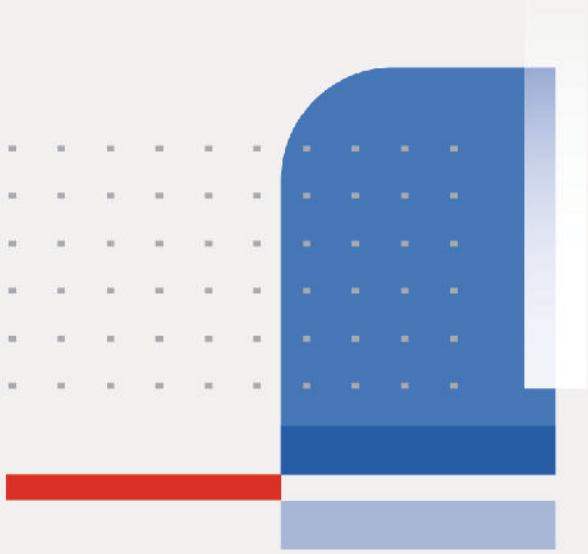
FORTINET CERTIFIED PROFESSIONAL Network Security

FortiManager Administrator Lab Guide

FortiManager 7.4

FORTINET Training Institute



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

12/18/2023

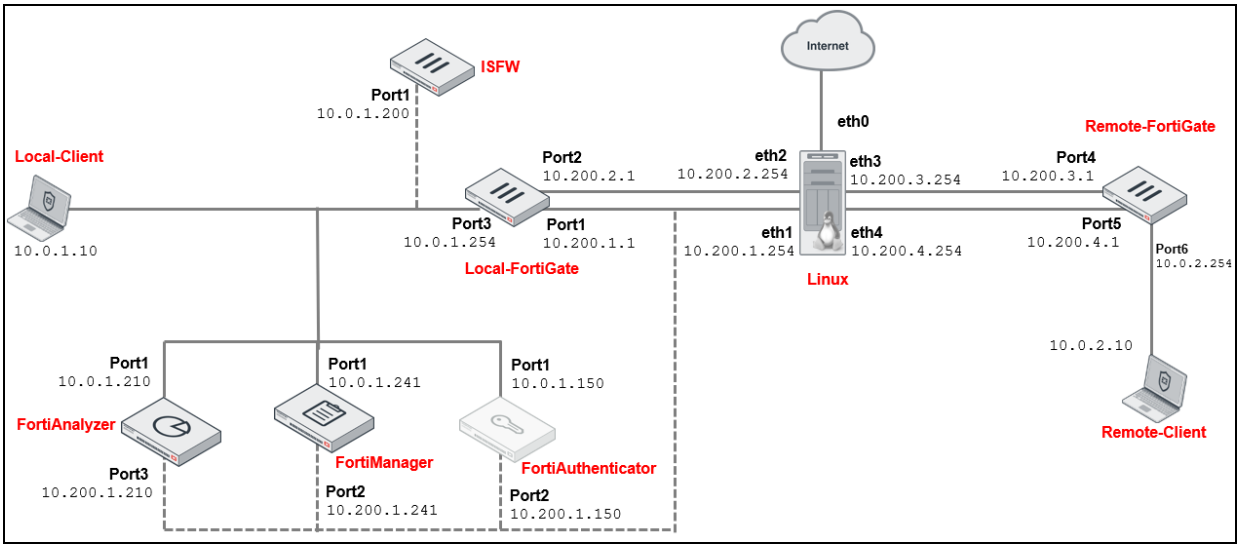
TABLE OF CONTENTS

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 13
Exercise 2: Configuring ADOMs 17
Enable ADOMs 17
View ADOM Information 17
Configure an ADOM 19
Exercise 3: Adding FortiAnalyzer to FortiManager 22
Lab 2: Administration and Management 26
Exercise 1: Creating and Assigning Administrators 27
Test Administrator Privileges 28
Restrict Administrator Access Using Trusted Hosts 29
Test the Restricted Administrator Access 30
Exercise 2: Enabling ADOM Locking (Workspace Mode) 32
Enable ADOM Locking (Workspace Mode) 32
Exercise 3: Backing Up and Restoring FortiManager 34
Back Up the FortiManager Configuration 34
Restore the FortiManager Configuration 35
Exercise 4: Monitoring Alerts and Event Logs 37
Disable Offline Mode 37
View Event Logs 37
Lab 3: Device Registration 39
Exercise 1: Configuring System Templates 40
Configure System Templates 40
Disable ADOM Locking (Workspace Mode) 42
Exercise 2: Registering a Device on FortiManager 43
Review the Central Management Configuration on Local-FortiGate 43
Add Local-FortiGate Using the Add Device Wizard 44
View the Local-FortiGate Policy Package 47
Import System Template Settings From FortiGate 48
Add Remote-FortiGate Using the Add Device Wizard 49

Assign the System Template to Local-FortiGate and Remote-FortiGate 50
Lab 4: Device-Level Configuration and Installation 53
Exercise 1: Understanding the Statuses of Managed Devices 54
Exercise 2: Installing System Template Changes on Managed Devices 57
Install System Templates 57
Check the Status of the Managed Device 59
View the Pushed Configuration on FortiGate 61
Exercise 3: Viewing the Auto Update Status and Revision History 62
Make Local Changes on Local-FortiGate 62
Make Local Changes on Remote-FortiGate 63
View the Auto Update Status and Revision History 63
View the Installation Log 65
View the Auto Update Status, Revision History, and Installation Log for Remote-FortiGate (Optional) 66
Check the Task Monitor 66
Exercise 4: Configuring Device-Level Changes 68
Change the Interface Settings of the Managed FortiGate 68
Filter Devices Based on Status 69
Configure the Administrator Account 70
Exercise 5: Installing Configuration Changes 72
Use the Install Wizard 72
View the Revision Differences 74
Exercise 6: Using Scripts 77
Configure Scripts 77
Run and Install Scripts 78
Lab 5: Policies and Objects 82
Exercise 1: Importing Policies 83
Import Policies 83
Create ADOM Revisions 86
Exercise 2: Enabling Workflow Mode 87
Exercise 3: Creating a Common Policy for Multiple Devices 97
Create Dynamic Mappings for Address Objects 97
Disable the Change Note Requirement 99
Create Dynamic Mappings for Interfaces and Device Zones 100
Import and Install a CLI Script to Delete Policies 102
Run and Install the Scripts 103
Create a Common Policy Package, an Installation Target, and Use Install On 108
Lab 6: Global ADOM Policy Configuration 115
Exercise 1: Creating and Assigning Header Policies in the Global ADOM 116
Lab 7: Diagnostics and Troubleshooting 121
Exercise 1: Diagnosing and Troubleshooting Installation Issues 123

View the Installation Preview ... 123
View the DNS Configuration ... 125
Install Device-Level Configuration Changes ... 126
Exercise 2: Troubleshooting Policy Import Issues ... 130
View the Policy Package and Objects ... 130
Review Policies and Objects Locally on Remote-FortiGate ... 131
Import a Policy Package ... 131
Check the Impact of a Partial Policy Import (Optional) ... 134
Fix a Partial Policy Import Issue ... 136
Retrieve the New Configuration From FortiManager ... 137
Lab 8: Additional Configuration ... 141
Exercise 1: Examining FortiGuard Management ... 142
Diagnose FortiGuard Issues ... 143
Exercise 2: Upgrading FortiGate Firmware Using FortiManager ... 145

Network Topology



Lab 1: Initial Configuration

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

Objectives

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

Time to Complete

Estimated: 30 minutes

Prerequisites

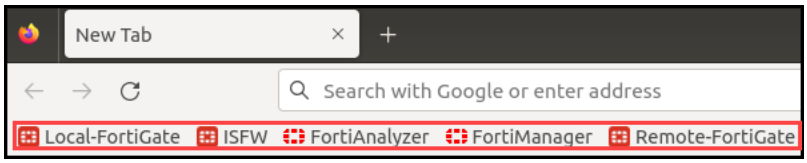
This lab environment is also used for *FortiGate Security 7.4* and *FortiGate Infrastructure 7.4* training and initializes in a different state than is required for *FortiManager 7.4* training.

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

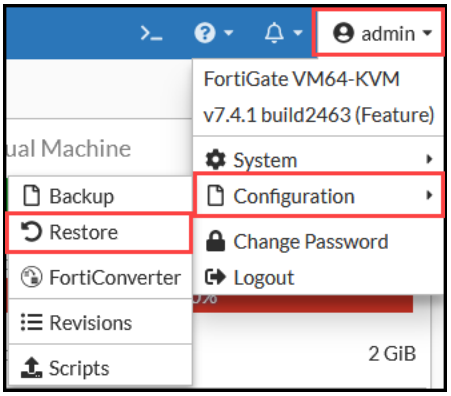
To restore the Remote-FortiGate configuration file

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`.

You can access all devices in this lab by clicking the bookmarks with their names.



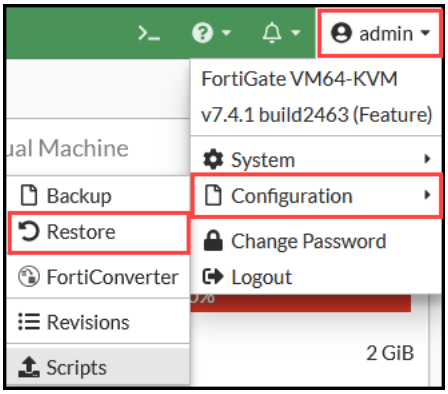
2. In the upper-right corner, click **admin**, and then click **Configuration** > **Restore**.



3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop** > **Resources** > **FortiManager-Administrator** > **Lab1-Introduction** > **Lab1-Initials**, select `Remote-FortiGate-Initial.conf`, and then click **Select**.
5. Click **OK**.
6. Click **OK** to reboot.

To restore the Local-FortiGate configuration file

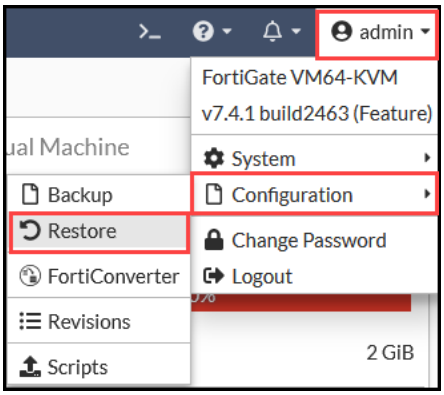
1. On the Local-Client VM, open a browser or a new browser tab, and then log in to the Local-FortiGate GUI at `10.0.1.254` with the username `admin` and password `password`.
2. In the upper-right corner, click **admin**, and then click **Configuration** > **Restore**.



3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop** > **Resources** > **FortiManager-Administrator** > **Lab1-Introduction** > **Lab1-Initials**, select `Local-FortiGate-Initial.conf`, and then click **Select**.
5. Click **OK**.
6. Click **OK** to reboot.
7. After both devices restart, close the browsers or browser tabs for the Remote-FortiGate GUI and Local-FortiGate GUI.

To restore the ISFW configuration file

1. On the Local-Client VM, open a browser or a new browser tab, and then log in to the ISFW GUI at `10.0.1.200` with the username `admin` and password `password`.
2. In the upper-right corner, click **admin**, and then click **Configuration** > **Restore**.



3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop** > **Resources** > **FortiManager-Administrator** > **Lab1-Introduction** > **Lab1-Initials**, select `ISFW-Initial.conf`, and then click **Select**.
5. Click **OK**.
6. Click **OK** to reboot.

Exercise 1: Examining the Initial Configuration

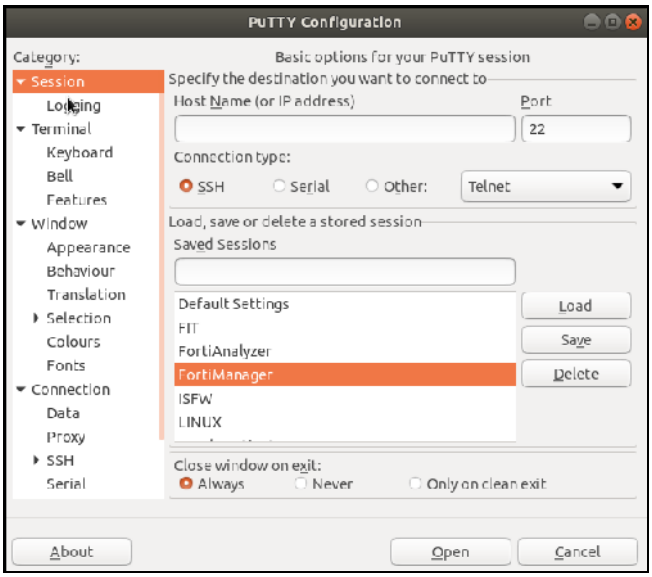
In this exercise, you will explore the basic configuration settings on the FortiManager CLI and GUI.

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. On the Local-Client VM, on the task bar, click the shortcut for PuTTY, and then open the saved session named **FortiManager**.



2. If you get a security alert message, click **Accept**, and then log in to FortiManager with the username `admin` and password `password`.
3. 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.	

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

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?	

5. 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.	

6. 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.	
`show system ntp`	Which server is configured for NTP? By default, Fortinet servers are configured for NTP.	

7. 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.	

8. 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
```

9. 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.

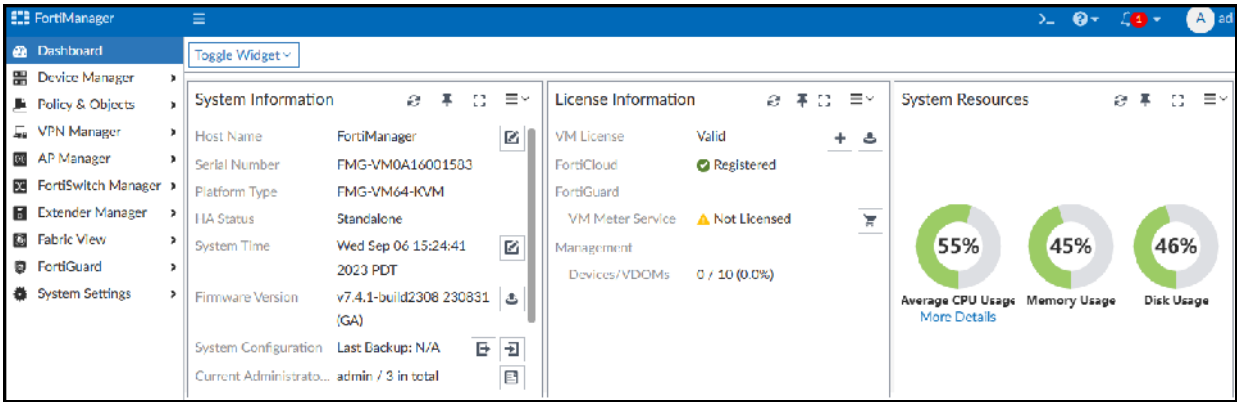
To examine the initial configuration using the GUI

1. On the Local-Client VM, open a browser, and then log in to the FortiManager GUI at `10.0.1.241` with the username `admin` and password `password`.

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

If a security alert appears, accept the self-signed certificate or security exemption.

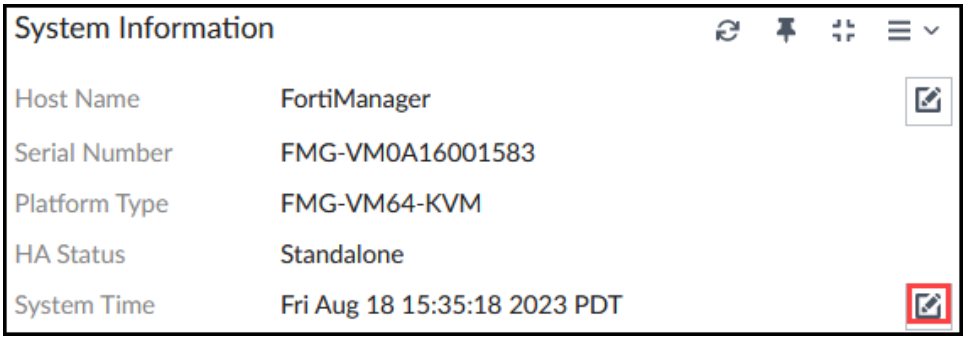
The dashboard shows several widgets that display information, such as **System Information**, **License Information**, **System Resources**, and more.



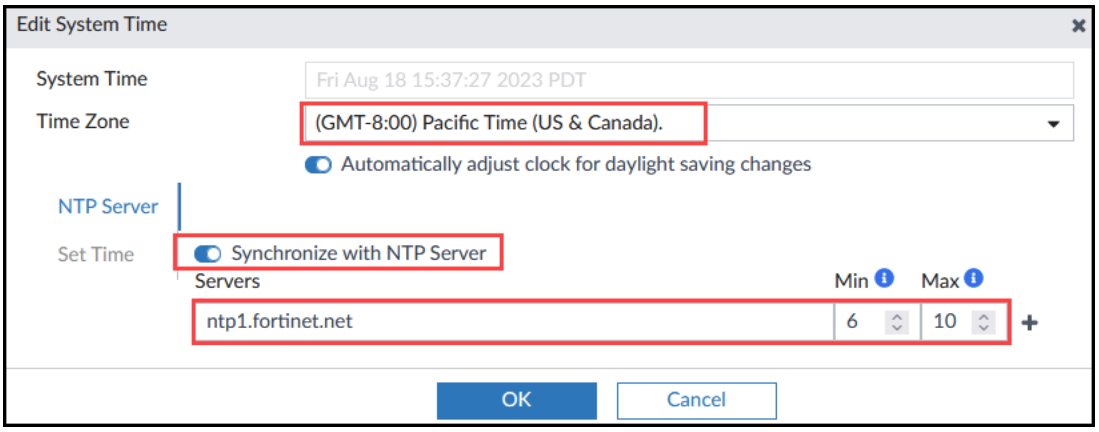
2. In the **System Information** and **License Information** widgets, locate the following information:
   - Firmware version
   - Administrative domain status
   - System time and time zone
   - License status (VM)

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

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



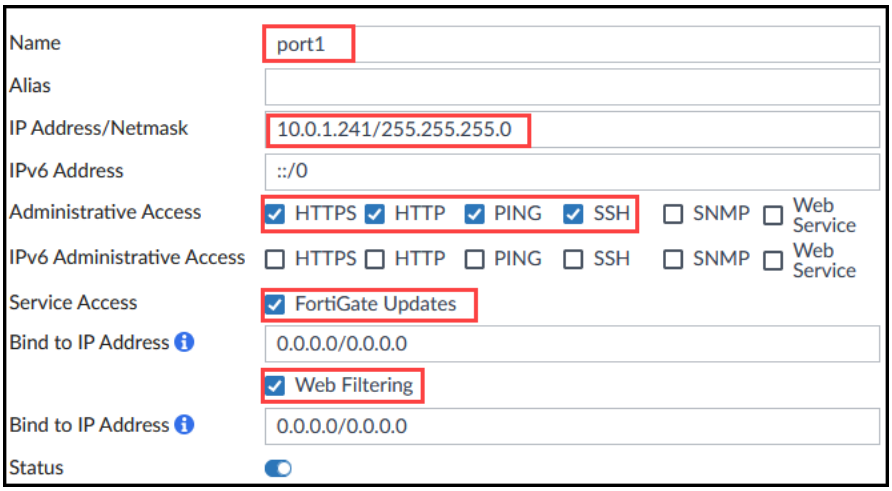
This displays the same information as the `get system ntp` and `show system ntp` CLI commands.



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

4. Click **System Settings** > **Network** > **port1**.
5. Select **port**, and then click **Edit**.

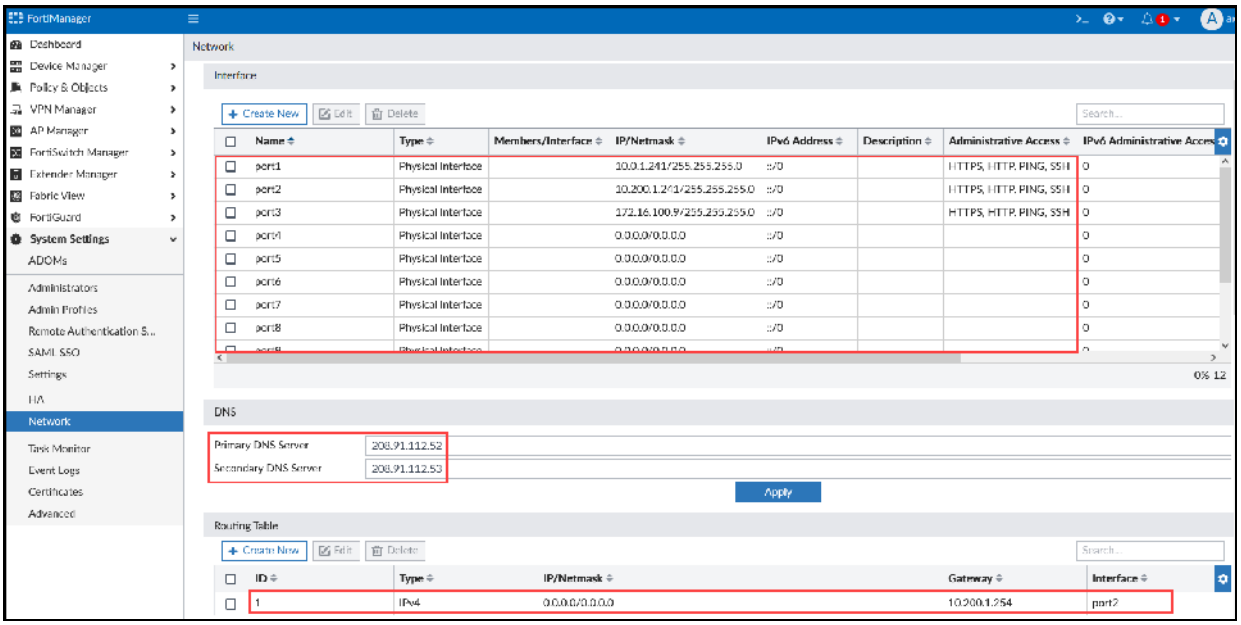
   This section displays information about the port1 management interface, including the IP address, administrative access protocols, and service access. This displays the same information as the `show system interface` CLI command.



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.

6. 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.



7. Leave the GUI session open for the next exercise.

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.

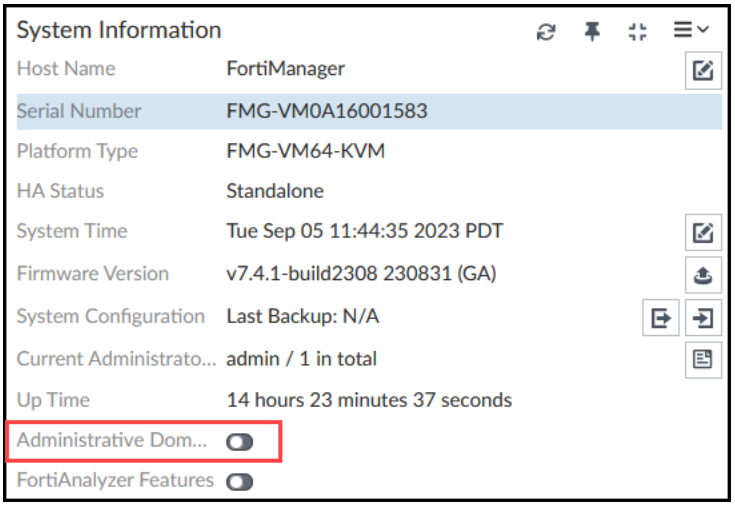
Enable ADOMs

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

You will enable ADOMs on FortiManager.

To enable ADOMs

1. On the FortiManager GUI, click **Dashboard**.
2. In the **System Information** widget, enable **Administrative Domain**.



3. Click **OK**.
   FortiManager logs you out of the GUI.

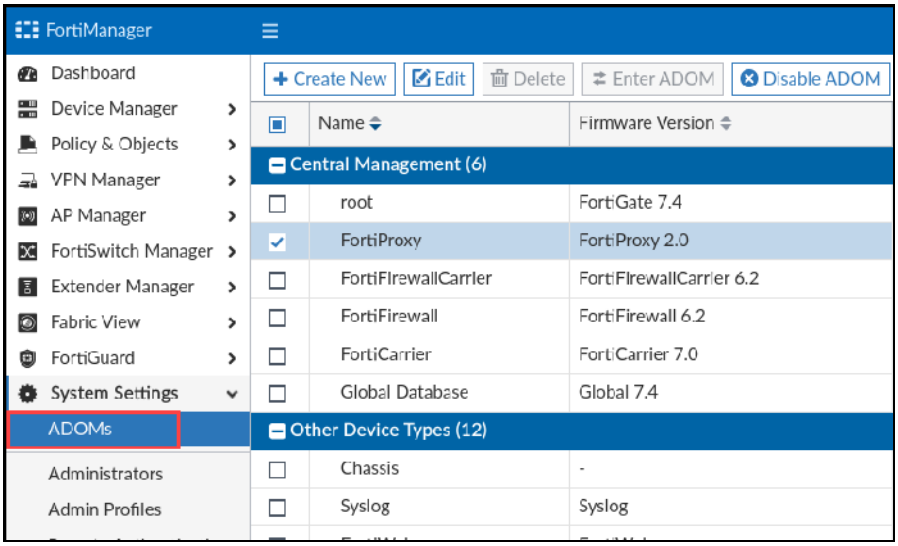
View ADOM Information

Before you create new ADOMs, you should know which types of ADOMs 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.

3. Click **System Settings** > **ADOMs**.



4. On the Local-Client VM, click the shortcut for PuTTY, and then open the saved session named **FortiManager**.
5. Log in to the FortiManager CLI with the username `admin` and password `password`.
6. Enter the following command to view the ADOMs that FortiManager currently supports and the type of device you can register to each ADOM:

The CLI output is easier to read if you maximize the console 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  7.3257
124      enabled  FAC     6.0   2       FortiAuthenticator  Normal  Policy & Device VPNs  20.302  7.3257
112      enabled  FCH     4.0   2       FortiCache          Normal  Policy & Device VPNs  0.0     7.3257
104      enabled  FOC     7.0   0       FortiCarrier        Normal  Policy & Device VPNs  21.336  7.3257
114      enabled  FCT     7.0   0       FortiClient         Normal  Policy & Device VPNs  21.336  7.3257
122      enabled  FDD     6.0   1       FortiDDoS           Normal  Policy & Device VPNs  20.302  7.3257
151      enabled  FDC     3.0   3       FortiDeceptor       Normal  Policy & Device VPNs  0.0     7.3257
149      enabled  FFW     6.0   2       FortiFirewall       Normal  Policy & Device VPNs  20.302  7.3257
159      enabled  FWC     6.0   2       FortiFirewallCarrier Normal Policy & Device VPNs  20.302  7.3257
106      enabled  FML     6.0   4       FortiMail           Normal  Policy & Device VPNs  20.302  7.3257
118      enabled  FMG     7.0   0       FortiManager        Normal  Policy & Device VPNs  21.336  7.3257
126      enabled  FPX     2.0   0       FortiProxy          Normal  Policy & Device VPNs  0.0     7.3257
120      enabled  FSA     4.0   0       FortiSandbox        Normal  Policy & Device VPNs  0.0     7.3257
110      enabled  FWB     6.0   3       FortiWeb            Normal  Policy & Device VPNs  20.302  7.3257
116      enabled  LOG     0.0   0       Syslog              Normal  Policy & Device VPNs  0.0     7.3257
128      enabled  FSF     7.0   0       Unmanaged_Devices   Normal  Policy & Device VPNs  21.336  7.3257
102      enabled  Chassis 6.0   0       Chassis             Normal  Policy & Device VPNs  20.302  7.3257
3        enabled  FOS     7.0   4       root                Normal  Policy & Device VPNs  21.336  7.3257
10       enabled  FOS     7.0   4       Global              Normal  Policy & Device VPNs  21.336  7.3257
---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 CLI session.

Configure an ADOM

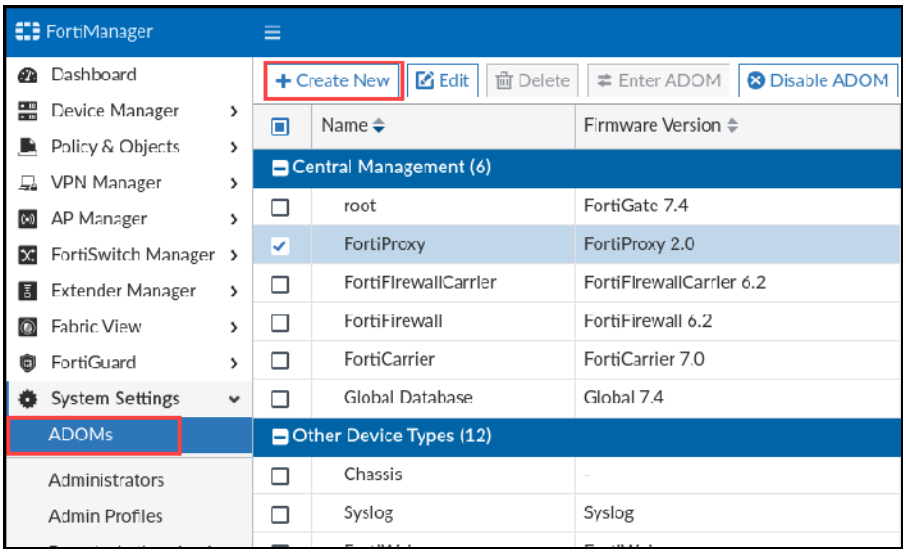
By default, when you enable ADOMs, FortiManager includes several ADOMs based on supported device types. The **root** ADOM is based on the FortiGate ADOM type.

When you create a new ADOM, you must specify its type. The ADOM type must match the device type you are planning to add later. For example, if you want to create an ADOM for FortiGate devices, you must select **FortiGate** as the ADOM type. The exception to this rule is the **Fabric** type, which allows you to add FortiGate and other types of devices. Additionally, you must select the firmware version for each new ADOM. This is because 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 an ADOM

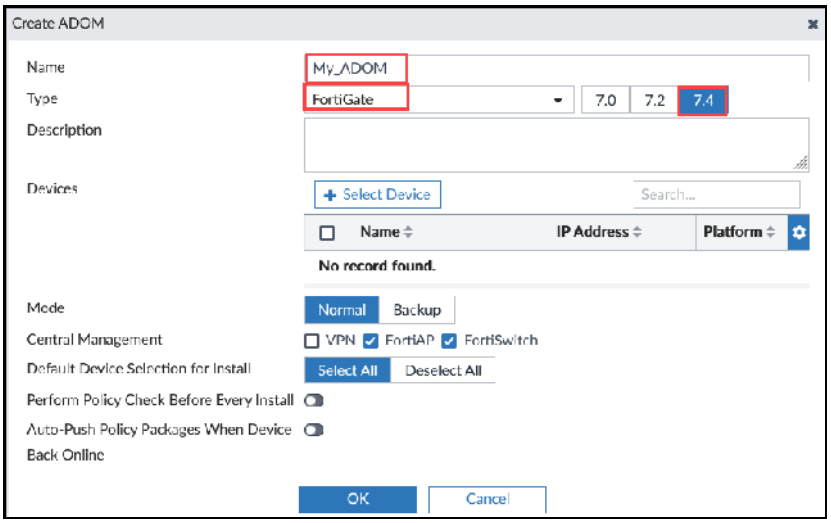
1. Continuing on the FortiManager GUI, click **System Settings** > **ADOMs** > **Create New**.



2. Configure the following settings:

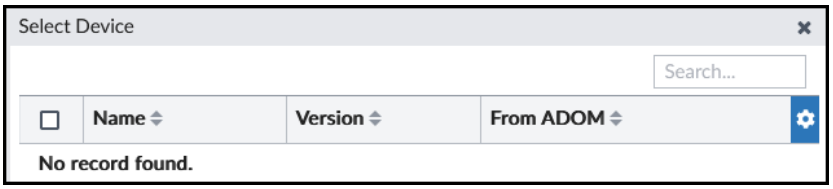
Field	Value
Name	My_ADOM
Type	Select **FortiGate** and **7.4**.

Your configuration should look like the following example:



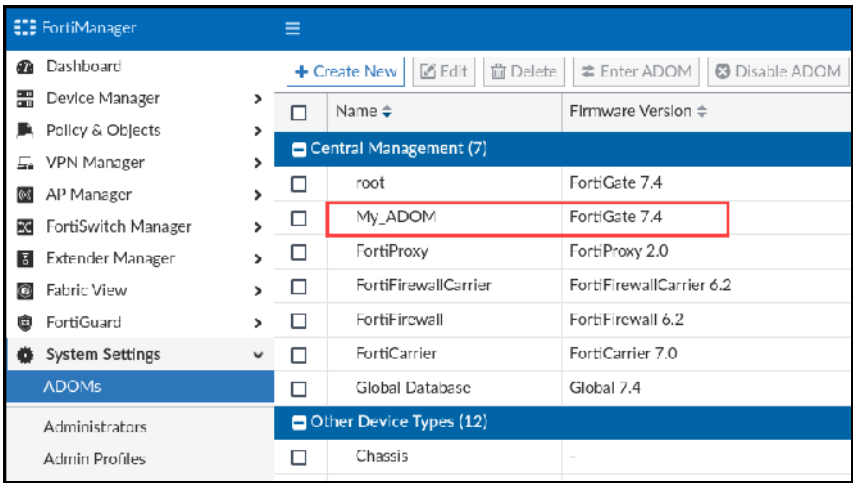
3. Click **Select Device**.

   In the **Select Device** window, if any devices were already registered to FortiManager, you could select them and add them to the ADOM. However, in this lab, the list is empty because no devices are registered.

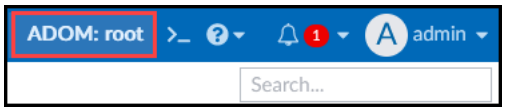


4. Click **Cancel**.
5. Keep the default values for all other settings, and then click **OK**.

   You should see your new ADOM in the list.

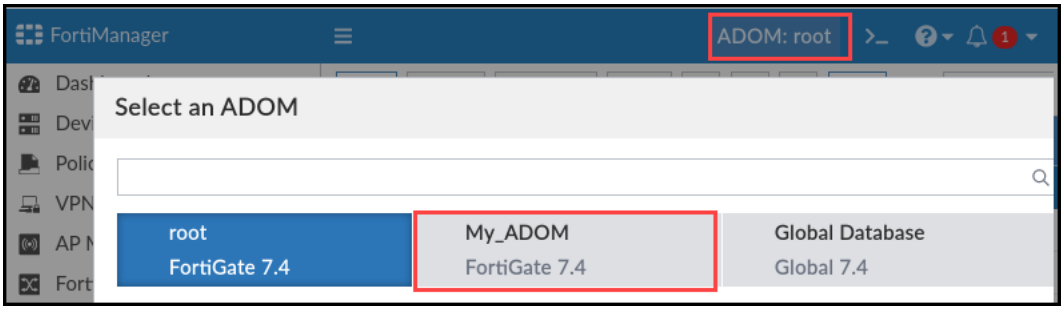


You can switch between ADOMs on the GUI without having to log out and log back in again. To switch between ADOMs, in the upper-right corner, click **ADOM:xxxx**, and then in the list, select the ADOM that you want.



Your administrator privileges determine which ADOMs you can access.

6. Click **ADOM:root**, and then click **My_ADOM** to switch to the new ADOM.



7. Leave the GUI session open for the next exercise.

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.

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

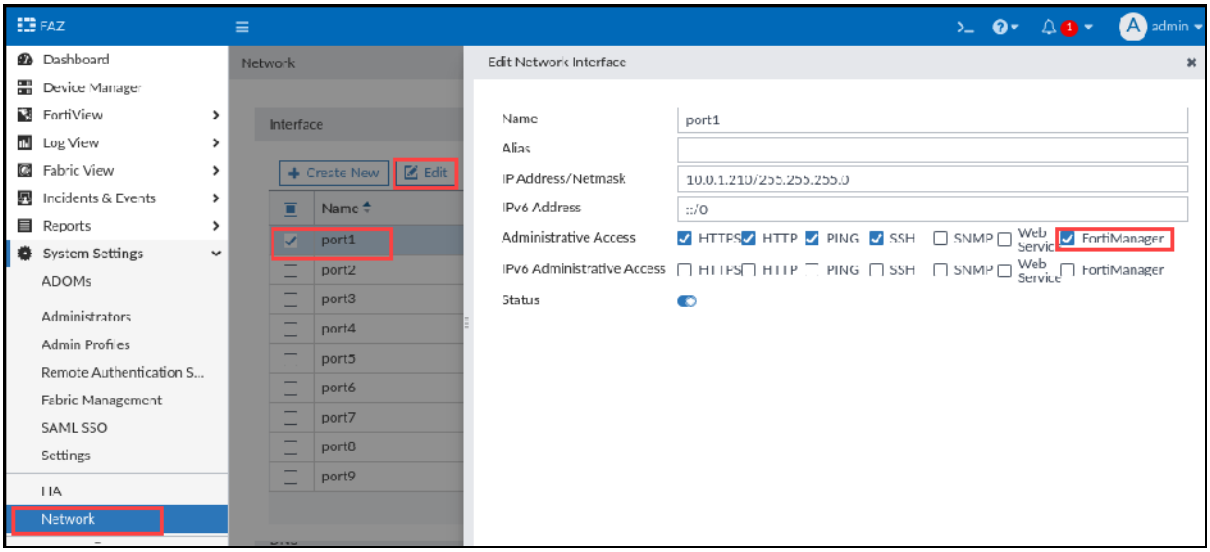
In this exercise, you will add FortiAnalyzer to FortiManager, so that you can manage FortiAnalyzer from FortiManager for logging and reporting.

To add FortiAnalyzer to FortiManager

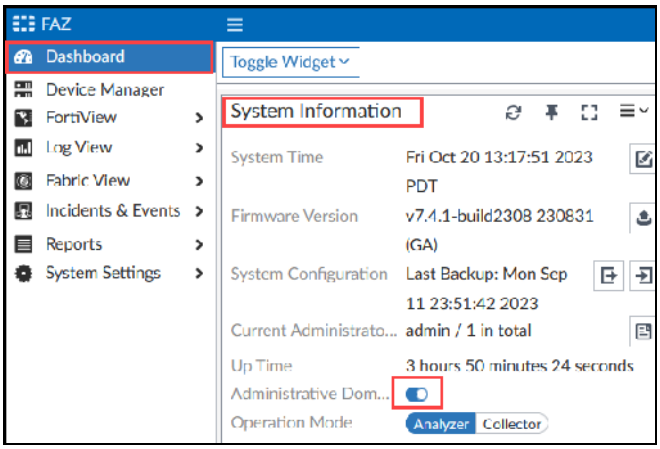
1. On the Local-Client VM, open a browser, and then log in to the FortiAnalyzer GUI at `10.0.1.210` with the username `admin` and password `password`.

   Before you add FortiAnalyzer to FortiManager, you must select the **FortiManager** administrative access checkbox on the FortiAnalyzer GUI.

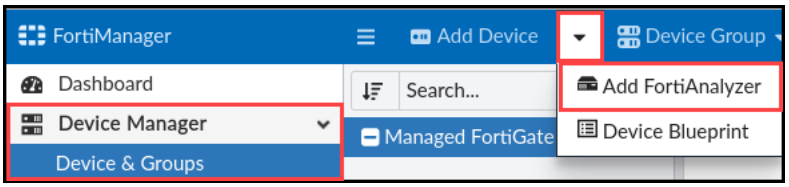
2. Click **System Settings** > **Network**.
3. Select **port1**, and then click **Edit**.
4. In the **Administrative Access** field, select the **FortiManager** checkbox.



5. Click **OK**.
6. Click **Dashboard**.
7. In the **System Information** widget, enable **Administrative Domain**.



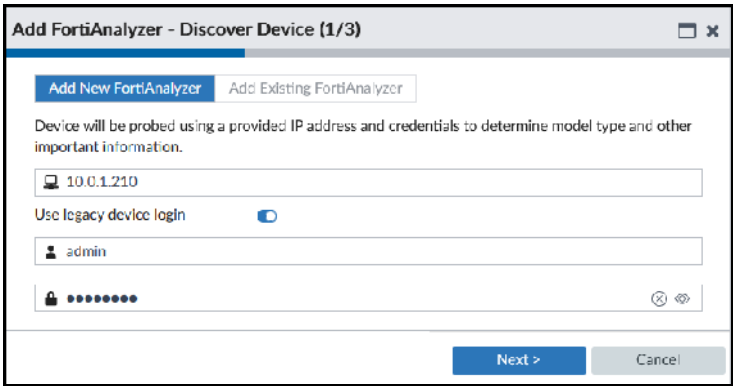
8. Click **OK**.
9. Return to the window, or tab, with the FortiManager GUI session.
10. Click **Device Manager**, and then click **Device & Groups**.
11. In the **Add Device** drop-down list, select **Add FortiAnalyzer**.



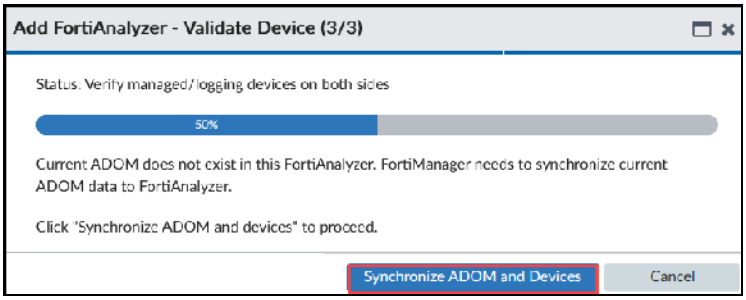
12. In the **Add FortiAnalyzer** wizard, configure the following settings:

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

13. Click **Next**.



14. Click **Next** one more time.
15. Click **Synchronize ADOM and Devices**.



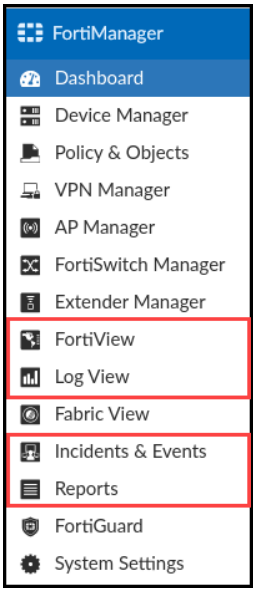
If the FortiManager ADOM does not exist on the FortiAnalyzer you are adding, you are prompted to **Synchronize ADOM and Devices**. This process adds the new ADOM to FortiAnalyzer, together with any existing devices in that ADOM.

Using the **Synchronize ADOM and Devices** option creates the ADOM on FortiAnalyzer with unlimited disk space.

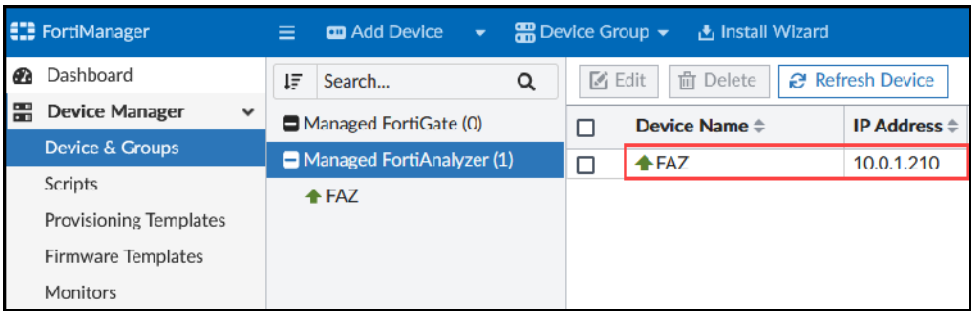
The FortiAnalyzer administrator should set the disk allocation to an appropriate size.

16. Click **Finish**.

    Now that you have added FortiAnalyzer to FortiManager, you will notice that more modules appear—**FortiView**, **Log View**, **Incidents & Events**, and **Reports**.



17. Click **Device Manager** > **Device & Groups**.
18. Expand **Managed FortiAnalyzer** to see that the FortiAnalyzer is listed and the connection is up.



You may need to refresh the page to see the FortiAnalyzer added.

19. Log out of the FortiManager GUI.

Lab 2: Administration and Management

In this lab, you will create and then configure a new administrator user. You will also restrict administrator access based on administrator profiles, 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, and view alert messages in the event logs.

Objectives

- Configure an administrator and restrict access to a newly created ADOM
- Enable and test ADOM locking
- Back up FortiManager, restore the backup, and disable offline mode

Time to Complete

Estimated: 45 minutes

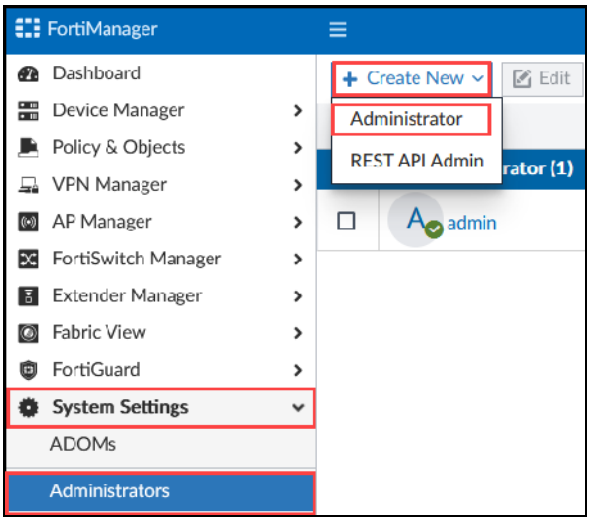
Exercise 1: Creating and Assigning Administrators

In this exercise, you will create a new 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

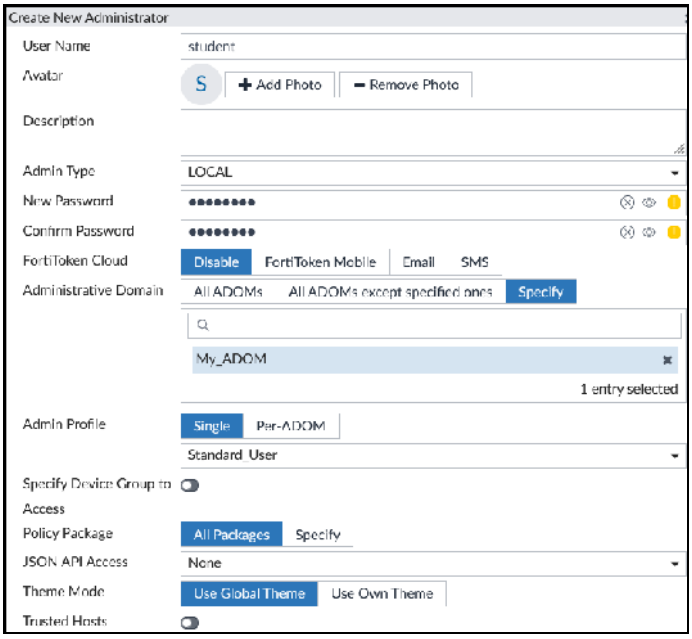
1. Log in to the FortiManager GUI with the username `admin` and password `password`.
2. Click **root**.
3. Click **System Settings** > **Administrators** > **Create New** > **Administrator**.



4. 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

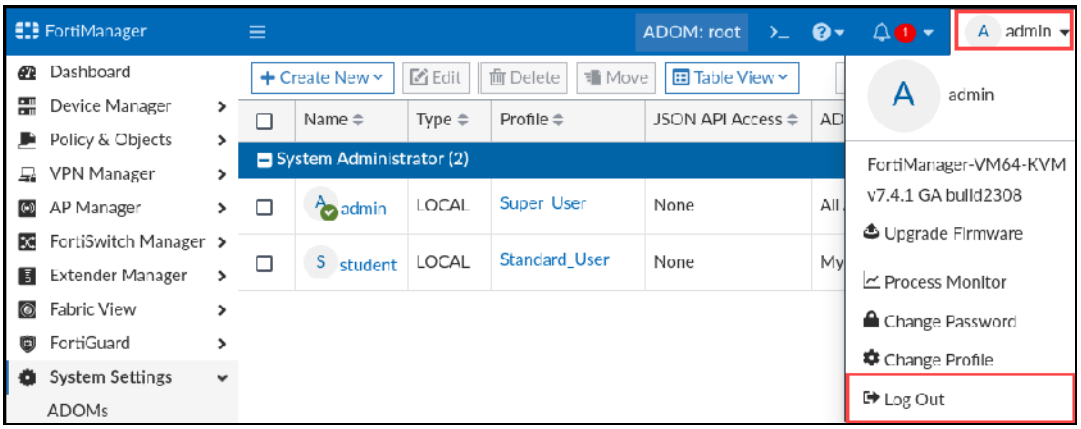
Your configuration should look like the following example:



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.

5. Keep the default values for all other settings, and then click **OK**.
6. In the upper-right corner, click **admin**, and then click **Log Out**.

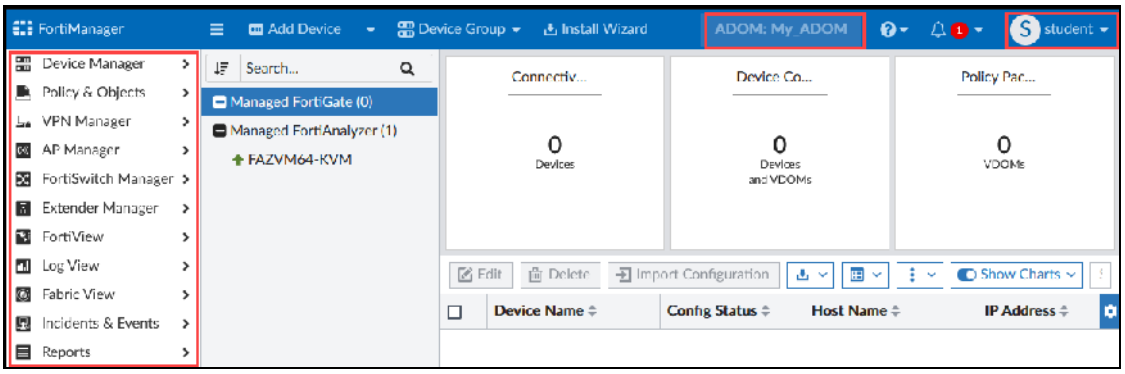


Test Administrator Privileges

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

To test administrator privileges

1. Log in to the FortiManager GUI with the username `student` and password `fortinet`.
2. Notice that this user did not have the option to select a specific ADOM and it is limited to the **My_ADOM** administrative domain.
3. Notice that the **Dashboard**, **System Settings**, and **FortiGuard** modules are not available to this user.



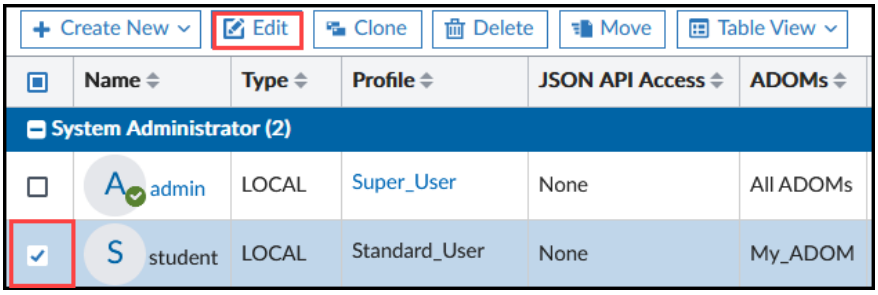
The preceding image shows an example of the effects of controlling or restricting administrator access based on administrative profiles and ADOMs.

Restrict Administrator Access Using Trusted Hosts

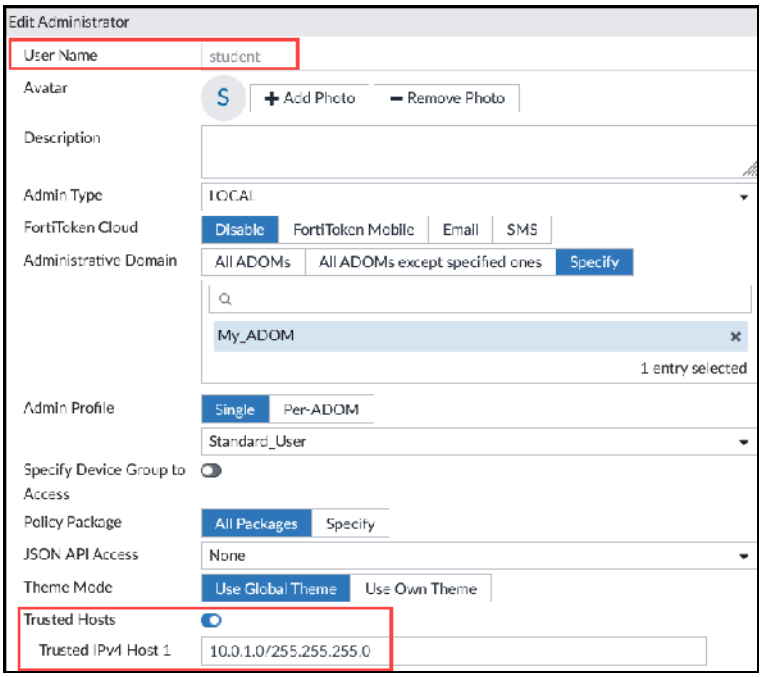
You will restrict access to FortiManager by configuring trusted hosts for the new administrator account. After the configuration, the **student** account must connect from a specific trusted subnet to be able to access FortiManager.

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** > **Administrators**.
5. Edit the **student** account.



6. Enable **Trusted Hosts**.
7. In the **Trusted IPv4 Host 1** field, type `10.0.1.0/255.255.255.0`.



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

Test the Restricted Administrator Access

You will confirm that the **student** account cannot access FortiManager from outside the subnet 10.0.1.0/24.

To test the restricted administrator access

1. Log in to the Remote-Client VM with the username `administrator` and password `password`.
2. Open a browser, and then go to `https://10.200.1.241`.
3. 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 Remote-Client VM, which has the IP address 10.0.2.10, your login authentication fails. This is because you restricted this account to log in only from 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 FortiManager.

4. Return to the Local-Client VM.
5. Ensure that you are still logged in to the FortiManager GUI as `admin`, and then enter the **root** ADOM.
6. Edit the **student** account to disable **Trusted Hosts**.
7. Click **OK**.

8. 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 subnet.

9. On the Remote-Client VM, log out of the FortiManager GUI, but leave the local Linux session in that VM open for the next exercise.

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

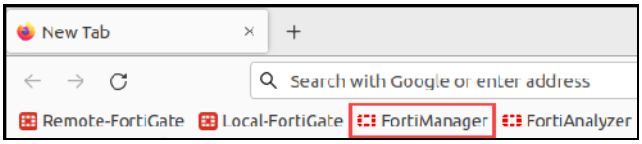
Enable ADOM Locking (Workspace Mode)

Before you enable ADOM locking, ensure that you notify all FortiManager administrators and ask them to save any unsaved changes that they made on FortiManager that they want to keep, because enabling ADOM locking terminates all management sessions.

To enable ADOM locking (workspace mode)

1. On the Local-Client VM, log in to the FortiManager GUI with the username `admin` and password `password`.
2. Click **My_ADOM**.
3. Browse to **System Settings** > **Advanced** > **Workspace**.
4. Click **Workspace(ALL ADOMs)**, click **Apply**, and then click **OK**.
   FortiManager logs you out.
5. Log in to the FortiManager GUI with the username `student` and password `fortinet`.
6. At the top of the page, click the lock icon.

   The lock icon changes from unlocked to locked, and the background from blue to green.
7. On the Remote-Client VM, open a browser, and then click the **FortiManager** bookmark.



8. Log in to the FortiManager GUI with the username `admin` and password `password`.
   Notice that the lock icon is locked for **My_ADOM**.
9. Hover over the lock icon.
   The name of the administrator who locked the ADOM appears, along with the date and time it was locked.

10. Click **My_ADOM**.
11. Log out of the FortiManager **admin** account.
12. Return to the Local-Client VM, and then log out of the FortiManager **student** account.

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

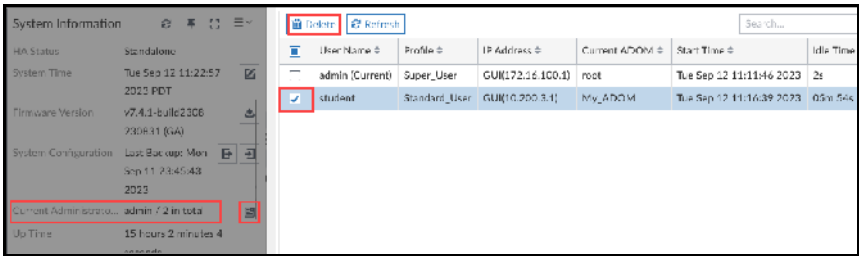
In this example, when the **student** administrator locked **My_ADOM**, and then logged out, FortiManager unlocked **My_ADOM**.

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, you can delete the session manually using the GUI or CLI. You must be logged in using an account with the required permissions to be able to close other administrator sessions.

On the GUI, on the **Dashboard**, go to the **System Information** widget, and then click the **Current Session List** icon beside **Current Administrators**.



On the CLI, enter the `diagnose system admin-session list` command to find the ID of all current sessions, and then enter the `diagnose system admin-session kill <id>` command to delete the session you want to close.

```
FortiManager# diagnose sys admin-session list
*** entry 1 ***
session_id: 6671 (seq: 0)
username: admin
admin template: admin
from: GUI(10.0.1.10) (type 1)
profile: Super_User (type 3)
adom: My_ADOM
session length: 1308 (seconds)
idle: 284 (seconds)
...
FortiManager # diagnose sys admin-session kill 6671
```

Exercise 3: Backing Up and Restoring FortiManager

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

In a production scenario, it is a best practice to back up the device configuration before you make any configuration changes. If the new configuration does not perform as expected, you can revert to the last working configuration.

FortiManager configuration files are not stored in plain text 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.

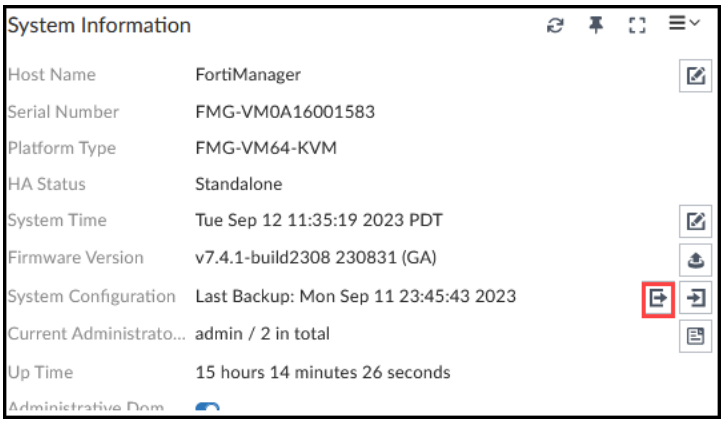
Back Up the FortiManager Configuration

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 page, click the lock icon to lock the ADOM.

1. Click **Dashboard**.
2. In the **System Information** widget, in the **System Configuration** section, click the **backup** icon.



3. Click to disable the **Encryption** option.
4. Click **OK**.

   The backup process starts and the resulting file is saved automatically to the **Downloads** folder.

5. Go to the **Downloads** folder, and then rename this file to `Lab2.dat`.
6. Return to the FortiManager GUI, and then click **System Settings** > **Administrators**.
7. Right-click **student**, and then click **Delete**.
8. Click **OK**.

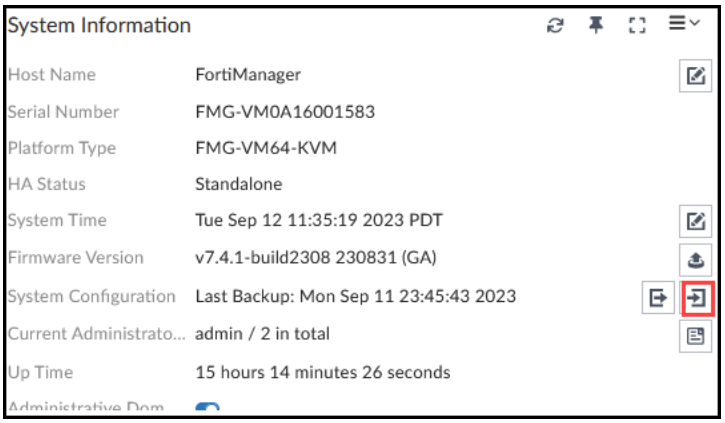
Restore the FortiManager Configuration

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

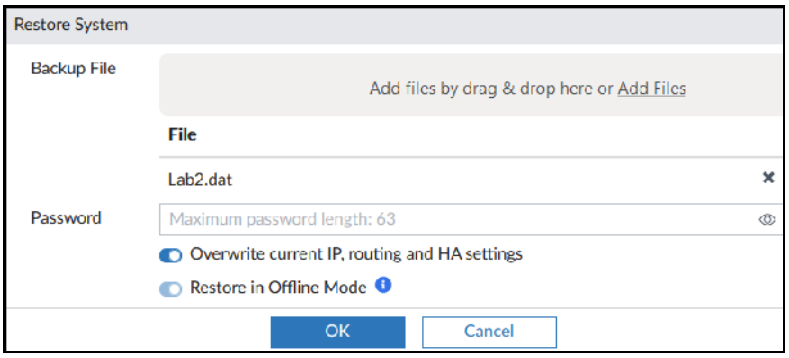
- **Overwrite current IP, routing and HA settings**: By default, this option is enabled. If FortiManager has an existing configuration, restoring a backup overwrites everything, including the current IP address, routing, and HA settings. If you disable this option, FortiManager restores the configuration settings that are related to the device information and global database information, but preserves 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 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. To reenable the communication, you must disable **Offline Mode**.

To restore FortiManager

1. Continuing on the FortiManager GUI, click **Dashboard**.
2. In the **System Information** widget, in the **System Configuration** section, click the **restore** icon.



3. Click **Add Files**, and then browse to the **Downloads** folder.
4. Click the `Lab2.dat` backup file, and then click **Select**.
   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 uploads the file and then reboots. This process takes a couple of minutes to finish.
7. Wait for FortiManager to reboot, and then log in to the FortiManager GUI with the username `admin` and password `password`.
8. Click **root**.
9. Click **System Settings** > **Administrators**, and then verify that the **student** administrator account was restored from the backup file.
10. Keep the FortiManager GUI session open for the next exercise.

Exercise 4: Monitoring Alerts and Event Logs

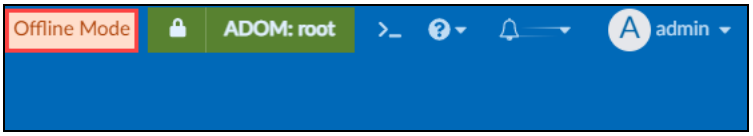
In this exercise, you will disable offline mode, which is enabled by default when the FortiManager backup configuration is restored. Then, you will view the messages displayed in the event logs.

Disable Offline Mode

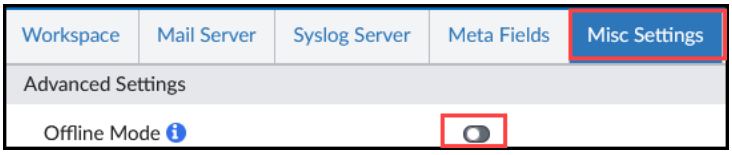
You will disable offline mode on FortiManager.

To disable offline mode

1. Continuing on the FortiManager GUI session, click the lock icon to lock the ADOM.
   You should see a label at the top of the page indicating that FortiManager is in **Offline Mode**.



2. Click **System Settings** > **Advanced** > **Misc Settings**.
3. Disable **Offline Mode**.



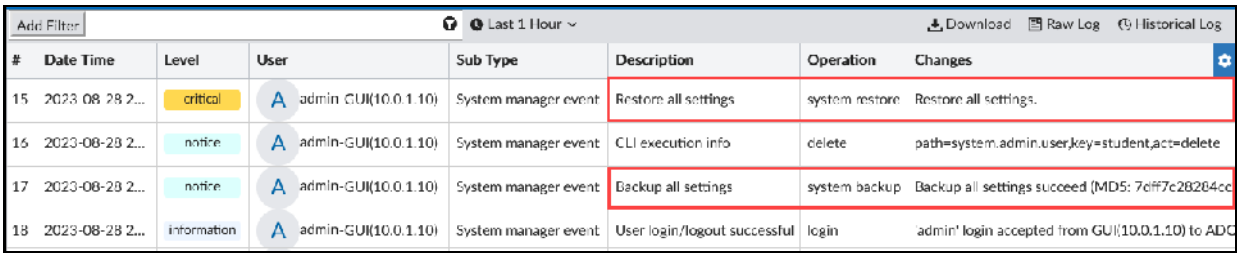
4. Click **Apply**.
5. Refresh the page, and then confirm that the **Offline Mode** label disappears.
   At this point, FortiManager can establish a management connection with the managed devices.

View Event Logs

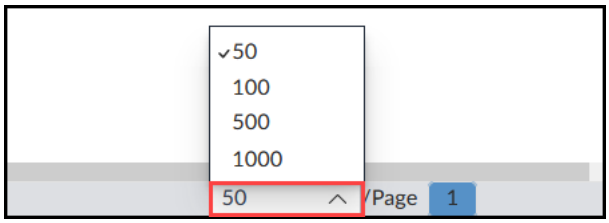
You will view the logs under **Event Logs**.

To view event logs

1. Continuing on the FortiManager GUI, click **System Settings** > **Event Logs**.
   You should see a **Restore all settings** message, along with other messages related to recent actions.



If you cannot find the events you are looking for, you can try modifying the time frame at the top of this page, or increase the number of entries displayed by selecting a higher value at the bottom of the page.



2. Log out of the FortiManager GUI.

Lab 3: Device Registration

In this lab, you will explore the common operations performed using the device manager. You will use the device manager to add FortiGate devices and apply system templates.

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

Exercise 1: Configuring System Templates

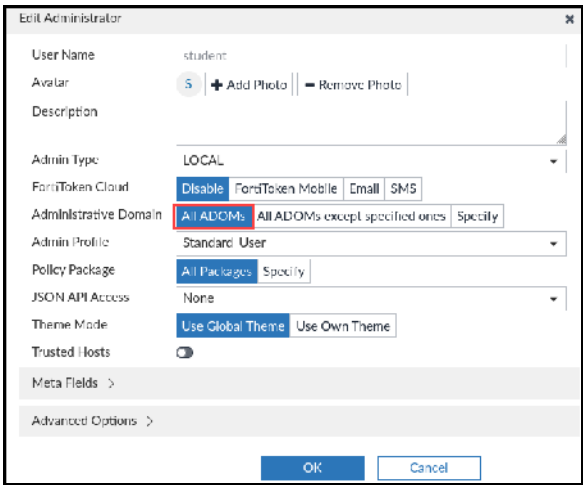
You can configure system templates on FortiManager to provision common system-level settings on FortiGate devices. You can configure the templates in advance, and then apply them either to FortiGate devices when they are first added to FortiManager or to FortiGate devices that FortiManager is currently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

Configure System Templates

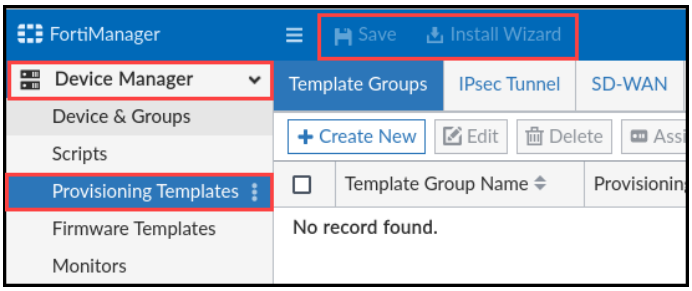
You will configure and apply system templates to FortiGate.

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** > **Administrators**.
4. Select the **student** checkbox, click **Edit**, and then in the **Administrative Domain** field, select **All ADOMs**.



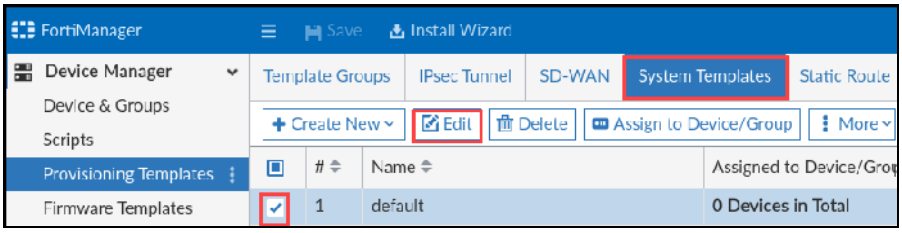
5. Click **OK**.
6. Log out of the FortiManager **admin** account.
7. Log in to the FortiManager GUI with the username `student` and password `fortinet`.
8. Click **My_ADOM**.
9. Click **Device Manager** > **Provisioning Templates**.
   You will notice that you have read-only access.



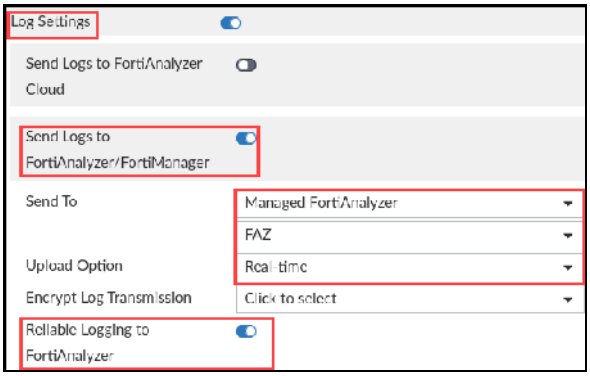
This is because when ADOM locking is enabled, you must lock the ADOM before making configuration changes.

10. At the top of the page, click the lock icon to lock **My_ADOM**.

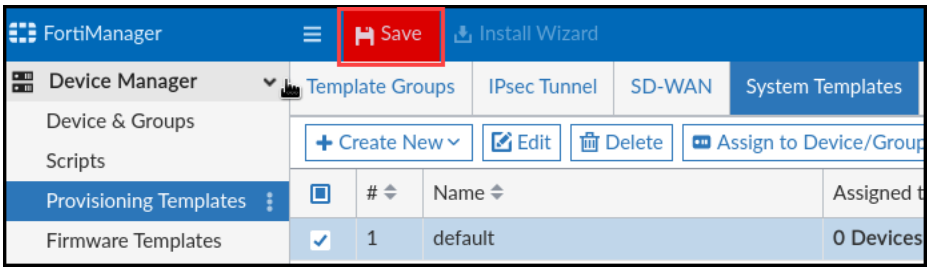
11. On the **System Templates** tab, select the **default** checkbox, and then click **Edit**.



12. Scroll down to the **Log Settings** section, and then enable **Send Logs to FortiAnalyzer/FortiManager**.
13. In the **Send To** fields, select **Managed FortiAnalyzer**, and then select **FAZ**.
14. In the **Upload Option** field, select **Real-time**.
15. Enable **Reliable Logging to FortiAnalyzer**.
    Your configuration should look like the following example:



16. Click **OK**.
17. Click **Save**.



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

18. At the top of the page, click the lock icon to unlock **My_ADOM**.
19. 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 FortiManager to work on.

In a production environment, before you disable workspace mode, ensure that all administrators connected to FortiManager save their work.

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** > **Advanced** > **Workspace**.
4. Click **Disable**, click **Apply**, and then click **OK**.
   Disabling workspace mode logs administrators out of FortiManager and saves the changes.
5. Keep the FortiManager GUI session open for the next exercise.

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 on FortiManager.
- Add multiple devices using the device manager.

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

In this lab, **FMG-Access** on both FortiGate devices is already enabled on the interfaces connected to FortiManager. **FGFM** 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                : none
   schedule-config-restore: enable
   schedule-script-restore: enable
   allow-push-configuration: enable
   allow-push-firmware : disable
   allow-remote-firmware-upgrade: disable
   allow-monitor       : enable
   local-cert          :
   vdom                : root
   server-list:
       == [ 1 ]
       id:     1       server-type: update rating
   fmg-update-port     : 8890
   include-default-servers: disable
   enc-algorithm       : high
   ```

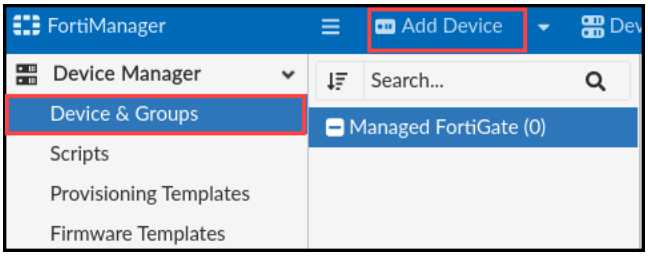
4. Close the PuTTY session.

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

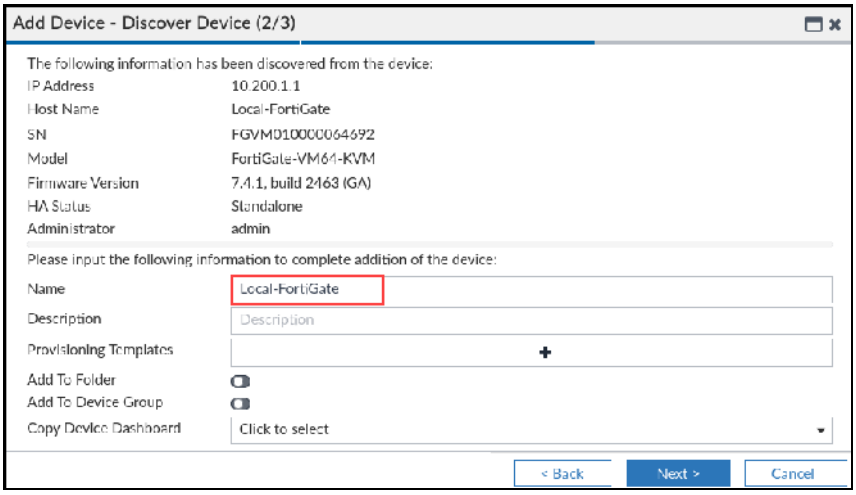
1. On the Local-Client VM, open a browser, and then log in to the FortiManager GUI at `10.0.1.241` with the username `student` and password `fortinet`.
2. Click **My_ADOM**.
3. Click **Device Manager** > **Device & Groups** > **Add Device**.



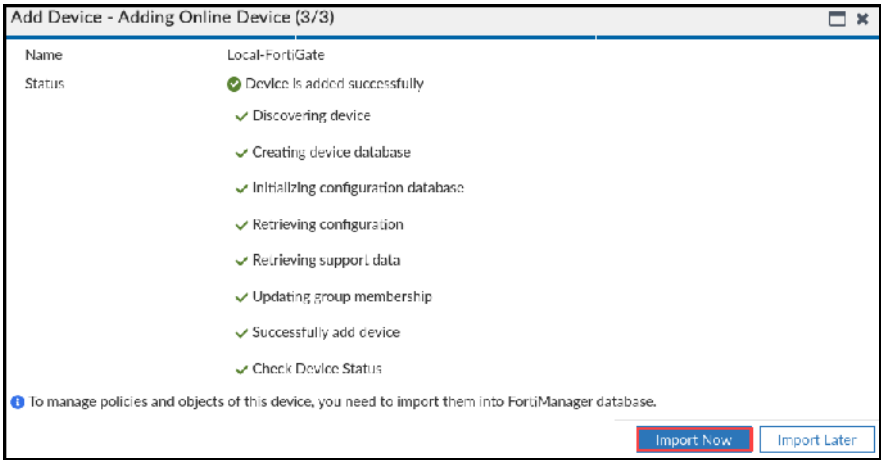
4. In the **Add Device** wizard, select **Discover Device**, and then configure the following settings:

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

5. Click **Next**.
6. Review the discovered device information, and ensure that **Name** is set to **Local-FortiGate**.

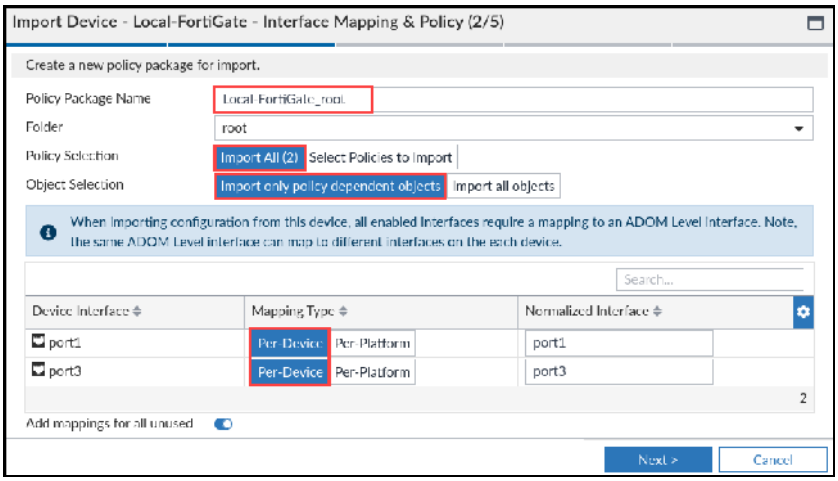


7. Click **Next**.
8. Click **Import Now** to import the policies and objects from Local-FortiGate.



9. Select the **Import Policy Package** checkbox.
10. Click **Next**.
11. On the policy package import page, do the following:
    - 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**.

    Your configuration should look like the following image:



12. Click **Next**.
13. On the conflict page, click **View Conflict** for each entry.

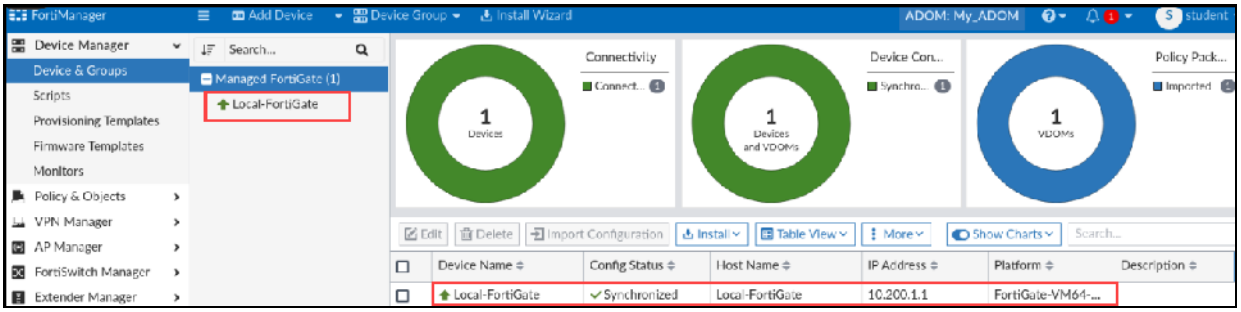
    This shows you the details of the configuration differences between FortiGate and FortiManager.
14. In the **Use Value From** column, keep the default setting of **FortiGate**.

15. Click **Next**.
    Note the objects identified—these should be identified as duplicates, new, or updating existing FortiManager.
16. Click **Next**.
17. Click **Download Import Report**.
18. In a text editor, such as Pluma, open the import report to review the objects that have been imported or skipped.

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.

19. Close the text editor.
20. Click **Finish**.
    Local-FortiGate should now be listed in the device manager.



21. On the Local-Client VM, open PuTTY, and then connect over SSH to the **Local-FortiGate** saved session.
22. Log in with the username `admin` and password `password`.
23. 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                 : "::ffff:10.200.1.241"
fmg-source-ip       : 0.0.0.0
fmg-source-ip6      : ::
local-cert          :
ca-cert             :
vdom                : root
server-list:
    == [ 1 ]
    id:     1       server-type: update rating
fmg-update-port     : 8890
include-default-servers: disable
enc-algorithm       : high
interface-select-method: auto
```

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.

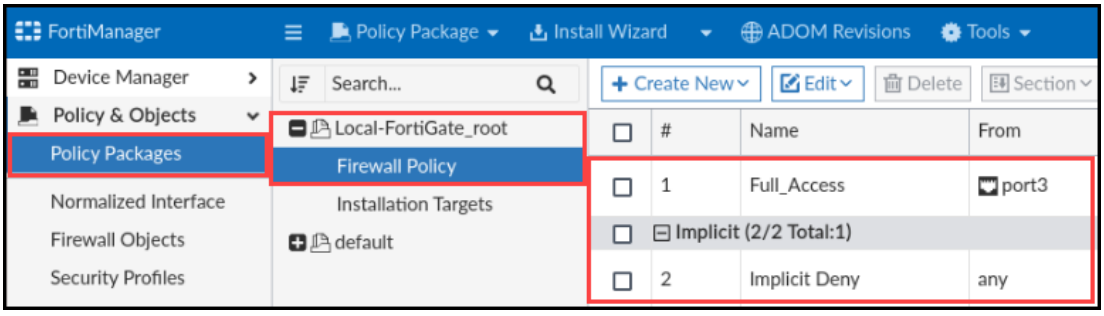
24. Close the PuTTY session.

View the Local-FortiGate Policy Package

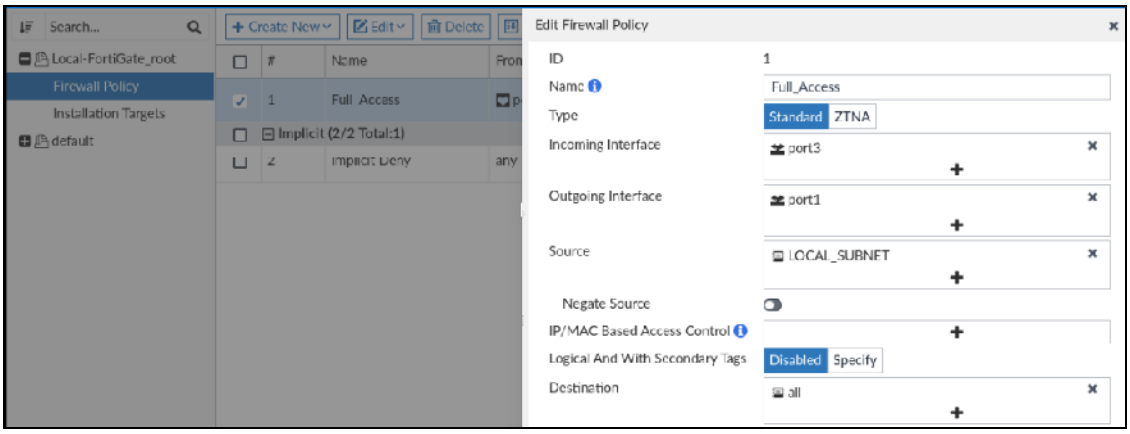
Now that you have imported policy and dependent objects for Local-FortiGate, you will view the policy package created for Local-FortiGate.

To view the Local-FortiGate policy package

1. Continuing on the FortiManager GUI, click **Policy & Objects** > **Policy Packages**.
   You will notice that a policy package named **Local-FortiGate_root** was created when you imported firewall policies from Local-FortiGate.



2. Double click the **Full_Access** policy.



The settings on this policy match those currently on Local-FortiGate, since they were imported from it.

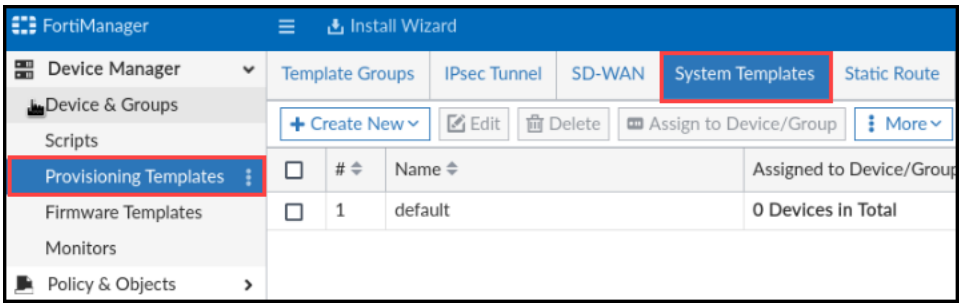
3. Click **Cancel**.

Import System Template Settings From FortiGate

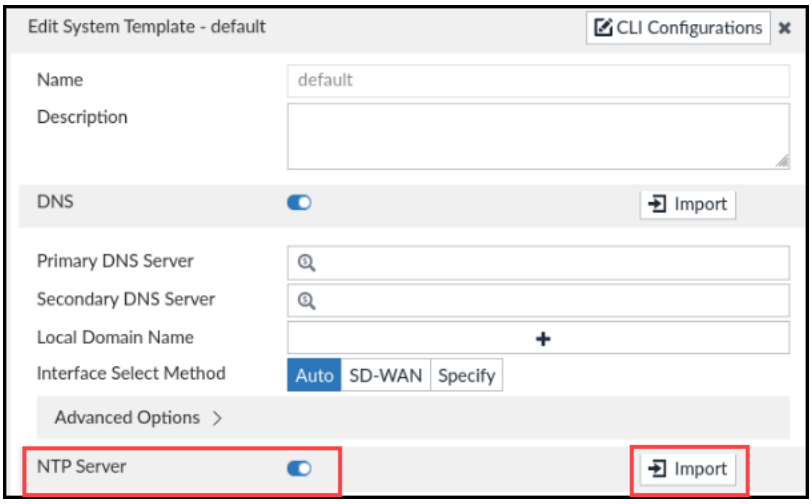
Now that you have added Local-FortiGate to FortiManager, you will import NTP server settings from Local-FortiGate into a system template. This template can then be applied to multiple FortiGate devices later.

To import system template settings from FortiGate

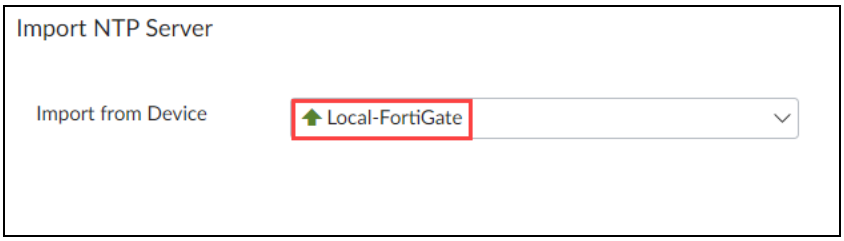
1. Continuing on the FortiManager GUI, browse to **Device Manager** > **Provisioning Templates** > **System Templates**.



2. Select the **default** checkbox, and then click **Edit**.
3. Verify that **NTP Server** is enabled, and then click **Import**.



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



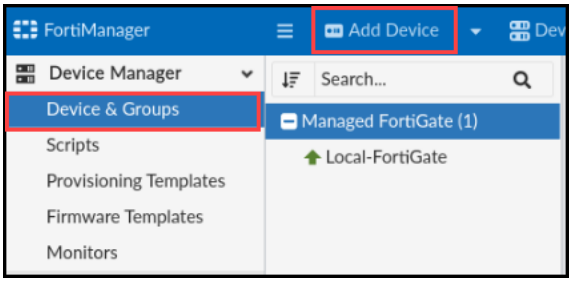
5. Click **OK**, and then click **OK** one more time to save the changes.

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

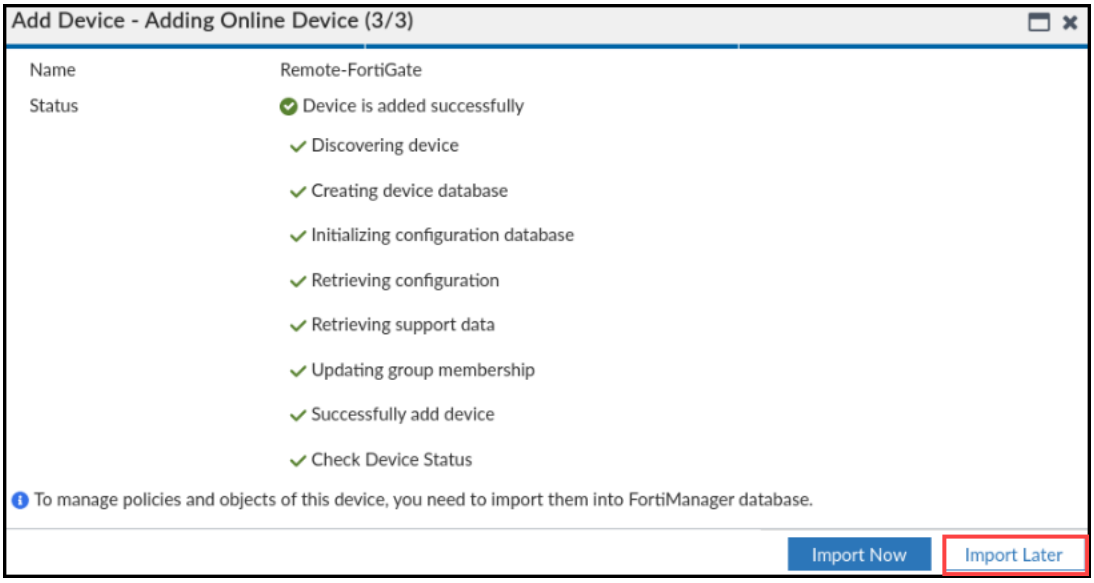
1. Continuing on the FortiManager GUI, click **Device & Groups**.
2. Click **Add Device**.



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**.



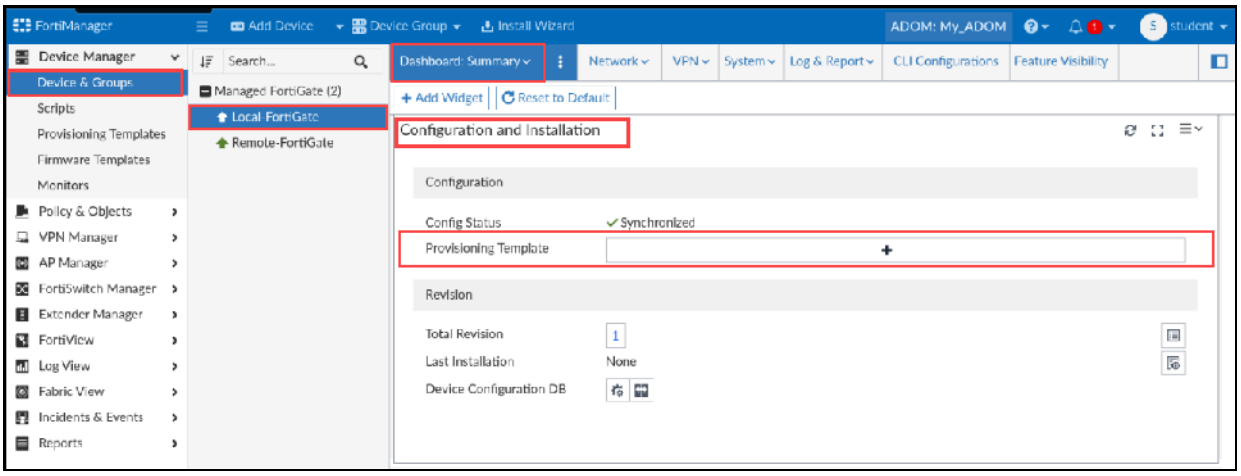
The **Remote-FortiGate** device should now be listed on the **Device & Groups** page.

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

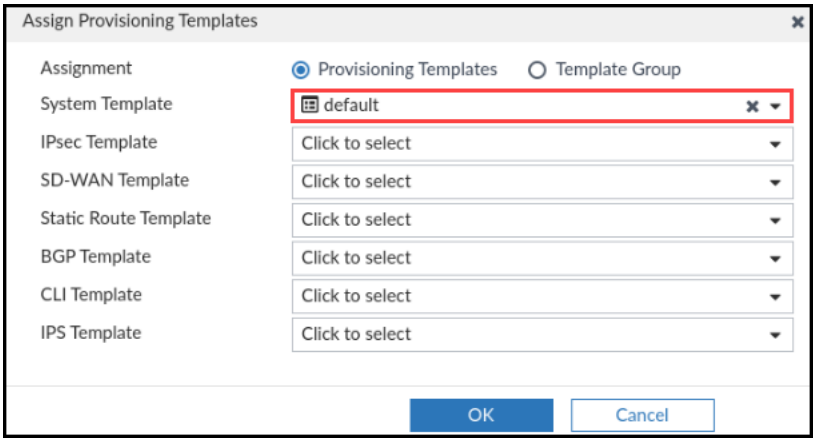
You will assign the **default** system template to Local-FortiGate and Remote-FortiGate to apply system settings.

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

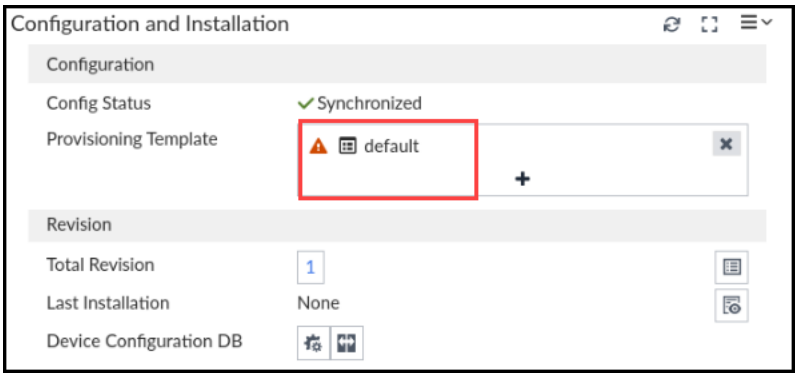
1. Continuing on the FortiManager GUI, click **Device & Groups**.
2. Click **Local-FortiGate**.
3. On the **Dashboard Summary** tab, scroll down to the **Configuration and Installation** widget, and then in the **Provisioning Template** field, click **+**.



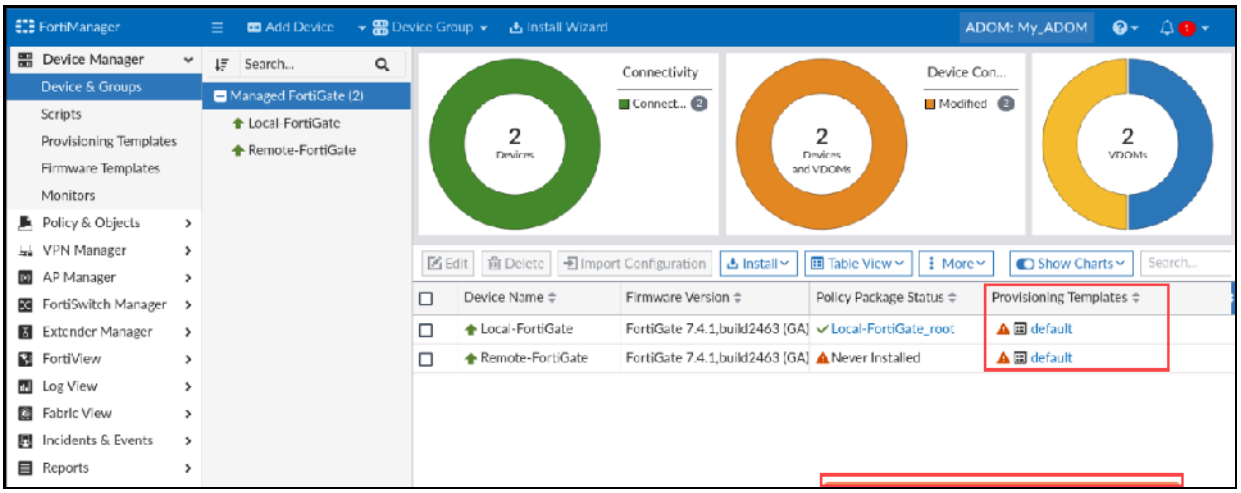
4. In the **Assign Provisioning Templates** window, in the **System Template** field, select **default**.



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



6. Repeat steps 2–5 for Remote-FortiGate.
7. Click **Managed FortiGate(2)**, and then scroll to the right to display the **Provisioning Templates** column.
   This column should display **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.

	Device Name	Config Status	Policy Package Status
☐	Local-FortiGate	✓ Synchronized	✓ Local-FortiGate_root
☐	Remote-FortiGate	✓ Synchronized	⚠ Never installed

8. Log out of the FortiManager GUI.

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

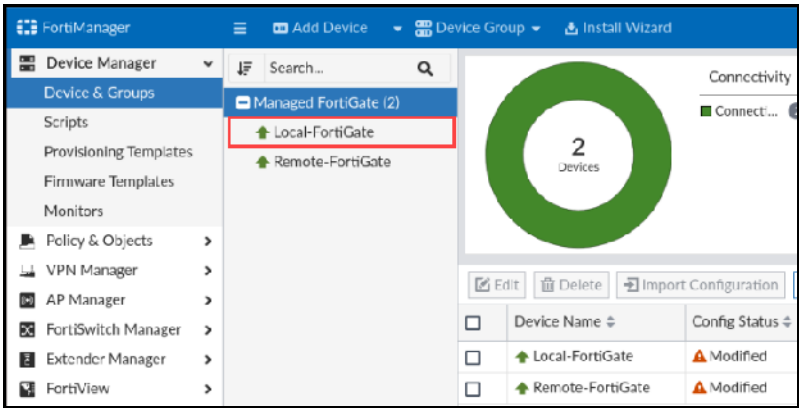
Exercise 1: Understanding the Statuses of Managed Devices

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**.

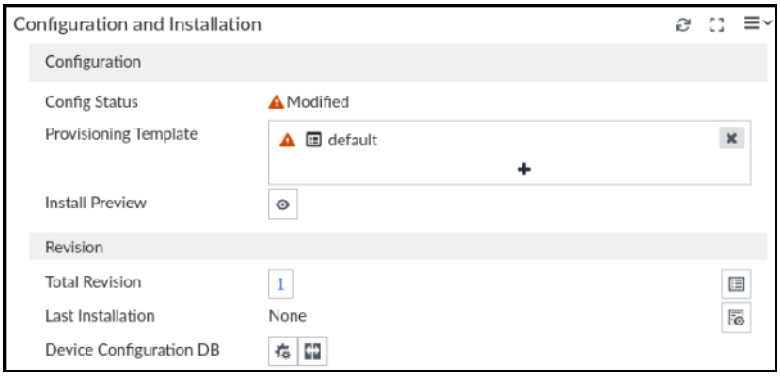
- The **Sync Status** indicates whether the FortiGate configuration matches the latest revision history.
- The **Device Settings Status** indicates whether the FortiGate configuration stored in the device-level database matches the latest running revision history.

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. Browse to **Device Manager** > **Devices & Groups**.
4. Click **Local-FortiGate**.



5. In the **Configuration and Installation** widget, in the **Config Status** field, verify that the value is **Modified**.



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. This change made the configuration running on the FortiManager device-level database different from the latest revision history. For this reason, the **Config Status** was changed to **Modified**. You must install the provisioning template changes on the FortiGate devices to return the devices to the synchronized state.

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`?

```
184     FGVM010000064692 -       10.200.1.1      Local-FortiGate   My_ADOM  6.00741 (regular)  7.0 MR4 (2463)  N/A
|- 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
196     FGVM010000065036 -       10.200.3.1      Remote-FortiGate  My_ADOM  6.00741 (regular)  7.0 MR4 (2463)  N/A
|- 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 **Config Status** is the status between the device-level database configuration and the latest revision history. Assigning a provisioning template to a managed device, or editing a template that is already assigned, makes changes to the device-level database configuration, so it enters the **Modified** state (on the GUI). You can see these details when you run the `diagnose dvm device list` command on the `template` section.

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

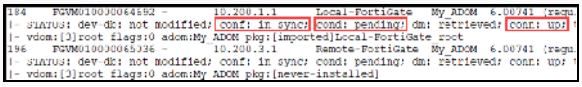
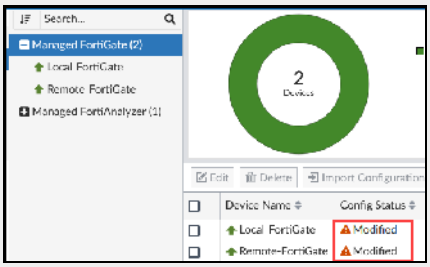
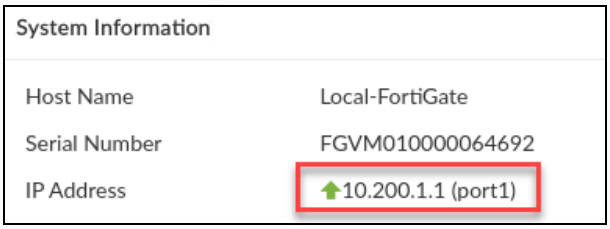
The output also shows the serial number of the device, the connecting IP address of the device, the firmware version, the name of the device on FortiManager, and the ADOM that you added the device to.

```
184     FGVM010000064692 -       10.200.1.1      Local-FortiGate   My_ADOM  6.00741 (regular)  7.0 MR4 (2463)  N/A
|- 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
196     FGVM010000065036 -       10.200.3.1      Remote-FortiGate  My_ADOM  6.00741 (regular)  7.0 MR4 (2463)  N/A
|- 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]
```

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

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 on 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.
11. Leave the GUI session open for the next exercise.

Exercise 2: Installing System Template Changes on Managed Devices

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

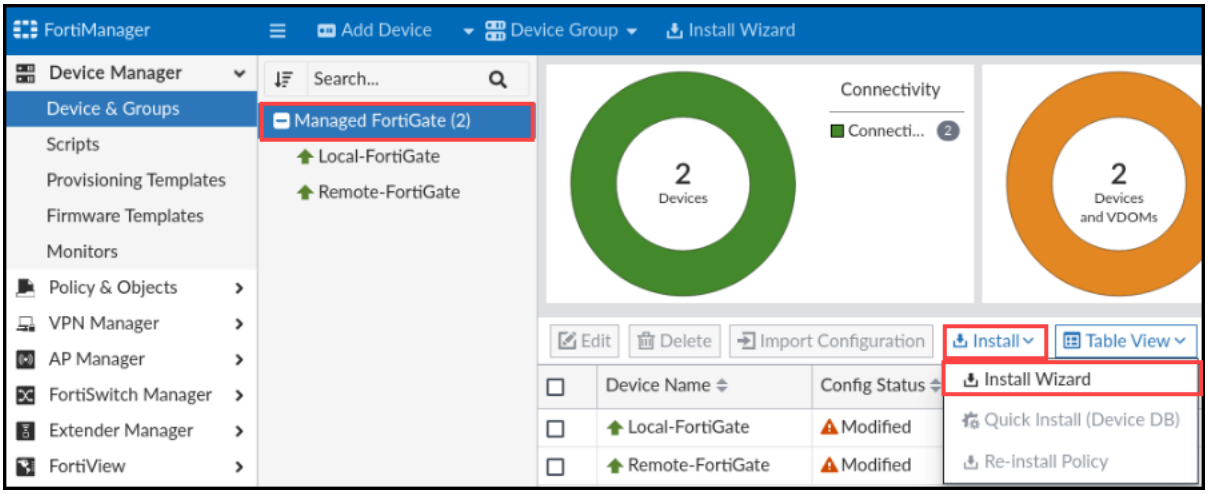
In this exercise, you will install system template changes on both FortiGate devices, and then view those changes locally, by logging in to each FortiGate.

Install System Templates

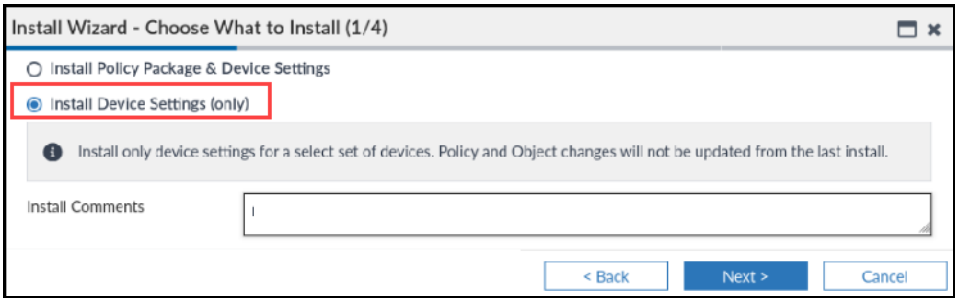
You will install the **default** system template changes to Local-FortiGate and Remote-FortiGate using the **Install Wizard**.

To install system templates

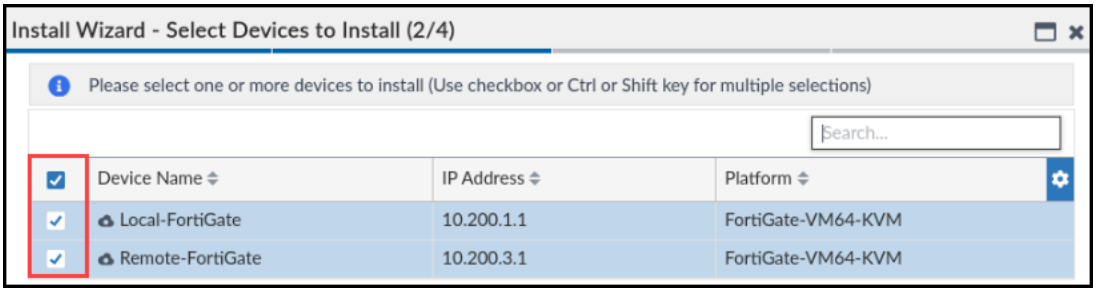
1. Log in to the FortiManager GUI with the username `student` and password `fortinet`.
2. Click **My_ADOM**.
3. Continuing on the FortiManager GUI, click **Managed FortiGate(2)**.
4. Click **Install** > **Install Wizard**.



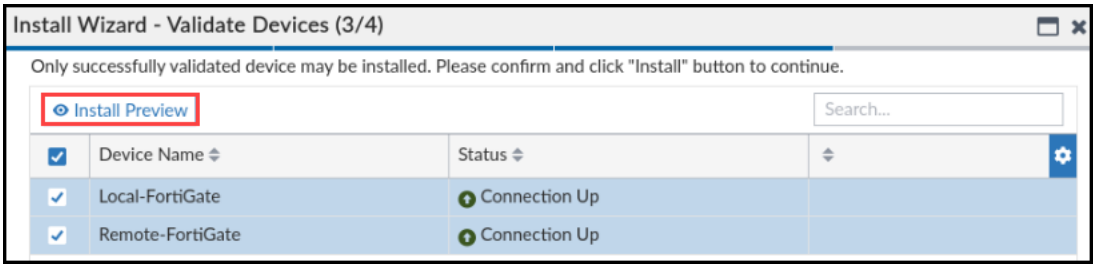
5. In the **Install Wizard**, confirm that **Install Device Settings (only)** is selected, and then click **Next**.



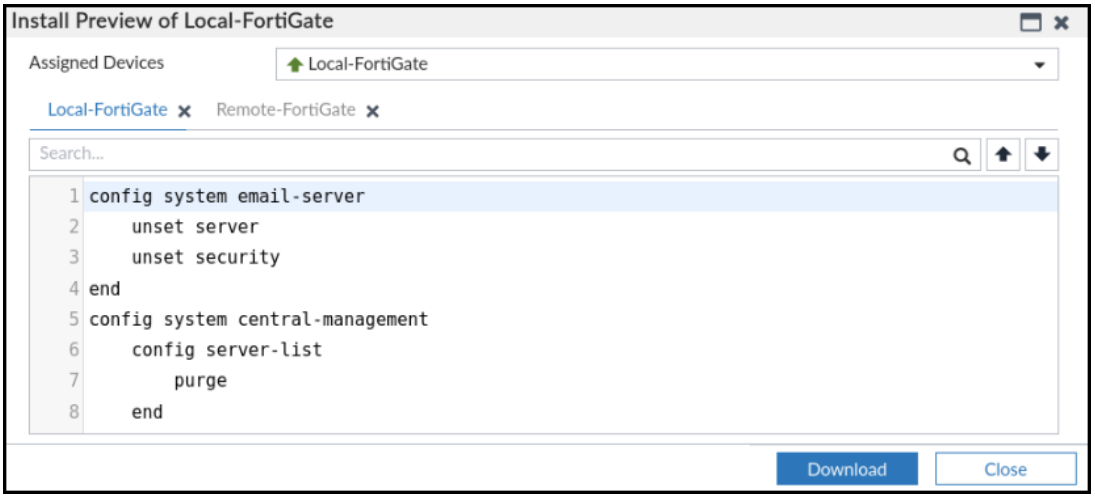
6. In the next window, ensure that both FortiGate devices are selected, and then click **Next**.



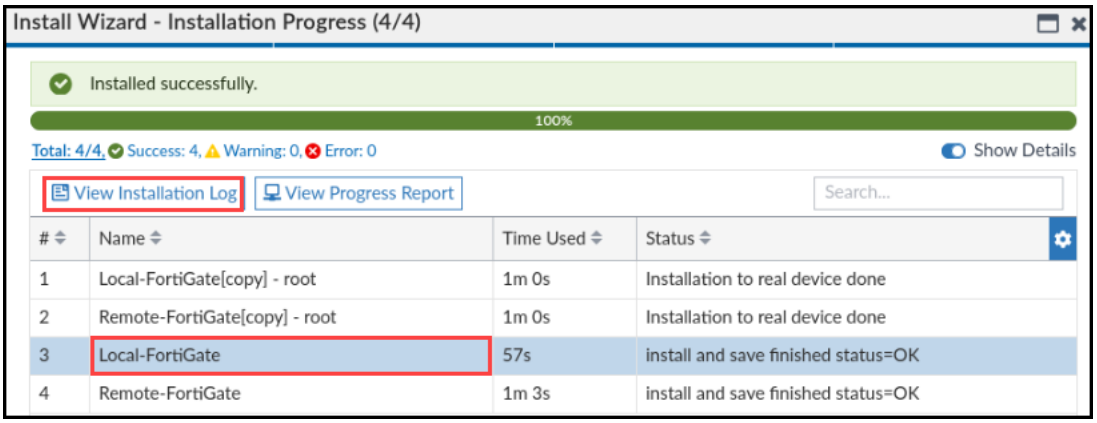
7. Click **Install Preview**.



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



8. On the **Install Preview** page, click **Close**.
   Optionally, you can select **Install Preview** for Remote-FortiGate.
9. Click **Install**.
10. 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:

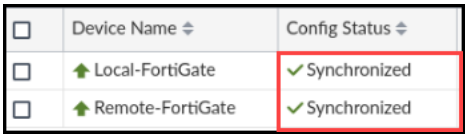
11. Click **Close**.
12. Click **Finish**.

Check the Status of the Managed Device

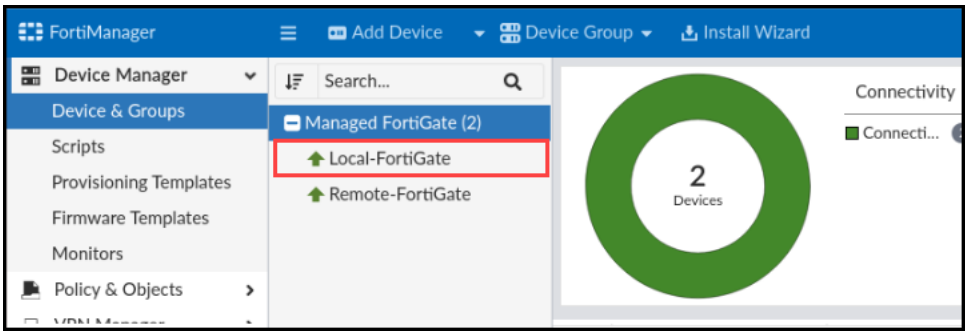
You will check the status of the managed device after the installation.

To check the status of the managed device

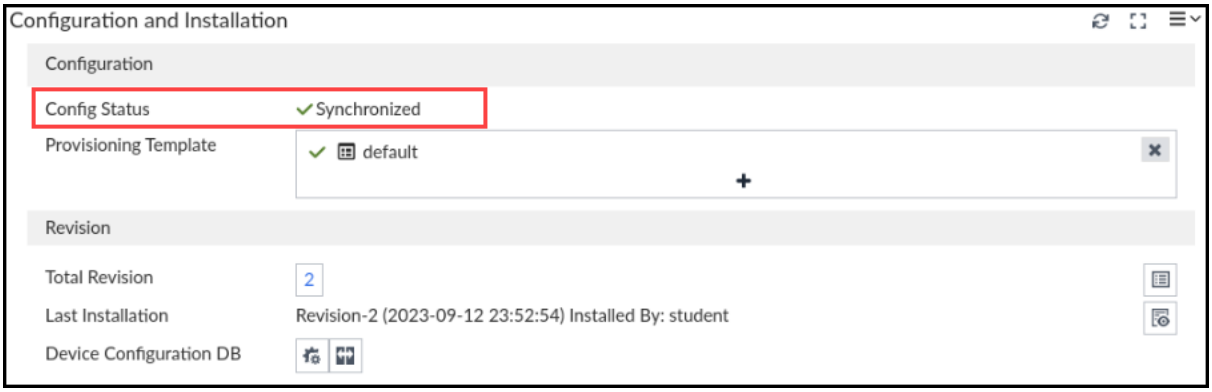
1. Continuing on the FortiManager GUI, review the values in the **Config Status** column. They should now appear as **Synchronized**.



2. Click **Local-FortiGate**.



3. In the **Configuration and Installation** widget, 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:

```
TYPE            OID   SN              HA      IP            NAME           ADOM     IPS            FIRMWARE          HW_GenX
fmgfaz-managed  169   FAZ-VM0000065040 -      10.0.1.210    FAZVM64-KVM    My_ADOM  N/A            7.0 MR4 (2308)    N/A
                |- STATUS: conn: up
fmgfaz-managed  170   FGVM010000064692 -      10.200.1.1    Local-FortiGate  My_ADOM  6.00741 (regular)  7.0 MR4 (2463)  N/A
                |- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: autoupdated; conn: up; template:[installed]default
                |- vdom:[3]root flags:0 adom:My_ADOM pkg:[imported]Local-FortiGate_root
fmgfaz-managed  180   FGVM010000065036 -      10.200.3.1    Remote-FortiGate  My_ADOM  6.00741 (regular)  7.0 MR4 (2463)  N/A
                |- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: autoupdated; conn: up; template:[installed]default
                |- vdom:[3]root flags:0 adom:My_ADOM pkg:[never-installed]
```

The `dev-db status` is `not modified`, which means that the FortiGate device-level database configuration matches the latest running revision history.

7. Enter the following command to display the statuses of the FGFM tunnels:

```
diagnose fgfm session-list
```

```
FortiManager # diagnose fgfm session-list
        FAZVM64-KVM(169) sn(FAZ-VM0000065040) ip(10.0.1.210)
                state(tunnel) tunnel(169.254.0.2) uptime:Mon Sep 11 20:25:45 2023
        Local-FortiGate(170) sn(FGVM010000064692) ip(10.200.1.1)
                state(tunnel) tunnel(169.254.0.7) uptime:Tue Sep 12 23:52:39 2023
        Remote-FortiGate(180) sn(FGVM010000065036) ip(10.200.3.1)
                state(tunnel) tunnel(169.254.0.8) uptime:Tue Sep 12 23:52:42 2023
        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

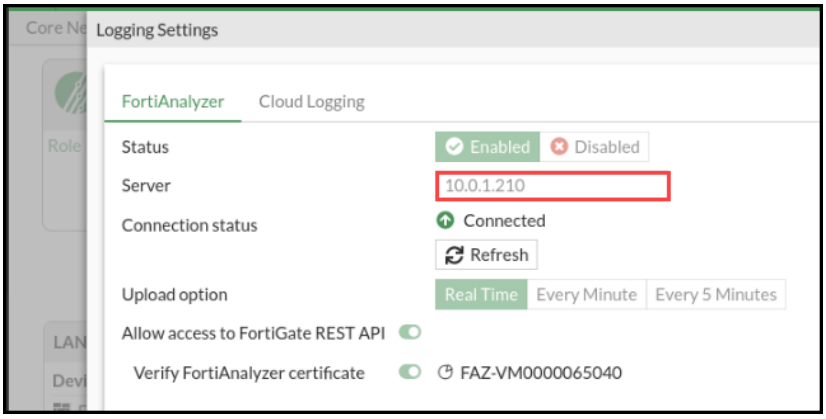
Using FortiManager, you installed the **default** system template configuration on both FortiGate devices. Now, you will log in to the Local-FortiGate and Remote-FortiGate GUIs to view their configurations.

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 **Security Fabric** > **Fabric Connectors** > **Logging & Analytics** > **View**.
   You will notice that FortiAnalyzer is now configured and connected.



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 **Security Fabric** > **Fabric Connectors** > **Logging & Analytics** > **View**.
   You will notice that FortiAnalyzer is configured. 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.

Exercise 3: Viewing the Auto Update Status and Revision History

By default, FortiManager automatically retrieves configuration changes made locally on FortiGate. These changes are reflected in the revision history. If required, you can disable the automatic update behavior on the FortiManager CLI using the `config system admin settings` command. 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 Local Changes on Local-FortiGate

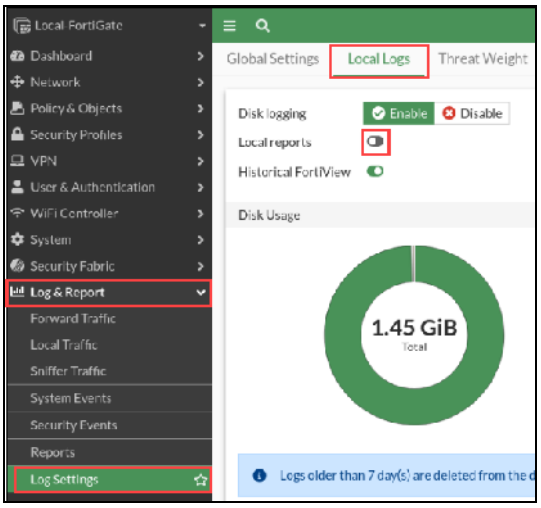
You will make changes directly on Local-FortiGate.

To make local 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** > **Local Logs**.
5. Disable **Local Reports**.



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

Make Local Changes on Remote-FortiGate

You will make changes directly on Remote-FortiGate. You will repeat the same steps for Remote-FortiGate that you did for Local-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. Click **Yes**.
4. Click **Log & Report** > **Log Settings** > **Local Logs**.
5. Disable **Local Reports**.
6. Click **Apply**.
7. Log out of the Remote-FortiGate GUI.

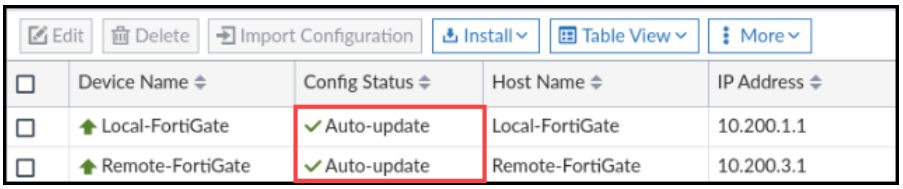
View the Auto Update Status and Revision History

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

To view the auto update status

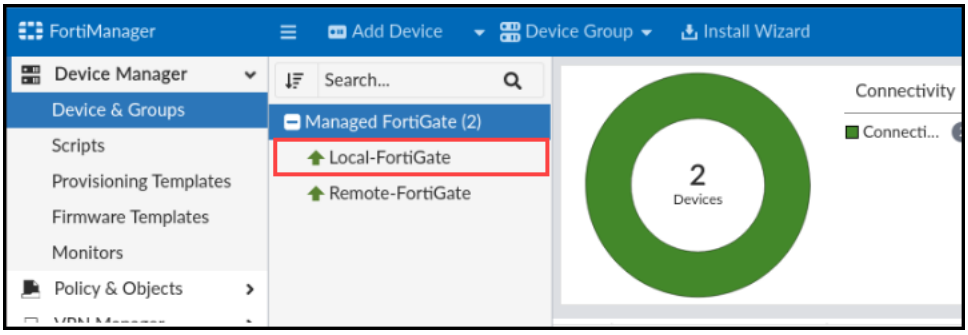
1. Log in to the FortiManager GUI with the username `student` and password `fortinet`.
2. Click **My_ADOM**.
3. Click **Device Manager** > **Device & Groups** > **Managed FortiGate**.
   You will notice that the **Config Status** is now in the **Auto-update** state for both FortiGate devices.

   This confirms that FortiManager received the changes you made locally.

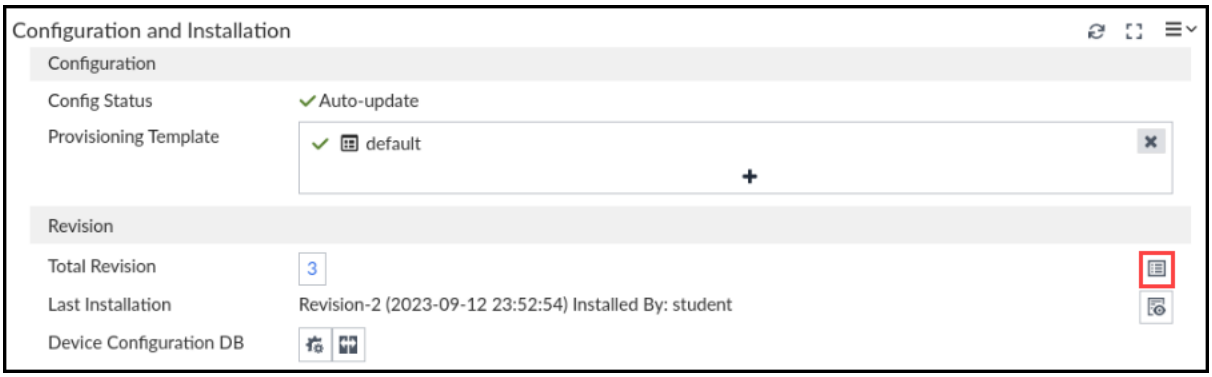


To view the revision history

1. Click **Local-FortiGate**.

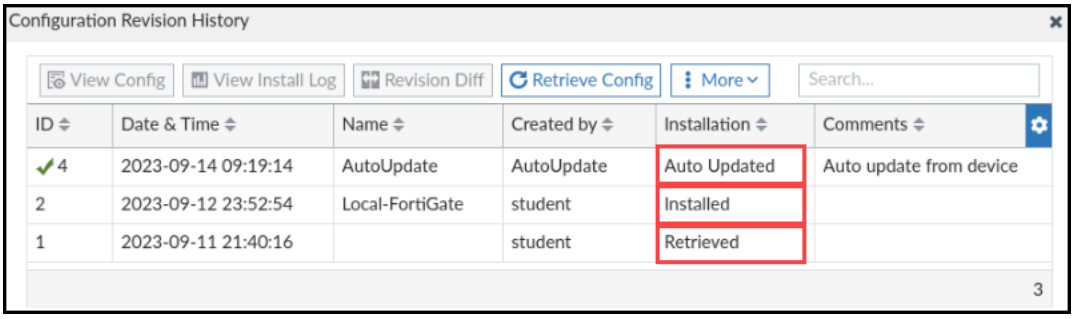


2. In the **Configuration and Installation** widget, click the **Revision History** icon.



Starting chronologically from the bottom, you should see the following three **Installation** statuses (you may have more if you made further changes):

- **Retrieved**: Indicates that this configuration was taken from the device running configuration, when it was added to FortiManager
- **Installed**: Indicates that these changes were made by FortiManager on the managed device
- **Auto Updated**: Indicates that these changes were made locally on FortiGate and were automatically updated on FortiManager

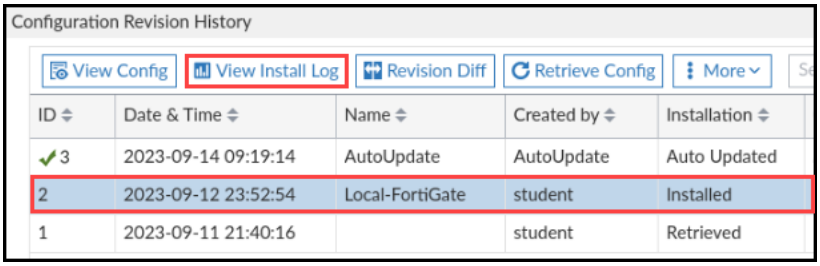


View the Installation Log

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.

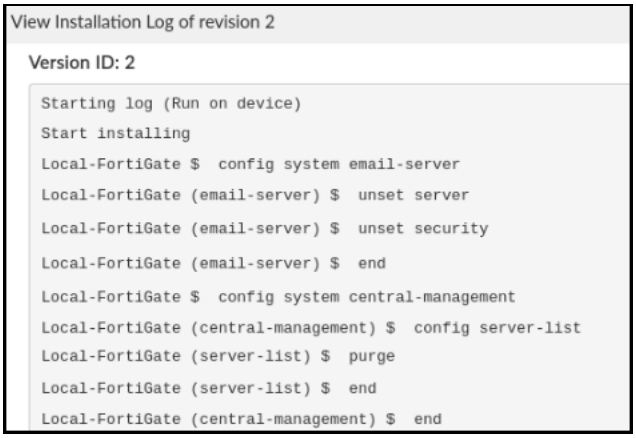
To view the installation log

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



If you made other changes, or if you received any errors previously, the **ID** numbers in your environment will be different from the ones in this image.

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



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 63.

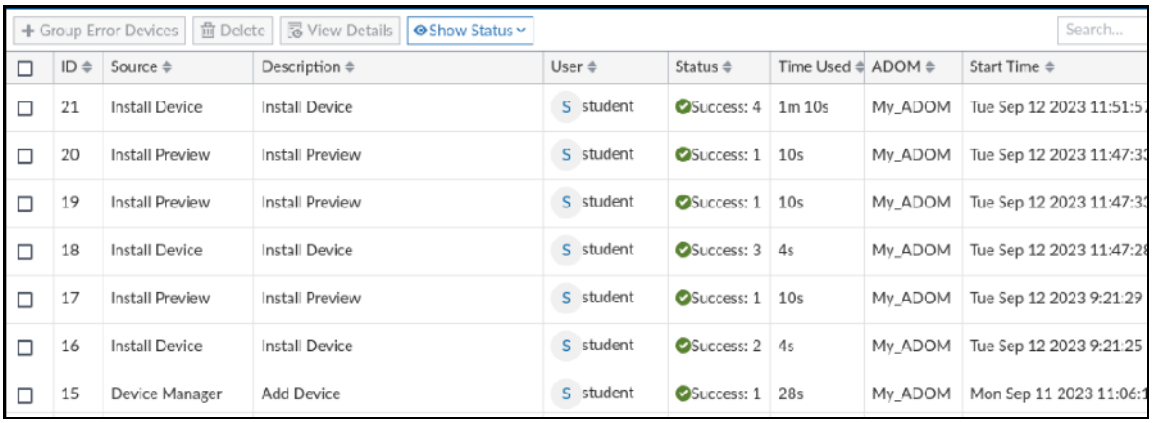
Check the Task Monitor

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.

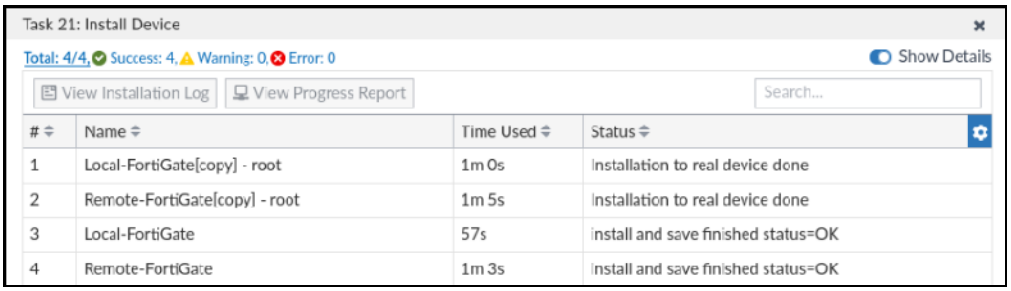
You will now check the entries in the task monitor.

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** > **Task Monitor**.
   The **Task Monitor** shows the tasks that all users performed.



4. Select one of the entries with the **Source** of **Install Device**, and then click **View Details**.



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

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

Exercise 4: Configuring Device-Level Changes

You can view and configure the device-level settings of the managed FortiGate using the device manager. 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 using the device manager.

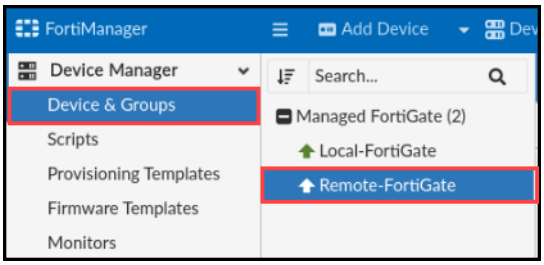
Change the Interface Settings of the Managed FortiGate

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.

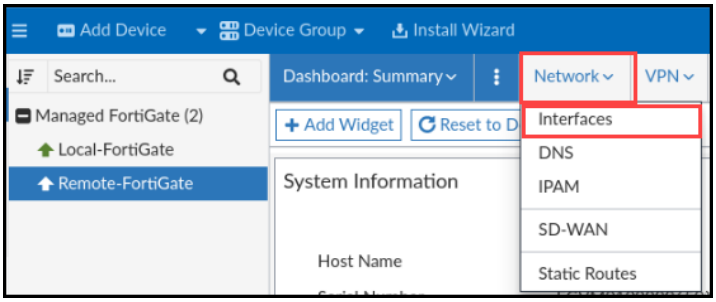
You will change the **Administrative Access** setting of the Remote-FortiGate port4 interface that Remote-FortiGate uses to communicate with FortiManager.

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** > **Device & Groups**.
4. Click **Remote-FortiGate**.



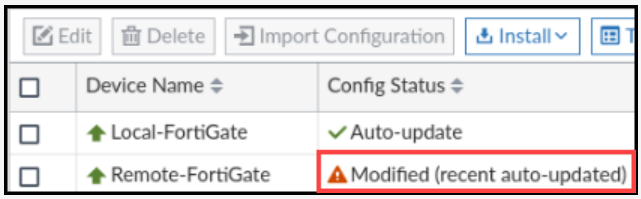
5. Click **Network** > **Interfaces**.



6. Right-click **port4**, and then click **Edit**.
7. In the **Restrict Access** > **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 you made a device-level database change to Remote-FortiGate when 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.

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.

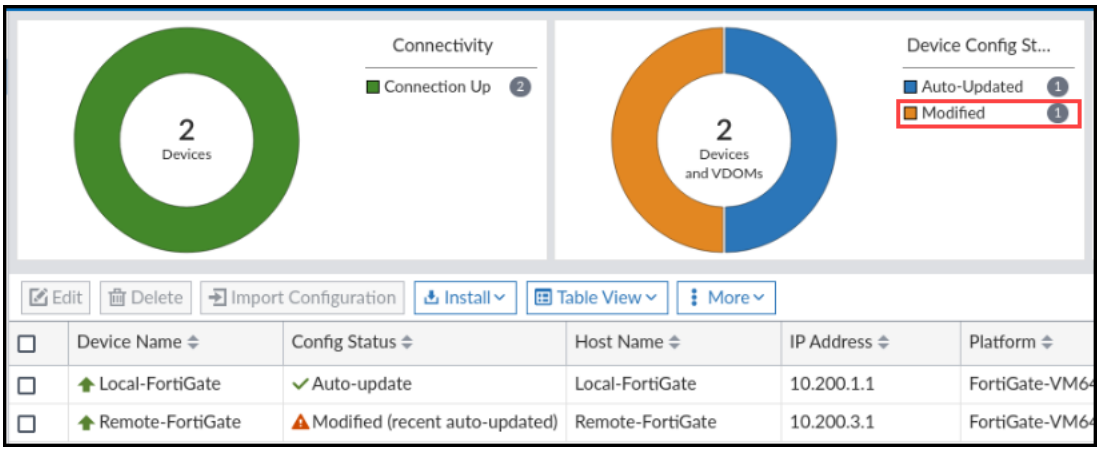
You can filter device statuses based on:

- 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**.



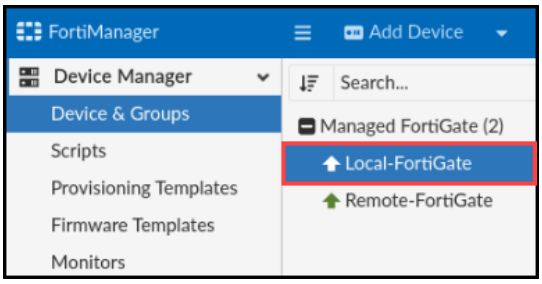
Only **Remote-FortiGate** appears in the **Managed FortiGate** list.

Configure the Administrator Account

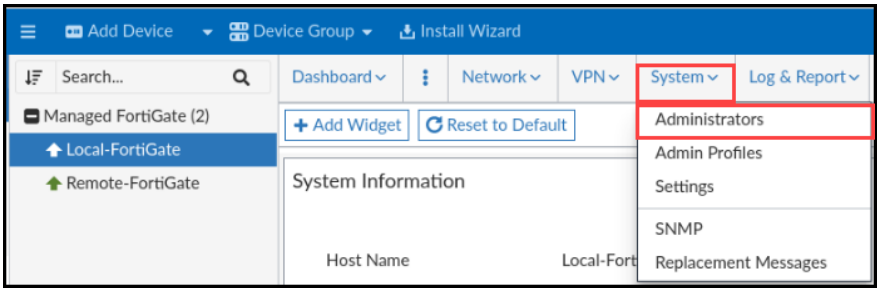
You will create a new administrator account for Local-FortiGate on FortiManager.

To configure the administrator account

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



2. Click **System** > **Administrators**.

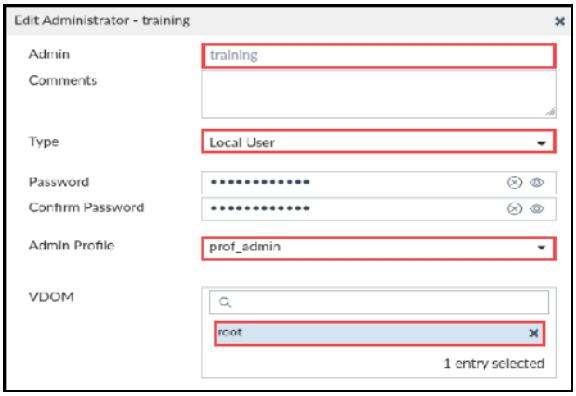


3. Click **Create New**.

4. Configure the following settings:

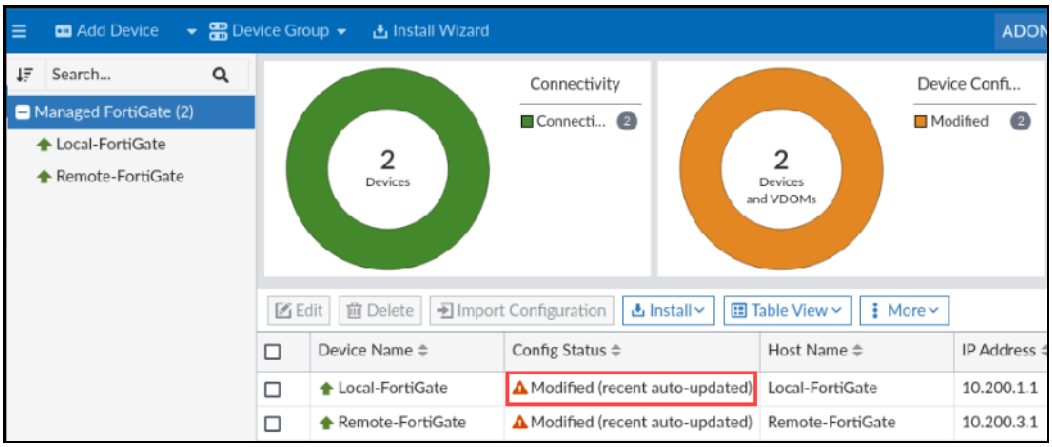
Field	Value
Admin	training
Type	Local User
Password	fortinet
Confirm Password	fortinet
Admin Profile	prof_admin
VDOM	root

Your configuration should look like the following example:



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

   You will notice that the **Config Status** for Local-FortiGate has changed to **Modified(recent auto-updated)**. This is because you made a device-level configuration change for Local-FortiGate by configuring the administrator account.



7. Keep the FortiManager GUI session open for the next exercise.

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.

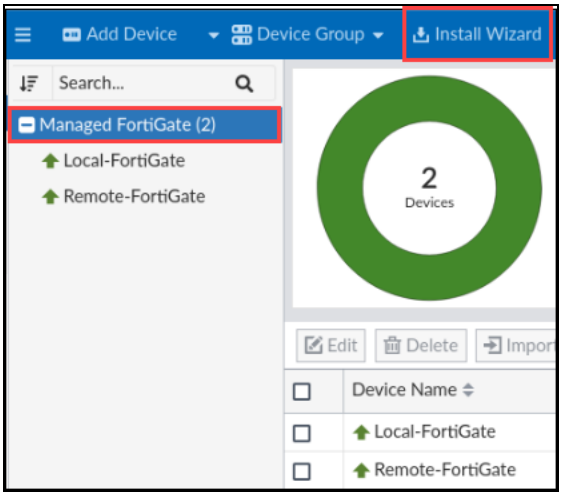
In this exercise, you will install these changes on the managed device using the **Install Wizard**, and then view the installation history. You will also compare the differences in the revision history configurations using the **Revision Diff** feature.

Use the Install Wizard

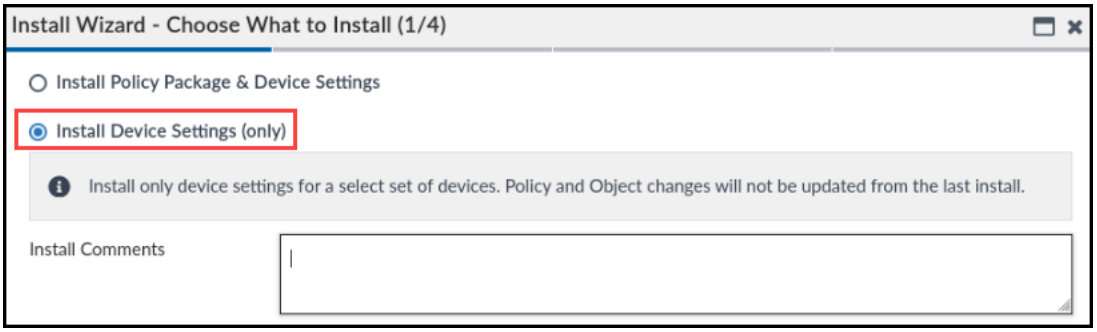
You will install these changes on the managed devices using the **Install Wizard**.

To install configuration changes on FortiGate using the Install Wizard

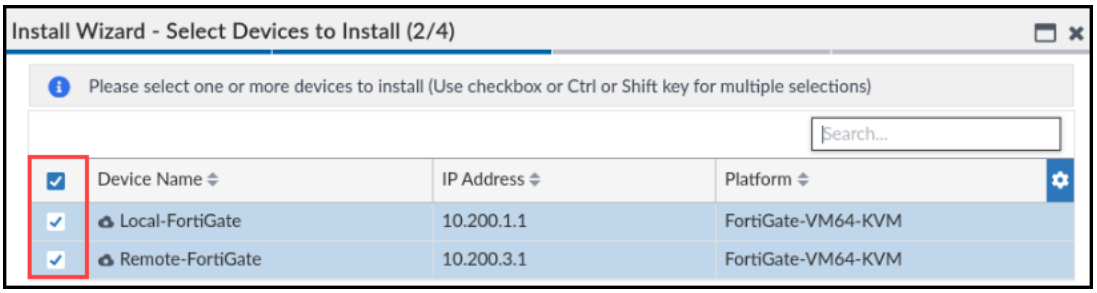
1. Continuing on the FortiManager GUI, click **Managed FortiGate** > **Install Wizard**.



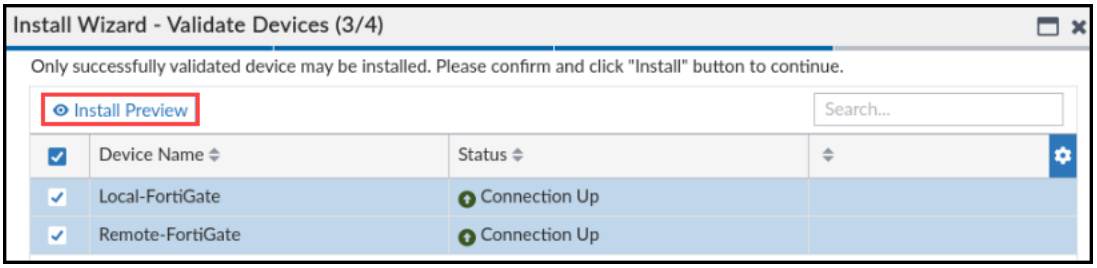
2. Verify that **Install Device Settings (only)** is selected, and then click **Next**.



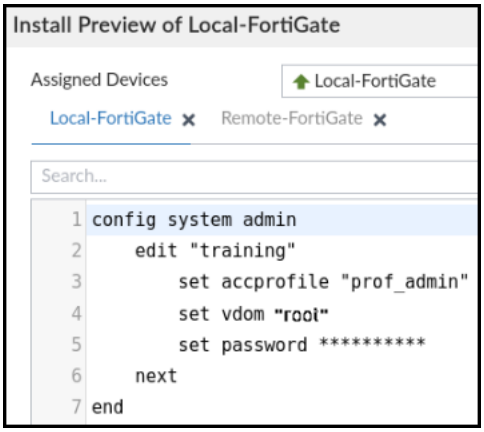
3. On the **Device Settings** page, make sure that both FortiGate devices are selected.



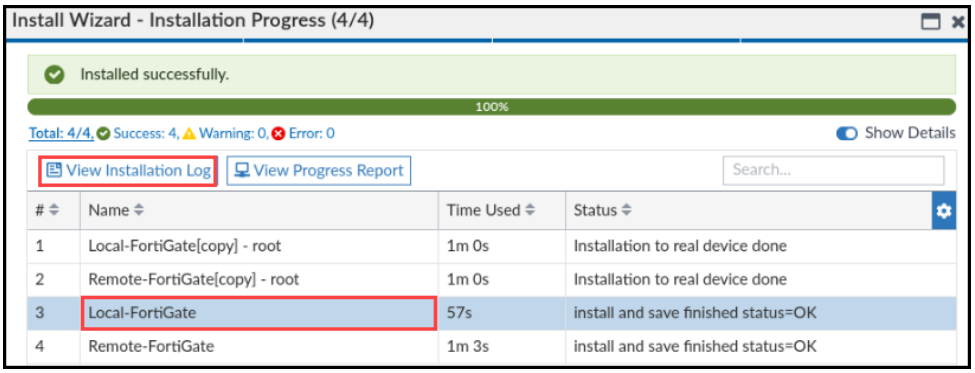
4. Click **Next**.
5. Click **Install Preview**.



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



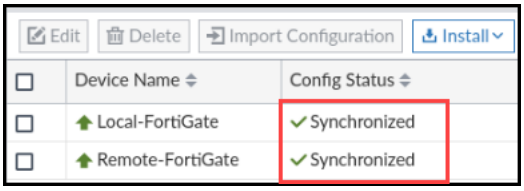
6. On the **Install Preview of Selected Devices** page, click **Close**.
   Optionally, you can also check the **Install Preview** for Remote-FortiGate.
7. Make sure that both FortiGate devices are selected, and then click **Install**.
8. Once the installation has completed successfully, select **Local-FortiGate**, and then click **View Installation Log**.



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

9. On the **Install Log** page, click **Close**.
10. Click **Finish**.
11. Click **Managed FortiGate**.

    The **Config Status** should now display the **Synchronized** state.



View the Revision Differences

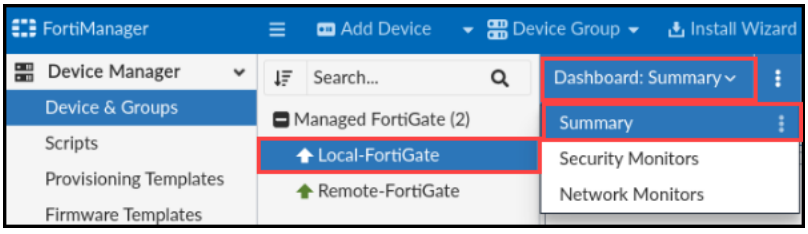
After every retrieve, auto update, and installation operation, FortiManager stores the FortiGate configuration checksum output with the revision history. This is how the out-of-sync condition is calculated.

The **Revision Diff** feature 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 the 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.

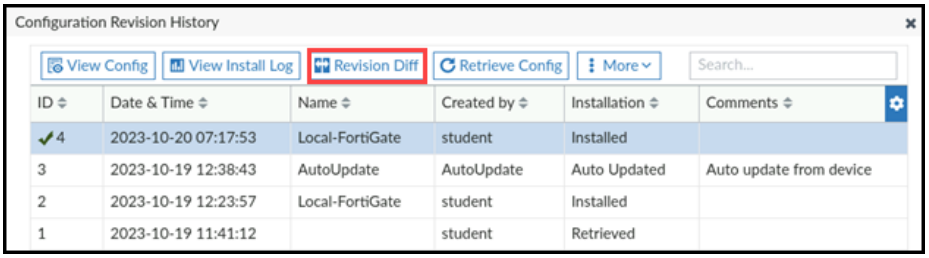
To view the revision differences

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

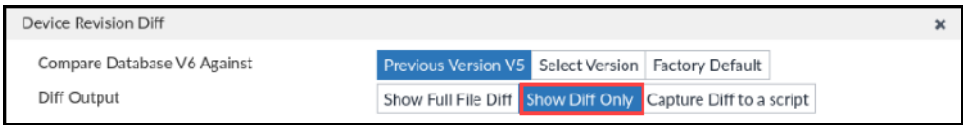


2. In the **Configuration and Installation** widget, click the **Revision History** icon.

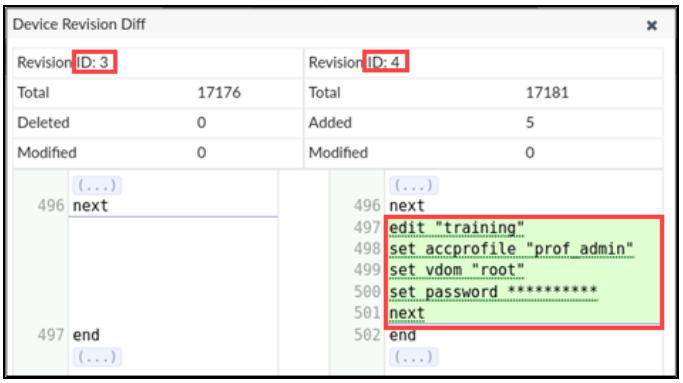
3. Click the most recent entry showing the **Installation** column as **Installed**, and then click **Revision Diff**.



4. In the **Diff Output** field, select **Show Diff Only**.



5. Click **Apply**.



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

6. Scroll down, and then click **Save Diff as Script**.

Firefox downloads the file automatically and saves it in the **Downloads** folder.

7. Click the filename to open the file with a text editor like Pluma.

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

8. Close the text editor.

This demonstrates capturing differences in the form of scripts. Make sure that the script captured is valid for other FortiGate devices before using it. 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 and you may need to remove it or edit it.

9. Return to the FortiManager GUI, and then click **Cancel** to close the **Device Revision Diff** window.
10. Click **Close**.
11. Keep the FortiManager GUI session open for the next exercise.

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.

You can configure scripts to run on the following locations:

- 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.

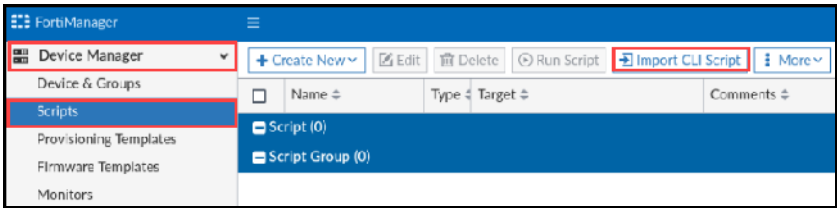
In this exercise, you will make configuration changes using the script feature, and then install the changes on the managed devices.

Configure Scripts

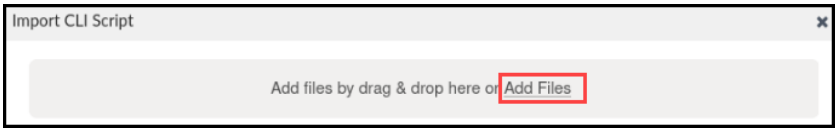
You will configure scripts for the managed devices.

To configure scripts

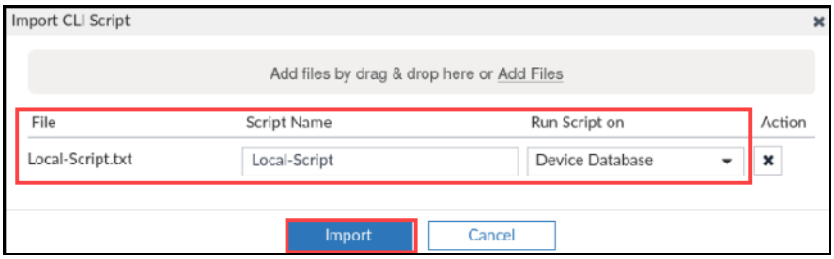
1. Continuing on the FortiManager GUI session, click **Device Manager** > **Scripts** > **Import CLI Script**.



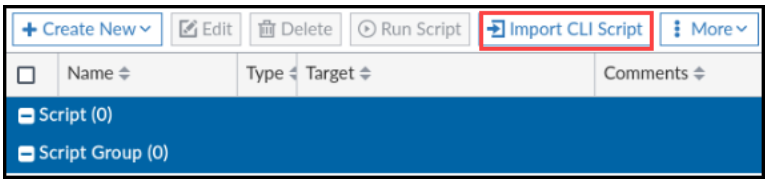
2. Click **Add Files**.



3. Click **Desktop** > **Resources** > **FortiManager-Administrator** > **Lab4-Device-Config** > **Lab4-Scripts**, and then select `Local-Script`.
4. Click **Open**, keep the default values for all other settings, and then click **Import**.



5. Click **Close**.
6. Click **Import CLI Script** again.



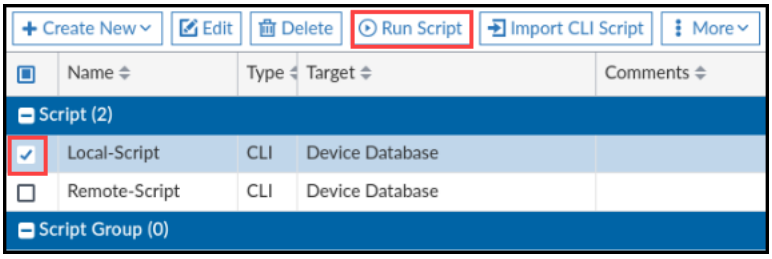
7. Click **Add Files**.
8. Click **Desktop** > **Resources** > **FortiManager-Administrator** > **Lab4-Device-Config** > **Lab4-Scripts**, and then select `Remote-Script`.
9. Click **Open**, keep the default values for all other settings, and then click **Import**.
10. Click **Close**.

Run and Install Scripts

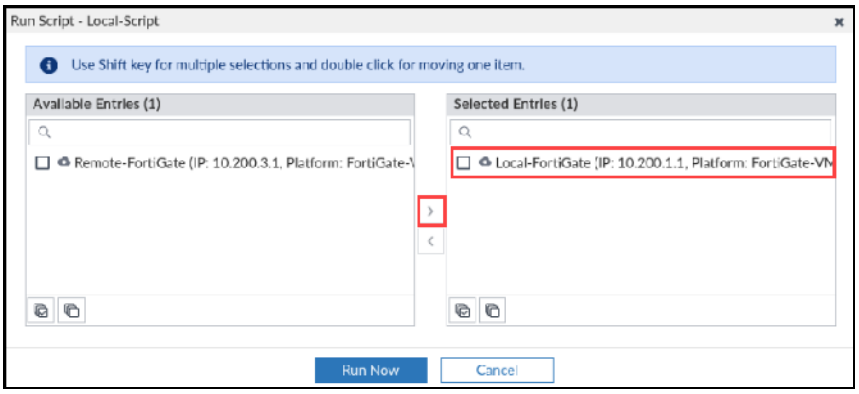
Because the scripts target the device database, you will first run the scripts against the device database, and then install the scripts on the managed devices.

To run scripts

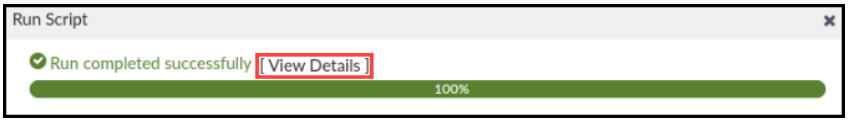
1. Continuing on the FortiManager GUI, select the **Local-Script** checkbox, and then click **Run Script**.



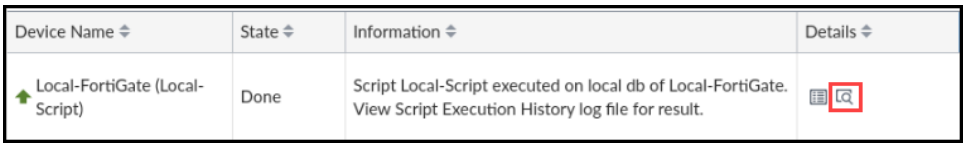
2. Select and add **Local-FortiGate** to the **Selected Entries** list.
   Your configuration should look like the following image:

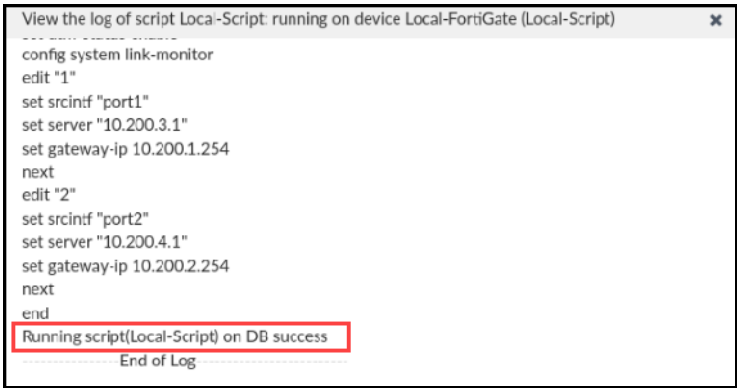


3. Click **Run Now**.
4. Click **OK** to confirm you want to run the script.
5. Click **View Details**.



6. Click the **View Script Executing History** icon, and then scroll to the bottom of the script execution window to check that the script ran successfully on the device database.





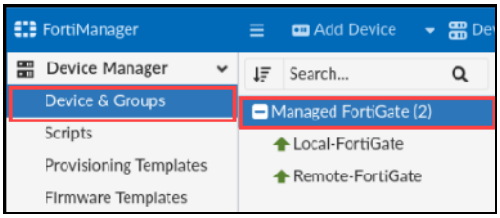
If required, you can also view the script execution history later in the **Configuration and Installation Status** widget or in the **Task Monitor**.

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

12. Click **Run Now**.
13. Click **OK** to confirm you want to run the script.
14. Wait for the script to complete, and then click **Close**.

To install scripts

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



2. Pay attention to the values under the **Config Status** and **Policy Package Status** columns for each FortiGate device.

You will need to scroll to the right to see the **Policy Package Status** column. Optionally, you can drag that column to place it in another location. This was done to obtain the image below.

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.

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**?

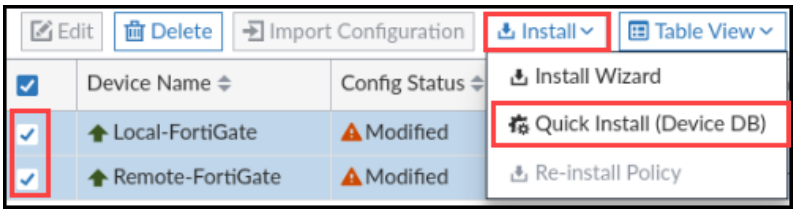
The scripts contain configuration changes related to device-level settings and policies.

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

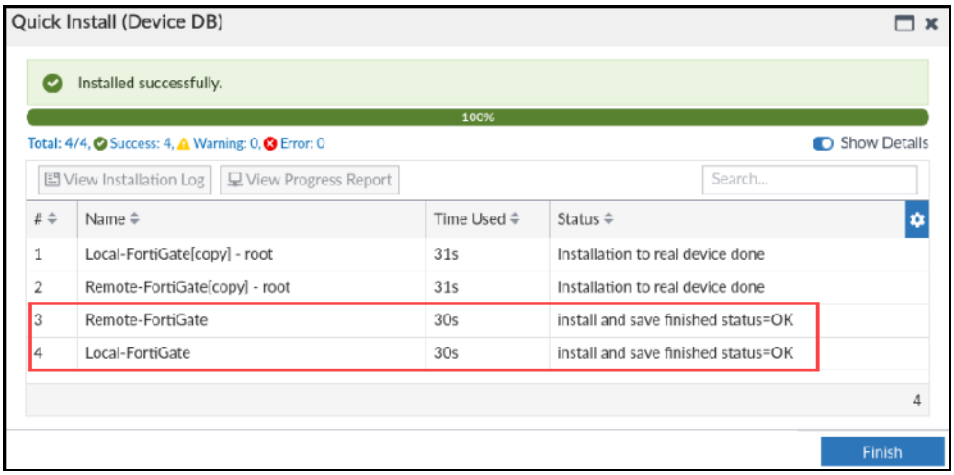
Because the Local-FortiGate policy package was imported when you added FortiGate, FortiManager detects policy-level changes, and marks the Local-FortiGate **Policy Package Status** as **Out of Sync**.

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

3. Select the **Local-FortiGate** and **Remote-FortiGate** checkboxes, click **Install**, and then click **Quick Install**.



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



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

5. Click **Finish**.
   The **Config Status** column should display **Synchronized** for both FortiGate devices.

You may need to refresh the page to display the updated **Config Status**.

6. Log out of the FortiManager GUI.

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 using the **Policy & Objects** pane

Time to Complete

Estimated: 70 minutes

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 Configuration** wizard, which will update the policy packages to reflect the configuration changes.

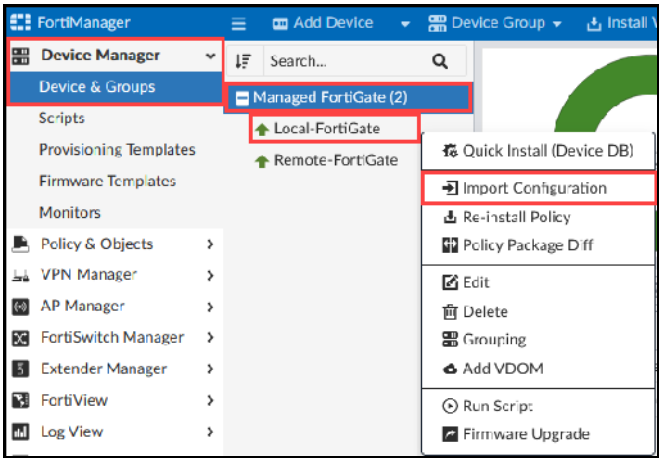
Additionally, you will create an ADOM revision, which is a snapshot of all the policy and object configurations for an ADOM.

Import Policies

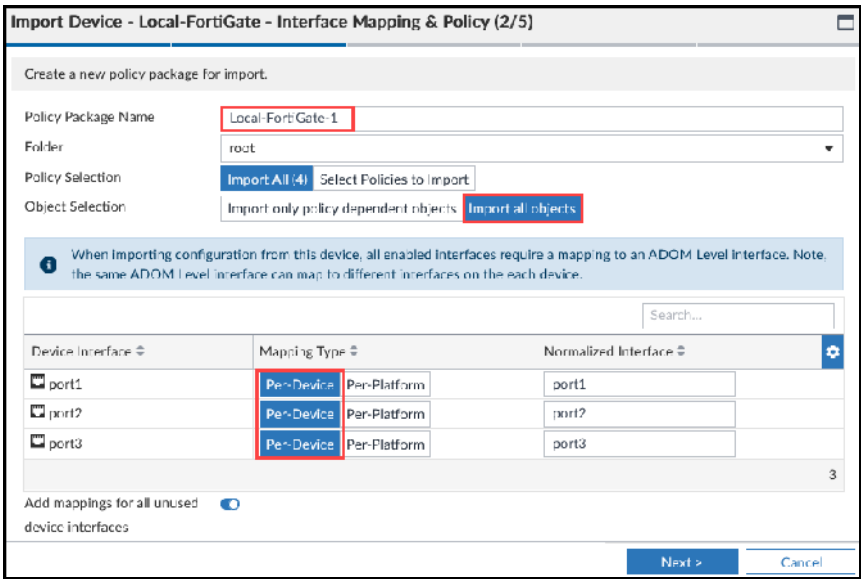
You will import policies and objects for both of the managed FortiGate devices.

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** > **Devices & Groups** > **Managed FortiGate(2)**.
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.
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**.

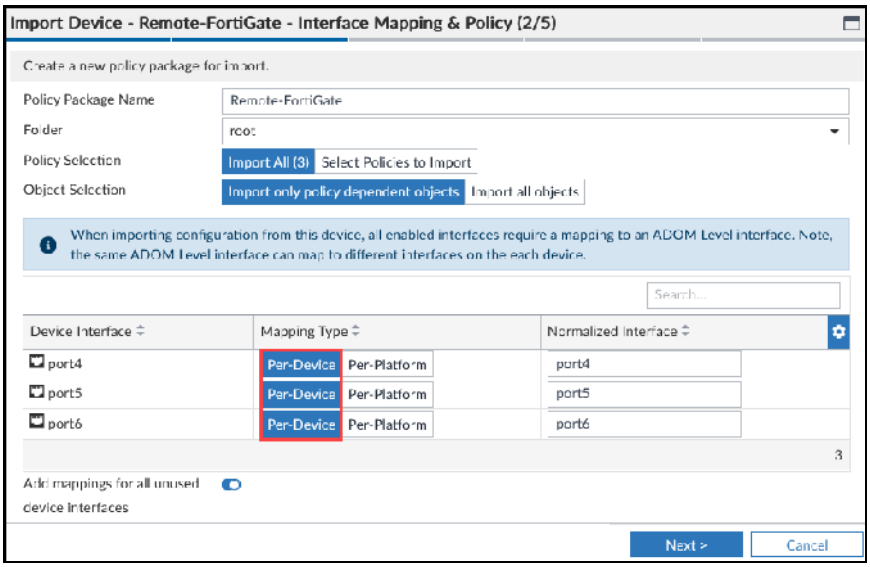


10. Click **Next**.
11. On the **Object Conflicts** page, click **Next**, and then review the objects that will be imported and updated.

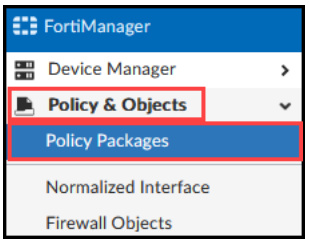
    You should see that a big number of objects will be updated, created, or skipped because they are duplicated. This occurs because you selected to import all objects.
12. Click **Next**.
13. Click **Download Import Report**.

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

14. In the **Downloads** folder, right-click the file, select **Open with**, select a text editor like Pluma, and then click **OK**.
15. Review the download import report, and then close the text editor.
16. 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.

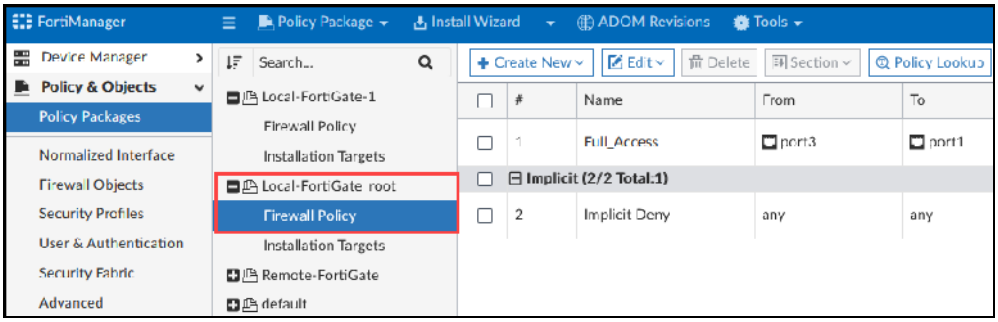


21. Click **Next**.
22. Click **Next** until you reach the **Import Device - Remote-FortiGate - Importing (5/5)** page.
23. Click **Finish**.
24. Click **Policy & Objects** > **Policy Packages**.

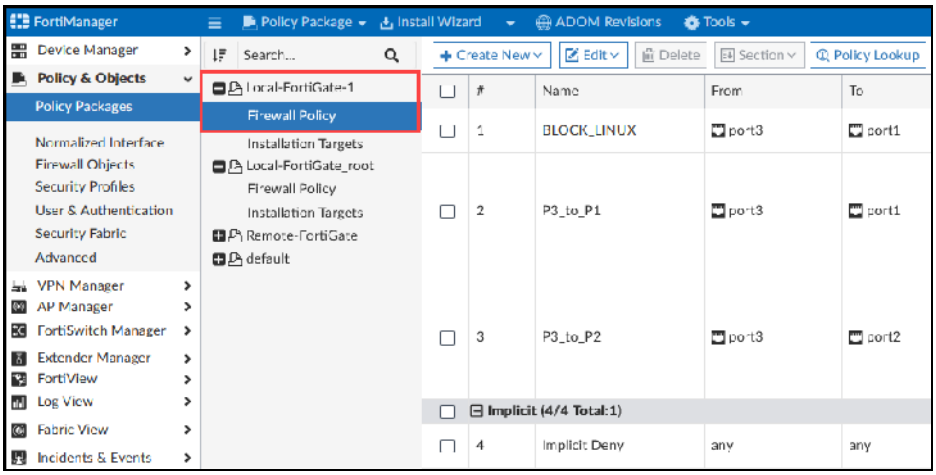


25. Click **Firewall Policy** for each policy package to compare the policies in the **Local-FortiGate_root** and **Local-FortiGate-1** policy packages.

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



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

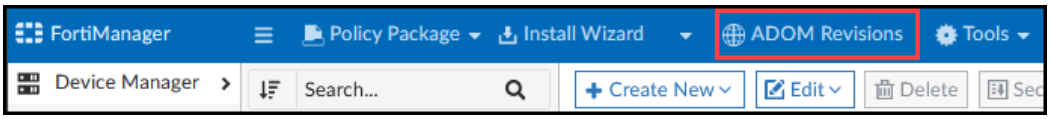


Create ADOM Revisions

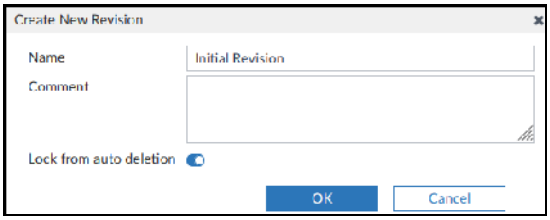
An ADOM revision creates a snapshot of the policy and object configuration for the ADOM. Now that you have imported policies and objects from both FortiGate devices, you will create ADOM revisions that are stored locally on FortiManager, and are useful for comparing the differences between two revisions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

To create an ADOM revision

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

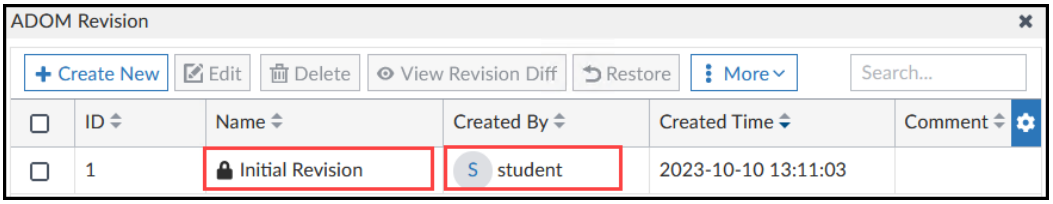


2. Click **Create New**, and then in the **Name** field, type `Initial Revision`.
3. Select **Lock from auto deletion**.



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**, and then log out of the FortiManager GUI.

Exercise 2: Enabling Workflow Mode

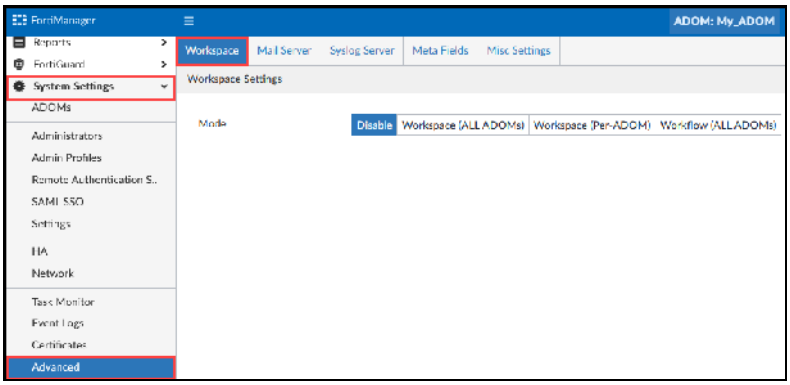
You can use workflow mode to control the creation, configuration, and installation of several settings on FortiManager. This helps to ensure that all changes are reviewed and approved before they are applied.

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

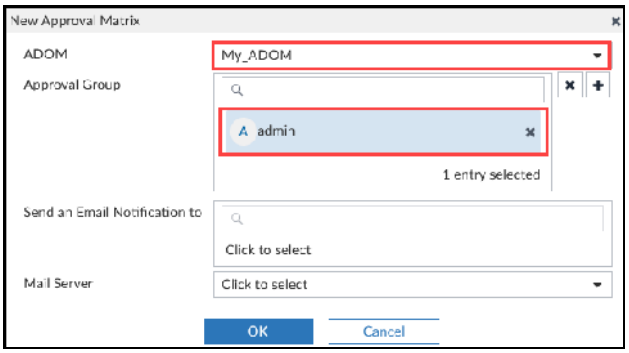
In this exercise, you will enable workflow mode, and then make configuration changes related to policies and objects. You will send the configuration changes for approval and, once they are approved, you will install the changes.

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** > **Advanced** > **Workspace**.



4. Click **Workflow(ALL ADOMs)**.
5. Click **Create New**.
6. In the **ADOM** field, select **My_ADOM**.
7. In the **Approval Group** field, select **admin**, and then click **OK**.



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

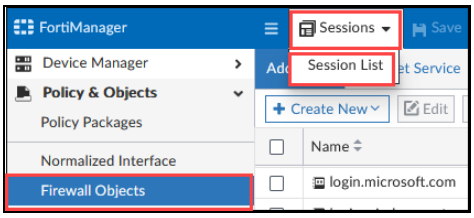
Before you enable workflow mode, ensure that all FortiManager administrators are notified to save their work on FortiManager. This is because enabling workflow mode terminates all management sessions.

10. Click **OK**.

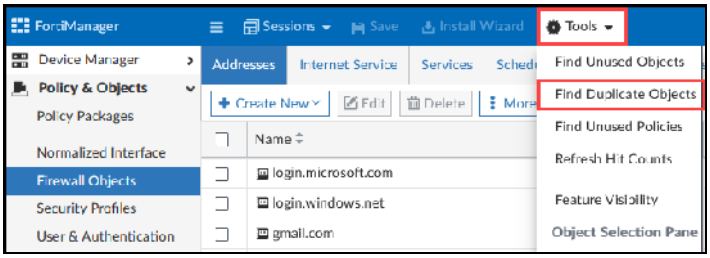
To configure policies and objects and send them for approval

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.

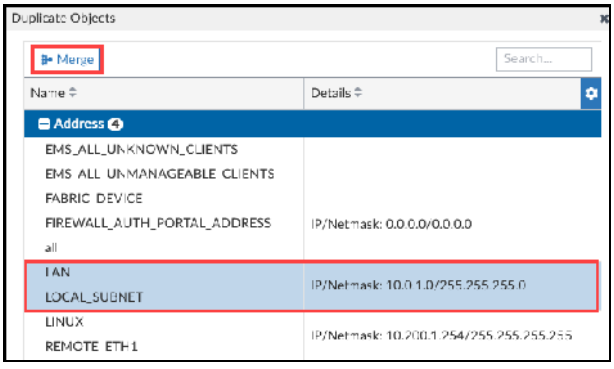
4. Click **Policy & Objects** > **Firewall Objects**.
5. Click **Sessions** > **Session List**.



6. Click **Create New Session**.
7. In the **Session Name** field, type `Training`.
8. Click **OK**.
9. Click **Tools** > **Find Duplicate Objects**.

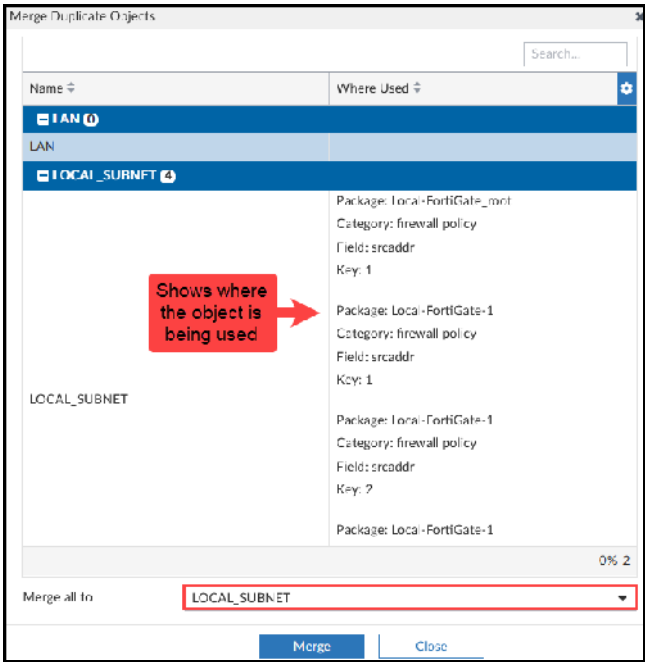


10. Expand **Address**, select the **LAN - LOCAL_SUBNET** row, and then click **Merge**.



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

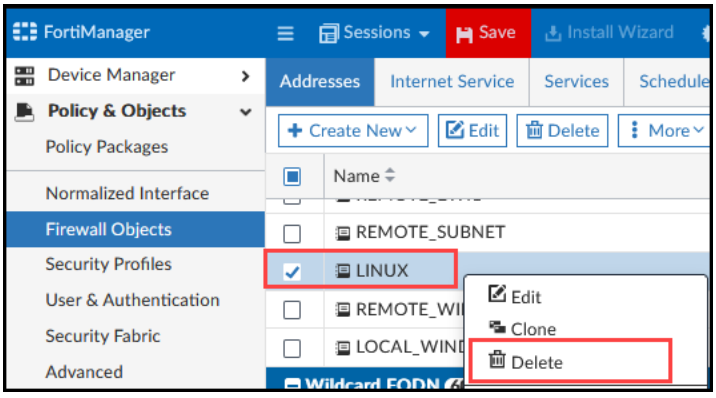
11. In the **Merge all to** field, select **LOCAL_SUBNET**.



12. Click **Merge**.
13. Click **Close**.

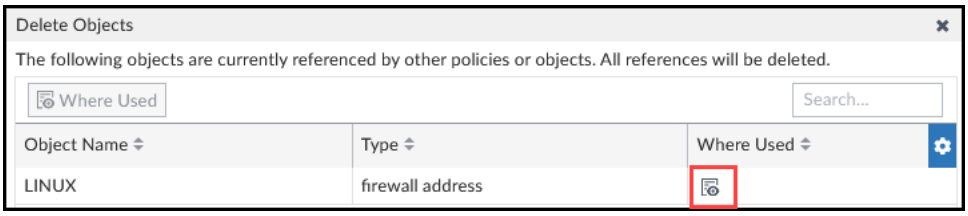
By merging the duplicate objects, you can reduce the object database, which may help to avoid overwhelming the FortiManager administrator with a large number of objects from different FortiGate devices in the same ADOM. You can also delete the unused objects in the same **Tools** menu if they will not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

14. Continuing on **Firewall Objects** > **Addresses**, right-click the **LINUX** address object, and then click **Delete**.

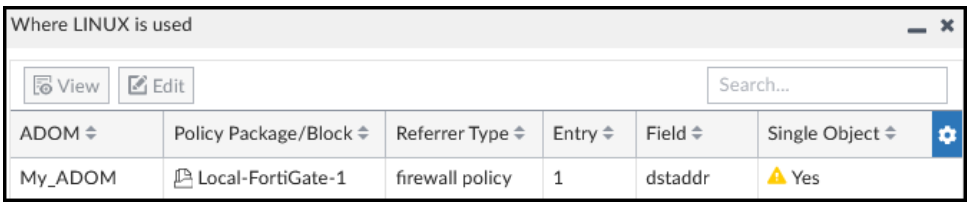


15. Click **OK** to confirm that you want to delete the object.
16. Click the **Where Used** icon.

    This shows where the object is referenced.



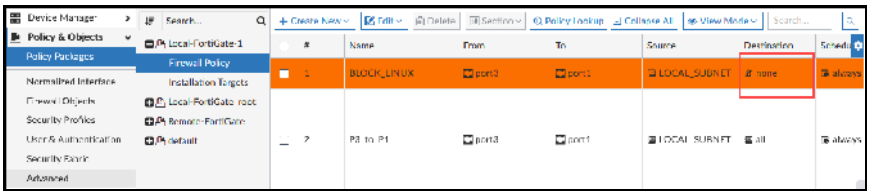
The object is referenced in the **Local-FortiGate-1** policy package in firewall policy **1** as the destination address (**dstaddr**) field.



17. Click **Close**.
18. Click **Delete Anyway**.

FortiManager allows you to delete a used object. However, you must be very careful because the object will be replaced by the **none** address 0.0.0.0/255.255.255.255.

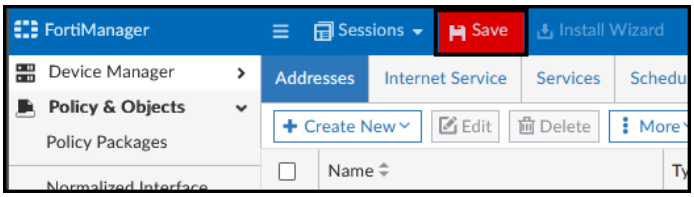
This means that any traffic that meets this specific firewall policy is blocked if there is no catch-all or shadowed policy under it. In this case, the **destination address** of firewall policy **1** in the **Local-FortiGate-1** policy package is replaced by **none** after the **LINUX** address object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



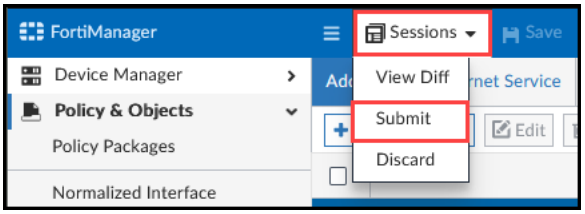
You will test this later in this exercise.

---

19. Click **Save**.



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



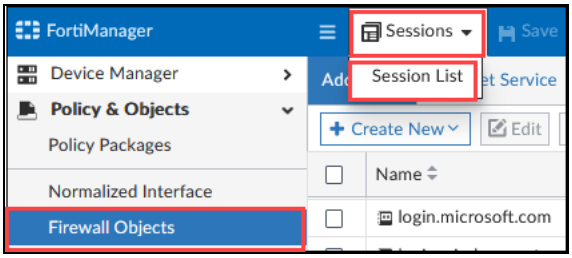
21. Click **OK**.
    The ADOM unlocks itself after you submit the changes.

Your changes are still not saved in the FortiManager database because they must first be approved by an 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**.
3. Click the lock icon to lock the ADOM.

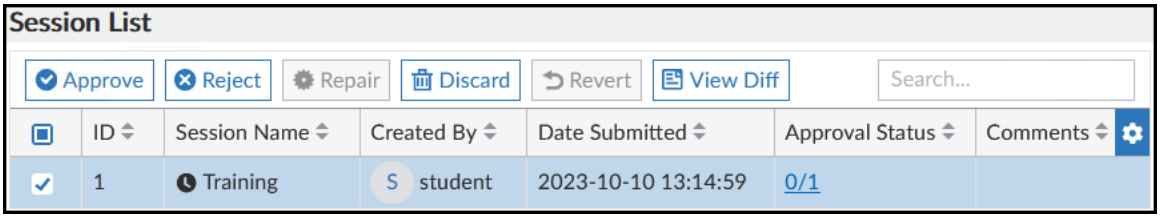
4. Click **Policy & Objects** > **Firewall Objects**.
5. Click **Sessions** > **Session List**.



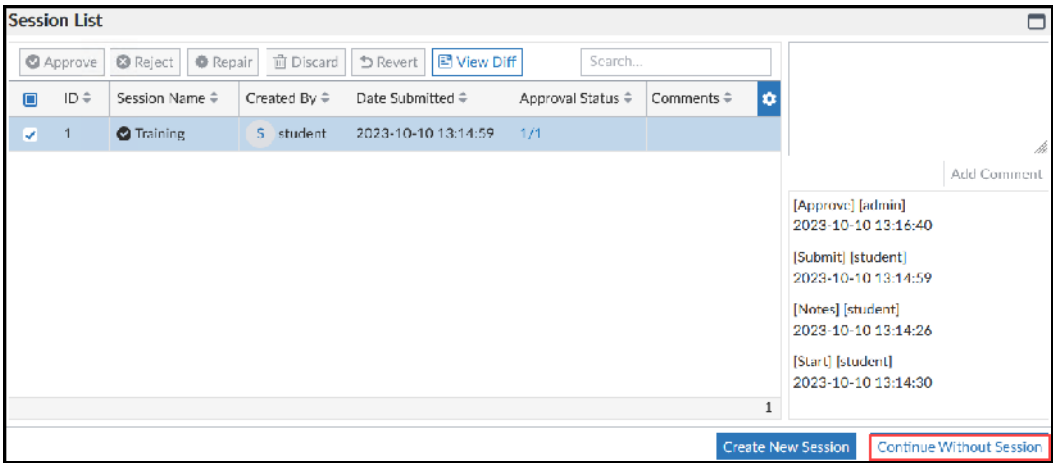
The session list shows you the name of the request made, user, date, and approval status.

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.

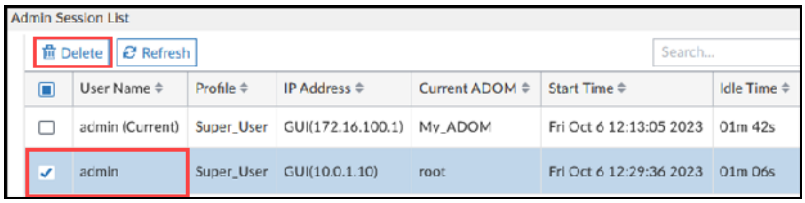
If an administrator locks ADOMs, and then logs out of the FortiManager GUI, the locks are released for all the ADOMs that the administrator locked.

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

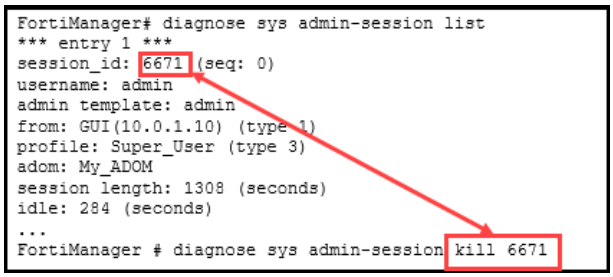
If a session is not closed gracefully (PC crash or closed browser window), FortiManager does not close the administrator session until the administrator session timeout is reached or the session is deleted. The locked ADOM remains locked.

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

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



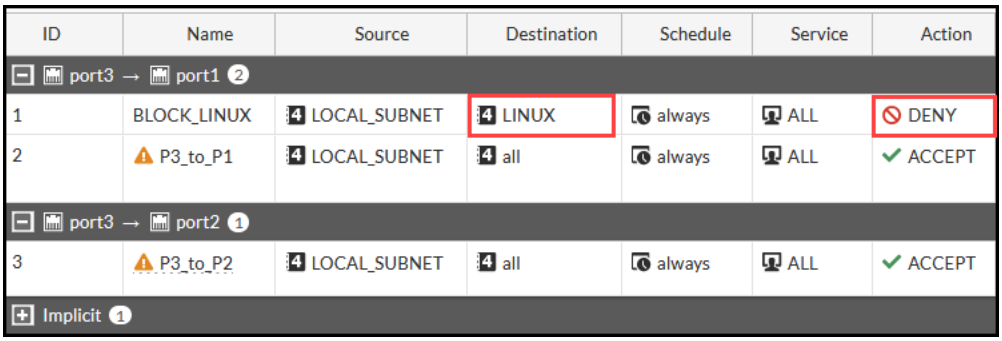
On the CLI:



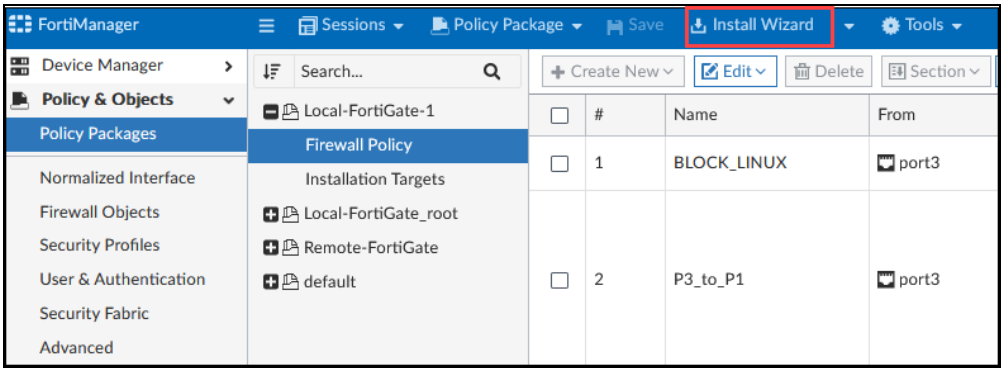
To install configuration changes after they are approved

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** > **Policy Packages**.
5. Click **Local-FortiGate-1** > **Firewall Policy**.
   You can see that **LINUX** is replaced by **none** in the destination field.
6. On the Local-Client VM, open a terminal window, and then ping the **LINUX** address object.
   ```
   ping 10.200.1.254
   ```
   You can see that the request times out because the firewall policy has the destination set to **LINUX** and the action set to **DENY** locally on Local-FortiGate.
7. Keep the terminal window that is sending the ping traffic open.
   You can connect directly to Local-FortiGate to examine its firewall policy settings. They should match the following image:



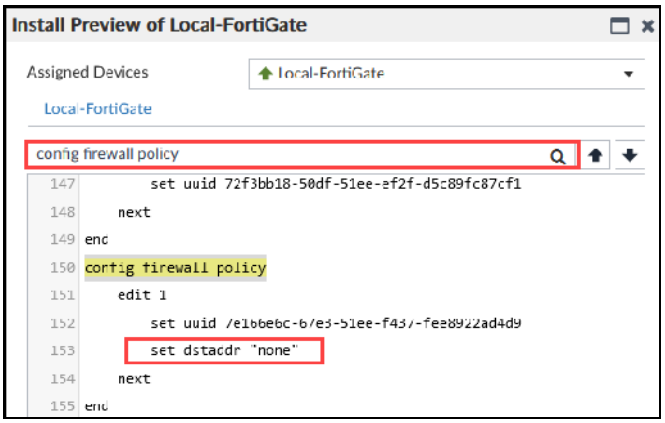
8. Return to the FortiManager GUI, and then click **Install Wizard**.

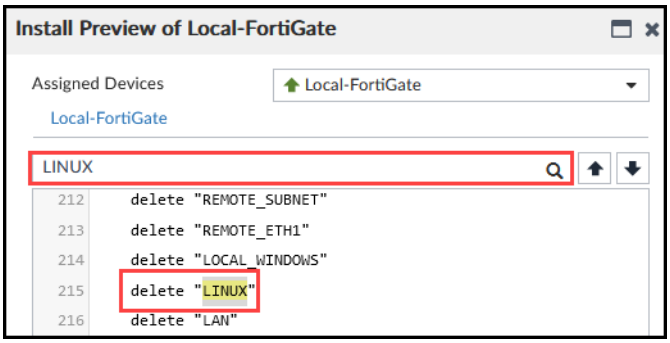


9. Make sure that the following settings are selected:
   - **Install Policy Package and Device Settings**
   - Policy Package: **Local-FortiGate-1**
10. Click **Next**.
11. Click **Next**.
12. Click **Install Preview**.
13. Using the search bar, search for the following:
    - config firewall policy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

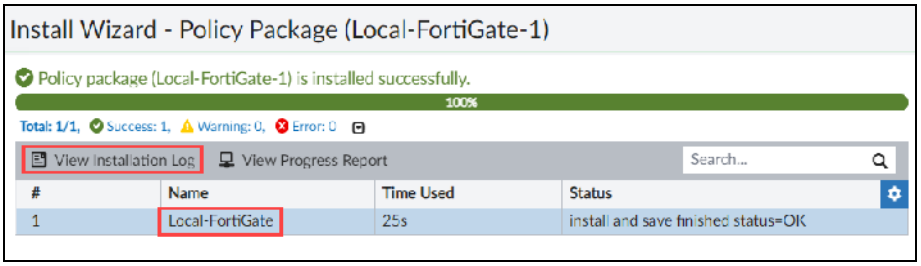
    You can see that FortiManager has replaced the destination address of firewall policy **1** with **none**, and has deleted the **LINUX** address object.

    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.





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



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

    You start to receive replies because there was a catch-all policy under the **BLOCK_LINUX** policy. After the installation, **LINUX** is replaced by **none**, and the **P3_to_P1** firewall policy starts processing the traffic, as shown in the following image taken directly on Local-FortiGate.

ID	Name	Source	Destination	Schedule	Service	Action
port3 → port1 2						
1	BLOCK_LINUX	LOCAL_SUBNET	none	always	ALL	DENY
2	P3_to_P1	LOCAL_SUBNET	all	always	ALL	ACCEPT
port3 → port2 1						
3	P3_to_P2	LOCAL_SUBNET	all	always	ALL	ACCEPT
Implicit 1						

20. Close the terminal window that is sending the ping traffic.

To disable workflow mode on the CLI

1. Open a new PuTTY window, 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:

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

   FortiManager logs out all administrators so that the changes can be saved. Therefore, before you disable workspace mode, inform all administrators logged in to the FortiManager GUI to save any changes they made that they want to keep.

4. Close the SSH session.

You can also disable workflow mode on the FortiManager GUI.

Exercise 3: Creating a Common Policy for Multiple Devices

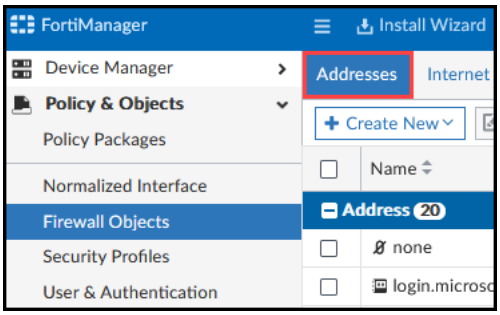
You will create a single policy package that can be shared by multiple devices, as opposed to having a policy package for each device, which is the current configuration. You will use the installation target setting in a firewall policy to target specific policies to specific FortiGate devices.

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

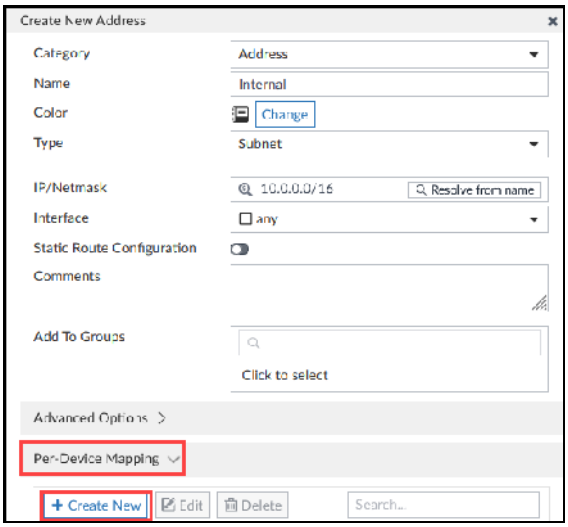
1. Log in to the FortiManager GUI with the username `student` and password `fortinet`.
2. Click **My_ADOM**.
3. Click **Policy & Objects**.
4. Click **Firewall Objects** > **Addresses**.



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

Field	Value
Name	Internal
Type	Subnet
IP/Netmask	10.0.0.0/16

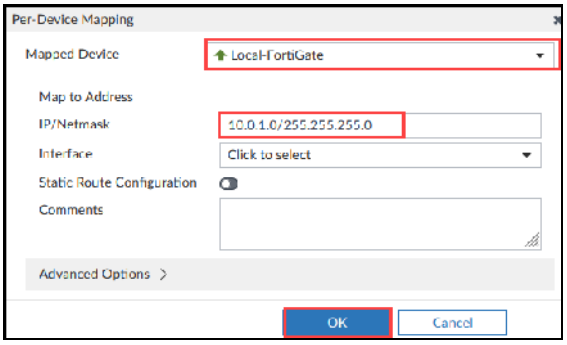
7. In the **Per-Device Mapping** section, configure the following settings:
   a. Expand **Per-Device Mapping**.
   b. Click **Create New**.



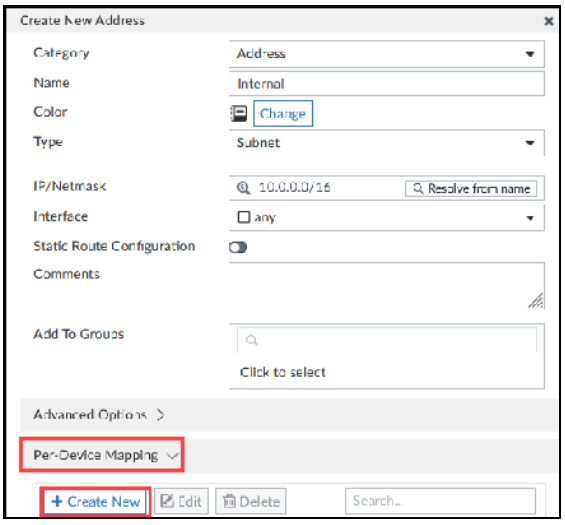
c. In the **Mapped Device** field, select **Local-FortiGate**.

d. In the **IP/NetMask** field, type `10.0.1.0/24`.

e. Click **OK**.



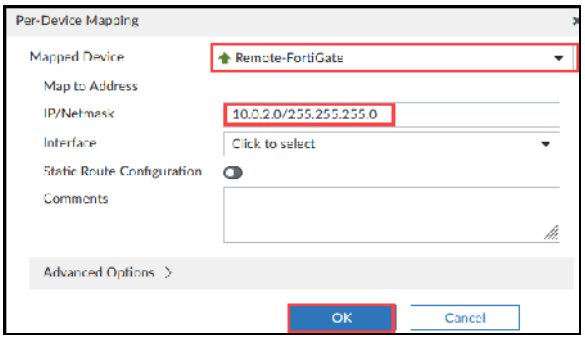
f. Click **Create New** again.



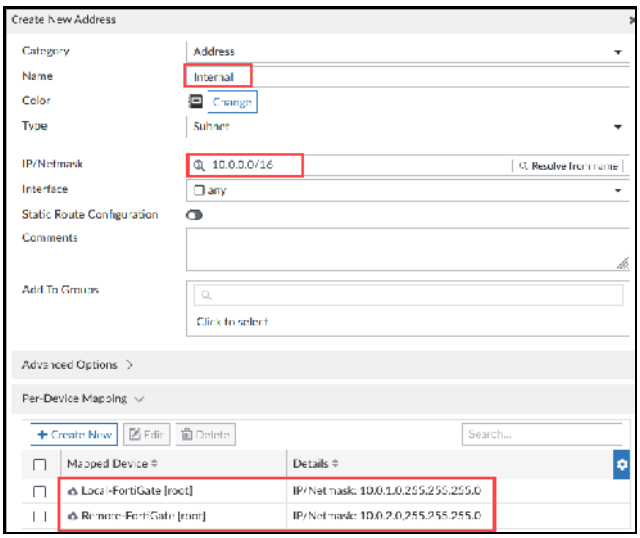
g. In the **Mapped Device** field, select **Remote-FortiGate**.

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

i. Click **OK**.



Your configuration should look like the following example:



8. In the **Change Note** field, type `New Address`.
9. Click **OK**.

Disable the Change Note Requirement

You will disable the requirement of adding a change note after making a configuration change.

To disable the change note requirement

1. Open a new PuTTY window, 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:

```
config system global
set object-revision-mandatory-note disabled
end
```

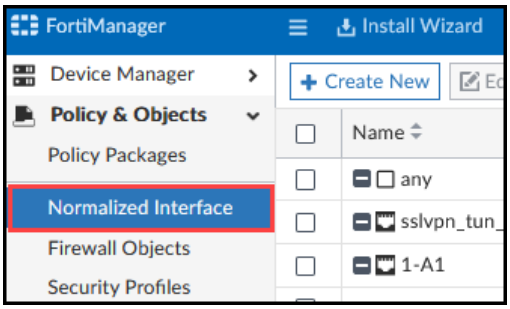
4. Close the SSH session, and then log out of the FortiManager GUI for the change to take effect.

Create Dynamic Mappings for Interfaces and Device Zones

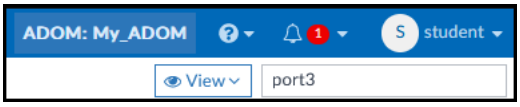
You will create dynamic mappings for interfaces and device zones.

To create dynamic mappings for interfaces

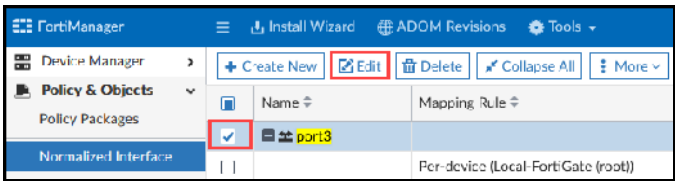
1. Log in to the FortiManager GUI with the username `student` and password `fortinet`.
2. Click **My_ADOM**.
3. Click **Policy & Objects** > **Normalized Interface**.



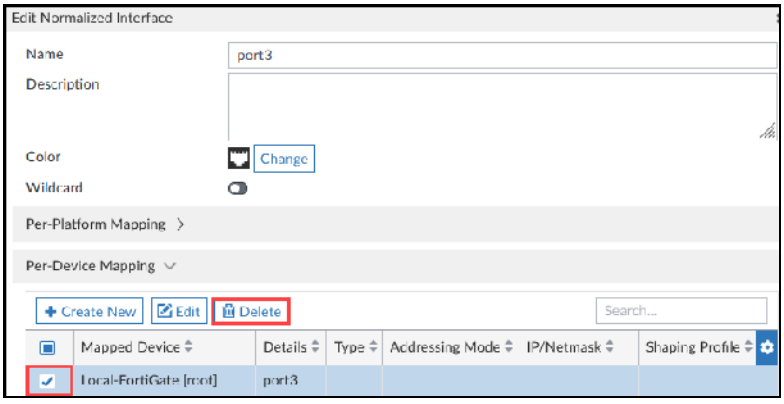
4. In the search field, type `port3`.



5. Select **port3**, and then click **Edit**.

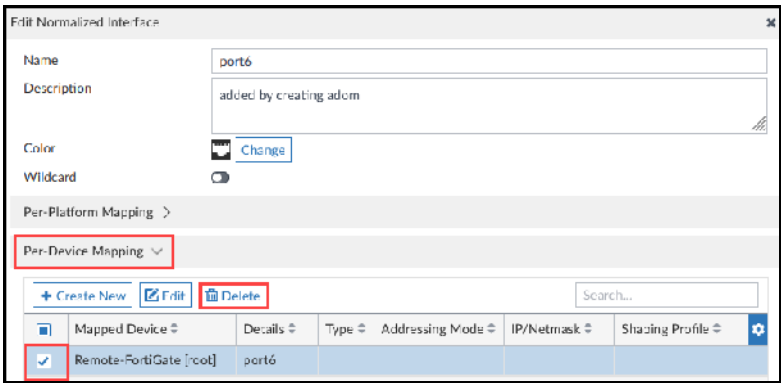


6. In the **Per-Device Mapping** section, in the **Mapped Device** column, select **Local-FortiGate(root)**, and then click **Delete**.



7. Click **OK**.
8. In the search field, type `port6`.
9. Select **port6**, and then click **Edit**.

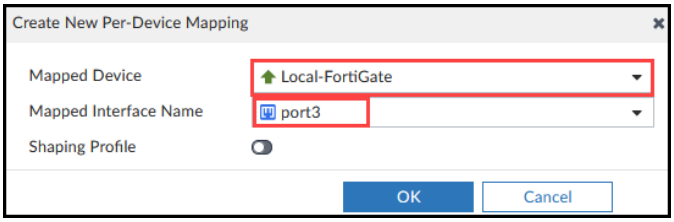
10. In the **Per-Device Mapping** section, in the **Mapped Device** column, select **Remote-FortiGate(root)**, and then click **Delete**.



11. Click **OK**.

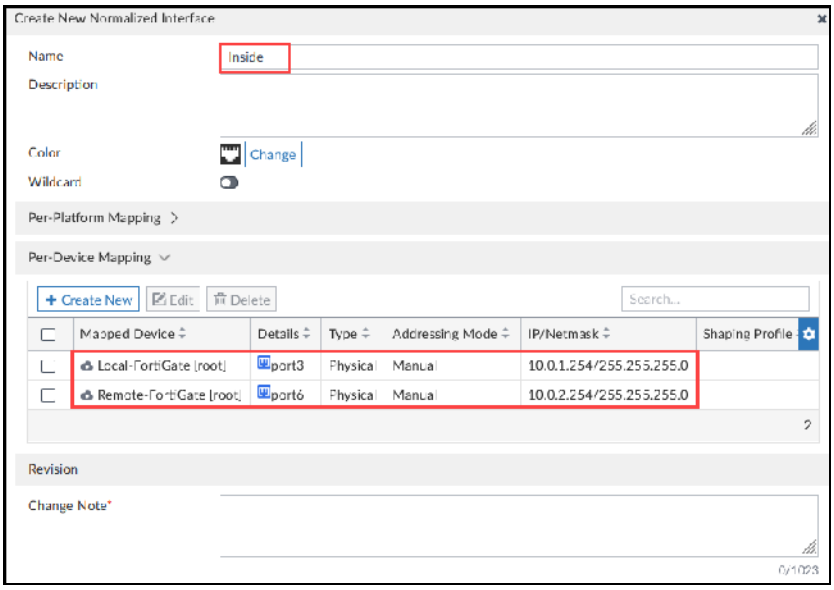
You must delete the **Per-Device Mapping**. This is because interfaces were dynamically mapped when the devices were added to FortiManager. After deleting the previous mapping, you can then map these interfaces to newly created normalized interfaces.

12. Clear the **port6** checkbox, and then click **Create New**.
13. In the **Name** field, type `Inside`.
14. Expand 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 **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 image:



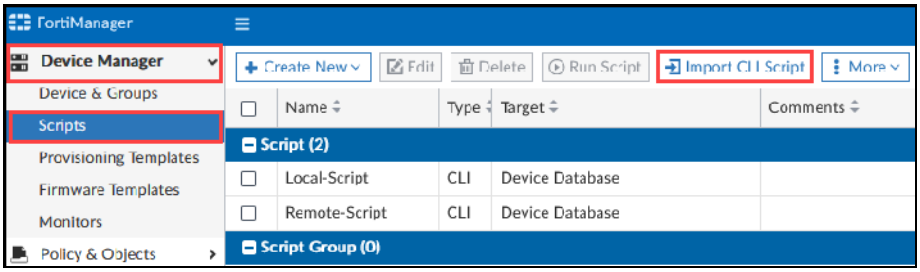
15. Click **OK**.

Import and Install a CLI Script to Delete Policies

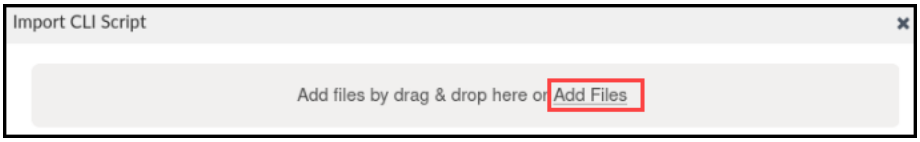
You will import and install a script on the policy package to delete policies.

To import and install a CLI script

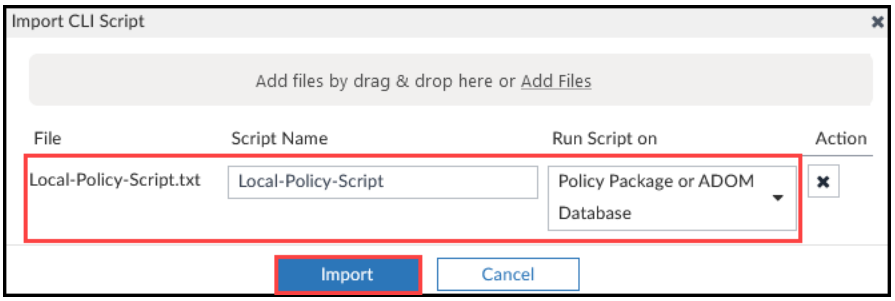
1. Continuing on the FortiManager GUI, click **Device Manager** > **Scripts** > **Import CLI Script**.



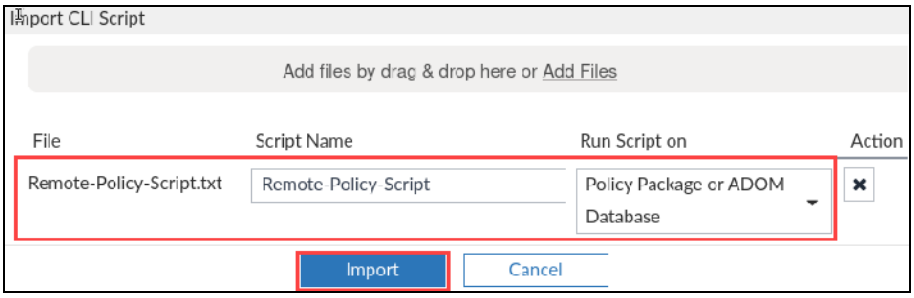
2. Click **Add Files**.



3. Click **Desktop** > **Resources** > **FortiManager-Administrator** > **Lab5-Policy** > **Lab5-Scripts**, and then select `Local-Policy-Script`.
4. Click **Open**, and then in the **Run Script on** field, select **Policy Package or ADOM Database**, as shown in the following image:



5. Click **Import**.
6. Click **Close**.
7. Click **Import CLI Script** again.
8. Click **Add Files**.
9. Click **Desktop** > **Resources** > **FortiManager-Administrator** > **Lab5-Policy** > **Lab5-Scripts**, and then select `Remote-Policy-Script`.
10. Click **Open**, and then in the **Run Script on** field, select **Policy Package or ADOM Database**, as shown in the following image:



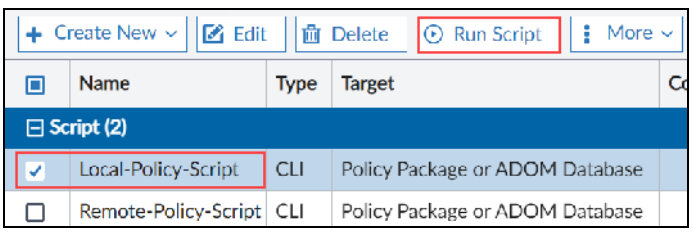
11. Click **Import**.
12. Click **Close**.

Run and Install the Scripts

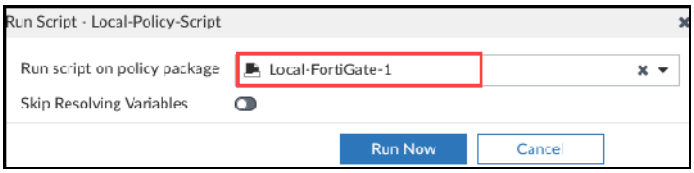
Because the scripts are targeting the policy package, you will first run the scripts against the policy package, and then install the scripts on the managed devices.

To run the scripts

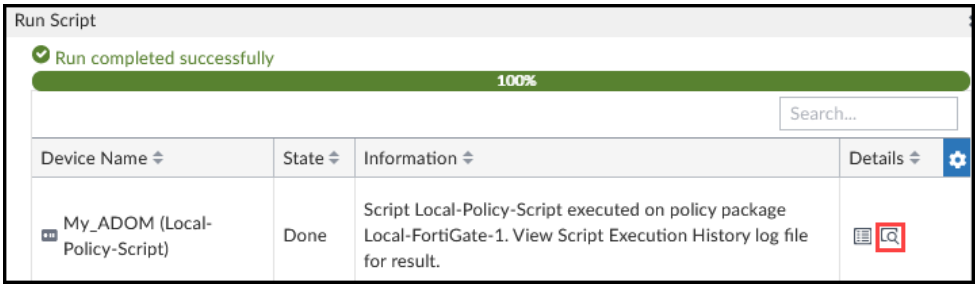
1. Continuing on the FortiManager GUI, select the **Local-Policy-Script** checkbox, and then click **Run Script**.



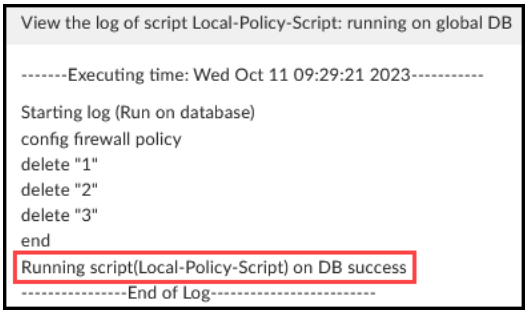
2. In the **Run script on policy package** field, select **Local-FortiGate-1**.



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

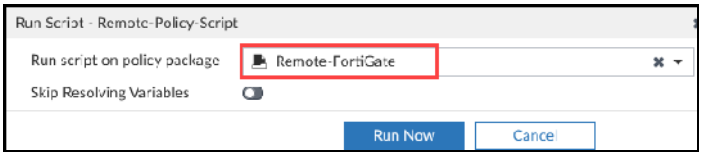


5. Scroll to the bottom of the script execution window to confirm that the script ran successfully on the policy package.



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

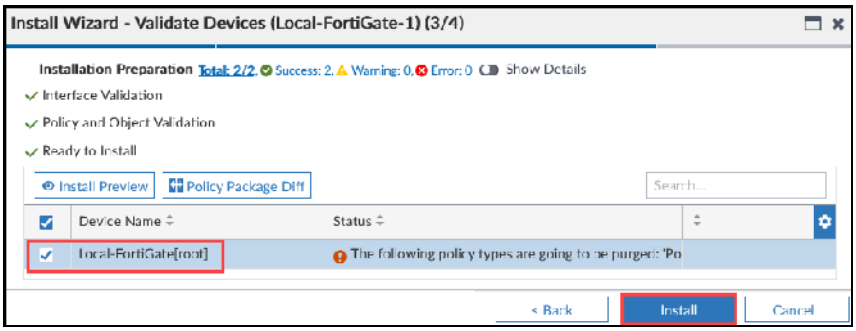
6. Click **Close**.
7. Click **Close** again.
8. Clear the **Local-Policy-Script** checkbox, select the **Remote-Policy-Script** checkbox, and then click **Run Script**.
9. In the **Run script on policy package** field, select **Remote-FortiGate**.



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

To install the 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. Click **Install**.

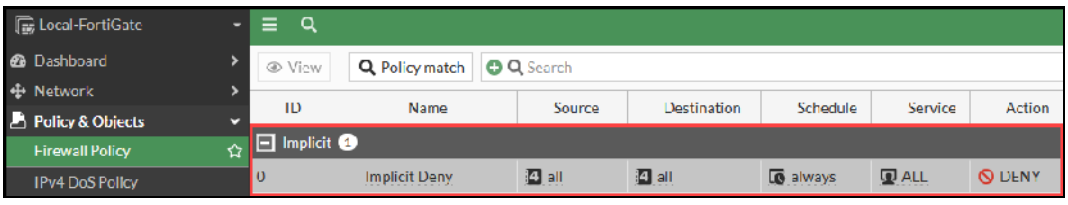


7. After the installation ends, click **Finish**.
8. Click **Install**, and then click **Install Wizard**.
9. Select **Install Policy Package & Device Settings**, and then in the **Policy Package** field, select **Remote-FortiGate**.
10. Click **Next**.
11. Make sure that **Remote-FortiGate** is selected,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

At this point, both FortiGate devices should show a **Config Status** of **Synchronized**, and a **Policy Package Status** of **Installed**.

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**.
   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`.

You cannot access Remote-FortiGate from the Local-Client VM because all firewall policies were removed. To perform this step, you must access Remote-FortiGate from the Remote-Client VM, or connect directly to Remote-FortiGate.

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!

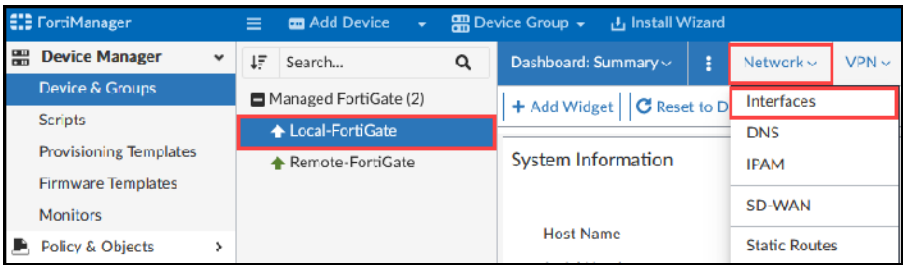
Why did you delete the policies on the FortiGate devices?

This is because the policies are already using some ports in the configuration. You cannot add interfaces to the zone that the policies on the FortiGate are already using.

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

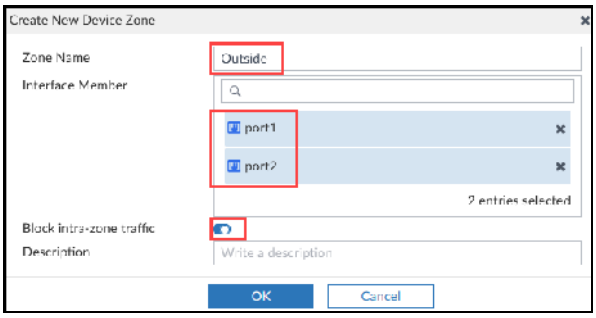
To create dynamic mappings for device zones

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

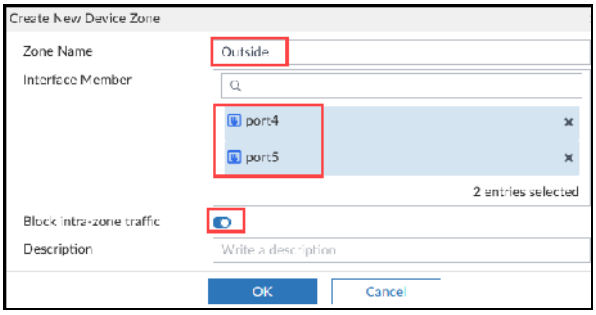


When you create a device zone, map the zone to a physical interface. To use the zone in a policy, you must also map the zone to a normalized interface.

3. Click **Create New** > **Device Zone**.
4. In the **Zone Name** field, type `Outside`.
5. Configure the following:
   a. In the **Interface Member** field, select **port1** and **port2**.
   b. Enable **Block intra-zone traffic**.
   c. Click **OK**.

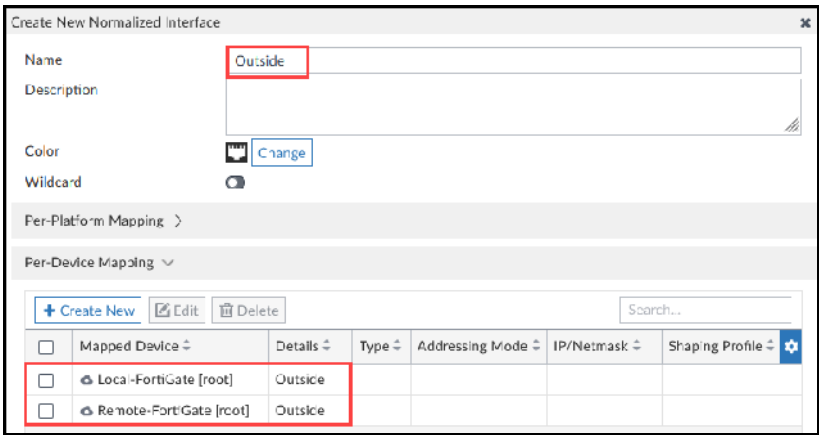


6. Click **Managed FortiGate** > **Remote-FortiGate**.
7. Click **Network** > **Interfaces**.
8. Click **Create New** > **Device Zone** again.
9. In the **Zone Name** field, type `Outside`.
10. Configure the following:
    a. In the **Interface Member** field, select **port4** and **port5**.
    b. Enable **Block intra-zone traffic**.
    c. Click **OK**.



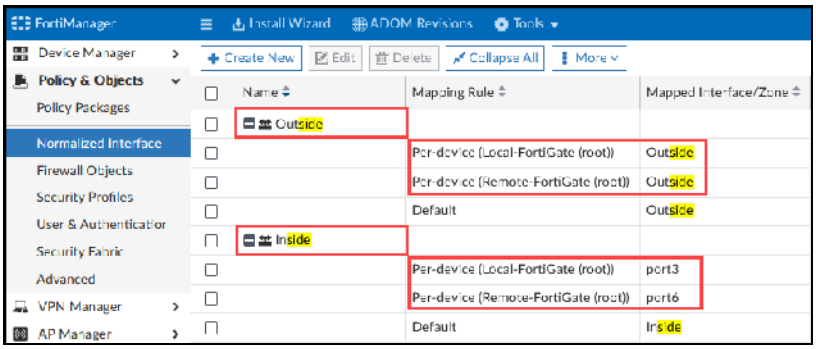
11. Click **Policy & Objects** > **Normalized Interface**.
12. Click **Create New**.
13. In the **Name** field, type `Outside`.
14. In the **Per-Device Mapping** section, click **Create New**, and then configure the following settings:
    a. In the **Mapped Device** field, select **Local-FortiGate**.
    b. In the **Mapped Interface Name** field, select **Outside**.
    c. Click **OK**.
15. Click **Create New** again.
16. 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**.
    c. Click **OK**.

    Your configuration should look like the following image:



17. Click **OK**.

    You have now created a dynamic interface and device zones.

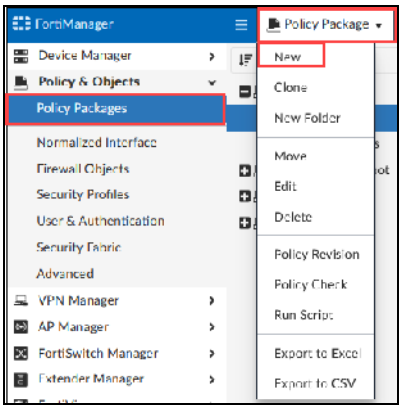


Create a Common Policy Package, an Installation Target, and Use Install On

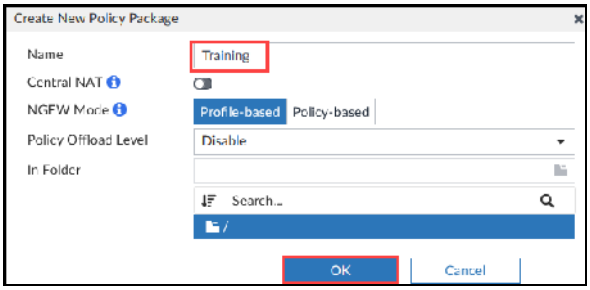
You can use FortiManager to target a common policy package to multiple devices. When you configure an installation target, by default, all policies in the policy package are targeted to all selected FortiGate devices. You can further restrict the policies in the policy package to be targeted to specific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

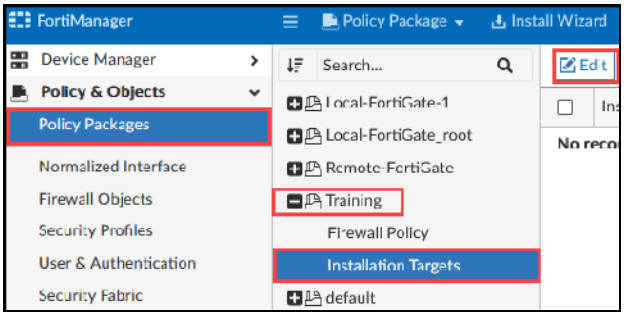


2. In the **Name** field, type `Training`, and then click **OK**.



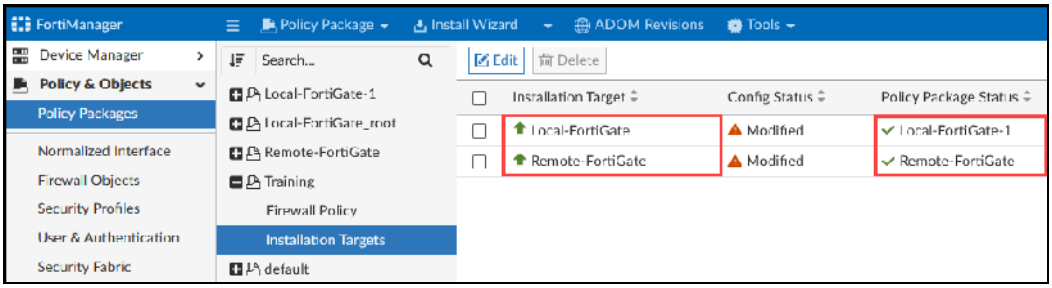
To configure an installation target and use Install On

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

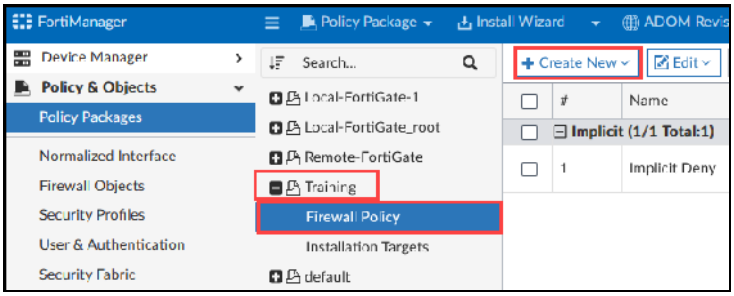


3. Select **Local-FortiGate** and **Remote-FortiGate**, and then add them to the **Selected Entries** section.
4. Click **OK**.

   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**.

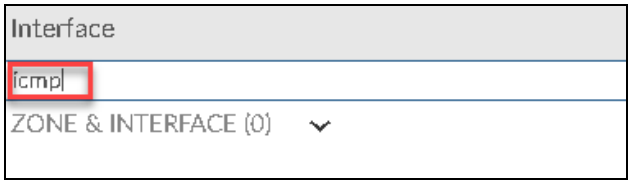


7. Configure the following settings:

Field	Value
Name	For_Local-FortiGate
Incoming Interface	Inside
Outgoing Interface	Outside
Source	Internal
Destination	all
Service	HTTP, HTTPS, ALL_ICMP
Schedule	always
Action	Accept
NAT	Enabled

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

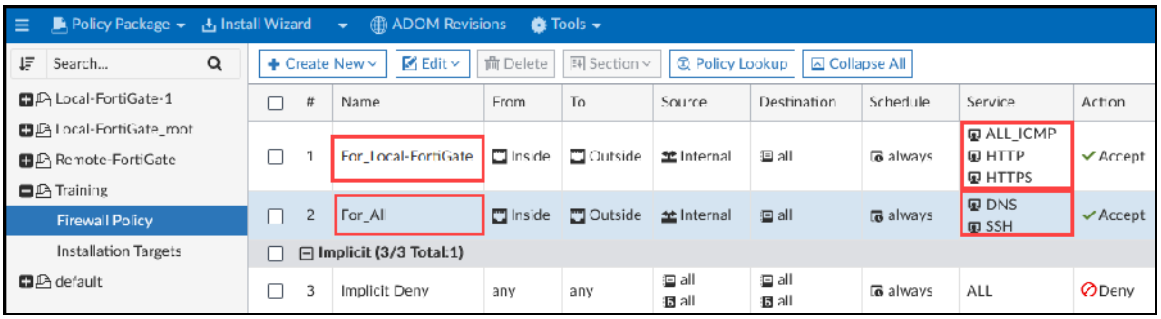
When you create the second policy, if you do not see all of the interfaces, make sure that you clear the interface filter when you select the interfaces.



Field	Value
Name	For_All
Incoming Interface	Inside

Field	Value
Outgoing Interface	Outside
Sources	Internal
Destination	all
Service	SSH, DNS
Schedule	always
Action	Accept
NAT	Enabled

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

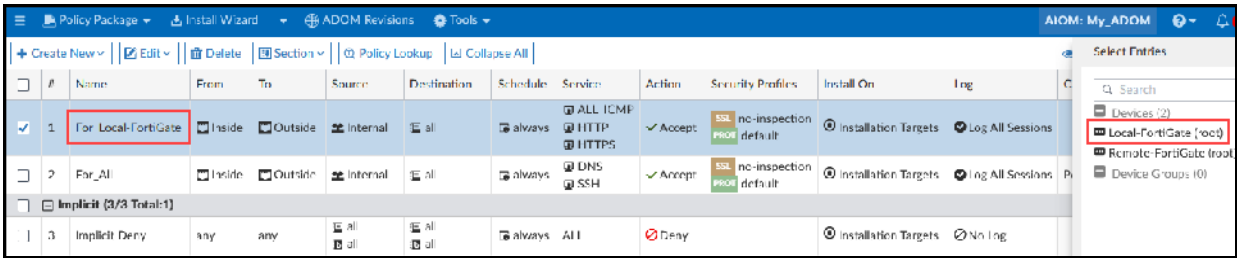


11. Scroll to the right to find the **Install On** column.
    Optionally, you can drag the column to where you want it positioned for easier access.

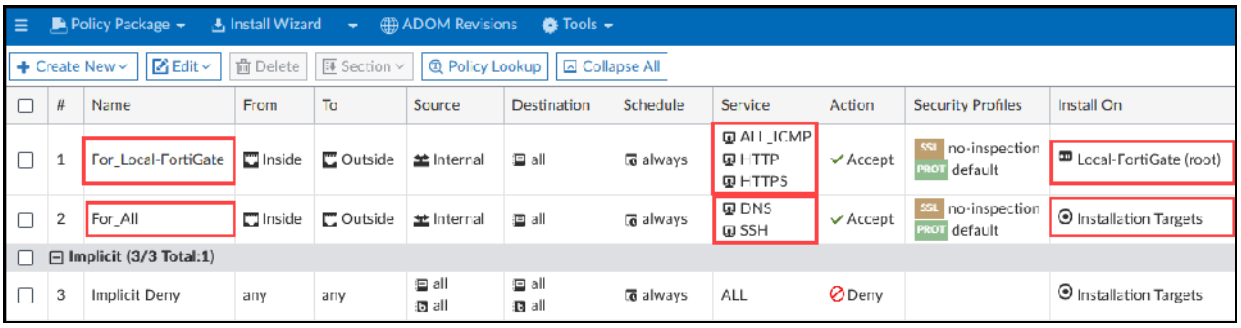
12. For the **For_Local-FortiGate** policy, hover over the **Installation Targets** field, and then click the **Edit** icon.

Depending on the browser you use, you may need to refresh the page to be able to see the list of devices on the next step.

13. Select **Local-FortiGate(root)**, and then click **Apply**.

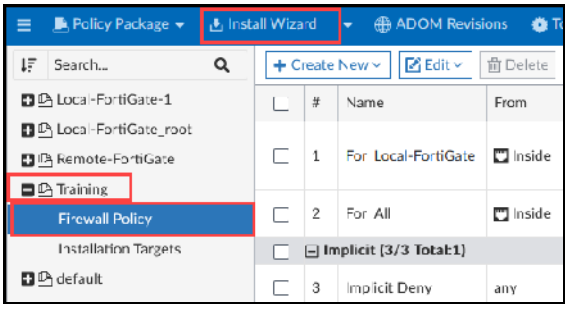


Your policies should look like the following image:

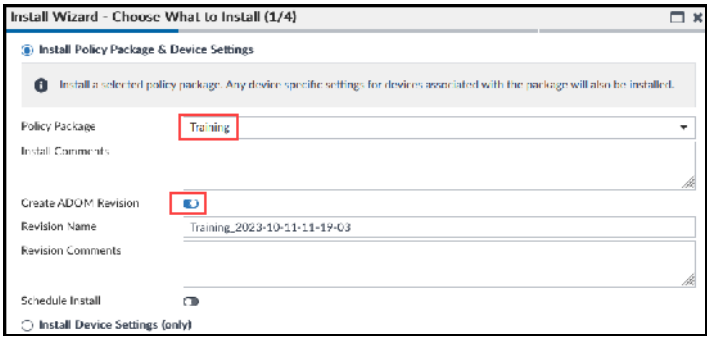


To install a policy package

1. Continuing on **Training** > **Firewall Policy**, click **Install Wizard**.

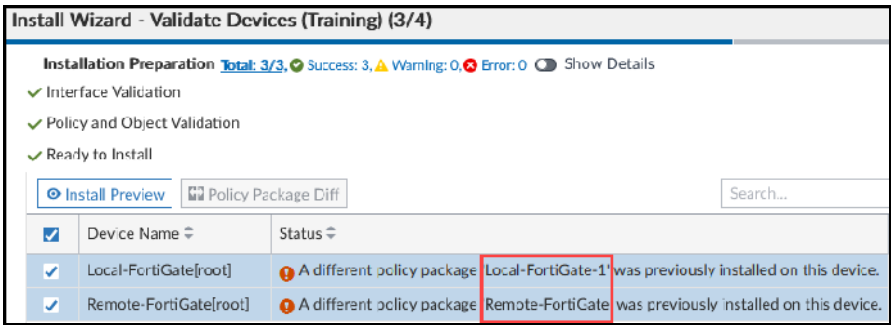


2. Make sure the following settings are selected:
   - **Install Policy Package & Device Settings**
   - Policy Package: **Training**
3. Select the **Create ADOM Revision** checkbox, and then leave the **Revision Name** field at the default value.

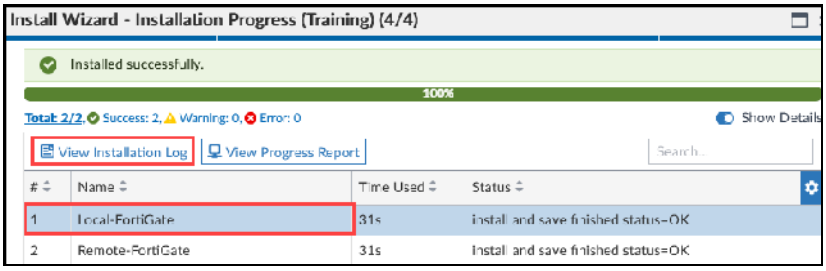


4. Click **Next**.
5. Make sure that both of the FortiGate devices are selected, and then click **Next**.
   If you expand, or the hover over the **Status** column, the name of the previous policy package is displayed.

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



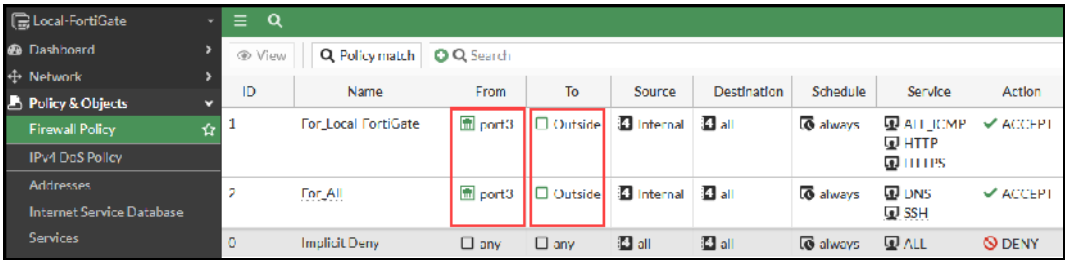
6. Make sure that both of the FortiGate devices are selected, and then click **Install**.
7. After the installation is successful, click **View Installation Log** to see the installation history for each FortiGate.



8. In the **View Install Log** window, click **Close**.
9. 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.



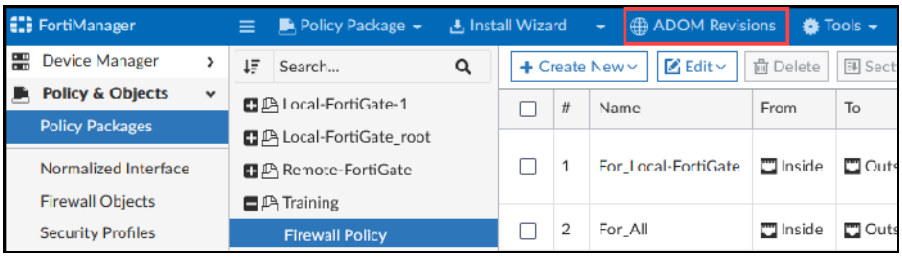
4. Click **Addresses**.
   Internal is translated to `10.0.1.0/24`, according to the dynamic mapping of address objects.
5. Click **Network** > **Interfaces**.
   An **Outside** zone is created with port1 and port2 interfaces, according to the dynamic mapping of interfaces and zones.

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**, and then select the **By Sequence** view.
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.

    Optionally, you can check the interface and zone under **Network**, and the **Internal** address object under **Addresses**, which is translated to `10.0.2.0/24`, according to the dynamic mapping of address objects.

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.

6. You can now log out of the FortiManager GUI.

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

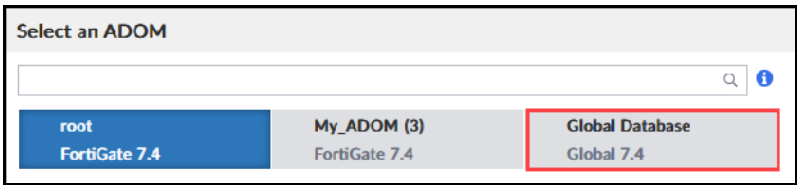
Exercise 1: Creating and Assigning Header Policies in the Global ADOM

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.

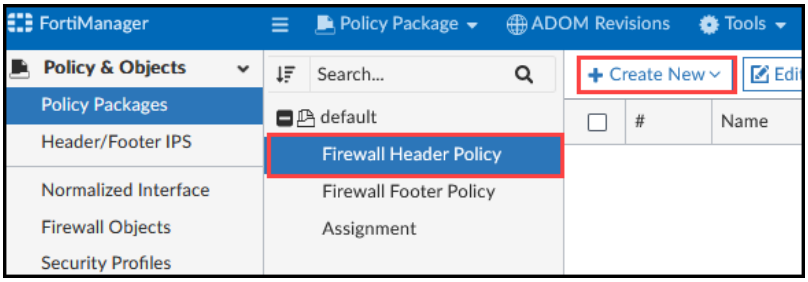
In this exercise, you will create the header policy in the global ADOM, and then assign the header policy to the managed devices in **My_ADOM**. Next, you will install the header policy on the managed devices.

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** > **Create New**.

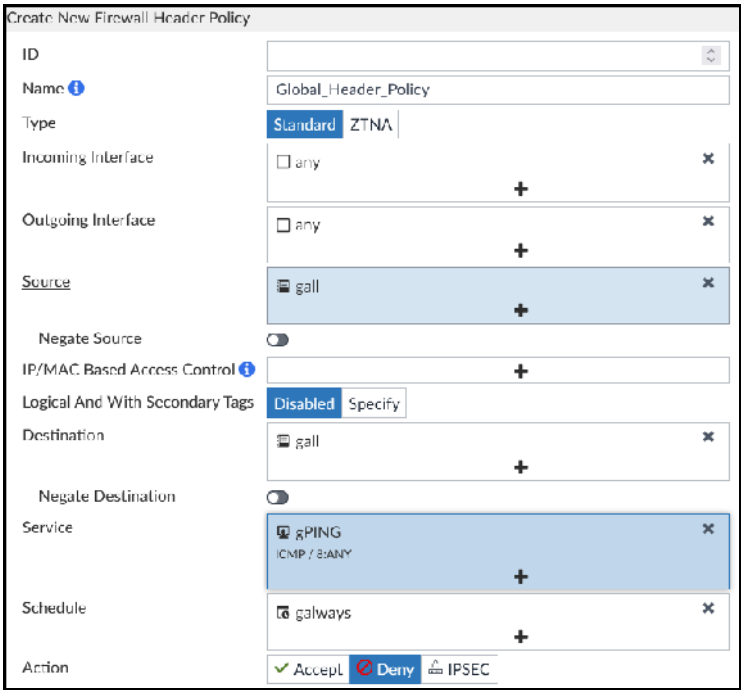


4. Configure the following settings:

Field	Value
ID	Leave this field empty. The ID is automatically generated.
Name	Global_Header_Policy
Incoming Interface	any
Outgoing Interface	any
Source	gall
Destination	gall
Service	gPING
Schedule	galways

Field	Value
Action	Deny

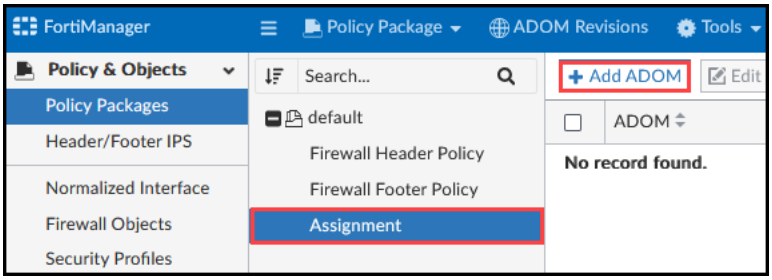
Your configuration should look like the following image (not all fields are shown):



5. Click **OK**.

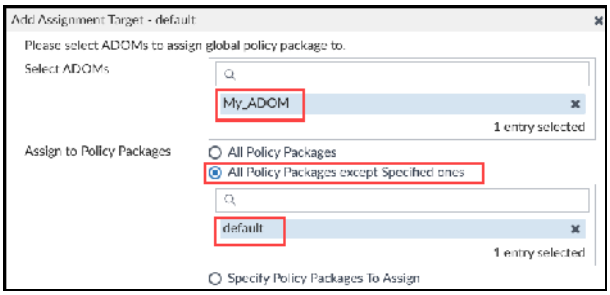
To assign a header policy

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

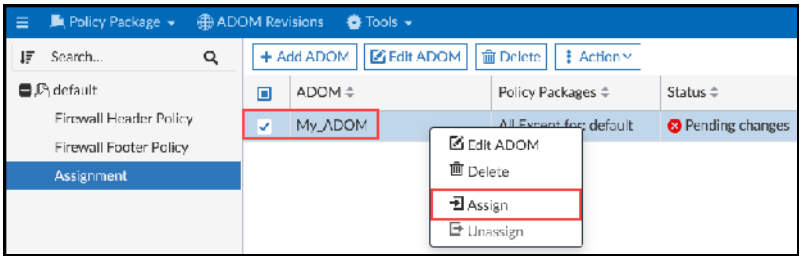


3. Configure the following settings:

Field	Value
Select ADOMs	My_ADOM
Assign to Policy Packages	Select **All Policy Packages except Specified ones**, and then select **default**.



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

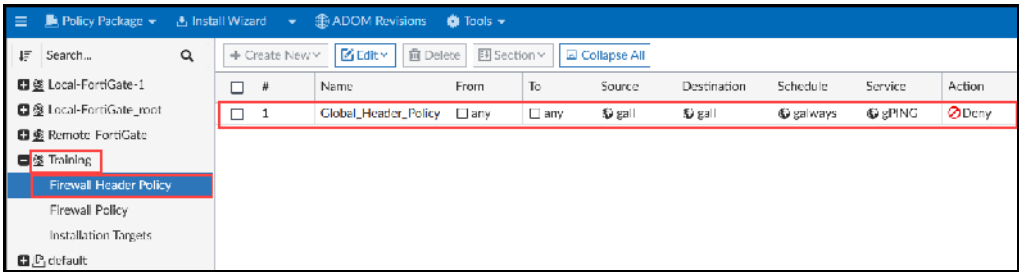


6. Click **Start to Assign**.
   FortiManager assigns the header policy to all policy packages except **default**.
7. Click **Close**.

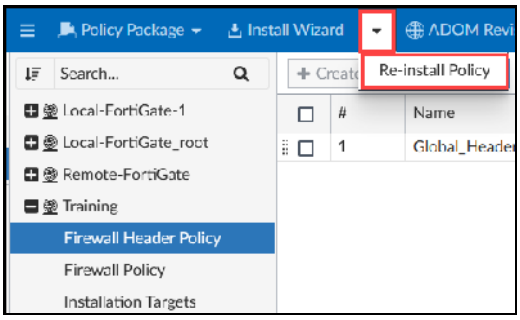
To install a header policy

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

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

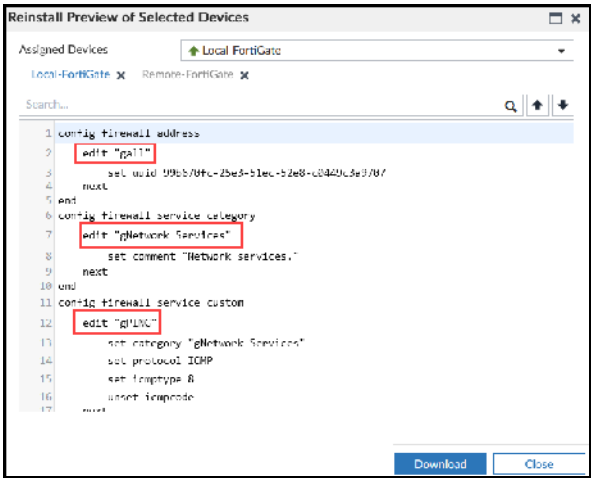


4. Click **Install Wizard** > **Re-install Policy**.



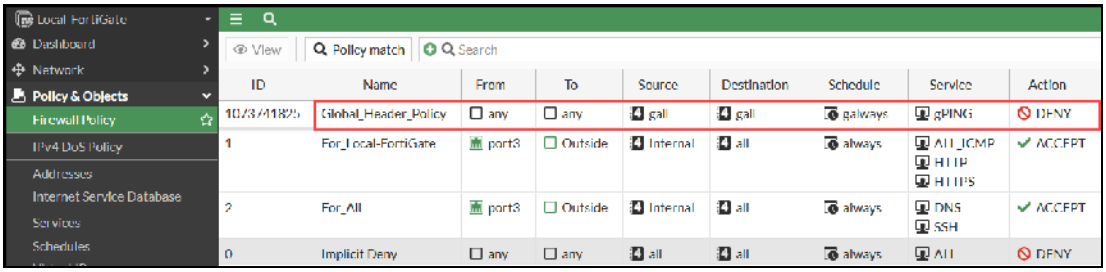
5. Click **OK**.
6. Click **Install Preview**.

   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`.
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.

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

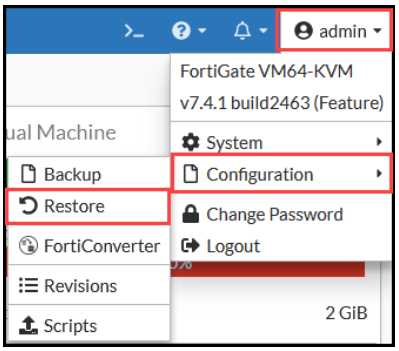
Estimated: 30 minutes

Prerequisites

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

To restore the FortiGate configuration file on both FortiGate devices

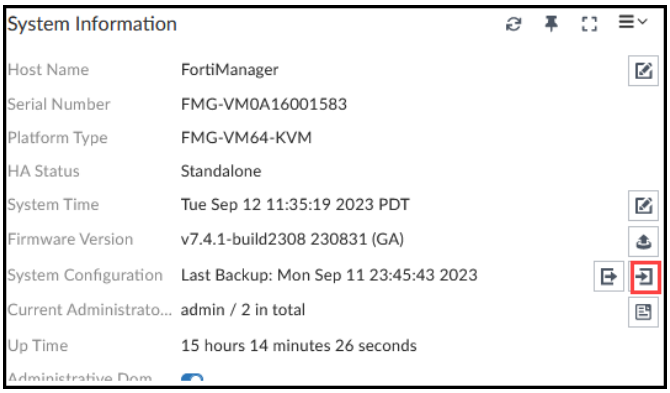
1. On the Local-Client VM, open a browser, and then log in to the Remote-FortiGate GUI with the username `admin` and password `password`.
2. Click **Login Read-Write**.
3. Click **Yes**.
4. In the upper-right corner, click **admin**, and then click **Configuration** > **Restore**.



5. Click **Local PC**, and then click **Upload**.
6. Click **Desktop** > **Resources** > **FortiManager-Administrator** > **Lab7-Troubleshooting** > **Lab7-Initial-Config**, and then select the `Remote-diag.conf` file.
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 **Lab7-Troubleshooting** > **Lab7-Initial-Config** folder, select the `Local-diag.conf` file.
11. After the reboot finishes, close both browser tabs.

To restore the FortiManager configuration

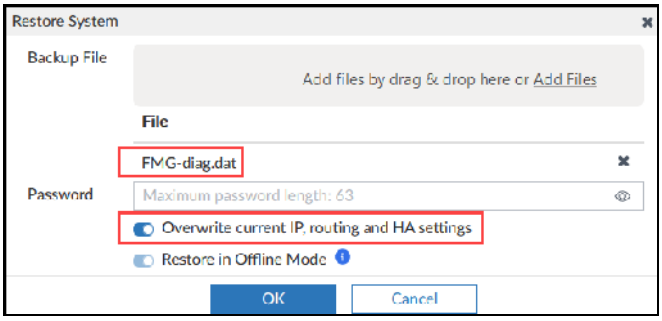
1. On the Local-Client VM, open a browser, and then log in to the FortiManager GUI with the username `admin` and password `password`.
2. Click **root**.
3. Click **System Settings**.
4. In the **System Information** widget, in the **System Configuration** field, click the **Restore** icon.



5. Click **Add Files**.
6. Click **Desktop** > **Resources** > **FortiManager-Administrator** > **Lab7-Troubleshooting** > **Lab7-Initial-Config**, and then select the `FMG-diag.dat` file.

   You do not have to enter a password because the file is not encrypted.

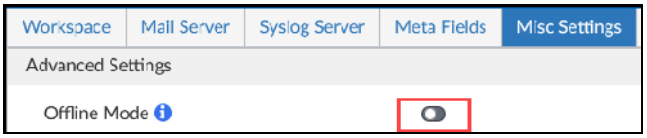
7. Leave **Overwrite current IP, routing and HA settings** enabled.



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** > **Advanced** > **Misc Settings**, and then disable **Offline Mode**.



12. Click **Apply**, and then refresh the page to confirm the **Offline Mode** message disappears.

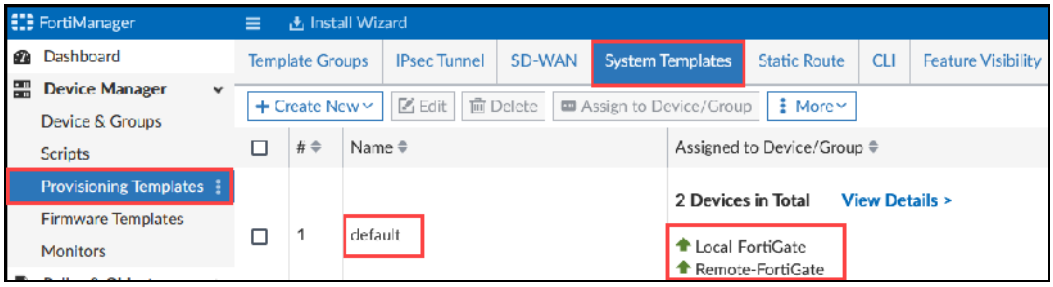
    Now, FortiManager can establish a management connection with the managed devices.

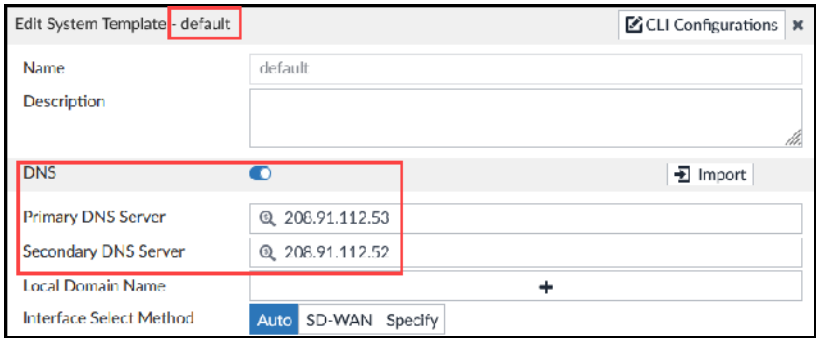
13. Log out of the FortiManager GUI before you begin the next exercise.

Exercise 1: Diagnosing and Troubleshooting Installation Issues

FortiManager is preconfigured as follows:

- ADOMs are enabled.
- **ADOM1** is configured for FortiGate firmware version 7.4.
- FortiManager is managing Local-FortiGate and Remote-FortiGate in **ADOM1**—the Remote-FortiGate policy package is not imported.
- The **default** system template is applied to Local-FortiGate and Remote-FortiGate, and the only widget it has configured is **DNS**.





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

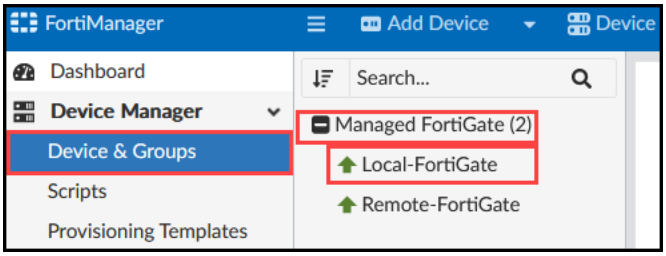
View the Installation Preview

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 settings on the FortiGate devices.

To view the installation preview for Local-FortiGate

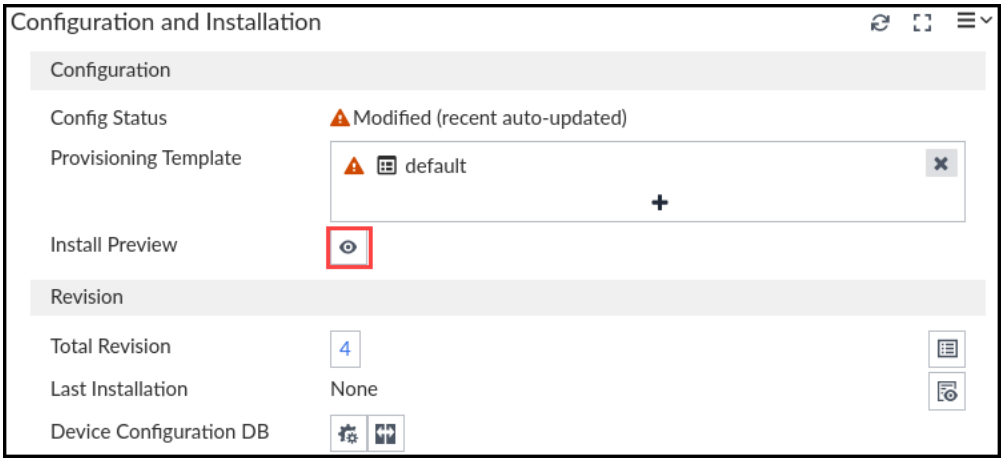
1. Log in to the FortiManager GUI with the username `student` and password `fortinet`.
2. Click **ADOM1**.

3. Click **Device Manager** > **Device & Groups** > **Managed FortiGate** > **Local-FortiGate**.



4. In the **Configuration and Installation** widget, in the **Install Preview** field, click the icon.
   Notice that **default** is listed as the template that is assigned to Local-FortiGate.

   The installation preview generates.



5. In the following table, write down the DNS settings that FortiManager will install on Local-FortiGate:

Primary:
Secondary:

6. Click **Close**.

To view the installation preview for Remote-FortiGate

1. On the FortiManager GUI, click **Remote-FortiGate**.
2. In the **Configuration and Installation** widget, in the **Install Preview** field, click the icon.
3. In the following table, 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 next 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-Client VM, open PuTTY, and then connect over SSH to the **FortiManager** saved session.
   It is recommended that you maximize the window with the SSH session to make the output easier to read.
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:

```
FortiManager # 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 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 display the command options.

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 "system dns"
   ```

   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 "system dns"
   ```

   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
   ```

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.

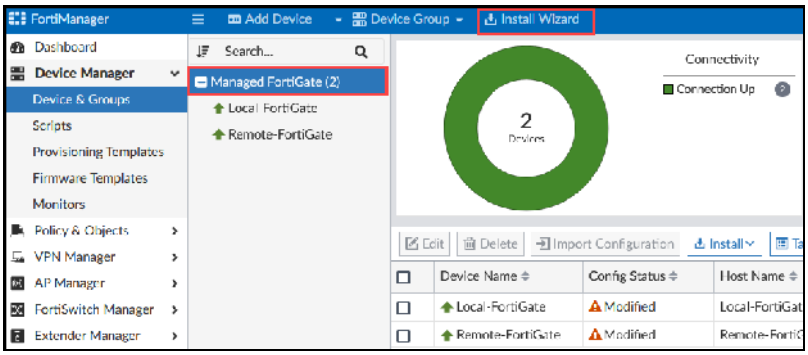
4. Close the PuTTY session.

Install Device-Level Configuration Changes

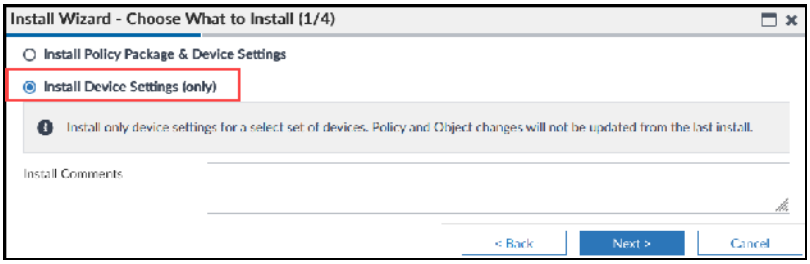
You will install device-level configuration changes (system templates) on the managed FortiGate devices.

To install device-level changes (system templates)

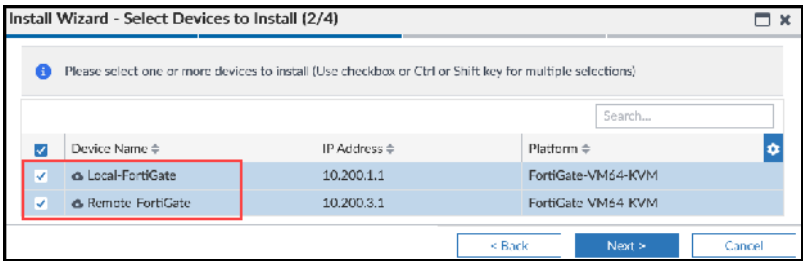
1. Return to the FortiManager GUI, and then click **Managed FortiGate**.
2. Click **Install Wizard**.



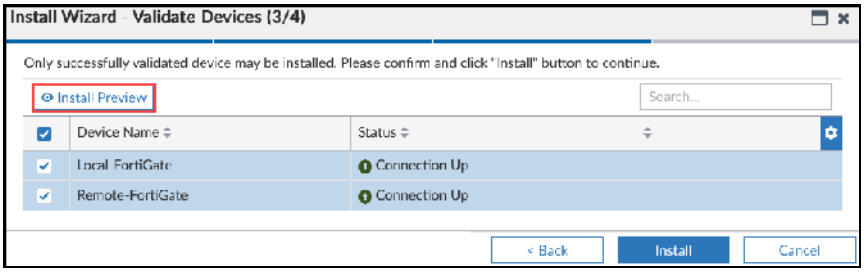
3. Select **Install Device Settings (only)**, and then click **Next**.



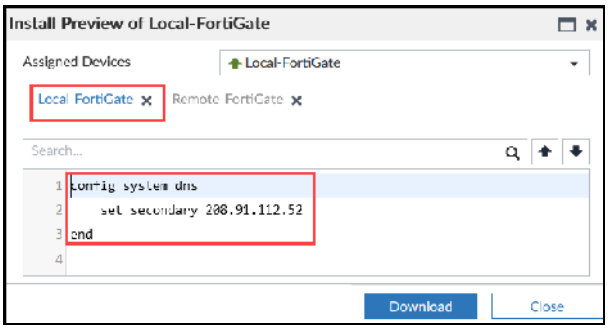
4. Make sure both devices are selected, and then click **Next**.



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

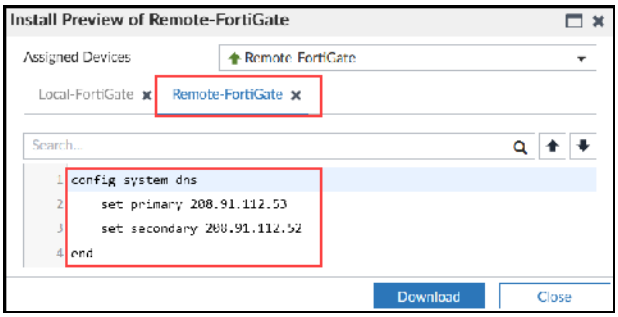


The preview generates and displays the configuration to be added to each device in separate tabs.



Optionally, you can download the preview.

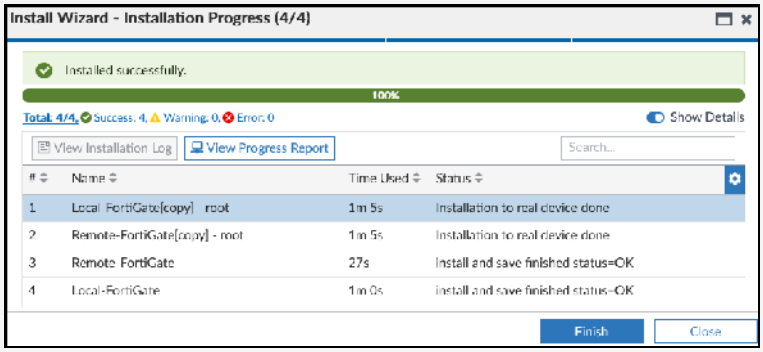
6. For the Remote-FortiGate install preview, click **Remote-FortiGate**.



7. Click **Close**.
8. Make sure both FortiGate devices are selected, click **Install**, and then wait for the installation to finish.

Stop and think!

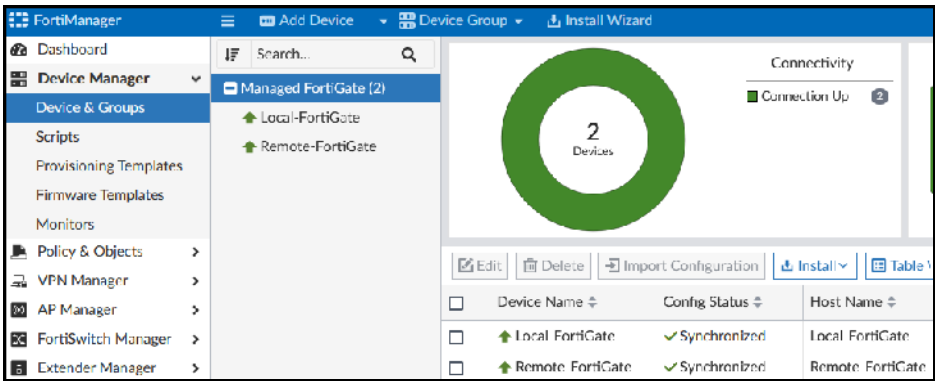
Why does FortiManager show two progress bars when installing changes on a FortiGate?



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.

9. Click **Finish**.

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



10. Keep the FortiManager session open for the next exercise.

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.

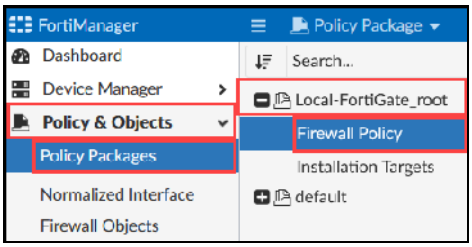
You will also diagnose and troubleshoot issues that occur while you import the Remote-FortiGate policy package.

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.

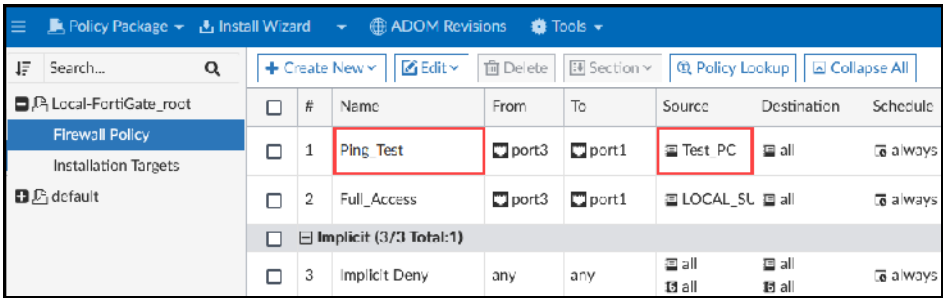
To view the policy package and objects for Local-FortiGate

1. On the FortiManager GUI, click **Policy & Objects** > **Policy Packages**.
2. Expand **Local-FortiGate_root**, and then click **Firewall Policy**.



You can see the two policies for Local-FortiGate.

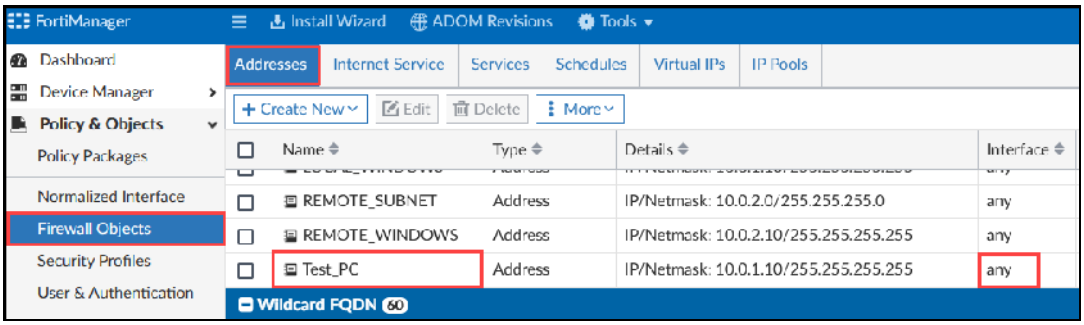
3. Notice the source address of **Test_PC** for the **Ping_Test** firewall policy.



4. Click **Firewall Objects**, and then click **Addresses**.
5. 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.

   You can use the search bar to find the **Test_PC** entry.

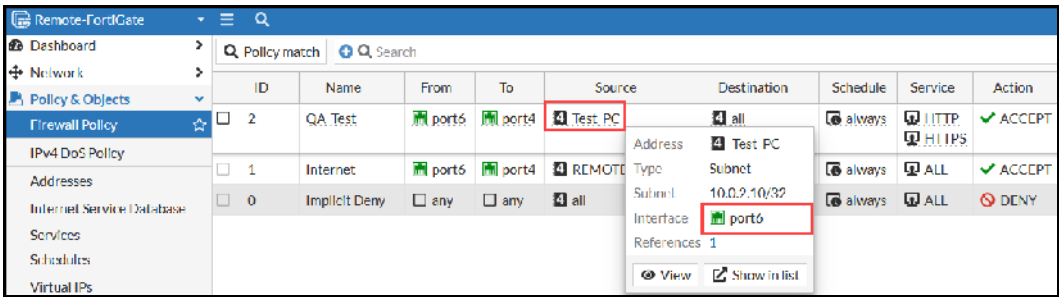


Review Policies and Objects Locally on Remote-FortiGate

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. In the notification window, click to select the new layout.
5. Expand the port6 to port4 policies.
6. 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.

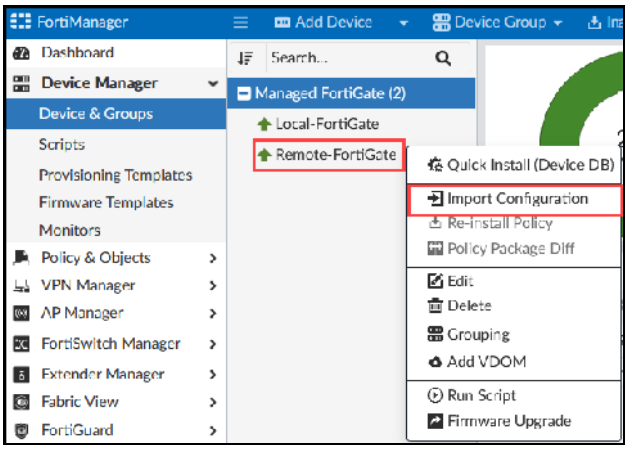
7. Log out of the Remote-FortiGate GUI.

Import a Policy Package

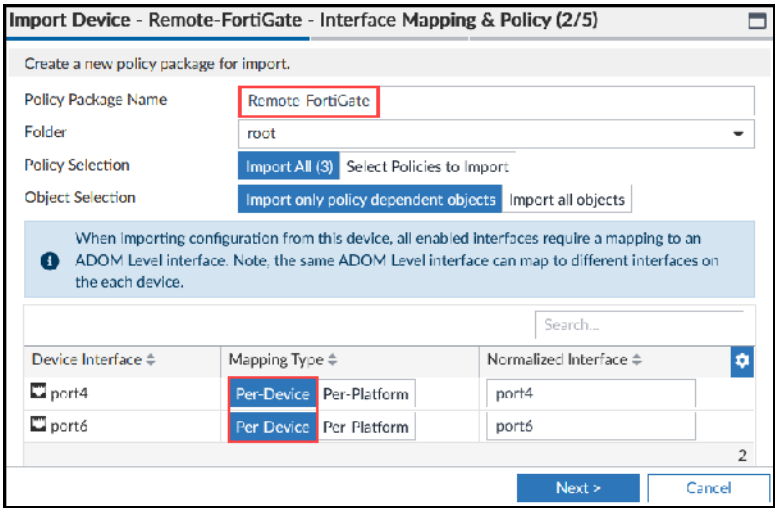
You will import the policies and objects for Remote-FortiGate into the policy package, and then troubleshoot issues with the policy import.

To import the policy package

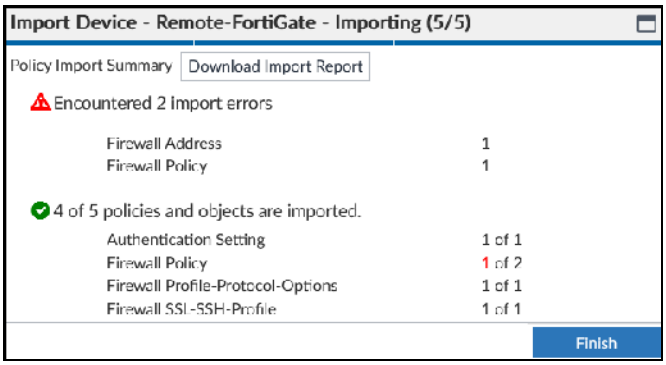
1. Return to the FortiManager GUI, and then click **Device Manager** > **Devices & Groups**.
2. Right-click **Remote-FortiGate**, and then click **Import Configuration**.



3. Select **Import Policy Package**, and then click **Next**.
4. Ensure that the policy package name is **Remote-FortiGate**, and that the **Mapping Type** is set to **Per-Device** for both **port4** and **port6**, as in the following image:



5. Keep the default values for all other settings, and then click **Next**.
6. Click **Next** two more times.
7. Notice that the two errors are related to a firewall policy and firewall address object.



8. Click **Download Import Report** to save the report to a file.
9. Open the file with a text editor to view the reason that the policy import skipped a firewall policy.
   Did you notice that the policy import failed when importing firewall policy `2` and the `Test_PC` address object?

```
Start to import config from device(Remote-FortiGate) vdom(root) to adom(ADOM1), package(Remote-FortiGate)
"authentication setting",SUCCESS,"(name=, oid=3755, new object)"

"firewall address",SKIPPED,"(name=all, oid=2657, DUPLICATE)"
"firewall address",FAIL,"(name=Test_PC, oid=3758, reason=interface((firewall address:Test_PC) any<-port6) binding fail)"
"firewall address",SKIPPED,"(name=REMOTE_SUBNET, oid=3761, DUPLICATE)"

"firewall policy",FAIL,"(name=2, oid=3566, reason=interface(interface binding contradiction. detail: (firewall
address:Test_PC) any<-port6) binding fail)"
"firewall policy",SUCCESS,"(name=1, oid=4031, new object)"

"firewall profile-protocol-options",SUCCESS,"(name=default, oid=3206, update previous object)"

"firewall schedule recurring",SKIPPED,"(name=always, oid=3194, DUPLICATE)"
"firewall service category",SKIPPED,"(name=General, oid=2697, DUPLICATE)"
"firewall service custom",SKIPPED,"(name=ALL, oid=2726, DUPLICATE)"
"firewall ssh local-ca",SKIPPED"(name=Fortinet_SSH_CA, oid=3203, reason=manually)"
"firewall ssh local-ca",SKIPPED"(name=Fortinet_SSH_CA_Untrusted, oid=3204, reason=manually)"

"firewall ssl-ssh-profile",SUCCESS,"(name=no-inspection, oid=3218, update previous object)"
```

Stop and think!

What does this `binding fail` 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, the policy with an ID of 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.

10. Close the import report, and then in the **Import Device** window, click **Finish**.

Check the Impact of a Partial Policy Import (Optional)

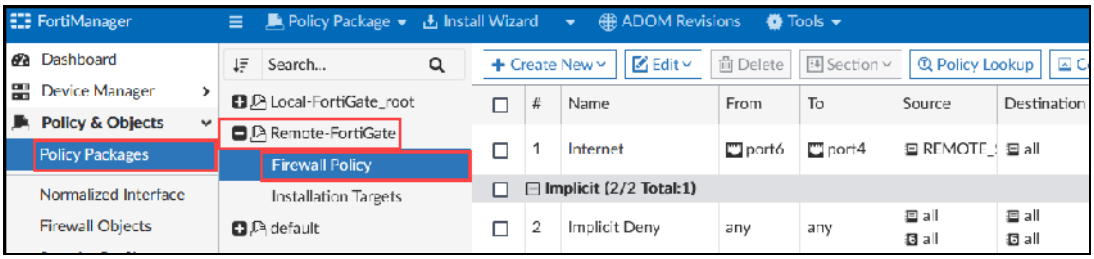
The following two procedures show the impact of making changes to the FortiManager **Remote-FortiGate** policy package, and then trying to install the policy package. FortiManager tries to delete the policy with an ID of 2 and the **Test_PC** address object on Remote-FortiGate. FortiManager also tries to delete any unused objects.

If you are now familiar with the behavior, you can skip the following procedures:

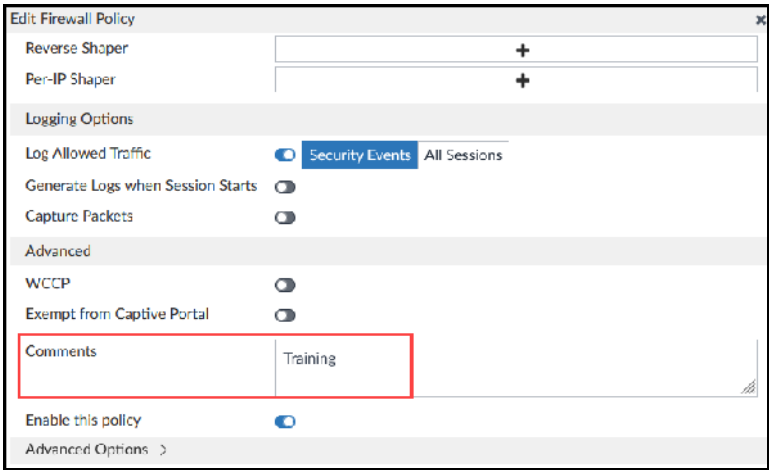
- To make configuration changes to the Remote-FortiGate policy package (optional)
- To preview the installation changes (optional)

To make configuration changes to the Remote-FortiGate policy package (optional)

1. On the FortiManager GUI, click **Policy & Objects** > **Policy Packages**.
2. Click the **Remote-FortiGate** policy package, and then click **Firewall Policy**.
   You can confirm that the firewall policy with **Test_PC** as the source address was not imported.

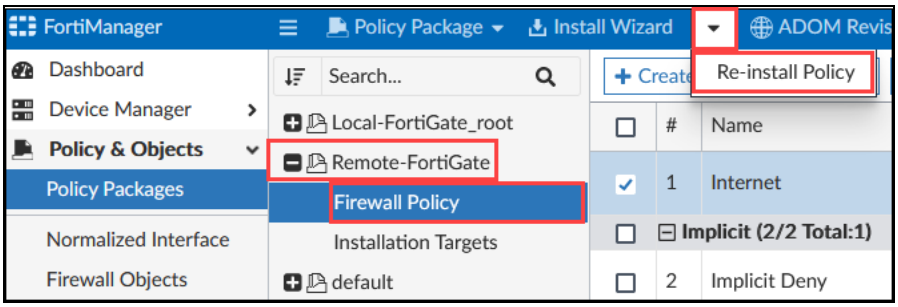


3. Double-click the policy named **Internet** to edit it.
4. In the **Comments** field, type `Training`, and then click **OK**.



To preview the installation changes (optional)

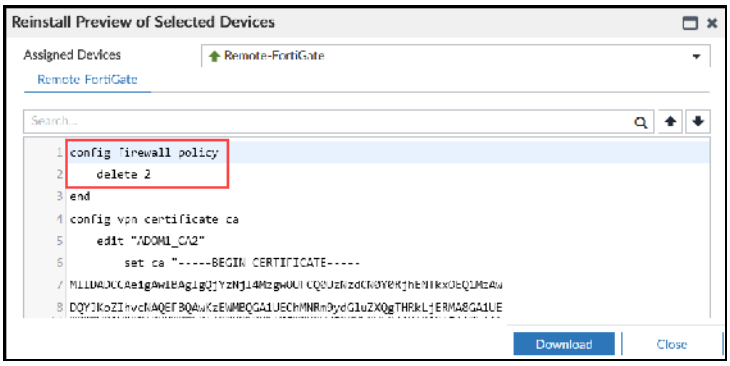
1. Ensure that **Firewall Policy** is selected for the **Remote-FortiGate** policy package, click the down arrow beside **Install Wizard**, and then select **Re-install Policy**.



2. Click **OK**.
3. Click **Install Preview**.
4. Notice that FortiManager is trying to delete the firewall policy with an ID of 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.



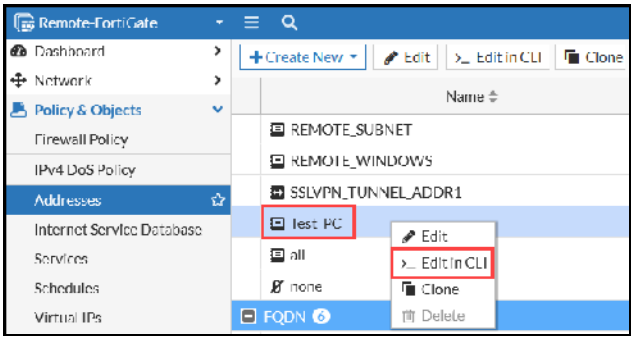
5. In the **Install Preview** window, click **Close**.
6. Click **Cancel** to cancel the policy installation.

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**.



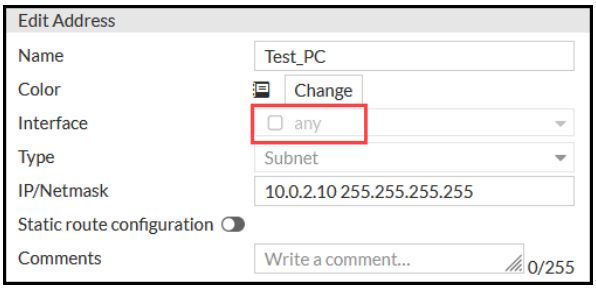
6. On the CLI, enter the following commands:

```
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 image:



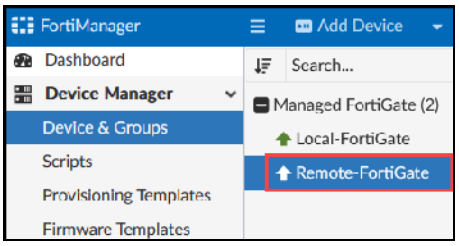
9. Click **Cancel**.
10. Log out of the Remote-FortiGate GUI.

Retrieve the New Configuration From FortiManager

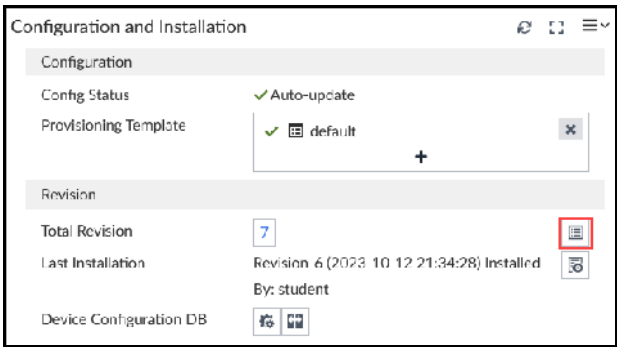
You will retrieve the change made to the Remote-FortiGate configuration on FortiManager.

To retrieve the Remote-FortiGate configuration change on FortiManager

1. Return to the FortiManager GUI, and then click **Device Manager** > **Device & Groups**.
2. Click **Remote-FortiGate**.



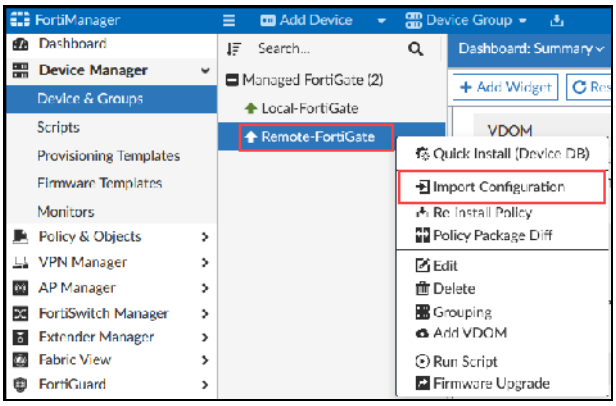
3. In the **Configuration and Installation** widget, click the **Revision History** icon.



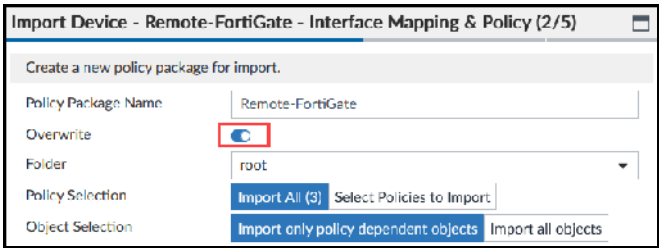
4. Click **Retrieve Config**.
5. Wait for this process to finish, and then click **Close** to close the **Retrieve Device Revision** window.
   Note that FortiManager creates a new configuration revision.
6. Click **Close** to close the **Configuration Revision History** window.

To import the policy package again

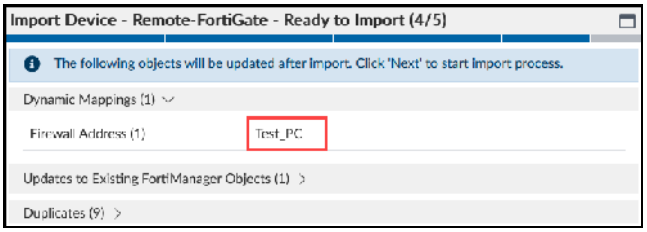
1. On the FortiManager GUI, click **Managed FortiGate**.
2. Right-click **Remote-FortiGate**, and then select **Import Configuration**.



3. Select **Import Policy Package**.
4. Click **Next**.
5. Enable **Overwrite**.



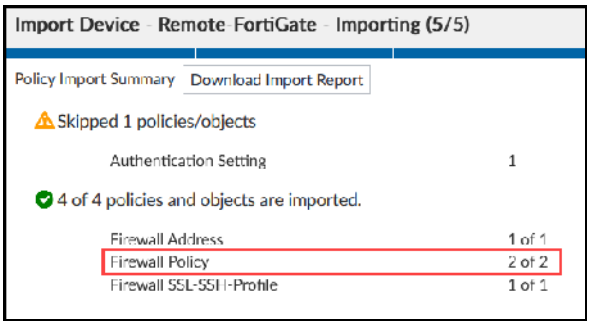
6. Click **Next**.
7. Keep all the default values, and then click **Next**.
8. Notice that **Test_PC** appears in the **Dynamic Mappings** section.



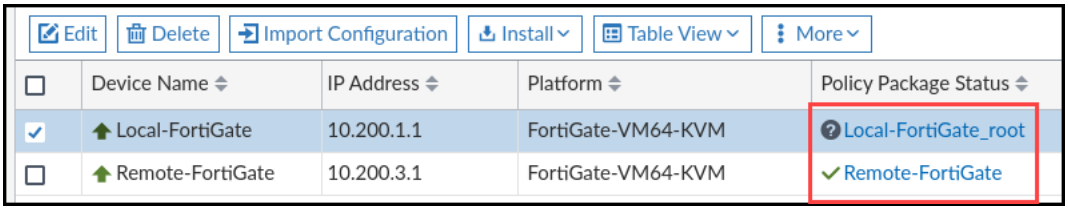
FortiManager automatically creates a dynamic mapping of the object with the same value. The interface must be the same as the ADOM database.

9. Click **Next**.

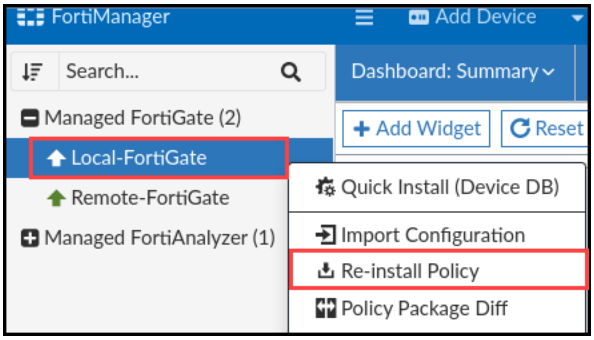
You can see that FortiManager imported both firewall policies this time.



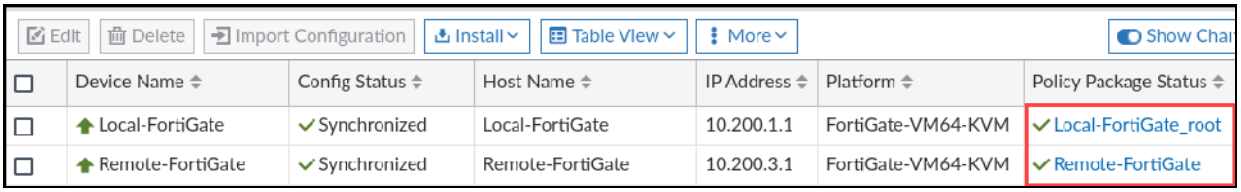
10. Click **Finish**.
11. In the **Policy Package Status** column, confirm that the status for **Remote-FortiGate** shows a green check mark and the status for **Local-FortiGate** shows the unknown icon.



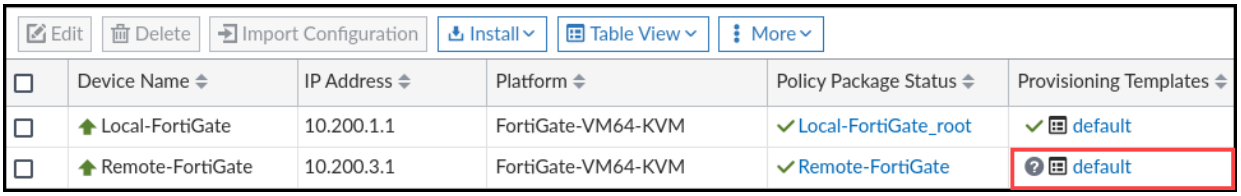
12. Right-click **Local-FortiGate**, and then select **Re-install Policy**.



13. Click **Next**, and then click **Finish**.
14. In the **Policy Package Status** column, confirm that the status for both **Remote-FortiGate** and **Local-FortiGate** now shows a green check mark.

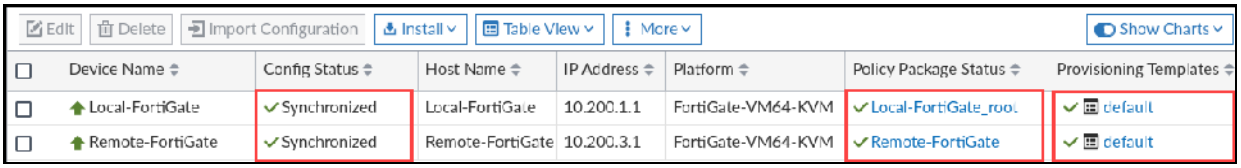


15. Examine the **Provisioning Templates** column to confirm that the value for **Remote-FortiGate** shows the unknown icon.



16. Right-click **Remote-FortiGate**, and then select **Quick Install (Device DB)**.
17. Click **OK**, and then wait for the installation to finish.
18. Click **Finish**.

    At this point, both FortiGate devices should be fully synchronized with FortiManager.



19. Log out of the FortiManager GUI.

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
- Import the firmware image for FortiGate devices and upgrade the devices using FortiManager

Time to Complete

Estimated: 15 minutes

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:

```
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. Enter the following command:

   ```
   diagnose fmupdate view-serverlist fds
   ```

   ```
   FortiManager # diagnose fmupdate view-serverlist fds
   Fortiguard Server Comm : Disabled
   Server Override Mode   : Loose
   ```

   There are two reasons that can make FortiManager unable to connect to the public FortiGuard servers: the network is unreachable or the service is disabled. In this lab environment, communication with the public FortiGuard servers is disabled.

4. Enter the following command:

   ```
   diagnose fmupdate update-status fds
   ```

   ```
   FortiManager # 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
   ```

   You should see that there is no information on `UpullStat` and `UpullServer`, because FortiManager is not connected to the public FortiGuard servers, which would provide that information.

5. Enter the following command:

   ```
   diagnose fmupdate dbcontract
   ```

   Note that the following image shows a partial output only:

```
FortiManager # diagnose fmupdate dbcontract
FAZ-VM0000065040 [SERIAL_NO]
  AccountID: courseware@fortinet.com
  Industry:
  Company:
  Contract:  9
        COMP-1-20-20260119
        ENHN-1-20-20260119
        FMWR-1-06-20260119
        FOAS-1-06-20250826
        FRVS-1-06-20260119
        PBDS-1-06-20260608
        SOAR-1-06-20260119
        SPRT-1-20-20260119
        ZHVO-1-06-20250809
  Contract Raw Data:
        Contract=COMP-1-20-20260119:0:1:1:0*ENHN-1-20-20260119:0:1:1:0*FMWR-1-06-20260119:0:1:1:0*FOAS-1-06
1:1:0*FRVS-1-06-20260119:0:1:1:0*PBDS-1-06-20260608:0:1:1:0*SOAR-1-06-20260119:0:1:1:0*SPRT-1-20-20260119:0
1-06-20250809:0:1:1:0|AccountID=courseware@fortinet.com

FGVM010000064692 [SERIAL_NO]
  AccountID: courseware@fortinet.com
  Industry:  Technology
  Company:   Fortinet
  Contract:  13
        AVDB-1-06-20260119
        AVEN-1-06-20260119
        COMP-1-20-20260119
        ENHN-1-20-20260119
        FGSA-1-06-20260119
        FMWR-1-06-20260119
        FRVS-1-06-20260119
        FURL-1-06-20260119
        HDWR-1-05-20260119
        NIDS-1-06-20260119
        SPAM-1-06-20260119
        SPRT-1-20-20260119
        ZHVO-1-06-20260119
```

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.

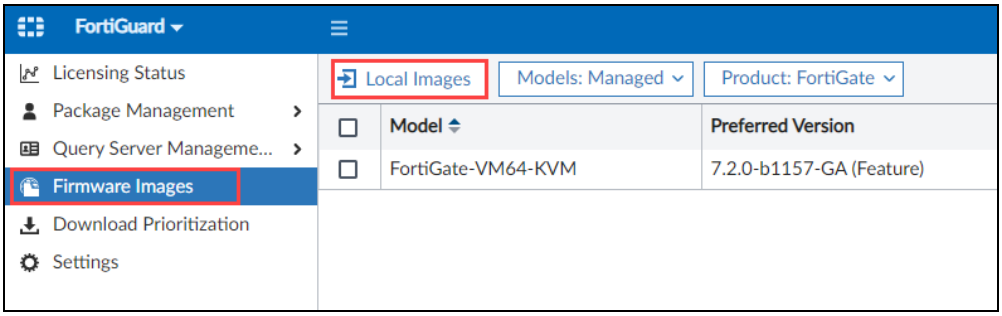
Exercise 2: Upgrading FortiGate Firmware Using FortiManager

You can use FortiManager as your local firmware cache, and to upgrade firmware on supported devices.

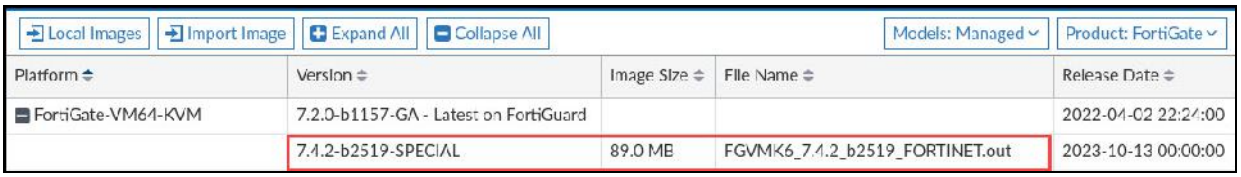
In this exercise, you will import the firmware image for FortiGate, and then upgrade both FortiGate devices using FortiManager.

To import and upgrade firmware

1. On the Local-Client VM, open a new browser window, and then log in to the FortiManager GUI with the username `admin` and password `password`.
2. Click **ADOM1**.
3. Click **FortiGuard** > **Firmware Images** > **Local Images**.



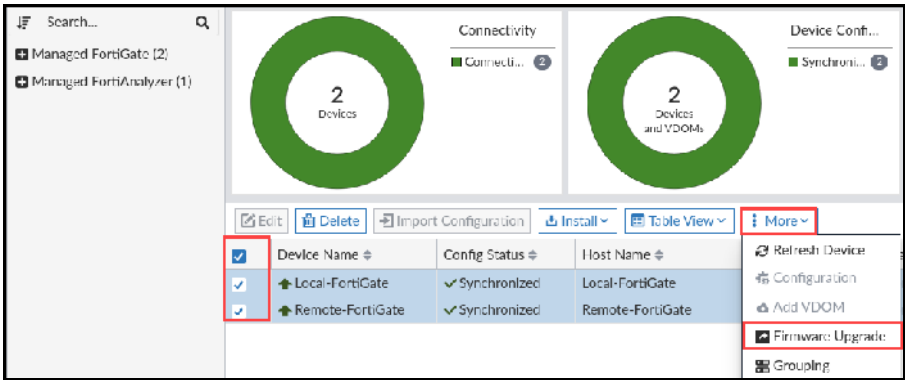
4. Click **Import**, and then click **Add Files**.
5. Click **Desktop** > **Resources** > **FortiManager-Administrator** > **Lab8-Additional-Configuration**, and then select `FGT_upgrade-build2519.out`.
6. Click **Select**, and then click **OK**.
   You can see the file upload progress.
7. Click **Close**.
   You can see that the firmware image has been saved on FortiManager.



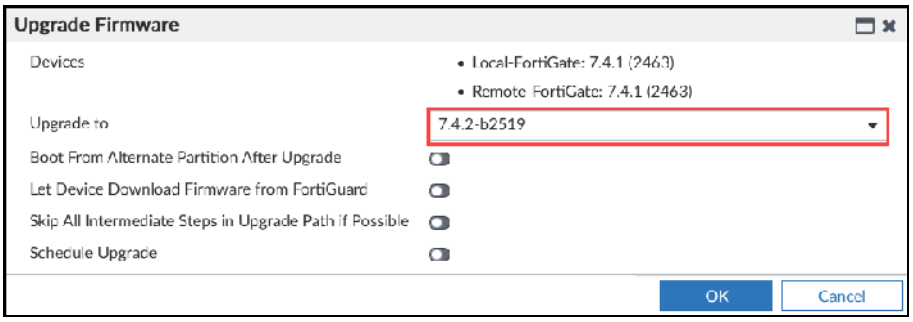
Refresh the page if you don't see the firmware you uploaded listed in the table.

8. Click **Device Manager** > **Device & Groups**.
9. Select the checkboxes for both FortiGate devices.

10. Click **More**, and then select **Firmware Upgrade**.

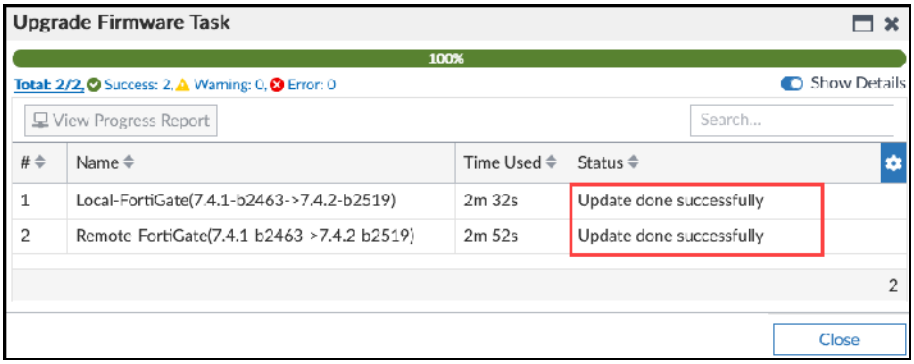


11. In the **Upgrade to** field, scroll down the drop-down list, and then select **Local Images** > **7.4.2-b2519**.



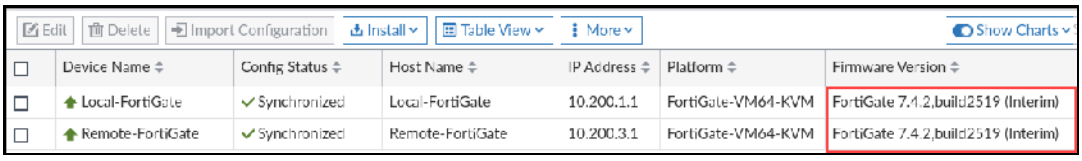
12. Click **OK**.

    The upgrade process begins. After a few minutes, in the **Status** column, you should see the **Update done successfully** status appear for both FortiGate devices.



13. Click **Close**.

    The upgraded firmware is displayed in the **Firmware Version** column.



14. Optionally, you can open the console connection for Local-FortiGate and Remote-FortiGate to confirm the firmware upgrade was successful.
15. Log out of the FortiManager GUI.