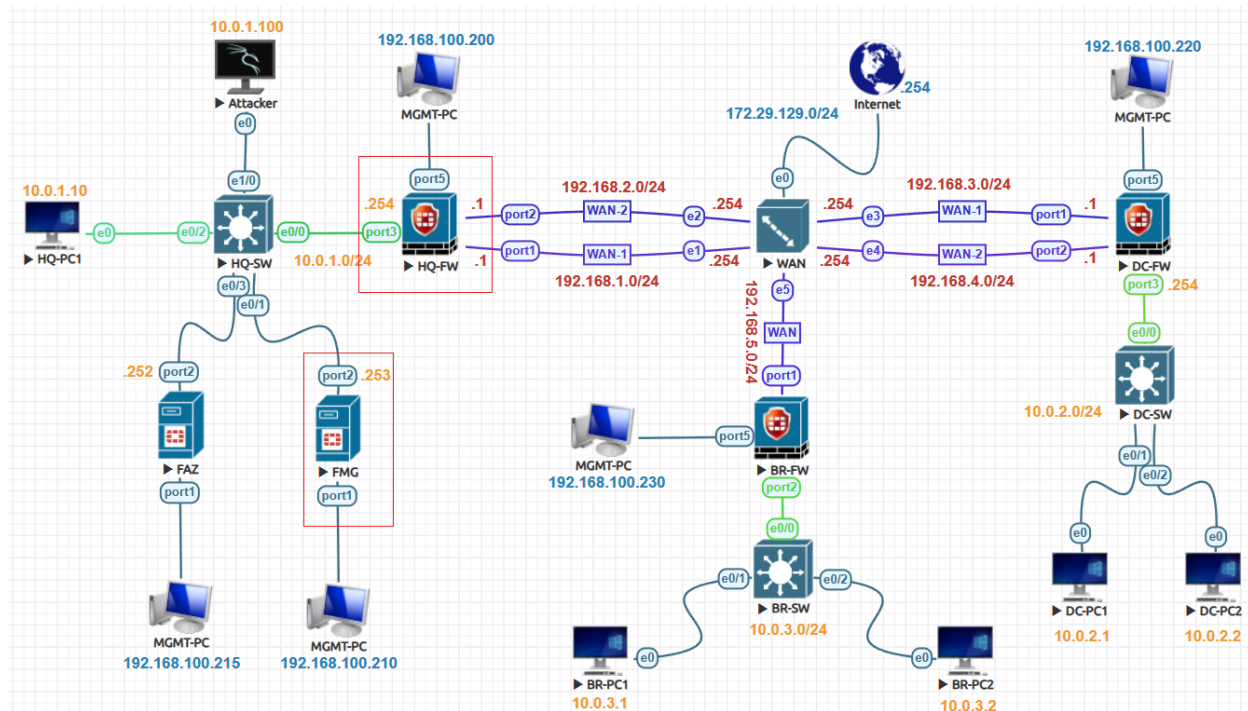


## Add HQ-FW to FortiManager:



## Creating ADOM:

Enable ADOMs, Go to **System Settings>Dashboard**. In the **System Information** widget, go to Administrative Domain, and **toggle On**. It will log you out login back.

← → ↻ ⚠ Not secure | <https://192.168.114.210/p/app/#!/sys/dashboard>

**System Settings**

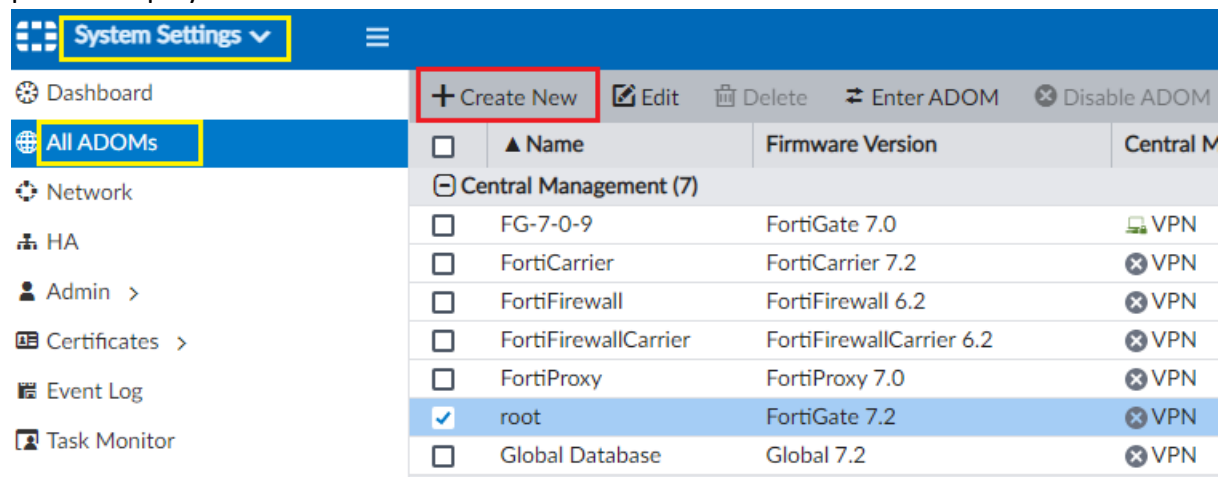
- Dashboard
- All ADOMs
- Network
- HA
- Admin >
- Certificates >
- Event Log
- Task Monitor
- Advanced >

**Toggle Widgets**

- System Information
 

Host Name	FMG
Serial Number	FMG-VMTM22015653
Platform Type	FMG-VM64-KVM
HA Status	Standalone
System Time	Fri Dec 23 21:57:20 2022 PST
Firmware Version	v7.2.0-build1124 220411 (GA)
System Configuration	Last Backup : N/A
Current Administrators	admin / 1 in total
Up Time	1 hour 7 minutes 37 seconds
<b>Administrative Domain</b>	<input checked="" type="checkbox"/>
FortiAnalyzer Features	<input type="checkbox"/>

Go to **System Settings > All ADOMs**. Click **Create New** in the toolbar. The Create New ADOM pane is displayed.



Configure the following settings, then click **OK** to create the ADOM. Type a name that allows you to distinguish this ADOM from your other ADOMs. Select the type FortiGate. Select the version of the devices in the ADOM. Select **Normal** mode. Select the **VPN** checkbox to enable central VPN management. If you want unchecked FortiAP and FortiSwitch.

**Create ADOM**

Name:

Type:  6.4 **7.0** 7.2

Description:

Devices

<input type="checkbox"/>	Name	IP Address	Platform
No record found.			

Mode: ☒ Normal ☐ Backup

Central Management: ☒ **VPN** ☒ FortiAP ☒ FortiSwitch

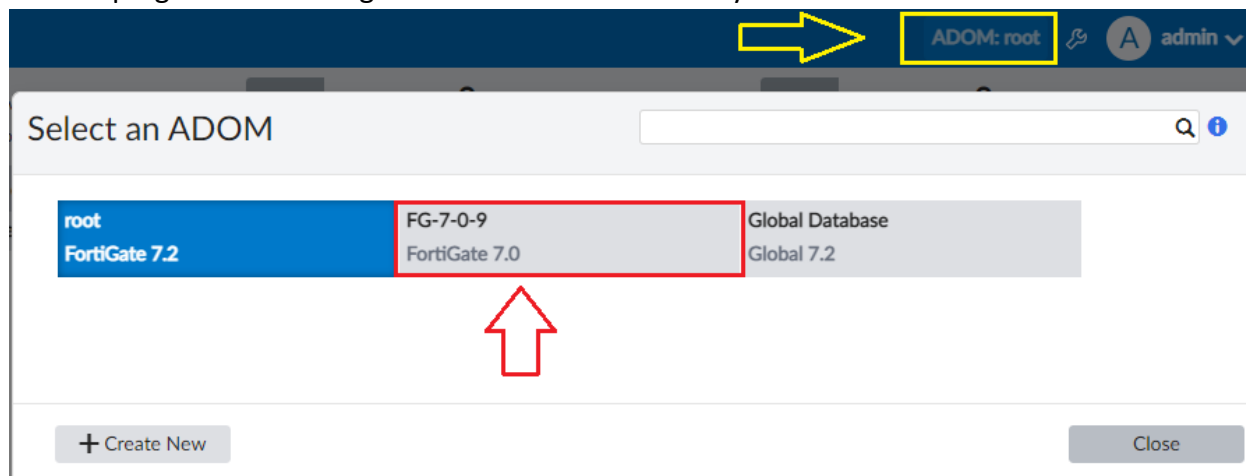
Default Device Selection for Install: ☒ Select All ☐ Deselect All

Perform Policy Check Before Every Install: ☐

Auto-Push Policy Packages When Device Back Online: ☐ Enable ☒ Disable

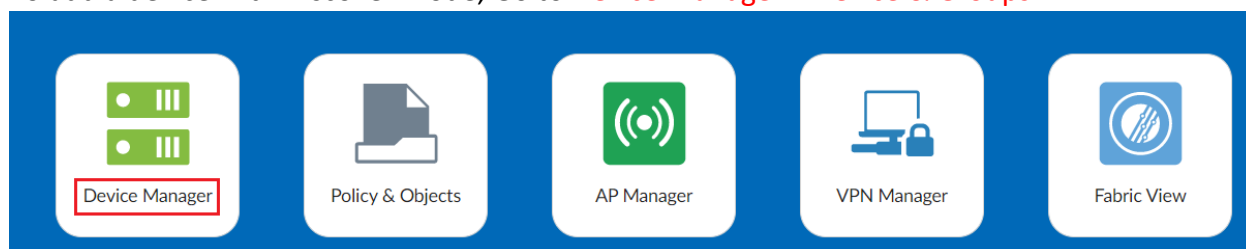
**OK** Cancel

From top right corner change the root ADOM to recently created **ADOM FG-7-0-9**

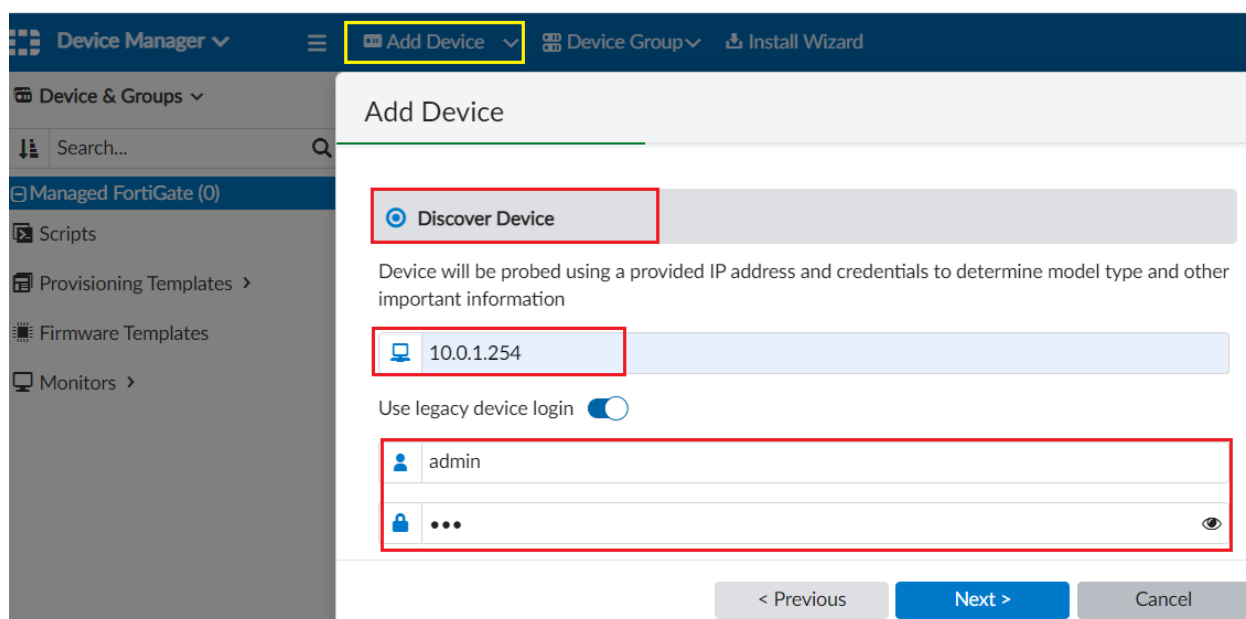


### Add HQ-FW FortiGate:

To add a device with Discover mode, Go to **Device Manager > Device & Groups**.



In the toolbar, click **Add Device**. The Add Device window opens. Select **Discover**, and then follow the prompts to configure the device settings. In the box, type the management port IP address for the device, and also type the **username and password** for the device in the wizard click **Next**.



After the device discovery process completes, the following page of information is displayed. Configure the following settings, and click **Next**.

Add Device	
The following information has been discovered from the device:	
IP Address	10.0.1.254
Host Name	HQ-FW
SN	FGVMEVA8B-NG085A
Model	FortiGate-VM64-KVM
Firmware Version	7.0.9, build444 (GA)
HA Status	Standalone
Administrator	admin

Please input the following information to complete addition of the device:

Name:

Description:

System Template:

☐ Add to Folder:

☐ Add to Device Group:

< Previous **Next >** Cancel

More information about the device is checked. After the wizard completes the checks, you are asked to choose whether to **import policies** and objects for the device now or later. Click **Finish** to finish adding the device and close the wizard.

Add Device	
Name	HQ-FW
IP Address	10.0.1.254
Status	<div><div>35%</div></div>
	✓ Discovering device
	✓ Creating device database
	Initializing configuration database
	Retrieving configuration
	Retrieving support data
	Updating group membership
	Successfully add device
	Check Device Status

Device Manager

Add Device
Device Group
Install Wizard

Device & Groups

Search...

Managed FortiGate (1)

HQ-FW

Scripts

Provisioning Templates

Firmware Templates

Monitors

Add Device

Name	HQ-FW
IP Address	10.0.1.254
Status	<div> <div>✓</div> Device is added successfully </div> <div> <div>✓</div> Discovering device </div> <div> <div>✓</div> Creating device database </div> <div> <div>✓</div> Initializing configuration database </div> <div> <div>✓</div> Retrieving configuration </div> <div> <div>✓</div> Retrieving support data </div> <div> <div>✓</div> Updating group membership </div> <div> <div>✓</div> Successfully add device </div> <div> <div>✓</div> Check Device Status </div>

To manage policies and objects of this device, you need to import them into FortiManager database.

Import Now

Import Later

### Synch Device:

This wizard allows you to import interface maps, policy databases, and objects. Select Import Policy Package, and click **Next**.

#### Import Device - HQ-FW

☒ Import Policy Package  
Import policy package used by the selected device.

☐ Import AP Profiles or FortiSwitch Templates  
Automatically import FortiAP profile and FortiSwitch template from selected device. For objects have the same name, configuration from device database will be used.

Next >

Cancel




Specify what policies and objects to import. Specify mapping types for enabled FortiGate interfaces. When finished mapping device interfaces, click **Next**.

### Import Device - HQ-FW [ root ]

Create a new policy package for import.

Policy Package Name	<input type="text" value="HQ-FW_root"/>
Folder	<input type="text" value="root"/>
Policy Selection	<input checked="" type="radio"/> Import All (2) <input type="radio"/> Select Policies to Import
Object Selection	<input type="radio"/> Import only policy dependent objects <input checked="" type="radio"/> Import all objects

When importing configuration from this device, all enabled interfaces require a mapping to an ADOM Level interface. Note, the same ADOM Level interface can map to different interfaces on the each device.

Device Interface	Mapping Type		Normalized Interface
 port1	<input checked="" type="radio"/> Per-Device	<input type="radio"/> Per-Platform	<input type="text" value="WAN1-Port"/>
 port2	<input checked="" type="radio"/> Per-Device	<input type="radio"/> Per-Platform	<input type="text" value="WAN2-Port"/>
 port3	<input checked="" type="radio"/> Per-Device	<input type="radio"/> Per-Platform	<input type="text" value="LAN-Port"/>

☒ Add mappings for all unused device interfaces

Next >

Cancel

The next page displays any object conflicts between the device and FortiManager. If object conflicts are detected, choose whether to use the value from FortiGate or FortiManager, and click **Next**. You can click Download Conflict File to save a file of the conflicts to your hard drive.

### Import Device - HQ-FW [ root ]

The following objects were found having conflicts. Please confirm your settings, then continue.

Conflicts (2)

Category	Name	Use Value From	
		<input type="radio"/> FortiGate	<input checked="" type="radio"/> FortiManager
Firewall Profile-Protocol-Options (1)	default	<input type="radio"/> FortiGate	<input checked="" type="radio"/> FortiManager <a href="#">View Conflict</a>
Firewall SSL-SSH-Profile (1)	no-inspection	<input type="radio"/> FortiGate	<input checked="" type="radio"/> FortiManager <a href="#">View Conflict</a>

[\[Download Conflict File\]](#)

Next >

Cancel

Click **Next** to start the import process. When the import process completes, a summary page is displayed.

## Import Device - HQ-FW [ root ]

The following objects will be updated after import. Click 'Next' to start import process.

### New Objects to Import (2)

Firewall SSH Local-Ca (2)	Fortinet_SSH_CA, Fortinet_SSH_CA_...
---------------------------	--------------------------------------

### Duplicates (7)

Firewall Address (1)	all
Firewall Profile-Protocol-Options (1)	default
Firewall SSL-SSH-Profile (1)	no-inspection
Firewall Schedule Recurring (2)	always, default-darrp-optimize
Firewall Service Category (1)	General
Firewall Service Custom (1)	ALL



Next >

Cancel

Click **Finish** to close the wizard.

## Import Device - HQ-FW [ root ]

Policy Import Summary [\[Download Import Report\]](#)

✔ 5 of 5 policies and objects are imported.

Authentication Setting	1 of 1
Firewall Policy	2 of 2
Firewall SSH Local-Ca	2 of 2



Finish

Finally, the device is added successfully

← → ↺ ⚠ Not secure | <https://192.168.114.210/p/app/#/!/adom/dvm/main/groups/-3>

Device Manager

Device & Groups

Search...

Managed FortiGate (1)

HQ-FW

Scripts

Provisioning Templates

Firmware Templates

1 Devices  
Total

0 Devices  
Connection Down

Edit Delete Import Configuration Install Table View More Column Settings

Device Name	Config Status	Host Name	IP Address	Platform	Description
✔ HQ-FW	✔ Synchronized	HQ-FW	10.0.1.254	FortiGate-VM64-KVM	