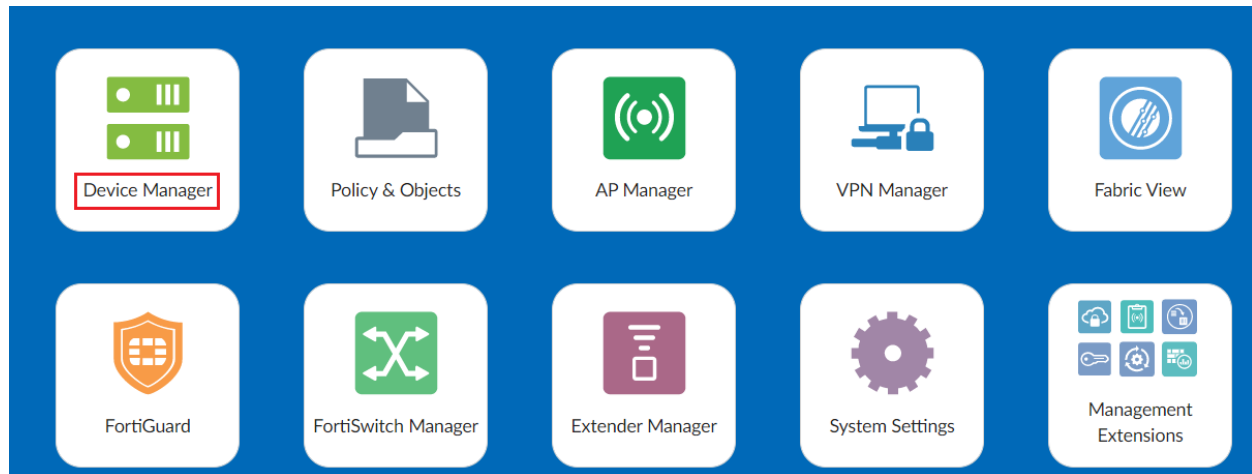
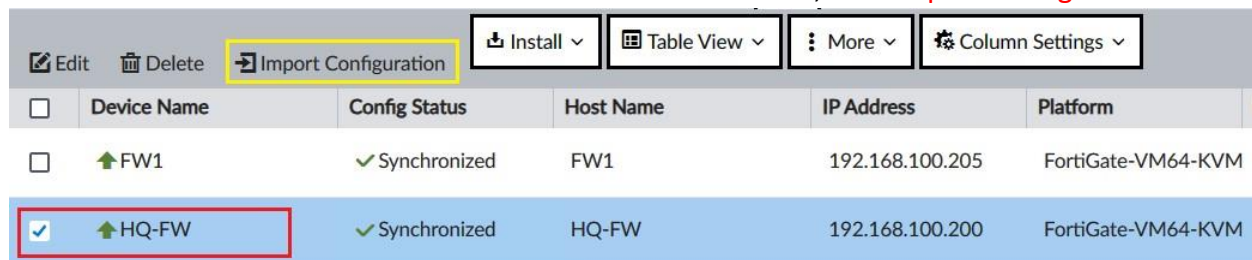


## Import Configuration:

Navigate to **Device Manager > Device & Groups>Managed FortiGates**.



Select the Firewall in this case **HQ-FW** after that in the toolbar, click **Import Configuration**.



This wizard allows you to import interface maps, policy databases, and objects. Specify what policies and objects to import. Specify mapping types for enabled FortiGate interfaces. When finished mapping device interfaces, click **Next**.

Policy Package Name: Keep Default

Folder: Keep Default

Policy Selection: **Import All**

Object Selection: **Import all objects**

Mapping Type: **Per-Device**

## Import Device - HQ-FW [ root ]

Create a new policy package for import.

Policy Package Name	<input type="text" value="HQ-FW"/>
Folder	<input type="text" value="root"/>
Policy Selection	<input checked="" type="radio"/> Import All (3) <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 Per-Platform	<input type="text" value="port1"/>
port2	<input checked="" type="radio"/> Per-Device Per-Platform	<input type="text" value="port2"/>
port3	<input checked="" type="radio"/> Per-Device Per-Platform	<input type="text" value="port3"/>

☒ 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.

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

Conflicts (33)

Category	Name	Use Value From
		<input type="radio"/> FortiGate <input checked="" type="radio"/> FortiManager
Firewall Service Custom (24)	AOL	<input type="radio"/> FortiGate <input checked="" type="radio"/> FortiManager <a href="#">View Conflict</a>
	CVSPSERVER	<input type="radio"/> FortiGate <input checked="" type="radio"/> FortiManager <a href="#">View Conflict</a>
	FINGER	<input type="radio"/> FortiGate <input checked="" type="radio"/> FortiManager <a href="#">View Conflict</a>
	GOPHER	<input type="radio"/> FortiGate <input checked="" type="radio"/> FortiManager <a href="#">View Conflict</a>
	INFO_ADDRESS	<input type="radio"/> FortiGate <input checked="" type="radio"/> FortiManager <a href="#">View Conflict</a>
	INFO_REQUEST	<input type="radio"/> FortiGate <input checked="" type="radio"/> FortiManager <a href="#">View Conflict</a>
	Internet-Locator-Service	<input type="radio"/> FortiGate <input checked="" type="radio"/> FortiManager <a href="#">View Conflict</a>
	MMS	<input type="radio"/> FortiGate <input checked="" type="radio"/> FortiManager <a href="#">View Conflict</a>
	NNTP	<input type="radio"/> FortiGate <input checked="" type="radio"/> FortiManager <a href="#">View Conflict</a>
	NONE	<input type="radio"/> FortiGate <input checked="" type="radio"/> FortiManager <a href="#">View Conflict</a>
	NetMeeting	<input type="radio"/> FortiGate <input checked="" type="radio"/> FortiManager <a href="#">View Conflict</a>
	PING6	<input type="radio"/> FortiGate <input checked="" type="radio"/> FortiManager <a href="#">View Conflict</a>
	QUAKE	<input type="radio"/> FortiGate <input checked="" type="radio"/> FortiManager <a href="#">View Conflict</a>



Next >

Cancel

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

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

Duplicates (271) <span>▼</span>		
Antivirus Profile (3)	default, sniffer-profile, wifi-default	
Application List (1)	sniffer-profile	
DLP Filepattern (2)	builtin-patterns, all_executables	
DLP Sensitivity (3)	Private, Critical, Warning	
DLP Sensor (2)	default, sniffer-profile	
DNSfilter Profile (1)	default	
Emailfilter Profile (2)	sniffer-profile, default	
File-Filter Profile (2)	default, sniffer-profile	
Firewall Address (12)	none, login.microsoftonline.com, logi...	
Firewall Address6 (3)	SSLVPN_TUNNEL_IPv6_ADDR1, all, ...	
Firewall Addrgrp (2)	G Suite, Microsoft Office 365	
Firewall Multicast-Address (6)	all, all_hosts, all_routers, Bonjour, EIG...	
Firewall Multicast-Address6 (1)	all	
Firewall Profile-Protocol-Options (1)	default	
Firewall SSL-SSH-Profile (4)	certificate-inspection, custom-deep-i...	
Firewall Schedule Recurring (3)	always, none, default-darrp-optimize	
Firewall Service Category (10)	General Web Access File Access F	

Next >
Cancel

Click **Finish** to close the wizard.

## Import Device - HQ-FW [ root ]

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

✓ 3 of 3 policies and objects are imported.

Authentication Setting	1 of 1
Firewall Policy	2 of 2

Finish

Finally, verify that the **Policy Package Status**.

<span>Edit</span> <span>Delete</span> <span>Import Configuration</span> <span>Install ▼</span> <span>Table View ▼</span> <span>More ▼</span> <span>Column Settings</span>					
<input type="checkbox"/>	Device Name	Config Status	Host Name	IP Address	▲ Policy Package Status
<input type="checkbox"/>	FW1	✓ Synchronized	FW1	192.168.100.205	✓ FW1
<input checked="" type="checkbox"/>	HQ-FW	✓ Synchronized	HQ-FW	192.168.100.200	✓ HQ-FW

Navigate to **Policy & Objects >Policy Packages** choose the firewall in this case **HQ-FW>Firewall Policy** to verify the policies are there.

#	Name	From	To
1	LAN-to-WAN1	port3	port1
2	LAN-to-WAN2	port3	port2
▼ Implicit (3-3 / Total: 1)			
3	Implicit Deny	any	any

Repeat the same steps for FW1 to import the configuration.

#	Name	From	To	Source
1	LAN-to-WAN	port2	port1	all
▼ Implicit (2-2 / Total: 1)				
2	Implicit Deny	any	any	all

Finally, verify that the **Policy Package Status**.

Device Name	Config Status	Host Name	IP Address	Policy Package Status
FW1	✓ Synchronized	FW1	192.168.100.205	✓ FW1
HQ-FW	✓ Synchronized	HQ-FW	192.168.100.200	✓ HQ-FW