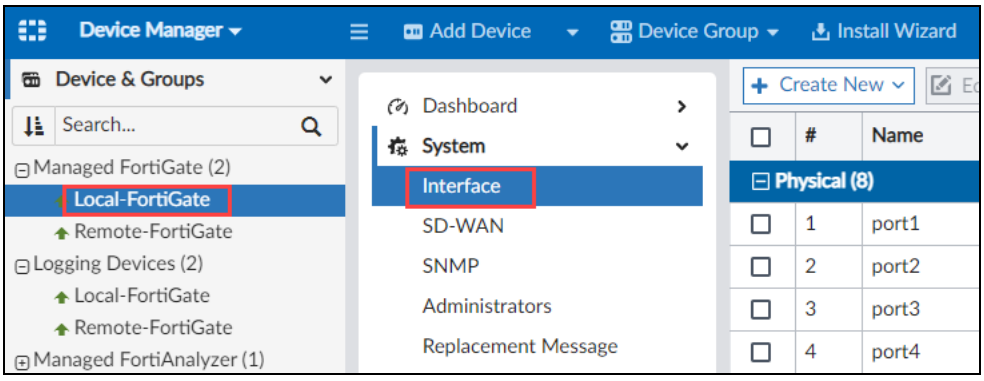
Why did you delete the policies on the FortiGate devices?

This is because external ports in the configuration were already being used by the policies. You cannot add interfaces to the zone that are already being used by the policies on the FortiGate.

You must update the policy packages on the devices before you add interfaces to the device zone.

To create dynamic mappings for device zones

1. Continuing on the FortiManager GUI, click **Device & Groups** > **Managed FortiGate**.
2. Click **Local-FortiGate**, and then click **System** > **Interface**.



When you create a device zone, map the zone to a physical interface. To use the zone in a policy, you must also map the zone to a normalized interface.

3. Click **Create New** > **Device Zone**.
4. In the **Zone Name** field, type `Outside`.
5. Configure the following:

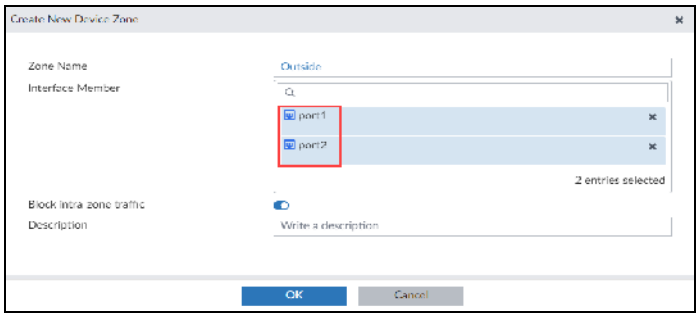
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

a. In the **Interface Member** field, select **port1** and **port2**.

b. Enable **Block intra-zone traffic**.

c. Click **OK**.

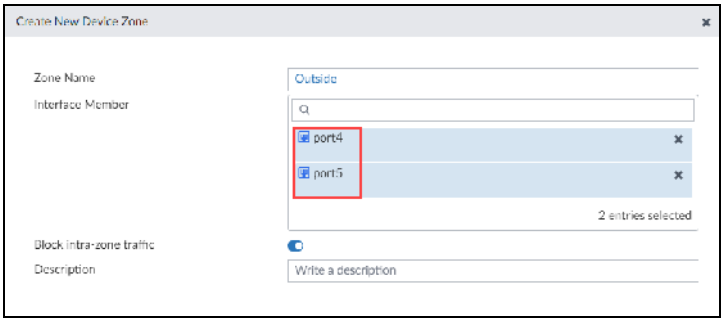


6. Click **Remote-FortiGate**.
7. Click **System** > **Interface**.
8. Click **Create New** > **Device Zone** again.
9. In the **Zone Name** field, type `Outside`.
10. Configure the following:

a. In the **Interface Member** field, select **port4** and **port5**.

b. Enable **Block intra-zone traffic**.

c. Click **OK**.



11. Click **Device Manager** > **Policy & Objects**.
12. Click **Object Configurations** and then click **Normalized Interface**.
13. Click **Create New**.
14. In the **Name** field, type `Outside`.
15. In the **Per-Device Mapping** section, click **Create New** and then configure the following settings:

a. In the **Mapped Device** field, select **Local-FortiGate**.

b. In the **Mapped Interface Name** field, select **Outside**.

c. Click **OK**.

16. Click **Create New** again.
17. In the **Per-Device Mapping** section, configure the following settings:

a. In the **Mapped Device** field, select **Remote-FortiGate**.

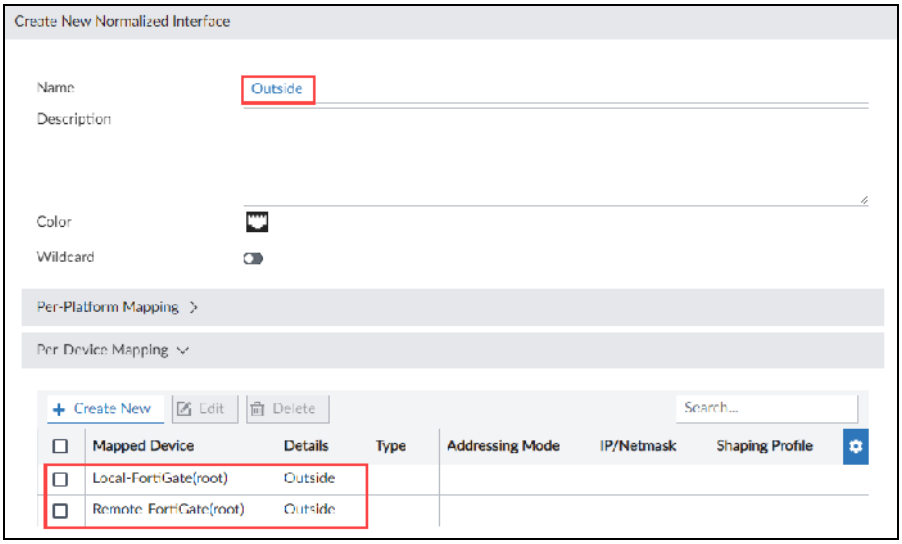
b. In the **Mapped Interface Name** field, select **Outside**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

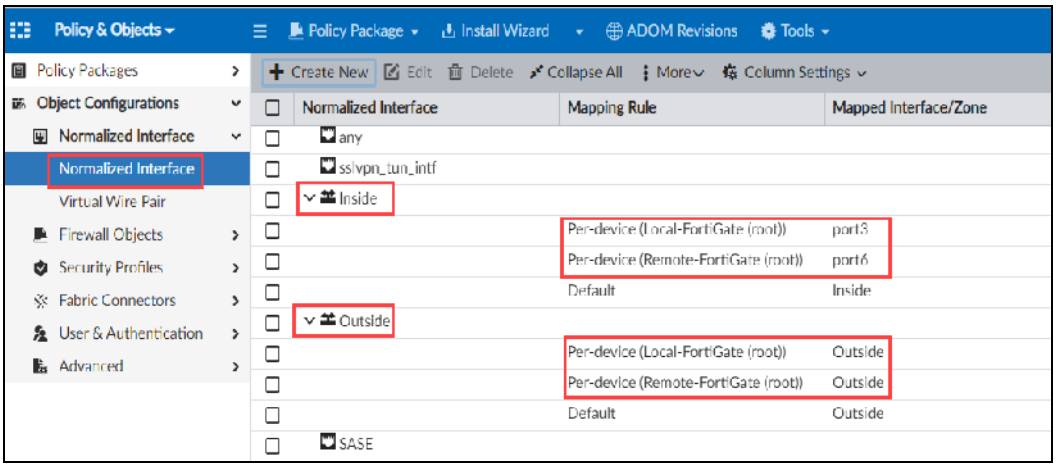
c. Click **OK**.

Your configuration should look like the following example:



18. In the **Change Note** field, add any notes.
19. Click **OK**.

You have now created a dynamic interface and device zones.



Create a Common Policy Package, an Installation Target, and Use Install On

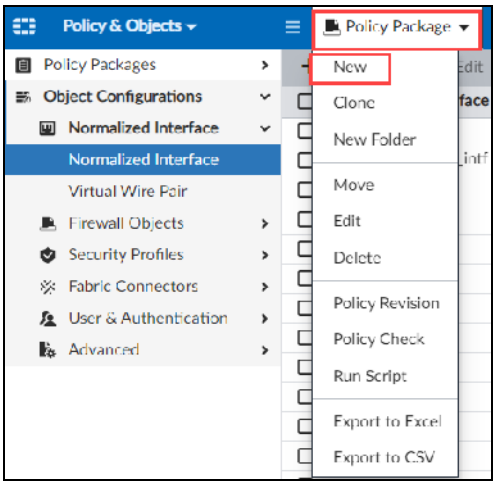
You can use FortiManager to target a common policy package to multiple devices. When you configure an installation target, by default, all policies in the policy package are targeted to all selected FortiGate devices. You can further restrict the policies in the policy package to be targeted to specific FortiGate devices by using the **Install On** feature, which targets specific policies in the policy package to selected FortiGate devices in the **Install On** column.

To create a common policy package

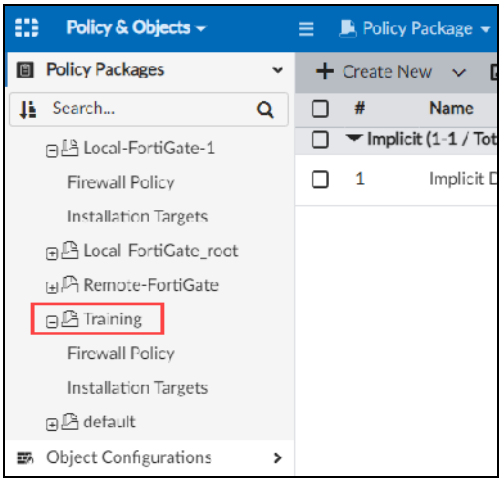
1. Continuing on the FortiManager GUI, click **Policy Package** > **New**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com



2. Name the new policy package `Training`, and then click **OK**.

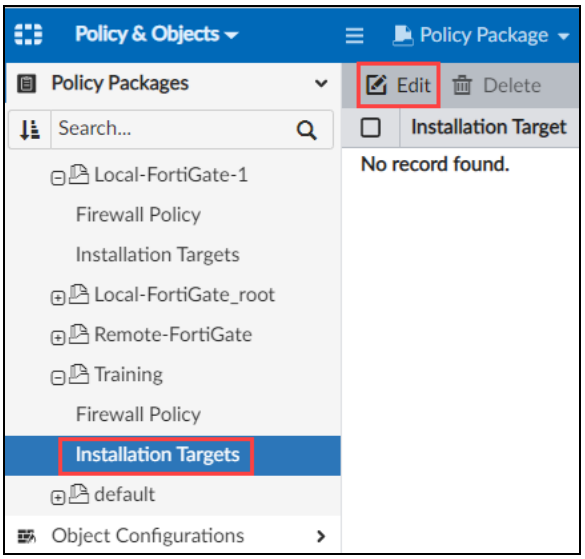


To configure an installation target and use Install On

1. Continuing on the FortiManager GUI, click **Installation Targets** for the **Training** policy package.
2. Click **Edit**.

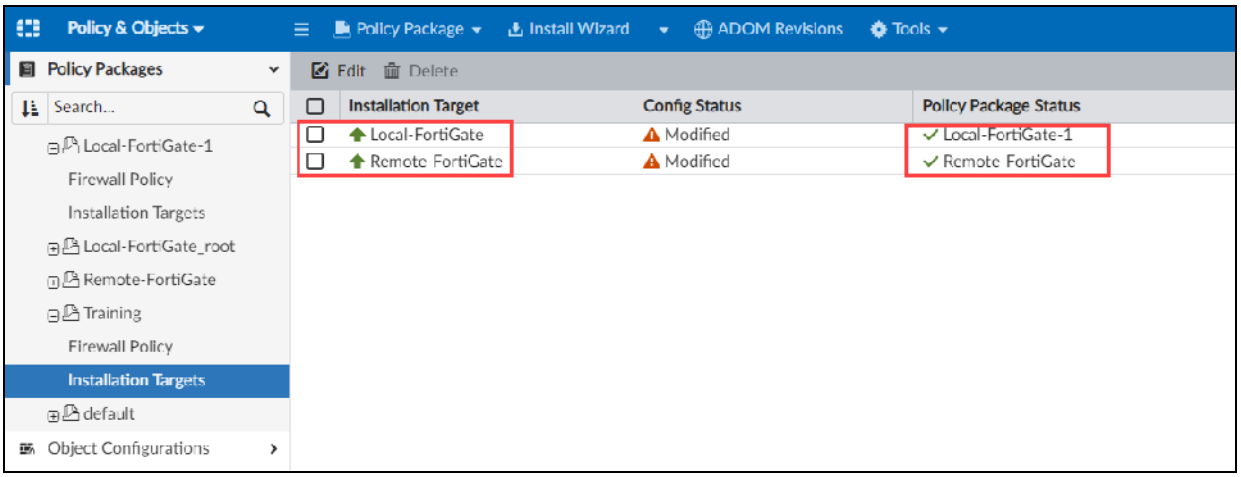
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET



3. Select **Local-FortiGate** and **Remote-FortiGate**, and then add them to the **Selected Entries** section.
4. Click **OK**.

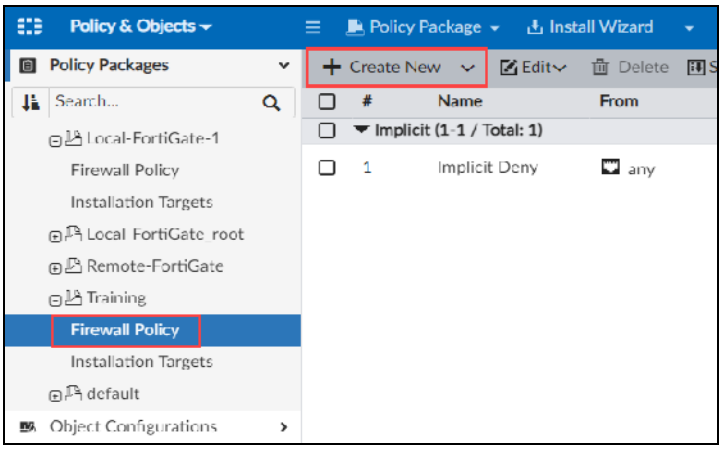
   The **Policy Package Status** column shows the name of the currently active policy packages for these FortiGate devices.



5. Click **Firewall Policy** for the **Training** policy package.
6. Click **Create New**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

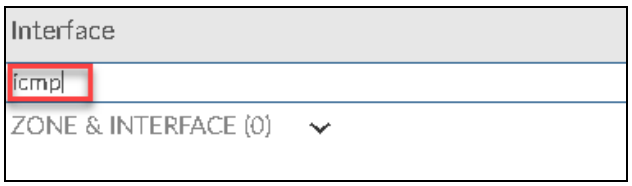


7. Configure the following settings:

Field	Value
Name	For_Local
Incoming Interface	Inside
Outgoing Interface	Outside
IPv4 Source Address	Internal
IPv4 Destination Address	all
Service	HTTP, HTTPS, ALL_ICMP
Schedule	always
Action	Accept
NAT	Select the checkbox.
Change Note	New firewall policy

8. Click **OK**.
9. Click **Create New** to create a second policy, and then configure the following settings:

When you create the second policy, if you do not see all of the interfaces, make sure that you clear the interface filter when you select the interfaces.

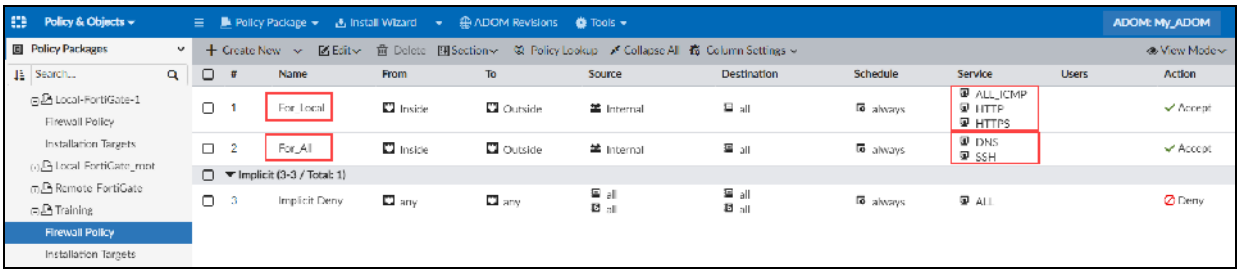


Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

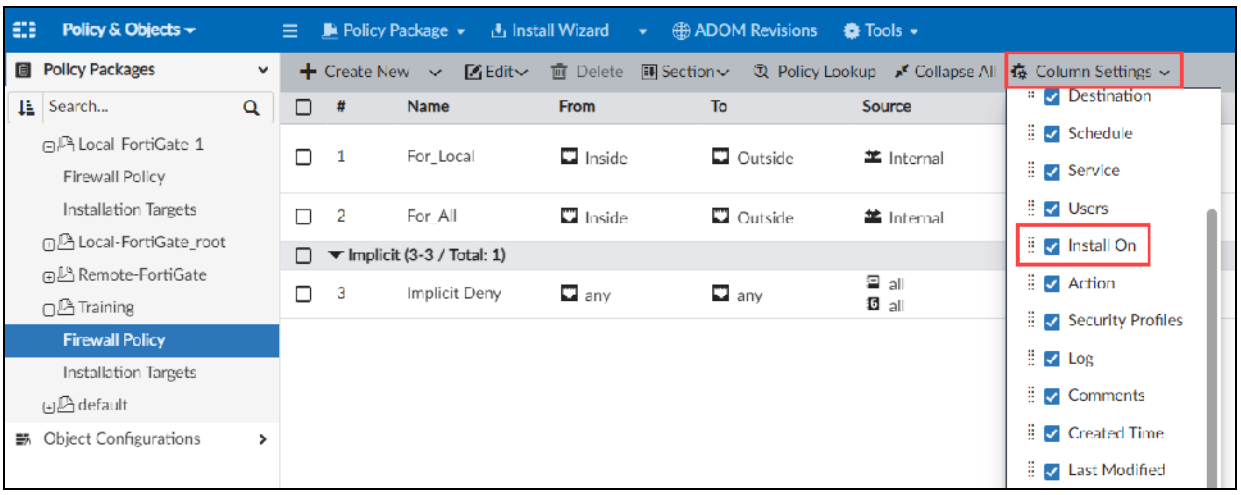
DO NOT REPRINT Brave-Dumps.com
© FORTINET

Field	Value
Name	For_All
Incoming Interface	Inside
Outgoing Interface	Outside
IPv4 Source Address	Internal
IPv4 Destination Address	all
Service	SSH, DNS
Schedule	always
Action	Accept
NAT	Select the checkbox.
Change Note	Policy 2

10. Click **OK**.
Your configuration should look like the following example:



11. Click the column settings icon, and then make sure that the **Install On** checkbox is selected. You need to scroll to the right to find **Install On** column.

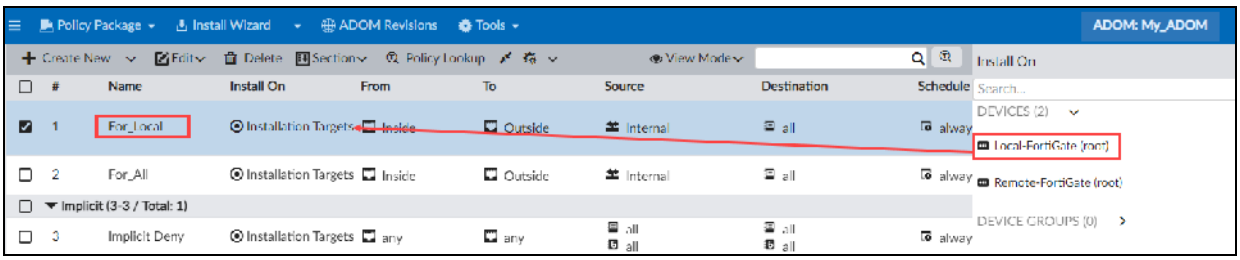


Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

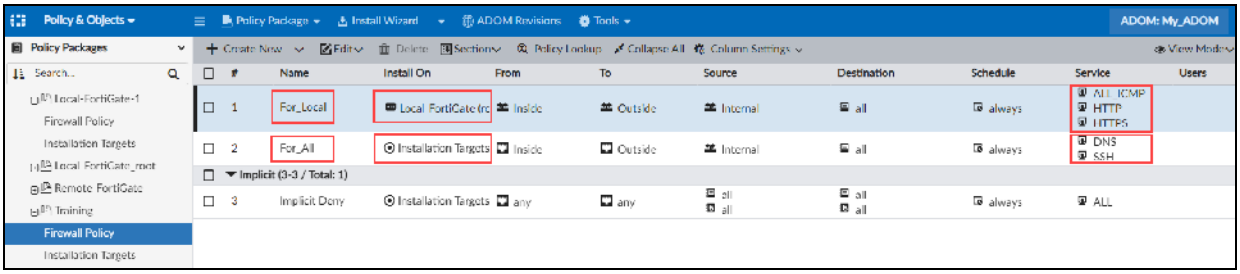
DO NOT REPRINT Brave-Dumps.com
© FORTINET

Once the **Install On** column is added, you can drag the column to where you want it positioned in the column list.

12. For the **For_Local** policy, click **Installation Targets**.
13. Select **Local-FortiGate**.
14. Click **OK**.

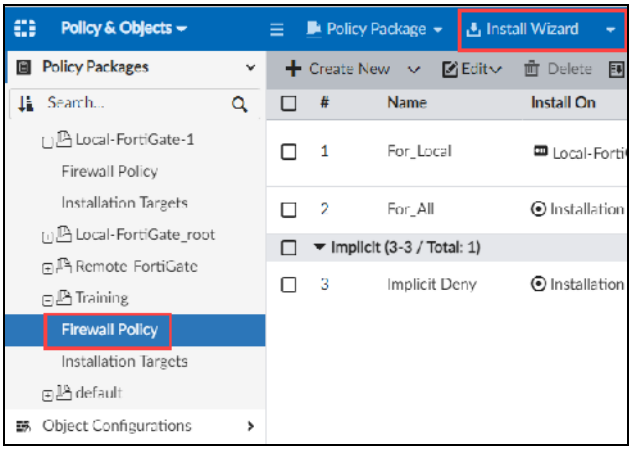


Your policies should look similar to the following example:



To install a policy package

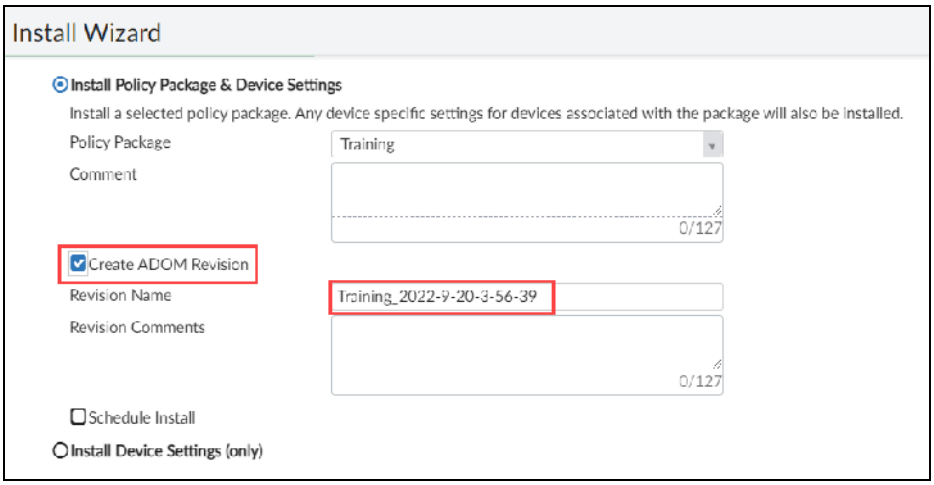
1. Return to **Policy Packages**, click **Training** > **Firewall Policy**, and then click **Install Wizard**.



2. Make sure the following settings are selected:
   - **Install Policy Package & Device Settings**
   - Policy Package: **Training**
3. Select the **Create ADOM Revision** checkbox, and then leave the **Revision Name** field at the default value.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

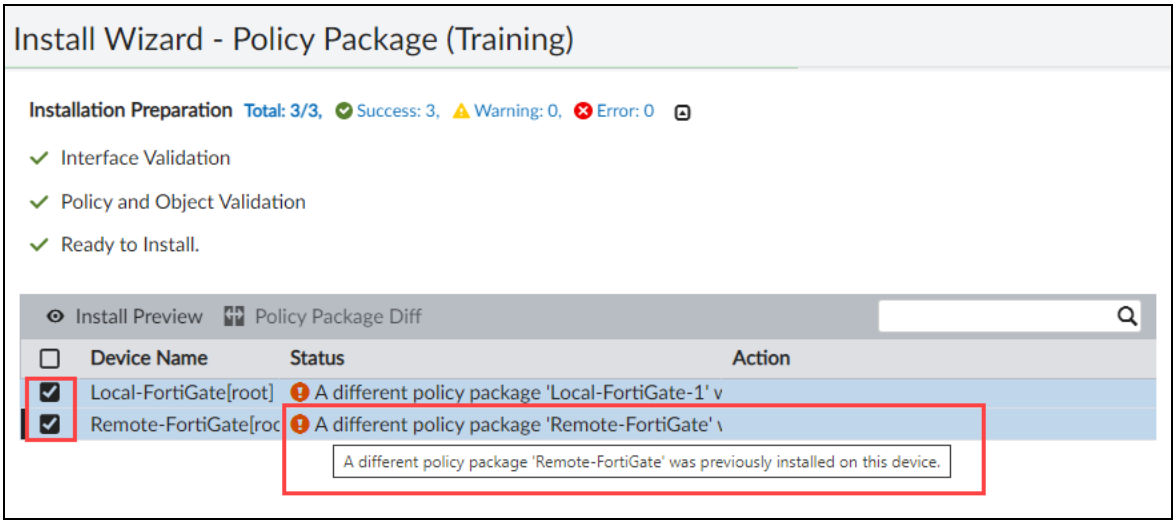
DO NOT REPRINT Brave-Dumps.com
© FORTINET



4. Click **Next**.
5. Select both of the FortiGate devices.
6. Click **Next**.

   If you hover over the **Status** column of the FortiGate devices, the name of the previous policy package is displayed.

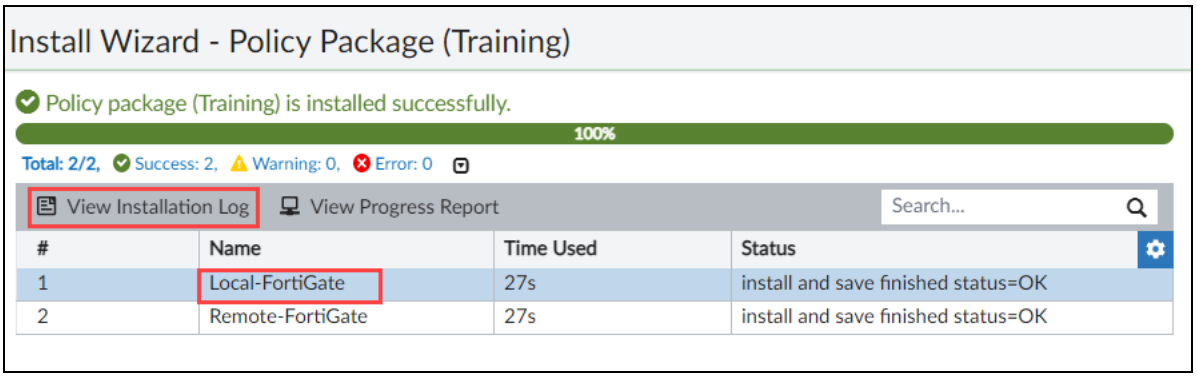
   Optionally, you can preview the changes before you install them.



7. Make sure that both of the FortiGate devices are selected, and then click **Install**.
8. After the installation is successful, you can click **View Installation Log** to see the installation history for each FortiGate.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

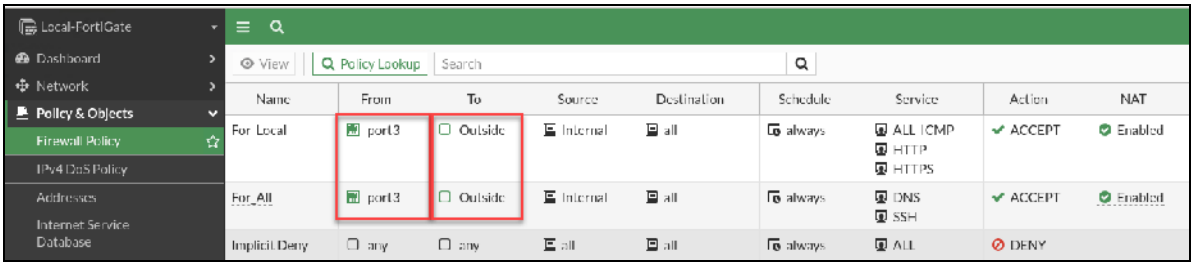
DO NOT REPRINT
© FORTINET
Brave-Dumps.com



9. In the **Install Log** window, click **Close**.
10. Click **Finish**.

To view configuration changes locally on FortiGate

1. Log in to the Local-FortiGate GUI with the username `admin` and password `password`.
2. Click **Login Read-Only**.
3. Click **Policy & Objects** > **Firewall Policy**, and then select the **By Sequence** view.
   You should see the following:
   - There are two firewall policies that are based on the **Training** policy package.
   - The **Inside** interface is translated to **port3** locally on FortiGate and the **Outside** zone is created locally on FortiGate, according to the dynamic mapping of interfaces and zones.



4. Click **Addresses**.
   Internal is translated to `10.0.1.0/24`, according to the dynamic mapping of address objects.
5. Click **Network** > **Interfaces**.
   An **Outside** zone is created with port1 and port2 interfaces, according to the dynamic mapping of interfaces and zones.
6. Log out of the Local-FortiGate GUI.
7. Log in to the Remote-FortiGate GUI with the username `admin` and password `password`.
8. Click **Login read-only**.
9. Click **Policy & Objects** > **Firewall Policy**.
10. You should see the following:
    - There is only one firewall policy that is based on the **Training** policy package **Install On** targets.
    - The **Inside** interface is translated to **port6** locally on FortiGate and the **Outside** zone is created locally on FortiGate, according to the dynamic mapping of interfaces and zones.

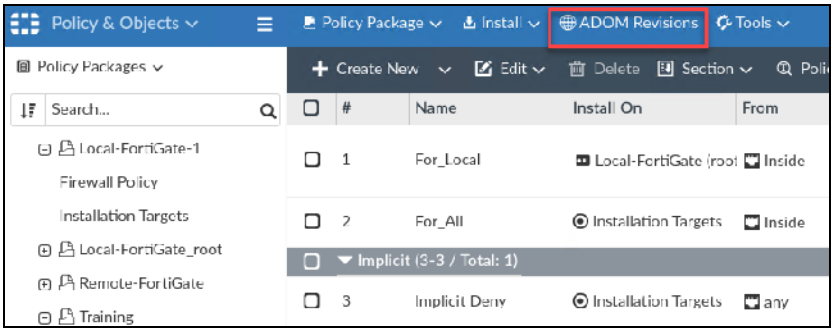
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

Optionally, you can check the interface and zone under **Network**, and the **Internal** address object under **Addresses**.

To review ADOM revisions

1. Return to the FortiManager GUI, and then click **ADOM Revisions**.



2. Right-click the **Training** revision, and then click **Lock Revision**.
3. Right-click **Initial revision**, and then click **Delete**.
4. Click **OK**.
5. Click **Close**.

You can use this revision to revert changes made to your policy packages and objects in your ADOM. Remember, this does not revert settings at the Device Manager level.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

Exercise 4: Running a FortiAnalyzer Report

When FortiManager manages a FortiAnalyzer, all configuration and data is stored on the FortiAnalyzer to support the following FortiAnalyzer features:

- FortiView
- Log view
- Incidents and events
- Reports

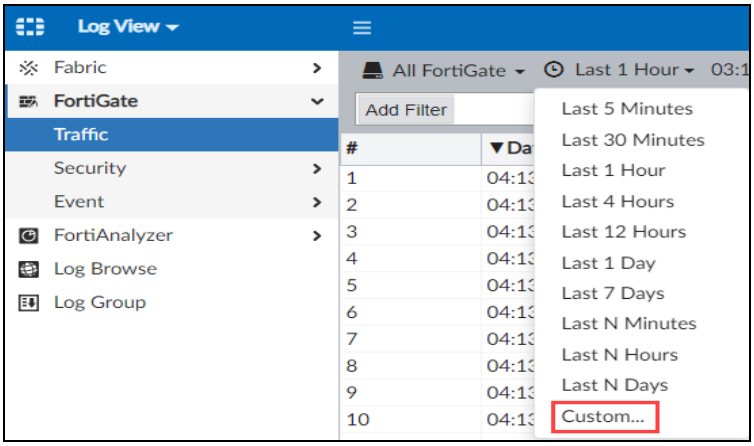
You will create a single FortiAnalyzer report using FortiManager.

View Logs

When a FortiManager manages a FortiAnalyzer, you can view the logs that the FortiAnalyzer receives. Now that FortiAnalyzer is added on FortiManager, and both FortiGate devices are configured to send logs to FortiAnalyzer, you will view the logs.

To view logs

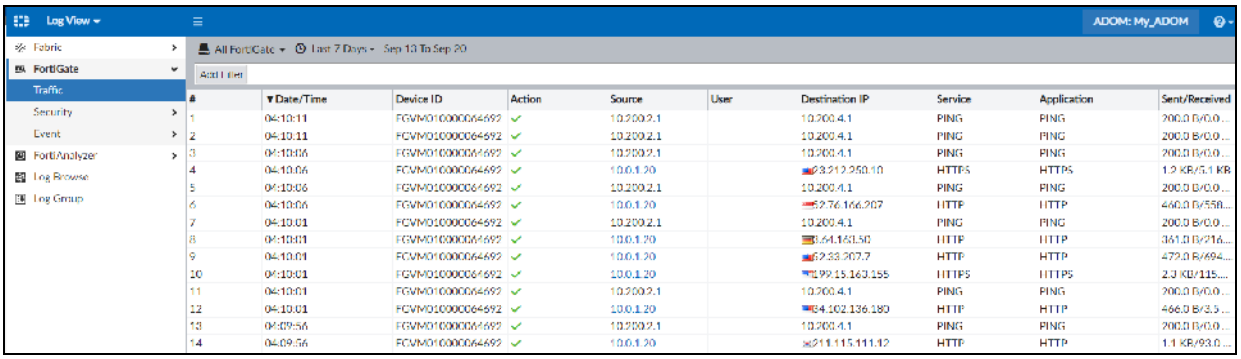
1. Log in to the FortiManager GUI with the username `student` and password `fortinet`.
2. Click **My_ADOM**.
3. Click **Log View**.
4. Click the time period drop-down list, and then select **Custom**.



5. Select **Any time**, and then click **OK**.
   You should see the various traffic logs generated by the FortiGate.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

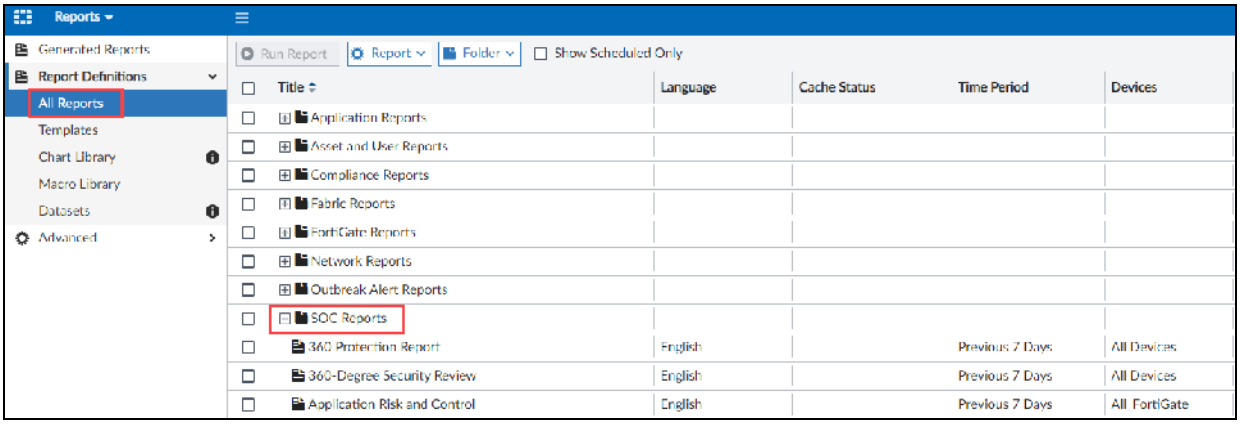


Run a FortiAnalyzer Report

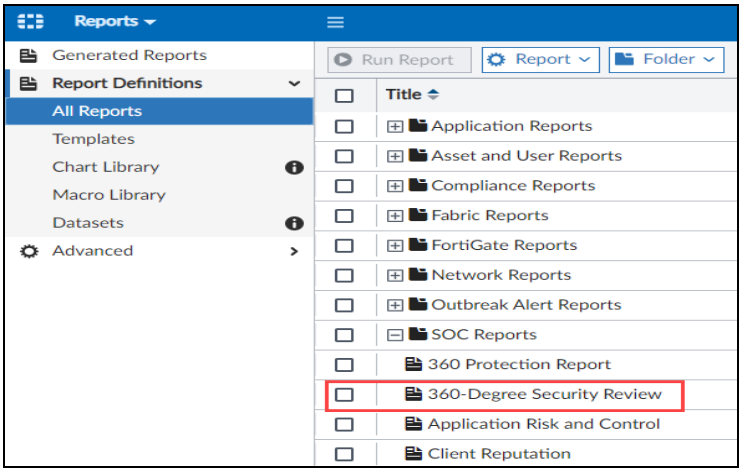
You will run a FortiAnalyzer report from FortiManager.

To run a FortiAnalyzer report

1. Continuing on the FortiManager GUI, click **Log View** > **Reports**.
2. Click **All Reports**, and then expand **SOC Reports**.



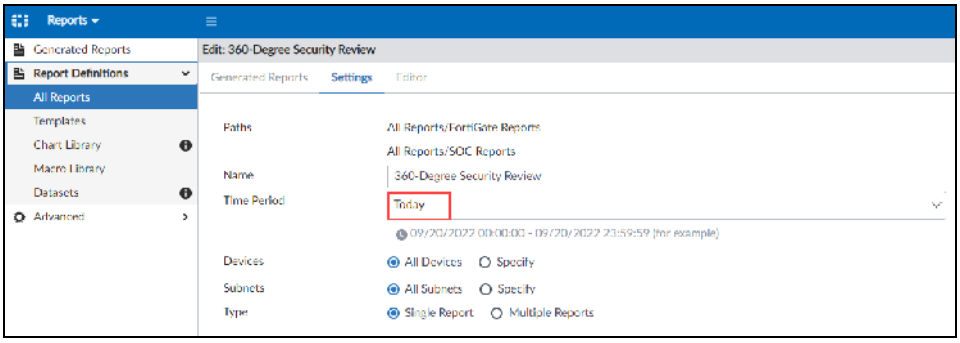
3. Double-click the report at **360-Degree Security Review**.



Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

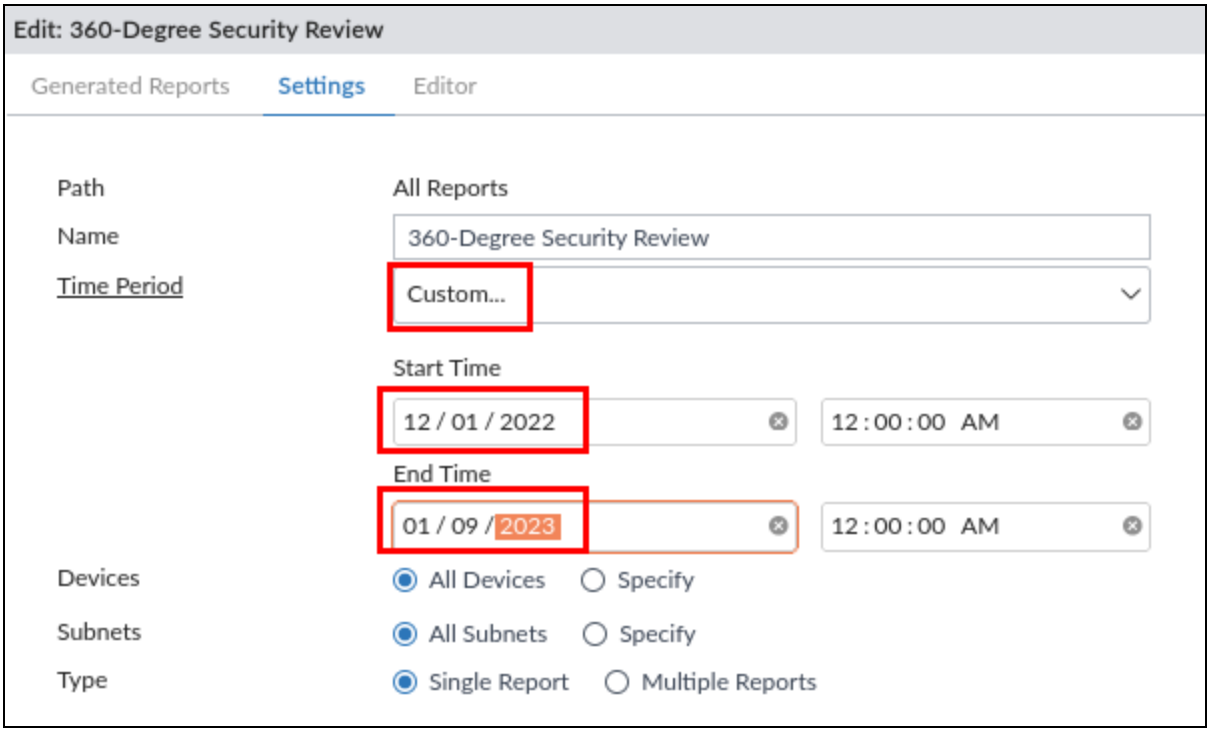
DO NOT REPRINT Brave-Dumps.com
© FORTINET

4. Depending on the class format, do one of the following:
   - Instructor-led class instructions: Click the **Settings** tab, and then in the **Time Period** field, select **Today**.



If you did not do the previous labs the same day you are doing this one, adjust the **Time Period** accordingly to avoid a report with little or no data.

   - Self-paced class instructions: Click the **Settings** tab, in the **Time Period** field, select **Custom**, and then specify the time range shown in the following image:

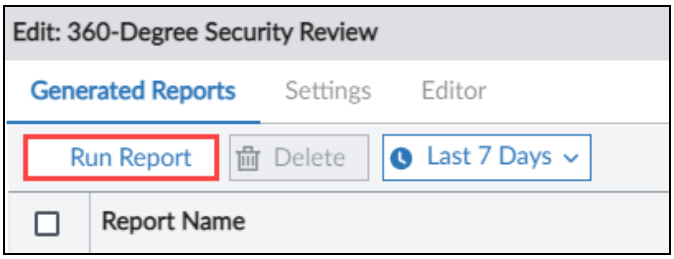


Selecting the specified time period ensures that the resulting report is not empty because some traffic was generated on those dates.

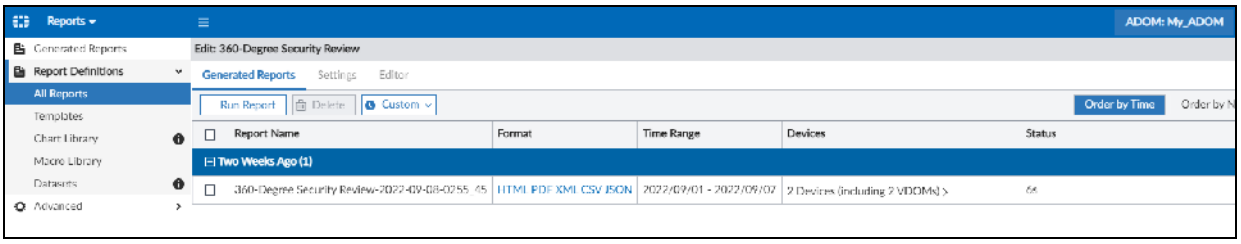
5. Click **Apply**.
6. Click the **Generated Reports** tab, and then click **Run Report** to run the report on demand.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

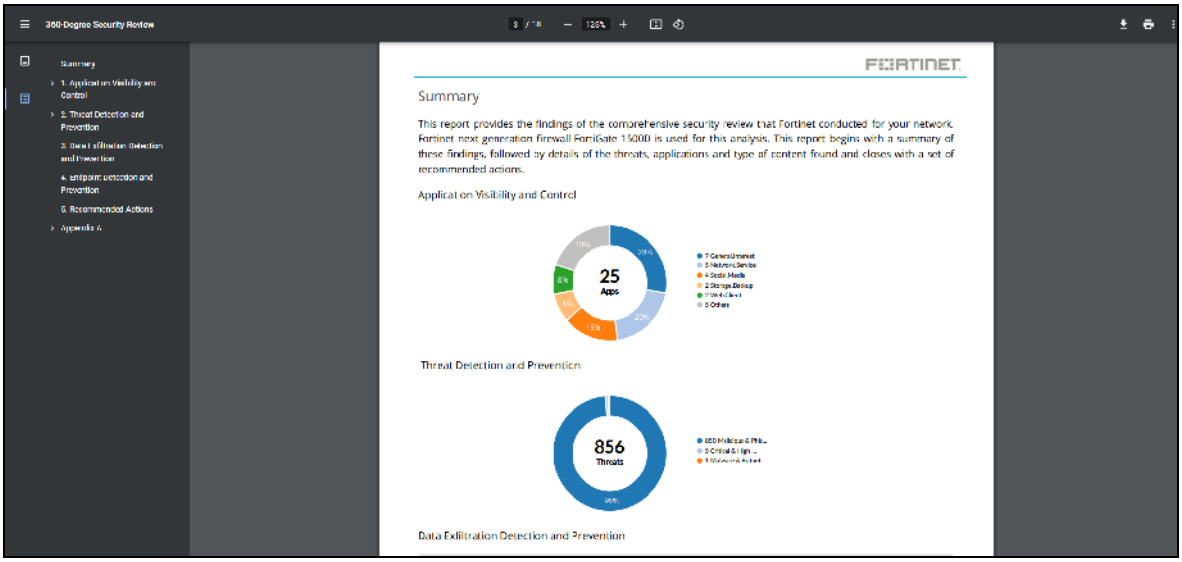
DO NOT REPRINT Brave-Dumps.com
© FORTINET



7. Click **Generated Reports**.
   After a few seconds, your report appears.



8. Under the **Format** column, click PDF to open the report.
   Your report may be different than the following report. You may select any reports to run based on the logs.



FortiManager remotely accesses FortiAnalyzer to retrieve the requested information for the FortiAnalyzer features. For example, if you use the **Reports** pane on FortiManager to create a report, the report is created on FortiAnalyzer, and then FortiManager remotely accesses the report.

Optionally, you can view the same report by accessing FortiAnalyzer.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

Lab 6: Global ADOM Policy Configuration

In this lab, you will enable and configure a global header policy.

Header and footer policies are used to envelop policies within each ADOM. These are typically invisible to users and devices in the ADOM layer. An example of where this is used is in a carrier environment, where the carrier allows customer traffic to pass through their network but does not allow the customer to have access to the carrier's network assets.

Objectives

- Create a global header policy
- Assign the policy to an ADOM
- Install the policy on devices

Time to Complete

Estimated: 15 minutes

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

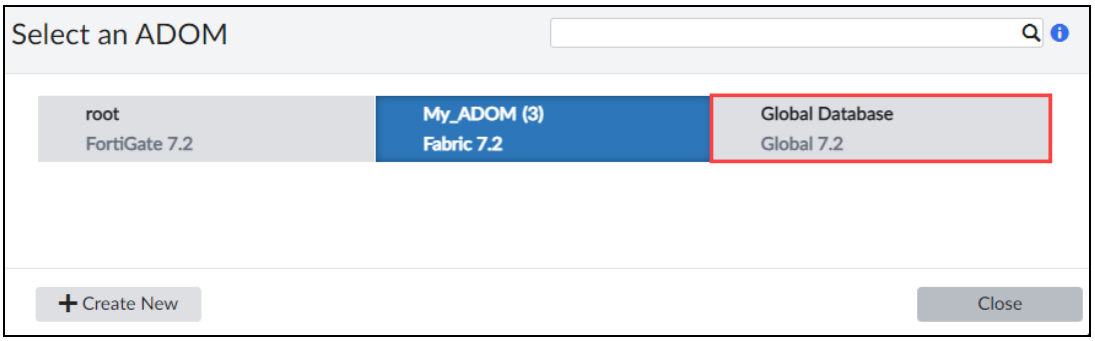
Exercise 1: Creating and Assigning Header Policies in the Global ADOM

Header and footer policies are used to envelop the policies in each ADOM. You can create the header and footer policies once in the global ADOM, and then assign them to multiple policy packages in other ADOMs.

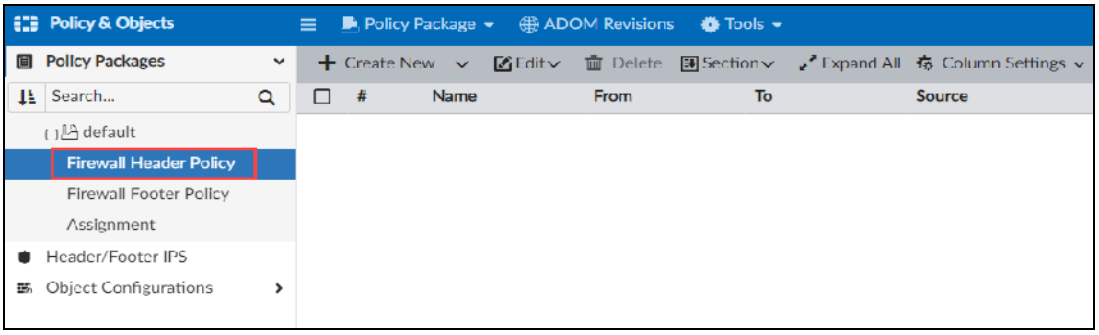
In this exercise, you will create the header policy in the global ADOM, and then assign the header policy to the managed devices in **My_ADOM**. Next, you will install the header policy on the managed devices.

To create a header policy

1. Log in to the FortiManager GUI with the username `admin` and password `password`.
2. Select the **Global Database** ADOM.



3. Click **Firewall Header Policy**.



4. Click **Create New**.
5. Configure the following settings:

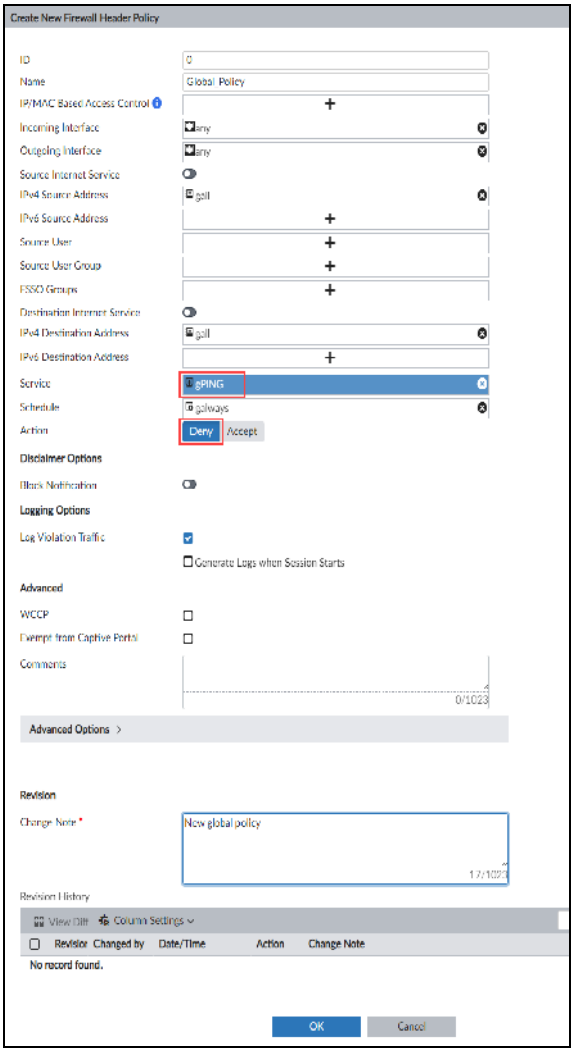
Field	Value
Name	Global_Policy
Incoming Interface	any
Outgoing Interface	any

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

Field	Value
IPv4 Source Address	gall
IPv4 Destination Address	gall
Service	gPING
Schedule	galways
Action	Deny
Change Note	New global policy

Your configuration should look like the following example:



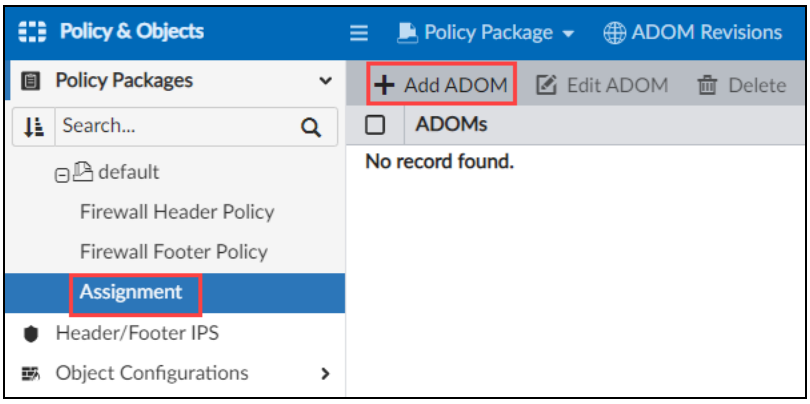
6. Click **OK**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

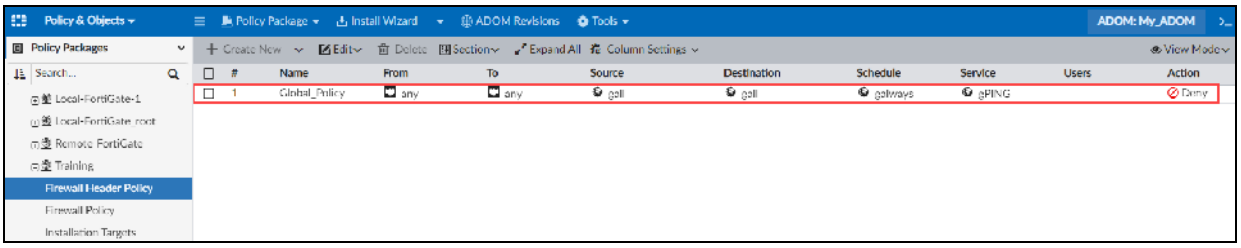
To assign a header policy

1. Click **Assignment**.
2. Click **Add ADOM**.

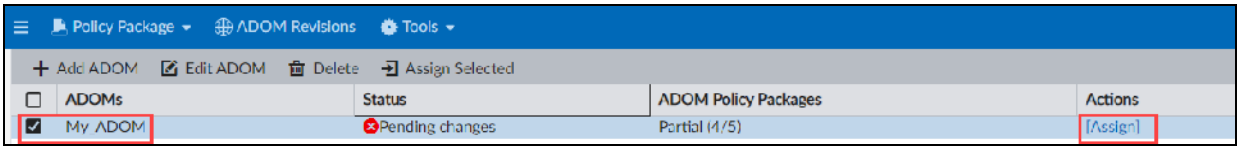


3. Configure the following settings:

Field	Value
ADOMs	My_ADOM
Specify Policy Packages To Exclude	Select the checkbox, and then select **default**.



4. Click **OK**.
5. Select **My_ADOM**, and then click **Assign**.



FortiManager assigns the header policy to the Local-FortiGate and Remote-FortiGate_root policy packages.

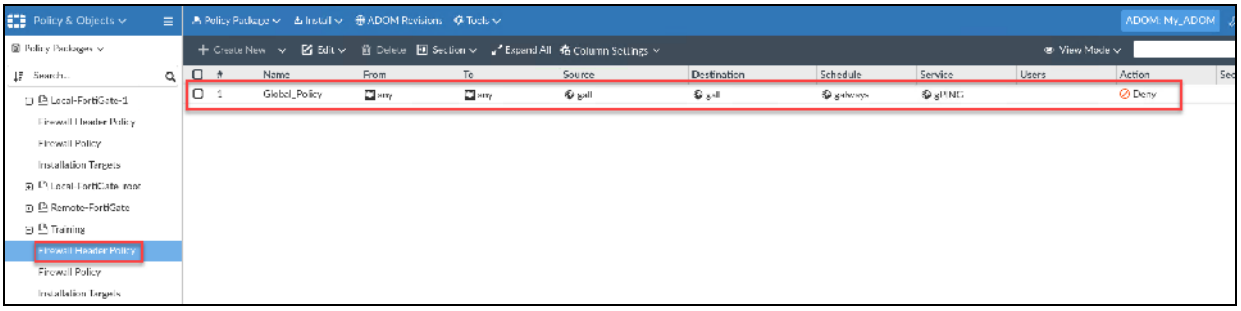
To install a header policy

1. Continuing on the FortiManager GUI, click **ADOM: Global Database**.

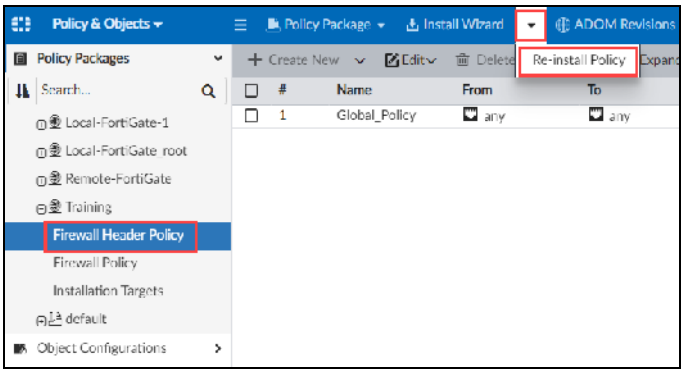
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

2. Click **My_ADOM**.
3. Click **Training** > **Firewall Header Policy** to view the assigned header policy.

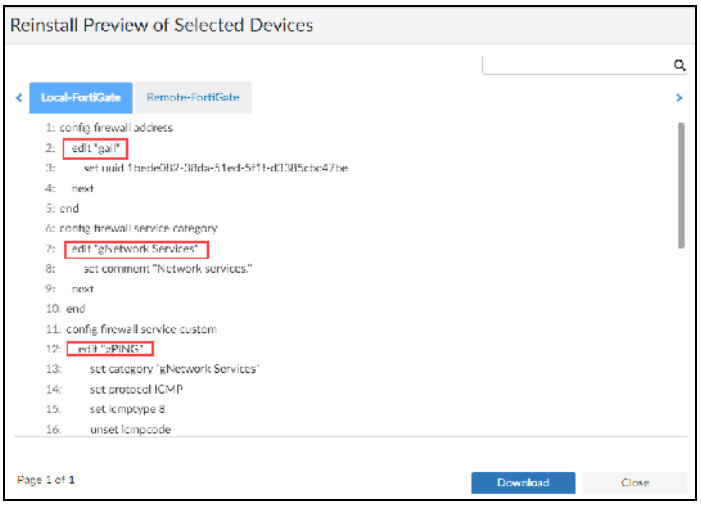


4. Click **Install Wizard** > **Re-install Policy**.



5. Click **OK**.
6. Click **Install Preview**.

   The configuration changes that FortiManager will install on FortiGate appear—in this case, the header policy and related objects.

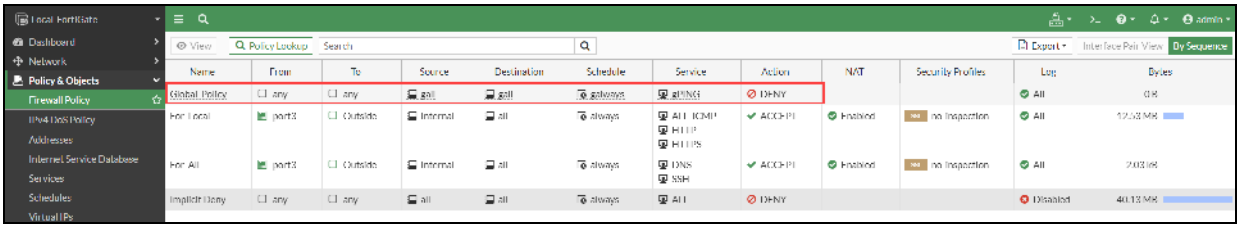


7. In the **Reinstall Preview** window, click **Close**.
8. Click **Next**.
9. Click **Finish**.
10. Log in to the Local-FortiGate and Remote-FortiGate GUIs with the username `admin` and password `password`.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

11. Click **Login Read-Only**.
12. Click **Policy & Objects** > **Firewall Policy**.
    You should see the header policy at the top.



13. Log out of both FortiGate devices.
14. On the Local-Client VM, open a terminal window, and then try to ping an external host (for example, `4.2.2.2`). You should see that the ping fails, because the header policy was configured to block the ping.
15. Close the terminal and PuTTY session window..

You can also promote ADOM objects to global objects. To do this, right-click any of the ADOM objects, and then select **Promote to Global**. You can use promoted objects in the global ADOM.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

Lab 7: Diagnostics and Troubleshooting

In this lab, you will perform diagnostics and troubleshooting when installing device-level settings and importing firewall policies.

Objectives

- Diagnose and troubleshoot issues when you install system templates
- Diagnose and troubleshoot issues when you import policy packages

Time to Complete

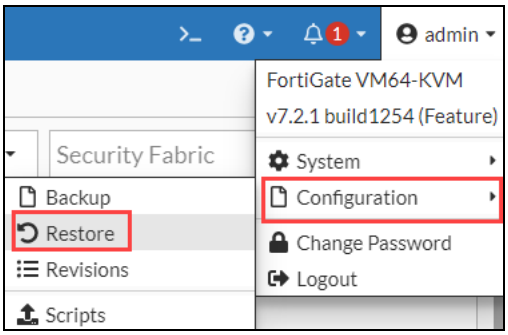
Estimated: 30 minutes

Prerequisites

Before beginning this lab, you must restore the configuration files to Remote-FortiGate, Local-FortiGate, and FortiManager.

To restore the FortiGate configuration file on both FortiGate devices

1. On the Local-Client VM, open a browser, and then log in to the Remote-FortiGate GUI with the username `admin` and password `password`.
2. Click **Login Read-Write**.
3. Click **Yes**.
4. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.



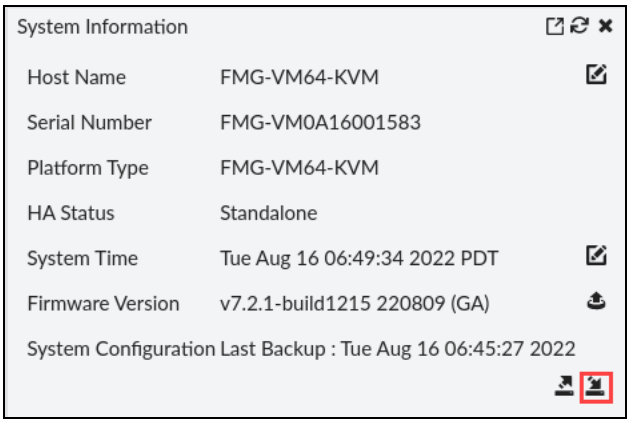
5. Click **Local PC**, and then click **Upload**.
6. Click **Desktop** > **Resources** > **FortiManager** > **Troubleshooting**, and then select `Remote-diag.conf`.
7. Click **OK**.
8. Click **OK** to reboot.
9. Log in to the Local-FortiGate GUI with the username `admin` and password `password`.
10. Repeat the same procedure to restore the system configuration for Local-FortiGate but, in the **Troubleshooting** folder, select `Local-diag.conf`.
11. After the reboot finishes, close both browser tabs.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

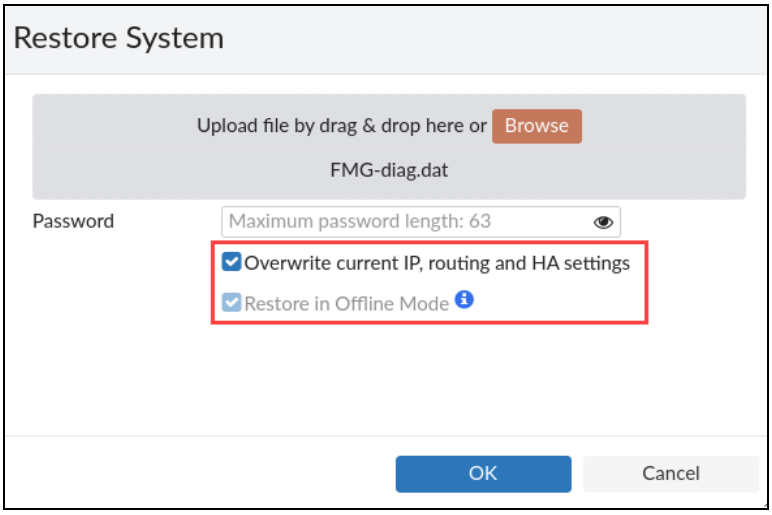
DO NOT REPRINT Brave-Dumps.com
© FORTINET

To restore the FortiManager configuration

1. On the Local-Client VM, open a browser, and then log in to the FortiManager GUI with the username `admin` and password `password`.
2. Click **root**.
3. Click **System Settings**.
4. In the **System Information** widget, in the **System Configuration** field, click the **Restore** icon.



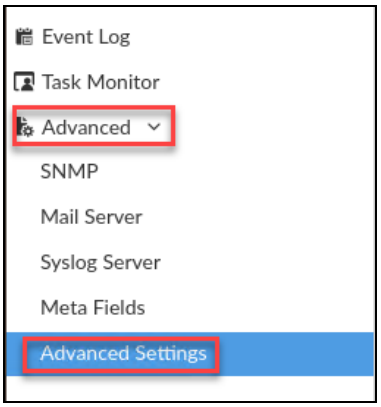
5. Click **Browse**.
6. Browse to **Desktop** > **Resources** > **FortiManager** > **Troubleshooting**, and then select `FMG-diag.dat`.
   You do not have to enter a password because the file is not encrypted.
7. Leave the **Overwrite current IP, routing and HA settings** checkbox selected.



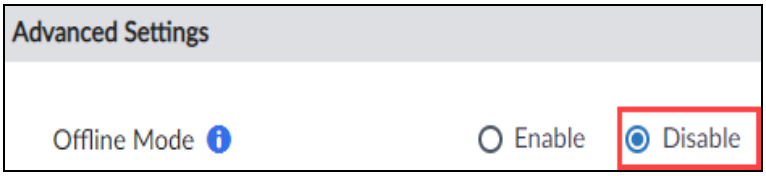
8. Click **OK**.
   FortiManager reboots.
9. Wait for FortiManager to reboot, and then log in to the FortiManager GUI as the `admin` user.
10. Click **root**.
11. Click **System Settings**.
12. Click **Advanced** > **Advanced Settings**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET



13. In the **Offline Mode** field, select **Disable**.



14. Click **Apply**.
    The **Offline Mode** message disappears. Now FortiManager can establish a management connection with the managed devices.
15. Log out of FortiManager.

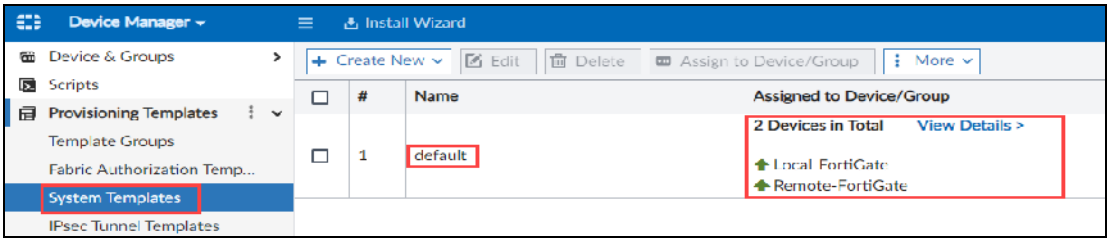
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

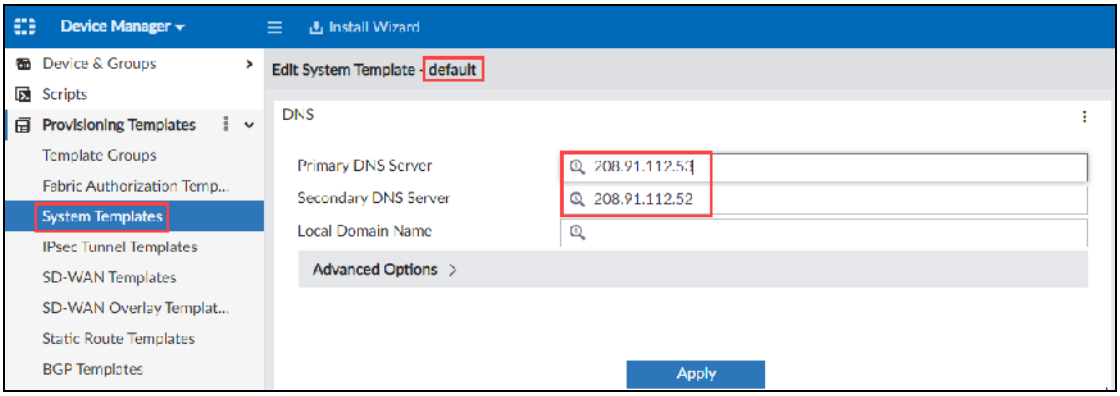
DO NOT REPRINT Brave-Dumps.com
© FORTINET

Exercise 1: Diagnosing and Troubleshooting Installation Issues

FortiManager is preconfigured as follows:

- ADOMs are enabled.
- **ADOM1** is configured for FortiGate firmware version 7.2.
- FortiManager is managing Local-FortiGate and Remote-FortiGate in **ADOM1**—the Remote-FortiGate policy package is not imported.
- The **default** system template is configured with the **DNS** widget only.
- The **default** system template is applied to Local-FortiGate and Remote-FortiGate.





In this exercise, you will diagnose and troubleshoot issues that occur when you install configuration changes on Local-FortiGate and Remote-FortiGate.

View the Installation Preview

You will view the installation preview to learn which device-level configuration changes FortiManager will install on the FortiGate devices. The objective of this task is to verify and troubleshoot to make sure FortiManager installs the correct configuration settingson the FortiGate devices.

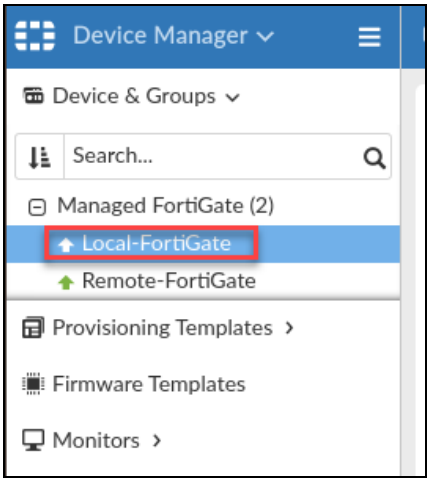
To view the installation preview for Local-FortiGate

1. Log in to the FortiManager GUI with the username `student` and password `fortinet`.
2. Click **ADOM1**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

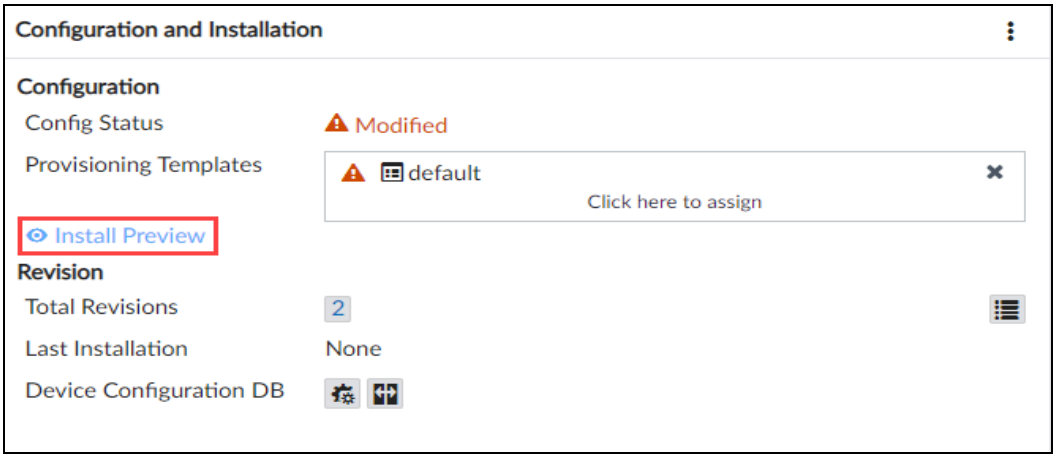
DO NOT REPRINT Brave-Dumps.com
© FORTINET

3. Click **Device Manager**.
4. Click **Local-FortiGate**.



5. In the **Configuration and Installation** widget, click **Install Preview**.
   Notice that **default** is listed as the **System Template**, which is preassigned to Local-FortiGate.

   The installation preview generates.



In the lab environment, the **Config Status** may remain as **Synchronized**.

To resolve this issue, remove the **default** template on the **Provisioning Templates** and then add it again. This step changes the status to **Modified** and then you can see the **Install Preview**.

6. Write down the DNS settings that FortiManager will install on Local-FortiGate.

Primary:
Secondary:

7. Click **Close**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

To view the installation preview for Remote-FortiGate

1. On the FortiManager GUI, click **Remote-FortiGate**.
2. In the **Configuration and Installation** widget, click **Install Preview**.

In the lab environment, the **Config Status** may remain as **Synchronized**.

To resolve this issue, remove the **default** template on the **Provisioning Templates** and then add it again. This step changes the status to **Modified** and then you can see the **Install Preview**.

1. Write down the DNS settings that FortiManager will install on Remote-FortiGate.

Primary:
Secondary:

4. Click **Close**.

Stop and think!

The system template was configured with two entries. Why does Local-FortiGate show only one DNS entry, but Remote-FortiGate shows two entries?

Local-FortiGate was preconfigured with the primary DNS entry `208.91.112.53`. When Local-FortiGate was added to FortiManager, it automatically updated in the device-level database. To verify this, check the current revision history and search for `config system dns`.

You can use the following procedure to view the system template and DNS settings on the CLI.

View the DNS Configuration

You will view the DNS configuration for the configured system template and compare it to the device-level database settings for DNS (for both Local-FortiGate and Remote-FortiGate). You will view the configuration on the CLI.

To view the system template configuration on the CLI

1. On the Local-Windows VM, open PuTTY, and then connect over SSH to the **FortiManager** saved session.
2. Log in as `admin`, and then enter the following command to view the CLI configuration for the system template configuration:

```
execute fmpolicy print-adom-package ADOM1 5 3547 533 dns
```

The following output should appear:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET


```
FMG-VM64 # FMG-VM64 # execute fmpolicy print-adom-package ADOM1 5 3547 533 dns
Dump object [dns] of category [device template widget] in adom [ADOM1] package [3547]:
---------------
config device template widget
edit "dns"
config action-list
edit 1
set action "conf-sys-dns"
set model "all"
set value "{\"server-hostname\":[],\"primary\":\"208.91.112.53\",\"secondary\":\"208.91.112.52\"}"
config var-list
```

The `execute fmpolicy print-` command tree allows you to view the CLI configuration for provisioning templates, ADOMs, and the device database on FortiManager.

The syntax for provisioning templates is:

```
execute fmpolicy print-adom-package <adom> <template name>
<package name> [<category name>|all][<key>|all|list]
```

You can use the help feature by typing `?` to open the command tree syntax.

To view the DNS settings for FortiGate (CLI)

1. In the **FortiManager** PuTTY session, enter the following command to view the Local-FortiGate DNS settings in the FortiManager device-level database:

   ```
   execute fmpolicy print-device-object ADOM1 Local-FortiGate root 15
   ```

   The following output should appear:

   ```
   Dump all objects for category [system dns] in device [Local-FortiGate] vdom[root]:
   ---------------
   config system dns
   set primary 208.91.112.53
   set secondary 4.2.2.2
   end
   ```

The syntax for the device object is:

```
execute fmpolicy print-device-object <adom> <devname> <vdom>
<category>|all [<key>|all|list]
```

2. Enter the following command to view the Remote-FortiGate DNS settings in the FortiManager device-level database:

   ```
   execute fmpolicy print-device-object ADOM1 Remote-FortiGate root 15
   ```

   The following output should appear:

   ```
   Dump all objects for category [system dns] in device [Remote-FortiGate] vdom[root]:
   ---------------
   config system dns
   set primary 4.2.2.2
   set secondary 8.8.8.8
   end
   ```


Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

3. Compare the FortiManager system template entries with each FortiGate.

   The primary DNS entry for Local-FortiGate matches the primary DNS entry in the default system template. Because of this, FortiManager skips the primary DNS entry for Local-FortiGate—Local-FortiGate has already been configured with the same entry.

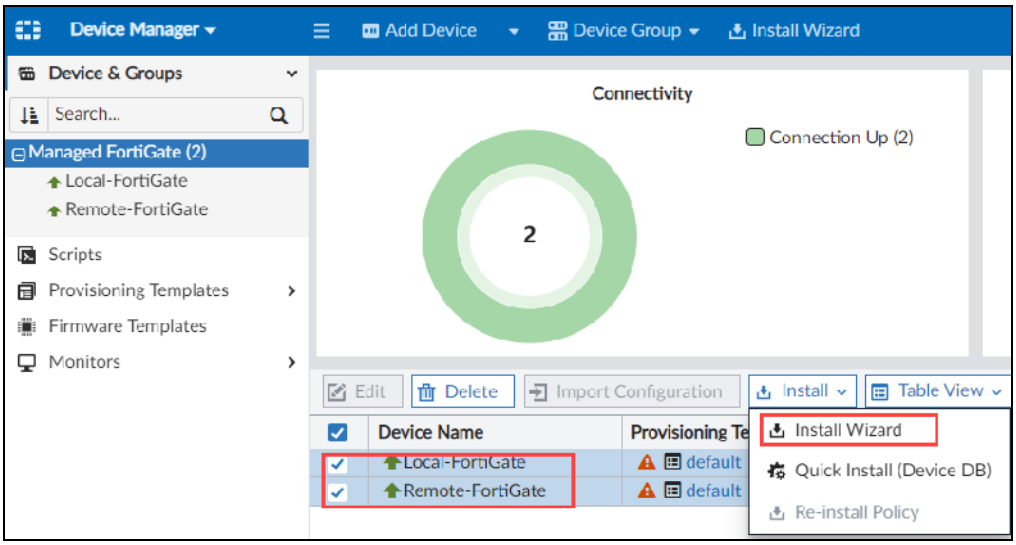
4. Close the PuTTY session.

Install Device-Level Configuration Changes

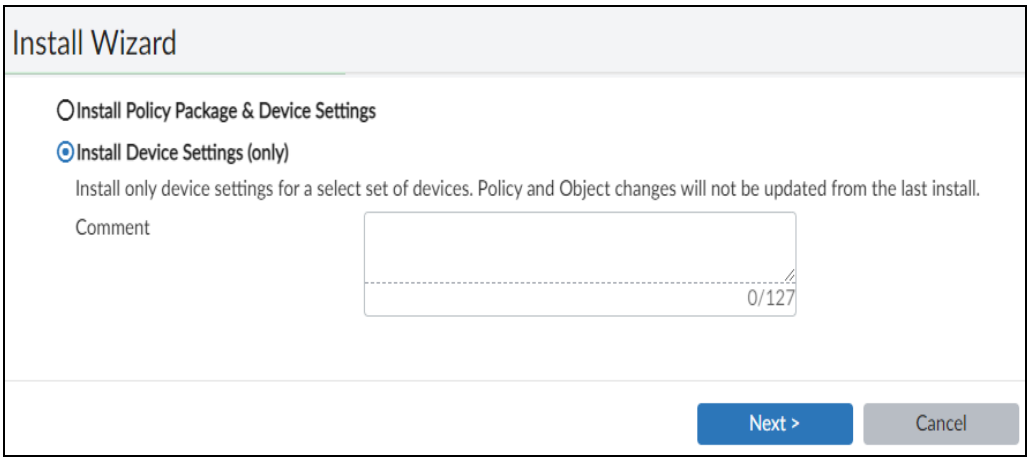
You will install device-level configuration changes (system templates) on the managed FortiGate devices.

To install device-level changes (system templates)

1. On the FortiManager GUI, click **Managed FortiGate**.
2. In the drop-down list, click **Install** > **Install Wizard**.



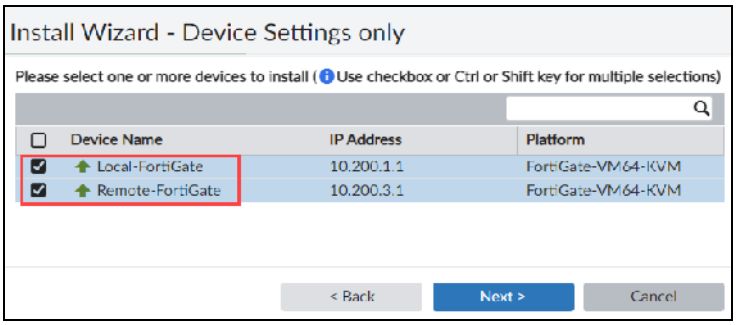
4. Select **Install Device Settings (only)**, and then click **Next**.



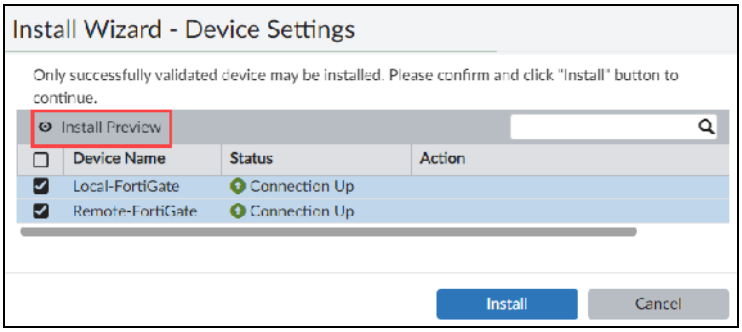
5. Make sure both devices are selected, and then click **Next**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

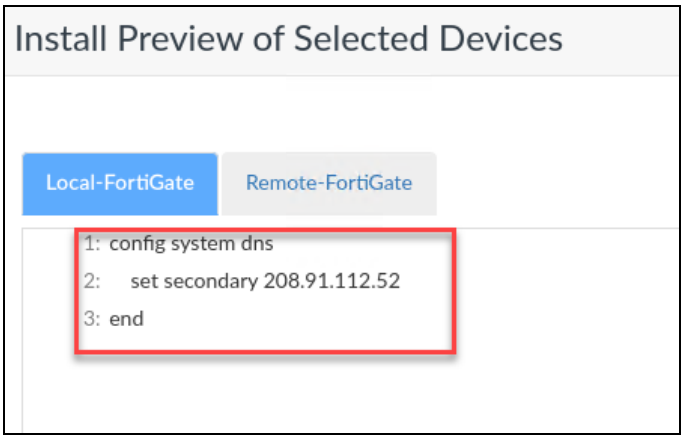
DO NOT REPRINT Brave-Dumps.com
© FORTINET



6. Click **Install Preview**, and then view the install preview for Local-FortiGate.



The preview generates.

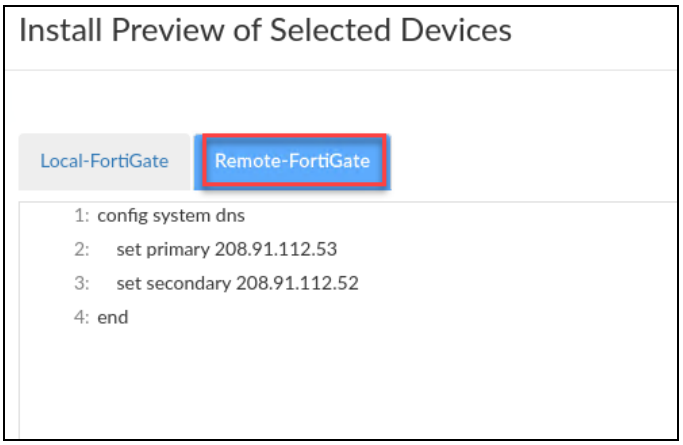


Optionally, you can download the preview.

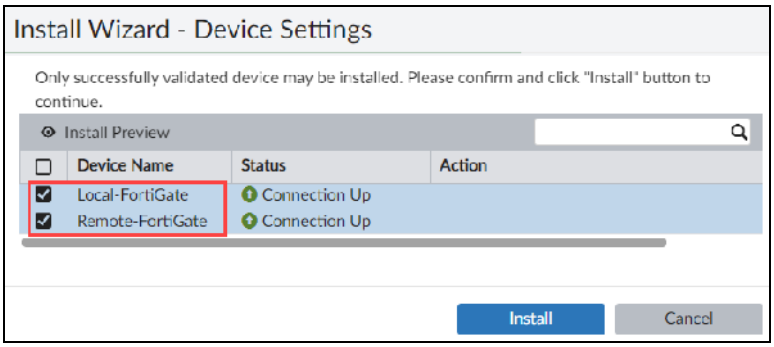
7. For the Remote-FortiGate install preview, click **Remote-FortiGate**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

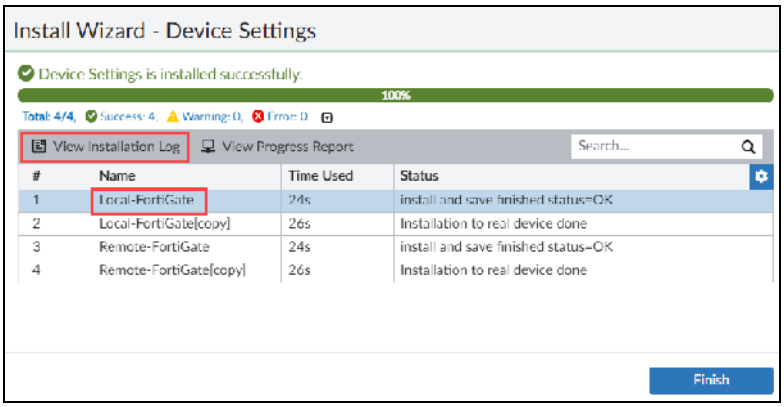
DO NOT REPRINT Brave-Dumps.com
© FORTINET



8. Click **Close**.
9. Make sure both FortiGate devices are selected, and then click **Install**.
   The installation begins.



10. After the installation finishes, select any of the FortiGate devices, and then click the **View Installation Log** icon to view and verify what is being installed on each device.



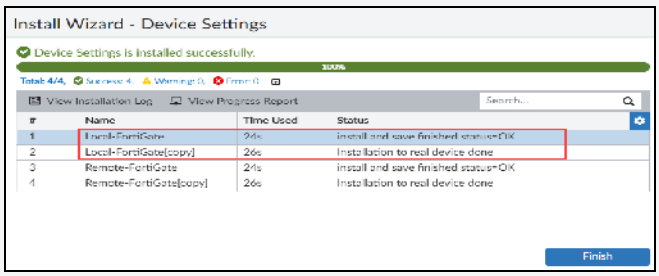
11. In the **Install Log** window, click **Close**.
12. Click **Finish**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

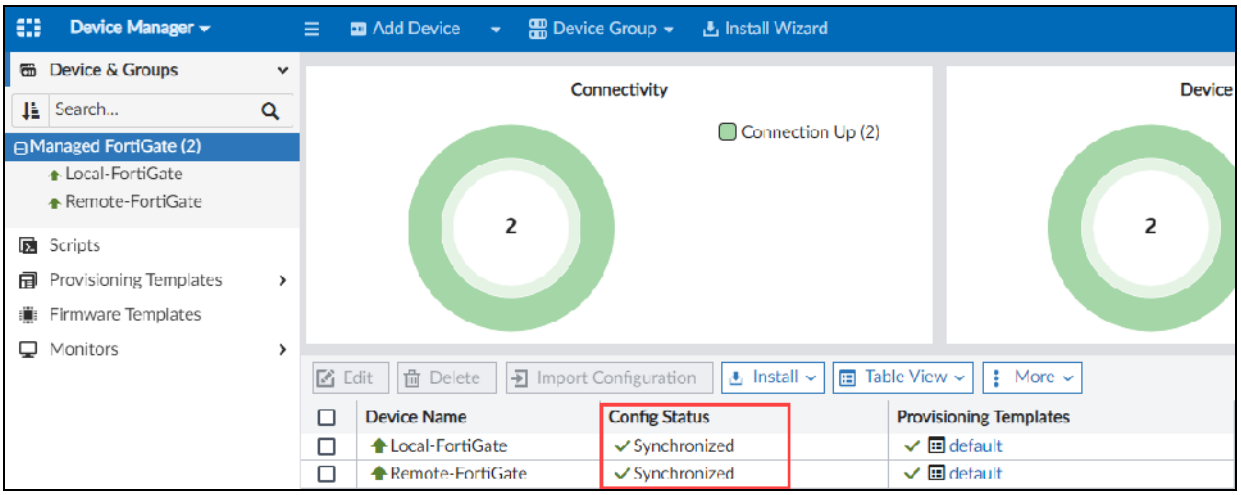
Stop and think!

Why does FortiManager show two progress bars when installing changes on a FortiGate?



As you learned in previous lessons, when you perform an installation, the copy operation is the first operation that FortiManager performs, before the actual installation.

The **Config Status** for both FortiGate devices should be **Synchronized**.



You may need to enable the **Config Status** column in the column settings to check the status.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

Exercise 2: Troubleshooting Policy Import Issues

In this exercise, you will view the policies and objects imported into the ADOM database. The objects share the common object database for each ADOM and are saved in the ADOM database, which can be shared or used among different managed FortiGate devices in the same ADOM.

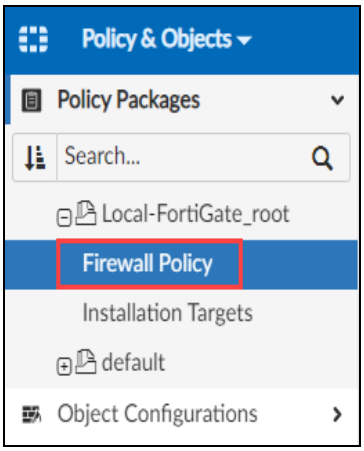
You will also diagnose and troubleshoot issues that occur while you import the Remote-FortiGate policy package.

View the Policy Package and Objects

Because the Local-FortiGate policy package is imported into ADOM1, you will view the Local-FortiGate policy package and objects imported into the **ADOM1** database.

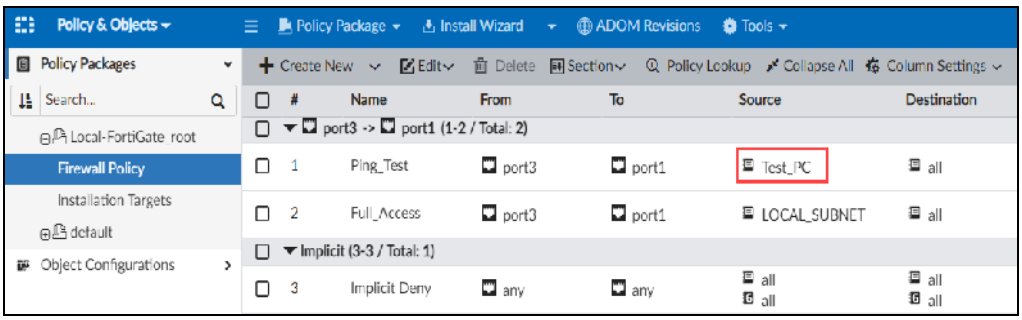
To view the policy package and objects for Local-FortiGate

1. Log in to the FortiManager GUI with the username `student` and password `fortinet`.
2. Click **ADOM1**.
3. Click **Policy & Objects**.
4. On the left side of the window, expand **Local-FortiGate_root**, and then click **Firewall Policy**.



You can see the two policies for Local-FortiGate.

Notice the source address of **Test_PC** for the **Ping_Test** firewall policy.

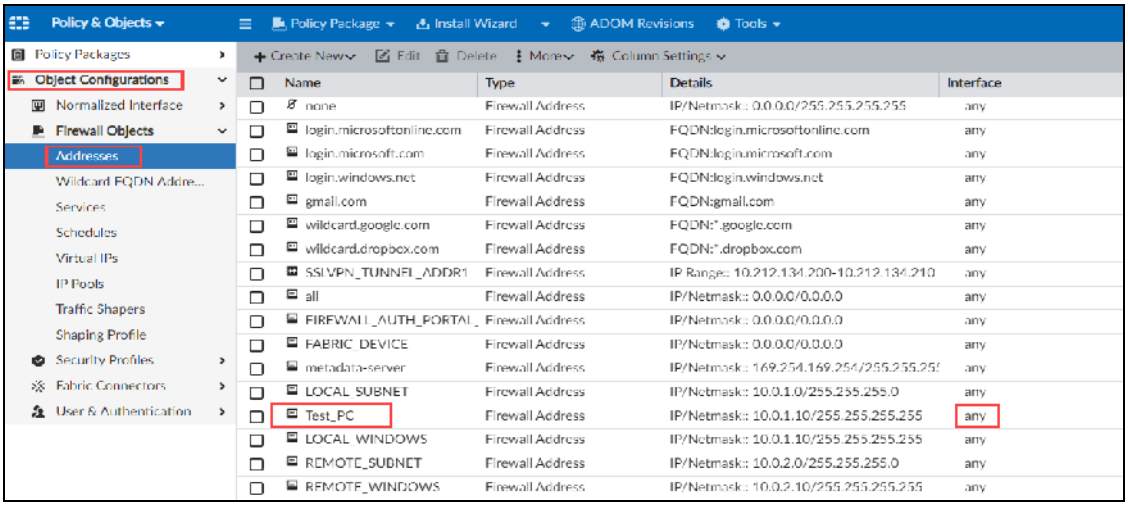


Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

5. Click **Object Configurations**.
6. Expand **Firewall Objects**, and then click **Addresses**.
7. Review the configuration for the **Test_PC** firewall address.

   In the ADOM database, **Test_PC** is set to the **any** interface based on the configuration imported from Local-FortiGate.



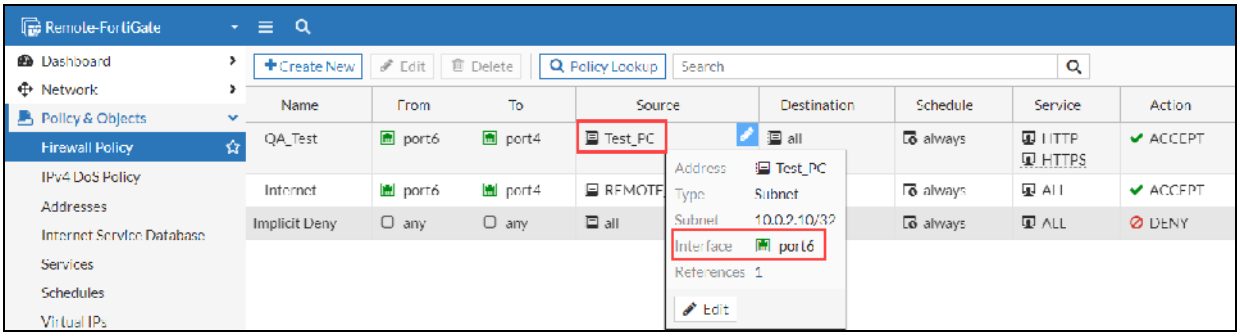
Review Policies and Objects Locally on Remote-FortiGate

You must import the policies and objects from Remote-FortiGate. But first, you will review the policies and objects locally on Remote-FortiGate.

To review policies and objects locally on Remote-FortiGate

1. Log in to the Remote-FortiGate GUI with the username `admin` and password `password`.
2. Click **Login Read-Only**.
3. Click **Policy & Objects** > **Firewall Policy**.
4. Expand the port6 to port4 policies.
5. In the **Source** column of the **QA_Test** firewall policy, hover over the **Test_PC** address object.

   You can see that the **Test_PC** address object is bound to the **port6** interface.



   Remember, the **Test_PC** address object is bound to the **any** interface in the ADOM database.

6. Log out of Remote-FortiGate.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

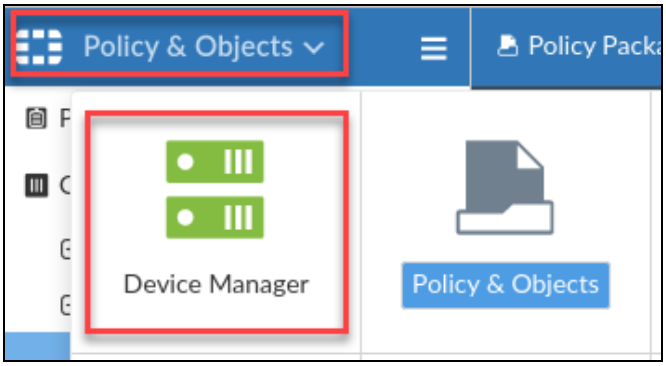
DO NOT REPRINT Brave-Dumps.com
© FORTINET

Import a Policy Package

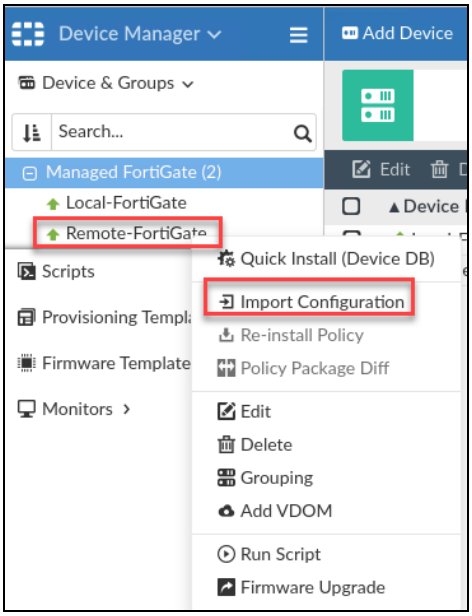
You will import the policies and objects for Remote-FortiGate into the policy package, and then troubleshoot issues with the policy import.

To import the policy package

1. Return to the FortiManager GUI, and then click **Policy & Objects** > **Device Manager**.



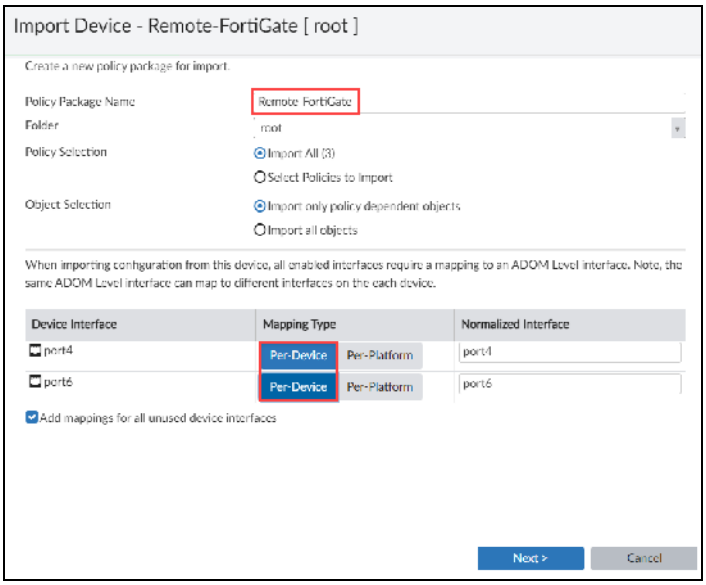
2. Right-click **Remote-FortiGate**, and then click **Import Configuration**.



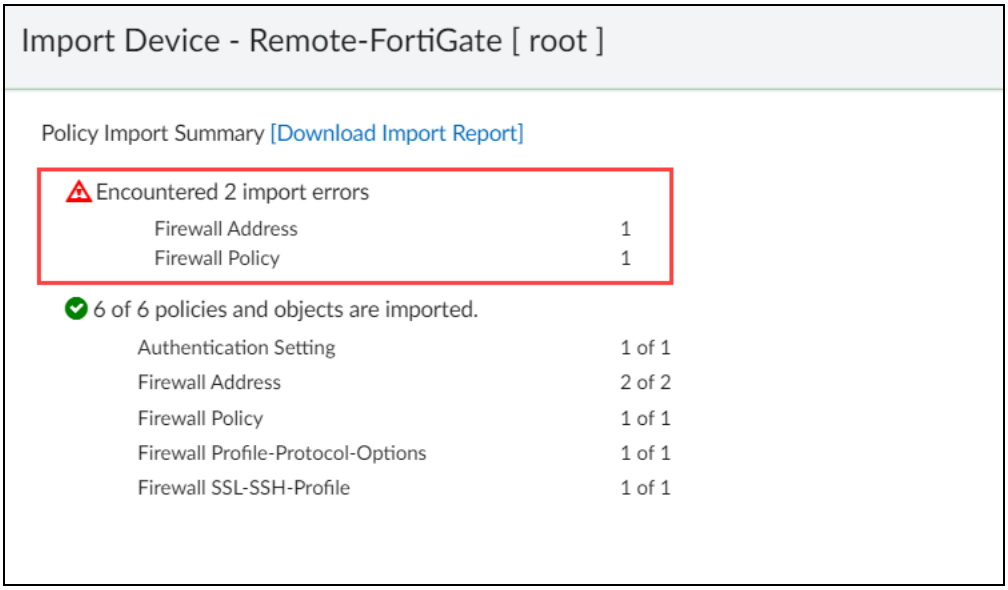
3. Select **Import Policy Package**.
4. Click **Next**.
5. Make sure the policy package name is `Remote-FortiGate`.
6. Make sure the **Mapping Type** is set to **Per-Device** for both **port4** and **port6**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET



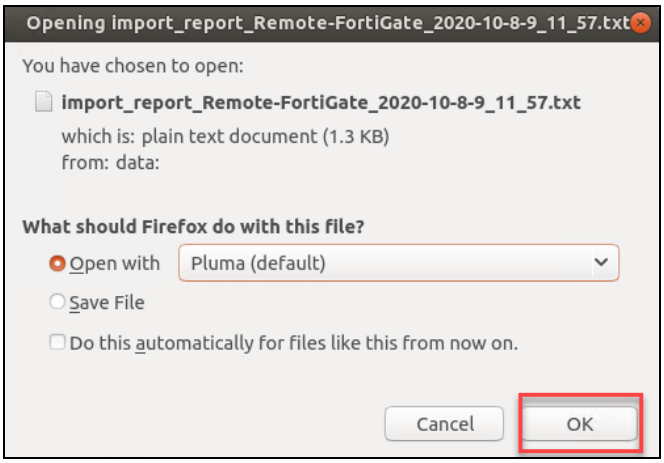
7. Keep the default values for all other settings, and then click **Next**.
8. Click **Next**.
   Did you notice that the policy import skipped one firewall policy and a firewall address object?



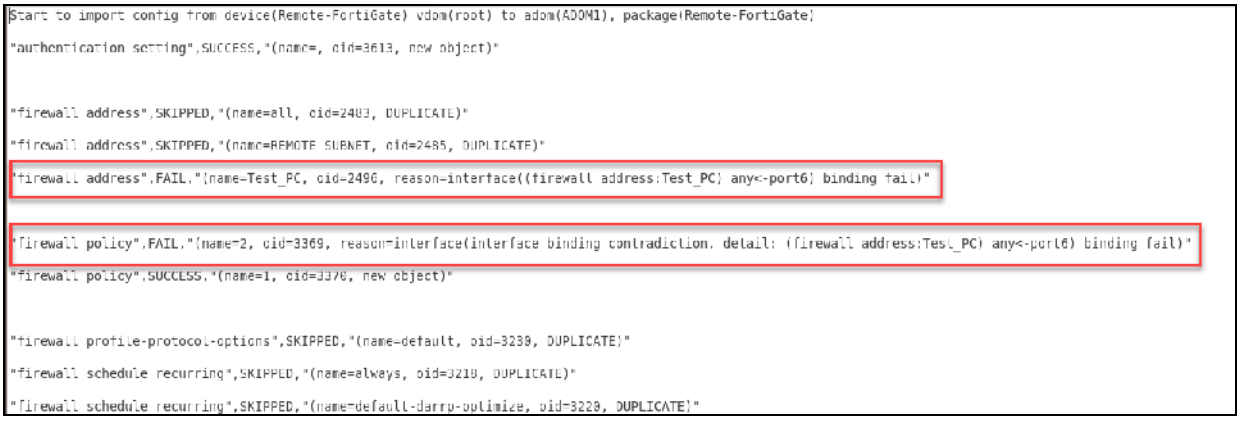
9. Click **Download Import Report** to view the reason that the policy import skipped a firewall policy.
10. Open the file (or save it for future reference).

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET



Did you notice that the policy import failed when importing firewall policy `2` and the `Test_PC` address object?



Stop and think!

The following output provides the reason for the policy import failure:

`reason=interface(interface binding contradiction. detail: any<-port6) binding fail)"`

What does this error mean? What is the impact? How can you fix this partial policy import issue?

Remember, in the **ADOM1** database, the **Test_PC** firewall address is bound to the **any** interface, based on the configuration imported from Local-FortiGate. On Remote-FortiGate, policy ID 2 is using the **Test_PC** firewall address bound to port6 as the source address.

This is the expected behavior on FortiManager because it doesn't allow the same address object name to bind to different interfaces.

Because FortiManager imported partial policies in the policy package, if you try to make a change to the policy package and install it, FortiManager deletes the skipped policies and objects associated with those policies, along with all unused objects.

You must change the **Test_PC** firewall address binding to the **any** interface by locally logging in to Remote-FortiGate.

11. Close the import report, and then click **Finish**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

Check the Impact of a Partial Policy Import (Optional)

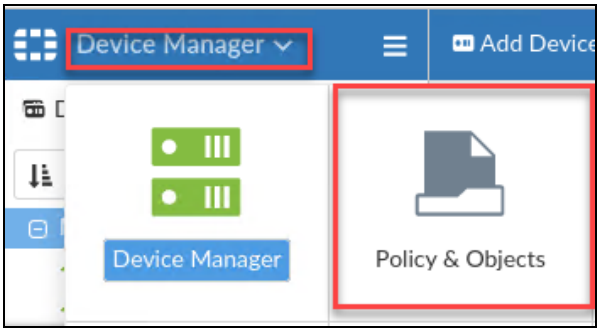
The following two procedures show the impact of making changes to the FortiManager policy package **Remote-FortiGate**, and then trying to install the policy package. FortiManager tries to delete policy ID 2 and the **Test_PC** address object on Remote-FortiGate. FortiManager also tries to delete any unused objects.

If you are now familiar with the behavior, you can skip the following procedures:

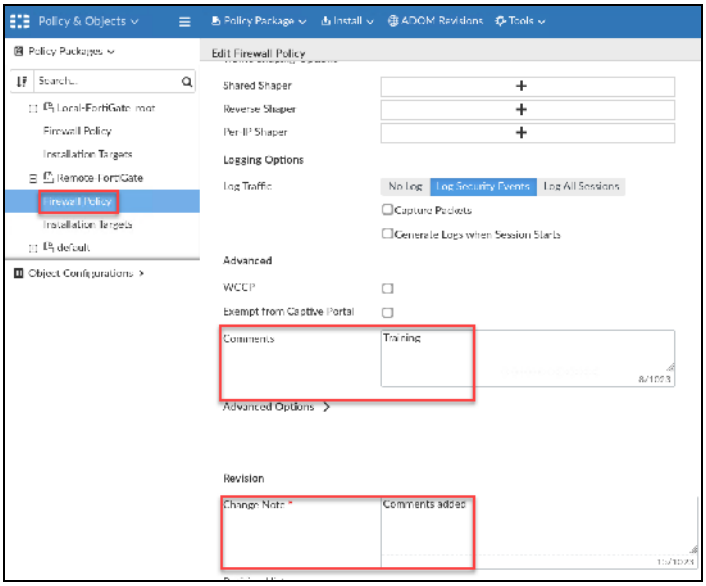
- To make configuration changes to the Remote-FortiGate policy package (optional)
- To preview the installation changes (optional)

To make configuration changes to the Remote-FortiGate policy package (optional)

1. On the FortiManager GUI, click **Device Manager** > **Policy & Objects** > **Policy Packages**.



2. Click the **Remote-FortiGate** policy package, and then click **Firewall Policy**.
   You can see that the firewall policy with **Test_PC** as the source address is not imported.
3. Double-click the **Seq# 1** firewall policy.
4. In the **Comments** field, type `Training`.
5. In the **Change Note** field, type `Comments Added`, and then click **OK**.

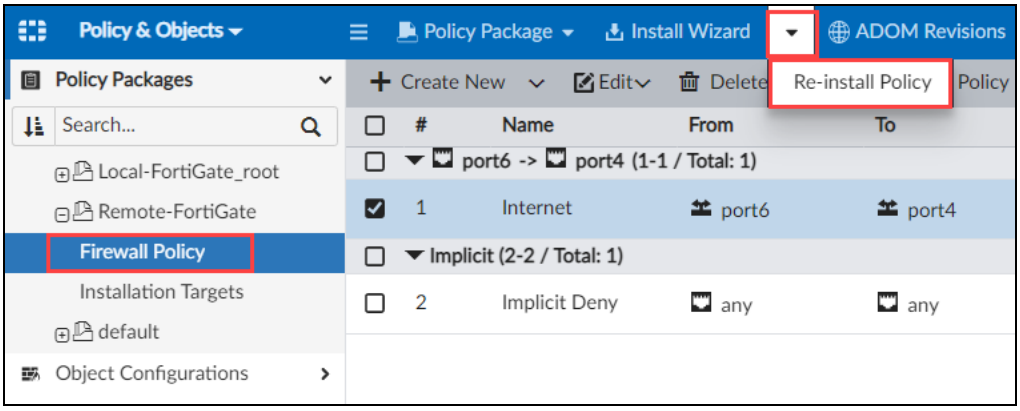


Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

To preview the installation changes (optional)

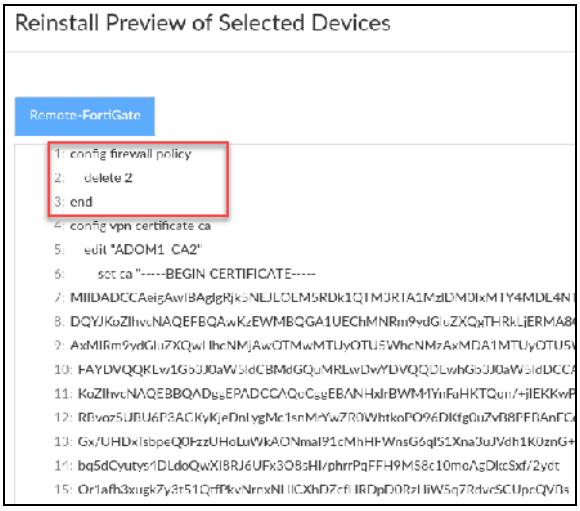
1. Ensure that **Firewall Policy** is selected for the **Remote-FortiGate** policy package, click the down arrow beside **Install Wizard**, and then select **Re-install Policy**.



2. Click **OK**.
3. Click **Install Preview**.
4. Notice that FortiManager is trying to delete the firewall policy with **ID=2** and the **Test_PC** address object.

When installing a policy package for the first time, FortiManager also deletes all unused objects.

This is the firewall policy with **Test_PC** as the source address.



Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

5. In the **Install Preview** window, click **Close**.
6. Click **Cancel** to cancel the policy installation.

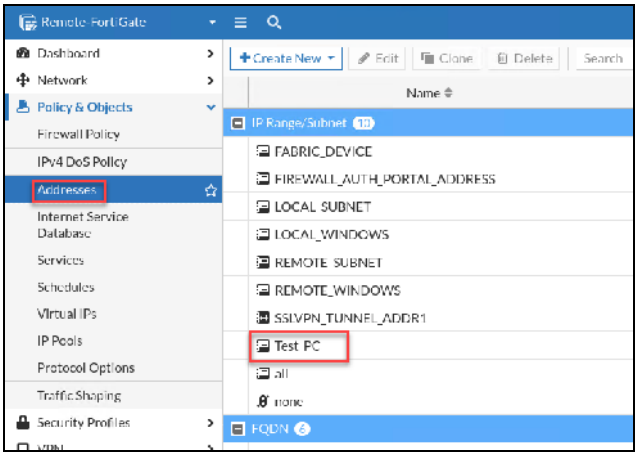
Fix a Partial Policy Import Issue

You must change the **Test_PC** firewall address binding to the **any** interface by locally logging in to Remote-FortiGate, and then retrieving the configuration to FortiManager.

Then, on FortiManager, you can import the policy package for Remote-FortiGate.

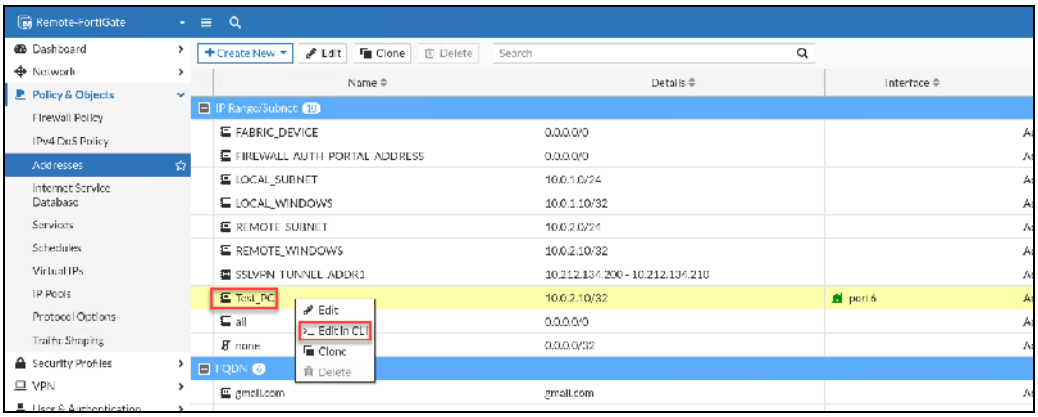
To make local changes on Remote-FortiGate

1. Log in to the Remote-FortiGate GUI with the username `admin` and password `password`.
2. Click **Login Read-Write**.
3. In the warning window, click **Yes**.
4. Click **Policy & Objects** > **Addresses**.
5. Right-click **Test_PC**, and then select **Edit in CLI**.



Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET



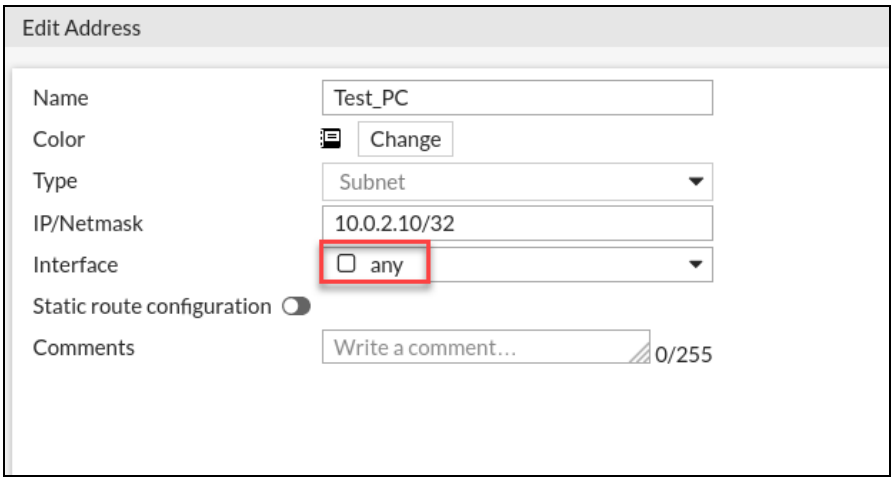
6. On the CLI, enter the following commands:

```
unset associated-interface
end
```

```
Remote-FortiGate # config firewall address

Remote-FortiGate (address) # edit Test_PC

Remote-FortiGate (Test_PC) # show
config firewall address
    edit "Test_PC"
        set uuid 29c1bc4a-09bc-51ec-3988-1ef46a43ad9e
        set associated-interface "port6"
        set subnet 10.0.2.10 255.255.255.255
    next
end

Remote-FortiGate (Test_PC) # unset associated-interface

Remote-FortiGate (Test_PC) # end

Remote-FortiGate #
```

7. Close the CLI console window.
8. Edit the **Test_PC** address.

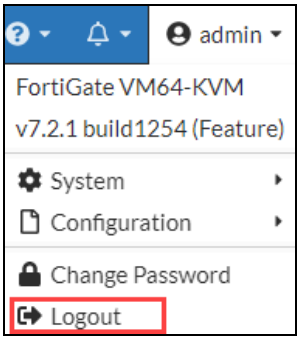
   Your configuration should look like the following example:



Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

9. Click **Cancel**.
10. Log out of Remote-FortiGate.

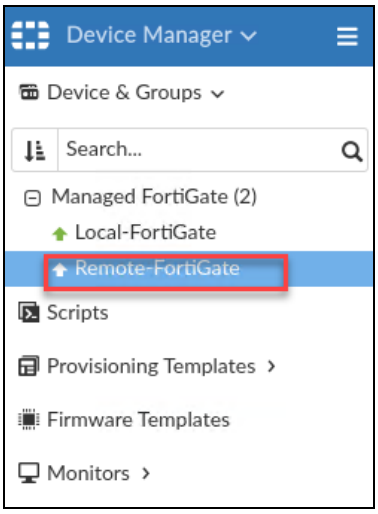


Retrieve the New Configuration From FortiManager

You will retrieve the change made to the Remote-FortiGate configuration on FortiManager.

To retrieve the Remote-FortiGate configuration change on FortiManager

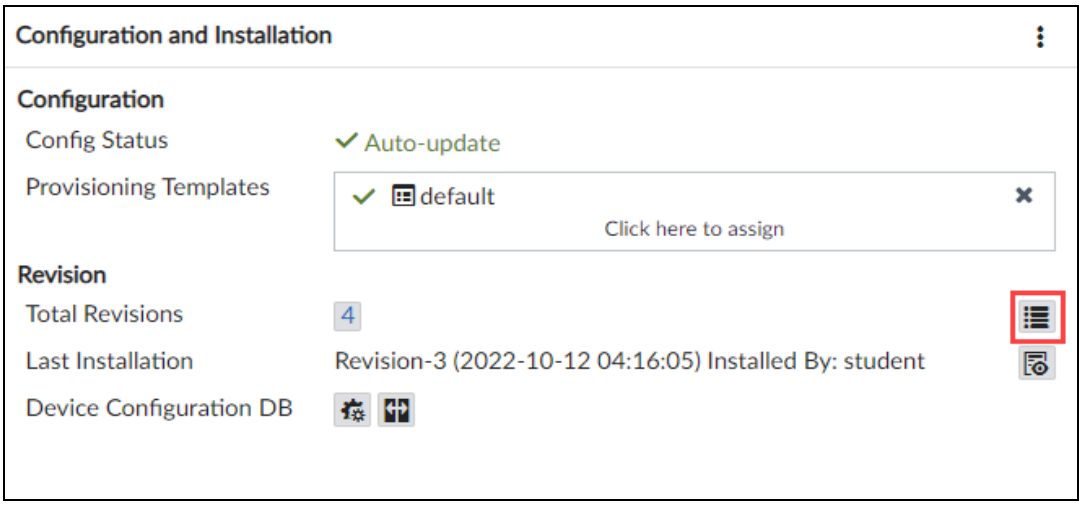
1. Return to the FortiManager GUI, and then click **Device Manager** > **Managed FortiGate**.
2. Click **Remote-FortiGate**.



3. In the **Configuration and Installation** widget, click the **Revision History** icon.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

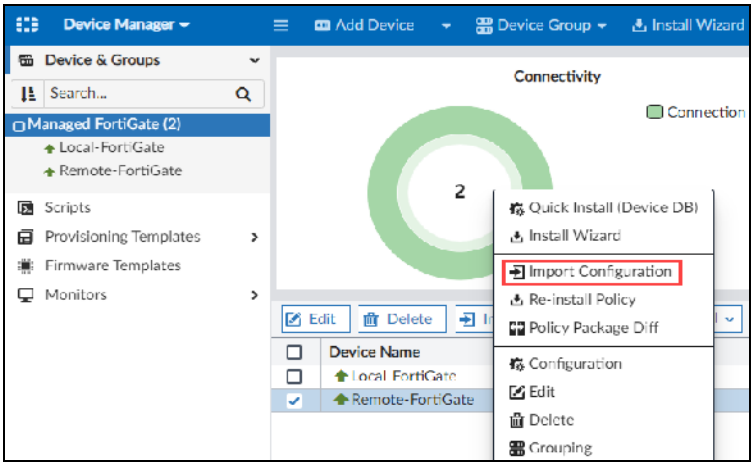
DO NOT REPRINT Brave-Dumps.com
© FORTINET



4. Click **Retrieve Config**.
5. Click **Close** to close the **Retrieve Device Revision** window.
6. Click **Close** to close the **Configuration Revision History** window.

To import the policy package again

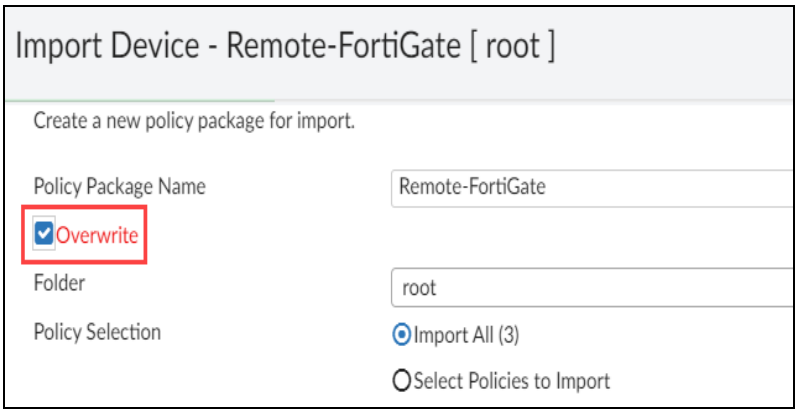
1. On the FortiManager GUI, click **Managed FortiGate**.
2. Right-click **Remote-FortiGate**, and then select **Import Configuration**.



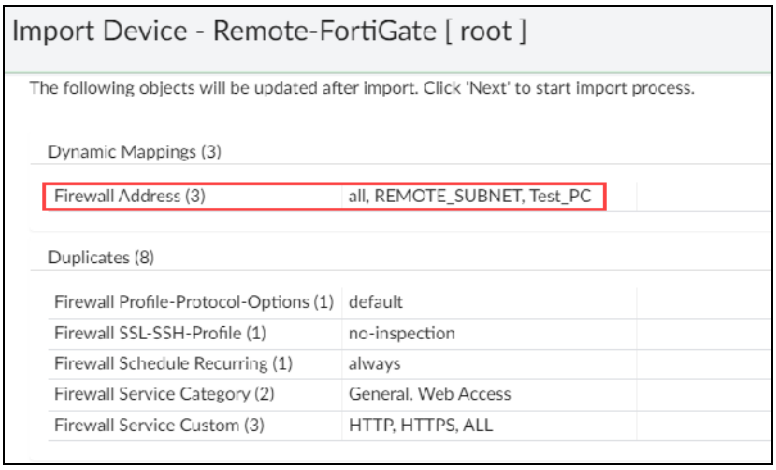
3. Select **Import Policy Package**.
4. Click **Next**.
5. Select the **Overwrite** checkbox.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

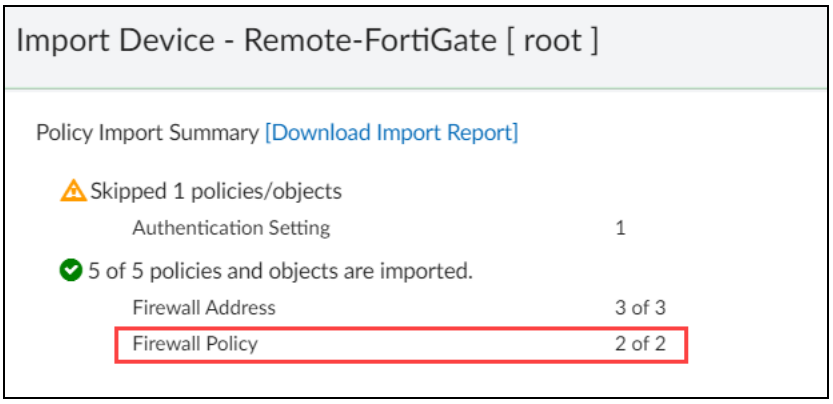


6. Click **Next**.
7. Keep the default values for all other settings, and then click **Next**.
   Did you notice that **Test_PC** appears as **Dynamic Mappings**?



   FortiManager automatically creates a dynamic mapping of the object with the same values. The interface must be the same as the ADOM database.

8. Click **Next**.
   You can see that FortiManager imported both firewall policies this time.



9. Click **Finish**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

Lab 8: Additional Configuration

In this lab, you will learn about the troubleshooting commands used for FortiGuard management, and how to use FortiManager to upgrade the firmware on managed FortiGate devices.

Objectives

- Review the central management configuration on both FortiGate devices
- Understand and run FortiGuard debug commands
- Import the firmware image for FortiGate devices and upgrade the devices using FortiManager

Time to Complete

Estimated: 15 minutes

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

Exercise 1: Examining FortiGuard Management

In this exercise, you will review the central management settings on FortiGate. Then, you will run CLI commands related to FortiGuard diagnostics on FortiManager to understand FortiGuard settings on FortiManager.

To review central management settings on both FortiGate devices

1. Open PuTTY, and then connect over SSH to the **Local-FortiGate** and **Remote-FortiGate** saved sessions.
2. Log in with the username `admin` and password `password`.
3. Enter the following command:

```
show system central-management
```

The outputs for Local-FortiGate and Remote-FortiGate should look similar to the following examples:

Local-FortiGate:

```
Local-FortiGate # show system central-management
config system central-management
    set type fortimanager
    set allow-push-firmware disable
    set allow-remote-firmware-upgrade disable
    set fmg "10.200.1.241"
    config server-list
        edit 1
            set server-type update rating
            set server-address 10.0.1.241
        next
    end
    set include-default-servers disable
end
```

Remote FortiGate:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET


```
Remote-FortiGate # show system central-management
config system central-management
    set type fortimanager
    set allow-push-firmware disable
    set allow-remote-firmware-upgrade disable
    set fmg "10.200.1.241"
    config server-list
        edit 1
            set server-type update rating
            set server-address 10.200.1.241
        next
    end
    set include-default-servers disable
end
```

You can see that `server-list` is configured on the FortiGate devices with the FortiManager IP address, and `include-default-servers` is disabled. This means the FortiGate devices are pointed to FortiManager for FortiGuard services, and access to public FortiGuard servers is disabled.

Diagnose FortiGuard Issues

You will run CLI commands on FortiManager to verify the FortiGuard configuration in order to troubleshoot FortiGuard issues.

To diagnose FortiGuard issues

1. Open PuTTY, and then connect over SSH to the **FortiManager** saved session.
2. Log in with the username `admin` and password `password`.
3. Run the following commands:

```
diagnose fmupdate view-serverlist fds
```

```
FMG-VM64 # diagnose fmupdate view-serverlist fds
Fortiguard Server Comm : Disabled
Server Override Mode   : Loose
```

FortiManager is unable to connect to the public FDN servers because of unreachability or disabled service. In this lab environment, communication with the public FortiGuard servers is disabled.

```
diagnose fmupdate update-status fds
```

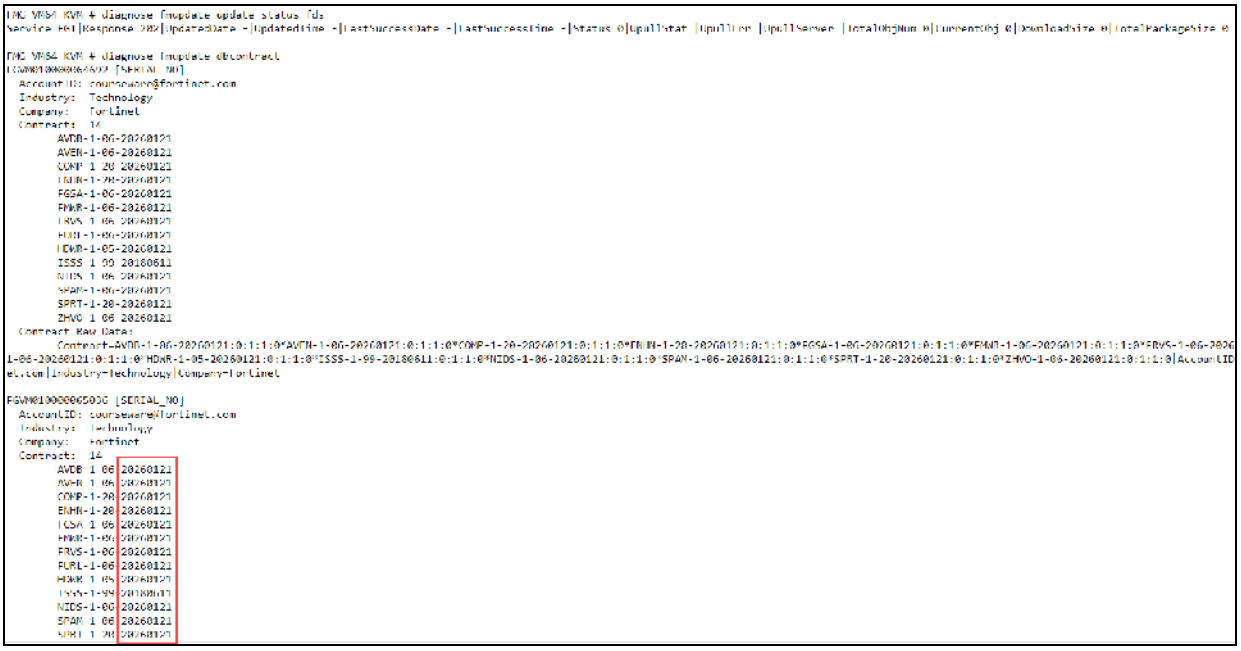
```
FMG-VM64 # diagnose fmupdate update-status fds
Service=FGT|Response=202|UpdatedDate=-|UpdatedTime=-|LastSuccessDate=-|LastSucce
ssTime=-|Status=0|UpullStat=|UpullErr= UpullServer= TotalObjNum=0|CurrentObj=0|D
ownloadSize=0|TotalPackageSize=0
```


Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

You should see that there is no information on `UpullStat` and `UpullServer`, because FortiManager is not connected to the public FDS, which would provide that information.

```
diagnose fmupdate dbcontract
```



FortiManager is operating in a closed network environment and license contracts are uploaded manually on FortiManager. You should see the contract information, which includes the types of contracts the device currently has, along with the expiry dates.

You can view the same information on the FortiGate GUI, in the **License Information** widget.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

Exercise 2: Upgrading FortiGate Firmware Using FortiManager

You can use FortiManager as your local firmware cache, and to upgrade firmware on supported devices.

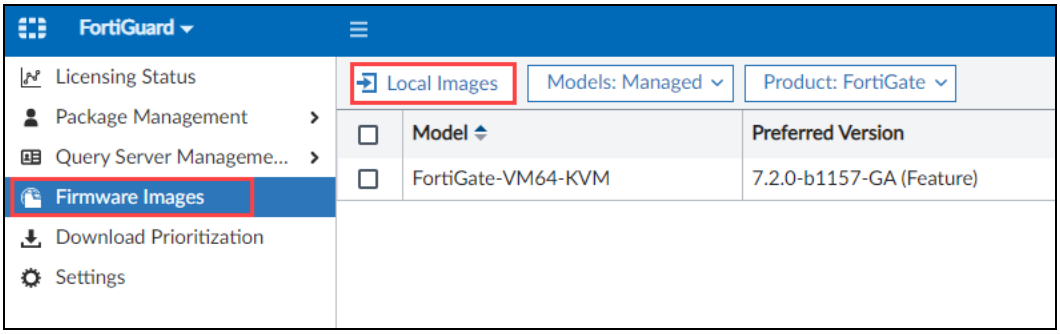
In this exercise, you will import the firmware image for FortiGate, and then upgrade both FortiGate devices using FortiManager.

To import and upgrade firmware

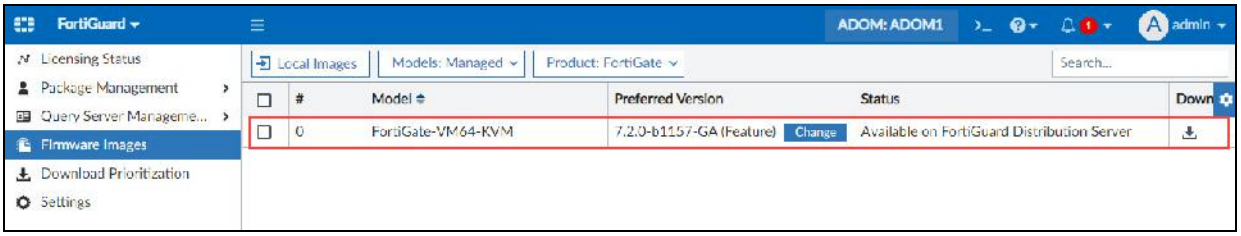
1. On the Local-Client VM, open a new private browser window, and then log in to the FortiManager GUI with the username `admin` and password `password`.

Make sure that you open a new private browser window. If you don't, your image will not appear in step 10 of this procedure.

2. Click **ADOM1**.
3. Click **FortiGuard** > **Firmware Images** > **Local Images**.



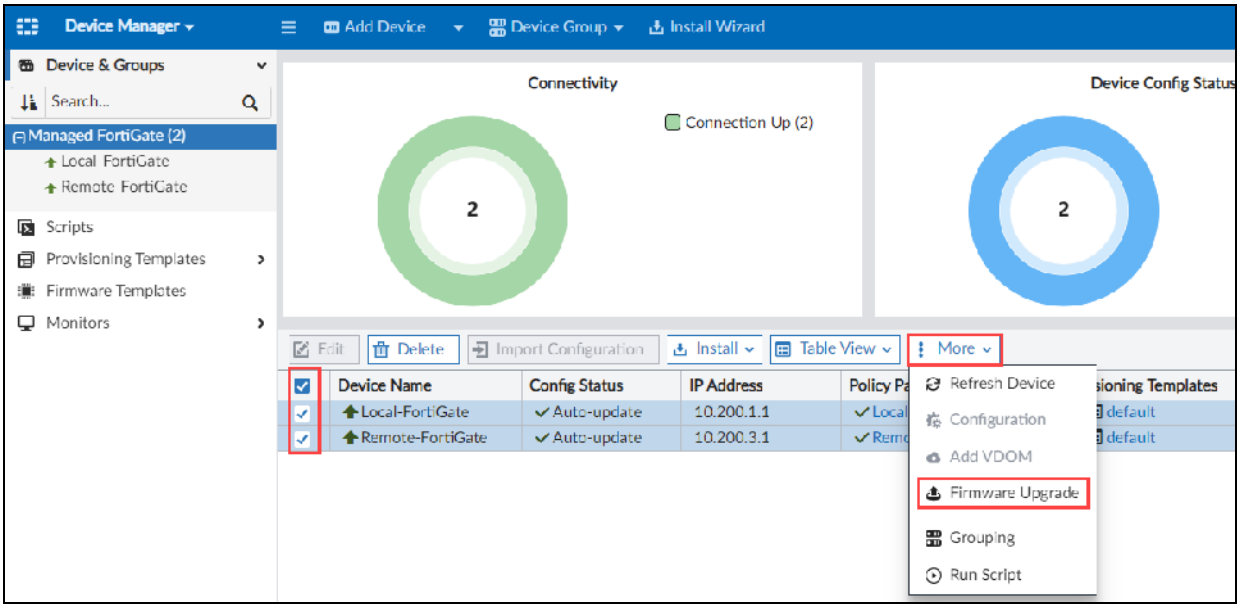
4. Click **Import**, and then click **Add Files**.
5. Click **Desktop** > **Resources** > **FortiManager** > **Additional-Configuration**, and then select `FGT_upgrade-build1255.out`.
6. Click **Open** > **OK**.
   You can see the file upload progress.
7. Click **Close**.
   You can see that the firmware image has been saved on FortiManager.



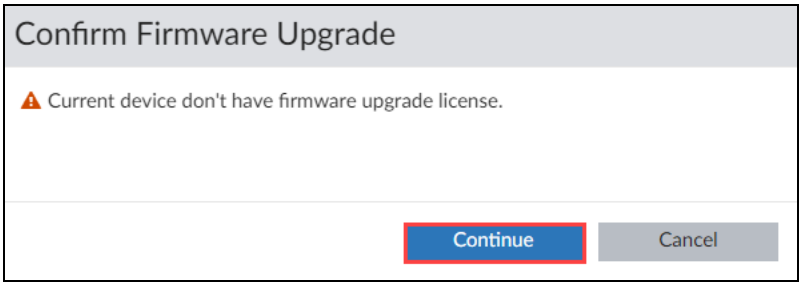
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

8. Click **FortiGuard** > **Device Manager**.
9. Select both FortiGate devices.
10. Click **More**, and then select **Firmware Upgrade**.



11. In the **Upgrade to** drop-down list, select **Local Images** > **7.2.2-b1255**.
12. Click **OK**.
13. In the **Confirm Firmware Upgrade** window, click **Continue**.

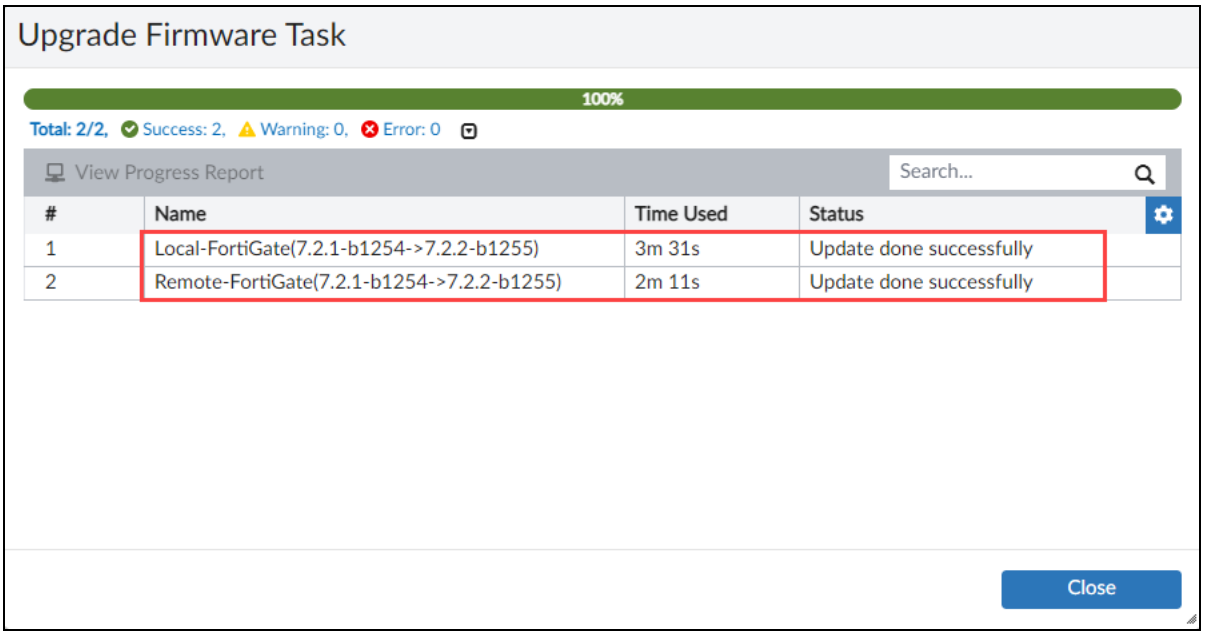


The firmware upgrade process may take several minutes.

14. Leave the **Upgrade Firmware Task** window open until the progress bar reaches 100%.
After a few minutes, you should see successful firmware upgrades for both FortiGate devices.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET



15. Click **Close**.
16. Optionally, you can open the console connection for Local-FortiGate and Remote-FortiGate to see the firmware upgrades.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT Brave-Dumps.com
© FORTINET

FORTINET

No part of this publication may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from Fortinet Inc., as stipulated by the United States Copyright Act of 1976.

Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations,and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com