FortiManager - New Features Guide

Version 6.2.0

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

September 11, 2020
FortiManager 6.2.0 New Features Guide
02-620-528939-20200911

TABLE OF CONTENTS

Change Log

Date	Change Description
2019-04-11	Initial release.
2019-04-16	Updated FortiClient EMS Connector on page 29.
2019-05-08	Added Fabric ADOM management on page 13.
2019-05-24	Added License for FortiGates with FortiManager Cloud Entitlement on page 143.
2019-05-30	Added Zero-touch provisioning for FortiSwitch on page 83 and Zero-touch provisioning for FortiAP on page 78.
2019-07-04	Updated the URL for FNDN in Swagger support for FNDN API Tool on page 142.
2020-09-11	Updated Zero Touch Provisioning - CLI Template with Variables on page 68.

Expanding Fabric

This section lists the new features added to FortiManager for the expanding fabric.

List of new features:

- Security Fabric Topology on page 7
- Fabric ADOM management on page 13
- Dynamic Mapping for SSID on page 16
- Split Task VDOM Mode Support on page 18

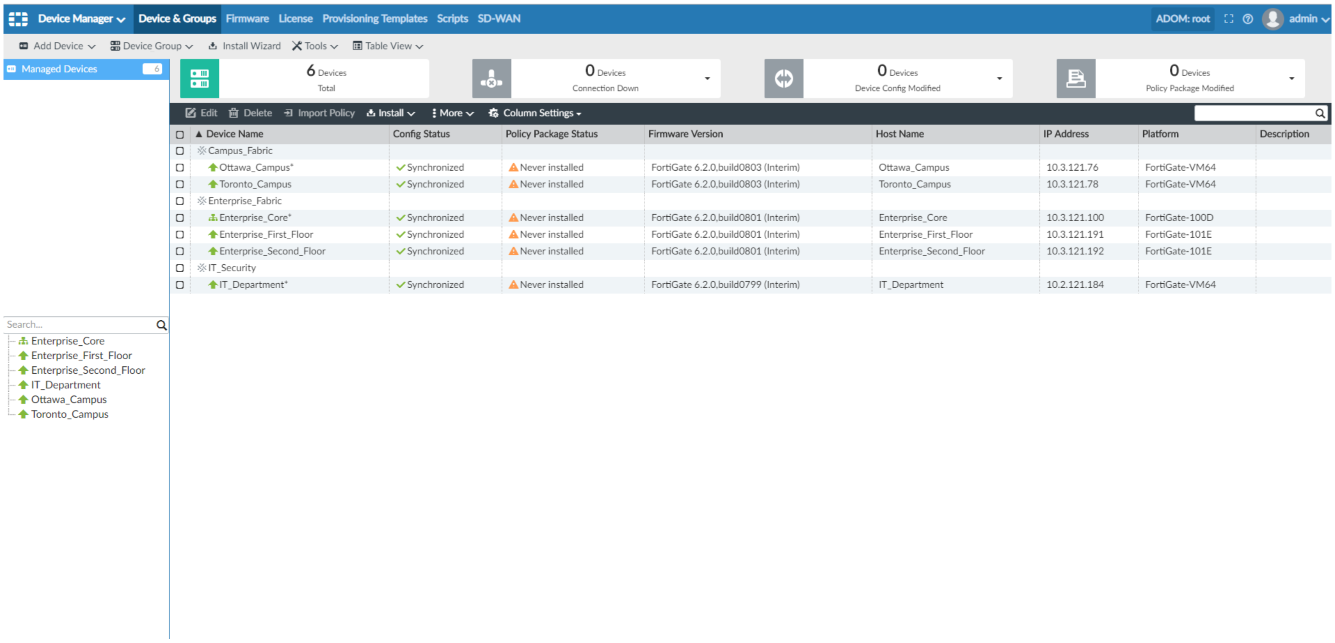
Security Fabric Topology

Both the Physical Topology and Logical Topology from Security Fabric deployments can now be accessed from FortiManager. In the event FortiManager is managing multiple Fabric deployments in the same ADOM, the administrator can switch between them from a single console. The FortiManager uses shared components with FortiGate, thereby supporting a consistent look and feel, level of detail, and usability exactly like FortiGate devices.

See Security Fabric Topology.

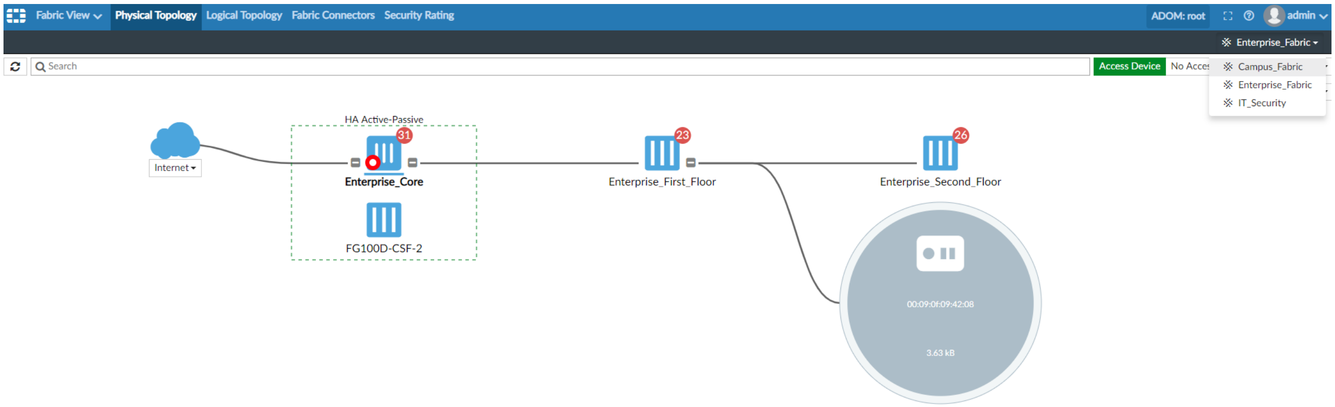
Security Fabric Deployments

Manage multiple Security Fabric deployments in an ADOM using FortiManager.



□	▲ Device Name	Config Status	Policy Package Status	Firmware Version	Host Name	IP Address	Platform	Description
□	Campus_Fabric							
□	Ottawa_Campus*	✓ Synchronized	⚠ Never installed	FortiGate 6.2.0,build0803 (Interim)	Ottawa_Campus	10.3.121.76	FortiGate-VM64	
□	Toronto_Campus	✓ Synchronized	⚠ Never installed	FortiGate 6.2.0,build0803 (Interim)	Toronto_Campus	10.3.121.78	FortiGate-VM64	
□	Enterprise_Fabric							
□	Enterprise_Core*	✓ Synchronized	⚠ Never installed	FortiGate 6.2.0,build0801 (Interim)	Enterprise_Core	10.3.121.100	FortiGate-100D	
□	Enterprise_First_Floor	✓ Synchronized	⚠ Never installed	FortiGate 6.2.0,build0801 (Interim)	Enterprise_First_Floor	10.3.121.191	FortiGate-101E	
□	Enterprise_Second_Floor	✓ Synchronized	⚠ Never installed	FortiGate 6.2.0,build0801 (Interim)	Enterprise_Second_Floor	10.3.121.192	FortiGate-101E	
□	IT_Security							
□	IT_Department*	✓ Synchronized	⚠ Never installed	FortiGate 6.2.0,build0799 (Interim)	IT_Department	10.2.121.184	FortiGate-VM64	

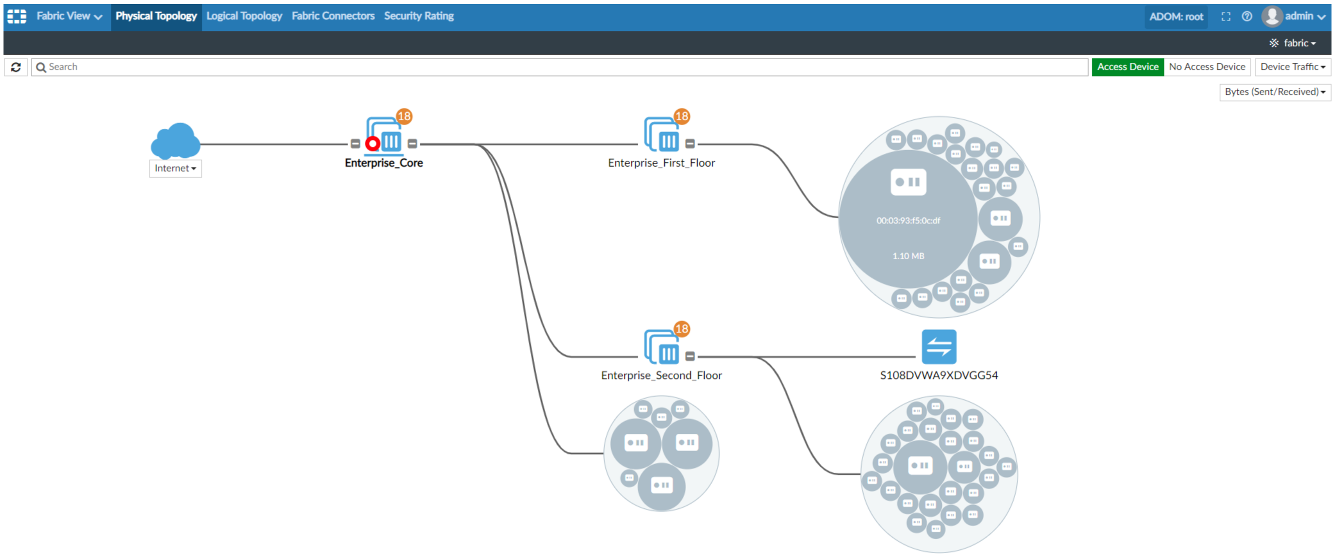
On FortiManager, go to *Fabric View*. *Physical Topology* tab and *Logical Topology* tab are shown at top menu bar. To switch between fabric deployments, go to top right hand corner fabric list and select a fabric deployment.



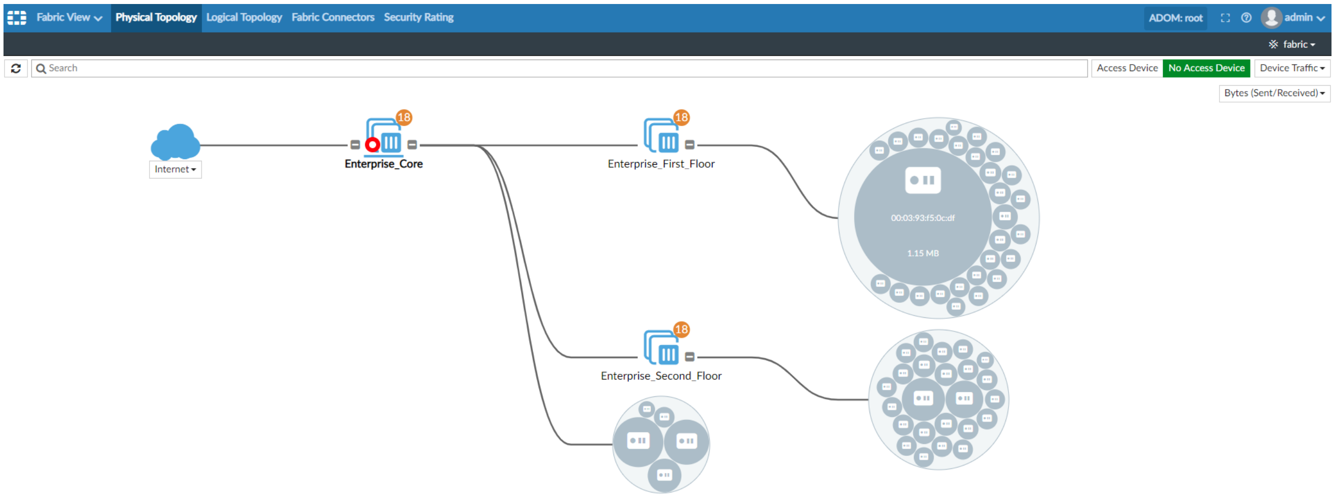
Physical Topology

The Physical Topology shows the devices in the Security Fabric and the devices they are connected to. You can also select whether or not to view access devices in this topology.

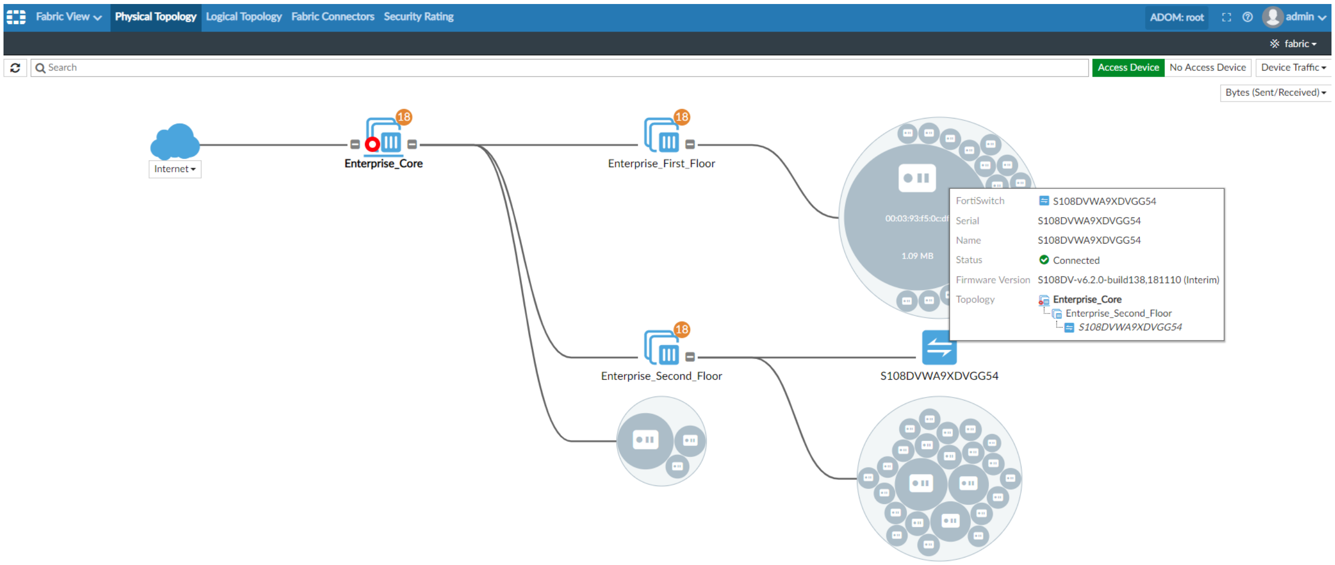
- Access Device View: In below example, the access device FortiSwitch "S108DVWA9XDVGG54" is shown.



- No Access Device View: In below example, the access device FortiSwitch "S108DVWA9XDVGG54" is not shown.

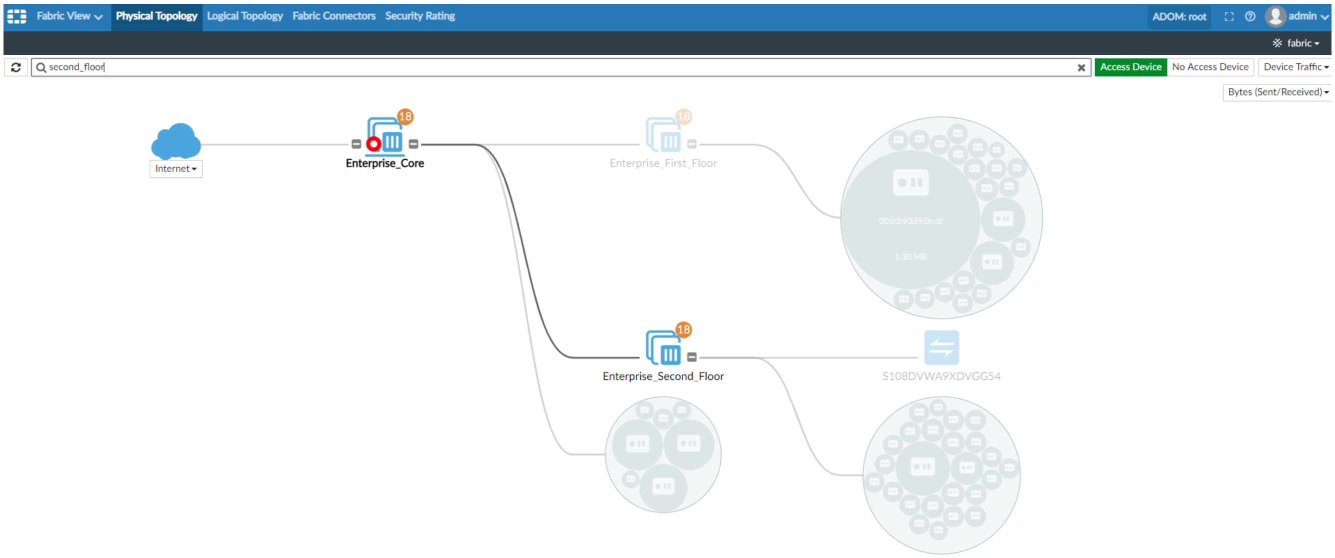


- More information: Hover over a device for more information.



FortiSwitch S108DVWA9XDVGG54
Serial S108DVWA9XDVGG54
Name S108DVWA9XDVGG54
Status ✓ Connected
Firmware Version S108DV-v6.2.0-build138,181110 (Interim)
Topology **Enterprise_Core**
Enterprise_Second_Floor
S108DVWA9XDVGG54

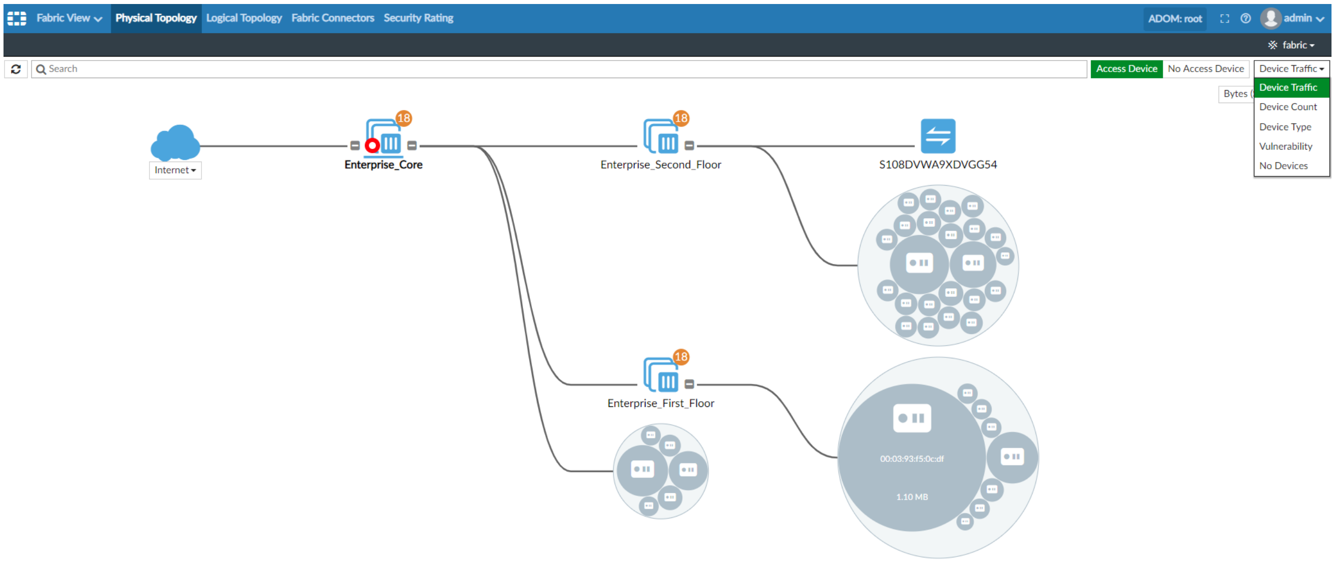
- Search: The search field is located above the view. The search highlights devices that match your search criteria, and grays out devices that don't match.



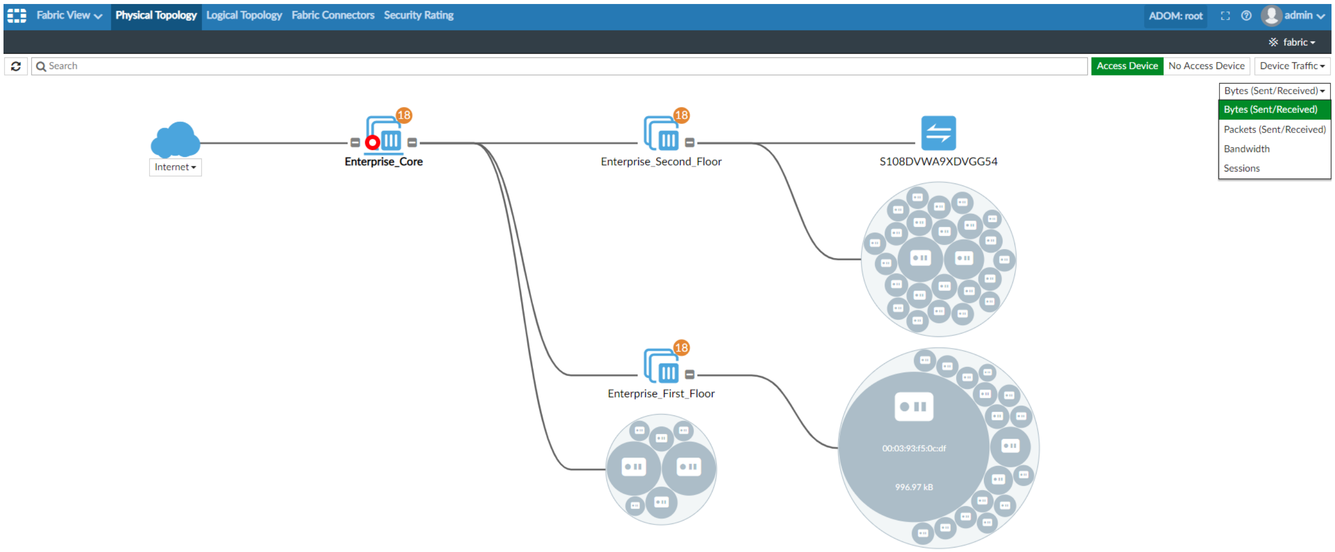
Filter Topology View

Use filters to narrow down the data on the topology views to find specific information. The filter menu is located at top right corner.

- Filter: Filter by Device Traffic, Device Count, Device Type, Vulnerability, or No Devices.



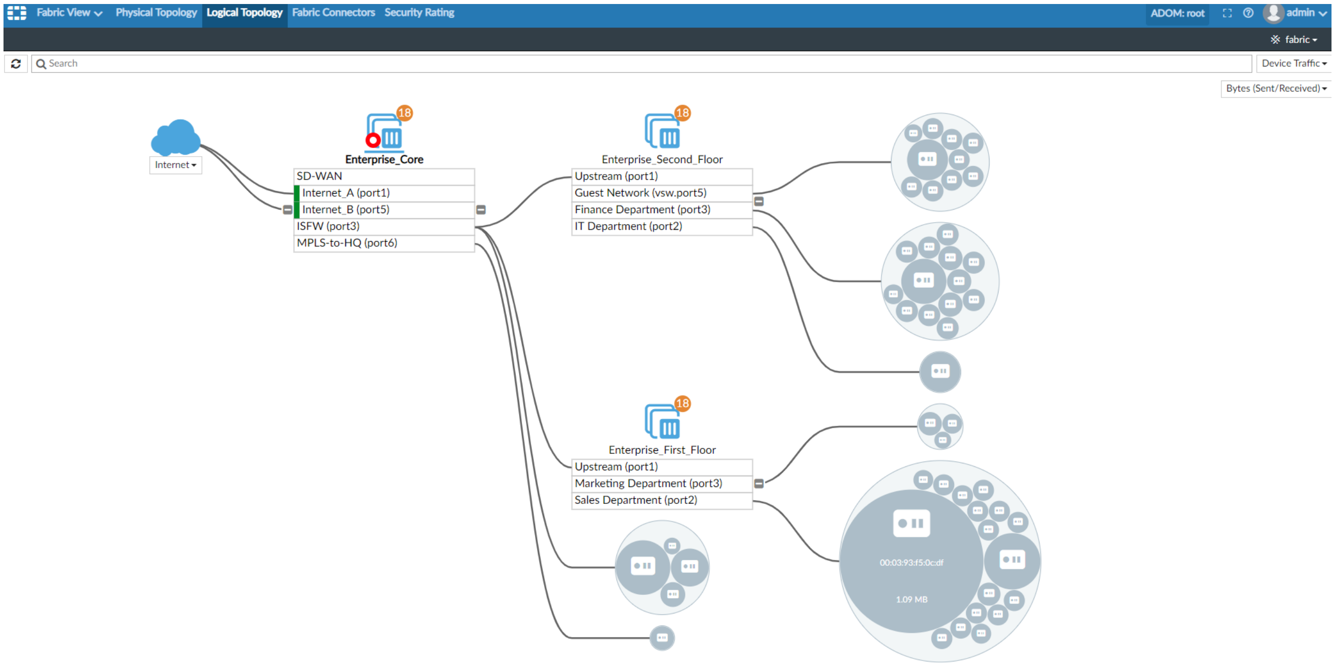
- Sub-filter: When the filter is set to Device Traffic or Device Count, there is a sub-filter that provides Bytes, Packets, Bandwidth, and Sessions options.



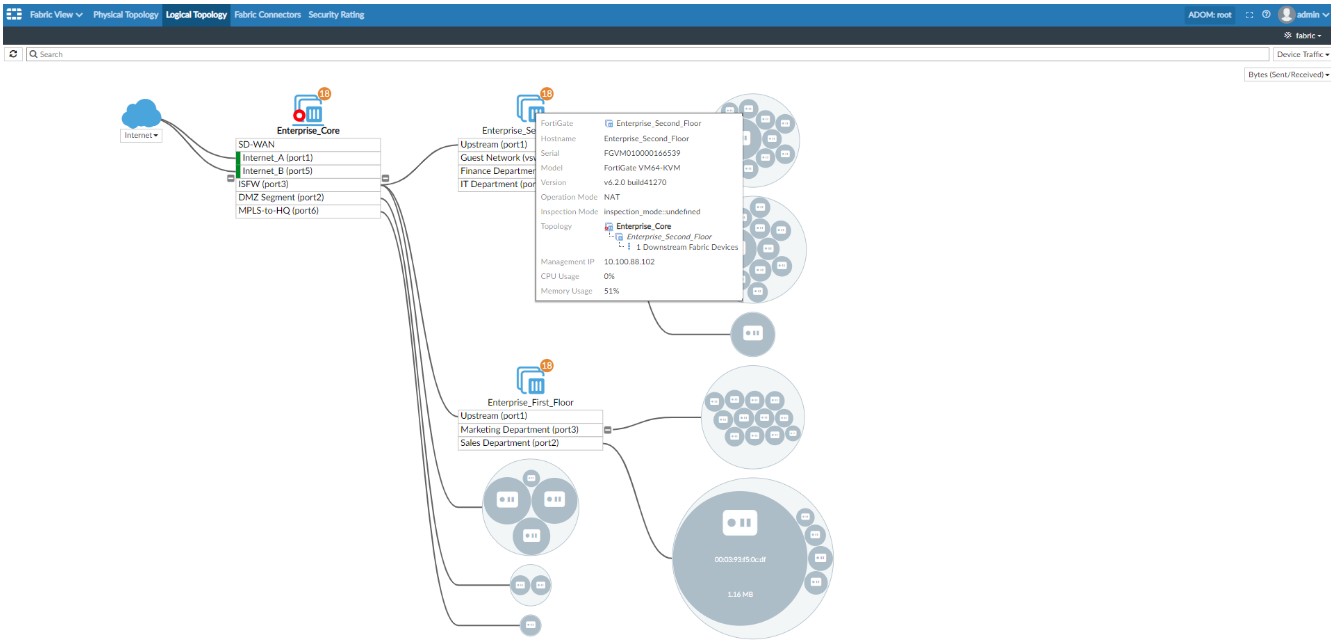
Logical Topology

The Logical Topology view is similar to the Physical Topology view, but it shows the network interfaces, logical or physical, that are used to connect devices in the Security Fabric. Logical Topology provides the same search function, tooltips for device information and the filter view as Physical Toplogy. Logical Topology does not have Access Device view and No Access Device view, which is different from Physical Topology.

To see the Logical Topology, go to *Fabric View > Logical Topology*.

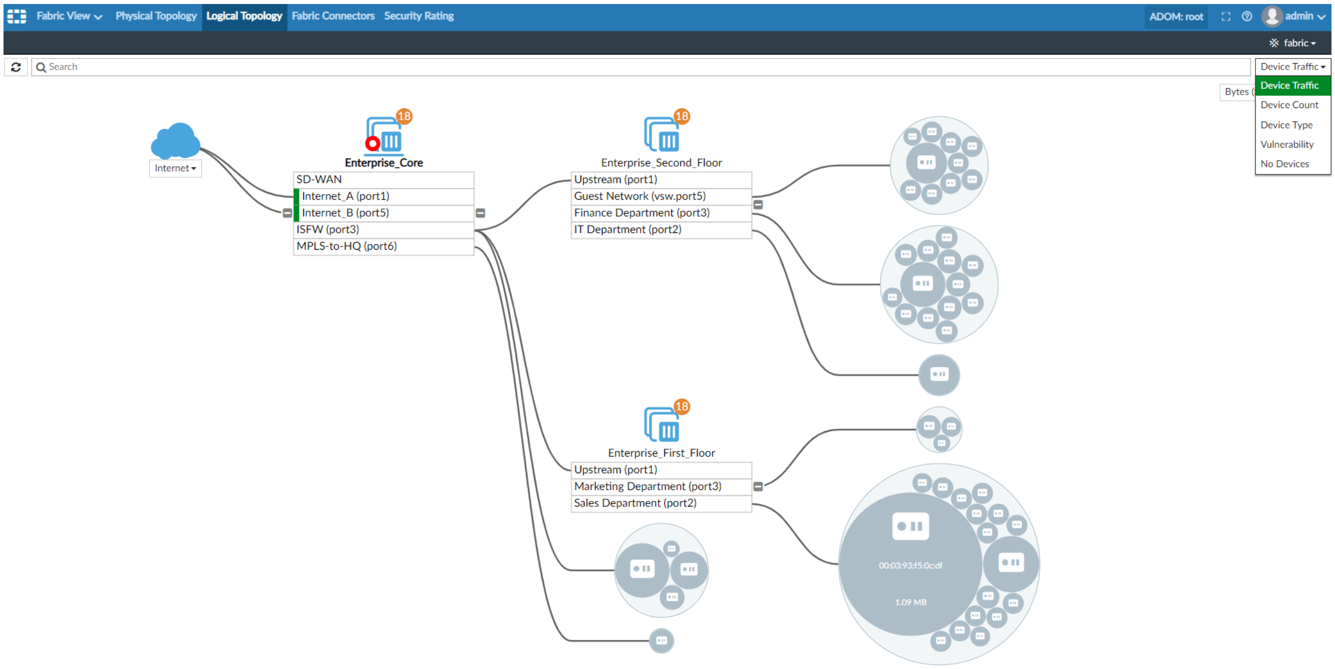


- Device Information: Hover over a icon to see information for a device.

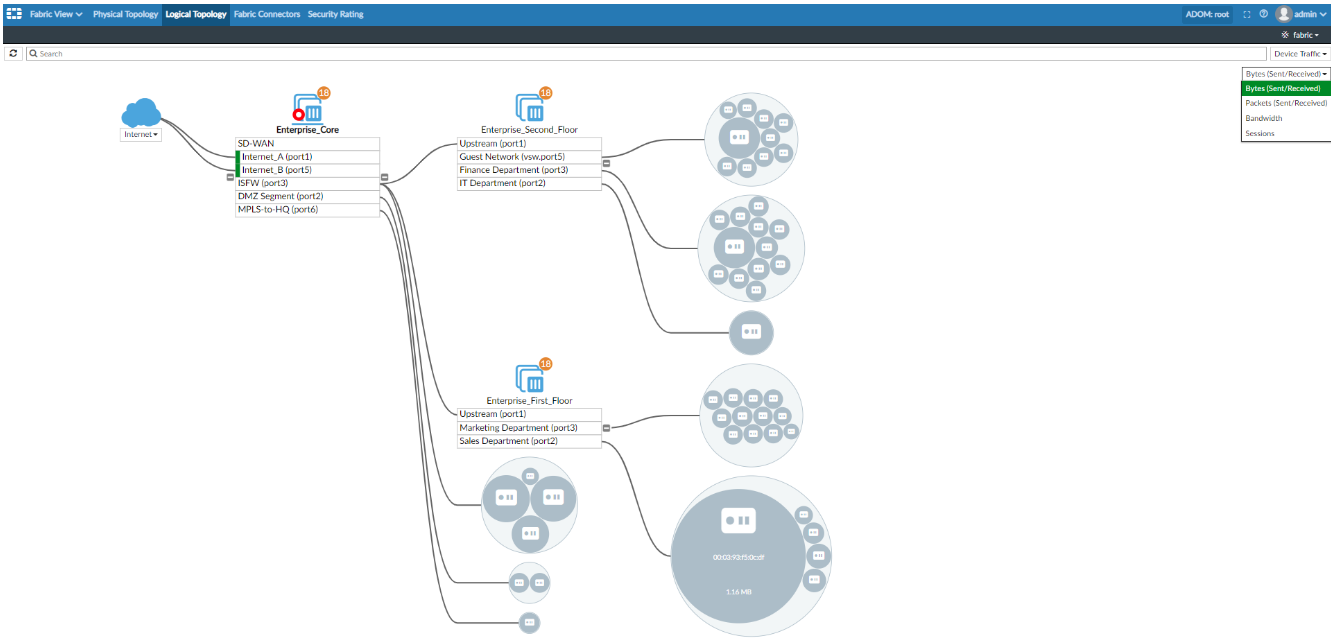


FortiGate	Enterprise_Second_Floor
Hostname	Enterprise_Second_Floor
Serial	FGVM010000166539
Model	FortiGate VM64-KVM
Version	v6.2.0 build41270
Operation Mode	NAT
Inspection Mode	inspection_mode::undefined
Topology	Enterprise_Core *Enterprise_Second_Floor* 1 Downstream Fabric Devices
Management IP	10.100.88.102
CPU Usage	0%
Memory Usage	51%

- Filter: Logical Topology view can be filtered by Device Traffic, Device Count, Device Type, Vulnerability or No Devices.



- Sub-filter: When the filter is set to Device Traffic or Device Count, the view can be further filtered by Bytes, Packets, Bandwidth, and Sessions.



Fabric ADOM management

Starting from 6.2.0, FortiAnalyzer supports a new ADOM type called Fabric ADOM, which contains logs from all Fabric products (FortiGate, FortiMail, FortiWeb, FortiSandbox, FortiClient, and so on). When FortiManager is managing a FortiAnalzyer that contains a Fabric ADOM:

- ADOM type on FortiManager will be converted to a Fabric ADOM.
- Devices will be synchronized to the new ADOM (non-FortiGate devices are synchronized as log-only devices).
- Users can access logs from all devices in the remote ADOM.

This feature requires both FortiManager and FortiAnalyzer to be running version 6.2.0 or later.

FortiManager adds FortiAnalyzer devices by using central management. Any FortiGate devices that exist in FortiManager, but not in FortiAnalyzer will synchronize to FortiAnalyzer as logging devices. Any FortiGate devices that exists in FortiAnalyzer, but not in FortiManager will synchronize to FortiManager as configuration and logging devices, which means you must provide valid IP addresses and login credentials when adding the device. The non-FortiGate logging devices that exist in FortiAnalyzer, but not in FortiManager will synchronize to FortiManager as logging-only devices.

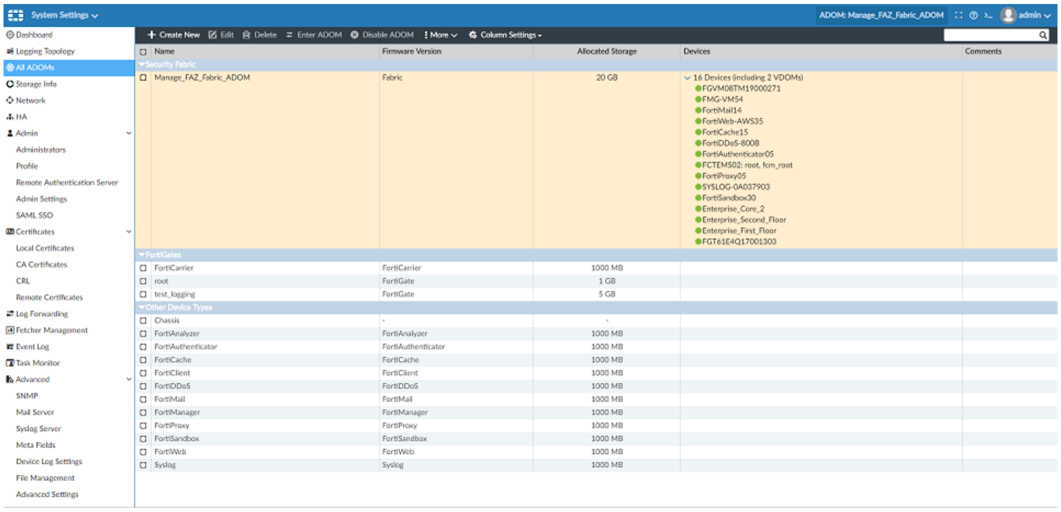
This procedure requires the following steps:

1. On FortiAnalyzer, create a Fabric ADOM.
2. On FortiManager, add an ADOM, and add the FortiAnalyzer device to the ADOM

To create a Fabric ADOM on FortiAnalyzer:

1. On FortiAnalyzer create a Fabric ADOM.
2. Open the ADOM, and add FortiGate logging devices, Security Fabric group and non-FortiGate logging devices,

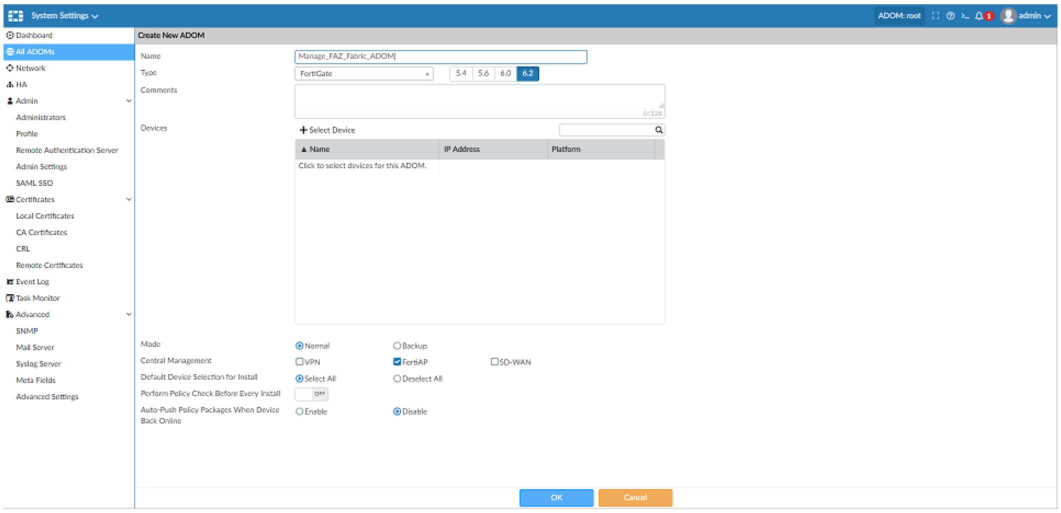
such as FortiWeb, FortiCache, FortiSandbox, and so on.



Name	Firmware Version	Allocated Storage	Devices	Comments
Security Fabric				
Manage_FAZ_Fabric_ADOM	Fabric	20 GB	16 Devices (including 2 VDOMs) FGVM08TM19000271 FMG-VM54 FortiMail14 FortiWeb-AWS35 FortiCache15 FortiDDoS-800B FortiAuthenticator05 FCTEMS02: root, fcm_root FortiProxy05 SYSLOG-0A037903 FortiSandbox30 Enterprise_Core_2 Enterprise_Second_Floor Enterprise_First_Floor FGT61E4Q17001303	
FortiGates				
FortiCarrier	FortiCarrier	1000 MB		
root	FortiGate	1 GB		
test_logging	FortiGate	5 GB		
Other Device Types				
Chassis	-	-		
FortiAnalyzer	FortiAnalyzer	1000 MB		
FortiAuthenticator	FortiAuthenticator	1000 MB		
FortiCache	FortiCache	1000 MB		
FortiClient	FortiClient	1000 MB		
FortiDDoS	FortiDDoS	1000 MB		
FortiMail	FortiMail	1000 MB		
FortiManager	FortiManager	1000 MB		
FortiProxy	FortiProxy	1000 MB		
FortiSandbox	FortiSandbox	1000 MB		
FortiWeb	FortiWeb	1000 MB		
Syslog	Syslog	1000 MB		

To configure FortiManager:

1. On FortiManager, create a FortiGate ADOM with the same name as the Fabric ADOM in FortiAnalyzer.
   The FortiGate ADOM will be used to manage the FortiAnalyzer Fabric ADOM. Although FortiManager supports Fabric ADOMs, you cannot use the GUI to create a Fabric ADOM.

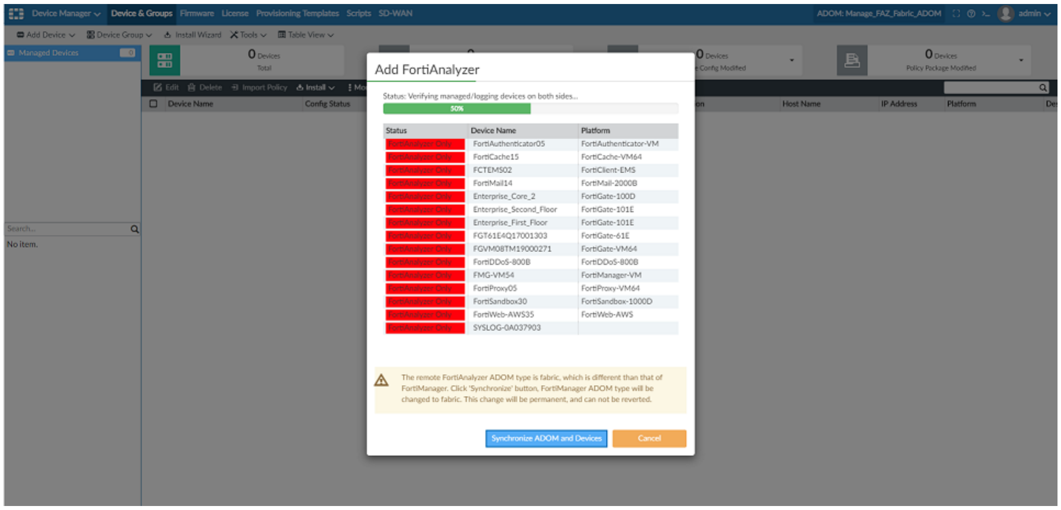
   Create New ADOM

   Name: Manage_FAZ_Fabric_ADOM
   Type: FortiGate 5.4 5.6 6.0 [✓ 6.2]
   Comments:
   Devices:

▲ Name	IP Address	Platform
Click to select devices for this ADOM.		

   Mode: ● Normal ○ Backup
   Central Management: □ VPN ☑ FortiAP □ SD-WAN
   Default Device Selection for Install: ● Select All ○ Deselect All
   Perform Policy Check Before Every Install: OFF
   Auto-Push Policy Packages When Device Back Online: ○ Enable ● Disable

2. Open the ADOM, and go to *Device Manager*.
3. From the *Add Device* menu, select *Add FortiAnalyzer* to use the wizard to add the FortiAnalyzer device.
   When the FortiAnalyzer ADOM type is Fabric, a warning is displayed. If you continue to synchronize the ADOM, the FortiManager ADOM type will change from FortiGate to Fabric.



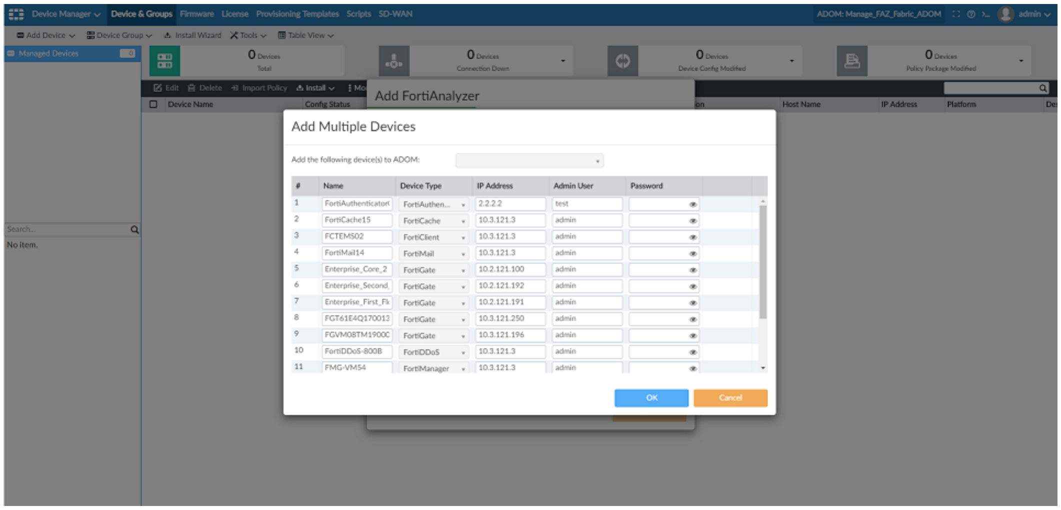
Add FortiAnalyzer

Status: Verifying managed/logging devices on both sides...

Status	Device Name	Platform
FortiAnalyzer Only	FortiAuthenticator05	FortiAuthenticator-VM
FortiAnalyzer Only	FortiCache15	FortiCache-VM64
FortiAnalyzer Only	FCTEMS02	FortiClient-EMS
FortiAnalyzer Only	FortiMail14	FortiMail-2000B
FortiAnalyzer Only	Enterprise_Core_2	FortiGate-100D
FortiAnalyzer Only	Enterprise_Second_Floor	FortiGate-101E
FortiAnalyzer Only	Enterprise_First_Floor	FortiGate-101E
FortiAnalyzer Only	FGT61E4Q17001303	FortiGate-61E
FortiAnalyzer Only	FGVM08TM19000271	FortiGate-VM64
FortiAnalyzer Only	FortiDDoS-800B	FortiDDoS-800B
FortiAnalyzer Only	FMG-VM54	FortiManager-VM
FortiAnalyzer Only	FortiProxy05	FortiProxy-VM64
FortiAnalyzer Only	FortiSandbox30	FortiSandbox-1000D
FortiAnalyzer Only	FortiWeb-AWS35	FortiWeb-AWS
FortiAnalyzer Only	SYSLOG-0A037903	

The remote FortiAnalyzer ADOM type is fabric, which is different than that of FortiManager. Click 'Synchronize' button, FortiManager ADOM type will be changed to fabric. This change will be permanent, and can not be reverted.

4. Click *Synchronize ADOM and Devices*.
   FortiManager starts to synchronize devices, and the *Add Multiple Devices* dialog box is displayed where you can edit the device name/ IP Address/ Admin User/ Password.



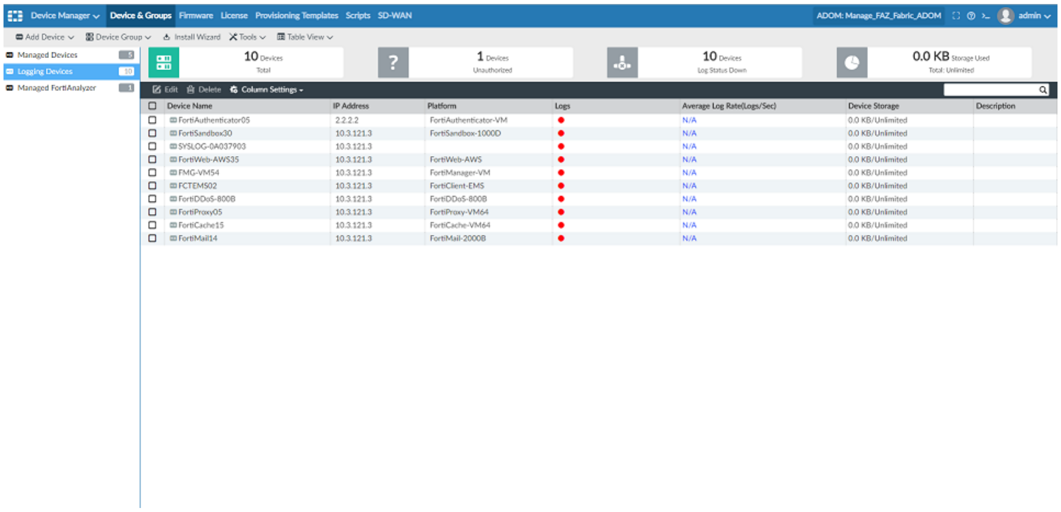
Add Multiple Devices

Add the following device(s) to ADOM:

#	Name	Device Type	IP Address	Admin User	Password
1	FortiAuthenticator(	FortiAuthen...	2.2.2.2	test	
2	FortiCache15	FortiCache	10.3.121.3	admin	
3	FCTEMS02	FortiClient	10.3.121.3	admin	
4	FortiMail14	FortiMail	10.3.121.3	admin	
5	Enterprise_Core_2	FortiGate	10.2.121.100	admin	
6	Enterprise_Second_	FortiGate	10.2.121.192	admin	
7	Enterprise_First_Fk	FortiGate	10.2.121.191	admin	
8	FGT61E4Q170013	FortiGate	10.3.121.250	admin	
9	FGVM08TM1900C	FortiGate	10.3.121.196	admin	
10	FortiDDoS-800B	FortiDDoS	10.3.121.3	admin	
11	FMG-VM54	FortiManager	10.3.121.3	admin	

A valid IP address and login credentials are required to add FortiGate devices.

After all devices are synchronized, FortiAnalyzer is successfully added to FortiManager.



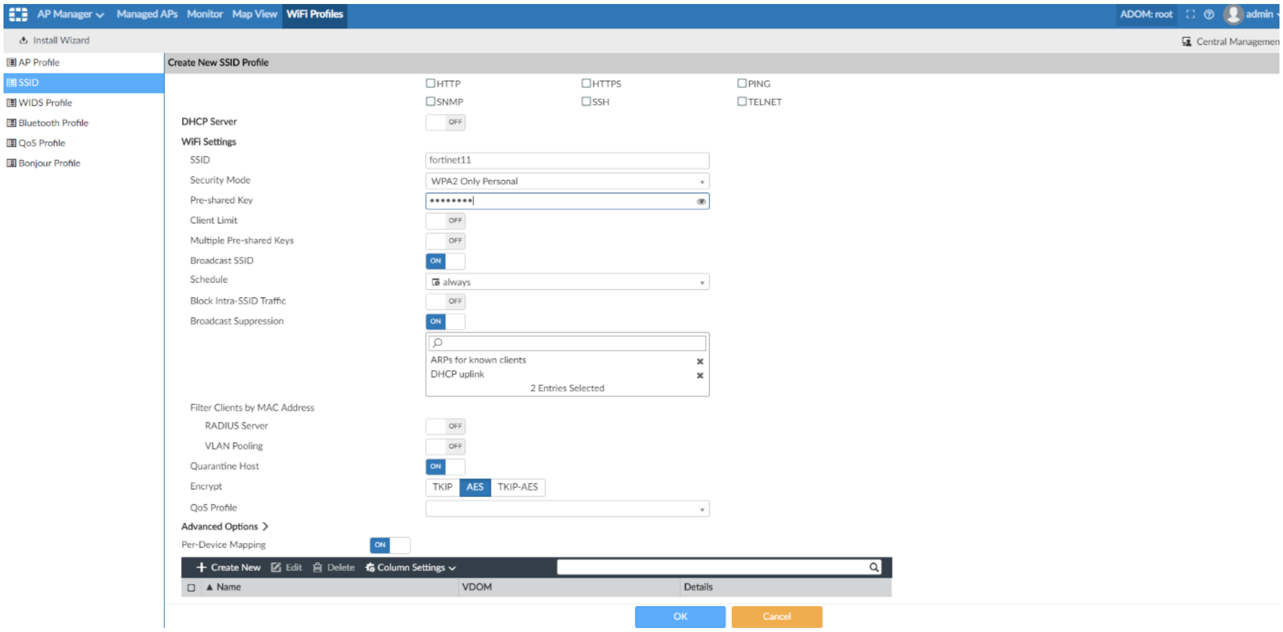
□	Device Name	IP Address	Platform	Logs	Average Log Rate(Logs/Sec)	Device Storage	Description
□	FortiAuthenticator05	2.2.2.2	FortiAuthenticator-VM	●	N/A	0.0 KB/Unlimited	
□	FortiSandbox30	10.3.121.3	FortiSandbox-1000D	●	N/A	0.0 KB/Unlimited	
□	SYSLOG-0A037903	10.3.121.3		●	N/A	0.0 KB/Unlimited	
□	FortiWeb-AWS35	10.3.121.3	FortiWeb-AWS	●	N/A	0.0 KB/Unlimited	
□	FMG-VM54	10.3.121.3	FortiManager-VM	●	N/A	0.0 KB/Unlimited	
□	FCTEMS02	10.3.121.3	FortiClient-EMS	●	N/A	0.0 KB/Unlimited	
□	FortiDDoS-800B	10.3.121.3	FortiDDoS-800B	●	N/A	0.0 KB/Unlimited	
□	FortiProxy05	10.3.121.3	FortiProxy-VM64	●	N/A	0.0 KB/Unlimited	
□	FortiCache15	10.3.121.3	FortiCache-VM64	●	N/A	0.0 KB/Unlimited	
□	FortiMail14	10.3.121.3	FortiMail-2000B	●	N/A	0.0 KB/Unlimited	

Dynamic Mapping for SSID

Dynamically map IP subnets to FortiGate devices where the SSID credentials are the same, but the subnet is different. This saves time for administrators since they can use the same SSID profile, and change granular settings using per-device mapping.

To configure per-device mapping for SSID:

1. Go to *AP Manager > WiFi Profiles > SSID*.
2. Toggle *Per-Device Mapping* to *ON*.



Create New SSID Profile

□HTTP □HTTPS □PING
□SNMP □SSH □TELNET

DHCP Server: OFF

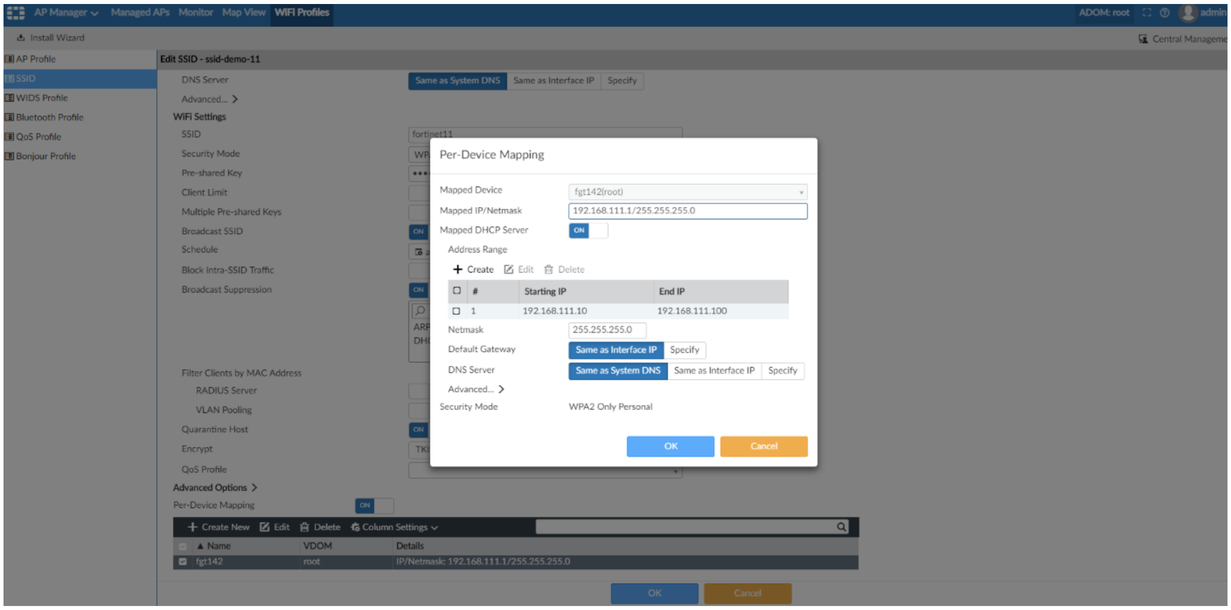
WiFi Settings
- SSID: fortinet11
- Security Mode: WPA2 Only Personal
- Pre-shared Key: ••••••••
- Client Limit: OFF
- Multiple Pre-shared Keys: OFF
- Broadcast SSID: ON
- Schedule: always
- Block Intra-SSID Traffic: OFF
- Broadcast Suppression: ON
  - ARPs for known clients ×
  - DHCP uplink ×
  - 2 Entries Selected
- Filter Clients by MAC Address
  - RADIUS Server: OFF
  - VLAN Pooling: OFF
- Quarantine Host: ON
- Encrypt: TKIP [✓ AES] TKIP-AES
- QoS Profile:

Advanced Options >

Per-Device Mapping: ON

□	▲ Name	VDOM	Details

3. Create a new SSID or edit an existing SSID. Configure the following settings:
   a. Select the mapped FortiGate device.
   b. Specify the *Mapped IP/Netmask*.
   c. Toggle *Mapped DHCP Server* to *ON*. Click *Create New* and specify the *Address Range*.



Edit SSID - ssid-demo-11

DNS Server: Same as System DNS | Same as Interface IP | Specify

Advanced...

WiFi Settings

SSID: fortinet11

Security Mode, Pre-shared Key, Client Limit, Multiple Pre-shared Keys, Broadcast SSID, Schedule, Block Intra-SSID Traffic, Broadcast Suppression, Filter Clients by MAC Address, RADIUS Server, VLAN Pooling, Quarantine Host, Encrypt, QoS Profile

Advanced Options

Per-Device Mapping: ON

Per-Device Mapping

Mapped Device: fgt142(root)

Mapped IP/Netmask: 192.168.111.1/255.255.255.0

Mapped DHCP Server: ON

Address Range

+ Create Edit Delete

□	#	Starting IP	End IP
□	1	192.168.111.10	192.168.111.100

Netmask: 255.255.255.0

Default Gateway: Same as Interface IP | Specify

DNS Server: Same as System DNS | Same as Interface IP | Specify

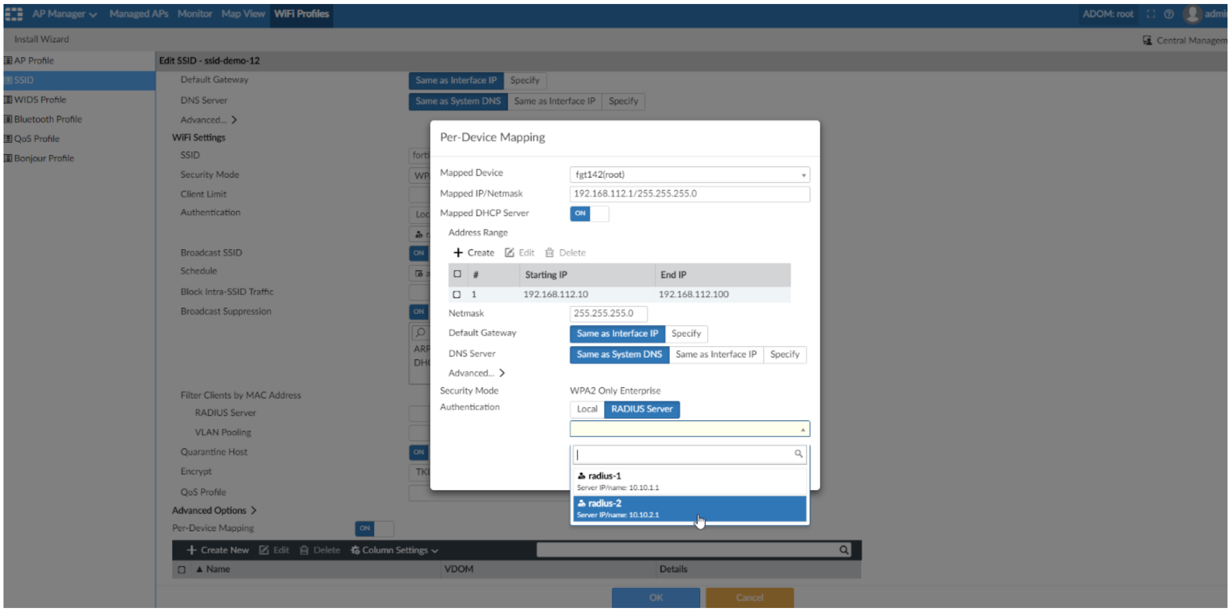
Advanced...

Security Mode: WPA2 Only Personal

OK Cancel

Name	VDOM	Details
fgt142	root	IP/Netmask: 192.168.111.1/255.255.255.0

   d. Select the SSID security mode as *WPA Enterprise*, *WPA only Enterprise* or *WPA2 Only Enterprise*, to override the authentication settings for mapped devices.



Edit SSID - ssid-demo-12

Default Gateway: Same as Interface IP | Specify

DNS Server: Same as System DNS | Same as Interface IP | Specify

Advanced...

WiFi Settings

SSID, Security Mode, Client Limit, Authentication, Broadcast SSID, Schedule, Block Intra-SSID Traffic, Broadcast Suppression, Filter Clients by MAC Address, RADIUS Server, VLAN Pooling, Quarantine Host, Encrypt, QoS Profile

Advanced Options

Per-Device Mapping: ON

Per-Device Mapping

Mapped Device: fgt142(root)

Mapped IP/Netmask: 192.168.112.1/255.255.255.0

Mapped DHCP Server: ON

Address Range

+ Create Edit Delete

□	#	Starting IP	End IP
□	1	192.168.112.10	192.168.112.100

Netmask: 255.255.255.0

Default Gateway: Same as Interface IP | Specify

DNS Server: Same as System DNS | Same as Interface IP | Specify

Advanced...

Security Mode: WPA2 Only Enterprise

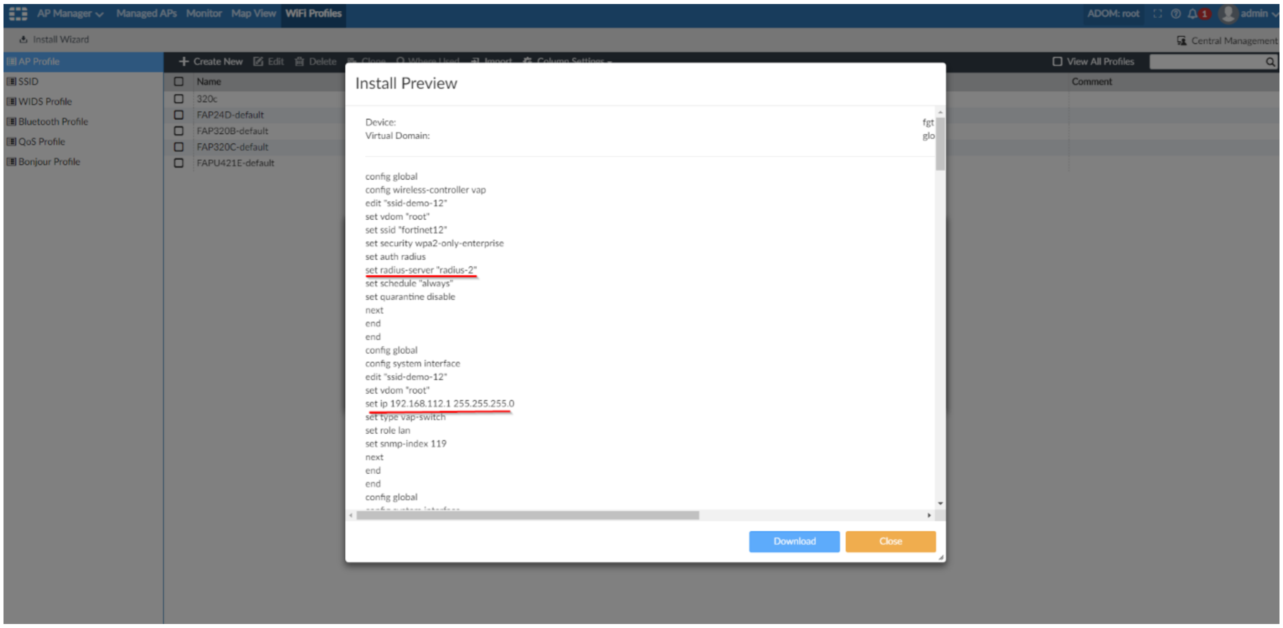
Authentication: Local | RADIUS Server

radius-1
Server IP/name: 10.10.1.1

radius-2
Server IP/name: 10.10.2.1

Name	VDOM	Details

4. When the SSIDs are being used for the mapped FortiGate device, install the per-device settings on FortiGate instead of the default settings in the SSID.



Install Preview

Device: fgt
Virtual Domain: glo

```
config global
config wireless-controller vap
edit "ssid-demo-12"
set vdom "root"
set ssid "fortinet12"
set security wpa2-only-enterprise
set auth radius
set radius-server "radius-2"
set schedule "always"
set quarantine disable
next
end
end
config global
config system interface
edit "ssid-demo-12"
set vdom "root"
set ip 192.168.112.1 255.255.255.0
set type vap-switch
set role lan
set snmp-index 119
next
end
end
config global
```

Split Task VDOM Mode Support

FortiManager 6.2.0 supports management of the new FortiGate Split Task VDOM mode.

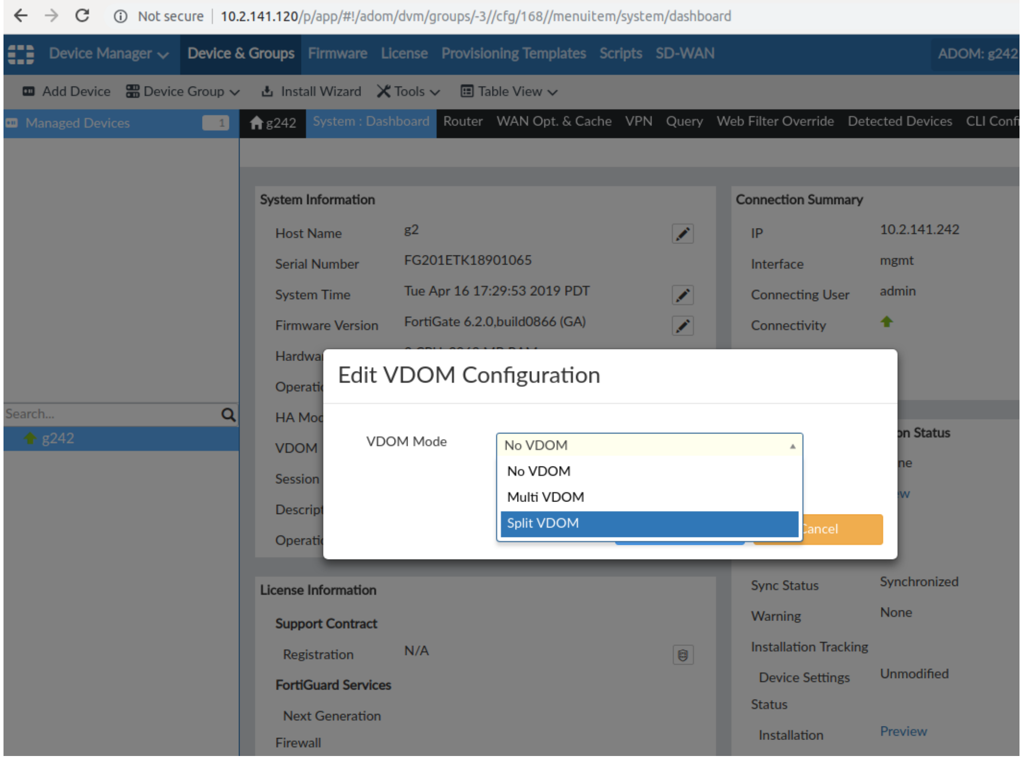
There are three VDOM modes available:

- *No VDOM*is when no VDOMs can be created.
- *Multi VDOM* is the original VDOMs enabled mode. You can create as many vdoms as you want, up to the VDOM license limit.
- *Split VDOM* is a specialized VDOM mode, with only 2 VDOMs - *FG-traffic* and *root*. More VDOMs cannot be added. FG-traffic is a regular VDOM. It is intended to have all the policies, addresses, UTM profiles for the device, and it will handle all the traffic, just like in No VDOM mode. root does not (and cannot) have policies or profiles. root is intended for the management of the FGT itself. Interfaces like *mgmt* , *ha* should be assigned to root and the rest of the interfaces to FG-traffic.

Multi VDOM and *Split VDOM* modes are not related and there is no compatibility between them. It is not possible to switch between Multi VDOM and Split VDOM. Any change has to go through *No VDOM* mode.

To configure Split VDOM:

- Turn on Split VDOM.



System Information

Host Name	g2
Serial Number	FG201ETK18901065
System Time	Tue Apr 16 17:29:53 2019 PDT
Firmware Version	FortiGate 6.2.0,build0866 (GA)

Connection Summary

IP	10.2.141.242
Interface	mgmt
Connecting User	admin
Connectivity	↑

Edit VDOM Configuration

VDOM Mode: No VDOM

- No VDOM
- Multi VDOM
- Split VDOM

License Information

Support Contract

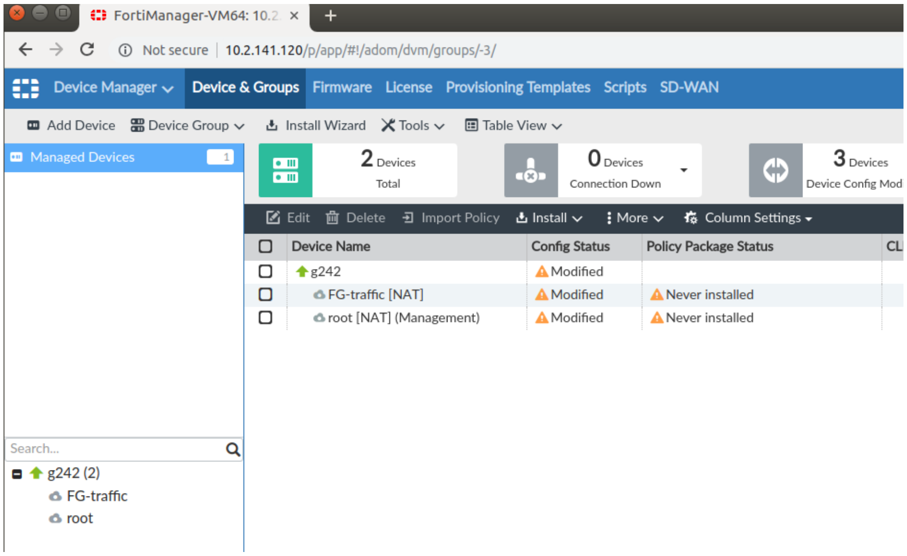
Registration	N/A

FortiGuard Services

Next Generation Firewall

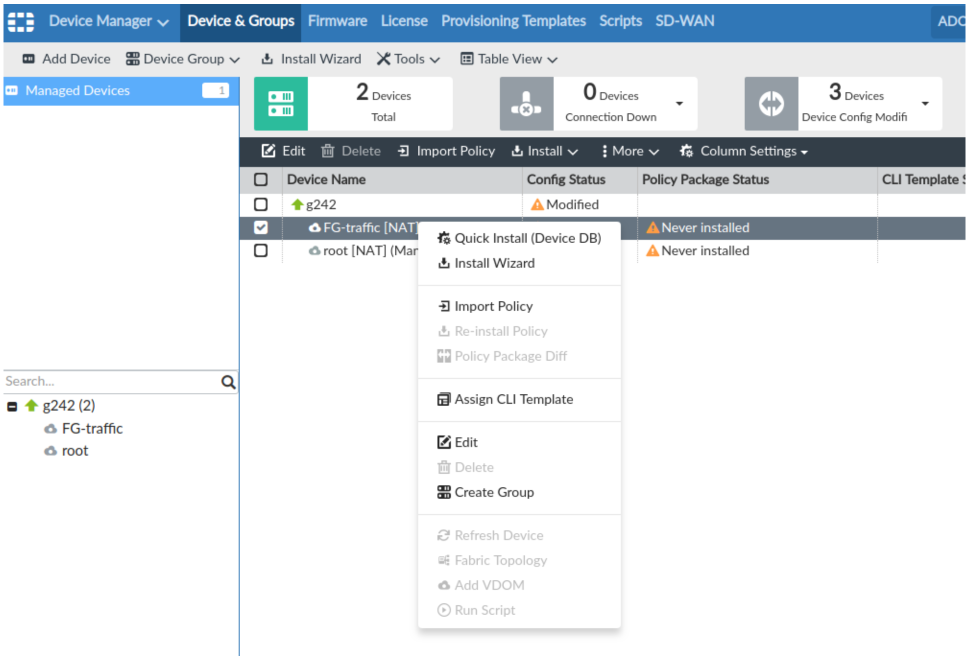
Sync Status	Synchronized
Warning	None
Installation Tracking	
Device Settings Status	Unmodified
Installation	Preview

- Two pre-defined VDOMs are available - FG-traffic and root.



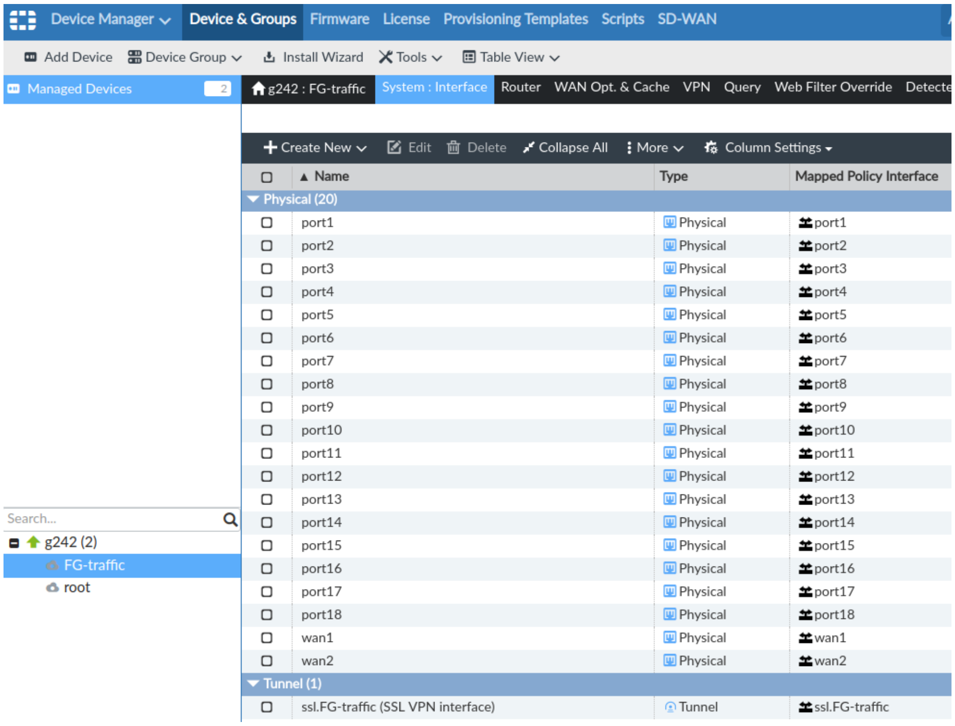
☐	Device Name	Config Status	Policy Package Status	CL
☐	g242	⚠ Modified		
☐	FG-traffic [NAT]	⚠ Modified	⚠ Never installed	
☐	root [NAT] (Management)	⚠ Modified	⚠ Never installed	

- You cannot add or delete VDOMs. The options are disabled in the right-click menu.



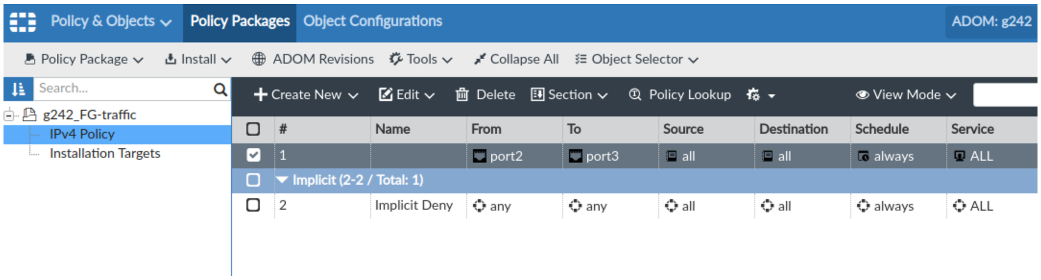
☐	Device Name	Config Status	Policy Package Status	CLI Template S
☐	g242	Modified		
☑	FG-traffic [NAT]		Never installed	
☐	root [NAT] (Mar		Never installed	

- Map all interfaces to ADOM.



☐	Name	Type	Mapped Policy Interface
	Physical (20)		
☐	port1	Physical	port1
☐	port2	Physical	port2
☐	port3	Physical	port3
☐	port4	Physical	port4
☐	port5	Physical	port5
☐	port6	Physical	port6
☐	port7	Physical	port7
☐	port8	Physical	port8
☐	port9	Physical	port9
☐	port10	Physical	port10
☐	port11	Physical	port11
☐	port12	Physical	port12
☐	port13	Physical	port13
☐	port14	Physical	port14
☐	port15	Physical	port15
☐	port16	Physical	port16
☐	port17	Physical	port17
☐	port18	Physical	port18
☐	wan1	Physical	wan1
☐	wan2	Physical	wan2
	Tunnel (1)		
☐	ssl.FG-traffic (SSL VPN interface)	Tunnel	ssl.FG-traffic

- Create policies and policy packages in FG-traffic and install.



□	#	Name	From	To	Source	Destination	Schedule	Service
☑	1		port2	port3	all	all	always	ALL
□	Implicit (2-2 / Total: 1)							
□	2	Implicit Deny	any	any	all	all	always	ALL

Fabric Connectors

This section lists the new features added to FortiManager for Fabric Connectors.

List of new features:

- Cisco pxGrid/ISE on page 22
- Multiple Concurrent Fabric Connectors on page 28
- FortiClient EMS Connector on page 29
- Cloud Connector - OCI on page 33
- Cloud Connector - GCP on page 38
- Cloud Connector - ESXi on page 43
- SDN Connector - Kubernetes (K8S) (Multiple Clouds) on page 49
- Cloud Connector - AliCloud on page 56

Cisco pxGrid/ISE

A new fabric connector is added for Cisco pxGrid. When enabled, FortiManager centralizes the updates from pxGrid for all FortiGate devices, and leverages the efficient FSSO protocol to apply dynamic policy updates to FortiGate.

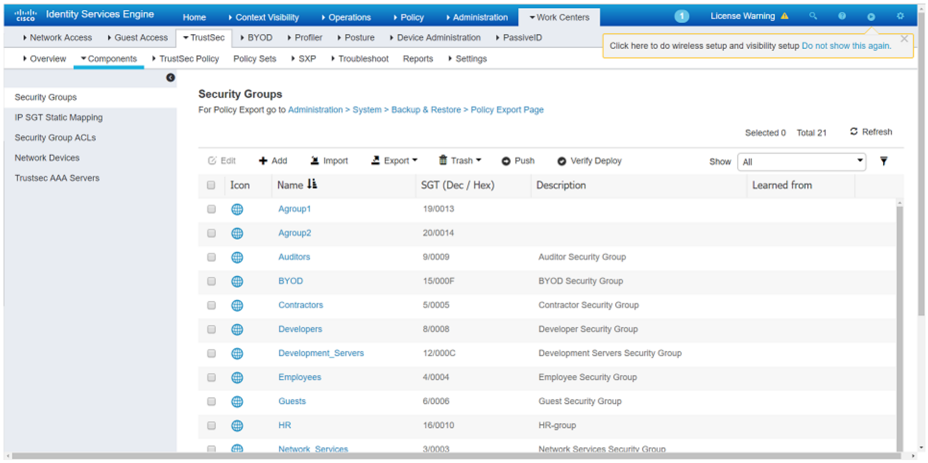
Deploying pxGrid connector consists of the following steps:

1. Configure Cisco ISE Server.
2. Configure FortiManager.

Configure Cisco ISE Server

To configure Cisco ISE server:

1. Create a Security Group: Go to *ISE* > *Work Centers* > *TrustSec* > *Components* > *Security Groups*. Click *Add*.



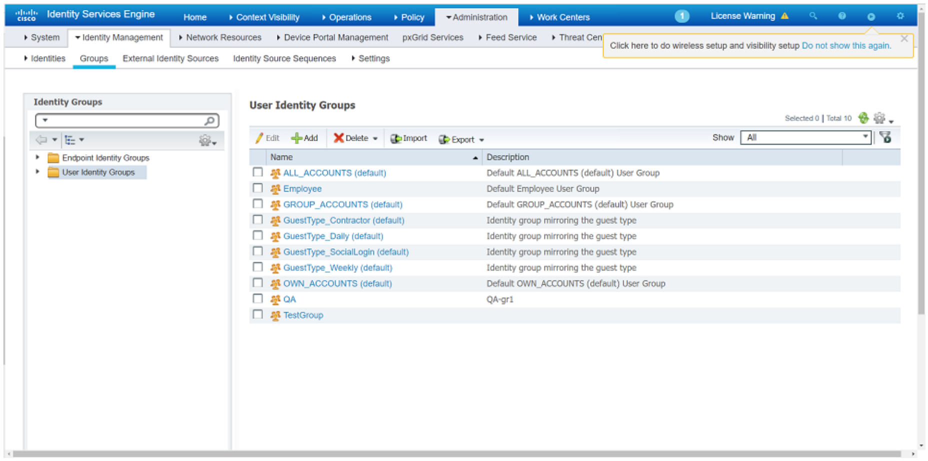
Security Groups

For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Selected 0 Total 21

Icon	Name	SGT (Dec / Hex)	Description	Learned from
🌐	Agroup1	19/0013		
🌐	Agroup2	20/0014		
🌐	Auditors	9/0009	Auditor Security Group	
🌐	BYOD	15/000F	BYOD Security Group	
🌐	Contractors	5/0005	Contractor Security Group	
🌐	Developers	8/0008	Developer Security Group	
🌐	Development_Servers	12/000C	Development Servers Security Group	
🌐	Employees	4/0004	Employee Security Group	
🌐	Guests	6/0006	Guest Security Group	
🌐	HR	16/0010	HR-group	
🌐	Network_Services	3/0003	Network Services Security Group	

2. Create a User Identity Group: Go to *ISE* > *Administration* > *Identity Management* > *Groups* > *User Identity Groups*. Click *Add*.

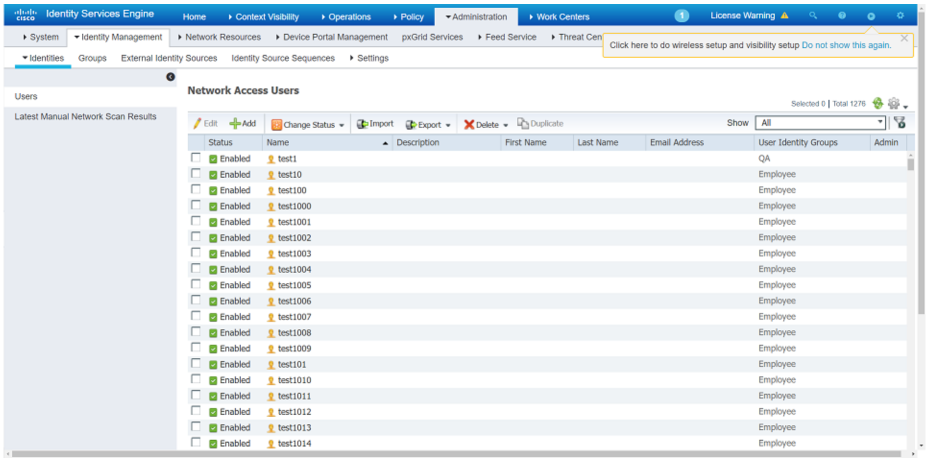


User Identity Groups

Selected 0 | Total 10

Name	Description
ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group
Employee	Default Employee User Group
GROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (default) User Group
GuestType_Contractor (default)	Identity group mirroring the guest type
GuestType_Daily (default)	Identity group mirroring the guest type
GuestType_SocialLogin (default)	Identity group mirroring the guest type
GuestType_Weekly (default)	Identity group mirroring the guest type
OWN_ACCOUNTS (default)	Default OWN_ACCOUNTS (default) User Group
QA	QA-gr1
TestGroup	

3. Create a user and add it to User Identity Group: Go to *ISE* > *Administration* > *Identity Management* > *Identities*. Click *Add*.

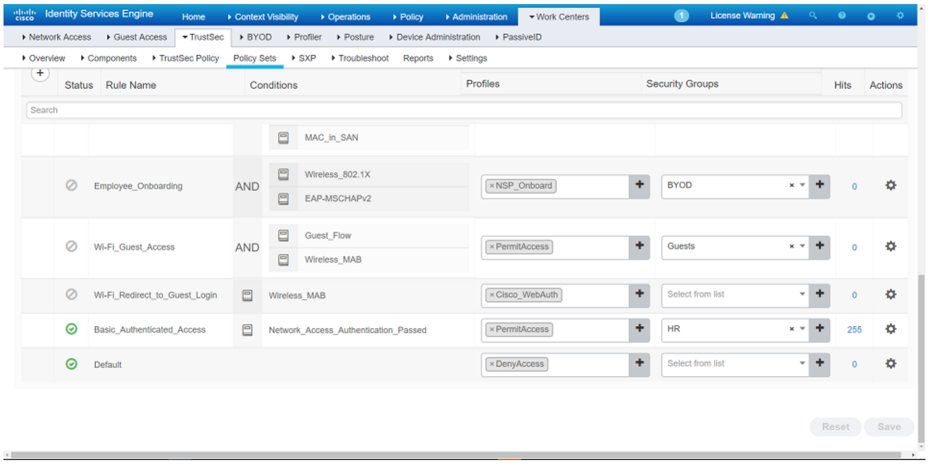


Network Access Users

Selected 0 | Total 1276

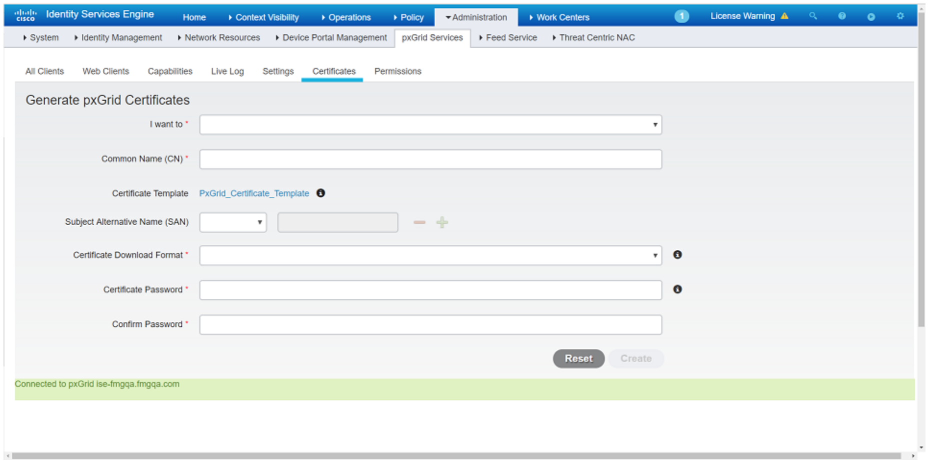
Status	Name	Description	First Name	Last Name	Email Address	User Identity Groups	Admin
Enabled	test1					QA	
Enabled	test10					Employee	
Enabled	test100					Employee	
Enabled	test1000					Employee	
Enabled	test1001					Employee	
Enabled	test1002					Employee	
Enabled	test1003					Employee	
Enabled	test1004					Employee	
Enabled	test1005					Employee	
Enabled	test1006					Employee	
Enabled	test1007					Employee	
Enabled	test1008					Employee	
Enabled	test1009					Employee	
Enabled	test101					Employee	
Enabled	test1010					Employee	
Enabled	test1011					Employee	
Enabled	test1012					Employee	
Enabled	test1013					Employee	
Enabled	test1014					Employee	

4. Match the Security Group with User Identity Group in the policy: Go to *ISE* > *Work Centers* >*TrustSec* > *Components* > *Policy Sets*. Right-click and go to *Authorization policy* > *Basic_Authenticatied _Access* and click *Edit* to match the Security Group with the User Identity Group.



Status	Rule Name	Conditions		Profiles	Security Groups	Hits	Actions
			MAC_in_SAN				
⊘	Employee_Onboarding	AND	Wireless_802.1X EAP-MSCHAPv2	× NSP_Onboard	BYOD	0	⚙
⊘	Wi-Fi_Guest_Access	AND	Guest_Flow Wireless_MAB	× PermitAccess	Guests	0	⚙
⊘	Wi-Fi_Redirect_to_Guest_Login		Wireless_MAB	× Cisco_WebAuth	Select from list	0	⚙
✓	Basic_Authenticated_Access		Network_Access_Authentication_Passed	× PermitAccess	HR	255	⚙
✓	Default			× DenyAccess	Select from list	0	⚙

5. Generate the pxGrid certificate and download it to the local computer: Go to *ISE > Administration > pxGrid Services > Certificate* and select *Generate pxGrid Certificates*.

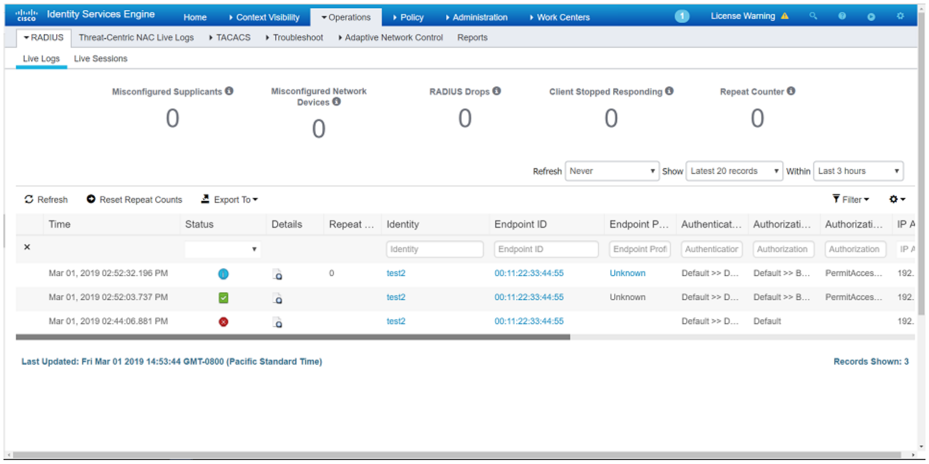


Generate pxGrid Certificates

I want to *	
Common Name (CN) *	
Certificate Template	PxGrid_Certificate_Template
Subject Alternative Name (SAN)	
Certificate Download Format *	
Certificate Password *	
Confirm Password *	

Connected to pxGrid ise-fmgqa.fmgqa.com

6. See log for current users: Go to *ISE > Operations > RADIUS > Live Logs*.



Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter
0	0	0	0	0

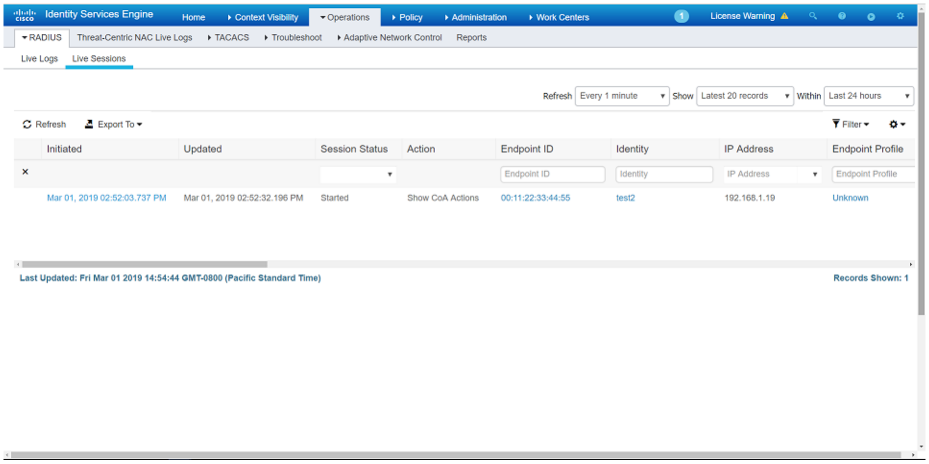
Refresh: Never; Show: Latest 20 records; Within: Last 3 hours

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authenticat...	Authorizati...	Authorizati...	IP A
Mar 01, 2019 02:52:32.196 PM	●		0	test2	00:11:22:33:44:55	Unknown	Default >> D...	Default >> B...	PermitAcces...	192.
Mar 01, 2019 02:52:03.737 PM	✓			test2	00:11:22:33:44:55	Unknown	Default >> D...	Default >> B...	PermitAcces...	192.
Mar 01, 2019 02:44:06.881 PM	⊗			test2	00:11:22:33:44:55		Default >> D...	Default		192.

Last Updated: Fri Mar 01 2019 14:53:44 GMT-0800 (Pacific Standard Time)

Records Shown: 3

7. See live sessions of current users: Go to *ISE > Operations > RADIUS > Live Sessions*.



Refresh: Every 1 minute; Show: Latest 20 records; Within: Last 24 hours

Initiated	Updated	Session Status	Action	Endpoint ID	Identity	IP Address	Endpoint Profile
Mar 01, 2019 02:52:03.737 PM	Mar 01, 2019 02:52:32.196 PM	Started	Show CoA Actions	00:11:22:33:44:55	test2	192.168.1.19	Unknown

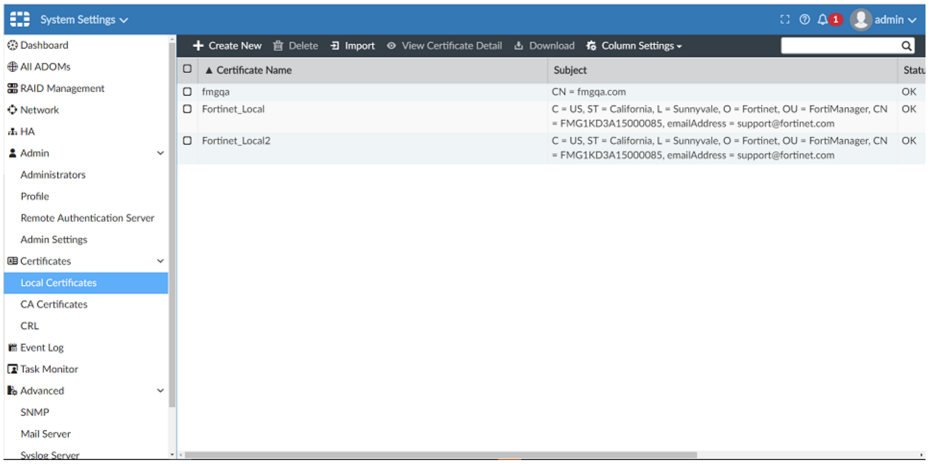
Last Updated: Fri Mar 01 2019 14:54:44 GMT-0800 (Pacific Standard Time)

Records Shown: 1

Configure FortiManager

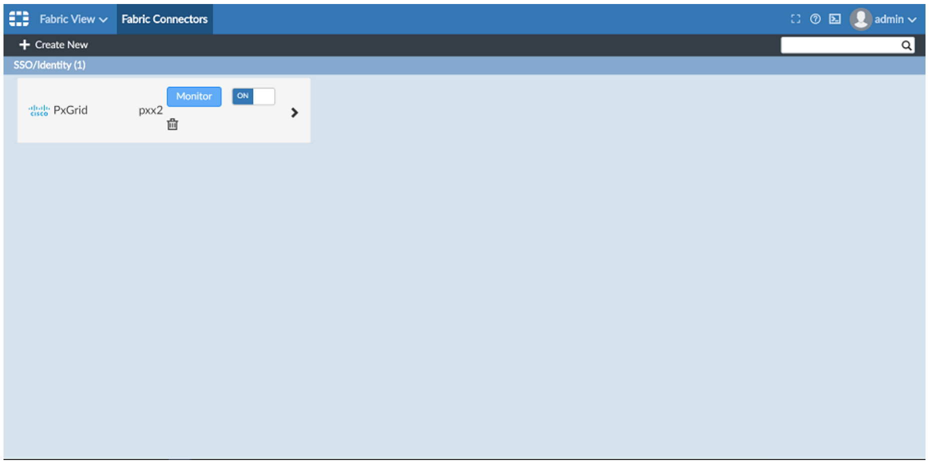
To configure FortiManager:

1. Go to *System Settings* > *Local Certificates* > *Import*. Import the downloaded certificate.

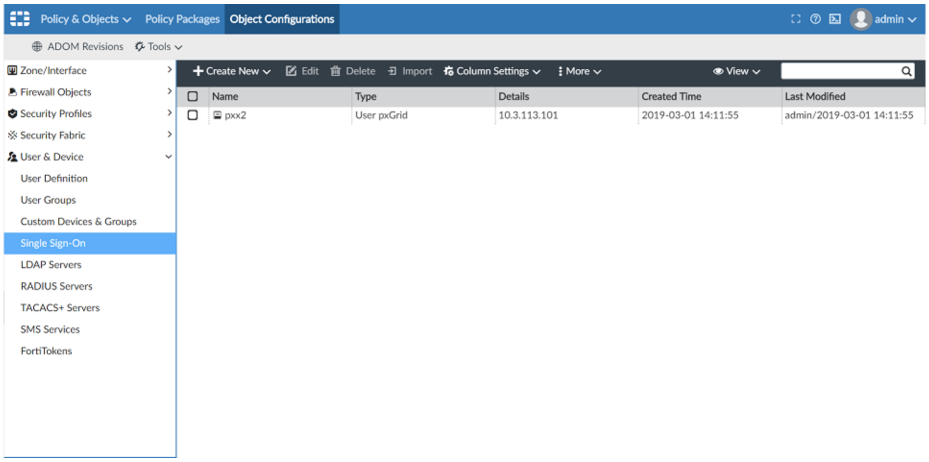


☐	▲ Certificate Name	Subject	Statu
☐	fmgqa	CN = fmgqa.com	OK
☐	Fortinet_Local	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiManager, CN = FMG1KD3A15000085, emailAddress = support@fortinet.com	OK
☐	Fortinet_Local2	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiManager, CN = FMG1KD3A15000085, emailAddress = support@fortinet.com	OK

2. Go to *Fabric View* > *Fabric Connectors*. Create a new pxGrid Fabric Connector with the imported certificate.

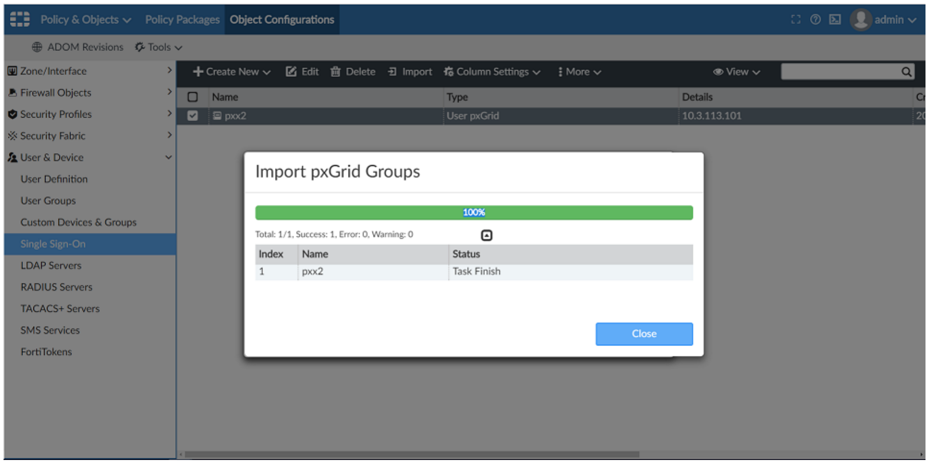


3. Go to *Policy & Objects* > *Object Configuration* > *Single Sign-On*. Select the connector and click *Import*.



☐	Name	Type	Details	Created Time	Last Modified
☐	pxx2	User pxGrid	10.3.113.101	2019-03-01 14:11:55	admin/2019-03-01 14:11:55

4. The pxGrid connector is imported. Click *Close* to close the import dialog.



Name	Type	Details
pxx2	User pxGrid	10.3.113.101

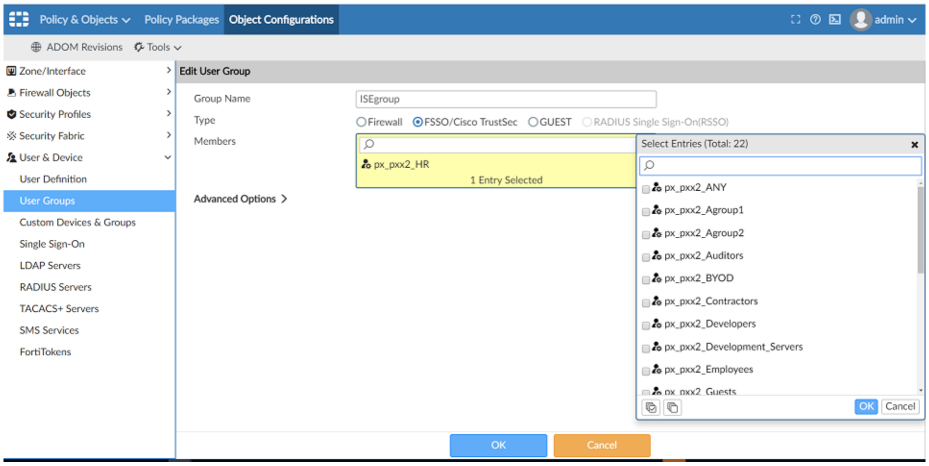
Import pxGrid Groups

100%

Total: 1/1, Success: 1, Error: 0, Warning: 0

Index	Name	Status
1	pxx2	Task Finish

5. Click *User Groups* and create a new group. Set the type as *FSSO/Cisco TrustSec*, and select *pxGrid* user as a member.



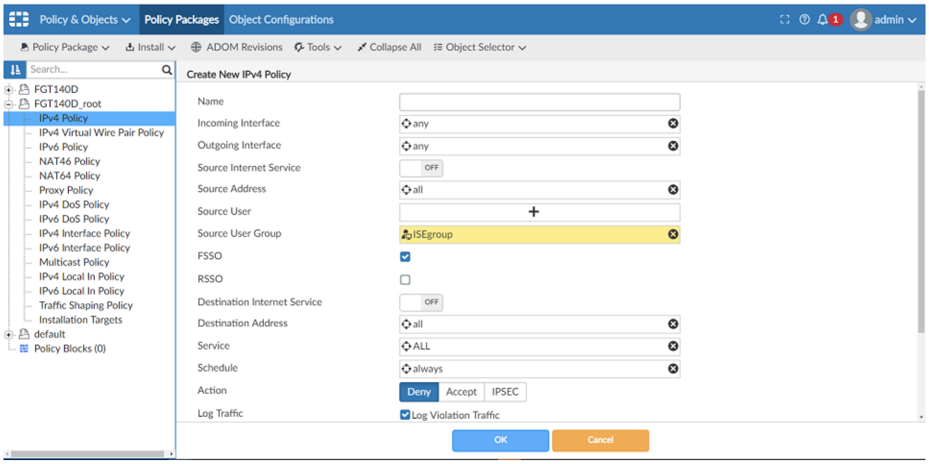
Edit User Group

Group Name	ISEgroup
Type	○ Firewall ● FSSO/Cisco TrustSec ○ GUEST ○ RADIUS Single Sign-On(RSSO)
Members	px_pxx2_HR 1 Entry Selected

Select Entries (Total: 22)

- □ px_pxx2_ANY
- □ px_pxx2_Agroup1
- □ px_pxx2_Agroup2
- □ px_pxx2_Auditors
- □ px_pxx2_BYOD
- □ px_pxx2_Contractors
- □ px_pxx2_Developers
- □ px_pxx2_Development_Servers
- □ px_pxx2_Employees
- □ px_pxx2_Guests

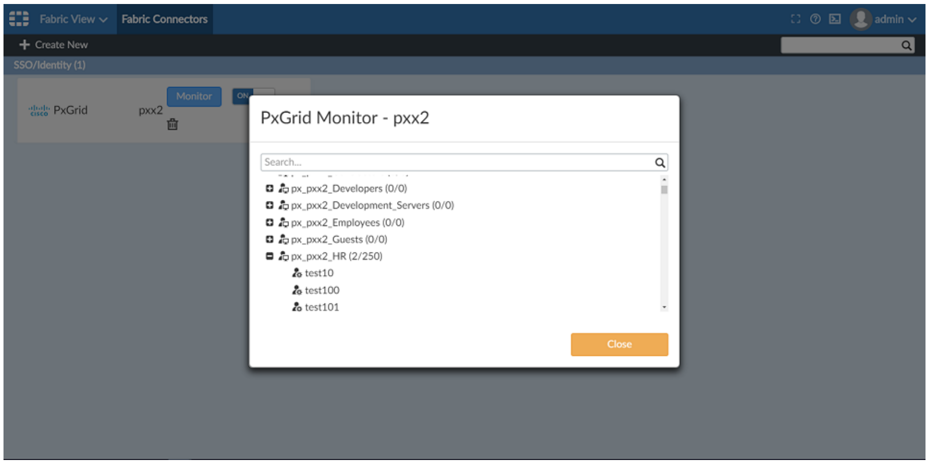
6. Create a policy with the *ISEgroup* user group and install the policy to FortiGate.



Create New IPv4 Policy

Name	
Incoming Interface	any
Outgoing Interface	any
Source Internet Service	OFF
Source Address	all
Source User	
Source User Group	ISEgroup
FSSO	☑
RSSO	□
Destination Internet Service	OFF
Destination Address	all
Service	ALL
Schedule	always
Action	Deny Accept IPSEC
Log Traffic	☑ Log Violation Traffic

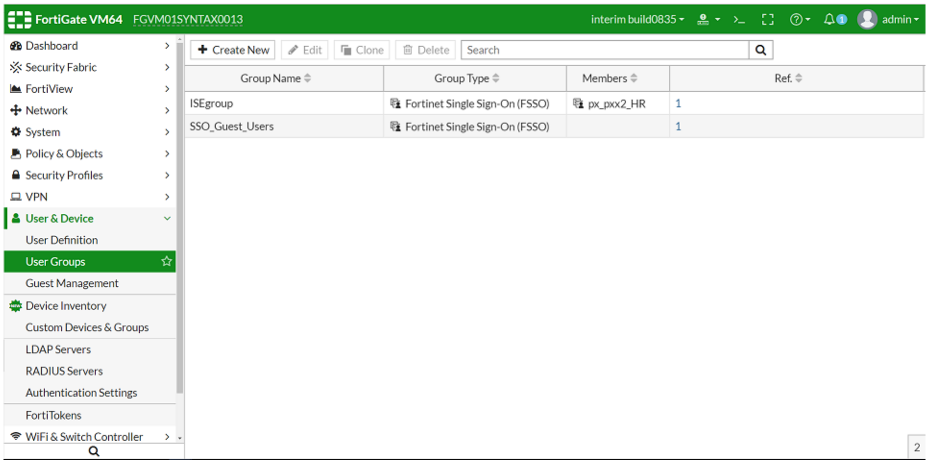
7. Go to *Fabric View* > *Fabric Connectors*. Click *Monitor* to see the users currently logged in.



PxGrid Monitor - pxx2

- px_pxx2_Developers (0/0)
- px_pxx2_Development_Servers (0/0)
- px_pxx2_Employees (0/0)
- px_pxx2_Guests (0/0)
- px_pxx2_HR (2/250)
  - test10
  - test100
  - test101

8. Log on to FortiGate to view the ISE user group.



Group Name	Group Type	Members	Ref.
ISEgroup	Fortinet Single Sign-On (FSSO)	px_pxx2_HR	1
SSO_Guest_Users	Fortinet Single Sign-On (FSSO)		1

9. On the FortiGate command line, use the `diagnose debug authd fsso` list to monitor the current user list.

Command Line

Command line for FortiManager:

```
config system connector
set
fsso-refresh-interval FSSO refresh interval (60 - 1800 seconds).
fsso-sess-timeout FSSO session timeout (30 - 600 seconds).
px-refresh-interval pxGrid refresh interval (60 - 1800 seconds).
px-svr-timeout pxGrid server timeout (30 - 600 seconds).
Realtime monitor debug to watch server connection:
diag debug application connector 255
```

Command line for FortiGate:

```
diag debug authd fsso server-status
diag debug authd fsso list-------> show connected users
----FSSO logons----
IP: 192.168.1.19 User: test2 Groups: px_fc1_security_grp1 Workstation: MemberOf: fscs1
```

```
IP: 192.168.1.20 User: test2 Groups: px_fc1_security_grp1 Workstation: MemberOf: fscs1
Total number of logons listed: 2, filtered: 0
----end of FSSO logons----
diag debug authd fsso refresh-logon
diag debug authd fsso refresh-group
```

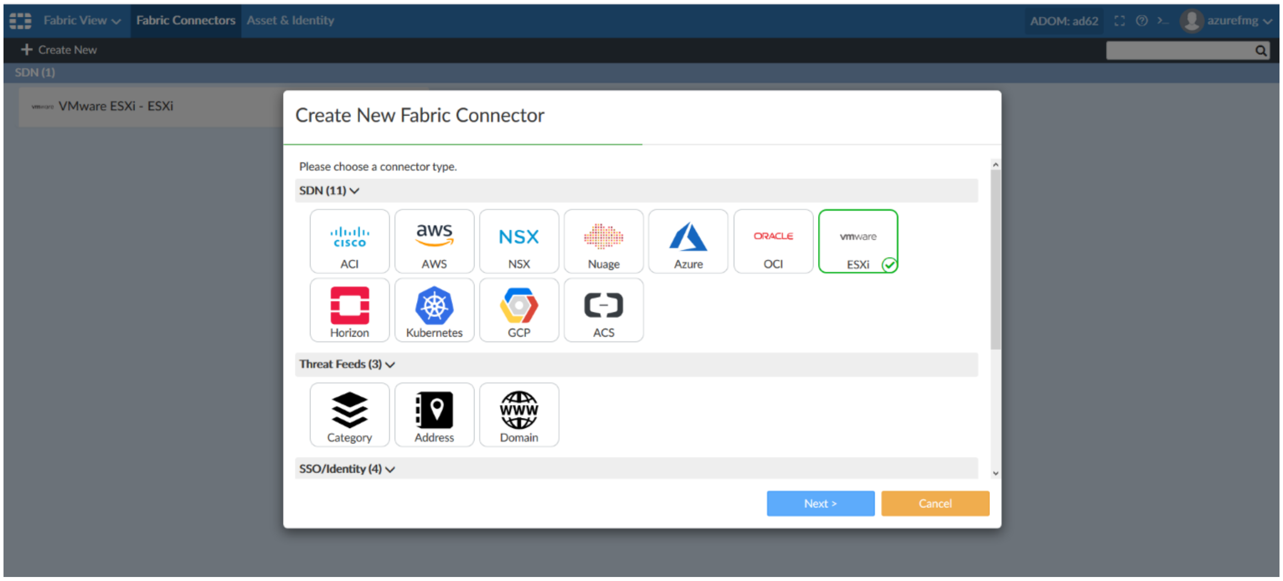
Multiple Concurrent Fabric Connectors

Previous versions of FortiManager allowed adding only one connector per type. For example, if you add the AWS connector, you could not add another AWS connector in FortiManager.

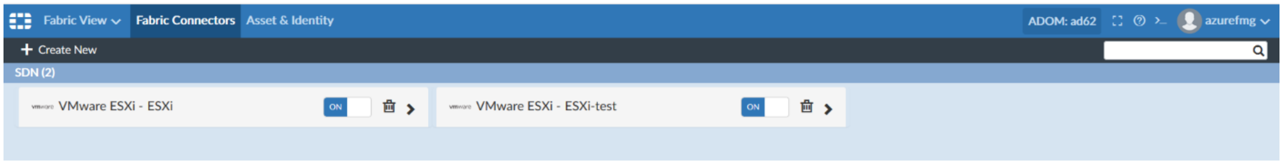
FortiManager version 6.2.0 allows adding multiple connectors of the same type.

To add multiple connectors of the same type from Fabric View:

1. Go to *Fabric View* and click *Create New*.
2. Select a fabric connector and configure the settings to add the connector.



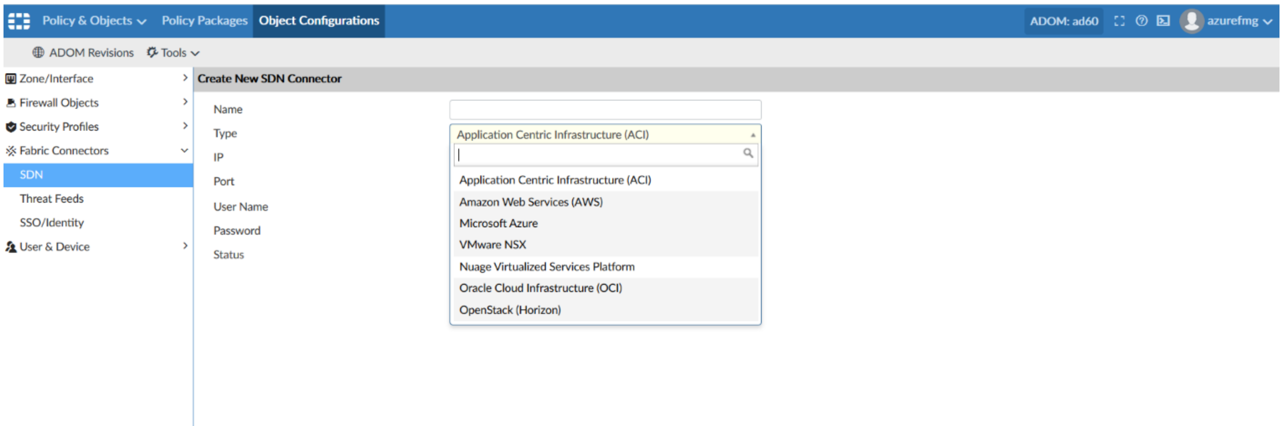
3. Select the same Fabric Connector and configure the settings to add the connector again.



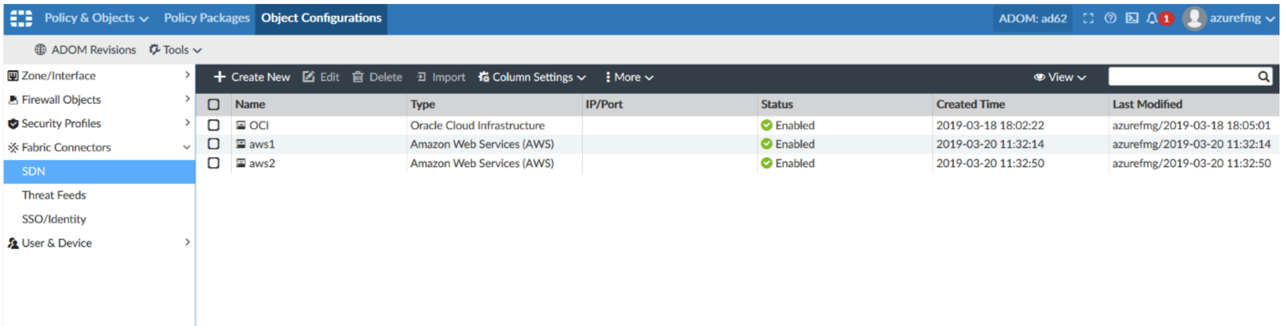
To add multiple connectors of the same type from Policy & Objects:

1. Go to *Policy & Objects* > *Object Configurations* > *Fabric Connectors*.
2. Click *Create New*.

3. Select a fabric connector and configure the settings to add the connector.



4. Select the same Fabric Connector and configure the settings to add the connector again.



□	Name	Type	IP/Port	Status	Created Time	Last Modified
□	OCI	Oracle Cloud Infrastructure		✓ Enabled	2019-03-18 18:02:22	azurefmg/2019-03-18 18:05:01
□	aws1	Amazon Web Services (AWS)		✓ Enabled	2019-03-20 11:32:14	azurefmg/2019-03-20 11:32:14
□	aws2	Amazon Web Services (AWS)		✓ Enabled	2019-03-20 11:32:50	azurefmg/2019-03-20 11:32:50

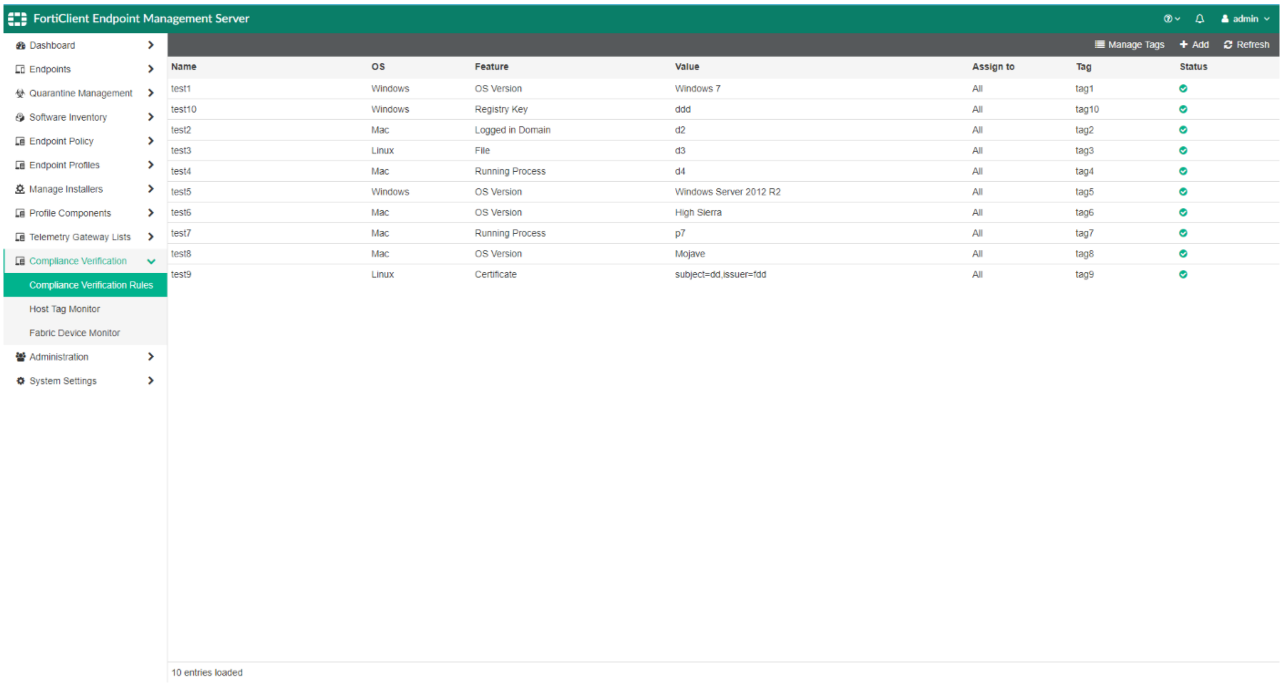
FortiClient EMS Connector

The FortiClient EMS Connector works virtually the same way as Active Directory / Single Sign On (FSSO) from the FortiManager's perspective:

- Configure the connector in FortiManager that manages the FortiGate devices. The administrator can define and install the dynamic groups and policies to FortiGate devices.
- FortiGate will communicate directly to FortiClient EMS to learn dynamic group changes and apply them in runtime.

To configure FortiClient EMS Connector with FSSO in FortiManager:

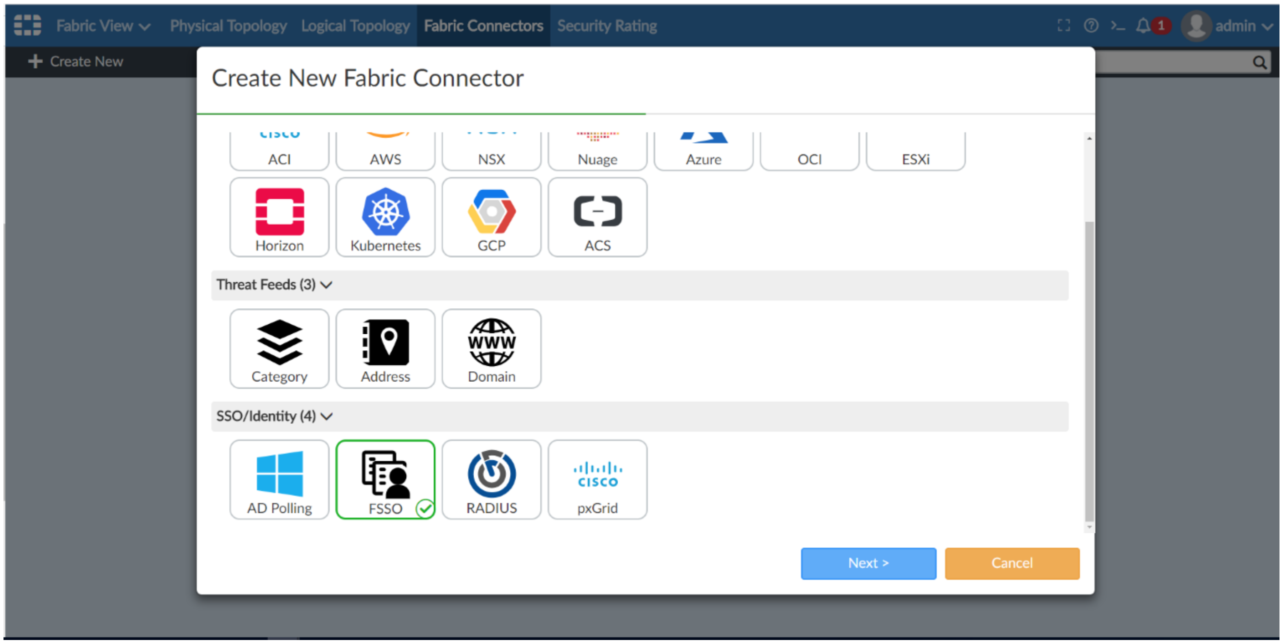
1. Install FortiClient Endpoint Management Server in Windows server. Log on to the EMS server and go to *Compliance Verification* > *Compliance Verification Rules* and click *Add Rules*. Create a few rules with different tags.



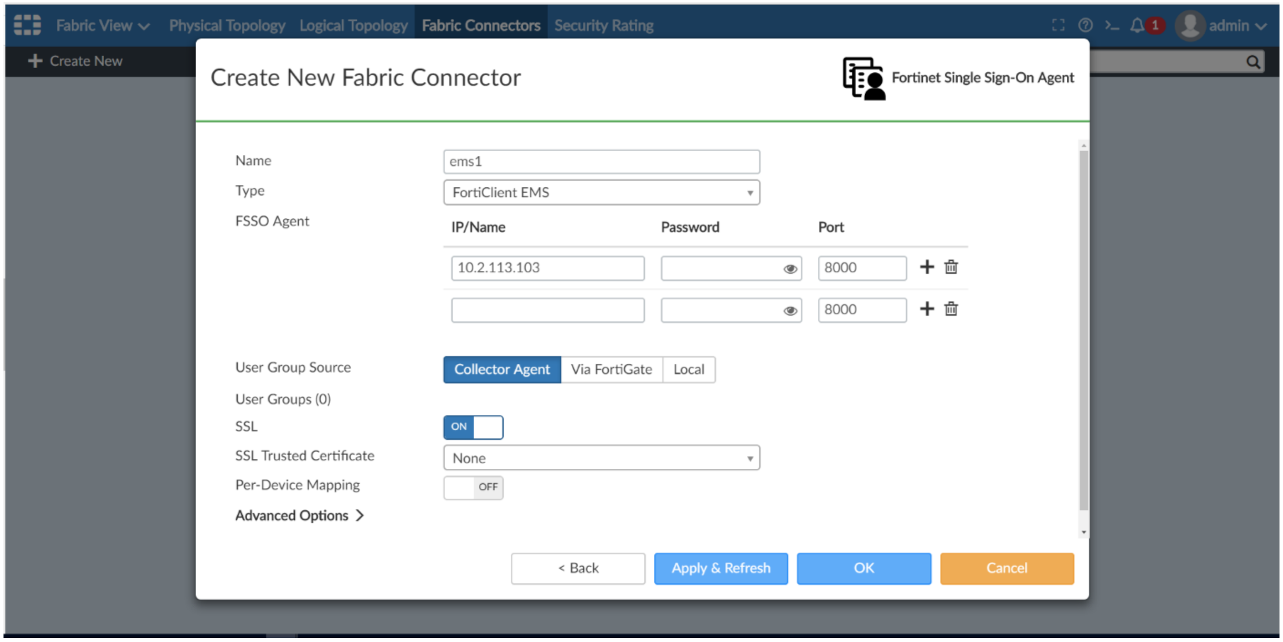
Name	OS	Feature	Value	Assign to	Tag	Status
test1	Windows	OS Version	Windows 7	All	tag1	✓
test10	Windows	Registry Key	ddd	All	tag10	✓
test2	Mac	Logged in Domain	d2	All	tag2	✓
test3	Linux	File	d3	All	tag3	✓
test4	Mac	Running Process	d4	All	tag4	✓
test5	Windows	OS Version	Windows Server 2012 R2	All	tag5	✓
test6	Mac	OS Version	High Sierra	All	tag6	✓
test7	Mac	Running Process	p7	All	tag7	✓
test8	Mac	OS Version	Mojave	All	tag8	✓
test9	Linux	Certificate	subject=dd,issuer=fdd	All	tag9	✓

10 entries loaded

2. Log on to FortiManager. Go to *Fabric View* > *Fabric Connectors* and click *Create*. Select *FSSO* and click *Next*.



3. In the *Create New Fabric Connector* screen, specify a *Name*, select the *Type* as *FortiClient EMS*, *IP/Name* as the Windows Server's IP and leave the password blank if the Windows Server does not have a password. Turn SSL to *ON*.



Create New Fabric Connector

Name	ems1
Type	FortiClient EMS

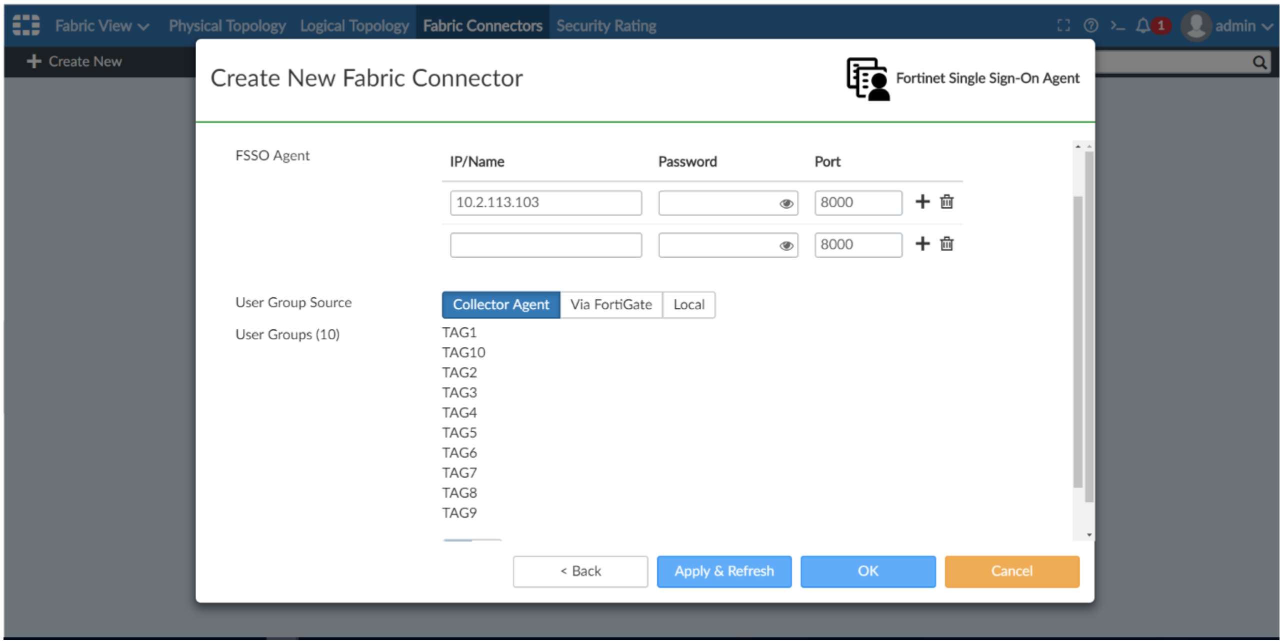
FSSO Agent

IP/Name	Password	Port
10.2.113.103		8000
		8000

User Group Source	Collector Agent / Via FortiGate / Local
User Groups (0)	
SSL	ON
SSL Trusted Certificate	None
Per-Device Mapping	OFF

Advanced Options >

4. Click *Apply and Refresh*. The connector gets a list of tags from the EMS server and shows them as User Groups. This is similar to the Active Directory group in the backend of the Windows Server.



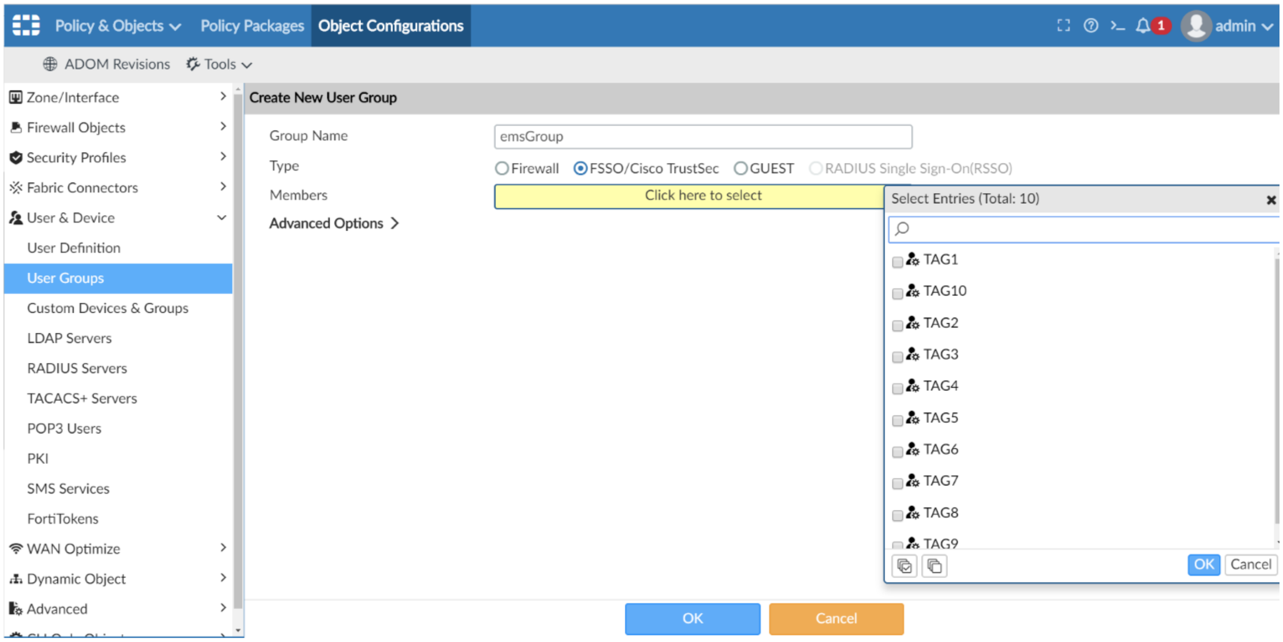
Create New Fabric Connector

FSSO Agent

IP/Name	Password	Port
10.2.113.103		8000
		8000

User Group Source	Collector Agent / Via FortiGate / Local
User Groups (10)	TAG1 TAG10 TAG2 TAG3 TAG4 TAG5 TAG6 TAG7 TAG8 TAG9

5. Go to *Policy & Objects* > *Object Configurations* > *User & Device* > *User Groups* and create a new user group. Specify a name for the group, select the type as *FSSO/Cisco TrustSec* and in *Select Entries*, select the tags from EMS server as members. Use this user group in a policy and install the policy to FortiGate devices.



Create New User Group

Group Name: emsGroup

Type: ○ Firewall ● FSSO/Cisco TrustSec ○ GUEST ○ RADIUS Single Sign-On(RSSO)

Members: Click here to select

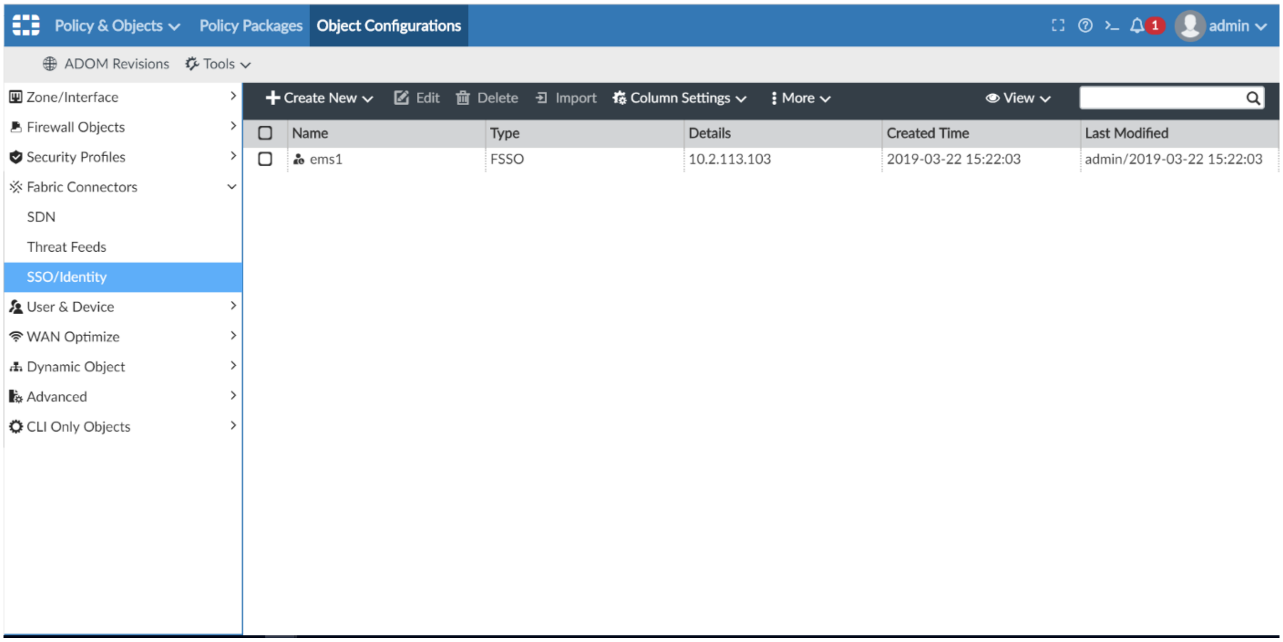
Advanced Options >

Select Entries (Total: 10)

- □ TAG1
- □ TAG10
- □ TAG2
- □ TAG3
- □ TAG4
- □ TAG5
- □ TAG6
- □ TAG7
- □ TAG8
- □ TAG9

OK Cancel

6. The Fabric Connectors are also visible in *Policy & Objects* > *Object Configurations* > *Fabric Connectors* > *SSO/Identity* where they can be edited if required.



□	Name	Type	Details	Created Time	Last Modified
□	ems1	FSSO	10.2.113.103	2019-03-22 15:22:03	admin/2019-03-22 15:22:03

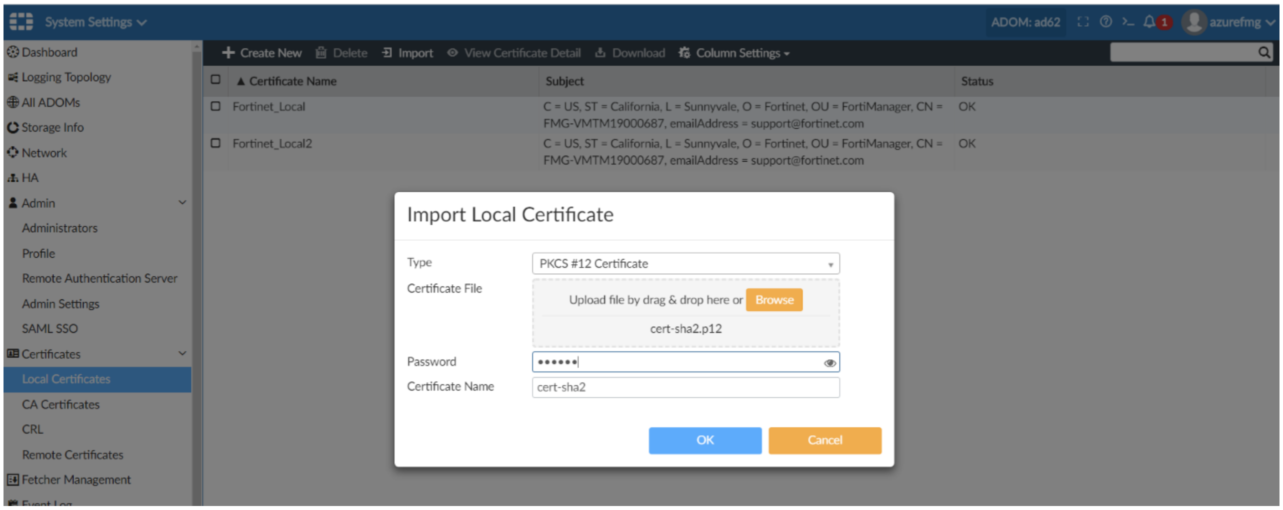
Refer to FortiClient Enterprise Management Server (EMS) Administration Guide or FortiClient Enterprise Management Server (EMS) Release Notes for system requirement and versions of Windows Server supported.

Cloud Connector - OCI

FortiOS 6.2 cloud connector for Oracle (OCI) can be centrally managed by FortiManager.

Create an OCI Certificate and Dynamic Local Certificate

- Import OCI certificate to FortiManager

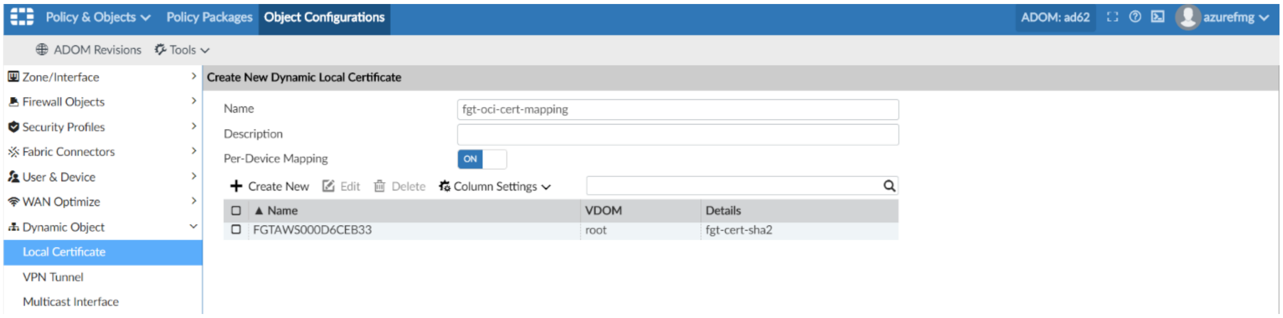


□	Certificate Name	Subject	Status
□	Fortinet_Local	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiManager, CN = FMG-VMTM19000687, emailAddress = support@fortinet.com	OK
□	Fortinet_Local2	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiManager, CN = FMG-VMTM19000687, emailAddress = support@fortinet.com	OK

Import Local Certificate

Type	PKCS #12 Certificate
Certificate File	Upload file by drag & drop here or Browse cert-sha2.p12
Password	••••••
Certificate Name	cert-sha2

- Create a New Dynamic Local Certificate mapping FortiGate OCI certificate from *Policy Packages > Objects Configurations > Dynamic Objects > Local Certificate*. This certificate is used to install to FortiGate with the correct OCI certificate configuration.



Create New Dynamic Local Certificate

Name	fgt-oci-cert-mapping
Description	
Per-Device Mapping	ON

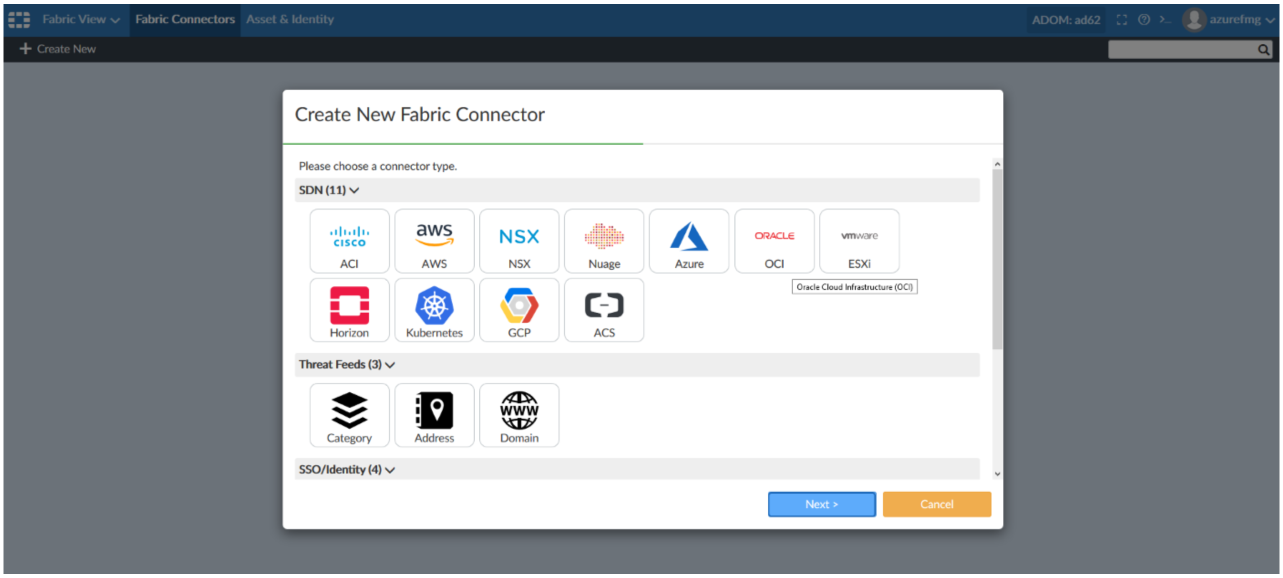
□	Name	VDOM	Details
□	FGTAWS000D6CEB33	root	fgt-cert-sha2

Create OCI SDN connector in Policy Packages

Create the SDN connector in Policy Packages.

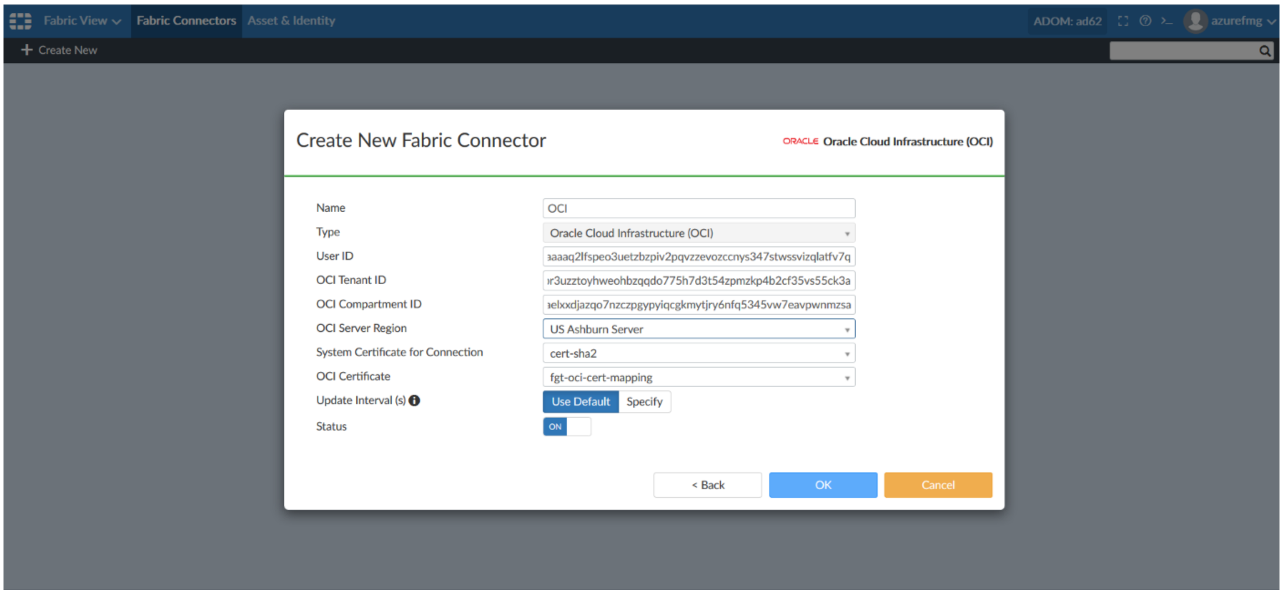
To create the SDN connector:

1. Go to *Policy & Objects* > *Fabric View* > *Fabric Connectors*.
2. Click *Create New*.



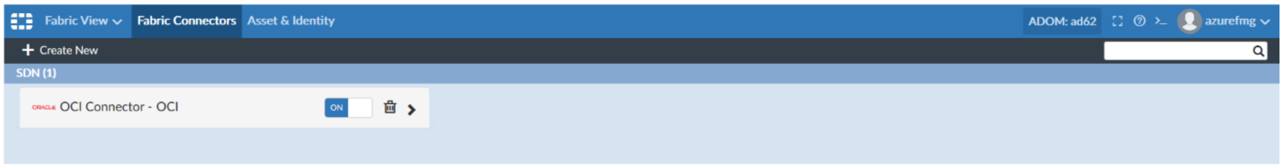
Please choose a connector type.

3. Select the *Oracle OCI* connector.
4. Specify the values. Most importantly, the *System Certificate for Connection* and the *OCI Certificate*.



Name	OCI
Type	Oracle Cloud Infrastructure (OCI)
User ID	ɔaaaq2lfspeo3uetzbzpiv2pqvzzevozccnys347stwssvizqlatfv7q
OCI Tenant ID	ɪr3uzztoyhweohbzqqdo775h7d3t54zpmzkp4b2cf35vs55ck3a
OCI Compartment ID	ɔelxxdjazqo7nzczpgypyiqcgkmytjry6nfq5345vw7eavpwnmzsa
OCI Server Region	US Ashburn Server
System Certificate for Connection	cert-sha2
OCI Certificate	fgt-oci-cert-mapping
Update Interval (s)	Use Default Specify
Status	ON

5. Click *OK*. The Oracle OCI connector is created.



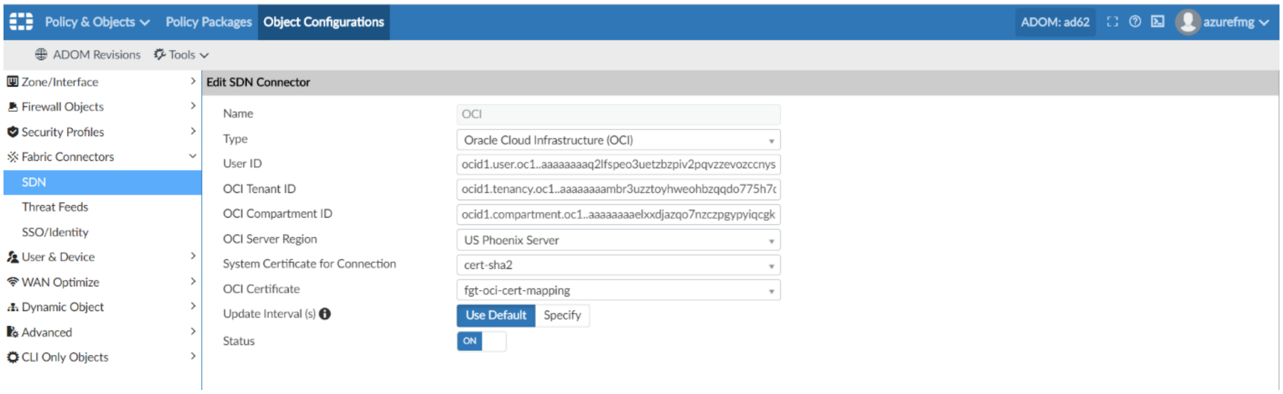
OCI Connector - OCI

Create OCI SDN connector in Object Configurations

Alternatively, you can create the SDN connector in Object Configurations.

To create the SDN connector:

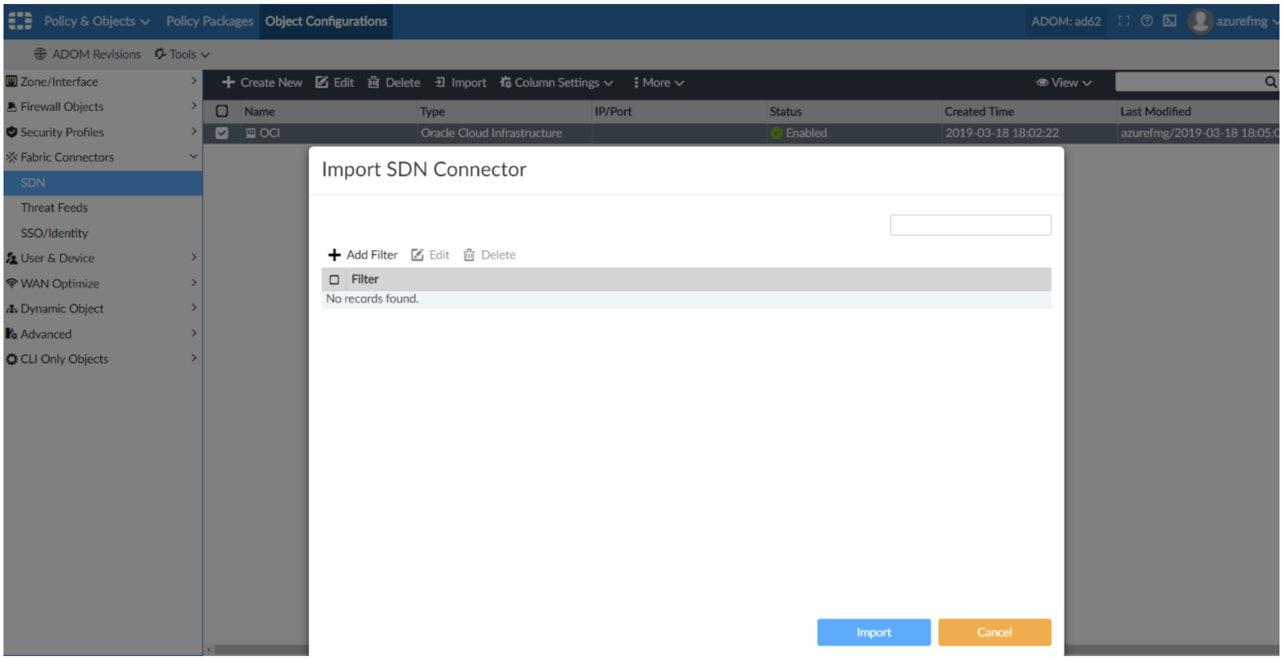
1. Go to *Policy & Objects* > *Object Configuration* > *Fabric Connectors*.
2. Click *SDN Connector* > *Oracle OCI connector*.



Edit SDN Connector

Name	OCI
Type	Oracle Cloud Infrastructure (OCI)
User ID	ocid1.user.oc1..aaaaaaaaq2lfspeo3uetzbzpiv2pqvzzevozccnys
OCI Tenant ID	ocid1.tenancy.oc1..aaaaaaaambr3uzztoyhweohbzqqdo775h7c
OCI Compartment ID	ocid1.compartment.oc1..aaaaaaaaelxxdjazqo7nzczpgypyiqcgk
OCI Server Region	US Phoenix Server
System Certificate for Connection	cert-sha2
OCI Certificate	fgt-oci-cert-mapping
Update Interval (s)	Use Default Specify
Status	ON

3. Click the *Import* to import OCI objects. The Import option is only available on *Policy & Objects* > *Object Configurations*.



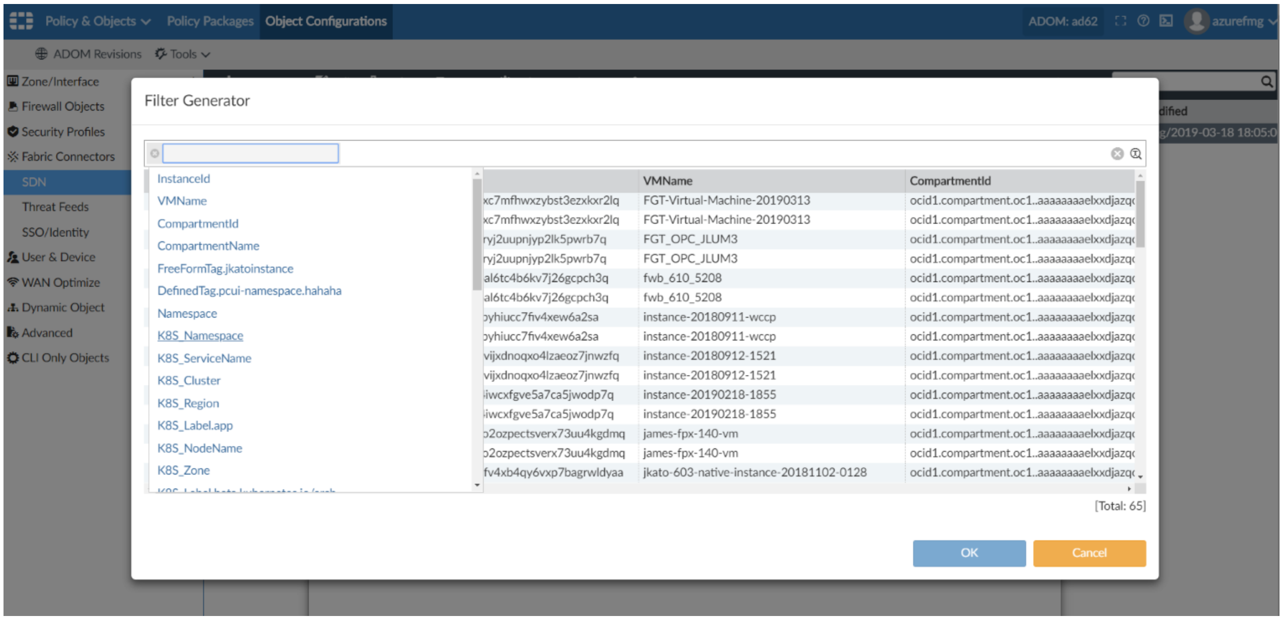
☐	Name	Type	IP/Port	Status	Created Time	Last Modified
☑	OCI	Oracle Cloud Infrastructure		Enabled	2019-03-18 18:02:22	azurefmg/2019-03-18 18:05:0

Import SDN Connector

☐	Filter

No records found.

4. Add the filter and then click *OK* to apply the selected filter.

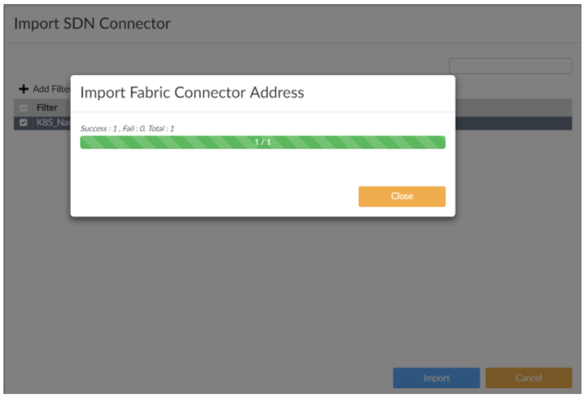


Filter Generator

	VMName	CompartmentId
xc7mfhwxzybst3ezxkxr2lq	FGT-Virtual-Machine-20190313	ocid1.compartment.oc1..aaaaaaaaelxxdjazq
xc7mfhwxzybst3ezxkxr2lq	FGT-Virtual-Machine-20190313	ocid1.compartment.oc1..aaaaaaaaelxxdjazq
ryj2uupnjyp2lk5pwrb7q	FGT_OPC_JLUM3	ocid1.compartment.oc1..aaaaaaaaelxxdjazq
ryj2uupnjyp2lk5pwrb7q	FGT_OPC_JLUM3	ocid1.compartment.oc1..aaaaaaaaelxxdjazq
al6tc4b6kv7j26gcpch3q	fwb_610_5208	ocid1.compartment.oc1..aaaaaaaaelxxdjazq
al6tc4b6kv7j26gcpch3q	fwb_610_5208	ocid1.compartment.oc1..aaaaaaaaelxxdjazq
oyhiucc7fiv4xew6a2sa	instance-20180911-wccp	ocid1.compartment.oc1..aaaaaaaaelxxdjazq
oyhiucc7fiv4xew6a2sa	instance-20180911-wccp	ocid1.compartment.oc1..aaaaaaaaelxxdjazq
vijxdnoqxo4lzaeoz7jnwzfq	instance-20180912-1521	ocid1.compartment.oc1..aaaaaaaaelxxdjazq
vijxdnoqxo4lzaeoz7jnwzfq	instance-20180912-1521	ocid1.compartment.oc1..aaaaaaaaelxxdjazq
iwcxfgve5a7ca5jwodp7q	instance-20190218-1855	ocid1.compartment.oc1..aaaaaaaaelxxdjazq
iwcxfgve5a7ca5jwodp7q	instance-20190218-1855	ocid1.compartment.oc1..aaaaaaaaelxxdjazq
o2ozpectsverx73uu4kgdmq	james-fpx-140-vm	ocid1.compartment.oc1..aaaaaaaaelxxdjazq
o2ozpectsverx73uu4kgdmq	james-fpx-140-vm	ocid1.compartment.oc1..aaaaaaaaelxxdjazq
fv4xb4qy6vxp7bagrwldyaa	jkato-603-native-instance-20181102-0128	ocid1.compartment.oc1..aaaaaaaaelxxdjazq

[Total: 65]

5. Click *Import* button to import.



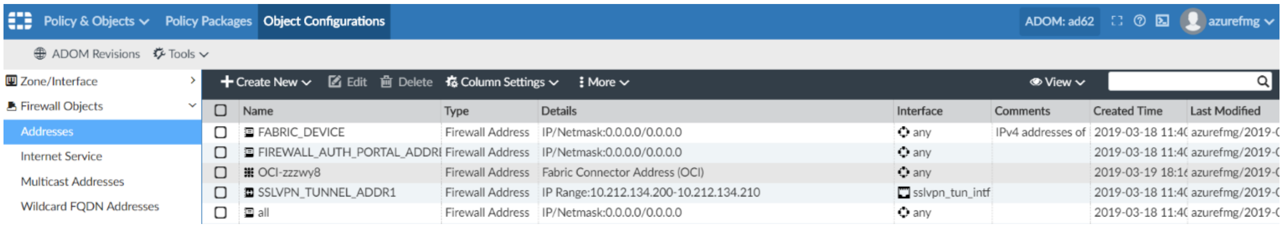
Import SDN Connector

Import Fabric Connector Address

Success : 1, Fail : 0, Total : 1

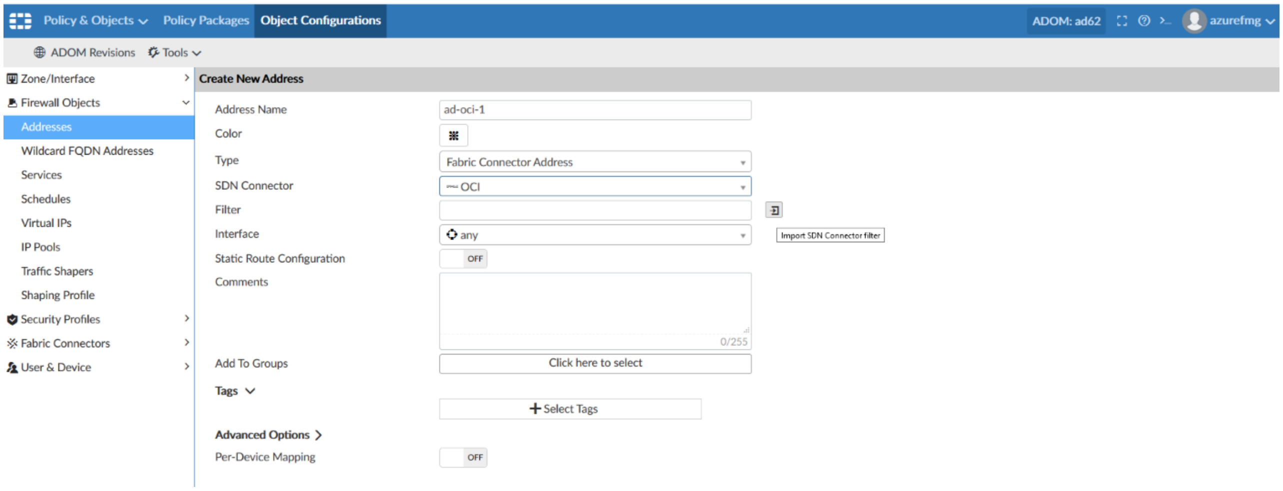
1 / 1

6. The new imported OCI address created.



□	Name	Type	Details	Interface	Comments	Created Time	Last Modified
□	FABRIC_DEVICE	Firewall Address	IP/Netmask:0.0.0.0/0.0.0.0	any	IPv4 addresses of	2019-03-18 11:4(	azurefmg/2019-(
□	FIREWALL_AUTH_PORTAL_ADDRI	Firewall Address	IP/Netmask:0.0.0.0/0.0.0.0	any		2019-03-18 11:4(	azurefmg/2019-(
□	OCI-zzzwy8	Firewall Address	Fabric Connector Address (OCI)	any		2019-03-19 18:1(	azurefmg/2019-(
□	SSLVPN_TUNNEL_ADDR1	Firewall Address	IP Range:10.212.134.200-10.212.134.210	sslvpn_tun_intf		2019-03-18 11:4(	azurefmg/2019-(
□	all	Firewall Address	IP/Netmask:0.0.0.0/0.0.0.0	any		2019-03-18 11:4(	azurefmg/2019-(

7. Create a new *Fabric Connector Address*. Import the connector or enter the details of the connector.



Policy & Objects | Policy Packages | Object Configurations | ADOM: ad62 | azurefmg

ADOM Revisions | Tools

- Zone/Interface
- Firewall Objects
  - Addresses
  - Wildcard FQDN Addresses
  - Services
  - Schedules
  - Virtual IPs
  - IP Pools
  - Traffic Shapers
  - Shaping Profile
- Security Profiles
- Fabric Connectors
- User & Device

Create New Address

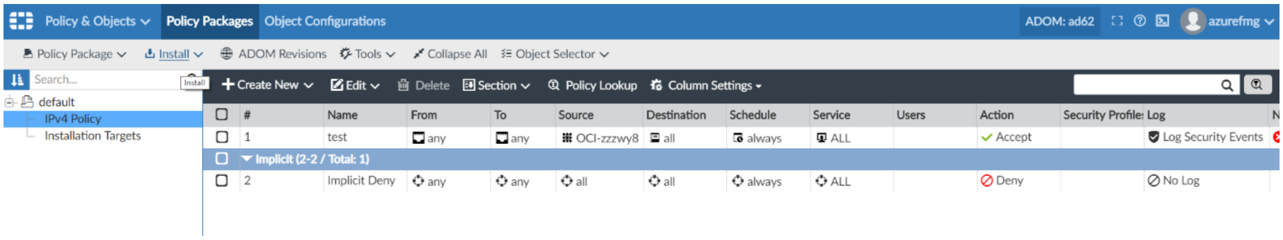
Address Name	ad-oci-1
Color	
Type	Fabric Connector Address
SDN Connector	OCI
Filter	
Interface	any
Static Route Configuration	OFF
Comments	0/255
Add To Groups	Click here to select
Tags	+ Select Tags
Advanced Options	
Per-Device Mapping	OFF

Import SDN Connector filter

Install the SDN connector to FortiGate

To install the SDN connector to FortiGate:

1. Install OCI SDN connector configuration and imported OCI dynamic object to FortiGate.



Policy & Objects | Policy Packages | Object Configurations | ADOM: ad62 | azurefmg

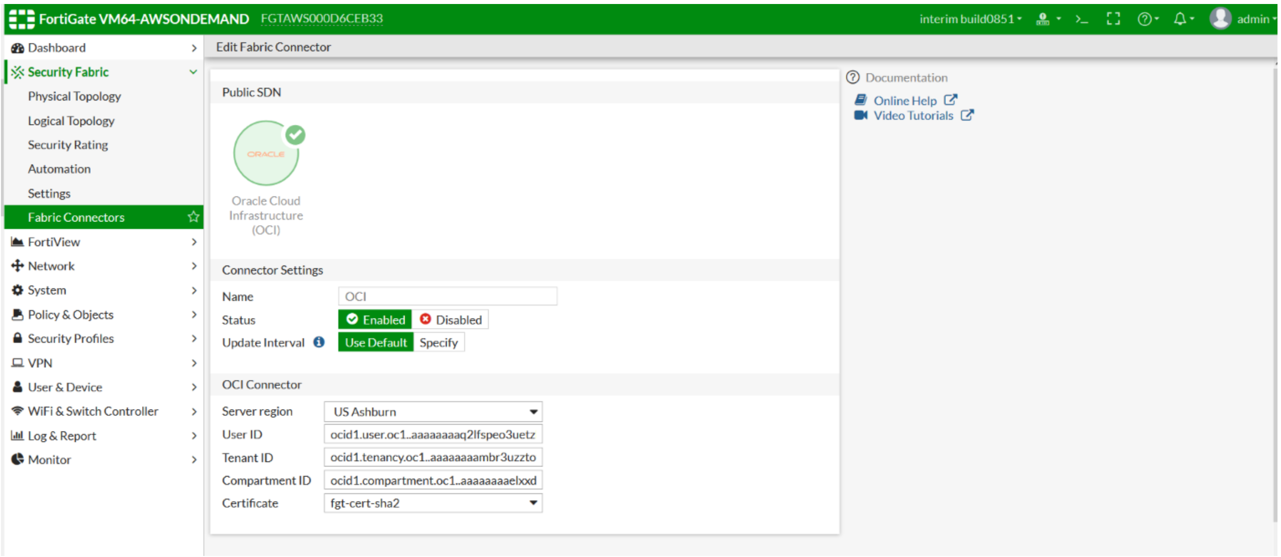
Policy Package | Install | ADOM Revisions | Tools | Collapse All | Object Selector

Create New | Edit | Delete | Section | Policy Lookup | Column Settings

- default
  - IPv4 Policy
  - Installation Targets

#	Name	From	To	Source	Destination	Schedule	Service	Users	Action	Security Profiles	Log
1	test	any	any	OCI-zzzwy8	all	always	ALL		Accept		Log Security Events
Implicit (2-2 / Total: 1)											
2	Implicit Deny	any	any	all	all	always	ALL		Deny		No Log

2. Check the FortiGate whether, the OCI connector and address is installed.



FortiGate VM64-AWSONDEMAND FGTAWS000D6CEB33 | interim build0851 | admin

- Dashboard
- Security Fabric
  - Physical Topology
  - Logical Topology
  - Security Rating
  - Automation
  - Settings
  - Fabric Connectors
- FortiView
- Network
- System
- Policy & Objects
- Security Profiles
- VPN
- User & Device
- WiFi & Switch Controller
- Log & Report
- Monitor

Edit Fabric Connector

Public SDN

Oracle Cloud Infrastructure (OCI)

Connector Settings

Name	OCI
Status	Enabled / Disabled
Update Interval	Use Default / Specify

OCI Connector

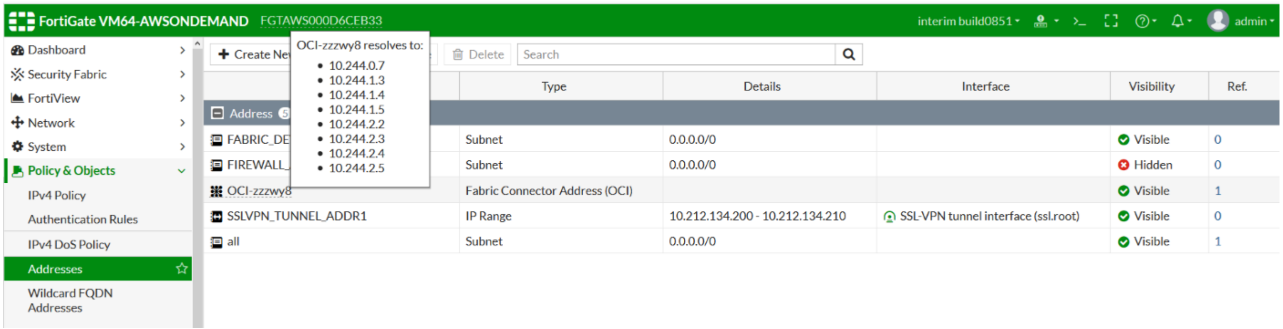
Server region	US Ashburn
User ID	ocid1.user.oc1..aaaaaaaaq2lfspeo3uetz
Tenant ID	ocid1.tenancy.oc1..aaaaaaaambr3uzzto
Compartment ID	ocid1.compartment.oc1..aaaaaaaaelxxd
Certificate	fgt-cert-sha2

Documentation

Online Help

Video Tutorials

3. The OCI address IP can now be resolved.



OCI-zzzwy8 resolves to:

- 10.244.0.7
- 10.244.1.3
- 10.244.1.4
- 10.244.1.5
- 10.244.2.2
- 10.244.2.3
- 10.244.2.4
- 10.244.2.5

	Type	Details	Interface	Visibility	Ref.
Address 5					
FABRIC_DE	Subnet	0.0.0.0/0		Visible	0
FIREWALL_	Subnet	0.0.0.0/0		Hidden	0
OCI-zzzwy8	Fabric Connector Address (OCI)			Visible	1
SSLVPN_TUNNEL_ADDR1	IP Range	10.212.134.200 - 10.212.134.210	SSL-VPN tunnel interface (ssl.root)	Visible	0
all	Subnet	0.0.0.0/0		Visible	1

Cloud Connector - GCP

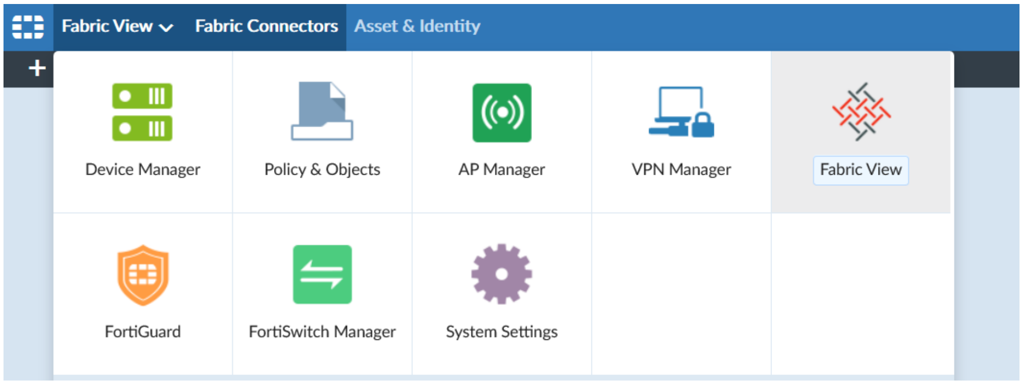
FortiOS 6.2 cloud connector for Google (GCP) can be centrally managed by FortiManager.

Create GCP SDN connector in Policy Packages

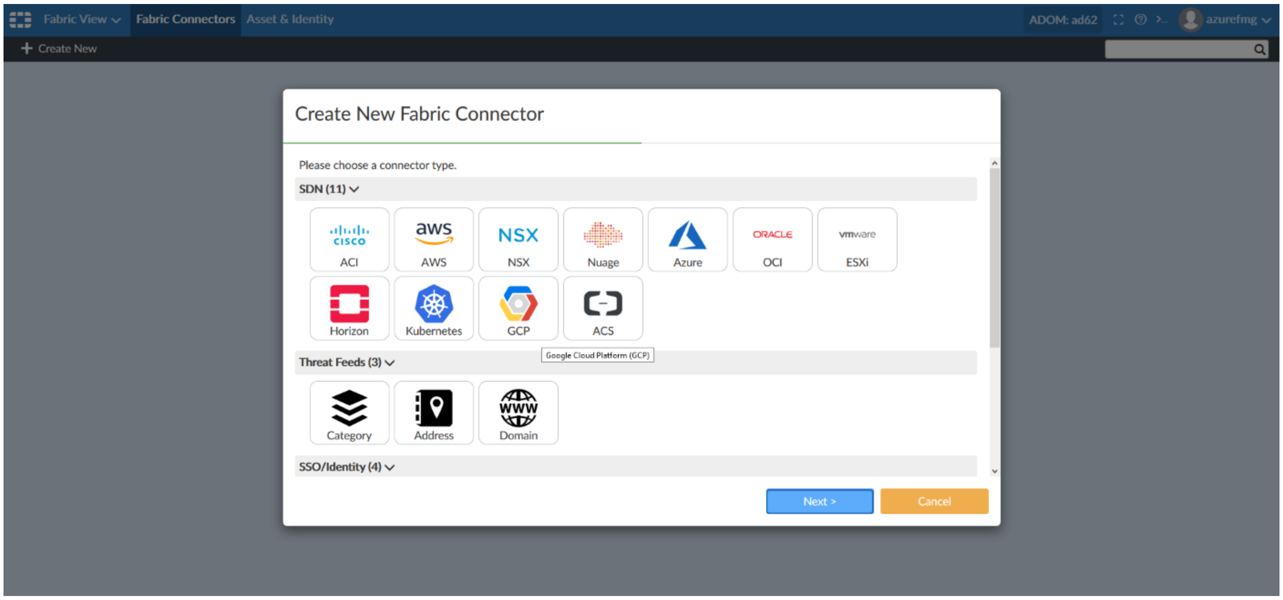
Create the SDN connector in Policy Packages.

To create the SDN connector:

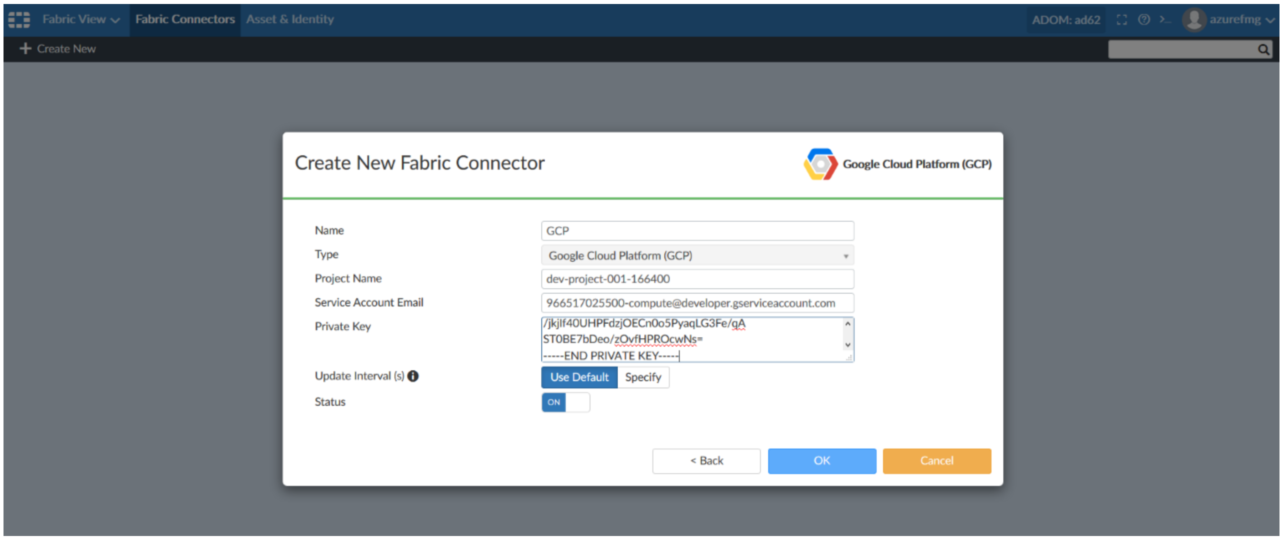
1. Go to *Policy & Objects > Fabric View > Fabric Connectors*.
2. Click *Create New*.



3. Select the *GCP*connector.



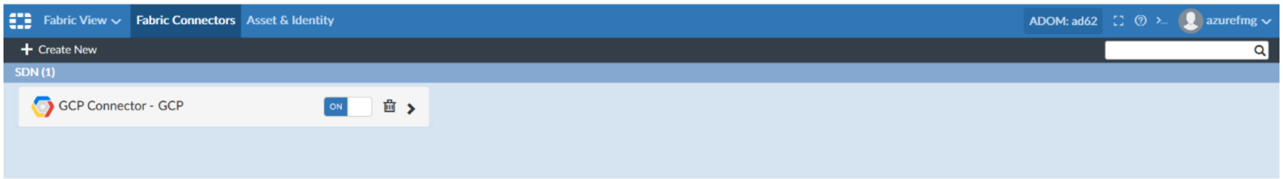
4. Specify the values.



Create New Fabric Connector

Name	GCP
Type	Google Cloud Platform (GCP)
Project Name	dev-project-001-166400
Service Account Email	966517025500-compute@developer.gserviceaccount.com
Private Key	/jkjIf40UHPFdzjOECn0o5PyaqLG3Fe/qA ST0BE7bDeo/zOvfHPROcwNs= -----END PRIVATE KEY-----
Update Interval (s)	Use Default / Specify
Status	ON

5. Click *OK*. The GCP connector is created.

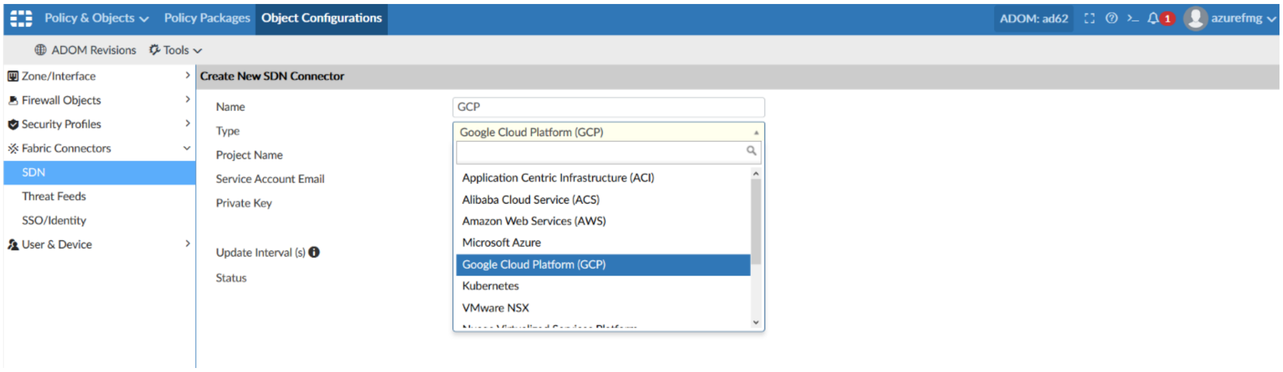


Create GCP connector in Object Configurations

Alternatively, you can create the SDN connector in Object Configurations.

To create the SDN connector:

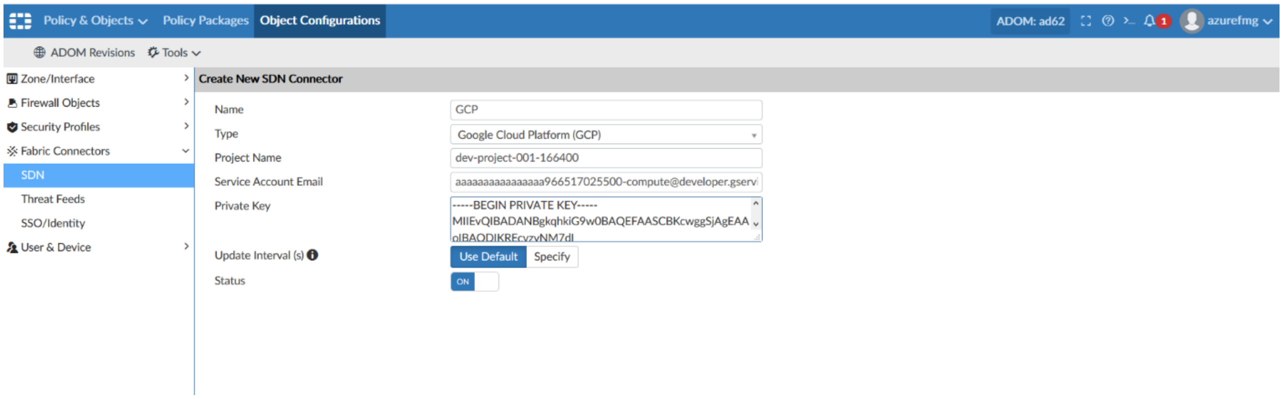
1. Go to *Policy & Objects* > *Object Configuration* > *Fabric Connectors*.
2. Click *SDN Connector* > *GCP* connector.



Create New SDN Connector

Name	GCP
Type	Google Cloud Platform (GCP)
Project Name	
Service Account Email	
Private Key	
Update Interval (s)	
Status	

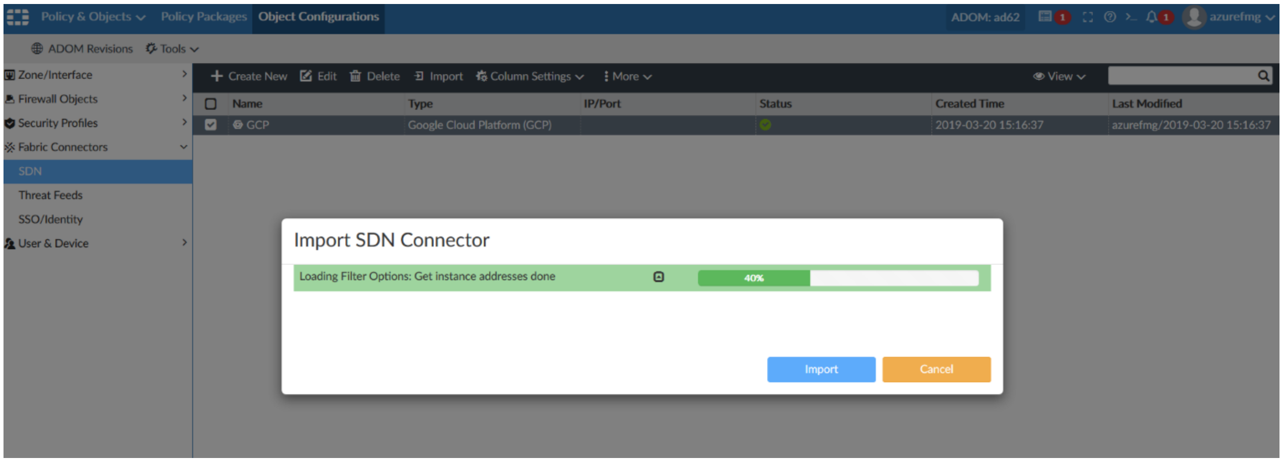
3. Configure the GCP connector information.



Create New SDN Connector

Name	GCP
Type	Google Cloud Platform (GCP)
Project Name	dev-project-001-166400
Service Account Email	aaaaaaaaaaaaaaa966517025500-compute@developer.gserv
Private Key	-----BEGIN PRIVATE KEY----- MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAA oIBAQDIKREcvzvNM7dI
Update Interval (s)	Use Default ● Specify
Status	ON

4. Click the *Import* to import GCP objects. The Import option is only available on *Policy & Objects* > *Object Configurations*.

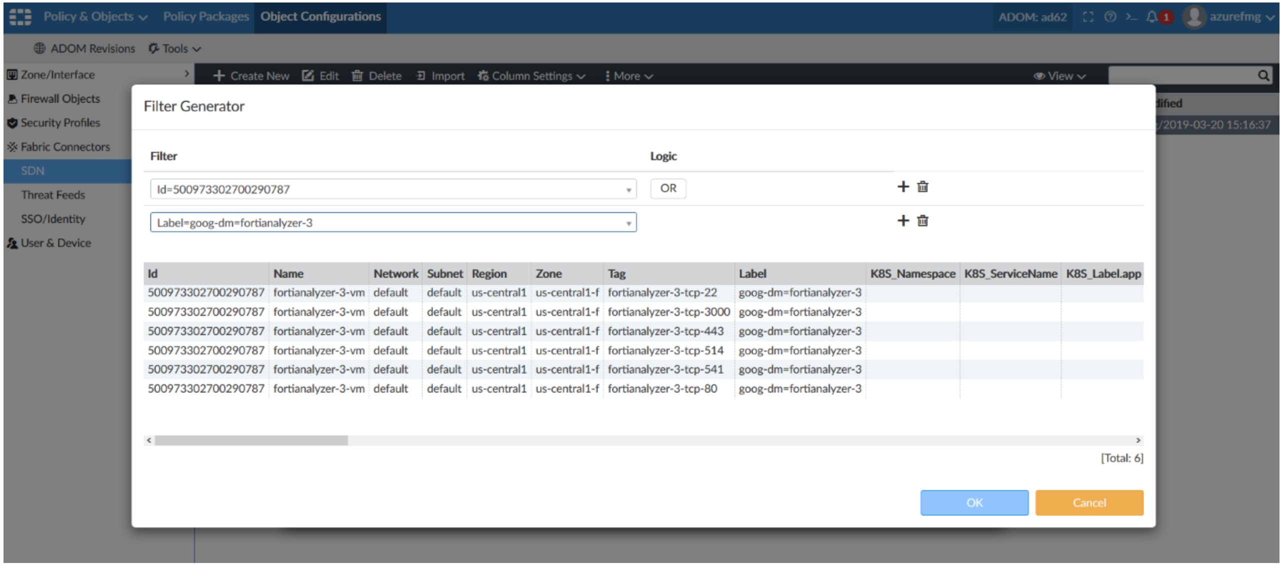


☐	Name	Type	IP/Port	Status	Created Time	Last Modified
☑	GCP	Google Cloud Platform (GCP)		✓	2019-03-20 15:16:37	azurefmg/2019-03-20 15:16:37

Import SDN Connector

Loading Filter Options: Get instance addresses done 40%

5. Add the filter and click *OK* to apply selected filter.



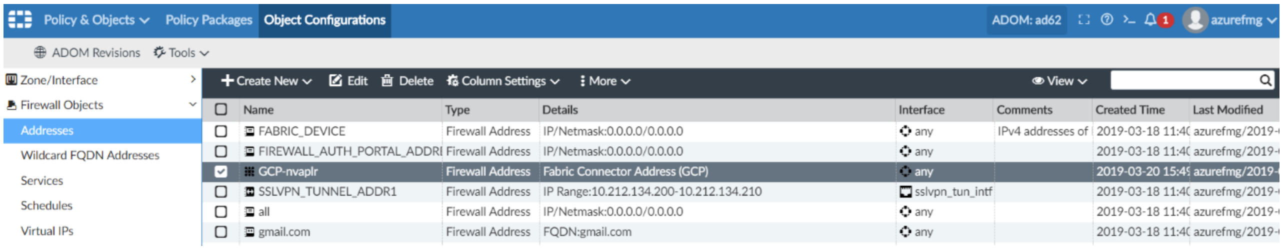
Filter Generator

Filter	Logic
Id=500973302700290787	OR
Label=goog-dm=fortianalyzer-3	

Id	Name	Network	Subnet	Region	Zone	Tag	Label	K8S_Namespace	K8S_ServiceName	K8S_Label.app
500973302700290787	fortianalyzer-3-vm	default	default	us-central1	us-central1-f	fortianalyzer-3-tcp-22	goog-dm=fortianalyzer-3			
500973302700290787	fortianalyzer-3-vm	default	default	us-central1	us-central1-f	fortianalyzer-3-tcp-3000	goog-dm=fortianalyzer-3			
500973302700290787	fortianalyzer-3-vm	default	default	us-central1	us-central1-f	fortianalyzer-3-tcp-443	goog-dm=fortianalyzer-3			
500973302700290787	fortianalyzer-3-vm	default	default	us-central1	us-central1-f	fortianalyzer-3-tcp-514	goog-dm=fortianalyzer-3			
500973302700290787	fortianalyzer-3-vm	default	default	us-central1	us-central1-f	fortianalyzer-3-tcp-541	goog-dm=fortianalyzer-3			
500973302700290787	fortianalyzer-3-vm	default	default	us-central1	us-central1-f	fortianalyzer-3-tcp-80	goog-dm=fortianalyzer-3			

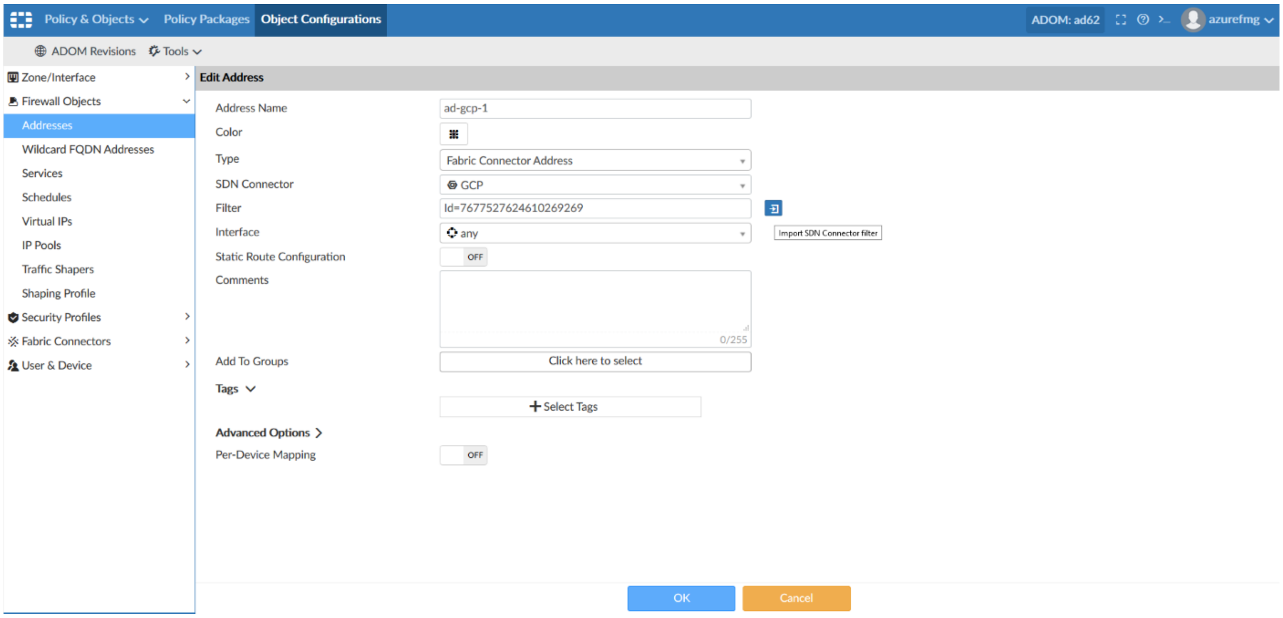
[Total: 6]

6. The new imported GCP address created.



☐	Name	Type	Details	Interface	Comments	Created Time	Last Modified
☐	FABRIC_DEVICE	Firewall Address	IP/Netmask:0.0.0.0/0.0.0.0	any	IPv4 addresses of	2019-03-18 11:4(	azurefmg/2019-
☐	FIREWALL_AUTH_PORTAL_ADDRE	Firewall Address	IP/Netmask:0.0.0.0/0.0.0.0	any		2019-03-18 11:4(	azurefmg/2019-
☑	GCP-nvaplr	Firewall Address	Fabric Connector Address (GCP)	any		2019-03-20 15:4!	azurefmg/2019-
☐	SSLVPN_TUNNEL_ADDR1	Firewall Address	IP Range:10.212.134.200-10.212.134.210	sslvpn_tun_intf		2019-03-18 11:4(	azurefmg/2019-
☐	all	Firewall Address	IP/Netmask:0.0.0.0/0.0.0.0	any		2019-03-18 11:4(	azurefmg/2019-
☐	gmail.com	Firewall Address	FQDN:gmail.com	any		2019-03-18 11:4(	azurefmg/2019-

7. Create a new *Fabric Connector Address*. Import the connector or enter the details of the connector.



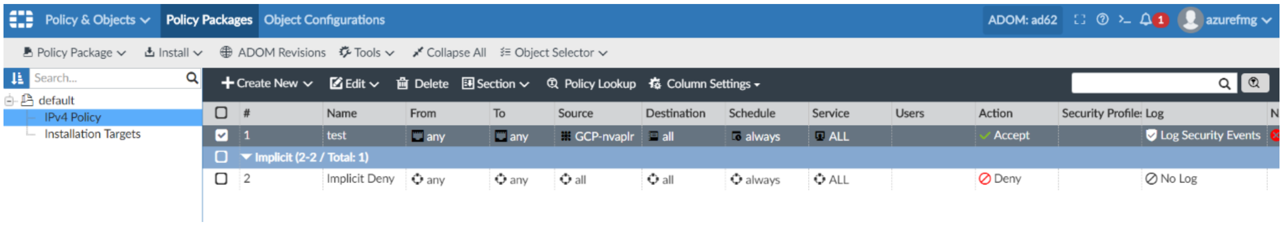
Edit Address

Address Name	ad-gcp-1
Color	
Type	Fabric Connector Address
SDN Connector	GCP
Filter	Id=7677527624610269269
Interface	any
Static Route Configuration	OFF
Comments	0/255
Add To Groups	
Tags	
Advanced Options	
Per-Device Mapping	OFF

Install the SDN connector to FortiGate

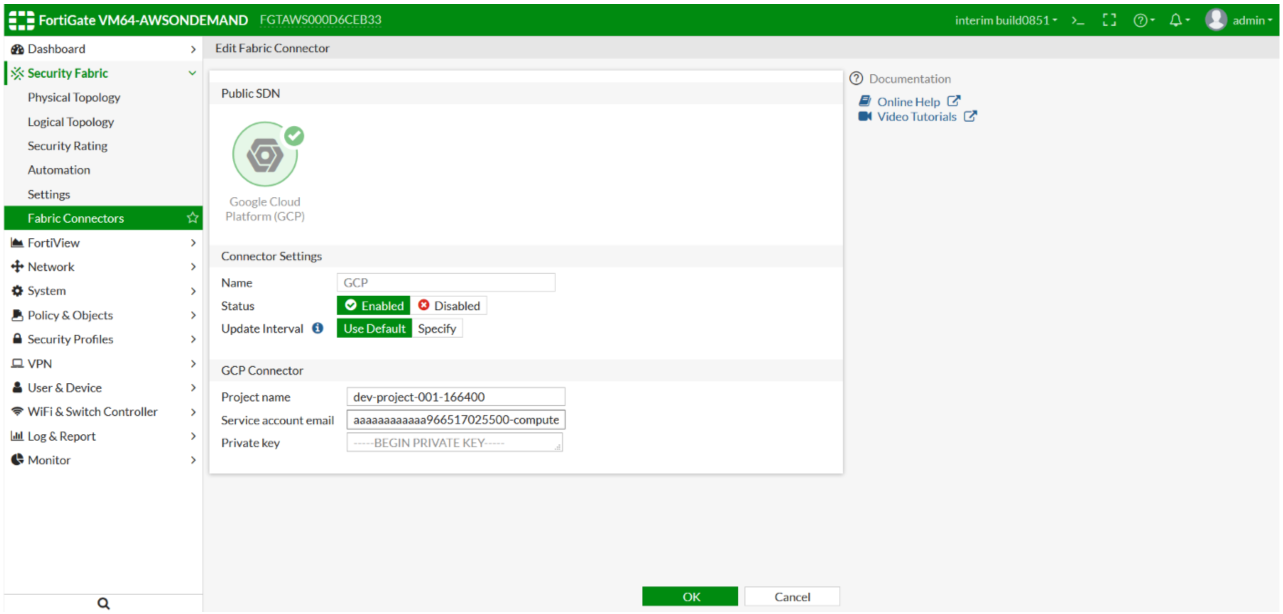
To install the SDN connector to FortiGate:

1. Install GCP SDN connector configuration and imported GCP dynamic object to FortiGate.



☐	#	Name	From	To	Source	Destination	Schedule	Service	Users	Action	Security Profiles	Log
☑	1	test	any	any	GCP-nvaplr	all	always	ALL		✓ Accept		Log Security Events
☐	Implicit (2-2 / Total: 1)											
☐	2	Implicit Deny	any	any	all	all	always	ALL		Deny		No Log

2. Check the FortiGate whether, the GCP connector and address is installed.



Edit Fabric Connector

Public SDN

Connector Settings

Name: GCP

Status: ✓ Enabled | Disabled

Update Interval: Use Default | Specify

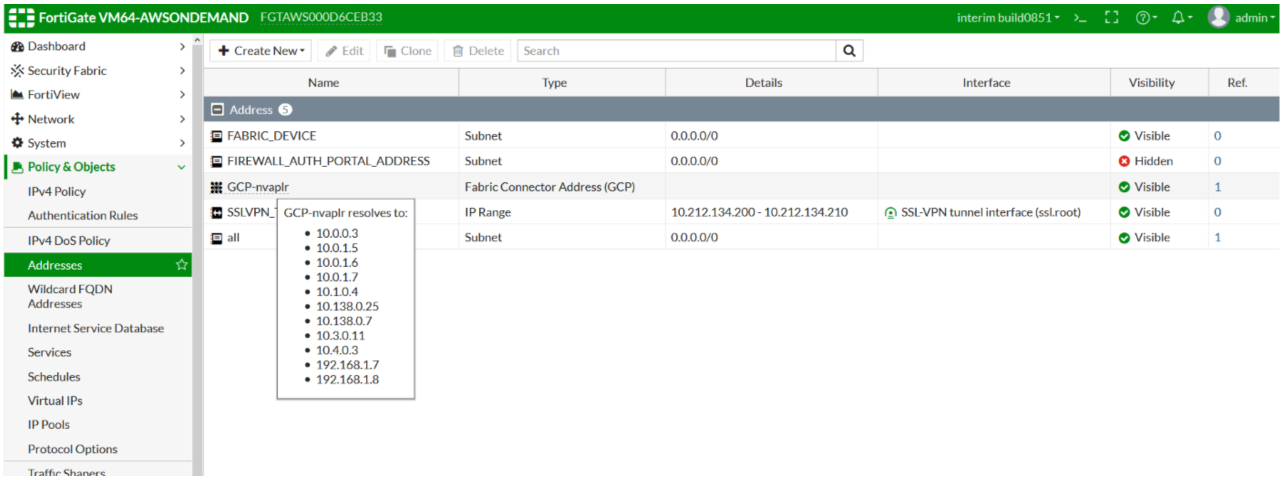
GCP Connector

Project name: dev-project-001-166400

Service account email: aaaaaaaaaaaa966517025500-compute

Private key: -----BEGIN PRIVATE KEY-----

3. The GCP address IP can now be resolved.



Name	Type	Details	Interface	Visibility	Ref.
Address 5					
FABRIC_DEVICE	Subnet	0.0.0.0/0		Visible	0
FIREWALL_AUTH_PORTAL_ADDRESS	Subnet	0.0.0.0/0		Hidden	0
GCP-nvaplr	Fabric Connector Address (GCP)			Visible	1
SSLVPN_	IP Range	10.212.134.200 - 10.212.134.210	SSL-VPN tunnel interface (ssl.root)	Visible	0
all	Subnet	0.0.0.0/0		Visible	1

GCP-nvaplr resolves to:

- 10.0.0.3
- 10.0.1.5
- 10.0.1.6
- 10.0.1.7
- 10.1.0.4
- 10.138.0.25
- 10.138.0.7
- 10.3.0.11
- 10.4.0.3
- 192.168.1.7
- 192.168.1.8

Cloud Connector - ESXi

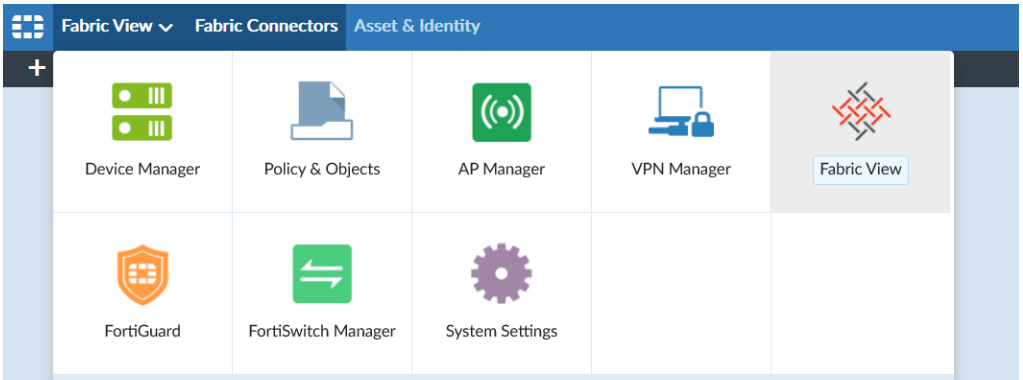
FortiOS 6.2 cloud connector for VMWare (ESXi) can be centrally managed by FortiManager.

Create ESXi SDN connector in Policy Packages

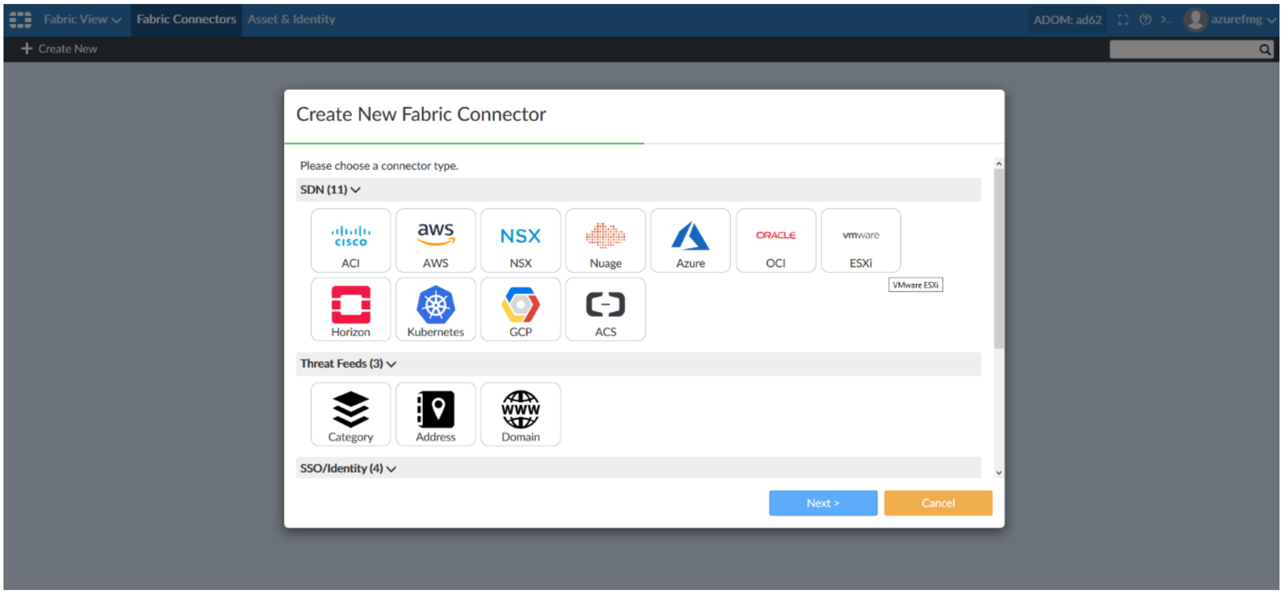
Create the SDN connector in Policy Packages.

To create the SDN connector:

1. Go to *Policy & Objects* > *Fabric View* > *Fabric Connectors*.
2. Click *Create New*.



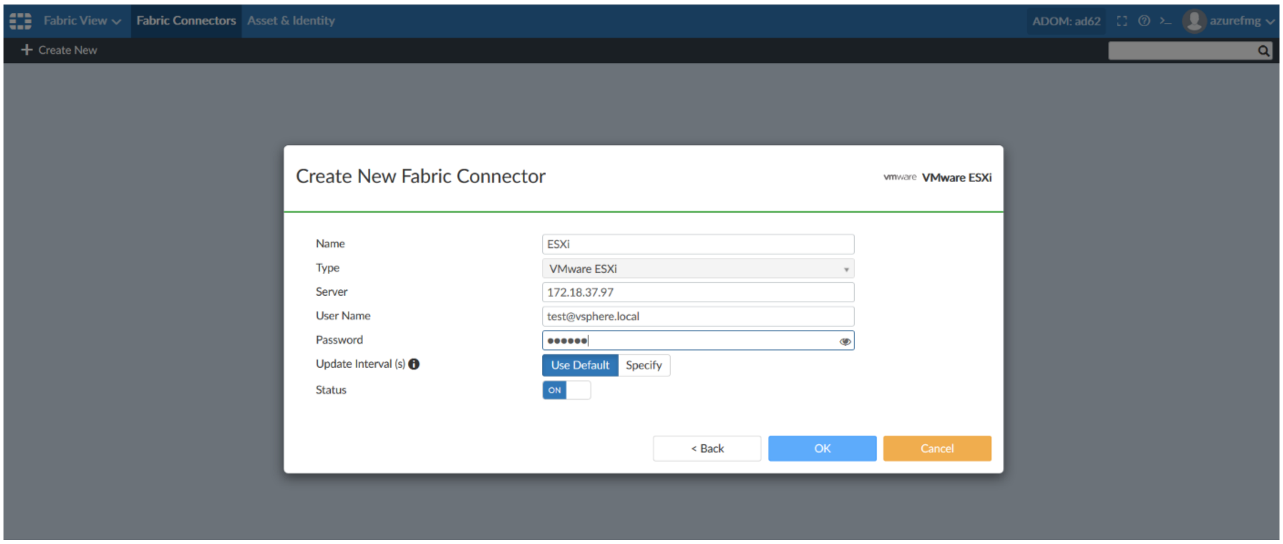
3. Select the *ESXi*connector.



Create New Fabric Connector

Please choose a connector type.

4. Specify the values.



Create New Fabric Connector

Name	ESXi
Type	VMware ESXi
Server	172.18.37.97
User Name	test@vsphere.local
Password	••••••
Update Interval (s)	Use Default / Specify
Status	ON

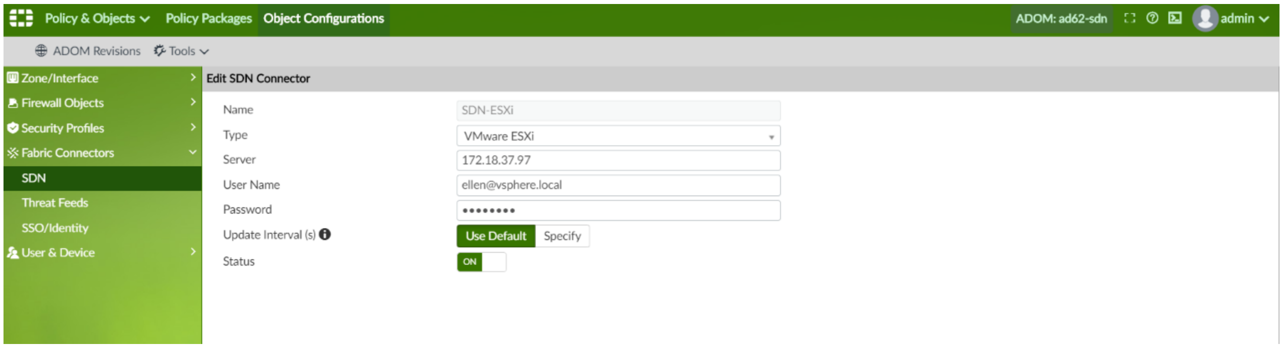
5. Click *OK*. The ESXi connector is created.

Create ESXi connector in Object Configurations

Alternatively, you can create the SDN connector in Object Configurations.

To create the SDN connector:

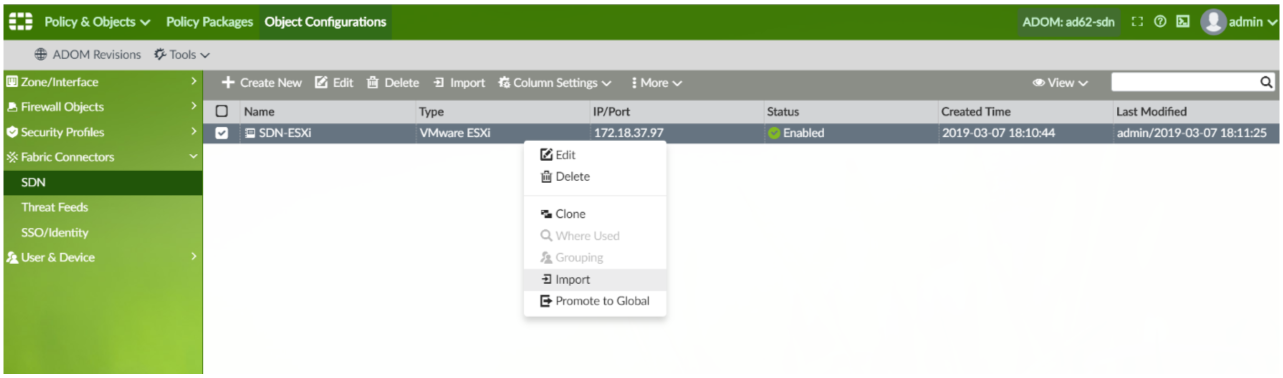
1. Go to *Policy & Objects* > *Object Configuration* > *Fabric Connectors*.
2. Click *SDN Connector* > *ESXi connector*.



Edit SDN Connector

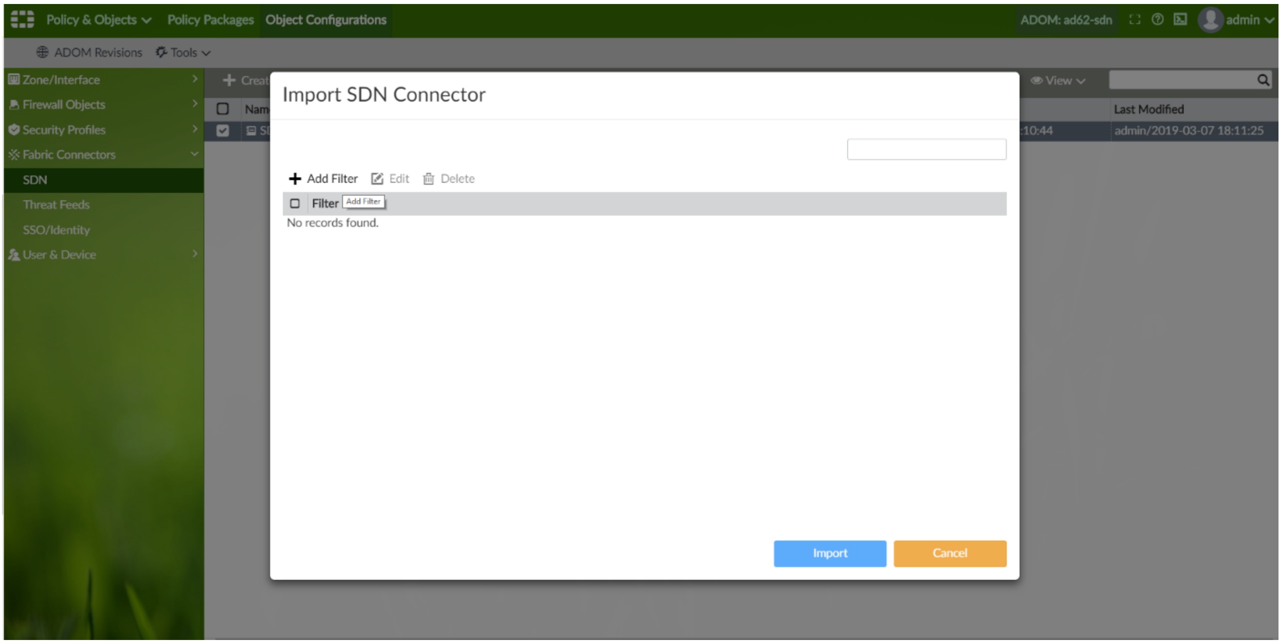
Name	SDN-ESXi
Type	VMware ESXi
Server	172.18.37.97
User Name	ellen@vsphere.local
Password	••••••••
Update Interval (s)	Use Default / Specify
Status	ON

3. Configure the ESXi connector information.



☐	Name	Type	IP/Port	Status	Created Time	Last Modified
☑	SDN-ESXi	VMware ESXi	172.18.37.97	Enabled	2019-03-07 18:10:44	admin/2019-03-07 18:11:25

4. Click the *Import* to import ESXi objects. The Import option is only available on *Policy & Objects* > *Object Configurations*.

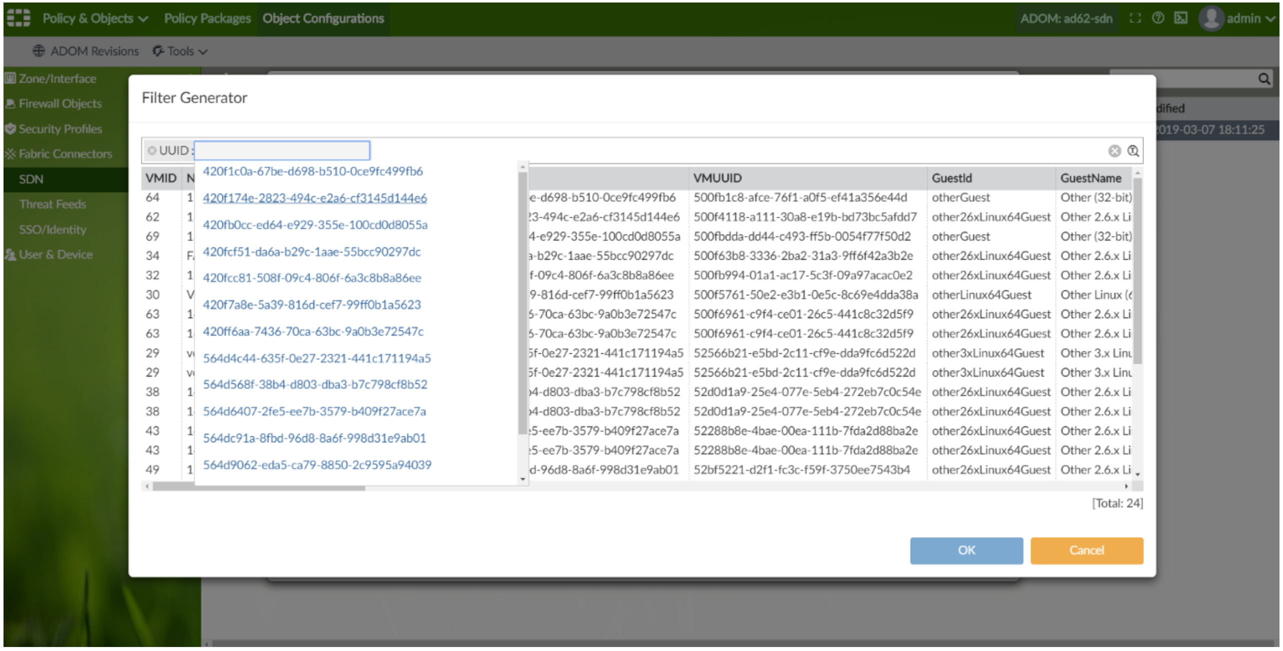


Import SDN Connector

☐ Filter

No records found.

5. Add the filter and click *OK* to apply selected filter.



Filter Generator

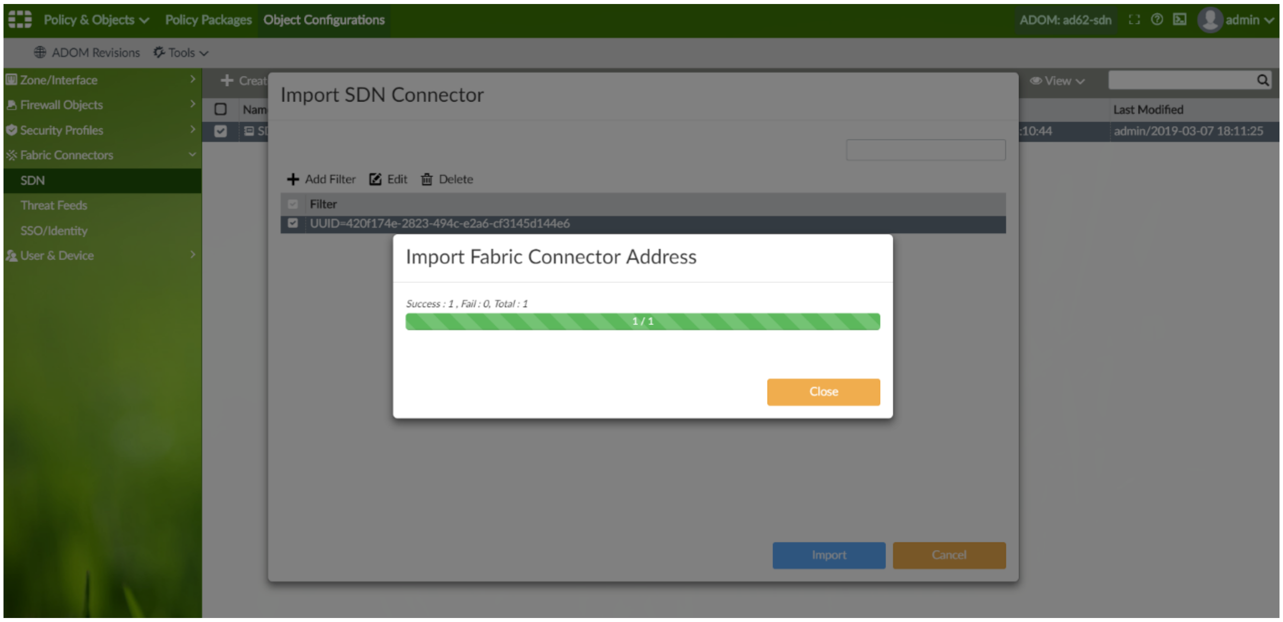
UUID :

420f1c0a-67be-d698-b510-0ce9fc499fb6
420f174e-2823-494c-e2a6-cf3145d144e6
420fb0cc-ed64-e929-355e-100cd0d8055a
420fcf51-da6a-b29c-1aae-55bcc90297dc
420fcc81-508f-09c4-806f-6a3c8b8a86ee
420f7a8e-5a39-816d-cef7-99ff0b1a5623
420ff6aa-7436-70ca-63bc-9a0b3e72547c
564d4c44-635f-0e27-2321-441c171194a5
564d568f-38b4-d803-dba3-b7c798cf8b52
564d6407-2fe5-ee7b-3579-b409f27ace7a
564dc91a-8fbd-96d8-8a6f-998d31e9ab01
564d9062-eda5-ca79-8850-2c9595a94039

VMID	N		VMUUID	GuestId	GuestName
64	1	e-d698-b510-0ce9fc499fb6	500fb1c8-afce-76f1-a0f5-ef41a356e44d	otherGuest	Other (32-bit)
62	1	23-494c-e2a6-cf3145d144e6	500f4118-a111-30a8-e19b-bd73bc5afdd7	other26xLinux64Guest	Other 2.6.x Li
69	1	4-e929-355e-100cd0d8055a	500fbdda-dd44-c493-ff5b-0054f77f50d2	otherGuest	Other (32-bit)
34	F	a-b29c-1aae-55bcc90297dc	500f63b8-3336-2ba2-31a3-9ff6f42a3b2e	other26xLinux64Guest	Other 2.6.x Li
32	1	f-09c4-806f-6a3c8b8a86ee	500fb994-01a1-ac17-5c3f-09a97acac0e2	other26xLinux64Guest	Other 2.6.x Li
30	V	9-816d-cef7-99ff0b1a5623	500f5761-50e2-e3b1-0e5c-8c69e4dda38a	otherLinux64Guest	Other Linux (
63	1	6-70ca-63bc-9a0b3e72547c	500f6961-c9f4-ce01-26c5-441c8c32d5f9	other26xLinux64Guest	Other 2.6.x Li
63	1	6-70ca-63bc-9a0b3e72547c	500f6961-c9f4-ce01-26c5-441c8c32d5f9	other26xLinux64Guest	Other 2.6.x Li
29	v	5f-0e27-2321-441c171194a5	52566b21-e5bd-2c11-cf9e-dda9fc6d522d	other3xLinux64Guest	Other 3.x Linu
29	v	5f-0e27-2321-441c171194a5	52566b21-e5bd-2c11-cf9e-dda9fc6d522d	other3xLinux64Guest	Other 3.x Linu
38	1	04-d803-dba3-b7c798cf8b52	52d0d1a9-25e4-077e-5eb4-272eb7c0c54e	other26xLinux64Guest	Other 2.6.x Li
38	1	04-d803-dba3-b7c798cf8b52	52d0d1a9-25e4-077e-5eb4-272eb7c0c54e	other26xLinux64Guest	Other 2.6.x Li
43	1	e5-ee7b-3579-b409f27ace7a	52288b8e-4bae-00ea-111b-7fda2d88ba2e	other26xLinux64Guest	Other 2.6.x Li
43	1	e5-ee7b-3579-b409f27ace7a	52288b8e-4bae-00ea-111b-7fda2d88ba2e	other26xLinux64Guest	Other 2.6.x Li
49	1	d-96d8-8a6f-998d31e9ab01	52bf5221-d2f1-fc3c-f59f-3750ee7543b4	other26xLinux64Guest	Other 2.6.x Li

[Total: 24]

6. Click *Import*.



Import SDN Connector

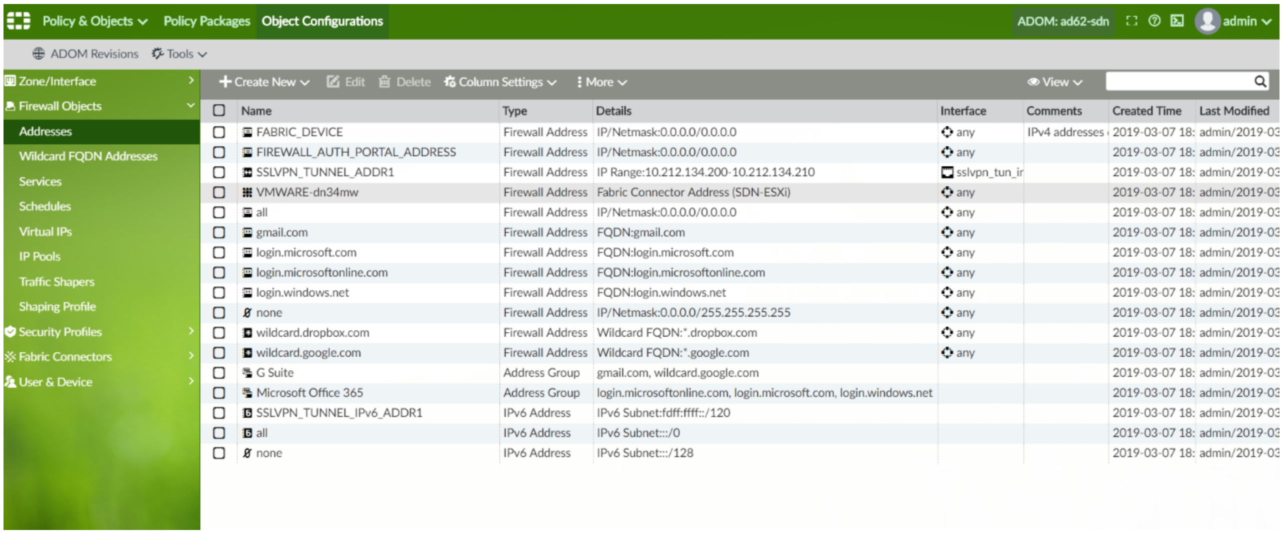
☐	Filter
☑	UUID=420f174e-2823-494c-e2a6-cf3145d144e6

Import Fabric Connector Address

Success : 1 , Fail : 0, Total : 1

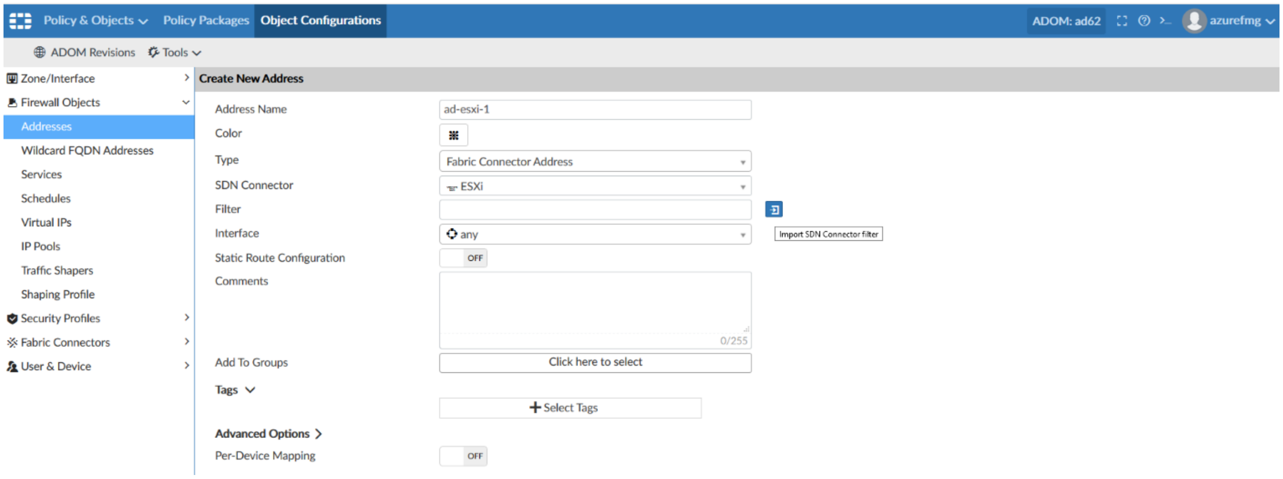
1 / 1

7. The new imported ESXi address created.



□	Name	Type	Details	Interface	Comments	Created Time	Last Modified
□	FABRIC_DEVICE	Firewall Address	IP/Netmask:0.0.0.0/0.0.0.0	any	IPv4 addresses	2019-03-07 18:	admin/2019-03
□	FIREWALL_AUTH_PORTAL_ADDRESS	Firewall Address	IP/Netmask:0.0.0.0/0.0.0.0	any		2019-03-07 18:	admin/2019-03
□	SSLVPN_TUNNEL_ADDR1	Firewall Address	IP Range:10.212.134.200-10.212.134.210	sslvpn_tun_ir		2019-03-07 18:	admin/2019-03
□	VMWARE-dn34mw	Firewall Address	Fabric Connector Address (SDN-ESXi)	any		2019-03-07 18:	admin/2019-03
□	all	Firewall Address	IP/Netmask:0.0.0.0/0.0.0.0	any		2019-03-07 18:	admin/2019-03
□	gmail.com	Firewall Address	FQDN:gmail.com	any		2019-03-07 18:	admin/2019-03
□	login.microsoft.com	Firewall Address	FQDN:login.microsoft.com	any		2019-03-07 18:	admin/2019-03
□	login.microsoftonline.com	Firewall Address	FQDN:login.microsoftonline.com	any		2019-03-07 18:	admin/2019-03
□	login.windows.net	Firewall Address	FQDN:login.windows.net	any		2019-03-07 18:	admin/2019-03
□	none	Firewall Address	IP/Netmask:0.0.0.0/255.255.255.255	any		2019-03-07 18:	admin/2019-03
□	wildcard.dropbox.com	Firewall Address	Wildcard FQDN:*.dropbox.com	any		2019-03-07 18:	admin/2019-03
□	wildcard.google.com	Firewall Address	Wildcard FQDN:*.google.com	any		2019-03-07 18:	admin/2019-03
□	G Suite	Address Group	gmail.com, wildcard.google.com			2019-03-07 18:	admin/2019-03
□	Microsoft Office 365	Address Group	login.microsoftonline.com, login.microsoft.com, login.windows.net			2019-03-07 18:	admin/2019-03
□	SSLVPN_TUNNEL_IPv6_ADDR1	IPv6 Address	IPv6 Subnet:fdff:ffff::/120			2019-03-07 18:	admin/2019-03
□	all	IPv6 Address	IPv6 Subnet:::/0			2019-03-07 18:	admin/2019-03
□	none	IPv6 Address	IPv6 Subnet:::/128			2019-03-07 18:	admin/2019-03

8. Create a new *Fabric Connector Address*. Import the connector or enter the details of the connector.



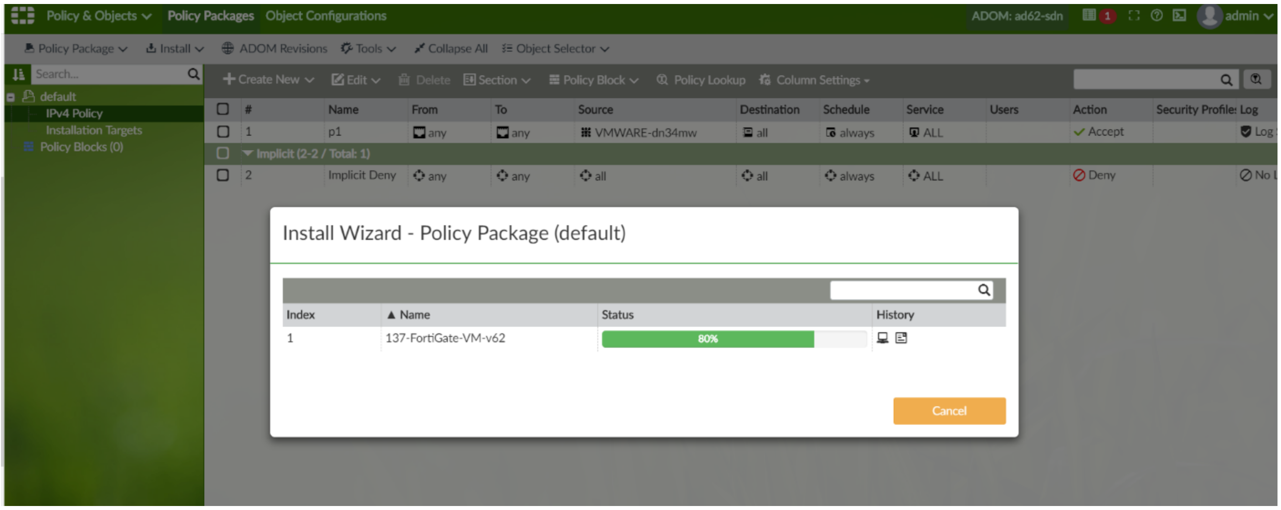
Create New Address

Address Name	ad-esxi-1
Color	
Type	Fabric Connector Address
SDN Connector	ESXi
Filter	
Interface	any
Static Route Configuration	OFF
Comments	0/255
Add To Groups	Click here to select
Tags	Select Tags
Per-Device Mapping	OFF

Install the SDN connector to FortiGate

To install the SDN connector to FortiGate:

1. Install ESXi SDN connector configuration and imported ESXi dynamic object to FortiGate.

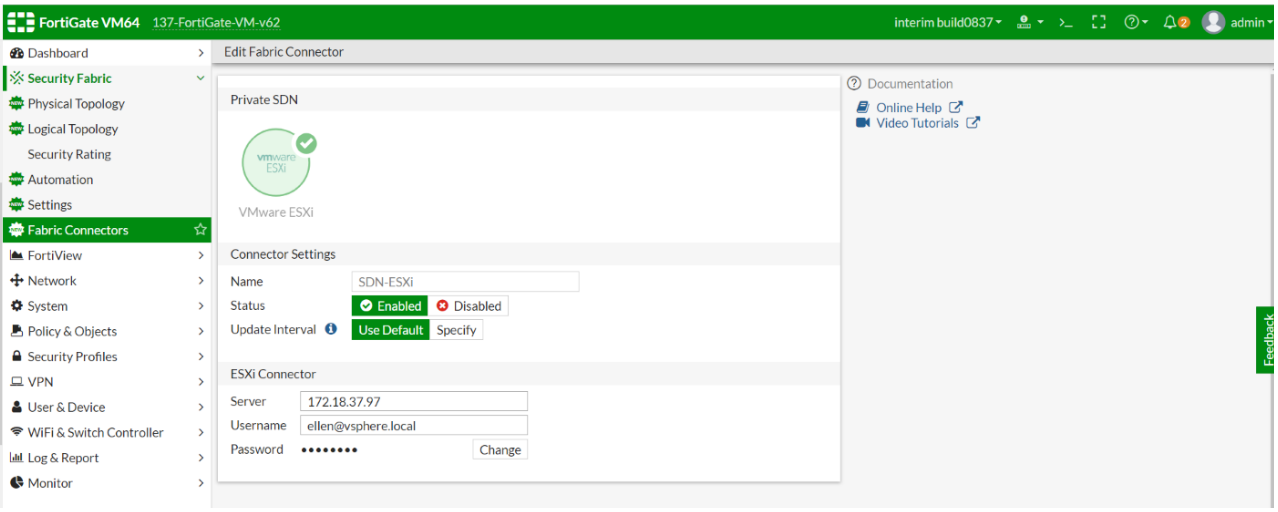


#	Name	From	To	Source	Destination	Schedule	Service	Users	Action	Security Profile:	Log
1	p1	any	any	VMWARE-dn34mw	all	always	ALL		✓ Accept		Log
Implicit (2-2 / Total: 1)											
2	Implicit Deny	any	any	all	all	always	ALL		Deny		No L

Install Wizard - Policy Package (default)

Index	Name	Status	History
1	137-FortiGate-VM-v62	80%	

2. Check the FortiGate whether, the ESXi connector and address is installed.



Edit Fabric Connector

Private SDN

VMware ESXi

Connector Settings

Name: SDN-ESXi

Status: [✓ Enabled] Disabled

Update Interval: [✓ Use Default] Specify

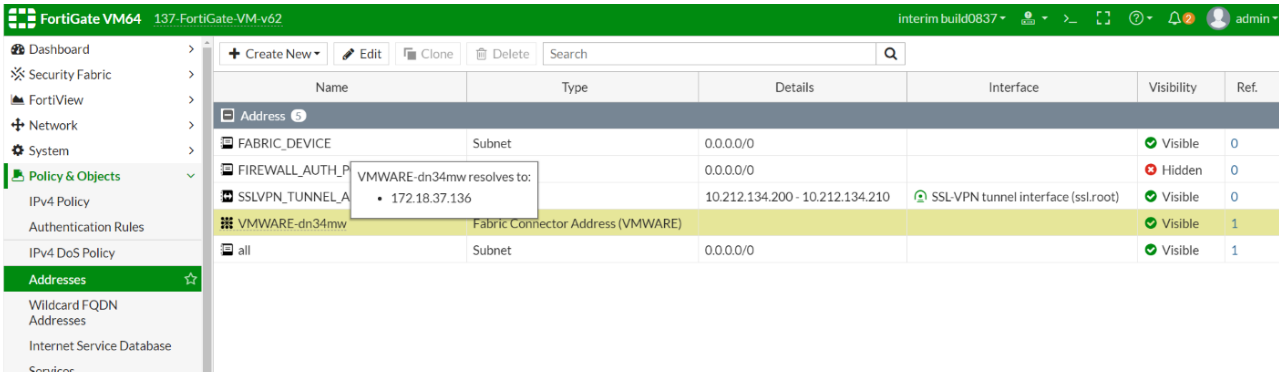
ESXi Connector

Server: 172.18.37.97

Username: ellen@vsphere.local

Password: •••••••• Change

3. The ESXi address IP can now be resolved.



Name	Type	Details	Interface	Visibility	Ref.
Address 5					
FABRIC_DEVICE	Subnet	0.0.0.0/0		✓ Visible	0
FIREWALL_AUTH_P		0.0.0.0/0		Hidden	0
SSLVPN_TUNNEL_A		10.212.134.200 - 10.212.134.210	SSL-VPN tunnel interface (ssl.root)	✓ Visible	0
VMWARE-dn34mw	Fabric Connector Address (VMWARE)			✓ Visible	1
all	Subnet	0.0.0.0/0		✓ Visible	1

VMWARE-dn34mw resolves to:

- 172.18.37.136

Filter IP Addresses from VMWare ESXi

To filter out the IPs from VMware ESXi and vCenter servers, following address filters are introduced:

- vmid
- host
- name
- uuid
- vmuuid
- vmnetwork
- guestid
- guestname
- annotation

SDN Connector - Kubernetes (K8S) (Multiple Clouds)

FortiOS 6.2 cloud connector for Kubernetes can be centrally managed by FortiManager. This includes:

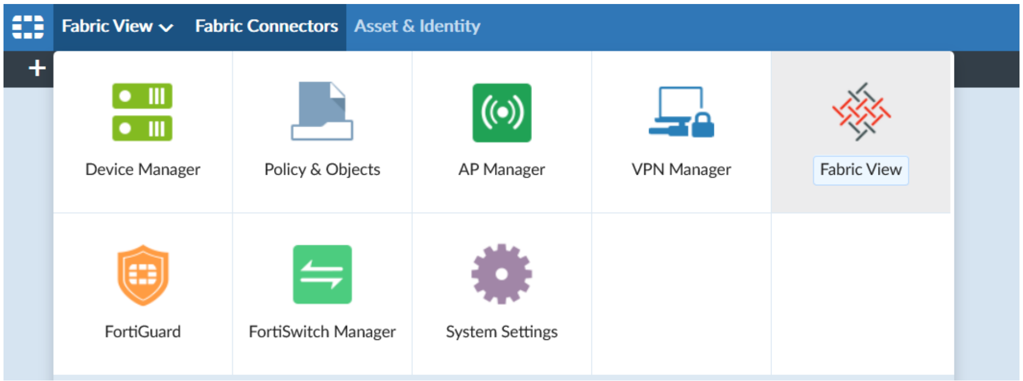
- Private Cloud (K8S)
- AWS (EKS)
- Azure (AKS)
- Google (GKE)
- Oracle (OKE)

Create Kubernetes SDN connector in Policy Packages

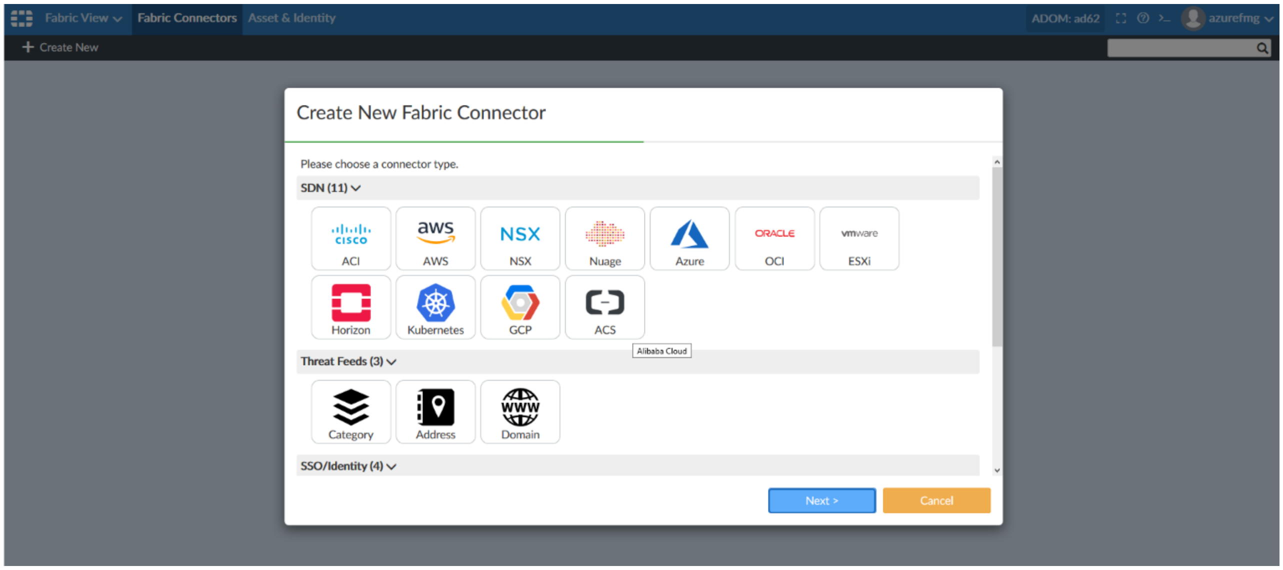
Create the SDN connector in Policy Packages.

To create the SDN connector:

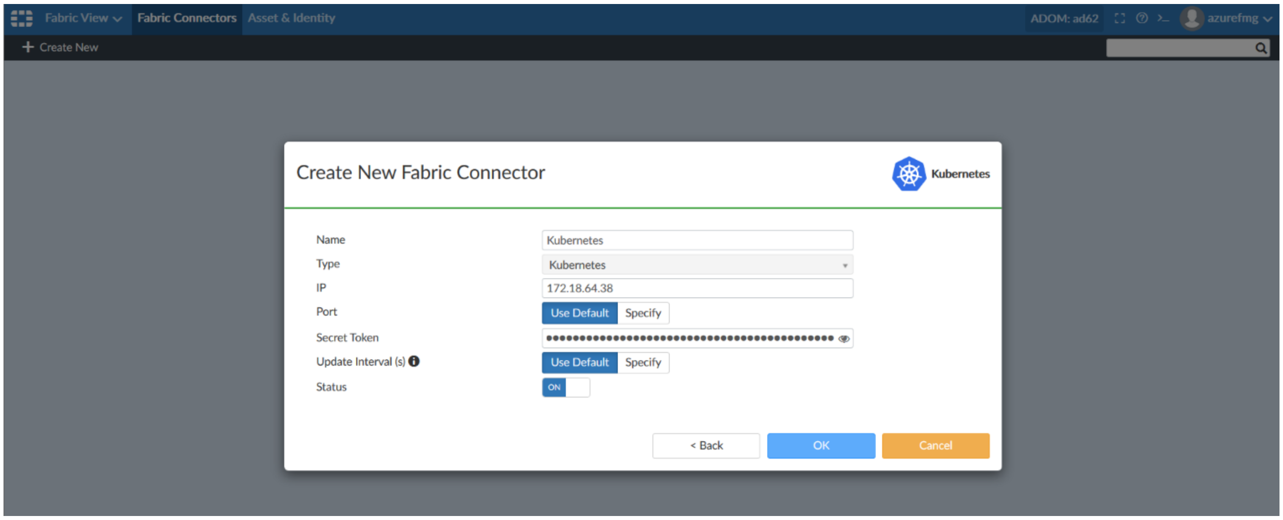
1. Go to *Policy & Objects* > *Fabric View* > *Fabric Connectors*.
2. Click *Create New*.



3. Select the *Kubernetes* connector.



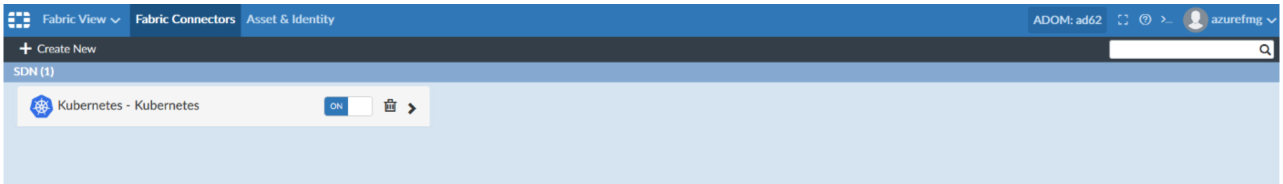
4. Specify the values.



Create New Fabric Connector

Name	Kubernetes
Type	Kubernetes
IP	172.18.64.38
Port	Use Default
Secret Token	••
Update Interval (s)	Use Default
Status	ON

5. Click *OK*. The Kubernetes connector is created.



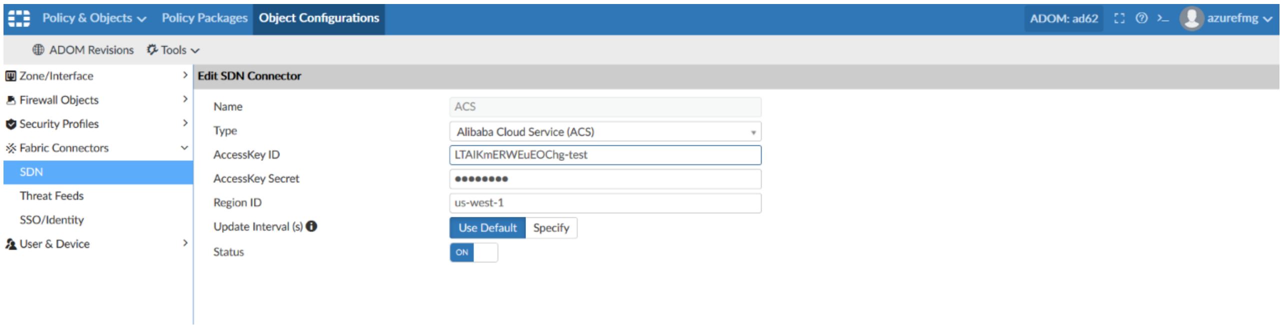
Kubernetes - Kubernetes ON

Create Kubernetes connector in Object Configurations

Alternatively, you can create the SDN connector in Object Configurations.

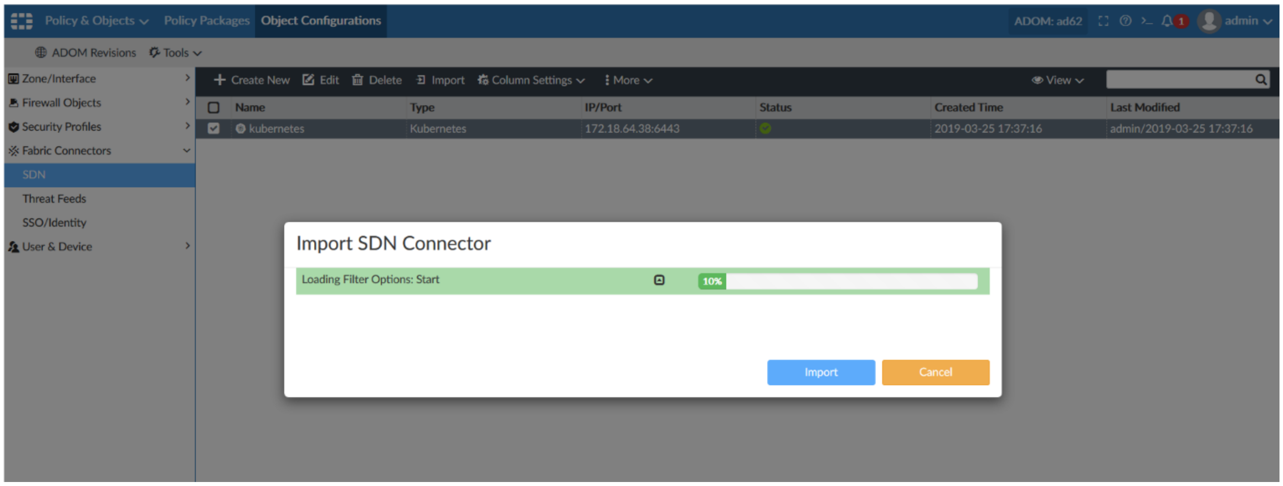
To create the SDN connector:

1. Go to *Policy & Objects* > *Object Configuration* > *Fabric Connectors*.
2. Click *SDN Connector* > *Kubernetes connector*.
3. Configure the Kubernetes connector information.



Name	ACS
Type	Alibaba Cloud Service (ACS)
AccessKey ID	LTAIKmERWEuEOChg-test
AccessKey Secret	••••••••
Region ID	us-west-1
Update Interval (s)	Use Default / Specify
Status	ON

4. Click the *Import* to import Kubernetes objects. The Import option is only available on *Policy & Objects* > *Object Configurations*.

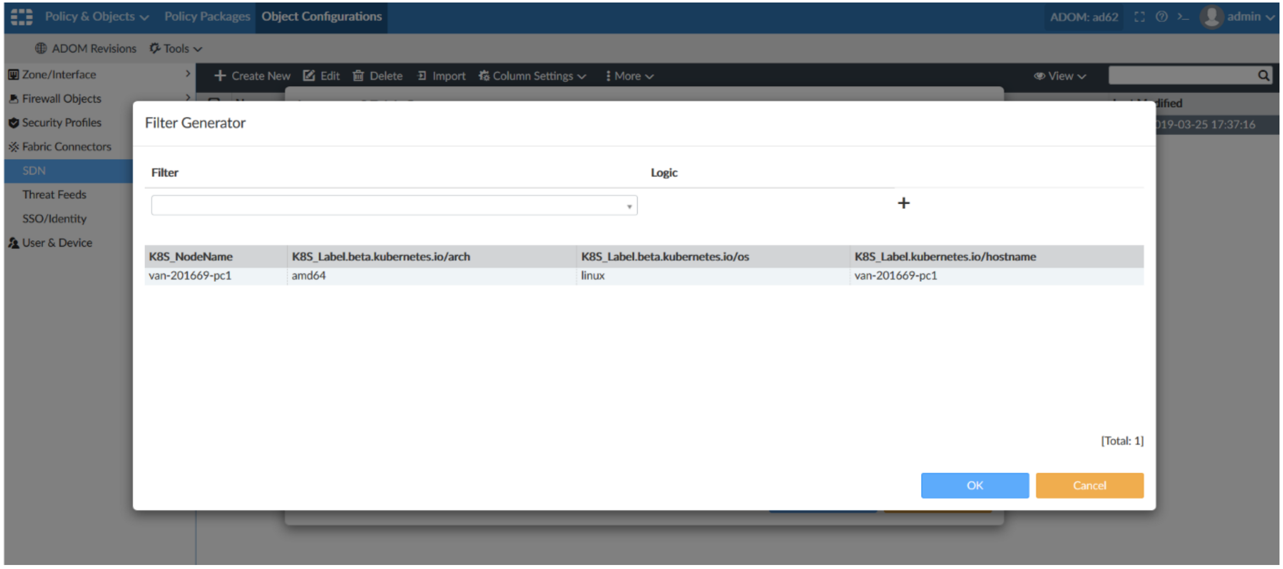


Name	Type	IP/Port	Status	Created Time	Last Modified
kubernetes	Kubernetes	172.18.64.38:6443	●	2019-03-25 17:37:16	admin/2019-03-25 17:37:16

Import SDN Connector

Loading Filter Options: Start 10%

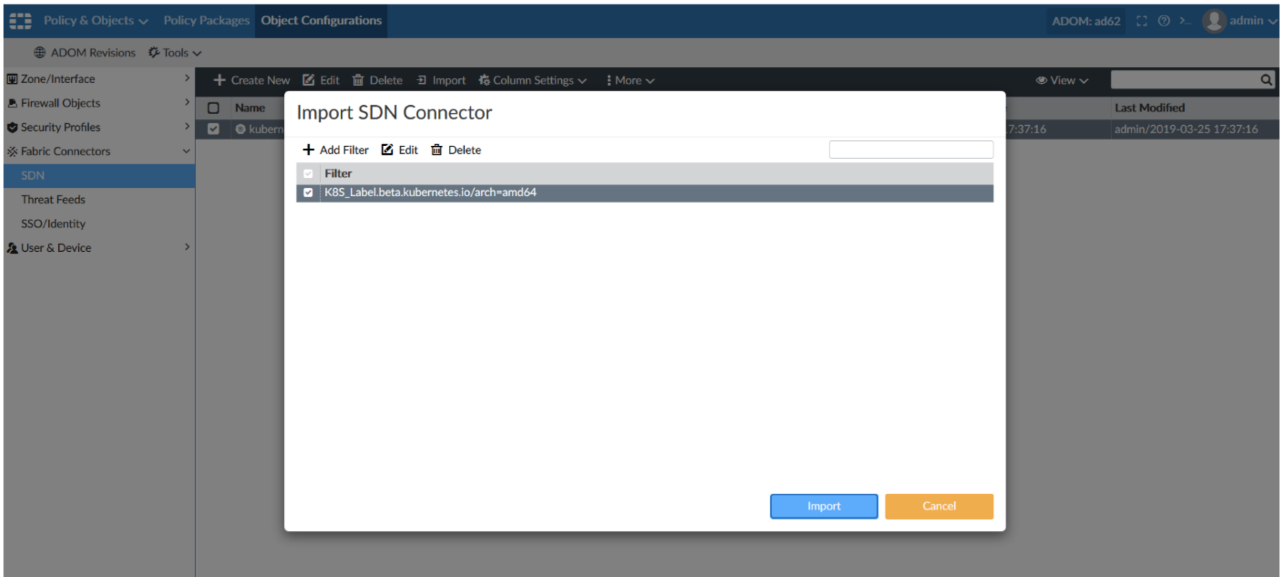
5. Add the filter and click *OK* to apply selected filter.



K8S_NodeName	K8S_Label.beta.kubernetes.io/arch	K8S_Label.beta.kubernetes.io/os	K8S_Label.kubernetes.io/hostname
van-201669-pc1	amd64	linux	van-201669-pc1

[Total: 1]

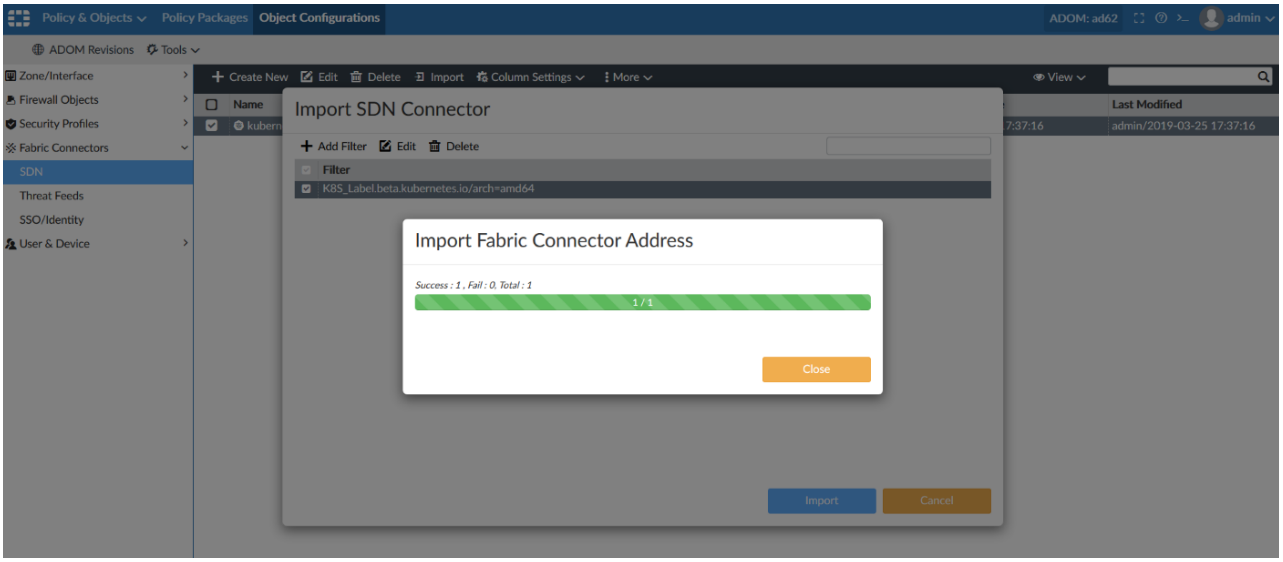
6. Click *Import*. Select the SDN connector.



Import SDN Connector

Filter
☑ K8S_Label.beta.kubernetes.io/arch=amd64

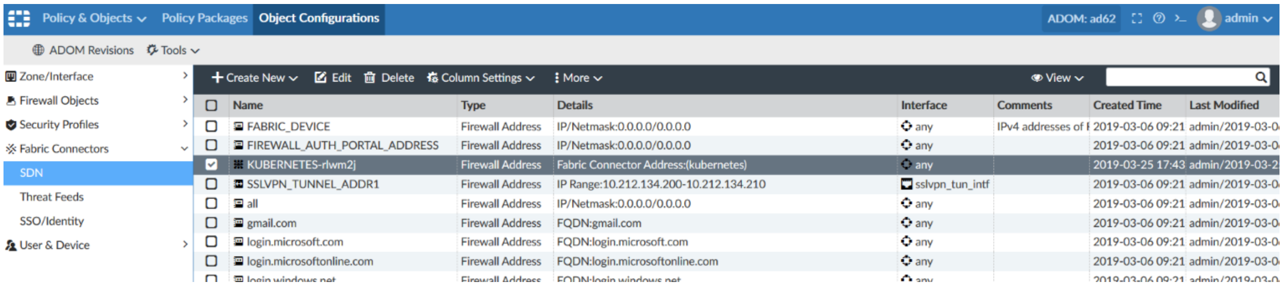
7. Click *Import*.



Import Fabric Connector Address

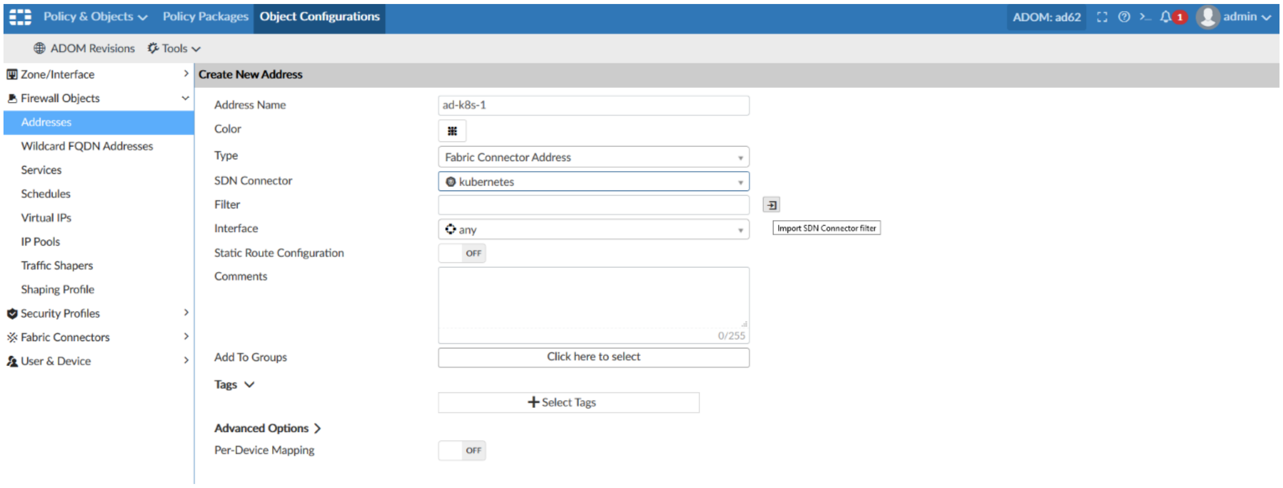
Success : 1 , Fail : 0, Total : 1

8. The new imported Kubernetes address created.



☐	Name	Type	Details	Interface	Comments	Created Time	Last Modified
☐	FABRIC_DEVICE	Firewall Address	IP/Netmask:0.0.0.0/0.0.0.0	any	IPv4 addresses of F	2019-03-06 09:21	admin/2019-03-0
☐	FIREWALL_AUTH_PORTAL_ADDRESS	Firewall Address	IP/Netmask:0.0.0.0/0.0.0.0	any		2019-03-06 09:21	admin/2019-03-0
☑	KUBERNETES-rlwm2j	Firewall Address	Fabric Connector Address:(kubernetes)	any		2019-03-25 17:43	admin/2019-03-2
☐	SSLVPN_TUNNEL_ADDR1	Firewall Address	IP Range:10.212.134.200-10.212.134.210	sslvpn_tun_intf		2019-03-06 09:21	admin/2019-03-0
☐	all	Firewall Address	IP/Netmask:0.0.0.0/0.0.0.0	any		2019-03-06 09:21	admin/2019-03-0
☐	gmail.com	Firewall Address	FQDN:gmail.com	any		2019-03-06 09:21	admin/2019-03-0
☐	login.microsoft.com	Firewall Address	FQDN:login.microsoft.com	any		2019-03-06 09:21	admin/2019-03-0
☐	login.microsoftonline.com	Firewall Address	FQDN:login.microsoftonline.com	any		2019-03-06 09:21	admin/2019-03-0
☐	login.windows.net	Firewall Address	FQDN:login.windows.net	any		2019-03-06 09:21	admin/2019-03-0

9. Create a new *Fabric Connector Address*. Import the connector or enter the details of the connector.



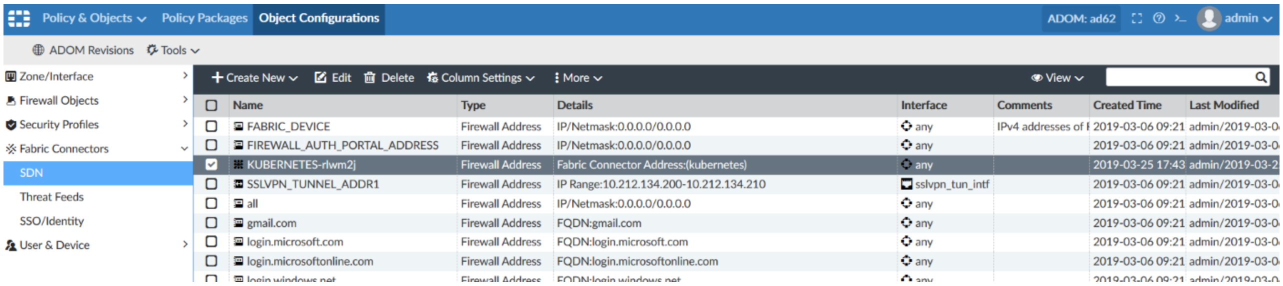
Create New Address

Address Name	ad-k8s-1
Color	
Type	Fabric Connector Address
SDN Connector	kubernetes
Filter	
Interface	any
Static Route Configuration	OFF
Comments	0/255
Add To Groups	Click here to select
Tags	+ Select Tags
Advanced Options	
Per-Device Mapping	OFF

Install the SDN connector to FortiGate

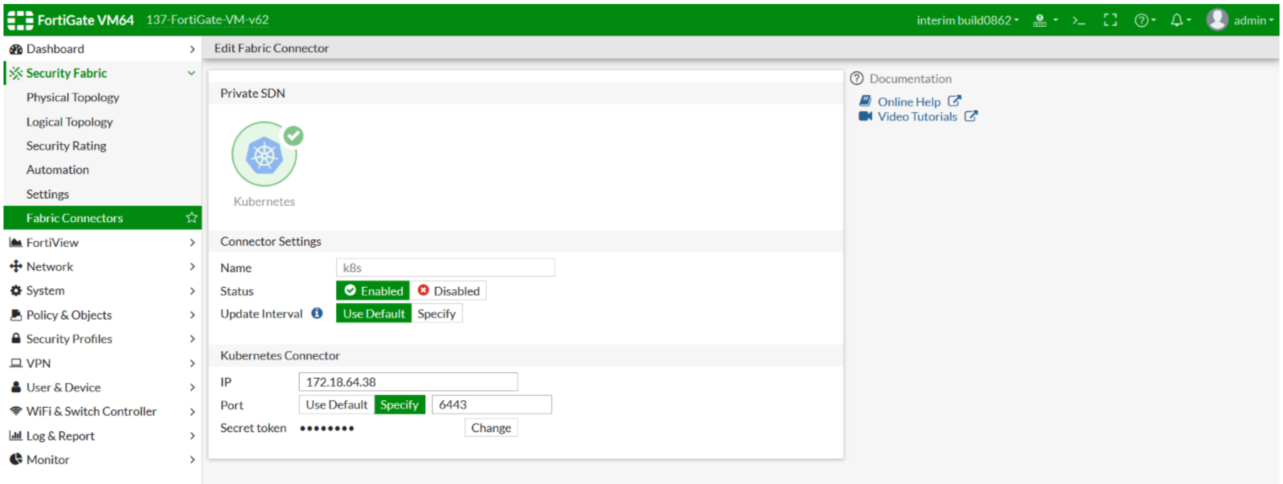
To install the SDN connector to FortiGate:

1. Install Kubernetes SDN connector configuration and imported Kubernetes dynamic object to FortiGate.



☐	Name	Type	Details	Interface	Comments	Created Time	Last Modified
☐	FABRIC_DEVICE	Firewall Address	IP/Netmask:0.0.0.0/0.0.0.0	any	IPv4 addresses of I	2019-03-06 09:21	admin/2019-03-0
☐	FIREWALL_AUTH_PORTAL_ADDRESS	Firewall Address	IP/Netmask:0.0.0.0/0.0.0.0	any		2019-03-06 09:21	admin/2019-03-0
☑	KUBERNETES-rlwm2j	Firewall Address	Fabric Connector Address:(kubernetes)	any		2019-03-25 17:43	admin/2019-03-2
☐	SSLVPN_TUNNEL_ADDR1	Firewall Address	IP Range:10.212.134.200-10.212.134.210	sslvpn_tun_intf		2019-03-06 09:21	admin/2019-03-0
☐	all	Firewall Address	IP/Netmask:0.0.0.0/0.0.0.0	any		2019-03-06 09:21	admin/2019-03-0
☐	gmail.com	Firewall Address	FQDN:gmail.com	any		2019-03-06 09:21	admin/2019-03-0
☐	login.microsoft.com	Firewall Address	FQDN:login.microsoft.com	any		2019-03-06 09:21	admin/2019-03-0
☐	login.microsoftonline.com	Firewall Address	FQDN:login.microsoftonline.com	any		2019-03-06 09:21	admin/2019-03-0
☐	login.windows.net	Firewall Address	FQDN:login.windows.net	any		2019-03-06 09:21	admin/2019-03-0

2. Check the FortiGate whether, the Kubernetes connector and address is installed.



Edit Fabric Connector

Private SDN

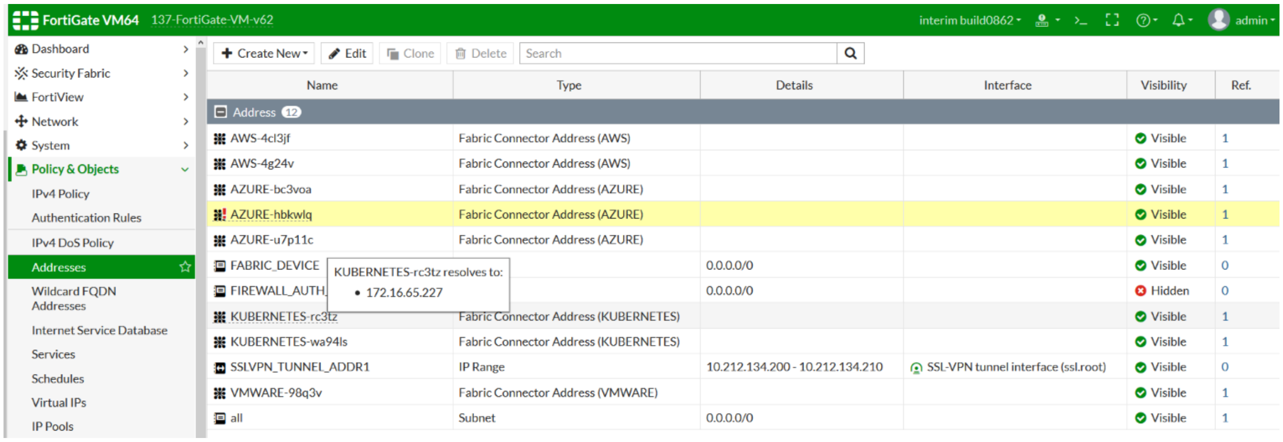
Connector Settings

Name	k8s
Status	Enabled ✓ / Disabled
Update Interval	Use Default ✓ / Specify

Kubernetes Connector

IP	172.18.64.38
Port	Use Default / Specify ✓ 6443
Secret token	•••••••• Change

3. The Kubernetes IP can now be resolved.

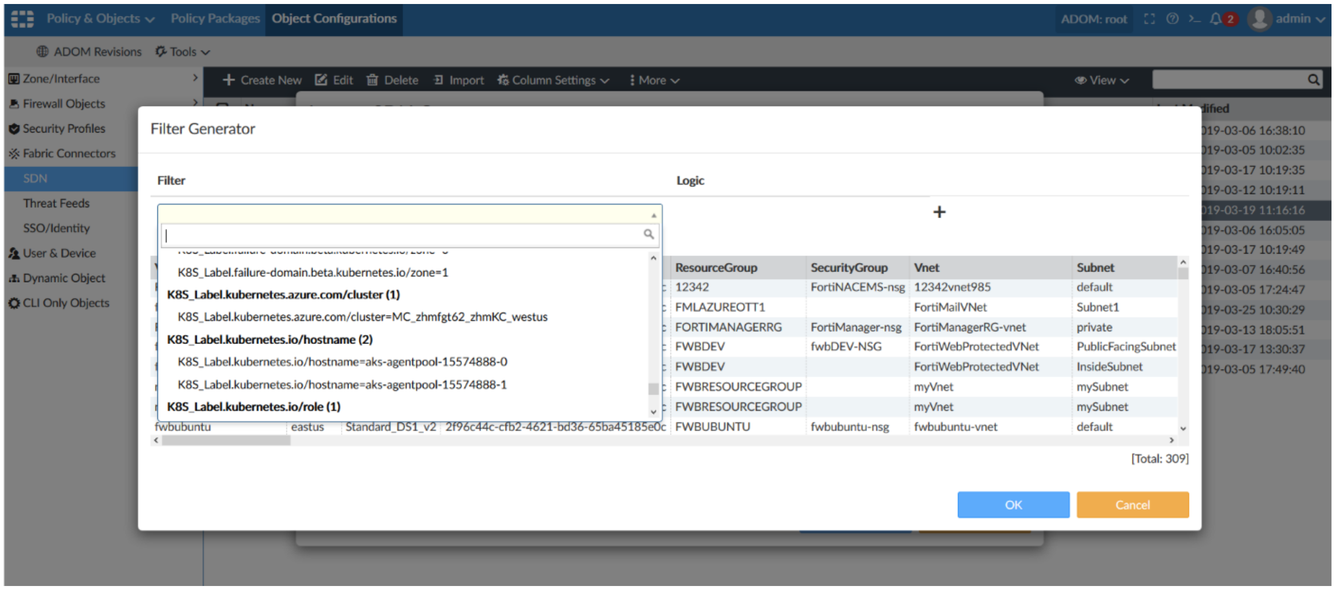


Name	Type	Details	Interface	Visibility	Ref.
Address 12					
AWS-4cl3jf	Fabric Connector Address (AWS)			Visible	1
AWS-4g24v	Fabric Connector Address (AWS)			Visible	1
AZURE-bc3voa	Fabric Connector Address (AZURE)			Visible	1
AZURE-hbkwlq	Fabric Connector Address (AZURE)			Visible	1
AZURE-u7p11c	Fabric Connector Address (AZURE)			Visible	1
FABRIC_DEVICE		0.0.0.0/0		Visible	0
FIREWALL_AUTH		0.0.0.0/0		Hidden	0
KUBERNETES-rc3tz	Fabric Connector Address (KUBERNETES)			Visible	1
KUBERNETES-wa94ls	Fabric Connector Address (KUBERNETES)			Visible	1
SSLVPN_TUNNEL_ADDR1	IP Range	10.212.134.200 - 10.212.134.210	SSL-VPN tunnel interface (ssl.root)	Visible	0
VMWARE-98q3v	Fabric Connector Address (VMWARE)			Visible	1
all	Subnet	0.0.0.0/0		Visible	1

KUBERNETES-rc3tz resolves to:

- 172.16.65.227

SDN Connector for Kubernetes for Azure



Filter Generator

Filter | Logic

K8S_Label.failure-domain.beta.kubernetes.io/zone=1

K8S_Label.kubernetes.azure.com/cluster (1)

K8S_Label.kubernetes.azure.com/cluster=MC_zhmfgt62_zhmKC_westus

K8S_Label.kubernetes.io/hostname (2)

K8S_Label.kubernetes.io/hostname=aks-agentpool-15574888-0

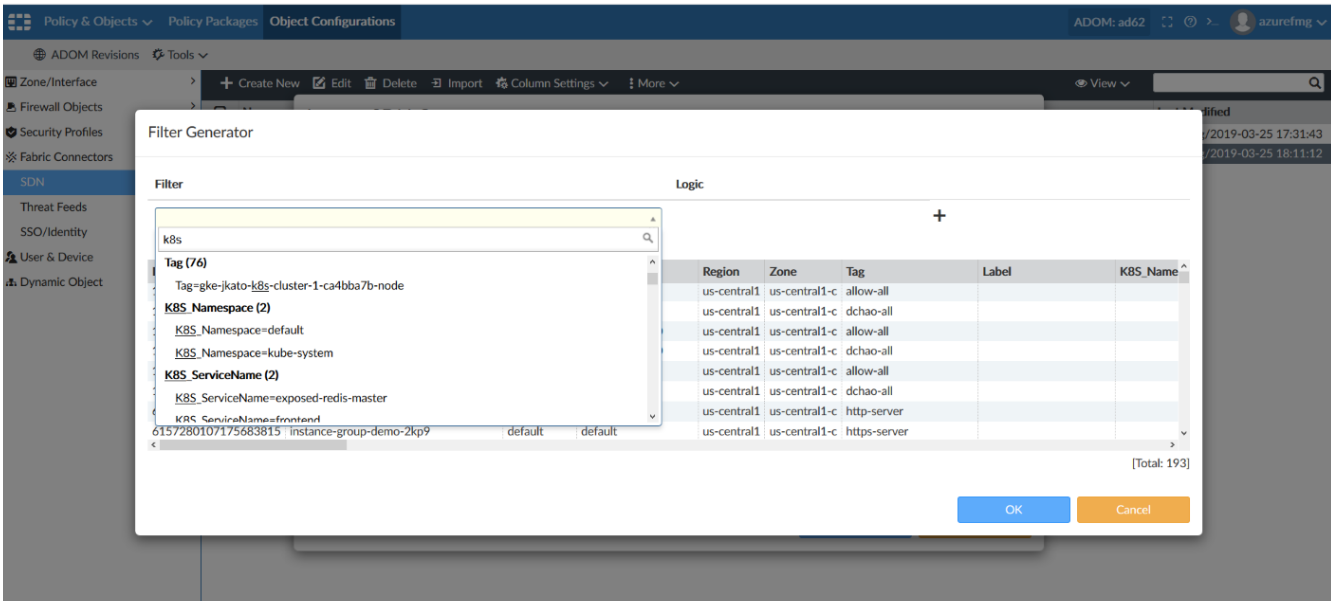
K8S_Label.kubernetes.io/hostname=aks-agentpool-15574888-1

K8S_Label.kubernetes.io/role (1)

				ResourceGroup	SecurityGroup	Vnet	Subnet
				12342	FortiNACEMS-nsg	12342vnet985	default
				FMLAZUREOTT1		FortiMailVNet	Subnet1
				FORTIMANAGERRG	FortiManager-nsg	FortiManagerRG-vnet	private
				FWBDEV	fwbDEV-NSG	FortiWebProtectedVNet	PublicFacingSubnet
				FWBDEV		FortiWebProtectedVNet	InsideSubnet
				FWBRESOURCEGROUP		myVnet	mySubnet
				FWBRESOURCEGROUP		myVnet	mySubnet
fwbubuntu	eastus	Standard_DS1_v2	2f96c44c-cfb2-4621-bd36-65ba45185e0c	FWBUBUNTU	fwbubuntu-nsg	fwbubuntu-vnet	default

[Total: 309]

SDN Connector for Kubernetes for GCP



k8s

Tag (76)

Tag=gke-jkato-k8s-cluster-1-ca4bba7b-node

K8S_Namespace (2)

K8S_Namespace=default

K8S_Namespace=kube-system

K8S_ServiceName (2)

K8S_ServiceName=exposed-redis-master

K8S_ServiceName=frontend

Region	Zone	Tag	Label	K8S_Name
us-central1	us-central1-c	allow-all		
us-central1	us-central1-c	dchao-all		
us-central1	us-central1-c	allow-all		
us-central1	us-central1-c	dchao-all		
us-central1	us-central1-c	allow-all		
us-central1	us-central1-c	dchao-all		
us-central1	us-central1-c	http-server		
us-central1	us-central1-c	https-server		

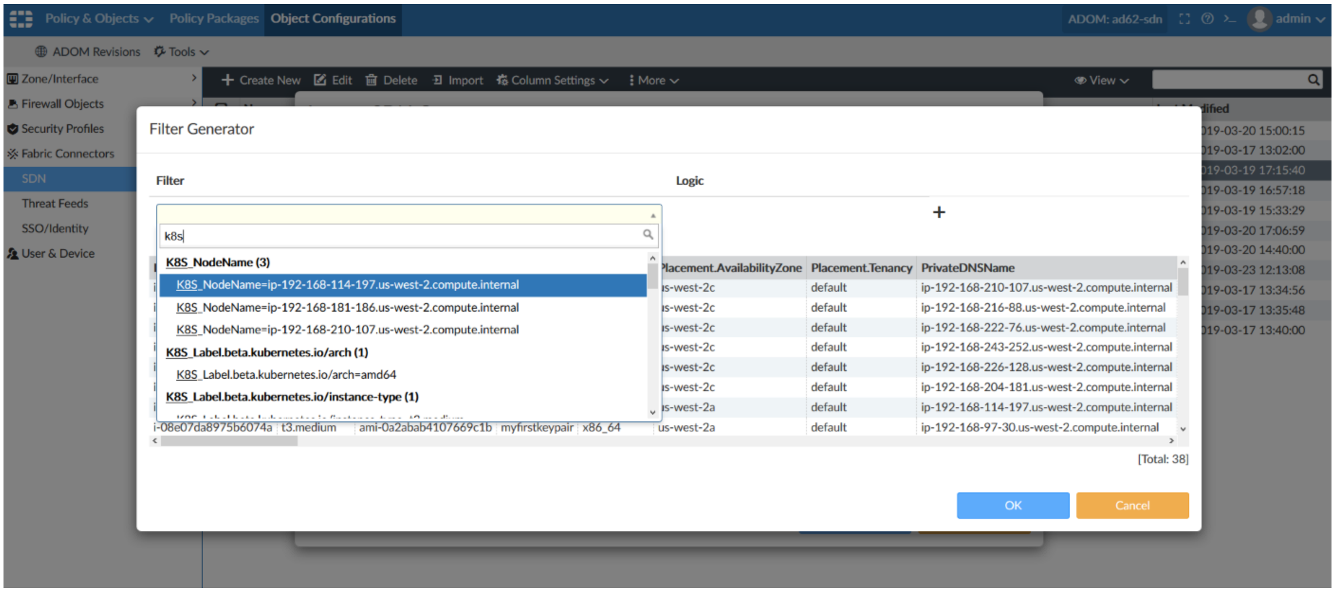
6157280107175683815 instance-group-demo-2kp9 default default

[Total: 193]

/2019-03-25 17:31:43

/2019-03-25 18:11:12

SDN Connector for Kubernetes for AWS



k8s

K8S_NodeName (3)

K8S_NodeName=ip-192-168-114-197.us-west-2.compute.internal

K8S_NodeName=ip-192-168-181-186.us-west-2.compute.internal

K8S_NodeName=ip-192-168-210-107.us-west-2.compute.internal

K8S_Label.beta.kubernetes.io/arch (1)

K8S_Label.beta.kubernetes.io/arch=amd64

K8S_Label.beta.kubernetes.io/instance-type (1)

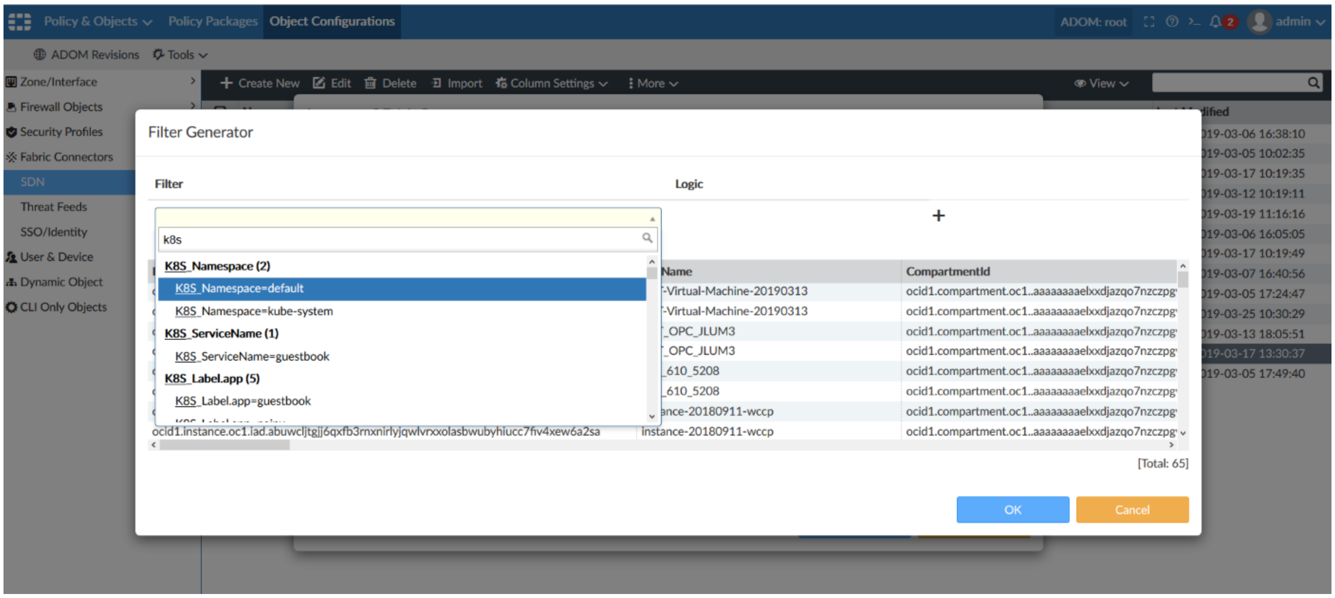
Placement.AvailabilityZone	Placement.Tenancy	PrivateDNSName
us-west-2c	default	ip-192-168-210-107.us-west-2.compute.internal
us-west-2c	default	ip-192-168-216-88.us-west-2.compute.internal
us-west-2c	default	ip-192-168-222-76.us-west-2.compute.internal
us-west-2c	default	ip-192-168-243-252.us-west-2.compute.internal
us-west-2c	default	ip-192-168-226-128.us-west-2.compute.internal
us-west-2c	default	ip-192-168-204-181.us-west-2.compute.internal
us-west-2a	default	ip-192-168-114-197.us-west-2.compute.internal
us-west-2a	default	ip-192-168-97-30.us-west-2.compute.internal

i-08e07da8975b6074a t3.medium ami-0a2abab4107669c1b myfirstkeypair x86_64

[Total: 38]

019-03-20 15:00:15
019-03-17 13:02:00
019-03-19 17:15:40
019-03-19 16:57:18
019-03-19 15:33:29
019-03-20 17:06:59
019-03-20 14:40:00
019-03-23 12:13:08
019-03-17 13:34:56
019-03-17 13:35:48
019-03-17 13:40:00

SDN Connector for Kubernetes for Oracle OCI



k8s

K8S_Namespace (2)
- K8S_Namespace=default
- K8S_Namespace=kube-system

K8S_ServiceName (1)
- K8S_ServiceName=guestbook

K8S_Label.app (5)
- K8S_Label.app=guestbook

Name	CompartmentId
-Virtual-Machine-20190313	ocid1.compartment.oc1..aaaaaaaaelxxdjazqo7nzczpg
-Virtual-Machine-20190313	ocid1.compartment.oc1..aaaaaaaaelxxdjazqo7nzczpg
_OPC_JLUM3	ocid1.compartment.oc1..aaaaaaaaelxxdjazqo7nzczpg
_OPC_JLUM3	ocid1.compartment.oc1..aaaaaaaaelxxdjazqo7nzczpg
_610_5208	ocid1.compartment.oc1..aaaaaaaaelxxdjazqo7nzczpg
_610_5208	ocid1.compartment.oc1..aaaaaaaaelxxdjazqo7nzczpg
ance-20180911-wccp	ocid1.compartment.oc1..aaaaaaaaelxxdjazqo7nzczpg
instance-20180911-wccp	ocid1.compartment.oc1..aaaaaaaaelxxdjazqo7nzczpg

ocid1.instance.oc1.iad.abuwcljtgjj6qxfb3rnxnirlyjqwlvrxxolasbwubyhiucc7fiv4xew6a2sa

[Total: 65]

Cloud Connector - AliCloud

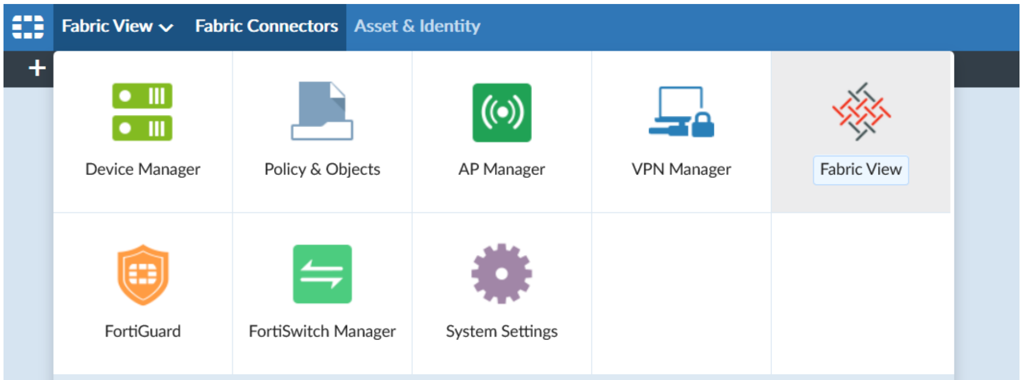
FortiOS 6.2 cloud connector for AliCloud (ACS) can be centrally managed by FortiManager.

Create ACS SDN connector in Policy Packages

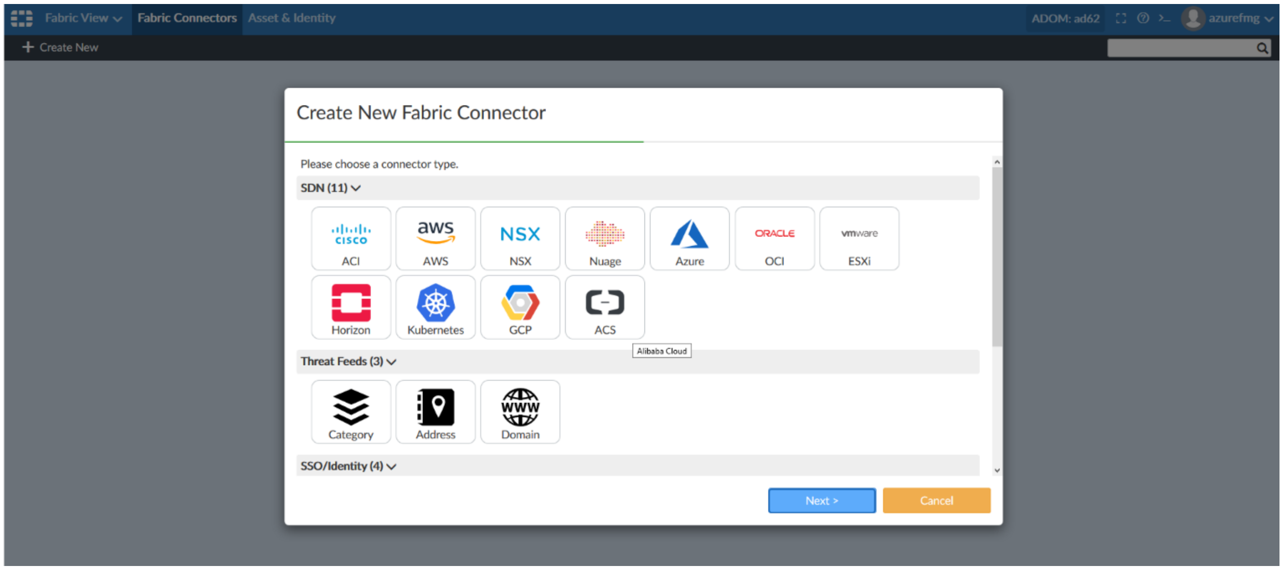
Create the SDN connector in Policy Packages.

To create the SDN connector:

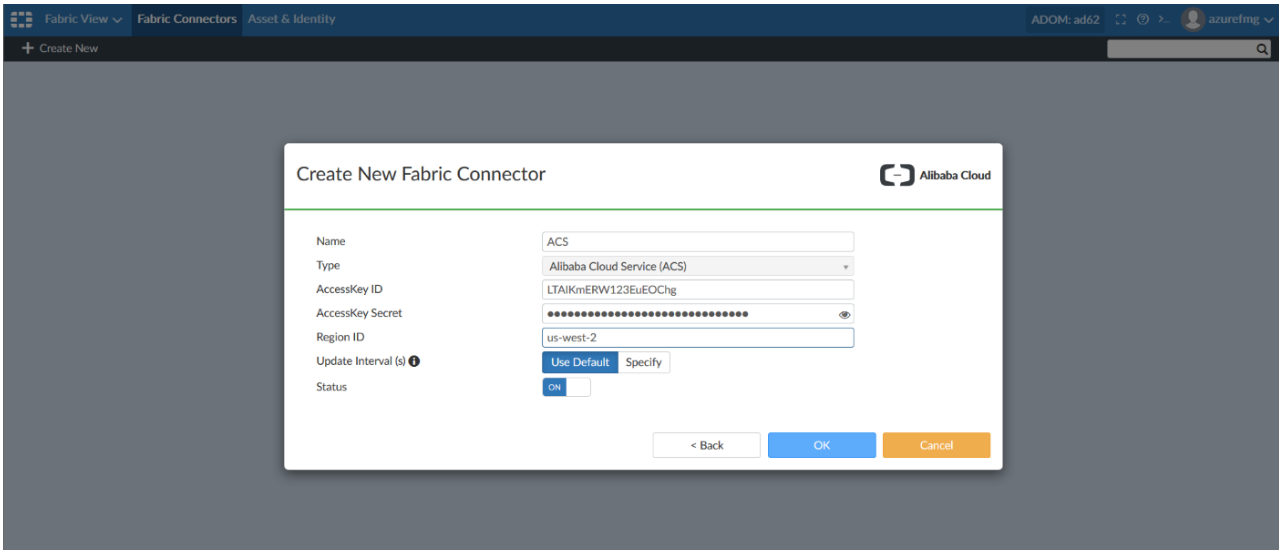
1. Go to *Policy & Objects > Fabric View > Fabric Connectors*.
2. Click *Create New*.



3. Select the *ACS*connector.



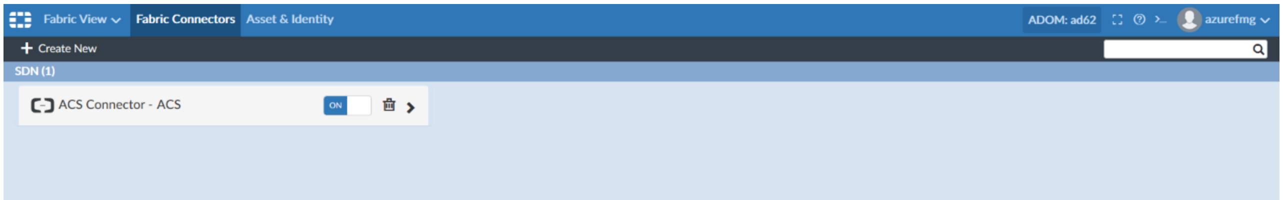
4. Specify the values.



Create New Fabric Connector

Name	ACS
Type	Alibaba Cloud Service (ACS)
AccessKey ID	LTAIKmERW123EuEOChg
AccessKey Secret	●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●
Region ID	us-west-2
Update Interval (s)	Use Default Specify
Status	ON

5. Click *OK*. The ACS connector is created.

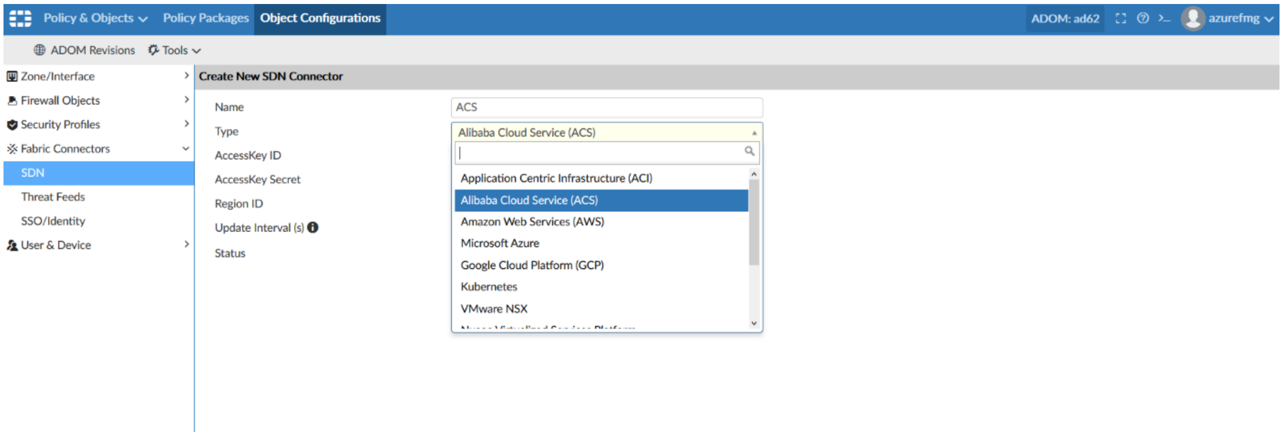


Create ACS connector in Object Configurations

Alternatively, you can create the SDN connector in Object Configurations.

To create the SDN connector:

1. Go to *Policy & Objects* > *Object Configuration* > *Fabric Connectors*.
2. Click *SDN Connector* > *ACS connector*.

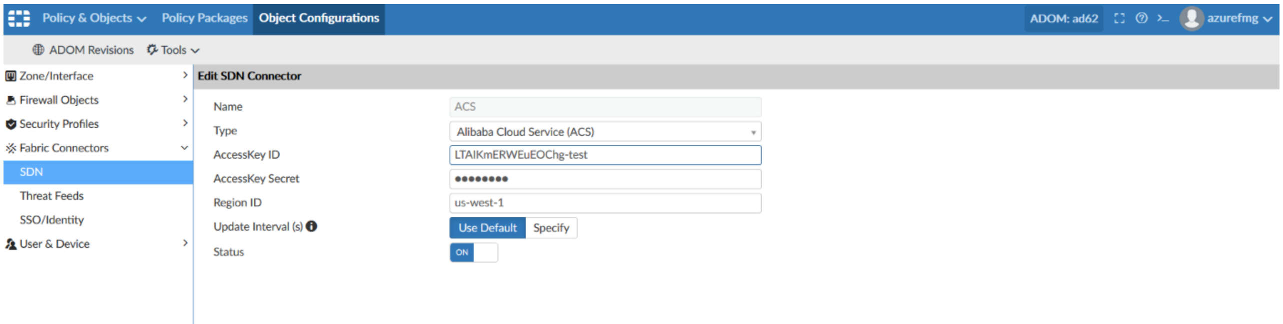


Create New SDN Connector

Name	ACS
Type	Alibaba Cloud Service (ACS)
AccessKey ID	
AccessKey Secret	
Region ID	
Update Interval (s)	
Status	

Application Centric Infrastructure (ACI)
Alibaba Cloud Service (ACS)
Amazon Web Services (AWS)
Microsoft Azure
Google Cloud Platform (GCP)
Kubernetes
VMware NSX

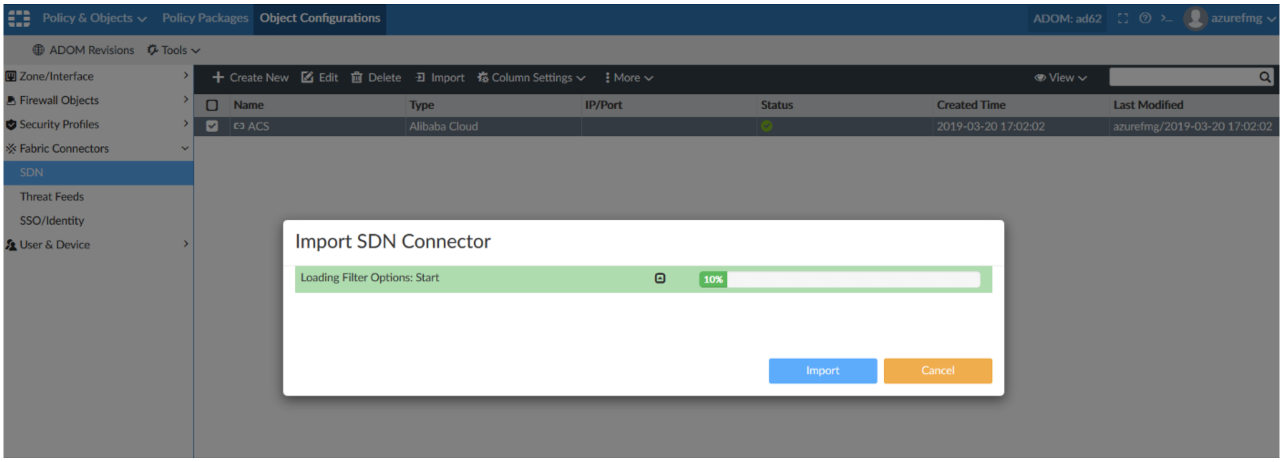
3. Configure the ACS connector information.



Edit SDN Connector

Name	ACS
Type	Alibaba Cloud Service (ACS)
AccessKey ID	LTAIKmERWEuEOChg-test
AccessKey Secret	••••••••
Region ID	us-west-1
Update Interval (s)	Use Default Specify
Status	ON

4. Click the *Import* to import ACS objects. The Import option is only available on *Policy & Objects* > *Object Configurations*.

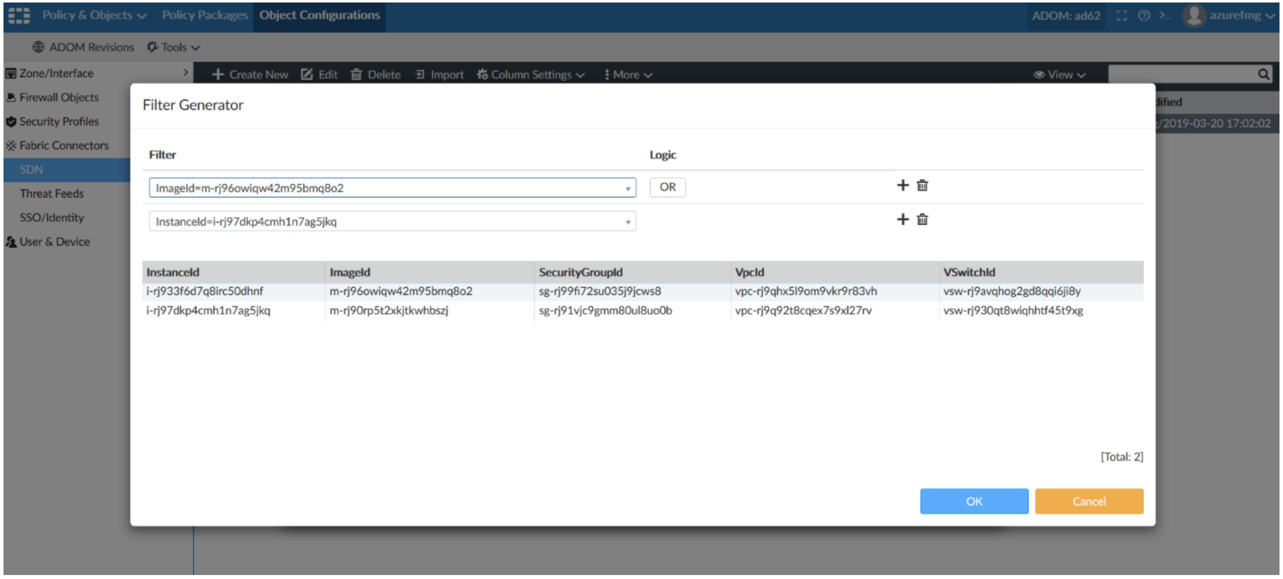


☐	Name	Type	IP/Port	Status	Created Time	Last Modified
☑	ACS	Alibaba Cloud		✓	2019-03-20 17:02:02	azurefmg/2019-03-20 17:02:02

Import SDN Connector

Loading Filter Options: Start 10%

5. Add the filter and click *OK* to apply selected filter.



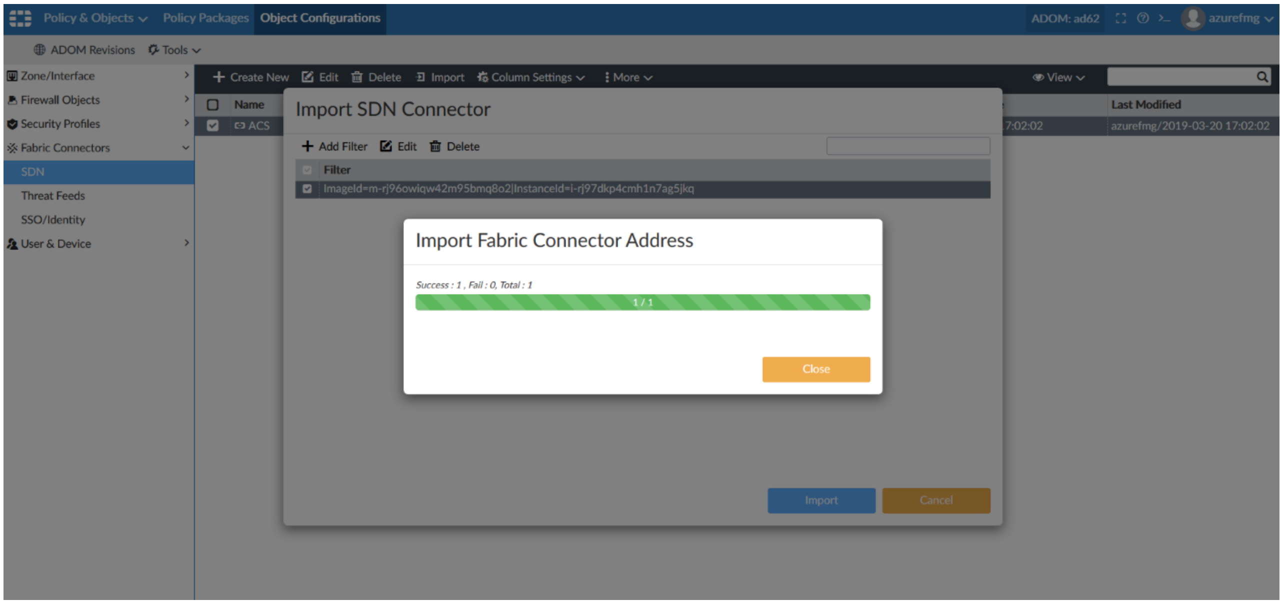
Filter Generator

Filter	Logic
ImageId=m-rj96owiqw42m95bmq8o2	OR
InstanceId=i-rj97dkp4cmh1n7ag5jkq	

InstanceId	ImageId	SecurityGroupId	VpcId	VSwitchId
i-rj933f6d7q8irc50dhnf	m-rj96owiqw42m95bmq8o2	sg-rj99fi72su035j9jcws8	vpc-rj9qhx5l9om9vkr9r83vh	vsw-rj9avqhog2gd8qqi6ji8y
i-rj97dkp4cmh1n7ag5jkq	m-rj90rp5t2xkjtkwhbszj	sg-rj91vjc9gmm80ul8uo0b	vpc-rj9q92t8cqex7s9xl27rv	vsw-rj930qt8wiqhhtf45t9xg

[Total: 2]

6. Click *Import*.



Import SDN Connector

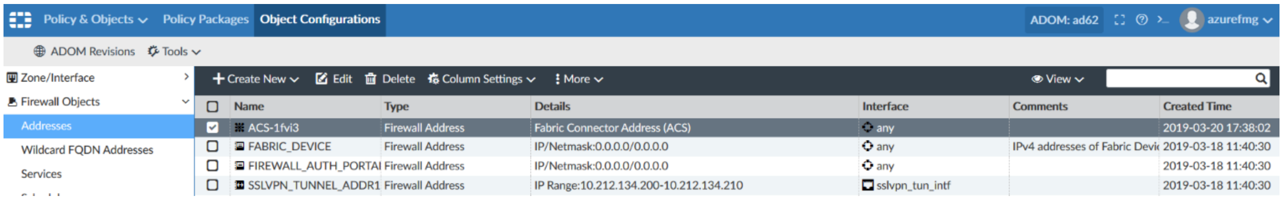
Filter
ImageId=m-rj96owiqw42m95bmq8o2|InstanceId=i-rj97dkp4cmh1n7ag5jkq

Import Fabric Connector Address

Success : 1 , Fail : 0, Total : 1

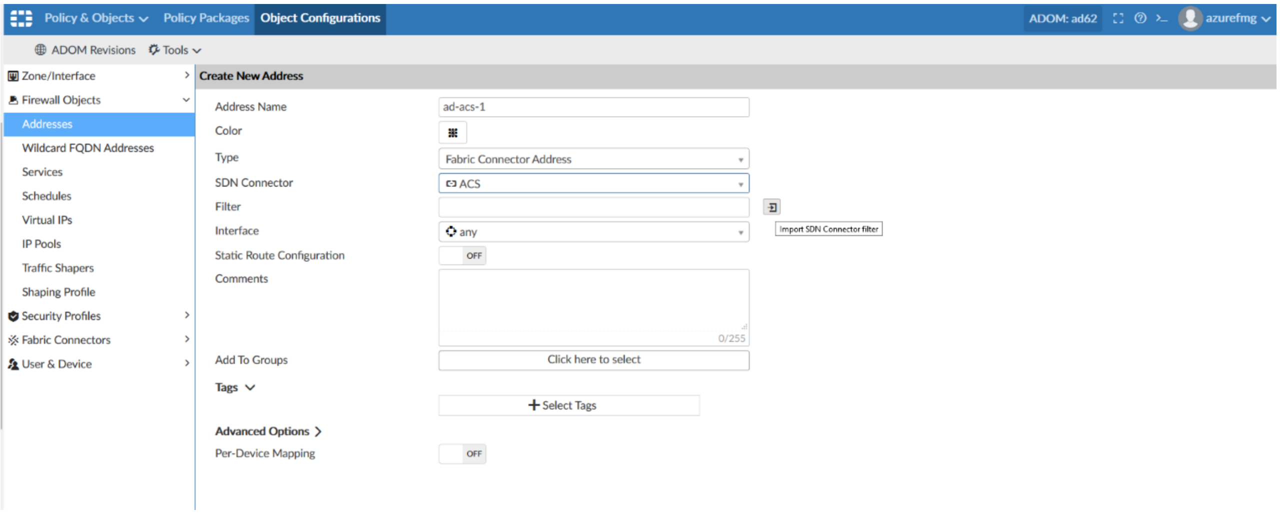
1 / 1

7. The new imported ACS address created.



	Name	Type	Details	Interface	Comments	Created Time
☑	ACS-1fvi3	Firewall Address	Fabric Connector Address (ACS)	any		2019-03-20 17:38:02
□	FABRIC_DEVICE	Firewall Address	IP/Netmask:0.0.0.0/0.0.0.0	any	IPv4 addresses of Fabric Devi	2019-03-18 11:40:30
□	FIREWALL_AUTH_PORTAI	Firewall Address	IP/Netmask:0.0.0.0/0.0.0.0	any		2019-03-18 11:40:30
□	SSLVPN_TUNNEL_ADDR1	Firewall Address	IP Range:10.212.134.200-10.212.134.210	sslvpn_tun_intf		2019-03-18 11:40:30

8. Create a new *Fabric Connector Address*. Import the connector or enter the details of the connector.



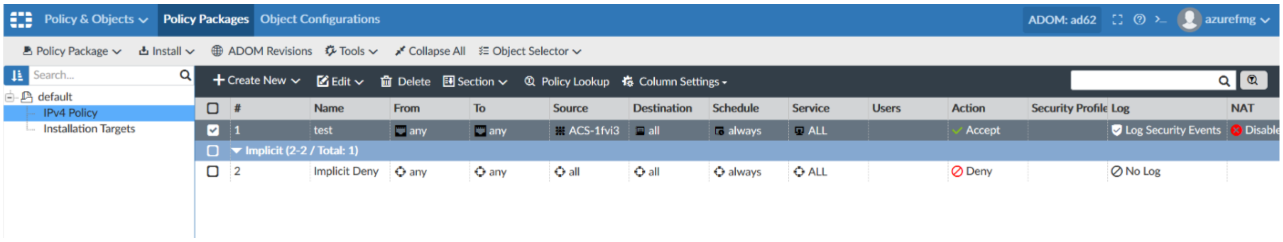
Create New Address

Address Name	ad-acs-1
Color	
Type	Fabric Connector Address
SDN Connector	ACS
Filter	
Interface	any
Static Route Configuration	OFF
Comments	0/255
Add To Groups	Click here to select
Tags	+ Select Tags
Advanced Options	
Per-Device Mapping	OFF

Install the SDN connector to FortiGate

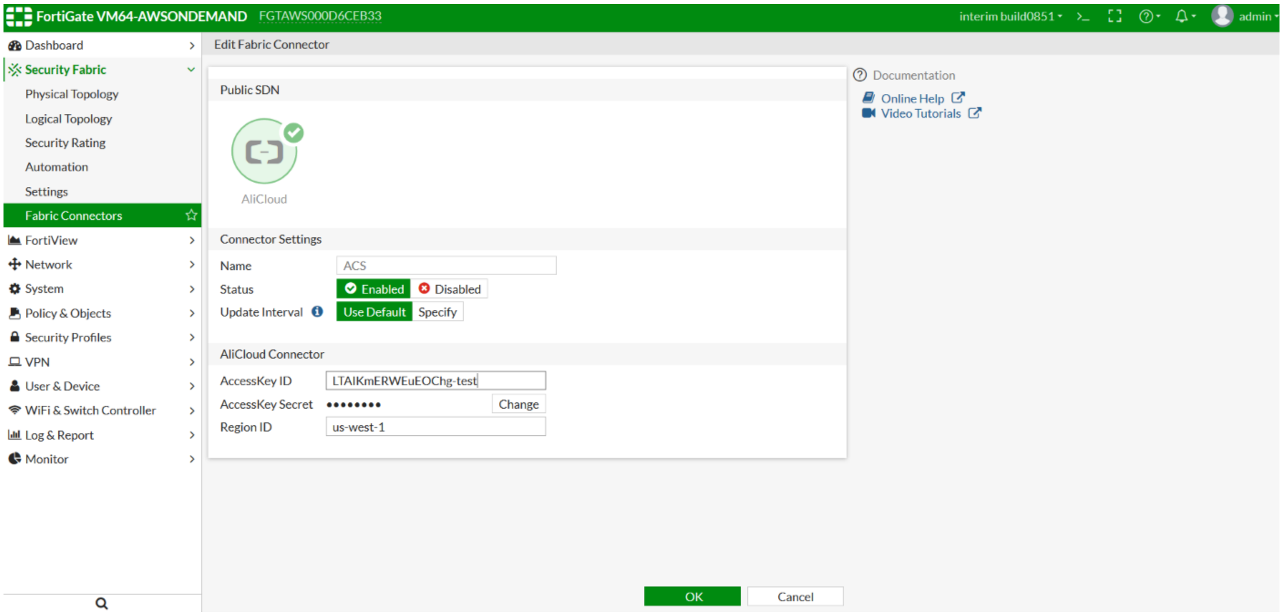
To install the SDN connector to FortiGate:

1. Install ACS SDN connector configuration and imported ACS dynamic object to FortiGate.



☐	#	Name	From	To	Source	Destination	Schedule	Service	Users	Action	Security Profile	Log	NAT
☑	1	test	any	any	ACS-1fvi3	all	always	ALL		✓ Accept		Log Security Events	Disable
☐	Implicit (2-2 / Total: 1)												
☐	2	Implicit Deny	any	any	all	all	always	ALL		Deny		No Log	

2. Check the FortiGate whether, the ACS connector and address is installed.



Edit Fabric Connector

Public SDN

AliCloud

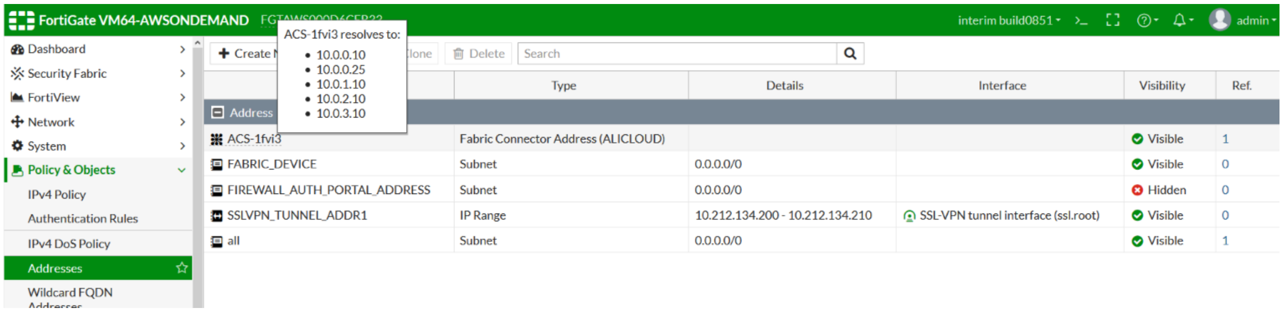
Connector Settings

Name	ACS
Status	✓ Enabled / Disabled
Update Interval	Use Default / Specify

AliCloud Connector

AccessKey ID	LTAIKmERWEuEOChg-test
AccessKey Secret	•••••••• Change
Region ID	us-west-1

3. The ACS address IP can now be resolved.



ACS-1fvi3 resolves to:

- 10.0.0.10
- 10.0.0.25
- 10.0.1.10
- 10.0.2.10
- 10.0.3.10

	Type	Details	Interface	Visibility	Ref.
Address					
ACS-1fvi3	Fabric Connector Address (ALICLOUD)			✓ Visible	1
FABRIC_DEVICE	Subnet	0.0.0.0/0		✓ Visible	0
FIREWALL_AUTH_PORTAL_ADDRESS	Subnet	0.0.0.0/0		✗ Hidden	0
SSLVPN_TUNNEL_ADDR1	IP Range	10.212.134.200 - 10.212.134.210	SSL-VPN tunnel interface (ssl.root)	✓ Visible	0
all	Subnet	0.0.0.0/0		✓ Visible	1

SD-WAN

This section lists the new features added to FortiManager for SD-WAN.

List of new features:

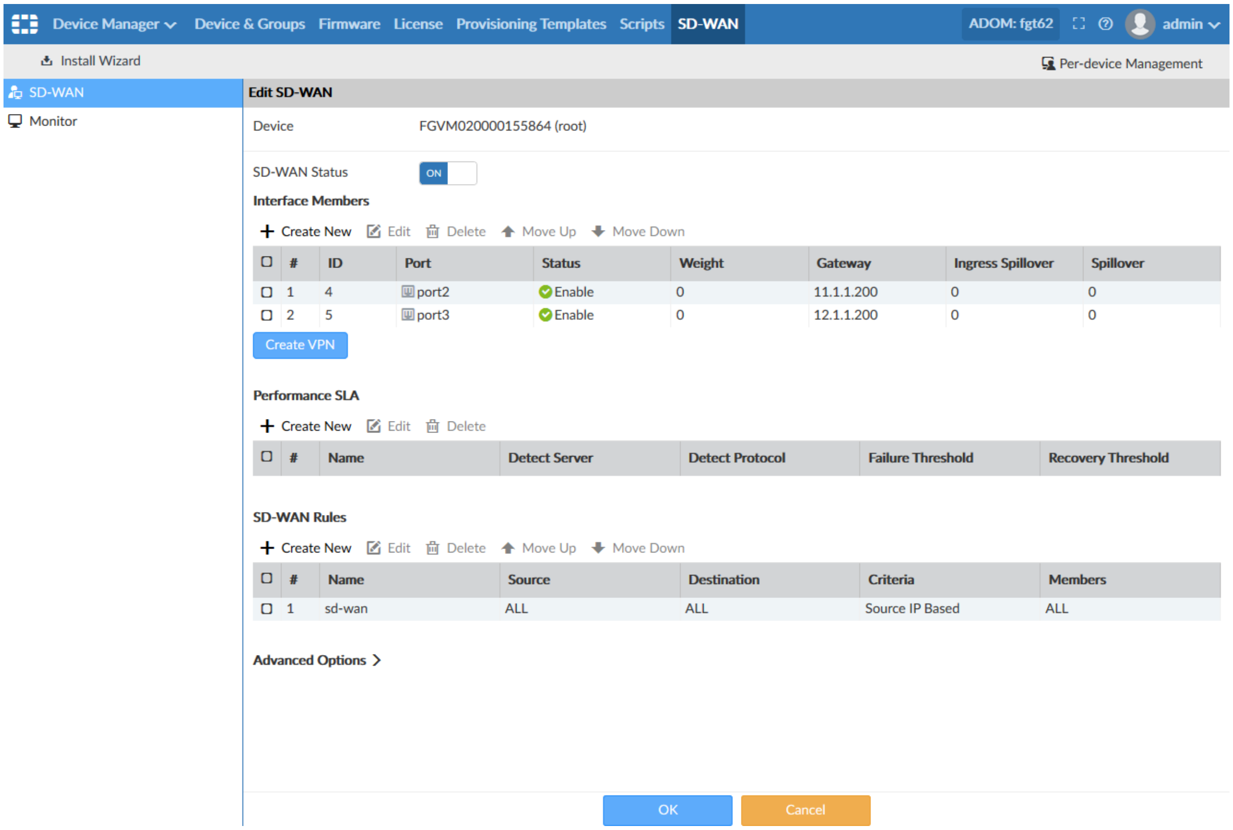
IPSEC Wizard in Device Manager

The SD-WAN Interface page in FortiManager now includes an IPsec VPN creation wizard.

Configuring the IPsec VPN in SD-WAN

1. Go to *System Settings* > *All ADOMs* and edit the ADOM. Disable *SD-WAN* in Central Management. Click *OK*.
2. Go to *Device Manager* > *SD-WAN*. Select any device or VDOM and click *Edit*. If no device is available, click *Create New*.

3. Click *Create VPN* under *Interface Members* in the *Create New SD-WAN* or *Edit SD-WAN page*.



Edit SD-WAN

Device: FGVM020000155864 (root)

SD-WAN Status: ON

Interface Members

☐	#	ID	Port	Status	Weight	Gateway	Ingress Spillover	Spillover
☐	1	4	port2	✓ Enable	0	11.1.1.200	0	0
☐	2	5	port3	✓ Enable	0	12.1.1.200	0	0

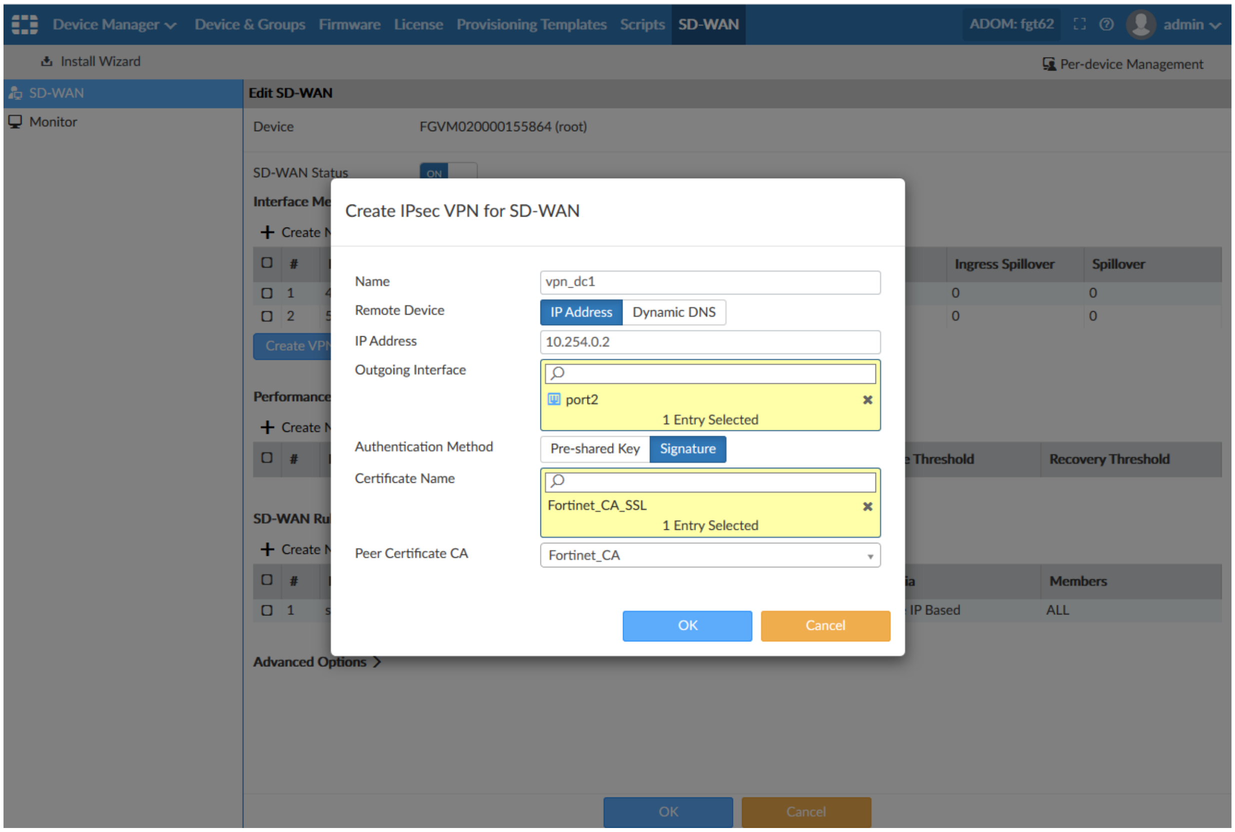
Performance SLA

☐	#	Name	Detect Server	Detect Protocol	Failure Threshold	Recovery Threshold

SD-WAN Rules

☐	#	Name	Source	Destination	Criteria	Members
☐	1	sd-wan	ALL	ALL	Source IP Based	ALL

4. Configure the settings. For *Outgoing Interface*, select one or more interfaces.



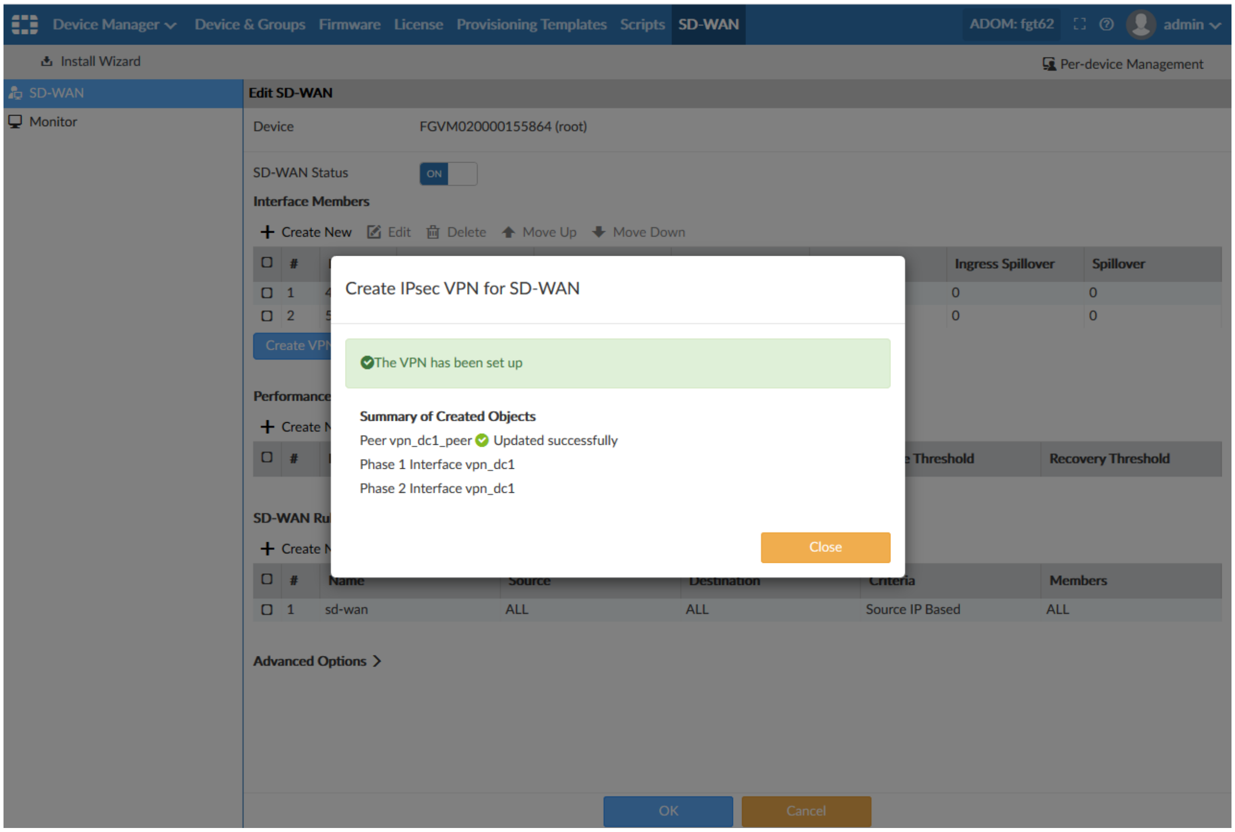
Device FGVM020000155864 (root)

Create IPsec VPN for SD-WAN

Name	vpn_dc1
Remote Device	IP Address / Dynamic DNS (IP Address selected)
IP Address	10.254.0.2
Outgoing Interface	port2 1 Entry Selected
Authentication Method	Pre-shared Key / Signature (Signature selected)
Certificate Name	Fortinet_CA_SSL 1 Entry Selected
Peer Certificate CA	Fortinet_CA

OK Cancel

5. Click *OK* to auto-generate IPsec VPNs.



Edit SD-WAN

Device FGVM020000155864 (root)

SD-WAN Status ON

Interface Members

☐	#		Ingress Spillover	Spillover
☐	1	4	0	0
☐	2	5	0	0

Performance

☐	#		Threshold	Recovery Threshold

SD-WAN Ru

☐	#	Name	Source	Destination	Criteria	Members
☐	1	sd-wan	ALL	ALL	Source IP Based	ALL

Create IPsec VPN for SD-WAN

✓ The VPN has been set up

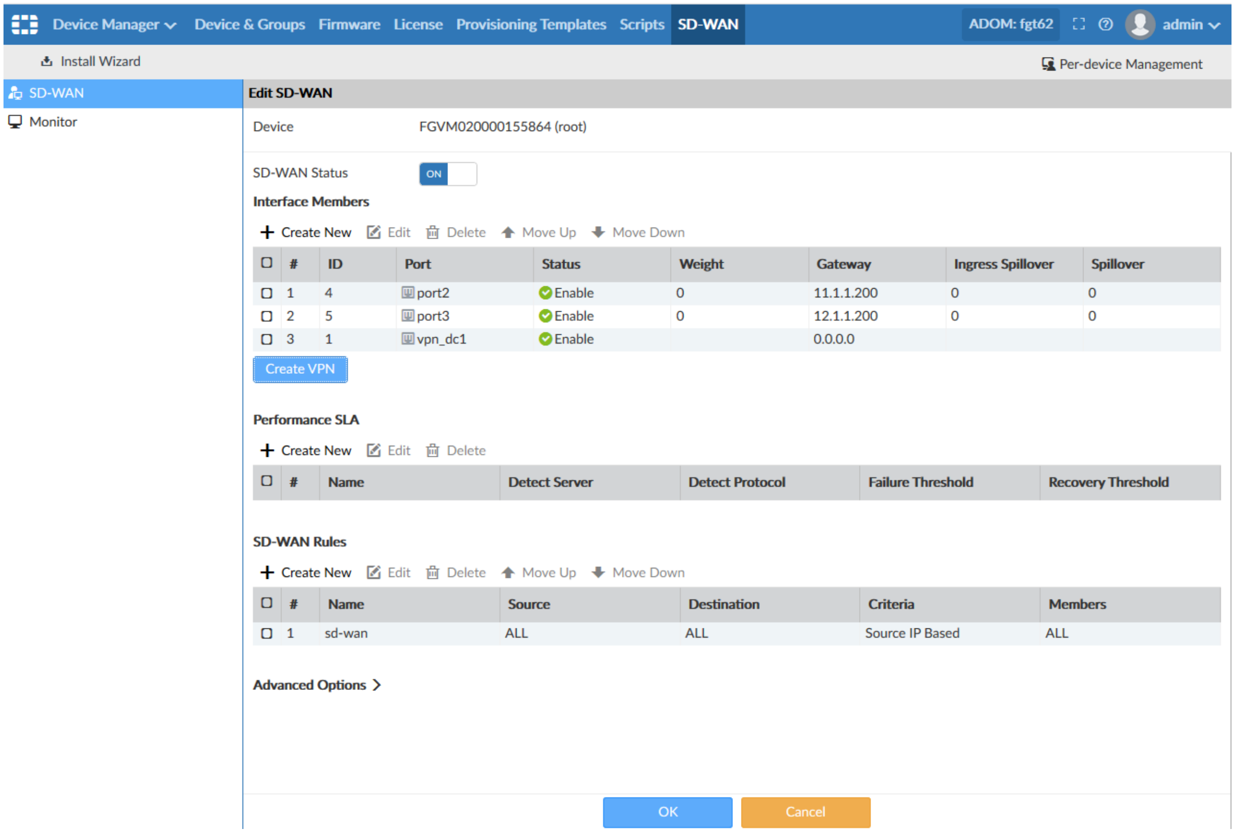
Summary of Created Objects

Peer vpn_dc1_peer ✓ Updated successfully

Phase 1 Interface vpn_dc1

Phase 2 Interface vpn_dc1

6. The auto-generated VPN interface are automatically added to the list of SD-WAN members.



Edit SD-WAN

Device FGVM020000155864 (root)

SD-WAN Status ON

Interface Members

□	#	ID	Port	Status	Weight	Gateway	Ingress Spillover	Spillover
□	1	4	port2	✓Enable	0	11.1.1.200	0	0
□	2	5	port3	✓Enable	0	12.1.1.200	0	0
□	3	1	vpn_dc1	✓Enable		0.0.0.0		

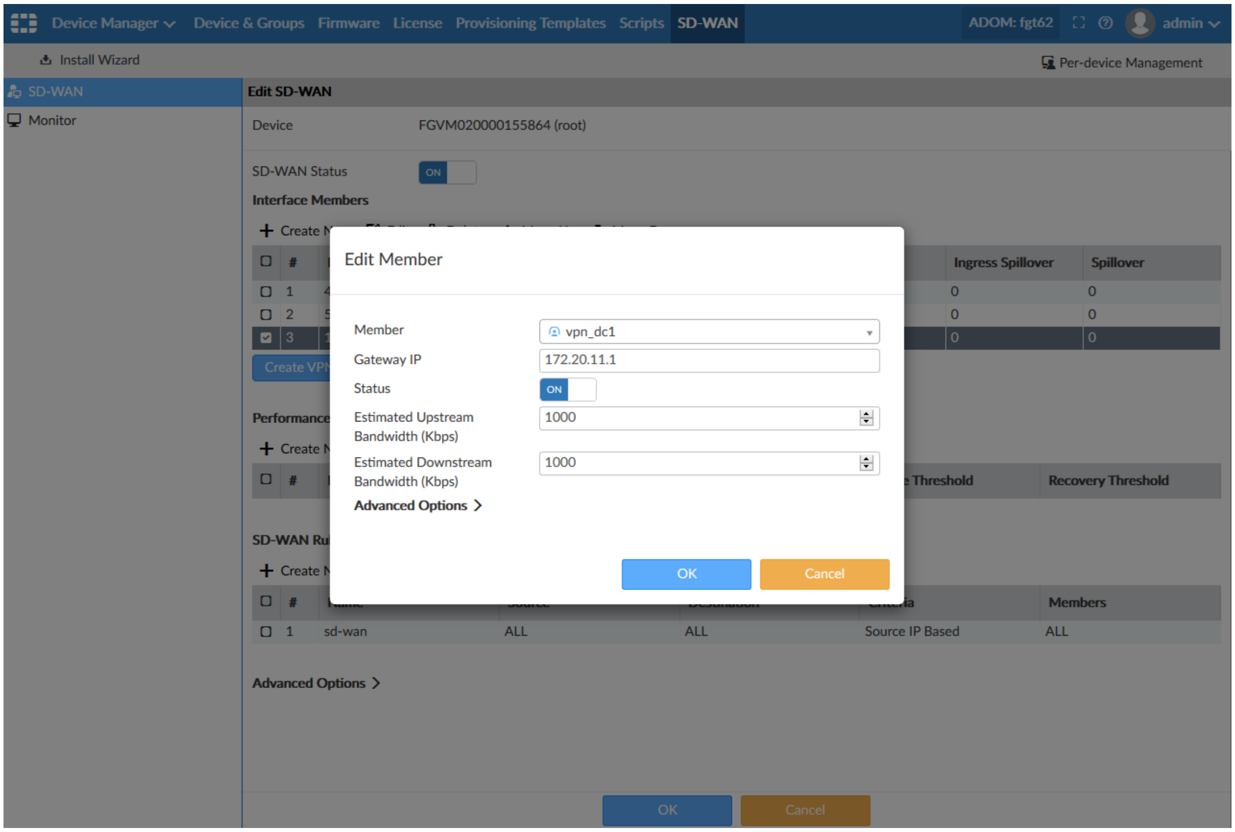
Performance SLA

□	#	Name	Detect Server	Detect Protocol	Failure Threshold	Recovery Threshold

SD-WAN Rules

□	#	Name	Source	Destination	Criteria	Members
□	1	sd-wan	ALL	ALL	Source IP Based	ALL

7. Edit the VPN in *Interface Members* to configure *Gateway IP*, *Estimated Upstream Bandwidth (Kbps)*, and *Estimated Downstream Bandwidth (Kbps)*.



Edit SD-WAN

Device FGVM020000155864 (root)

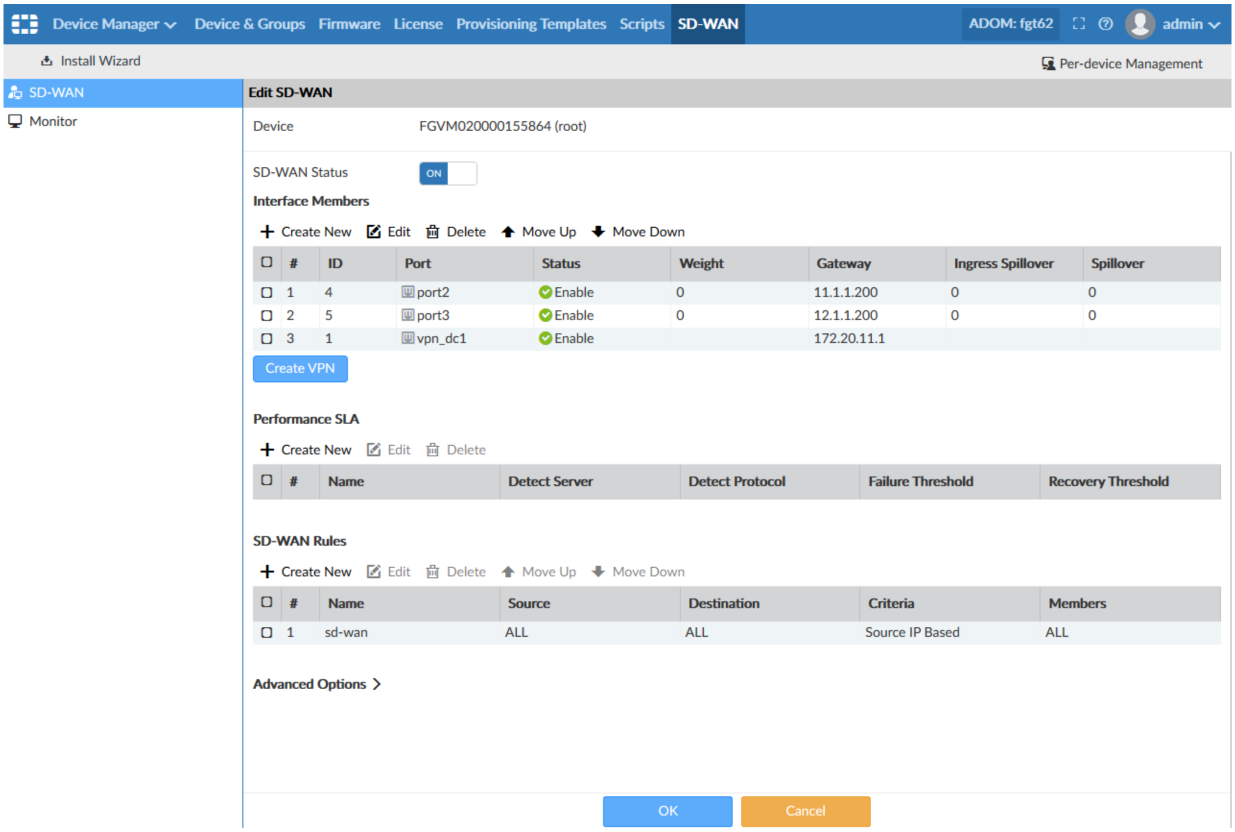
SD-WAN Status ON

Edit Member

Member	vpn_dc1
Gateway IP	172.20.11.1
Status	ON
Estimated Upstream Bandwidth (Kbps)	1000
Estimated Downstream Bandwidth (Kbps)	1000

Advanced Options >

8. The IPsec VPN with the configured settings is now available for use.



Edit SD-WAN

Device FGVM020000155864 (root)

SD-WAN Status ON

Interface Members

□	#	ID	Port	Status	Weight	Gateway	Ingress Spillover	Spillover
□	1	4	port2	✓Enable	0	11.1.1.200	0	0
□	2	5	port3	✓Enable	0	12.1.1.200	0	0
□	3	1	vpn_dc1	✓Enable		172.20.11.1		

Performance SLA

□	#	Name	Detect Server	Detect Protocol	Failure Threshold	Recovery Threshold

SD-WAN Rules

□	#	Name	Source	Destination	Criteria	Members
□	1	sd-wan	ALL	ALL	Source IP Based	ALL

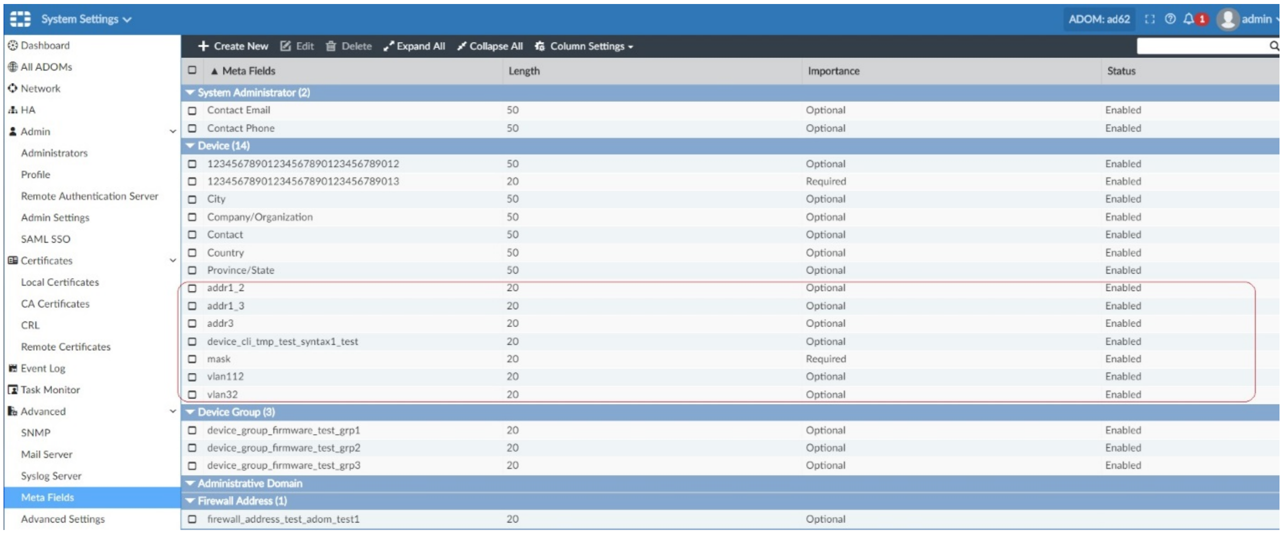
Advanced Options >

Zero Touch Provisioning - CLI Template with Variables

In FortiManager 6.2, it is now possible to define a CLI template using variables, and to assign those variable definition per-device. For Zero-Touch Provisioning (ZTP), this allows to define a model device, and to assign a template with variables, so that on the first connection, the unique configuration for that site can be deployed without manual intervention.

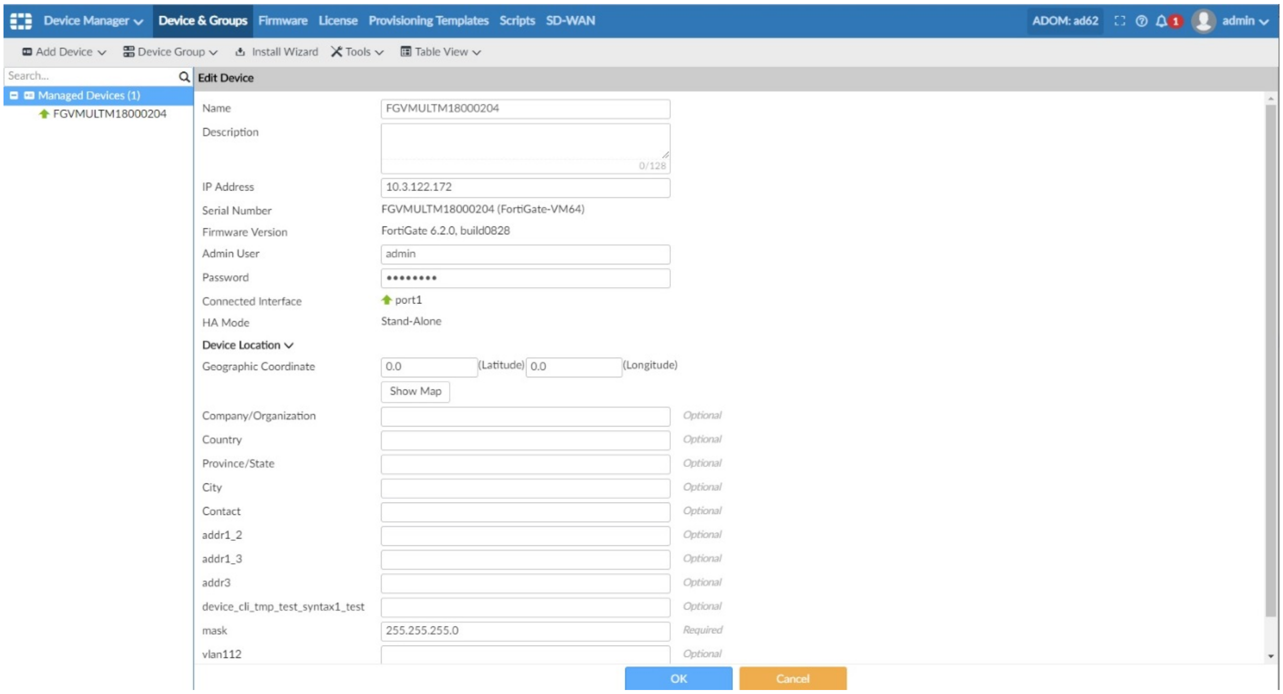
To configure a CLI Template with variables:

1. Go to *System Settings > Advanced > Meta Fields*. Define the variables which are used in the CLI templates.



Meta Fields	Length	Importance	Status
System Administrator (2)			
Contact Email	50	Optional	Enabled
Contact Phone	50	Optional	Enabled
Device (14)			
12345678901234567890123456789012	50	Optional	Enabled
12345678901234567890123456789013	20	Required	Enabled
City	50	Optional	Enabled
Company/Organization	50	Optional	Enabled
Contact	50	Optional	Enabled
Country	50	Optional	Enabled
Province/State	50	Optional	Enabled
addr1_2	20	Optional	Enabled
addr1_3	20	Optional	Enabled
addr3	20	Optional	Enabled
device_cli_tmp_test_syntax1_test	20	Optional	Enabled
mask	20	Required	Enabled
vlan112	20	Optional	Enabled
vlan32	20	Optional	Enabled
Device Group (3)			
device_group_firmware_test_grp1	20	Optional	Enabled
device_group_firmware_test_grp2	20	Optional	Enabled
device_group_firmware_test_grp3	20	Optional	Enabled
Administrative Domain			
Firewall Address (1)			
firewall_address_test_adom_test1	20	Optional	

2. Go to *Device Manager*, edit the device and enter the value for the variables.



Edit Device

Name	FGVMULTM18000204
Description	0/128
IP Address	10.3.122.172
Serial Number	FGVMULTM18000204 (FortiGate-VM64)
Firmware Version	FortiGate 6.2.0, build0828
Admin User	admin
Password	••••••••
Connected Interface	port1
HA Mode	Stand-Alone
Device Location	
Geographic Coordinate	0.0 (Latitude) 0.0 (Longitude) Show Map
Company/Organization	Optional
Country	Optional
Province/State	Optional
City	Optional
Contact	Optional
addr1_2	Optional
addr1_3	Optional
addr3	Optional
device_cli_tmp_test_syntax1_test	Optional
mask	255.255.255.0 Required
vlan112	Optional

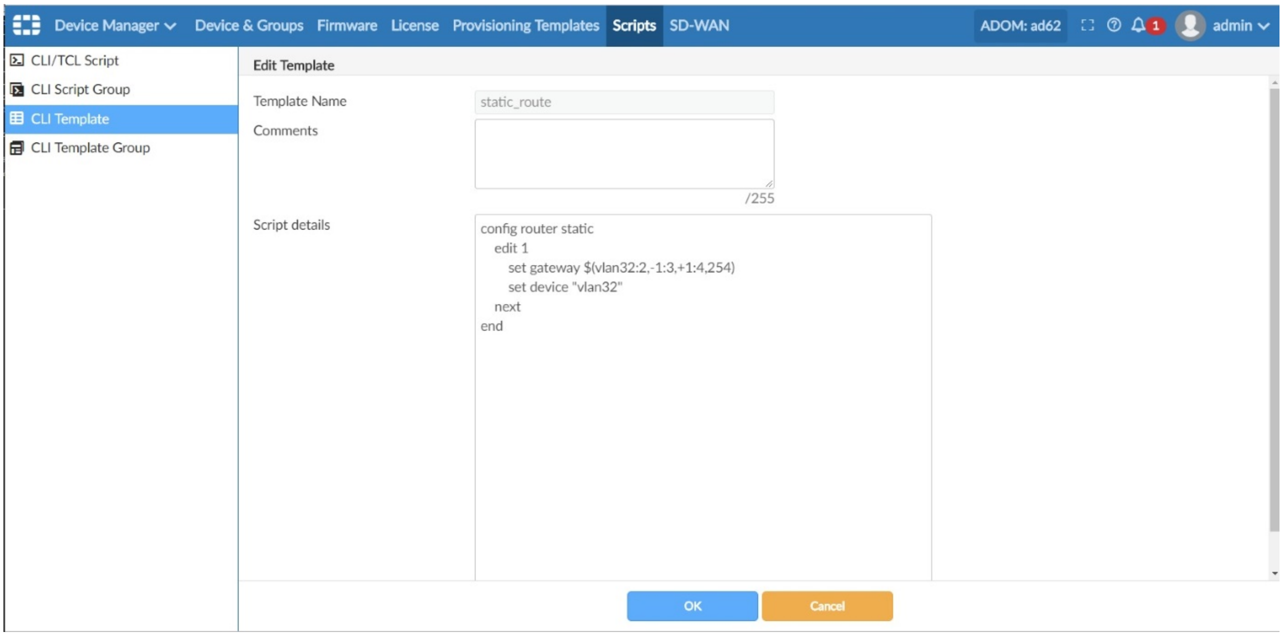
3. Go to *Script Manager*. There are two new script types: *CLI Template* and *CLI Template Group*. Create a new *CLI Script Template*. Here is an example of *CLI Template Script*.

   ```
   config system interface
      edit "vlan32"
          set ip $(vlan32) $(mask)
          set interface "port2"
          set vlanid 32
      next
   end
   ```

4. The variables in the CLI Template can be modified. FortiManager only supports modified variable for IPv4 address format. Here is the example that a CLI Template could contain modified variables.

   ```
   config router static
      edit 1
          set gateway $(vlan32:2,-1:3,+1:4,254)
          set device "vlan32"
      next
   end
   ```

   In this example, the CLI Template mechanism will subtract -1 to the 2nd byte of the IP address defined in the variable *subnet_lan* and add 1 to the 3rd byte, and finally will set the 4th byte to 254.



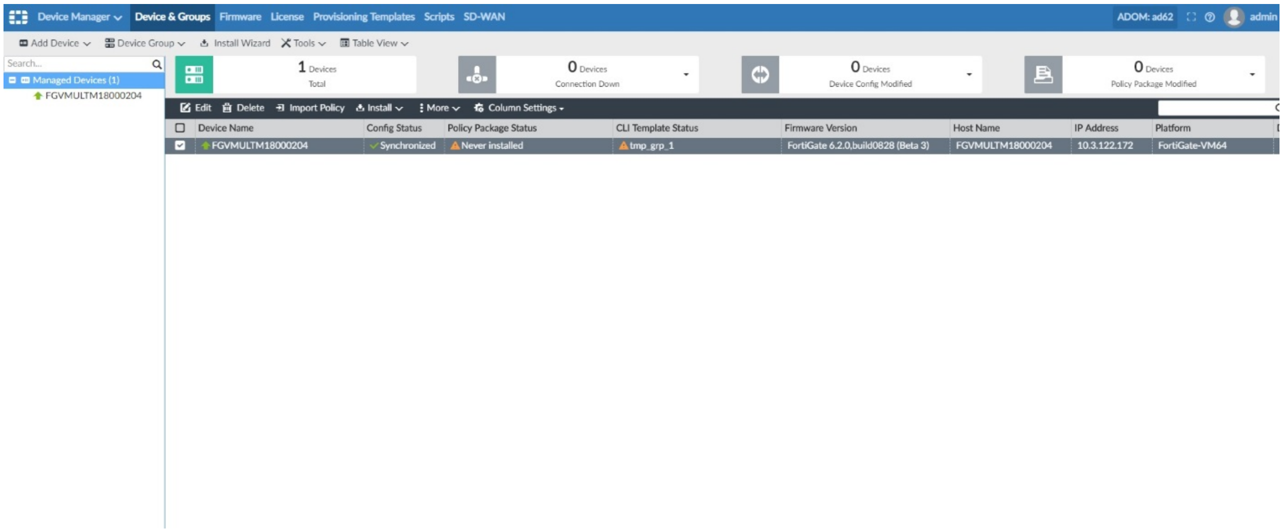
Template Name: static_route

Comments: /255

Script details:

```
config router static
   edit 1
      set gateway $(vlan32:2,-1:3,+1:4,254)
      set device "vlan32"
   next
end
```

5. Create a CLI template group. You can drag and drop to re-order members.
6. Assign the CLI template and template group to device (global) or VDOM.
7. On the Device Manager page, a new column *CLI Template Status* was added on *Managed FortiGate* list page, and it works together with *Config Status* and *Policy Package Status* to indicate device status. Either *Config Status* or *CLI Template Status* is dirty, it is able to install device configuration changes to FortiGate.



☐	Device Name	Config Status	Policy Package Status	CLI Template Status	Firmware Version	Host Name	IP Address	Platform
☑	FGVMULTM18000204	✓ Synchronized	⚠ Never installed	⚠ tmp_grp_1	FortiGate 6.2.0,build0828 (Beta 3)	FGVMULTM18000204	10.3.122.172	FortiGate-VM64

8. A CLI Template is implicitly applied when the administrator is triggering a push operation (Install Device Settings or Policy Package Install). There is no need for an explicit *Apply CLI Template* operation. When installing device settings or a policy package, FortiManager should always consider applying the CLI Template after all the copy operations.

SD-WAN History Monitoring

History graphs are now available for the SD-WAN Monitoring. You can View bandwidth, packet loss, latency and jitter history for each device / WAN-link interface and cloud applications. Additionally, the interface allows drill-down to selected time periods for deeper inspection of those events.

- Go to SD-WAN Monitoring > Table view. For each device / interface you can now see Bandwidth / Packet Loss / Latency / Jitter history
- Go to SD-WAN Monitoring > Table view. For each device, you can now see the interface status history.
- This feature is only for ADOM 6.2 and FortiOS 6.2.
- FortiOS 6.0 does not support history API and hence the drill-down is disabled in table view.

Enable or Disable SD-WAN History Monitoring

Enable/disable the SD-WAN history monitoring from the command line. The default is disable.

To enable SD-WAN History Monitoring:

```
config system admin setting
   set sdwan-monitor-history enable
end
```

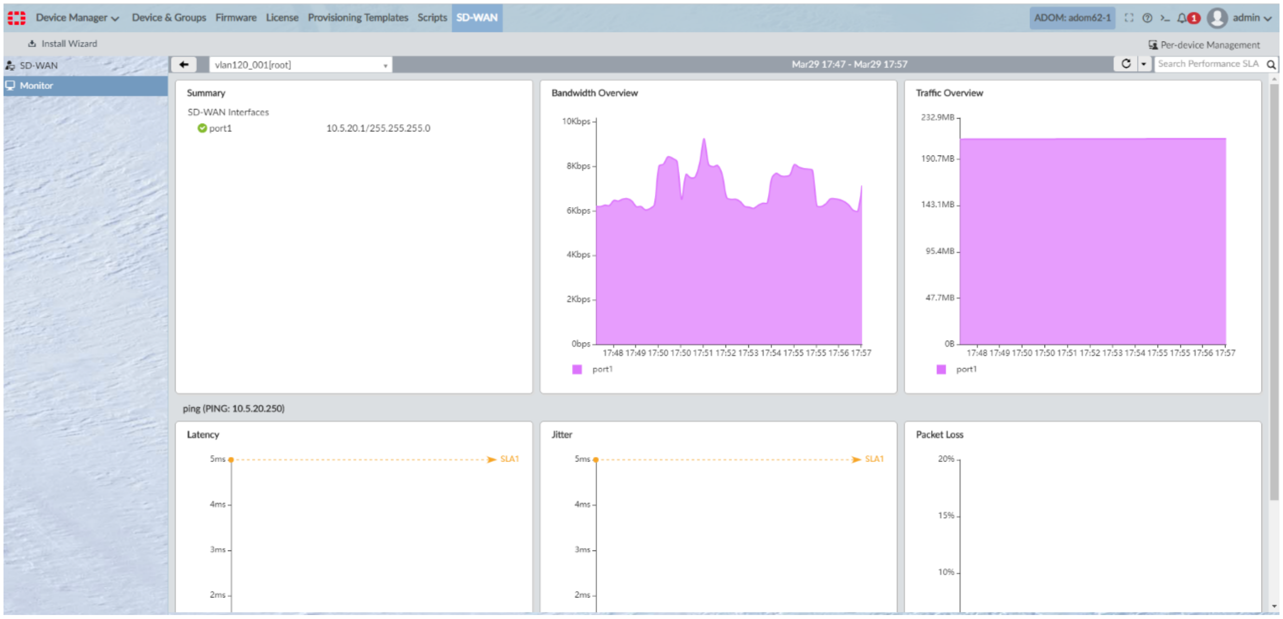
To disable SD-WAN History Monitoring:

```
config system admin setting
   set sdwan-monitor-history disable
end
```

When SD-WAN History Monitoring is disabled

When SD-WAN history monitoring is disabled, go to *SD-WAN Monitor> Table View* to view the drill-down monitor. When disabled, FortiManager shows only the history for the last 10 minutes querying the data directly from FortiGate devices.

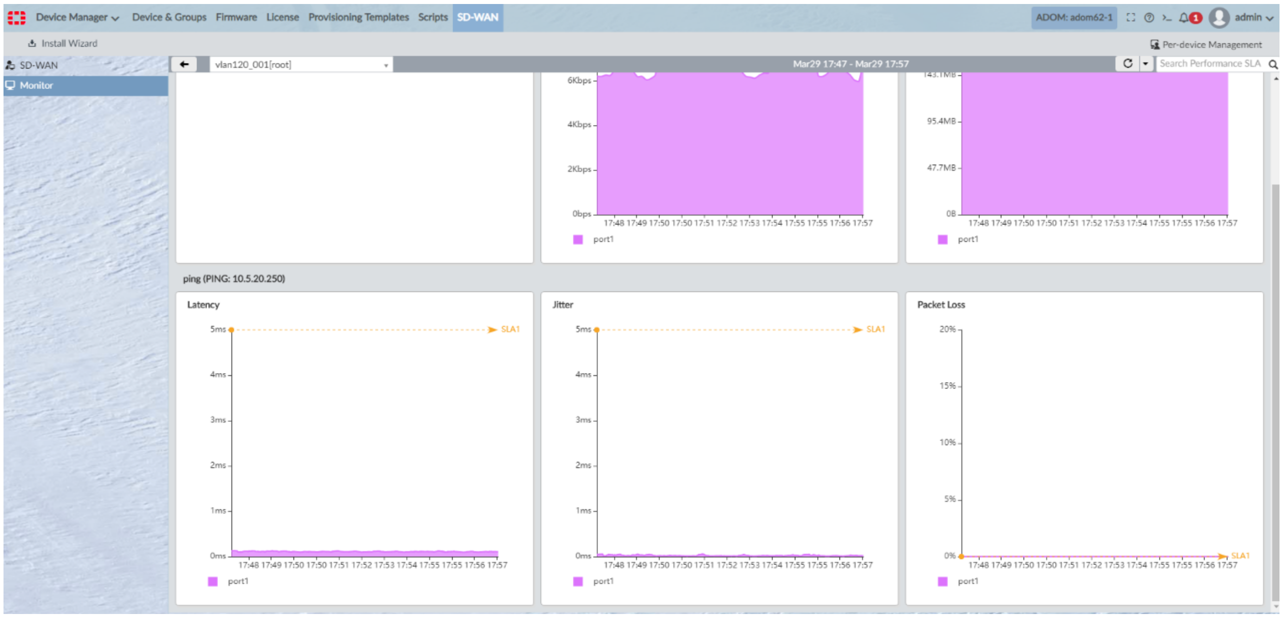
- Go to *SD-WAN Monitoring* > *Table View*. The drill-down is available to monitor Health Check History and Interface Status History.
- Go to *SD-WAN Monitoring* > *Table view*. For each device / interface you can now see Bandwidth Overview/ Traffic Overview.



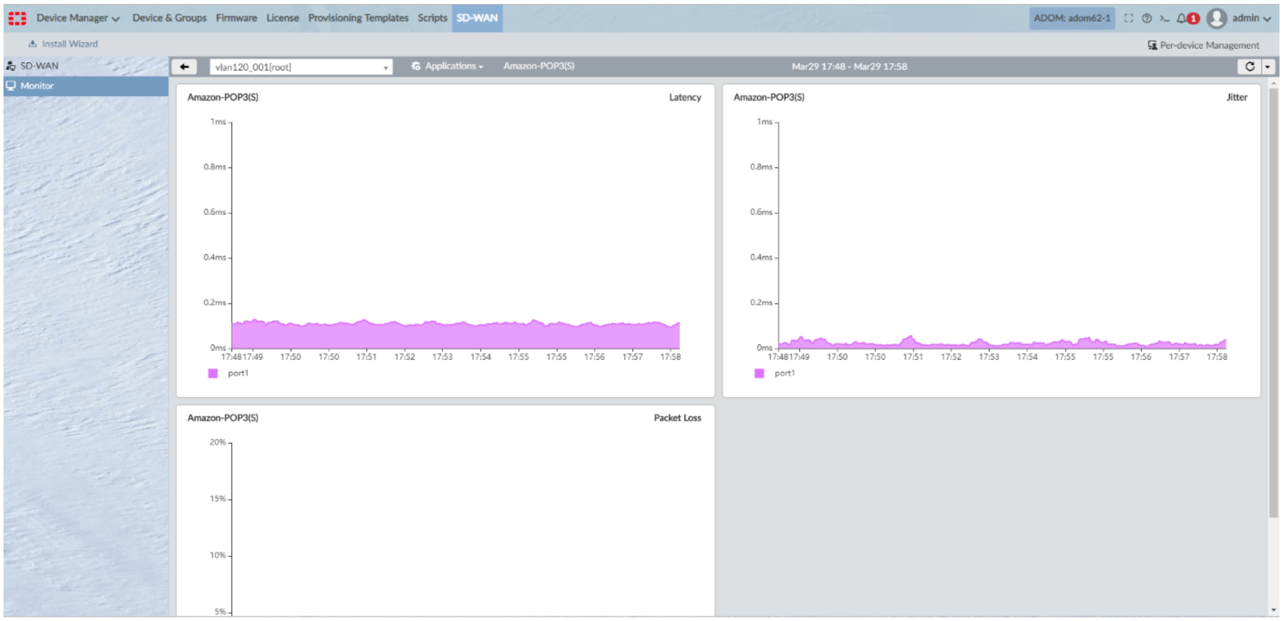
SD-WAN Interfaces

✓ port1 10.5.20.1/255.255.255.0

- Go to *SD-WAN Monitoring* > *Table view*. For each device / interface you can now see Packet Loss / Latency / Jitter history.



- Go to *SD-WAN Monitoring* > *Table view*. For each application, you can now see Packet Loss / Latency / Jitter history.



When SD-WAN History Monitoring is enabled

See Optimize FortiManager REST API querying of FortiGate on page 73.

Optimize FortiManager REST API querying of FortiGate

Longer-term history (up to 8 days) can be stored by FortiManager and available for drill-down and and trending analysis. This feature is enabled in CLI and should be assessed for deployment size, available storage, etc.

History graphs are now available for the SD-WAN Monitoring. You can View bandwidth, packet loss, latency and jitter history for each device / WAN-link interface and cloud applications. Additionally, the interface allows drill-down to selected time periods for deeper inspection of those events.

- Go to SD-WAN Monitoring > Table view. For each device / interface you can now see Bandwidth / Packet Loss / Latency / Jitter history
- Go to SD-WAN Monitoring > Table view. For each device, you can now see the interface status history.
- This feature is only for ADOM 6.2 and FortiOS 6.2.
- FortiOS 6.0 does not support history API and hence the drill-down is disabled in table view.

Enable or Disable SD-WAN History Monitoring

Enable/disable the SD-WAN history monitoring from the command line. The default is disable.

To enable SD-WAN History Monitoring:

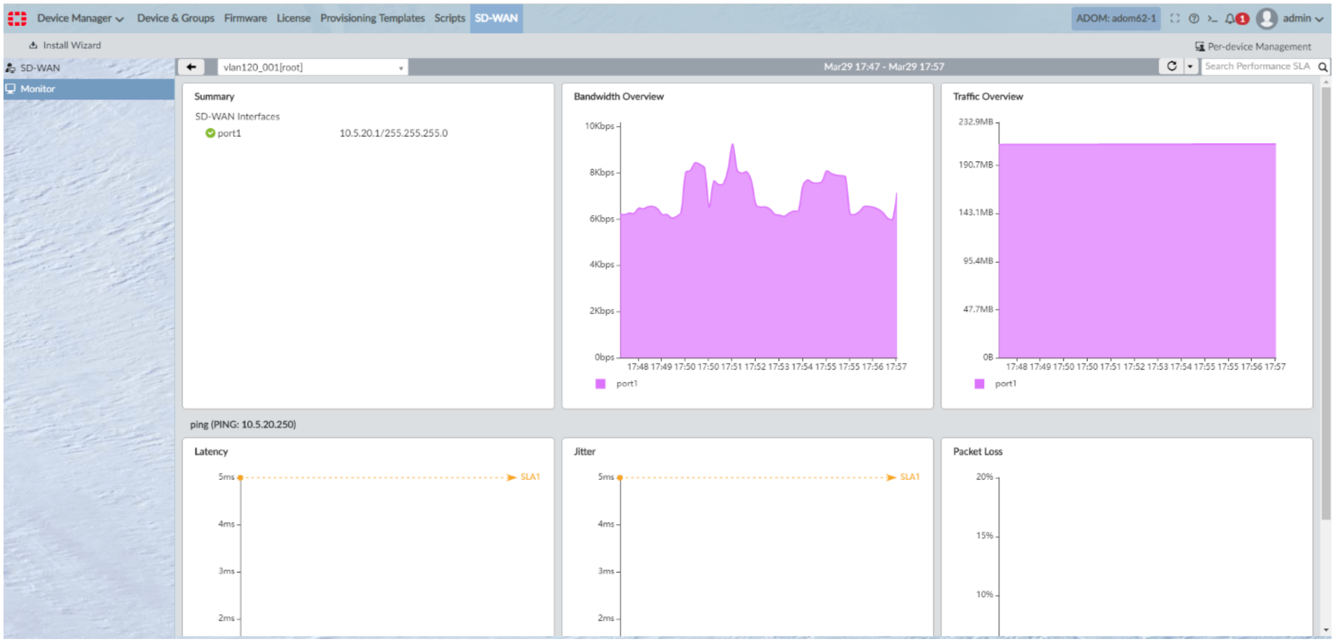
```
config system admin setting
   set sdwan-monitor-history enable
end
```

To disable SD-WAN History Monitoring:

```
config system admin setting
   set sdwan-monitor-history disable
end
```

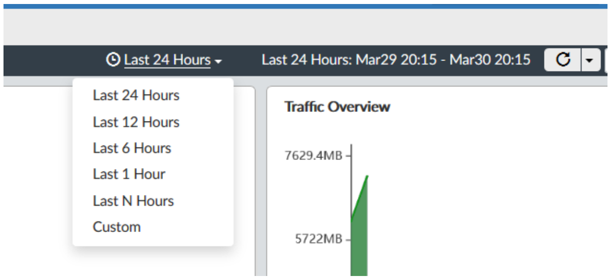
When SD-WAN History Monitoring is disabled

Go to *SD-WAN Monitoring* > *Table View*. The drill-down is available only for 10 minutes and is directly queried from FortiGate devices.

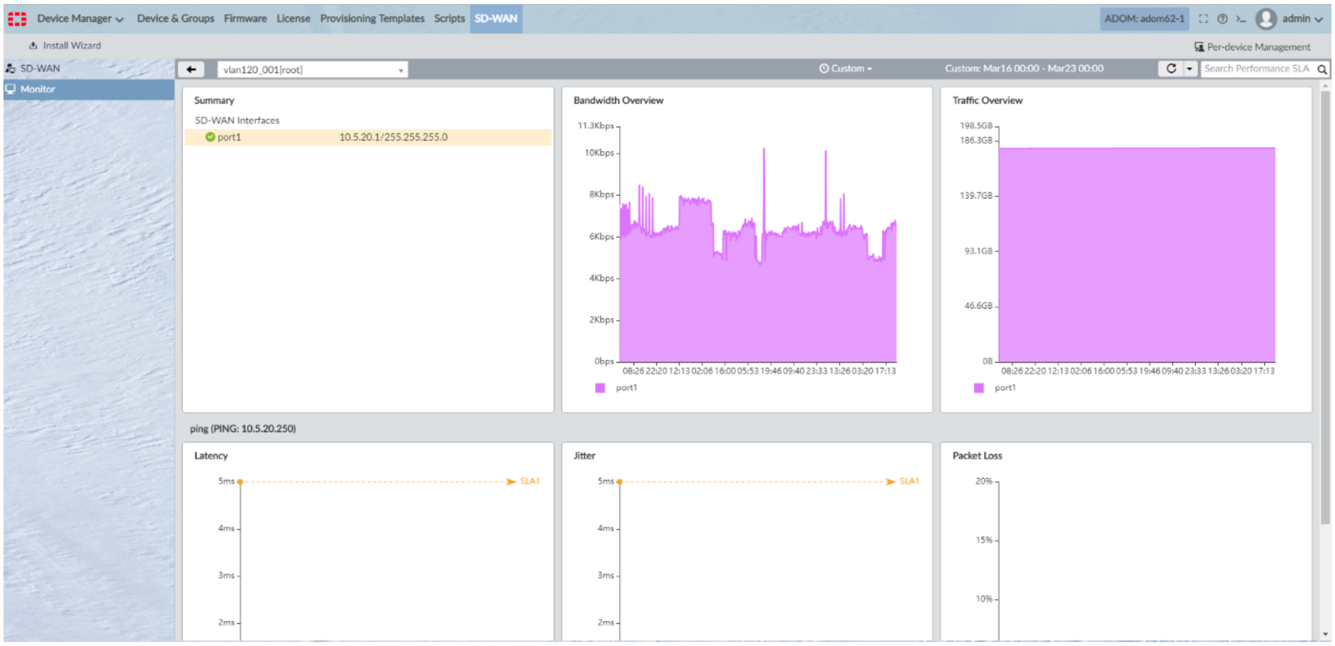


When SD-WAN History Monitoring is enabled

Go to *SD-WAN Monitoring* > *Table View*. The drill-down monitor can now select different time period for last 24/12/6/1/N hours, and custom days.



Maximum of 8 days data can be kept in the FortiManager database.

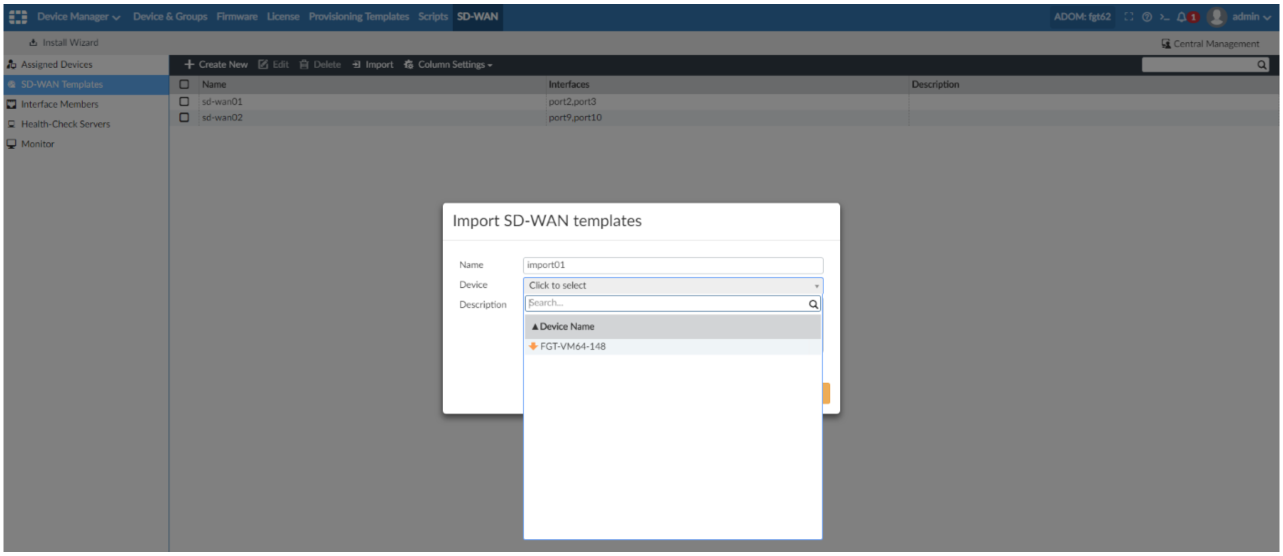


Template Import from Device

When central SD-WAN management is enabled, a device pre-configured device can have its configuration imported to central templates, which can then be reused for other devices in the deployment.

To import SD-WAN templates:

1. Go to *Device Manager* > *SD-WAN* > *SD-WAN Templates*.



Name	Interfaces	Description
sd-wan01	port2,port3	
sd-wan02	port9,port10	

Import SD-WAN templates

Name: import01

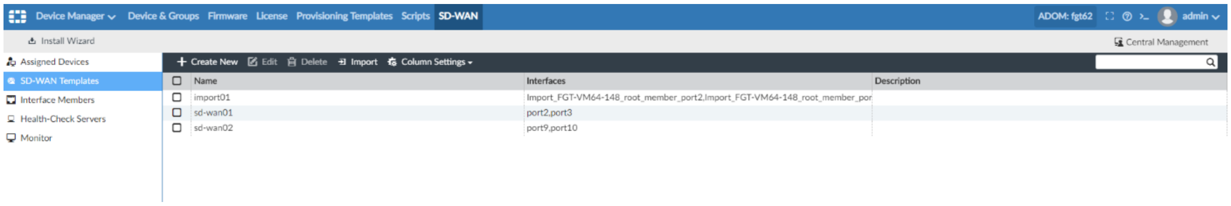
Device: Click to select

Description:

Search...

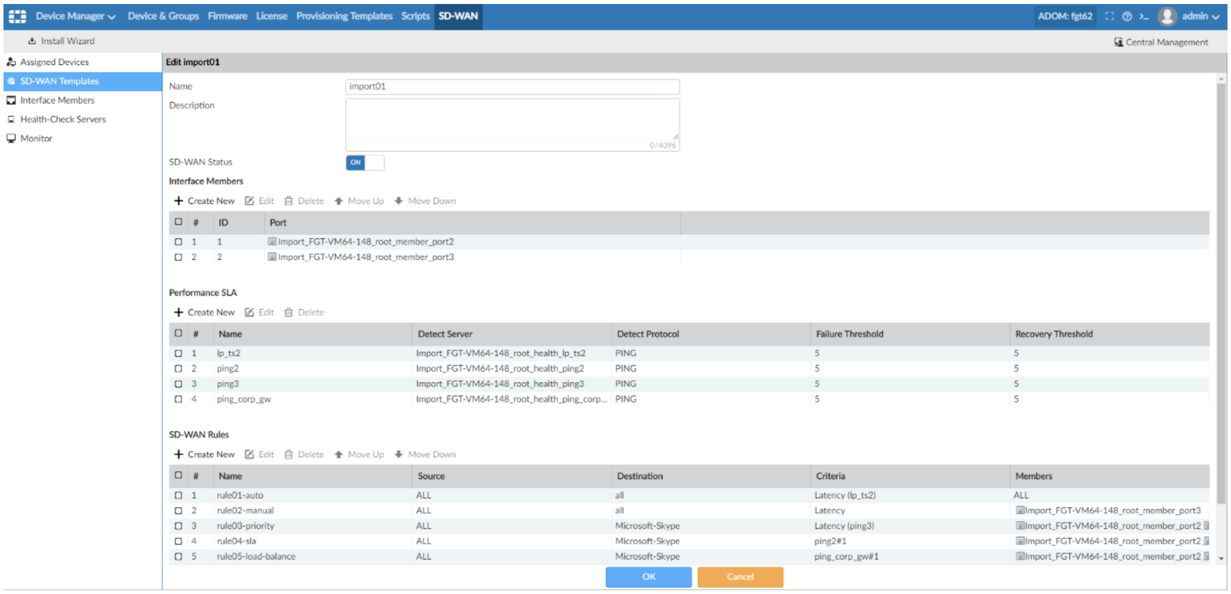
▲Device Name
FGT-VM64-148

2. Click *Import* and select the device/VDOM to import.
   - The SD-WAN templates are imported.



□	Name	Interfaces	Description
□	import01	Import_FGT-VM64-148_root_member_port2,Import_FGT-VM64-148_root_member_por	
□	sd-wan01	port2,port3	
□	sd-wan02	port9,port10	

   - The Interface Members, Performance SLA, and SD-WAN rules are also imported.



Edit import01

Name: import01

Description: 0/4096

SD-WAN Status: ON

Interface Members

□	#	ID	Port
□	1	1	Import_FGT-VM64-148_root_member_port2
□	2	2	Import_FGT-VM64-148_root_member_port3

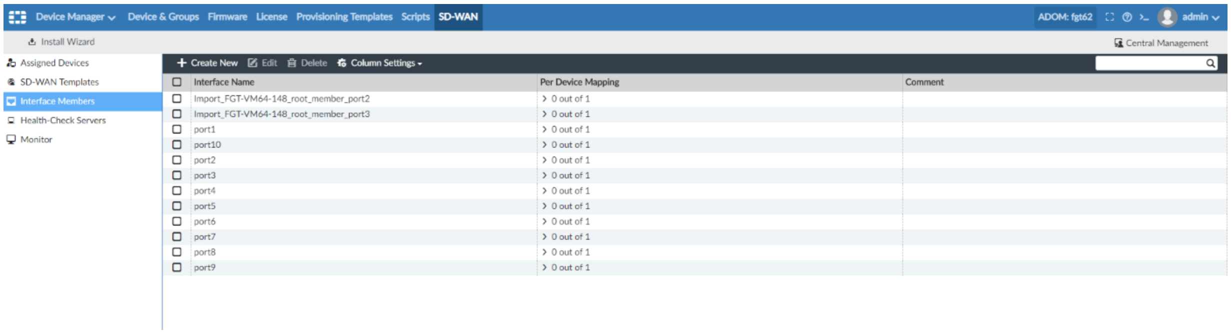
Performance SLA

□	#	Name	Detect Server	Detect Protocol	Failure Threshold	Recovery Threshold
□	1	lp_ts2	Import_FGT-VM64-148_root_health_lp_ts2	PING	5	5
□	2	ping2	Import_FGT-VM64-148_root_health_ping2	PING	5	5
□	3	ping3	Import_FGT-VM64-148_root_health_ping3	PING	5	5
□	4	ping_corp_gw	Import_FGT-VM64-148_root_health_ping_corp...	PING	5	5

SD-WAN Rules

□	#	Name	Source	Destination	Criteria	Members
□	1	rule01-auto	ALL	all	Latency (lp_ts2)	ALL
□	2	rule02-manual	ALL	all	Latency	Import_FGT-VM64-148_root_member_port3
□	3	rule03-priority	ALL	Microsoft-Skype	Latency (ping3)	Import_FGT-VM64-148_root_member_port2
□	4	rule04-sla	ALL	Microsoft-Skype	ping2#1	Import_FGT-VM64-148_root_member_port2
□	5	rule05-load-balance	ALL	Microsoft-Skype	ping_corp_gw#1	Import_FGT-VM64-148_root_member_port2

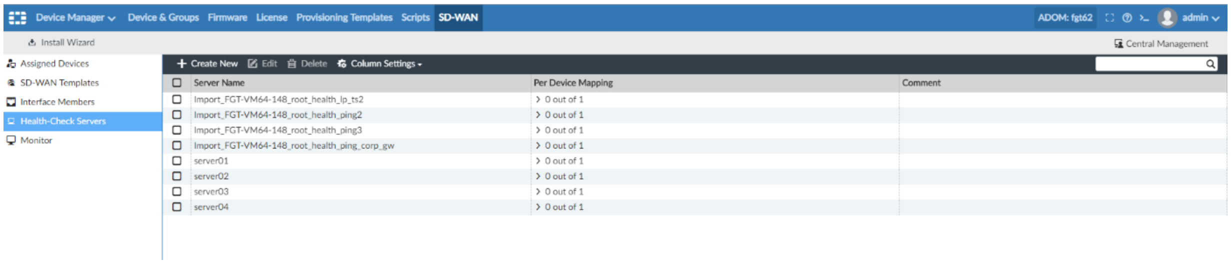
   - After import is completed, the Interface Members will generate a name like *Import_FGT-VM64-148_root_member_port2*. Default import name for member:*Import_{device-name}_{vdom-name}_member_{interface-name}*.



□	Interface Name	Per Device Mapping	Comment
□	Import_FGT-VM64-148_root_member_port2	> 0 out of 1	
□	Import_FGT-VM64-148_root_member_port3	> 0 out of 1	
□	port1	> 0 out of 1	
□	port10	> 0 out of 1	
□	port2	> 0 out of 1	
□	port3	> 0 out of 1	
□	port4	> 0 out of 1	
□	port5	> 0 out of 1	
□	port6	> 0 out of 1	
□	port7	> 0 out of 1	
□	port8	> 0 out of 1	
□	port9	> 0 out of 1	

   - After import is completed, the Health Check servers will generate a name like *Import_FGT-VM64-148_root_health_lp_ts2*. Default import name for member:*Import_{device-name}_{vdom-name}_health_{health-check-*

name}.



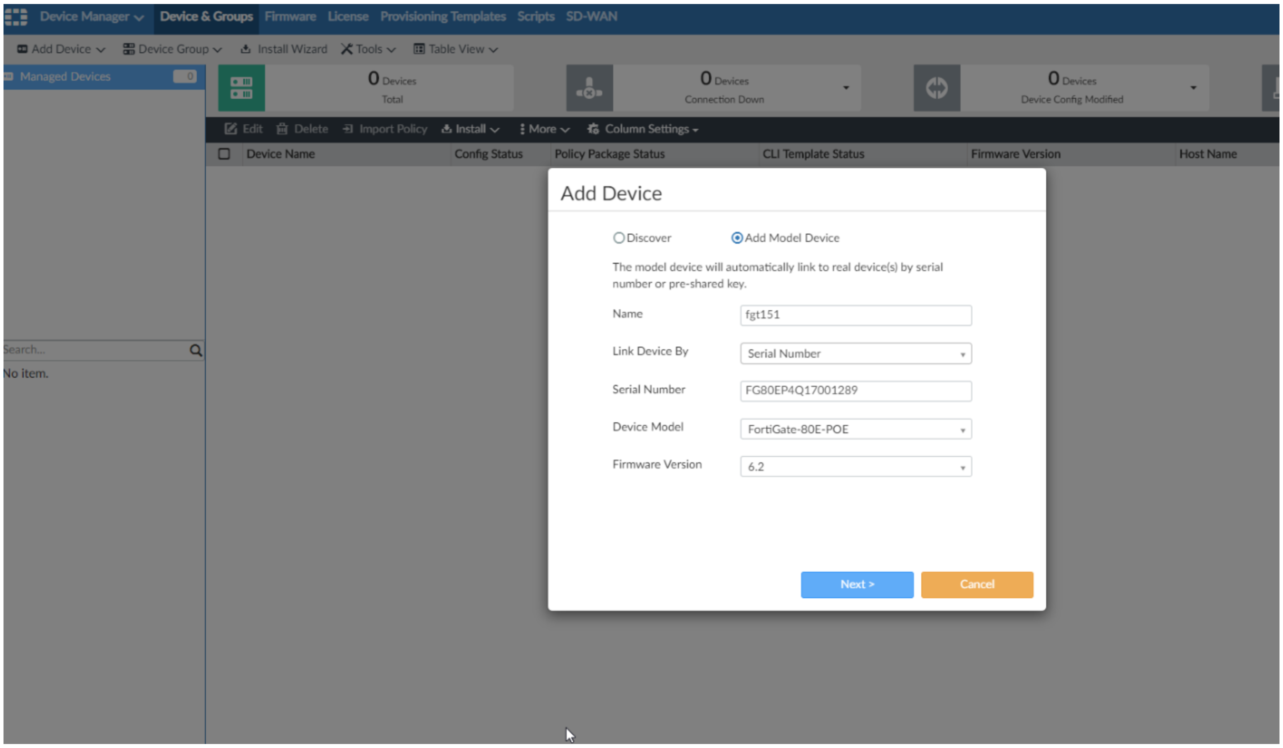
□	Server Name	Per Device Mapping	Comment
□	Import_FGT-VM64-148_root_health_lp_ts2	> 0 out of 1	
□	Import_FGT-VM64-148_root_health_ping2	> 0 out of 1	
□	Import_FGT-VM64-148_root_health_ping3	> 0 out of 1	
□	Import_FGT-VM64-148_root_health_ping_corp_gw	> 0 out of 1	
□	server01	> 0 out of 1	
□	server02	> 0 out of 1	
□	server03	> 0 out of 1	
□	server04	> 0 out of 1	

Zero-touch provisioning for FortiAP

Model devices used for ZTP can also be linked to model FortiSwitches, enabling provisioning of switch settings when first connected.

Pre-previsoning model FortiAP and link it to a model FortiGate

1. Create a Model FortiGate device by using a real FortiGate serial number.



Add Device

○ Discover ● Add Model Device

The model device will automatically link to real device(s) by serial number or pre-shared key.

Name: fgt151

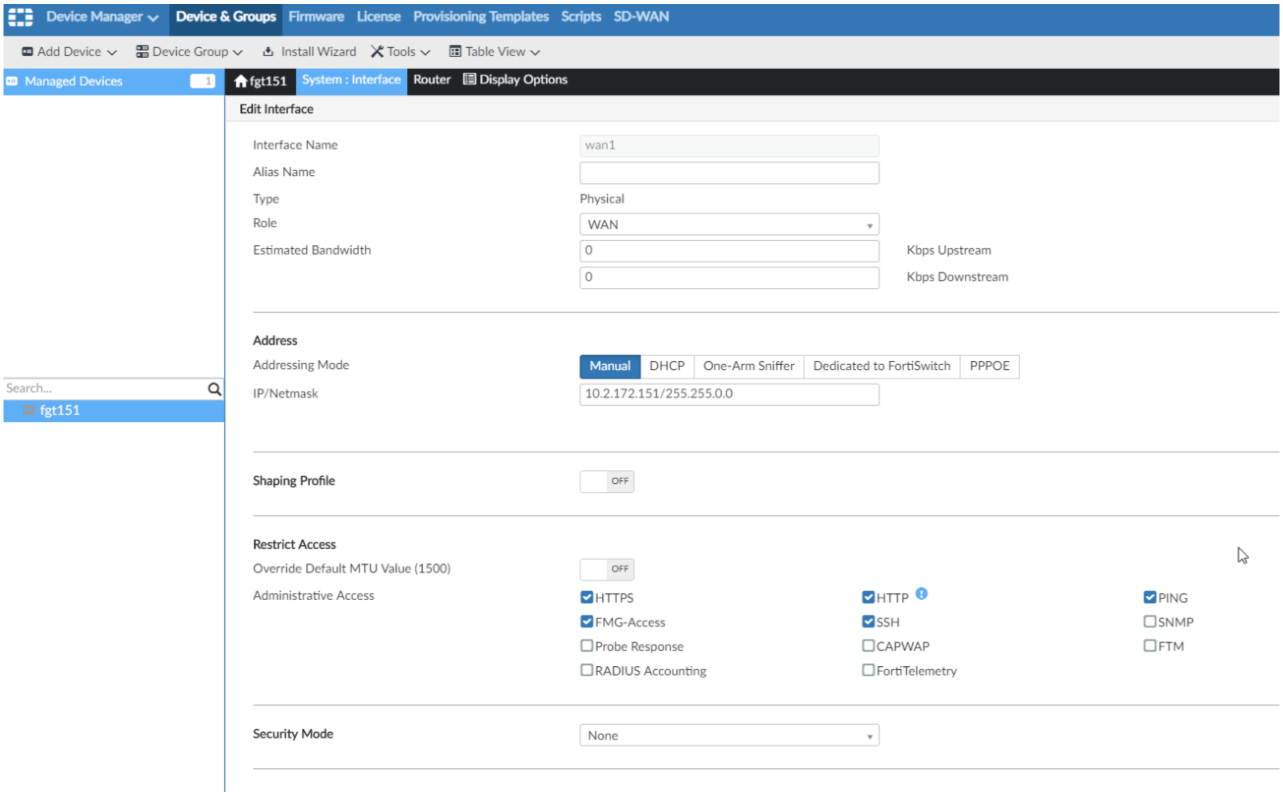
Link Device By: Serial Number

Serial Number: FG80EP4Q17001289

Device Model: FortiGate-80E-POE

Firmware Version: 6.2

2. Configure a model device interface IP, which will be used as the management IP by FortiManager.



Edit Interface

Interface Name: wan1
Alias Name:
Type: Physical
Role: WAN
Estimated Bandwidth: 0 Kbps Upstream
0 Kbps Downstream

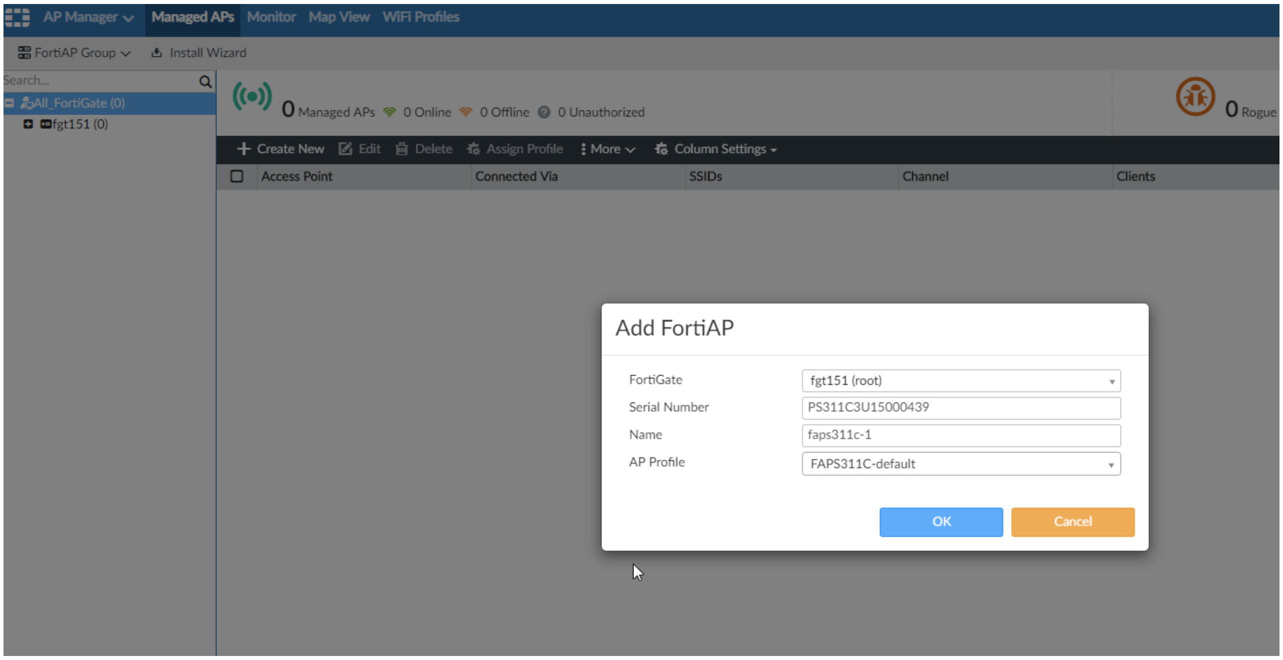
Address
Addressing Mode: Manual | DHCP | One-Arm Sniffer | Dedicated to FortiSwitch | PPPOE
IP/Netmask: 10.2.172.151/255.255.0.0

Shaping Profile: OFF

Restrict Access
Override Default MTU Value (1500): OFF
Administrative Access: ☑ HTTPS ☑ HTTP ☑ PING ☑ FMG-Access ☑ SSH □ SNMP □ Probe Response □ CAPWAP □ FTM □ RADIUS Accounting □ FortiTelemetry

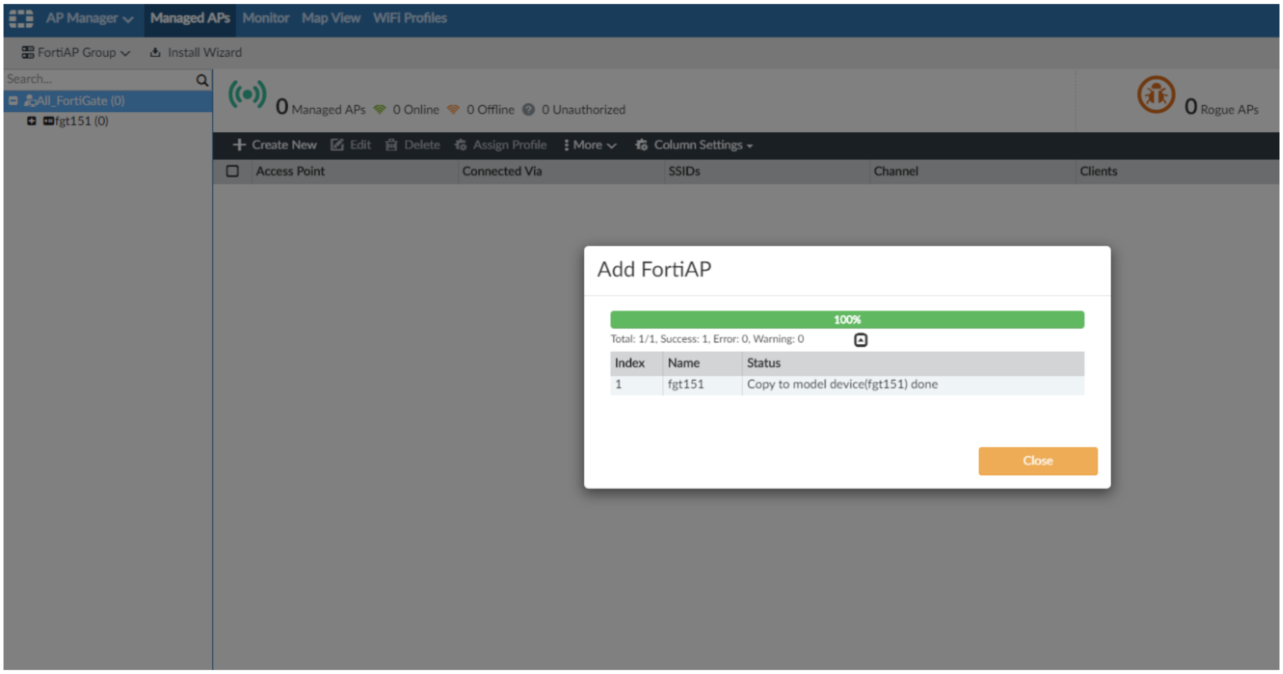
Security Mode: None

3. In AP Manager, create model APs on the model FortiGate by using a real FortiAP serial number.



Add FortiAP

FortiGate: fgt151 (root)
Serial Number: PS311C3U15000439
Name: faps311c-1
AP Profile: FAPS311C-default

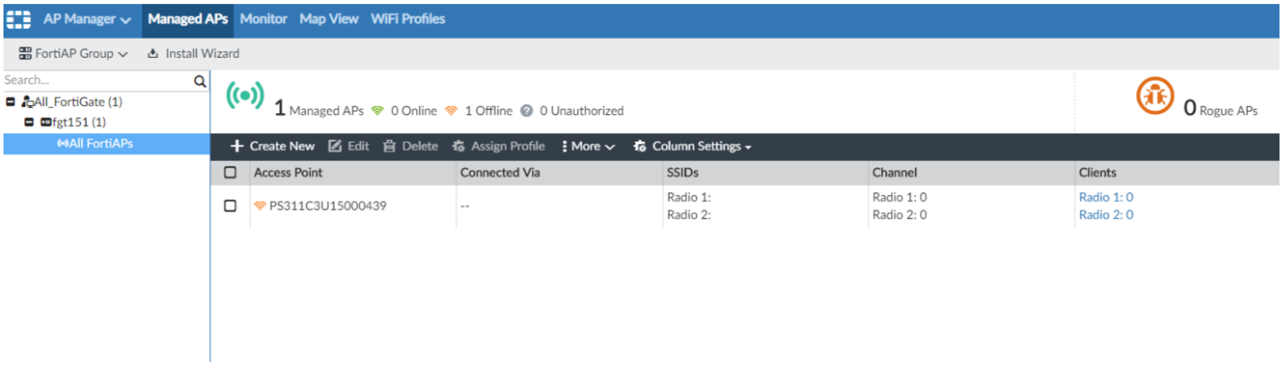


Add FortiAP

100%

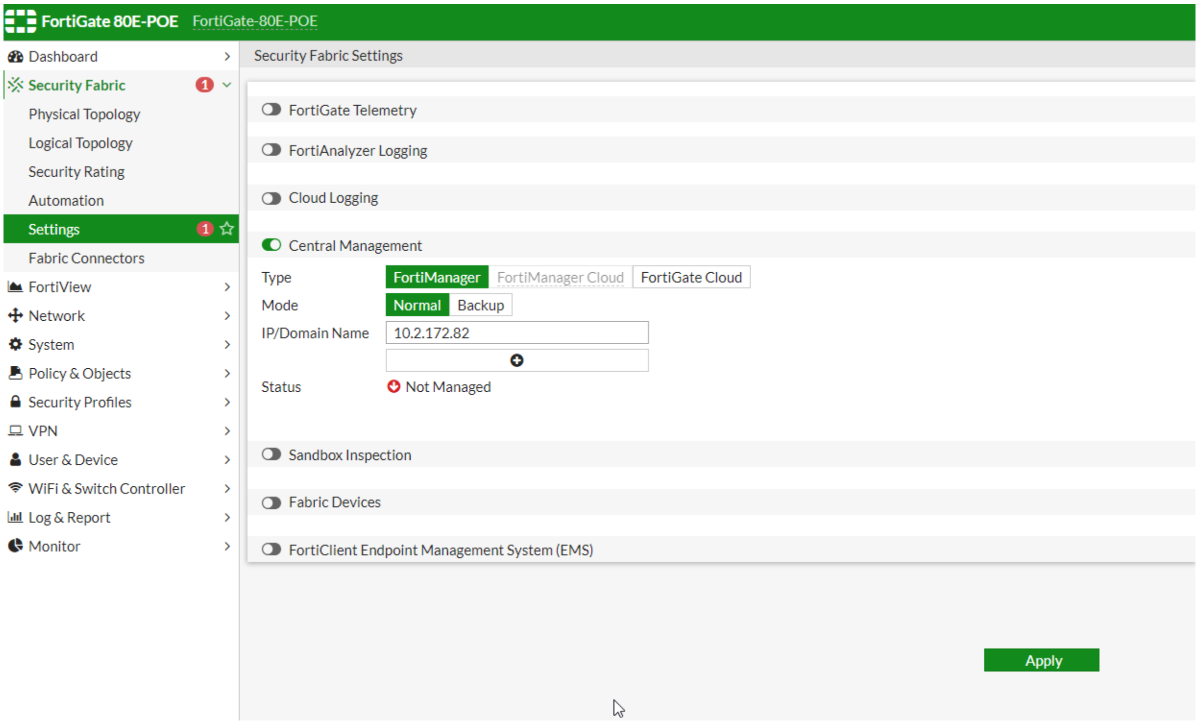
Total: 1/1, Success: 1, Error: 0, Warning: 0

Index	Name	Status
1	fgt151	Copy to model device(fgt151) done



□	Access Point	Connected Via	SSIDs	Channel	Clients
□	PS311C3U15000439	--	Radio 1: Radio 2:	Radio 1: 0 Radio 2: 0	Radio 1: 0 Radio 2: 0

4. Connect the physical AP to the real FortiGate, and connect the FortiGate with FortiManager through the network.
5. Log on to FortiGate. Go to *Security Fabric* > *Settings*, configure Central Management to FortiManager. (You can also use other methods to let FortiGate learn FortiManager IP and trigger FortiManager model device auto-link function).



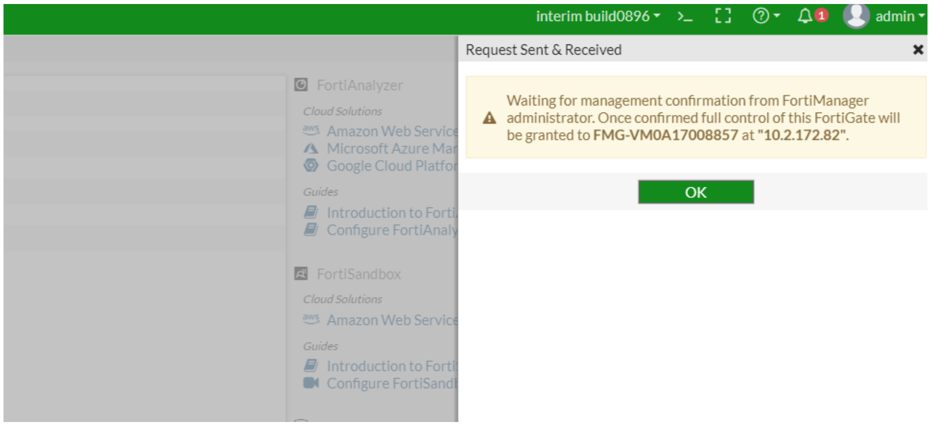
Type: FortiManager | FortiManager Cloud | FortiGate Cloud

Mode: Normal | Backup

IP/Domain Name: 10.2.172.82

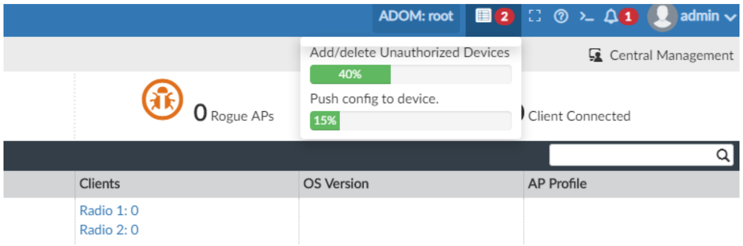
Status: Not Managed

6. Click *Apply* to apply the settings and click *OK* to confirm the grant to FortiManager.



Waiting for management confirmation from FortiManager administrator. Once confirmed full control of this FortiGate will be granted to **FMG-VM0A17008857** at **"10.2.172.82"**.

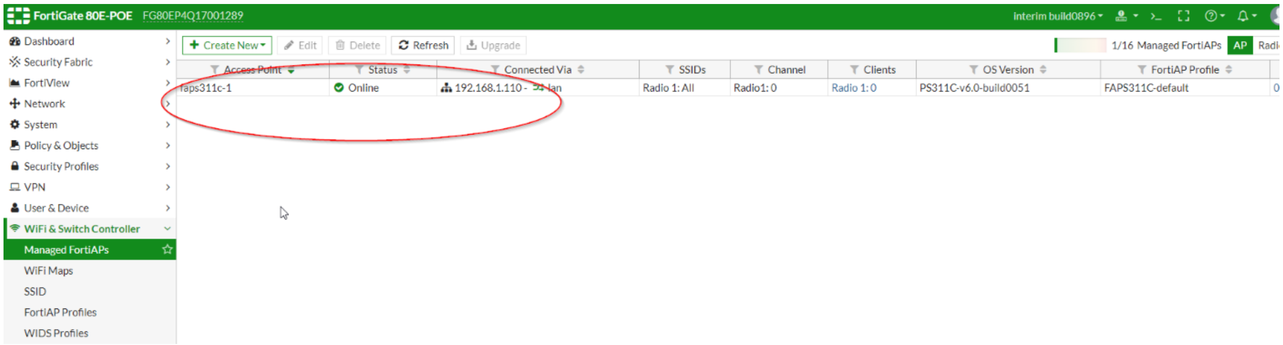
7. Go back to FortiManager to double-check the auto-link function status with the real FortiGate.



Add/delete Unauthorized Devices 40%

Push config to device. 15%

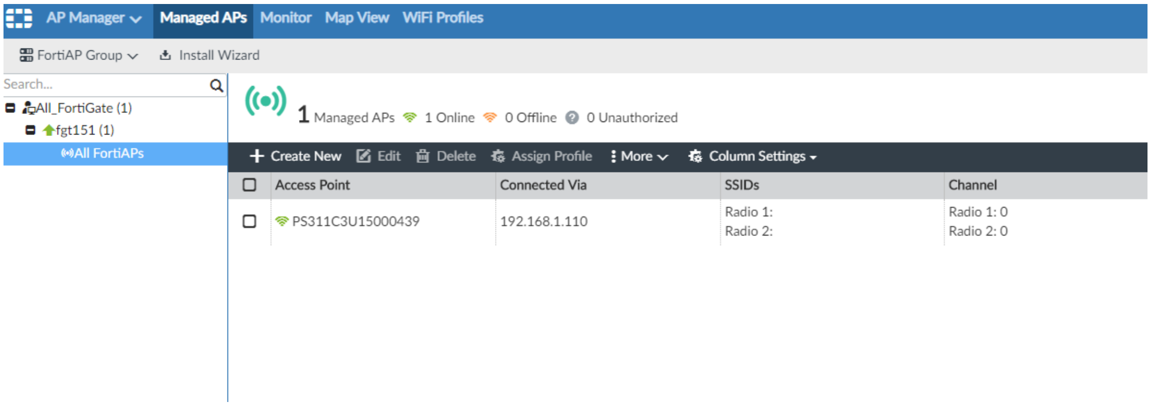
8. After the configuration is pushed to FortiGate, access FortiGate and verify that the FortiAP is enabled and displayed in Managed FortiAPs page.



FortiGate 80E-POE FG80EP4Q17001289

Access Point	Status	Connected Via	SSIDs	Channel	Clients	OS Version	FortiAP Profile
faps311c-1	Online	192.168.1.110 - lan	Radio 1: All	Radio1: 0	Radio 1: 0	PS311C-v6.0-build0051	FAPS311C-default

9. Log on to FortiManager. Go to *AP Manager > Managed APs*. The AP is now displayed as online.



1 Managed APs 1 Online 0 Offline 0 Unauthorized

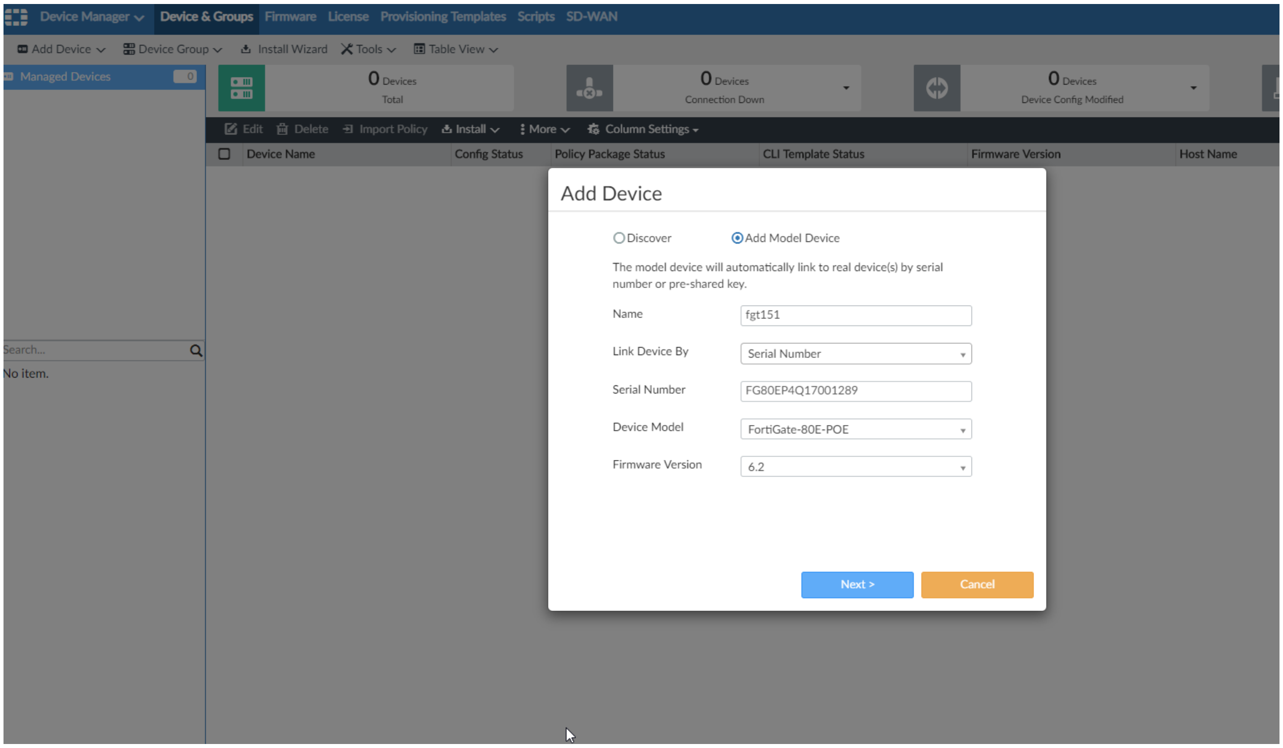
Access Point	Connected Via	SSIDs	Channel
PS311C3U15000439	192.168.1.110	Radio 1: Radio 2:	Radio 1: 0 Radio 2: 0

Zero-touch provisioning for FortiSwitch

Model devices used for ZTP can also be linked to model FortiAPs, enabling provisioning of AP settings when first connected.

Scenario 1: When FortiGate is provisioned as a Model Device and uses auto-link for zero-touch install

1. Create a model FortiGate device by using a real FortiGate serial number.



Add Device

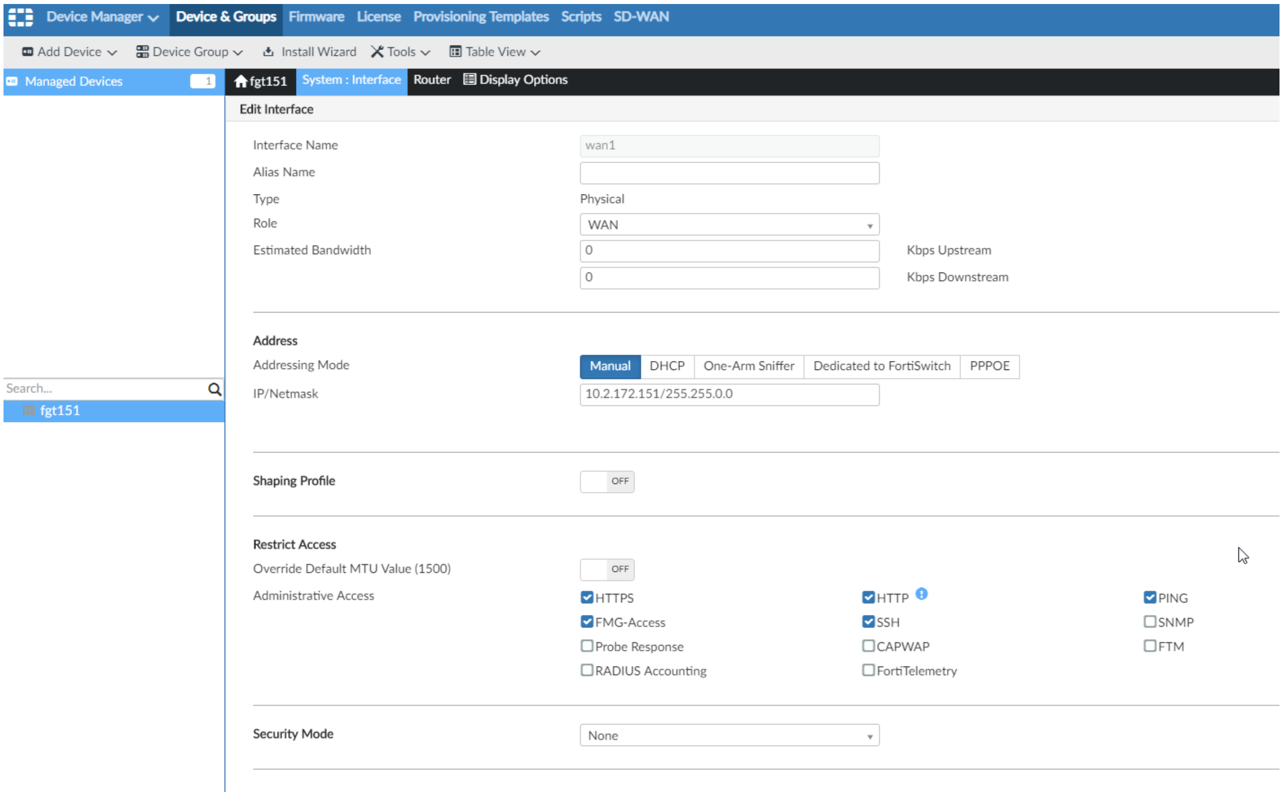
○ Discover ● Add Model Device

The model device will automatically link to real device(s) by serial number or pre-shared key.

Name	fgt151
Link Device By	Serial Number
Serial Number	FG80EP4Q17001289
Device Model	FortiGate-80E-POE
Firmware Version	6.2

Next > Cancel

2. Configure a model device interface IP, which will be used as the management IP to FortiManager.



Edit Interface

Interface Name: wan1
Alias Name:
Type: Physical
Role: WAN
Estimated Bandwidth: 0 Kbps Upstream; 0 Kbps Downstream

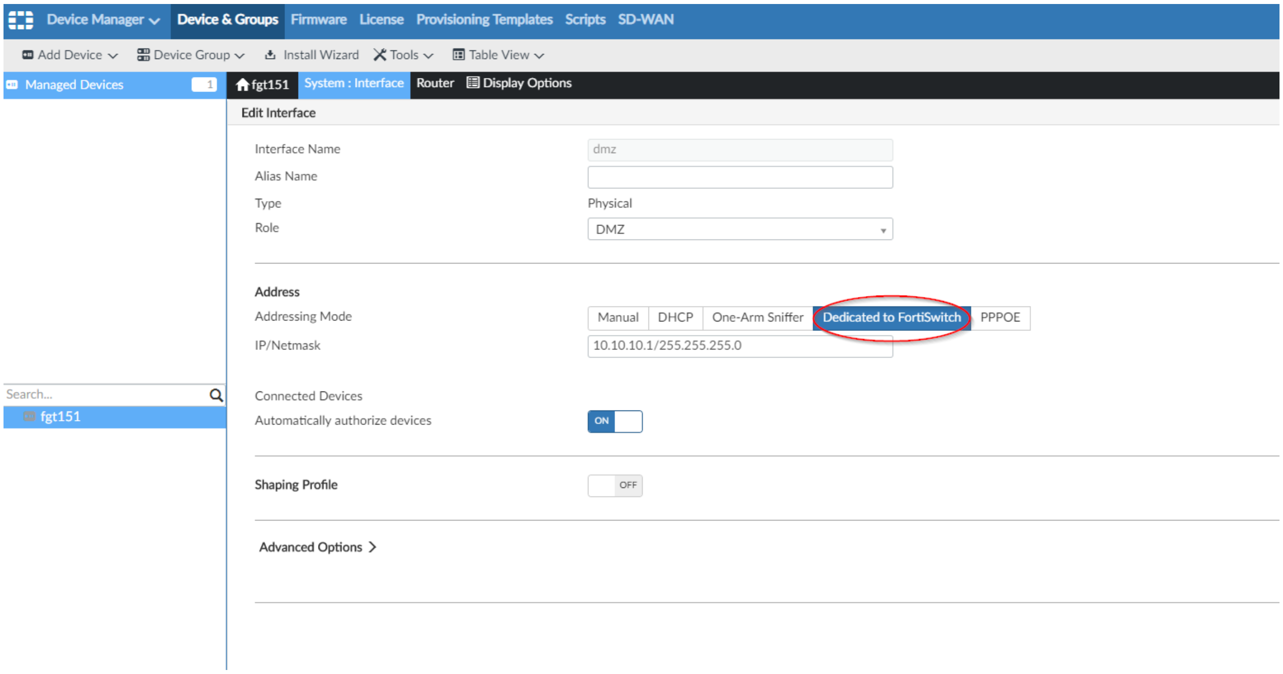
Address
Addressing Mode: [✓ Manual] DHCP One-Arm Sniffer Dedicated to FortiSwitch PPPOE
IP/Netmask: 10.2.172.151/255.255.0.0

Shaping Profile: OFF

Restrict Access
Override Default MTU Value (1500): OFF
Administrative Access:
☑ HTTPS ☑ HTTP ☑ PING
☑ FMG-Access ☑ SSH □ SNMP
□ Probe Response □ CAPWAP □ FTM
□ RADIUS Accounting □ FortiTelemetry

Security Mode: None

3. In the model device, choose the interface which will be used to connect FortiSwitch, enable FortiSwitch and specify the IP address.



Edit Interface

Interface Name: dmz
Alias Name:
Type: Physical
Role: DMZ

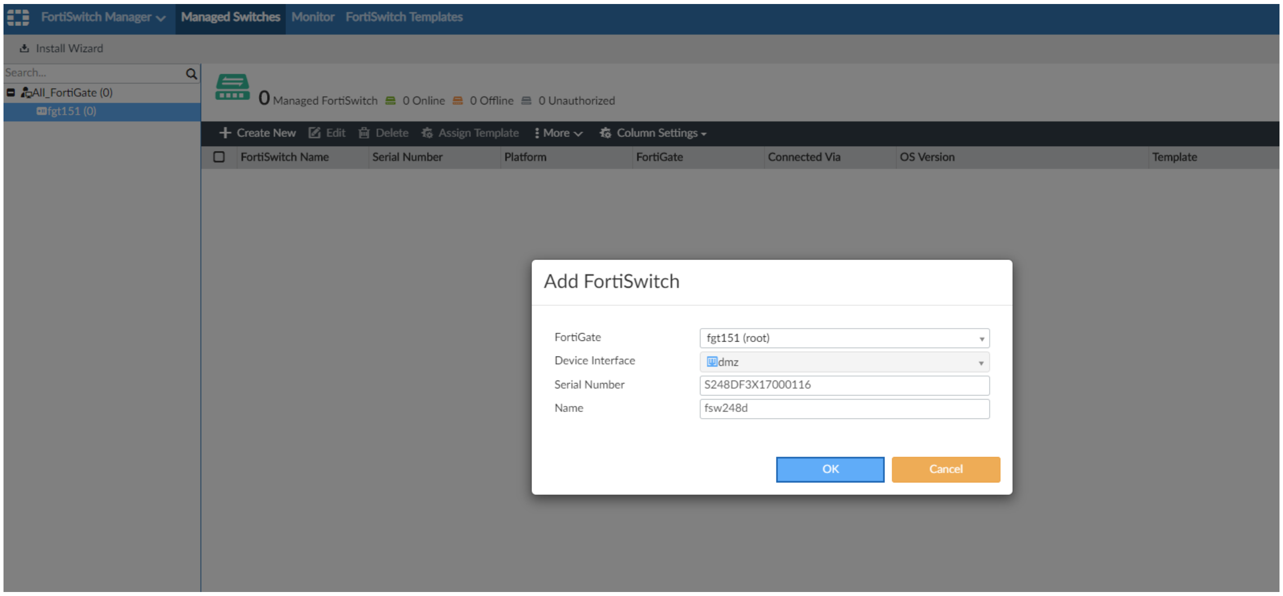
Address
Addressing Mode: Manual DHCP One-Arm Sniffer [✓ Dedicated to FortiSwitch] PPPOE
IP/Netmask: 10.10.10.1/255.255.255.0

Connected Devices
Automatically authorize devices: ON

Shaping Profile: OFF

Advanced Options >

4. In FortiSwitch Manager, create a model FortiSwitch on the FortiGate by using a real FortiSwitch serial number.

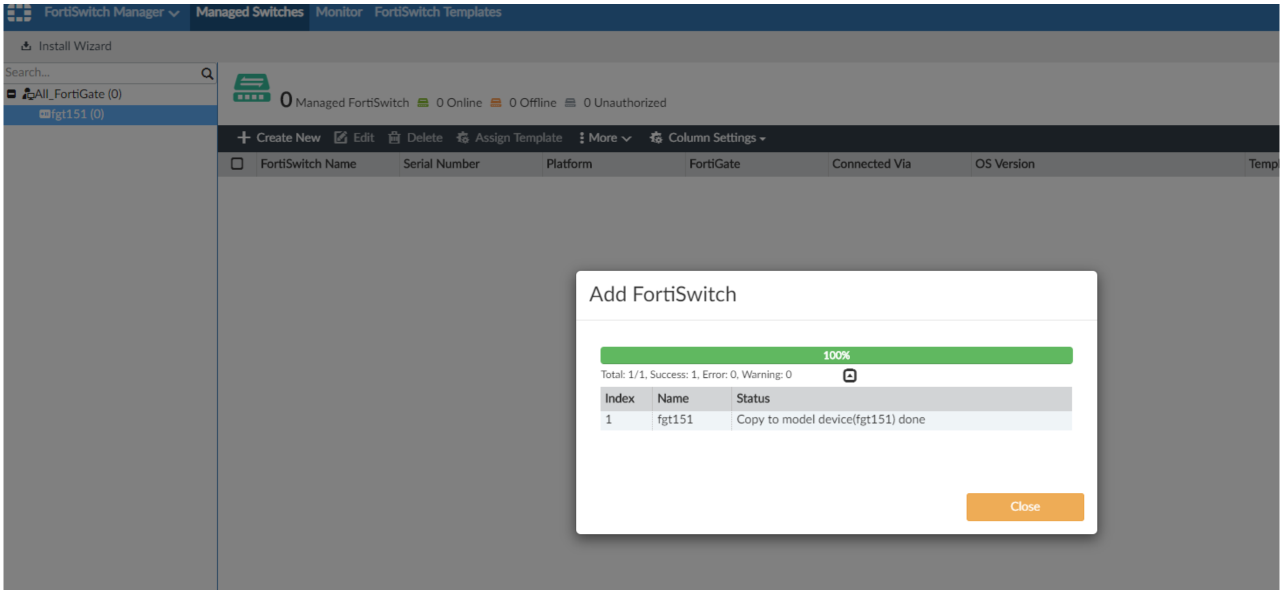


0 Managed FortiSwitch 0 Online 0 Offline 0 Unauthorized

□	FortiSwitch Name	Serial Number	Platform	FortiGate	Connected Via	OS Version	Template

Add FortiSwitch

FortiGate	fgt151 (root)
Device Interface	dmz
Serial Number	S248DF3X17000116
Name	fsw248d



0 Managed FortiSwitch 0 Online 0 Offline 0 Unauthorized

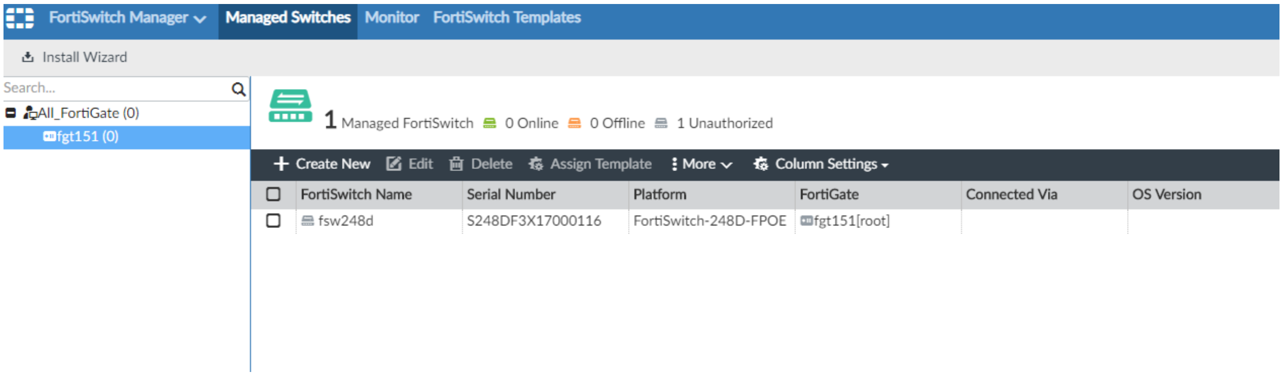
□	FortiSwitch Name	Serial Number	Platform	FortiGate	Connected Via	OS Version	Templ

Add FortiSwitch

100%

Total: 1/1, Success: 1, Error: 0, Warning: 0

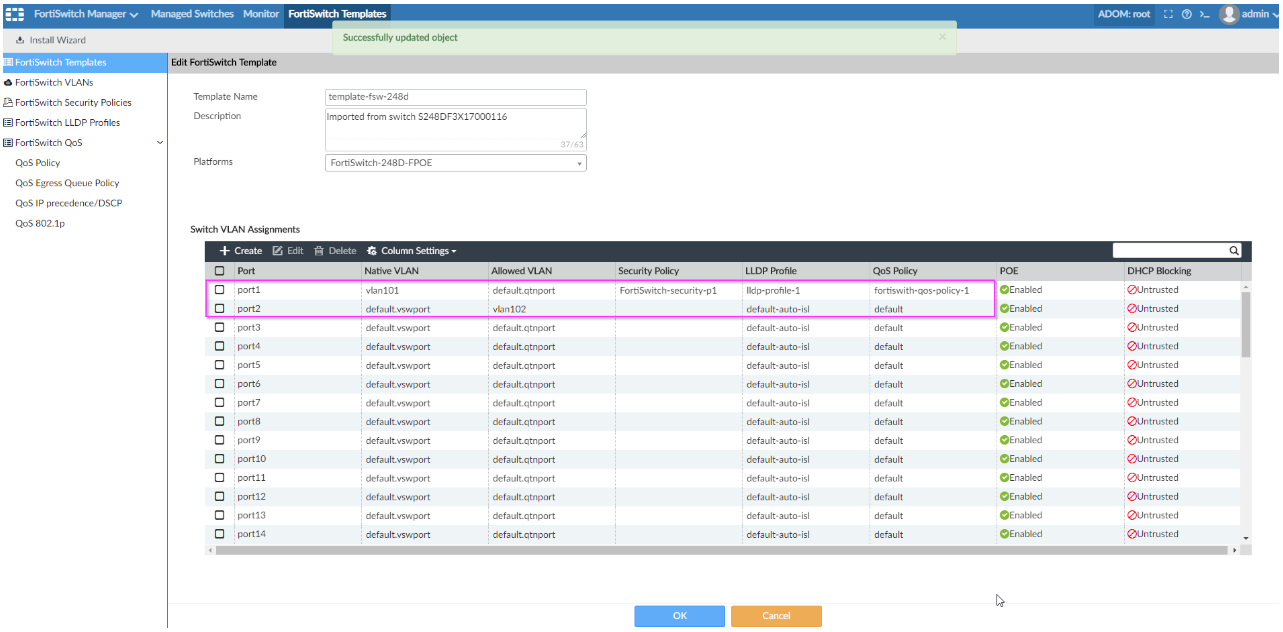
Index	Name	Status
1	fgt151	Copy to model device(fgt151) done



1 Managed FortiSwitch 0 Online 0 Offline 1 Unauthorized

□	FortiSwitch Name	Serial Number	Platform	FortiGate	Connected Via	OS Version
□	fsw248d	S248DF3X17000116	FortiSwitch-248D-FPOE	fgt151[root]		

5. In *FortiSwitch Manager > FortiSwitch Template*, create a FortiSwitch template, modify port settings and assign it to the model FortiSwitch.



Successfully updated object

Edit FortiSwitch Template

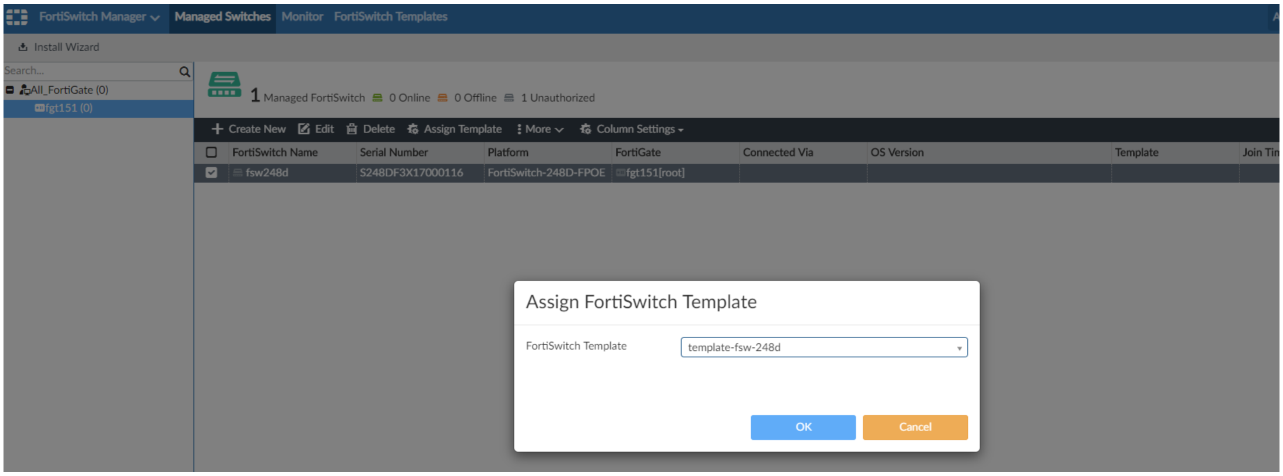
Template Name: template-fsw-248d

Description: Imported from switch S248DF3X17000116 (37/63)

Platforms: FortiSwitch-248D-FPOE

Switch VLAN Assignments

□	Port	Native VLAN	Allowed VLAN	Security Policy	LLDP Profile	QoS Policy	POE	DHCP Blocking
□	port1	vlan101	default.qtnport	FortiSwitch-security-p1	lldp-profile-1	fortiswith-qos-policy-1	Enabled	Untrusted
□	port2	default.vswport	vlan102		default-auto-isl	default	Enabled	Untrusted
□	port3	default.vswport	default.qtnport		default-auto-isl	default	Enabled	Untrusted
□	port4	default.vswport	default.qtnport		default-auto-isl	default	Enabled	Untrusted
□	port5	default.vswport	default.qtnport		default-auto-isl	default	Enabled	Untrusted
□	port6	default.vswport	default.qtnport		default-auto-isl	default	Enabled	Untrusted
□	port7	default.vswport	default.qtnport		default-auto-isl	default	Enabled	Untrusted
□	port8	default.vswport	default.qtnport		default-auto-isl	default	Enabled	Untrusted
□	port9	default.vswport	default.qtnport		default-auto-isl	default	Enabled	Untrusted
□	port10	default.vswport	default.qtnport		default-auto-isl	default	Enabled	Untrusted
□	port11	default.vswport	default.qtnport		default-auto-isl	default	Enabled	Untrusted
□	port12	default.vswport	default.qtnport		default-auto-isl	default	Enabled	Untrusted
□	port13	default.vswport	default.qtnport		default-auto-isl	default	Enabled	Untrusted
□	port14	default.vswport	default.qtnport		default-auto-isl	default	Enabled	Untrusted



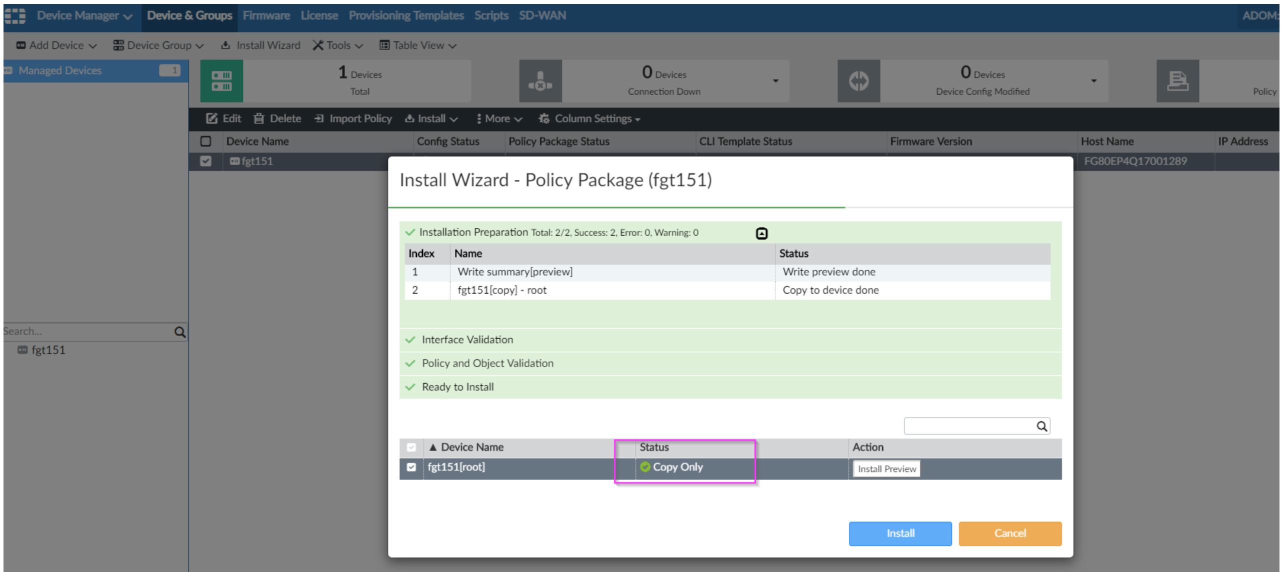
1 Managed FortiSwitch 0 Online 0 Offline 1 Unauthorized

□	FortiSwitch Name	Serial Number	Platform	FortiGate	Connected Via	OS Version	Template	Join Tin
☑	fsw248d	S248DF3X17000116	FortiSwitch-248D-FPOE	fgt151[root]				

Assign FortiSwitch Template

FortiSwitch Template: template-fsw-248d

6. Create a policy package for the model device, then do a policy copy and perform a *Copy Only* to the model FortiGate.



Install Wizard - Policy Package (fgt151)

✓ Installation Preparation Total: 2/2, Success: 2, Error: 0, Warning: 0

Index	Name	Status
1	Write summary[preview]	Write preview done
2	fgt151[copy] - root	Copy to device done

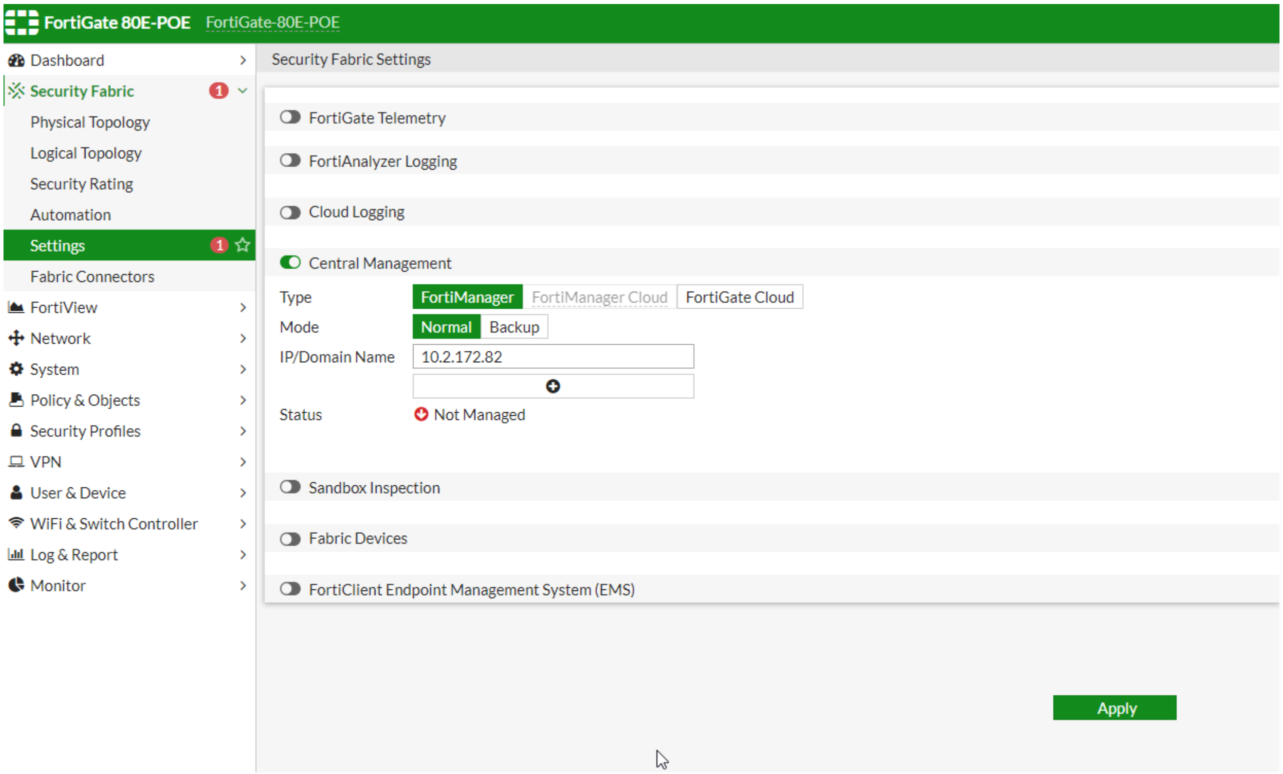
✓ Interface Validation

✓ Policy and Object Validation

✓ Ready to Install

☐	▲ Device Name	Status	Action
☑	fgt151[root]	Copy Only	Install Preview

7. Connect the real FortiSwitch to the real FortiGate, and connect the FortiGate to the network that FortiManager can reach.
8. Log on to FortiGate. Go to *Security Fabric* > *Settings* and configure central management to connect to FortiManager. (You can also use other method to let FortiGate learn FortiManager IP and trigger FortiManager model device auto-link function.)



Security Fabric Settings

○ FortiGate Telemetry

○ FortiAnalyzer Logging

○ Cloud Logging

● Central Management

Type: [✓ FortiManager] FortiManager Cloud FortiGate Cloud

Mode: [✓ Normal] Backup

IP/Domain Name: 10.2.172.82

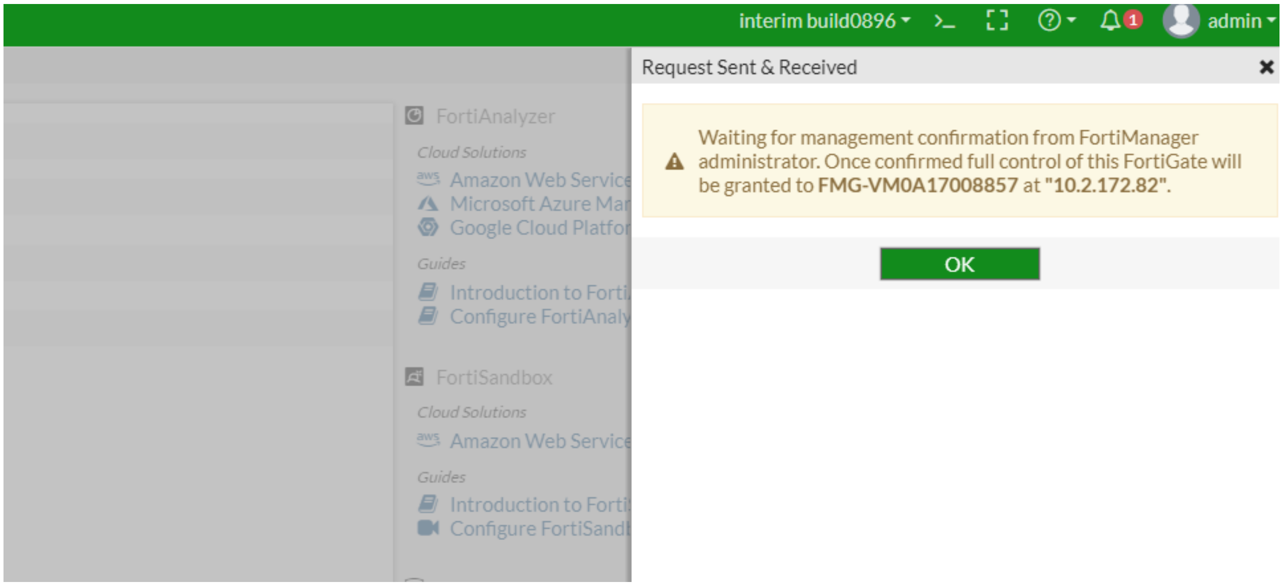
Status: Not Managed

○ Sandbox Inspection

○ Fabric Devices

○ FortiClient Endpoint Management System (EMS)

9. Click *Apply* to apply the settings and click OK to agree the grant to FortiManager.

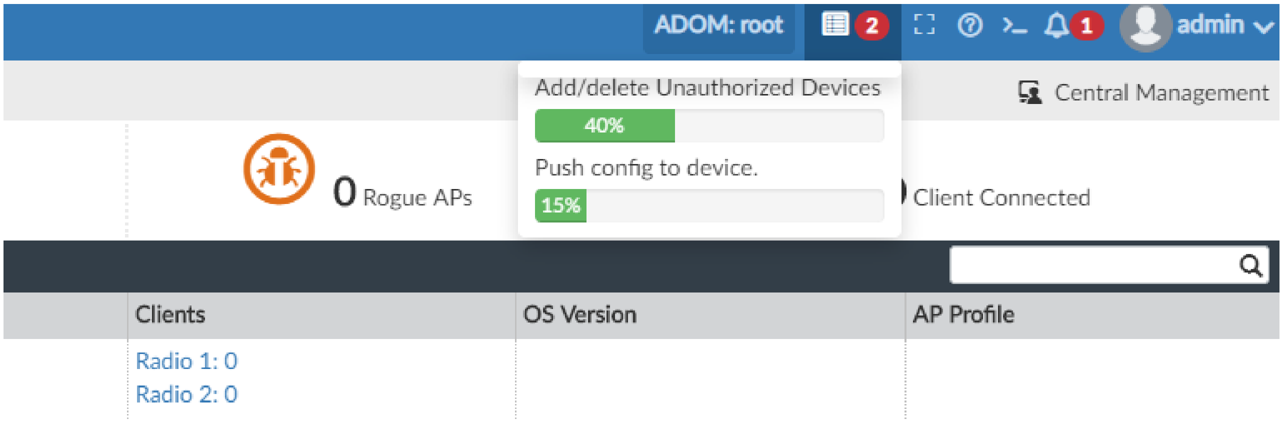


Request Sent & Received

Waiting for management confirmation from FortiManager administrator. Once confirmed full control of this FortiGate will be granted to **FMG-VM0A17008857** at **"10.2.172.82"**.

OK

10. Go back to FortiManager and double check model device auto link function status with the real FortiGate.



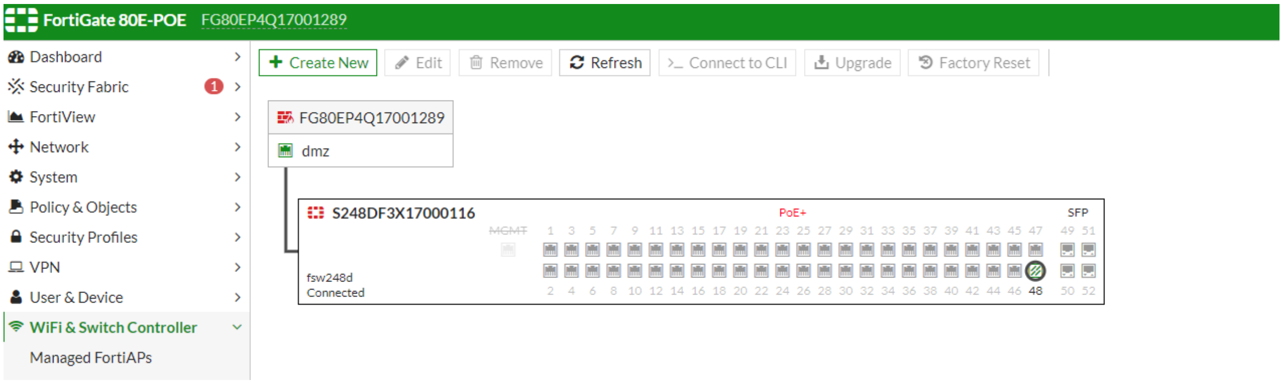
Add/delete Unauthorized Devices

40%

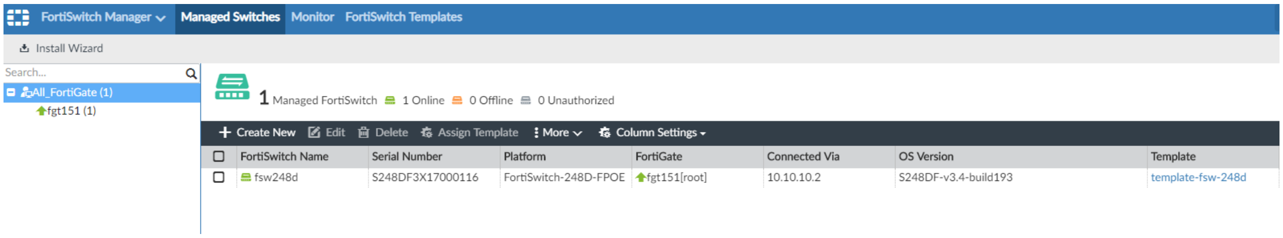
Push config to device.

15%

11. After the configuration is pushed to FortiGate, access FortiGate and verify that the FortiSwitch is enabled and displayed in FortiGate.



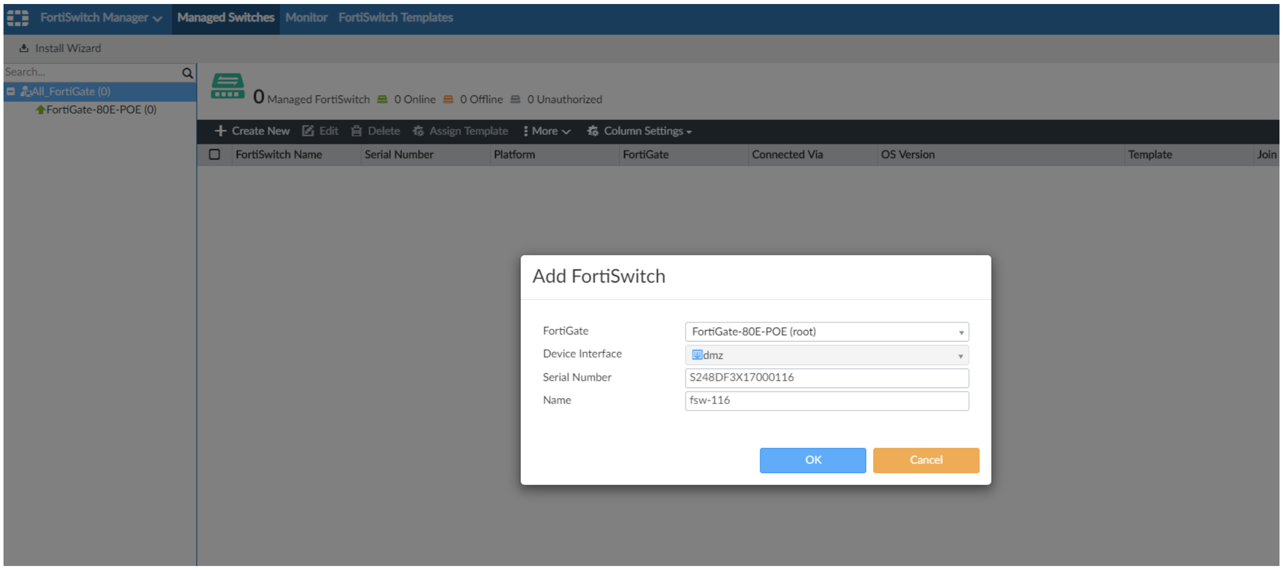
12. Go to *FortiManager* > *FortiSwitch Manager* > *Managed FortiSwitches*. You can see the FortiGate status is up and FortiSwitch is now online.



	FortiSwitch Name	Serial Number	Platform	FortiGate	Connected Via	OS Version	Template
□	fsw248d	S248DF3X17000116	FortiSwitch-248D-FPOE	fgt151[root]	10.10.10.2	S248DF-v3.4-build193	template-fsw-248d

Scenario 2: FortiGate is already managed by FortiManager

1. Log on to FortiManager. Go to *FortiSwitch Manager* > *Managed Switches*and click *Create New*. Choose FortiGate and FortiLink interface, enter the serial number, name, and click *OK*.

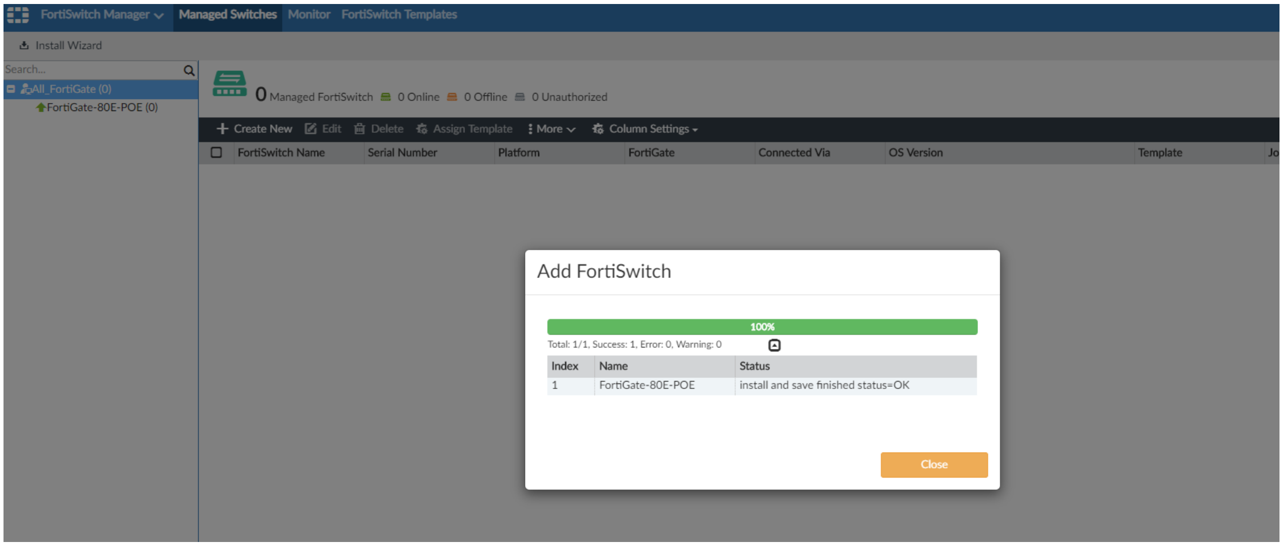


FortiGate: FortiGate-80E-POE (root)

Device Interface: dmz

Serial Number: S248DF3X17000116

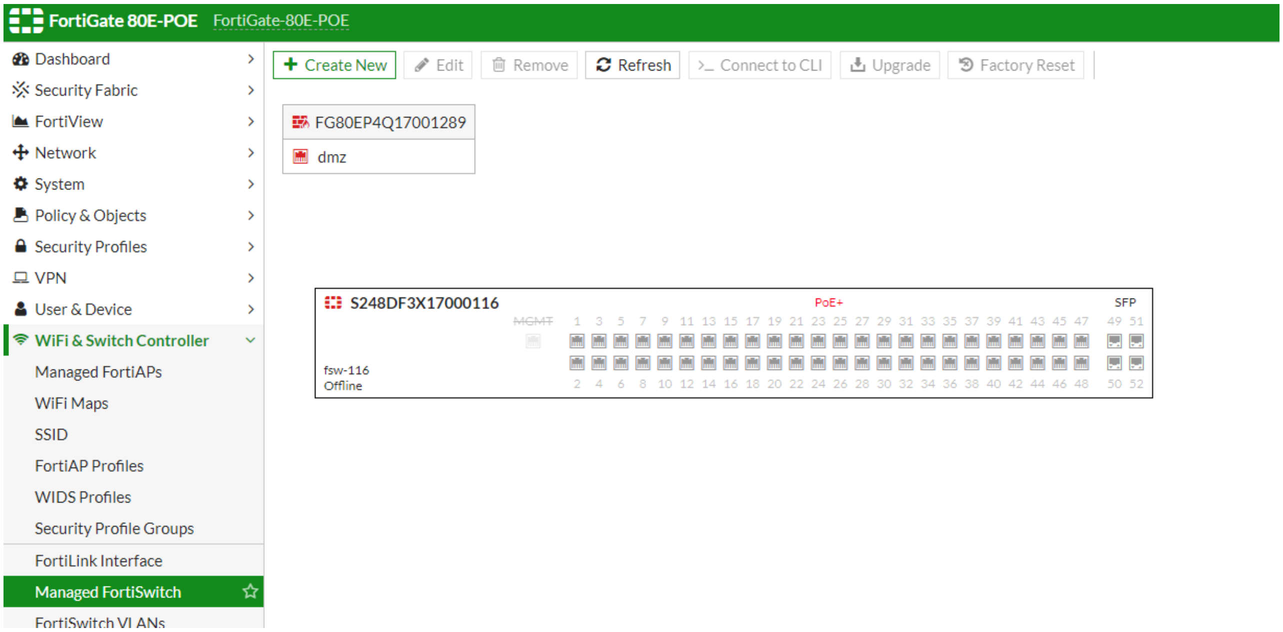
Name: fsw-116



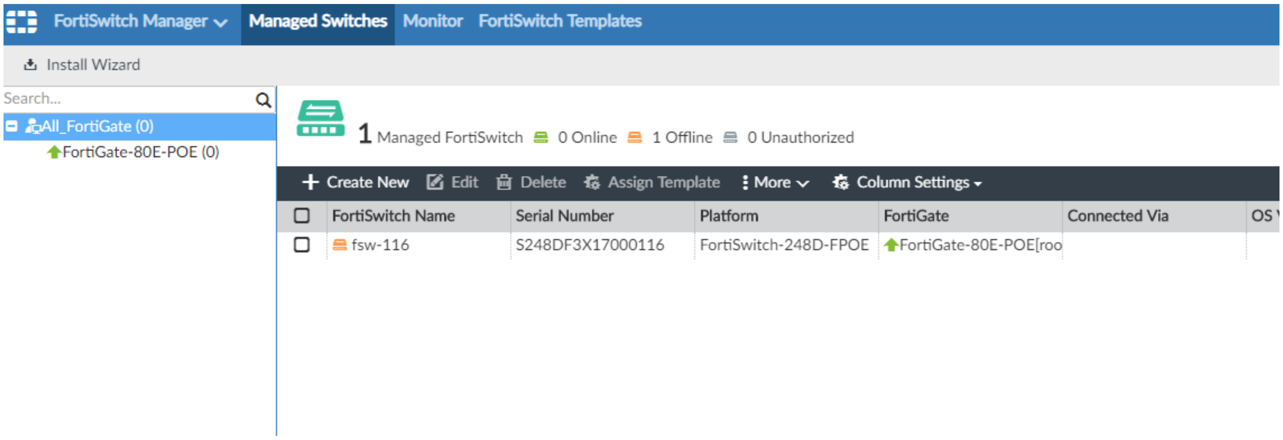
Total: 1/1, Success: 1, Error: 0, Warning: 0

Index	Name	Status
1	FortiGate-80E-POE	install and save finished status=OK

2. Log on to FortiGate. Go to *WiFi & Switch Controller* > *Managed FortiSwitch* and verify that the model FortiSwitch has been deployed.

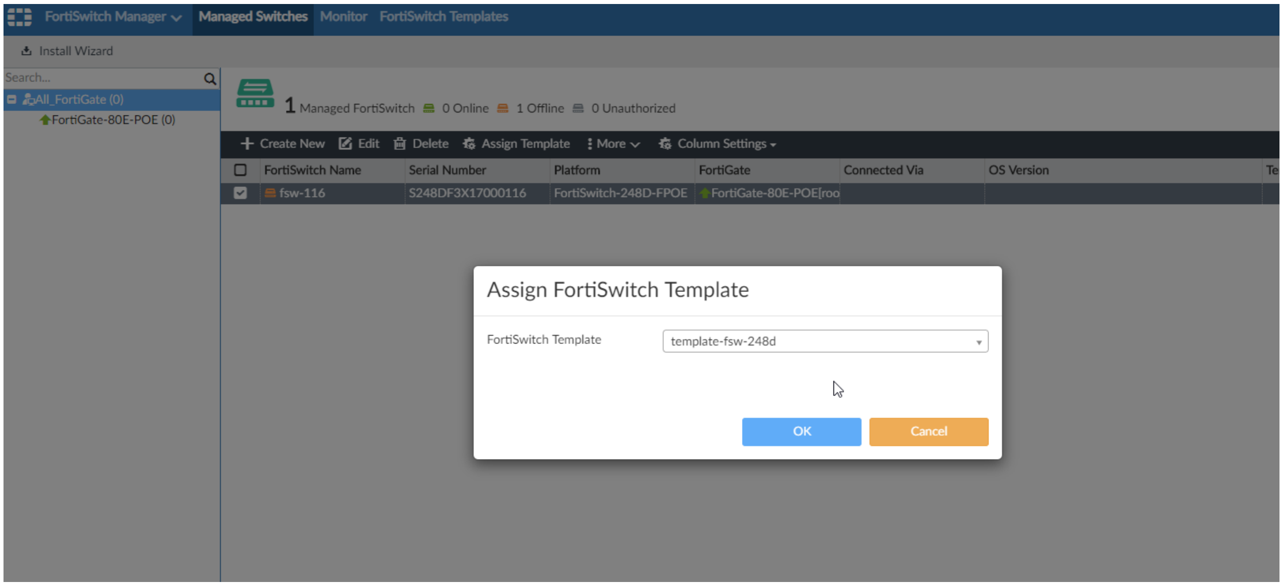


3. Go to FortiManager. Go to *FortiSwitch Manager* > *Managed Switches* and verify that the model switch is also displayed.



□	FortiSwitch Name	Serial Number	Platform	FortiGate	Connected Via	OS \
□	fsw-116	S248DF3X17000116	FortiSwitch-248D-FPOE	FortiGate-80E-POE[roo		

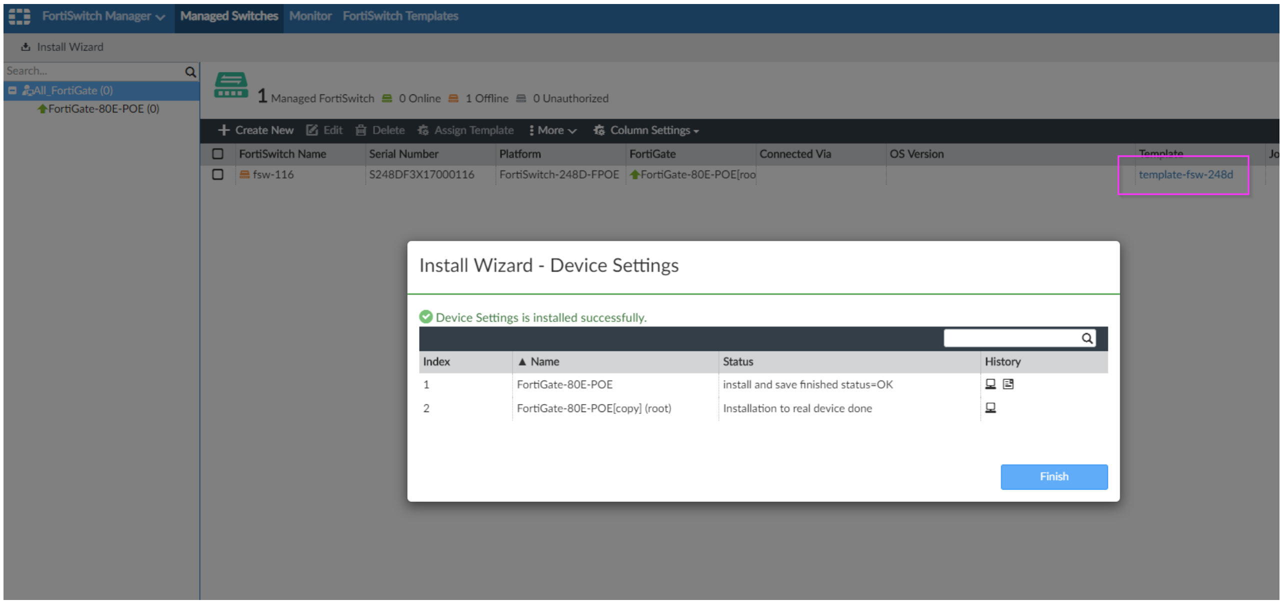
4. Assign the FortiSwitch template to the model FortiSwitch and deploy the template configuration to FortiGate.



☐	FortiSwitch Name	Serial Number	Platform	FortiGate	Connected Via	OS Version	Te
☑	fsw-116	S248DF3X17000116	FortiSwitch-248D-FPOE	FortiGate-80E-POE[roo			

Assign FortiSwitch Template

FortiSwitch Template: template-fsw-248d



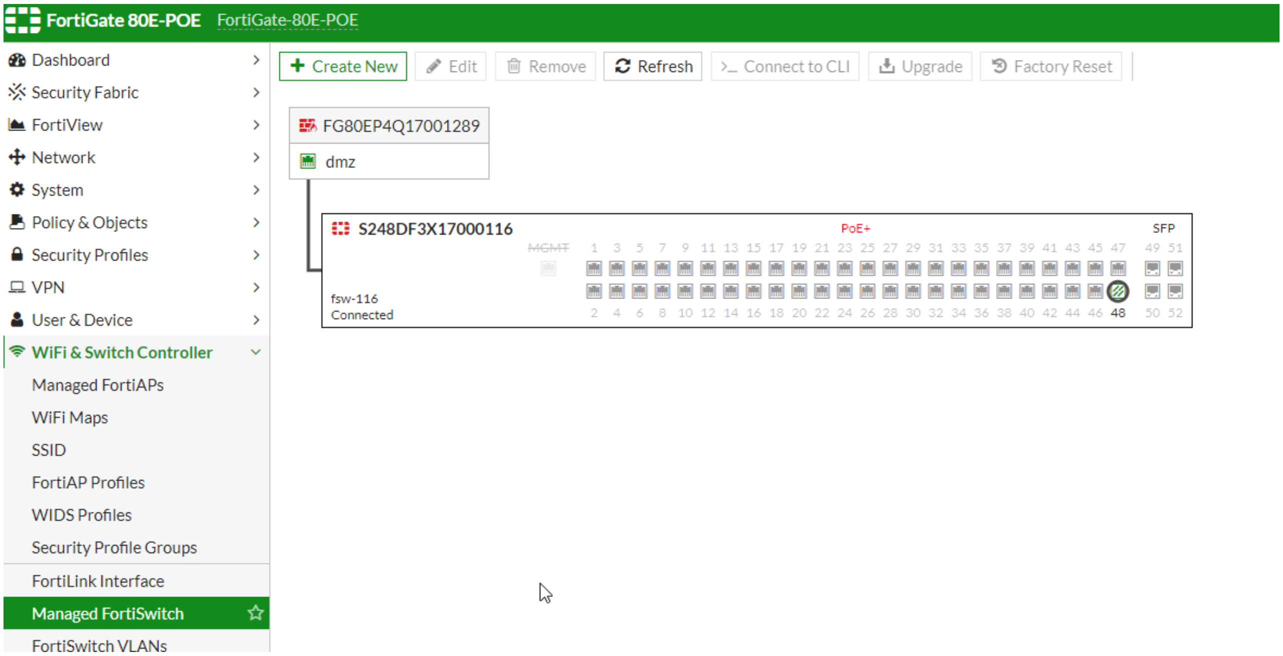
☐	FortiSwitch Name	Serial Number	Platform	FortiGate	Connected Via	OS Version	Template	Jo
☐	fsw-116	S248DF3X17000116	FortiSwitch-248D-FPOE	FortiGate-80E-POE[roo			template-fsw-248d	

Install Wizard - Device Settings

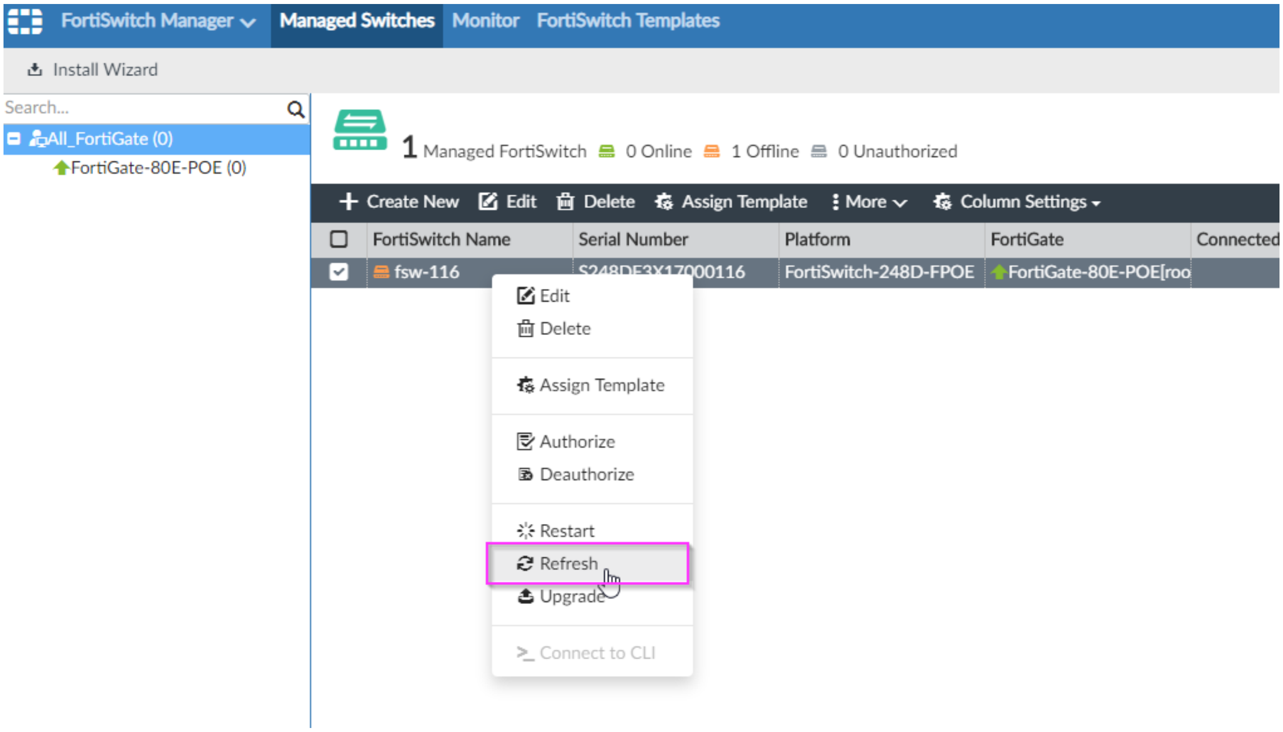
Device Settings is installed successfully.

Index	▲ Name	Status	History
1	FortiGate-80E-POE	install and save finished status=OK	🖥 🗎
2	FortiGate-80E-POE[copy] (root)	Installation to real device done	🖥

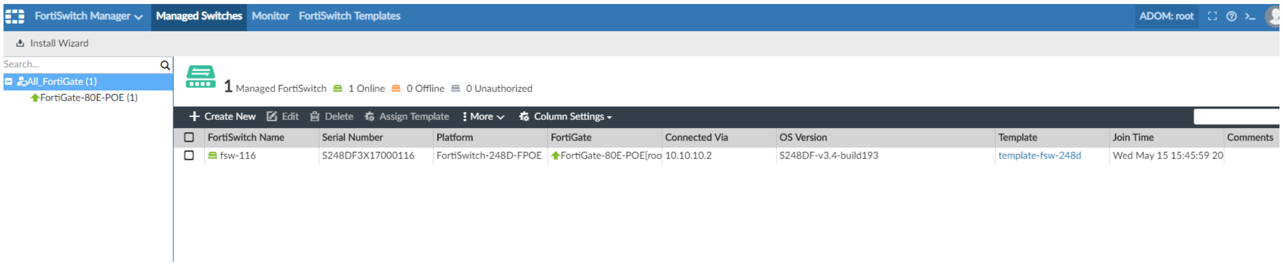
5. Connect the real FortiSwitch to the FortiGate by using FortiLink port and start the FortiSwitch. After FortiLink negotiation, the FortiSwitch is connected with FortiGate and its status is *online*.



6. Go back to *FortiManager > FortiSwitch Manager*, right-click the managed FortiSwitch and click *Refresh*. The FortiSwitch status will displayed as *Online*.



☐	FortiSwitch Name	Serial Number	Platform	FortiGate	Connected
☑	fsw-116	S248DF3X17000116	FortiSwitch-248D-FPOE	FortiGate-80E-POE[roo	



□	FortiSwitch Name	Serial Number	Platform	FortiGate	Connected Via	OS Version	Template	Join Time	Comments
□	fsw-116	S248DF3X17000116	FortiSwitch-248D-FPOE	FortiGate-80E-POE[roo	10.10.10.2	S248DF-v3.4-build193	template-fsw-248d	Wed May 15 15:45:59 20	

Multi-Cloud

This section lists the new features added to FortiManager for Multi-Cloud.

List of new features:

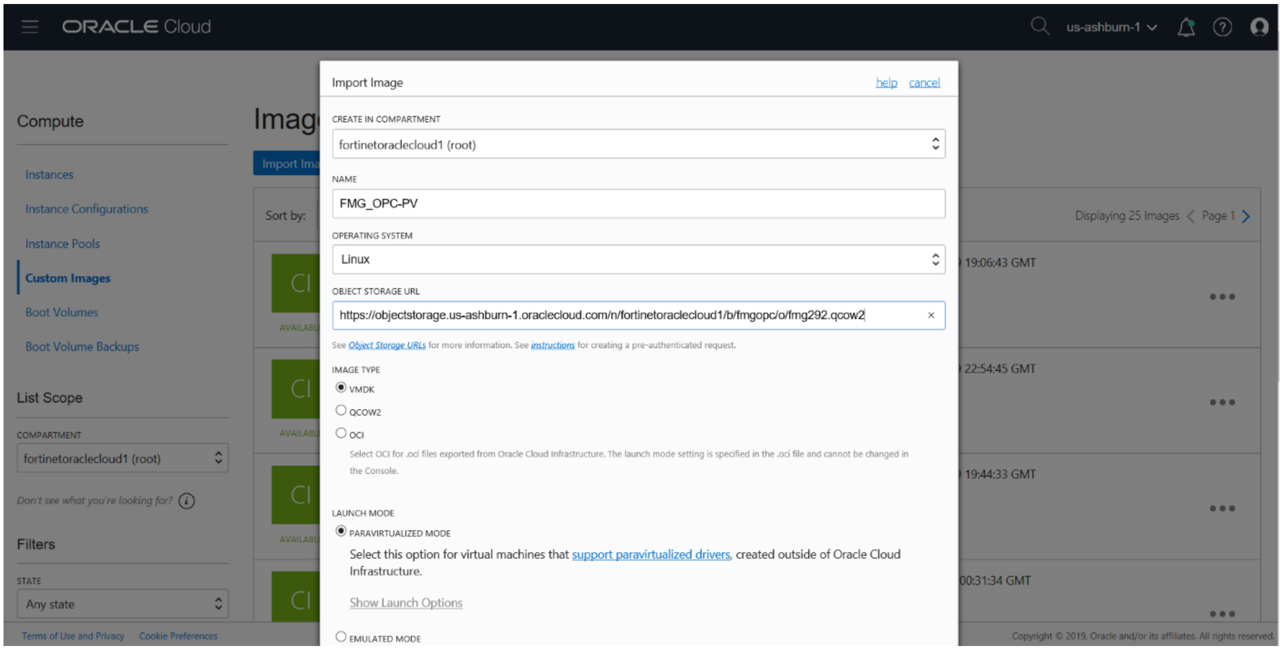
- Oracle Cloud - Paravirtualized Mode Support on page 94

Oracle Cloud - Paravirtualized Mode Support

FortiManager now supports Paravirtualized mode in Oracle Cloud.

Configuring Paravirtualized mode

1. Download *FMG_VM64_OPC-v6-build0292-FORTINET.out.OpenXen.zip* image from the Fortinet website.
2. Unzip the file and extract the fmg.qcow2 file. Rename the file to *fmg292.qcow2*.
3. Upload the *fmg292.qcow2* file to Oracle Object Storage.
4. Copy the *fmg292.qcow2* file link from the Oracle Object Storage web UI. For example, *https://objectstorage.us-ashburn-1.oraclecloud.com/n/fortinetoraclecloud1/b/fmgopc/o/fmg292.qcow2*.



Import Image

CREATE IN COMPARTMENT: fortinetoraclecloud1 (root)

NAME: FMG_OPC-PV

OPERATING SYSTEM: Linux

OBJECT STORAGE URL: https://objectstorage.us-ashburn-1.oraclecloud.com/n/fortinetoraclecloud1/b/fmgopc/o/fmg292.qcow2

See Object Storage URLs for more information. See instructions for creating a pre-authenticated request.

IMAGE TYPE

● VMDK
○ QCOW2
○ OCI

Select OCI for .oci files exported from Oracle Cloud Infrastructure. The launch mode setting is specified in the .oci file and cannot be changed in the Console.

LAUNCH MODE

● PARAVIRTUALIZED MODE

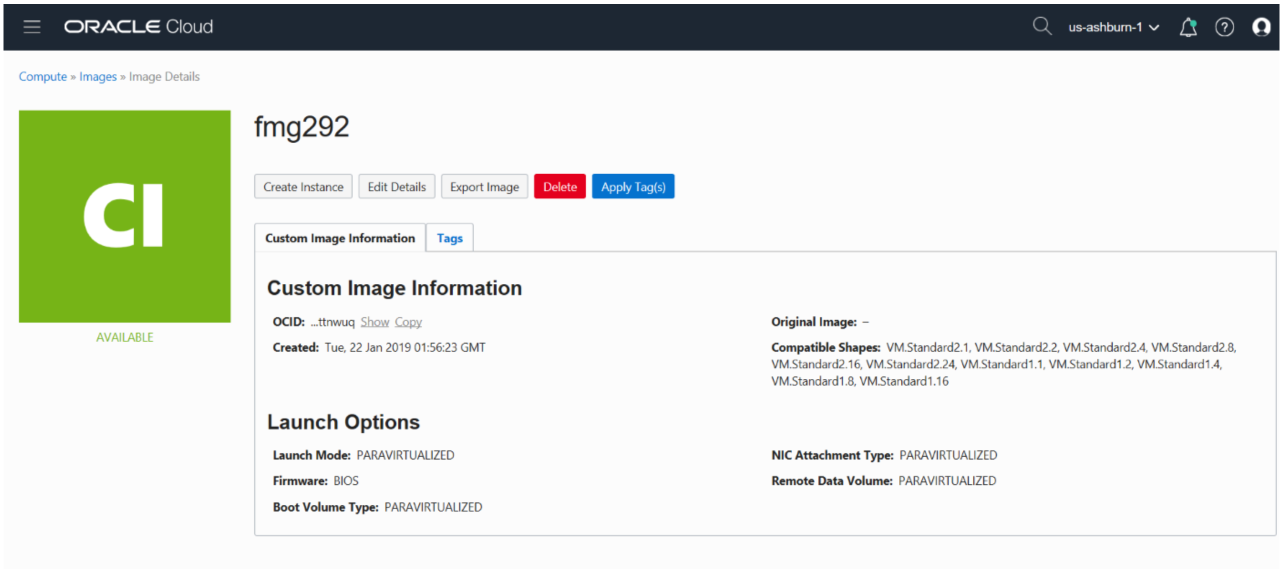
Select this option for virtual machines that support paravirtualized drivers, created outside of Oracle Cloud Infrastructure.

Show Launch Options

○ EMULATED MODE

5. Create a paravirtualized mode FortiManager image:
   a. Go to *Oracle Cloud* > *Compute* > *Custom Images* > *Import Image*.
   b. Select *Paravirtualized mode* in *Launch Mode* section. Depending on the Oracle Cloud traffic, make sure the image is available after approximately 30 minutes.

6. Create an instance with the above image.



fmg292

Custom Image Information

OCID: ...ttnwuq Show Copy

Created: Tue, 22 Jan 2019 01:56:23 GMT

Original Image: –

Compatible Shapes: VM.Standard2.1, VM.Standard2.2, VM.Standard2.4, VM.Standard2.8, VM.Standard2.16, VM.Standard2.24, VM.Standard1.1, VM.Standard1.2, VM.Standard1.4, VM.Standard1.8, VM.Standard1.16

Launch Options

Launch Mode: PARAVIRTUALIZED

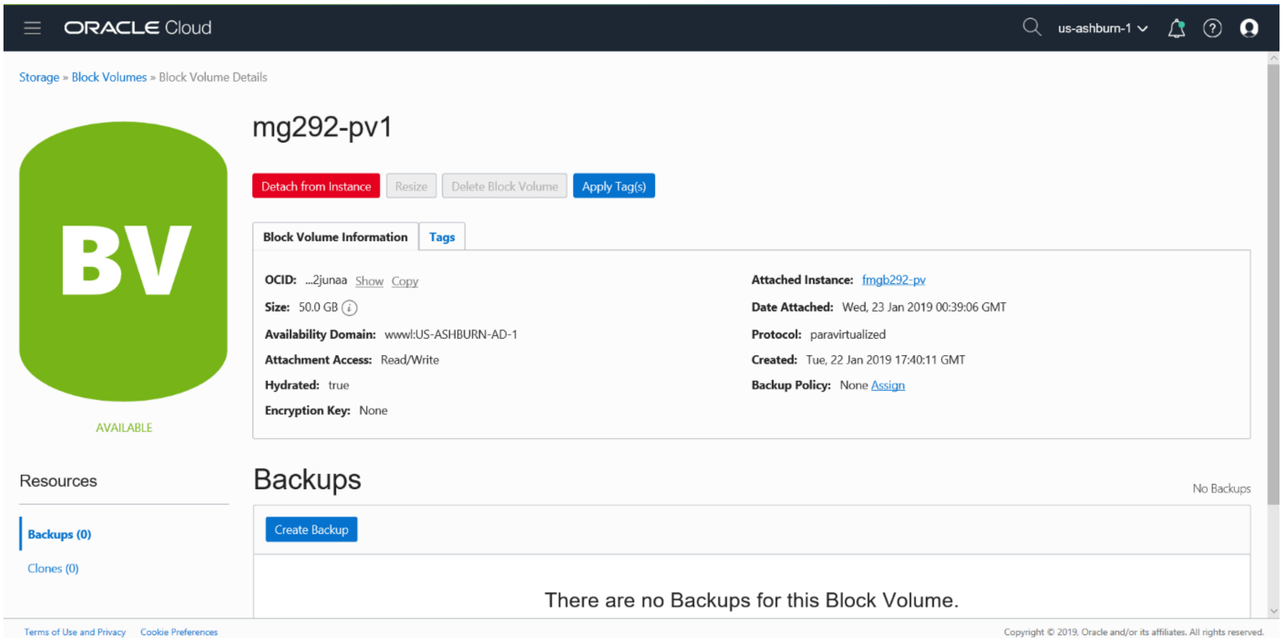
Firmware: BIOS

Boot Volume Type: PARAVIRTUALIZED

NIC Attachment Type: PARAVIRTUALIZED

Remote Data Volume: PARAVIRTUALIZED

7. Attach paravirtualized mode FMG-VM disk.



mg292-pv1

OCID: ...2junaa Show Copy

Size: 50.0 GB

Availability Domain: wwwl:US-ASHBURN-AD-1

Attachment Access: Read/Write

Hydrated: true

Encryption Key: None

Attached Instance: fmgb292-pv

Date Attached: Wed, 23 Jan 2019 00:39:06 GMT

Protocol: paravirtualized

Created: Tue, 22 Jan 2019 17:40:11 GMT

Backup Policy: None Assign

Backups

There are no Backups for this Block Volume.

8. Boot up the paravirtualized mode FMG-VM instance.

Compliance

This section lists the new features added to FortiManager for compliance.

List of new features:

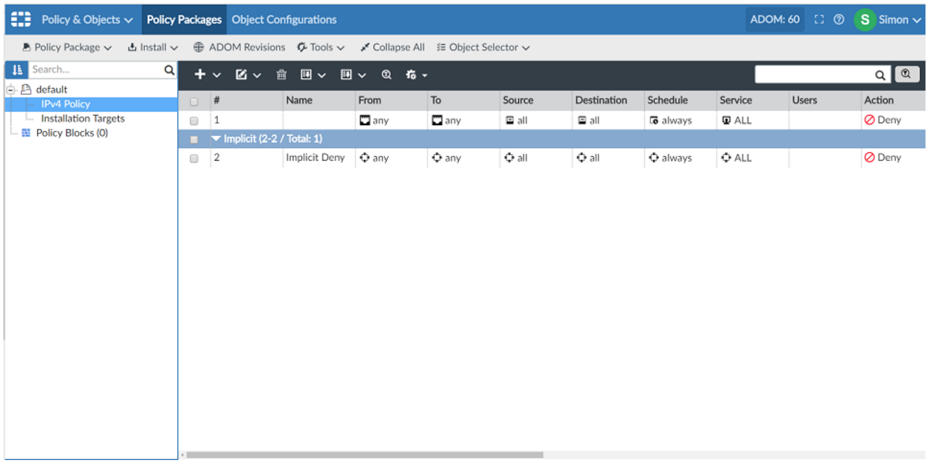
- FortiGate change log traceability on page 96
- Extended admin session logging on page 98

FortiGate change log traceability

The FortiManager administrator name is now visible in the System Events on FortiGate thereby providing end-to-end traceability.

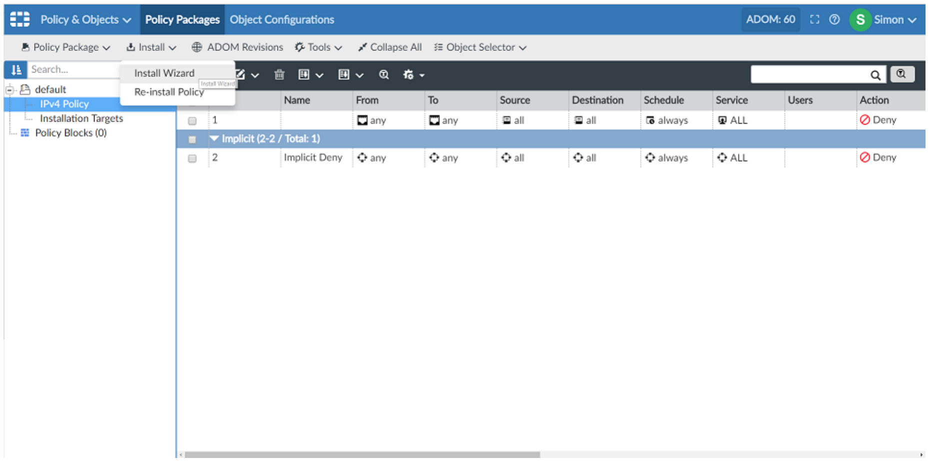
FortiManager Administrator Traceability

1. Log on to FortiManager. For this example, we have used the administrator name *Simon*.



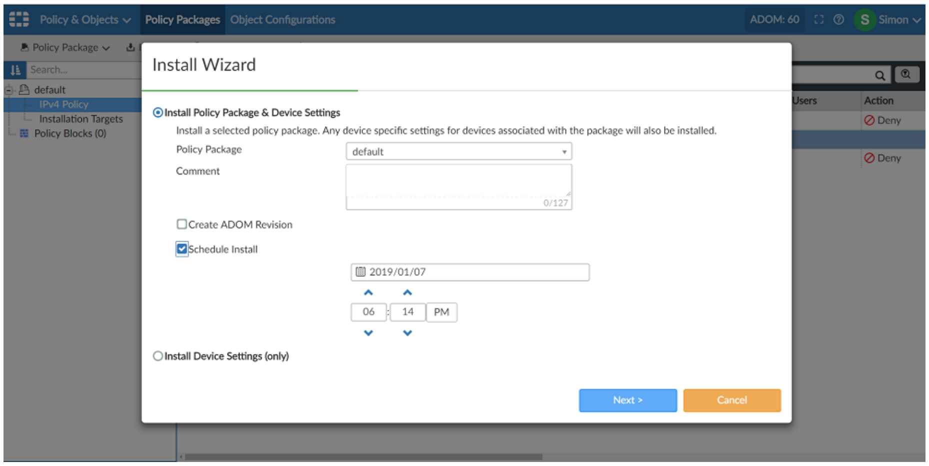
□	#	Name	From	To	Source	Destination	Schedule	Service	Users	Action
□	1		any	any	all	all	always	ALL		Deny
□	Implicit (2-2 / Total: 1)									
□	2	Implicit Deny	any	any	all	all	always	ALL		Deny

2. Install a Policy Package on a FortiGate device using the Install Wizard.



	Name	From	To	Source	Destination	Schedule	Service	Users	Action
1		any	any	all	all	always	ALL		Deny
Implicit (2-2 / Total: 1)									
2	Implicit Deny	any	any	all	all	always	ALL		Deny

3. Alternatively, schedule an installation.



● Install Policy Package & Device Settings

Install a selected policy package. Any device specific settings for devices associated with the package will also be installed.

Policy Package: default

Comment: 0/127

□ Create ADOM Revision

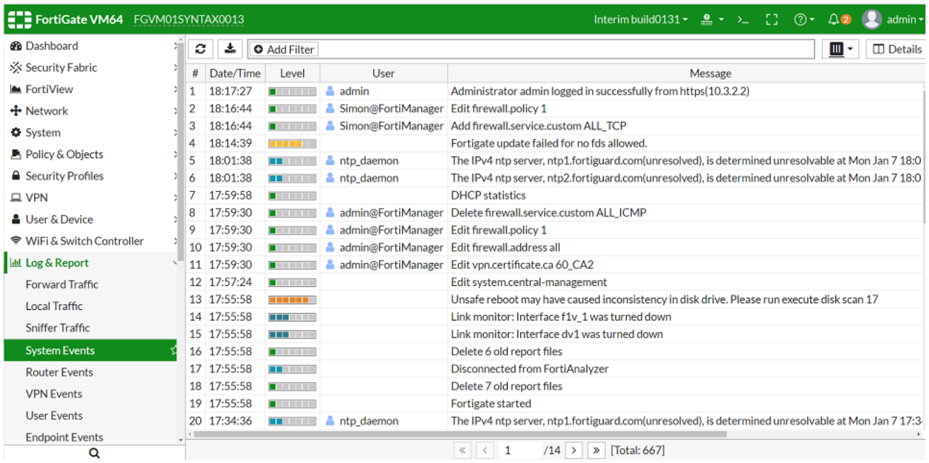
☑ Schedule Install

2019/01/07

06 : 14 PM

○ Install Device Settings (only)

4. After the installation is completed, logon to the FortiGate device. Go to *Log & Report* > *System Events* to see the actions of the administrator *Simon@FortiManager*.



#	Date/Time	Level	User	Message
1	18:17:27		admin	Administrator admin logged in successfully from https(10.3.2.2)
2	18:16:44		Simon@FortiManager	Edit firewall.policy 1
3	18:16:44		Simon@FortiManager	Add firewall.service.custom ALL_TCP
4	18:14:39			Fortigate update failed for no fds allowed.
5	18:01:38		ntp_daemon	The IPv4 ntp server, ntp1.fortiguard.com(unresolved), is determined unresolvable at Mon Jan 7 18:0
6	18:01:38		ntp_daemon	The IPv4 ntp server, ntp2.fortiguard.com(unresolved), is determined unresolvable at Mon Jan 7 18:0
7	17:59:58			DHCP statistics
8	17:59:30		admin@FortiManager	Delete firewall.service.custom ALL_ICMP
9	17:59:30		admin@FortiManager	Edit firewall.policy 1
10	17:59:30		admin@FortiManager	Edit firewall.address all
11	17:59:30		admin@FortiManager	Edit vpn.certificate.ca 60_CA2
12	17:57:24			Edit system.central-management
13	17:55:58			Unsafe reboot may have caused inconsistency in disk drive. Please run execute disk scan 17
14	17:55:58			Link monitor: Interface f1v_1 was turned down
15	17:55:58			Link monitor: Interface dv1 was turned down
16	17:55:58			Delete 6 old report files
17	17:55:58			Disconnected from FortiAnalyzer
18	17:55:58			Delete 7 old report files
19	17:55:58			Fortigate started
20	17:34:36		ntp_daemon	The IPv4 ntp server, ntp1.fortiguard.com(unresolved), is determined unresolvable at Mon Jan 7 17:3

1 /14 [Total: 667]

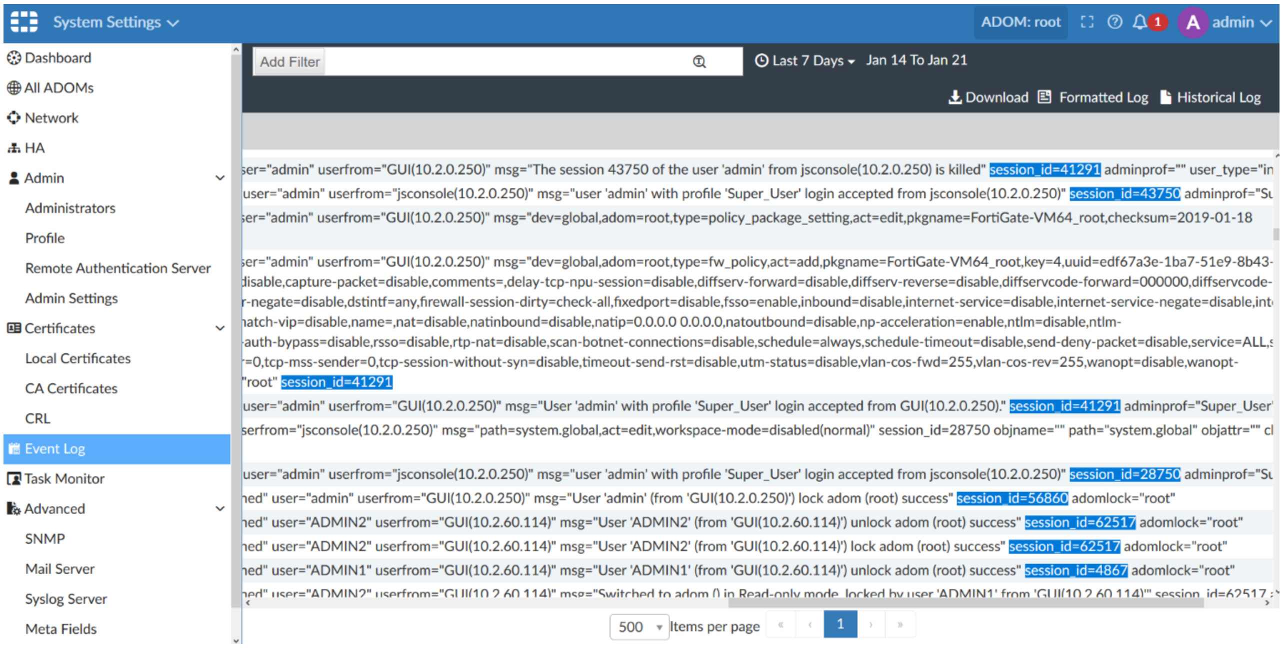
Extended admin session logging

In previous releases, the checksum Linux epoch timestamp was not clear. In version 6.2, it has been converted into human readable format for clarity. The ADOM pre-empt lock takeover event logs have also been made clear.

Event Log GUI

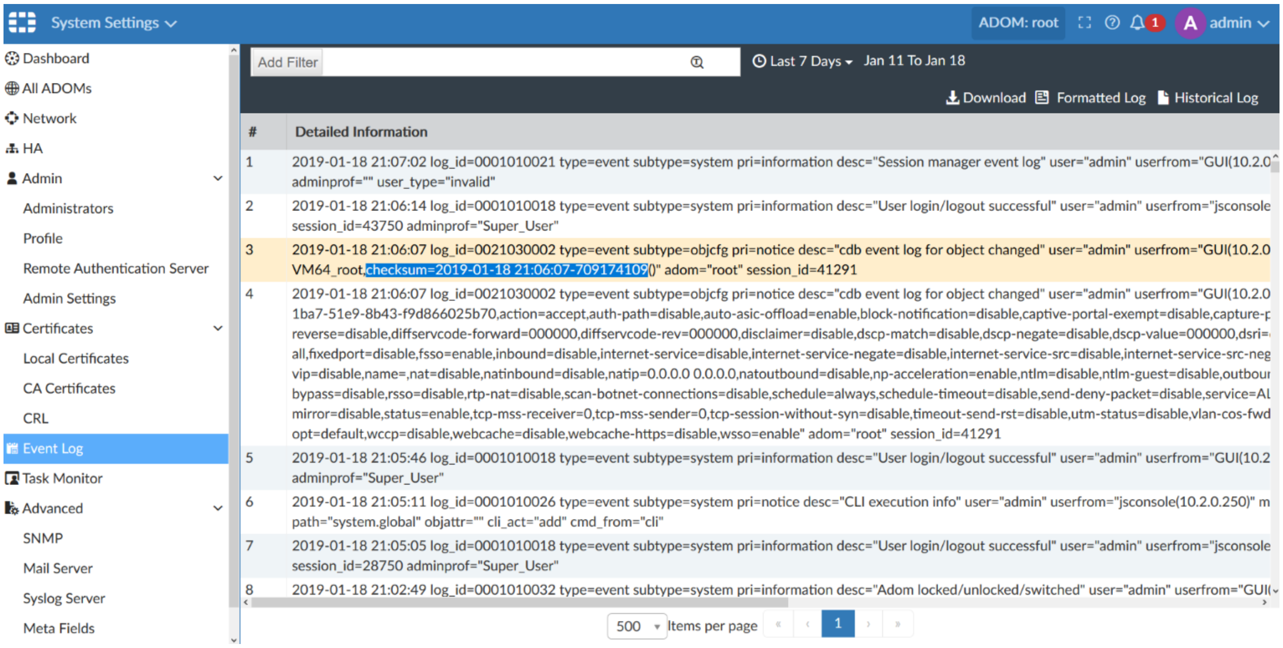
The following improvements have been made in the Event Log:

- Session ID added to each log entry:



```
ser="admin" userfrom="GUI(10.2.0.250)" msg="The session 43750 of the user 'admin' from jsconsole(10.2.0.250) is killed" session_id=41291 adminprof="" user_type="in
user="admin" userfrom="jsconsole(10.2.0.250)" msg="user 'admin' with profile 'Super_User' login accepted from jsconsole(10.2.0.250)" session_id=43750 adminprof="Su
ser="admin" userfrom="GUI(10.2.0.250)" msg="dev=global,adom=root,type=policy_package_setting,act=edit,pkgname=FortiGate-VM64_root,checksum=2019-01-18

ser="admin" userfrom="GUI(10.2.0.250)" msg="dev=global,adom=root,type=fw_policy,act=add,pkgname=FortiGate-VM64_root,key=4,uuid=edf67a3e-1ba7-51e9-8b43-
disable,capture-packet=disable,comments=,delay-tcp-npu-session=disable,diffserv-forward=disable,diffserv-reverse=disable,diffservcode-forward=000000,diffservcode-
r-negate=disable,dstintf=any,firewall-session-dirty=check-all,fixedport=disable,fsso=enable,inbound=disable,internet-service=disable,internet-service-negate=disable,int
hatch-vip=disable,name=,nat=disable,natinbound=disable,natip=0.0.0.0 0.0.0.0,natoutbound=disable,np-acceleration=enable,ntlm=disable,ntlm-
-auth-bypass=disable,rsso=disable,rtp-nat=disable,scan-botnet-connections=disable,schedule=always,schedule-timeout=disable,send-deny-packet=disable,service=ALL,s
=0,tcp-mss-sender=0,tcp-session-without-syn=disable,timeout-send-rst=disable,utm-status=disable,vlan-cos-fwd=255,vlan-cos-rev=255,wanopt=disable,wanopt-
"root" session_id=41291
user="admin" userfrom="GUI(10.2.0.250)" msg="User 'admin' with profile 'Super_User' login accepted from GUI(10.2.0.250)." session_id=41291 adminprof="Super_User"
serfrom="jsconsole(10.2.0.250)" msg="path=system.global,act=edit,workspace-mode=disabled(normal)" session_id=28750 objname="" path="system.global" objattr="" cl

user="admin" userfrom="jsconsole(10.2.0.250)" msg="user 'admin' with profile 'Super_User' login accepted from jsconsole(10.2.0.250)" session_id=28750 adminprof="Su
hed" user="admin" userfrom="GUI(10.2.0.250)" msg="User 'admin' (from 'GUI(10.2.0.250)') lock adom (root) success" session_id=56860 adomlock="root"
hed" user="ADMIN2" userfrom="GUI(10.2.60.114)" msg="User 'ADMIN2' (from 'GUI(10.2.60.114)') unlock adom (root) success" session_id=62517 adomlock="root"
hed" user="ADMIN2" userfrom="GUI(10.2.60.114)" msg="User 'ADMIN2' (from 'GUI(10.2.60.114)') lock adom (root) success" session_id=62517 adomlock="root"
hed" user="ADMIN1" userfrom="GUI(10.2.60.114)" msg="User 'ADMIN1' (from 'GUI(10.2.60.114)') unlock adom (root) success" session_id=4867 adomlock="root"
hed" user="ADMIN2" userfrom="GUI(10.2.60.114)" msg="Switched to adom () in Read-only mode, locked by user 'ADMIN1' from 'GUI(10.2.60.114)'" session_id=62517
```

- Existing checksum Linux epoch timestamps converted into human readable format:

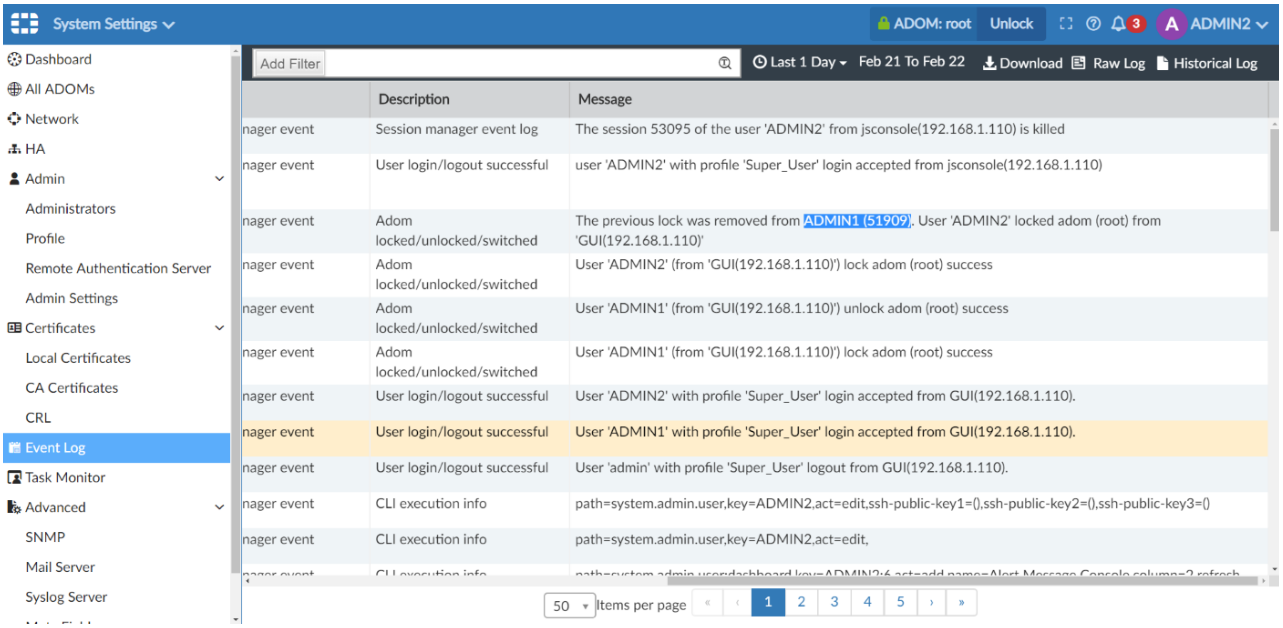


#	Detailed Information
1	2019-01-18 21:07:02 log_id=0001010021 type=event subtype=system pri=information desc="Session manager event log" user="admin" userfrom="GUI(10.2.0 adminprof="" user_type="invalid"
2	2019-01-18 21:06:14 log_id=0001010018 type=event subtype=system pri=information desc="User login/logout successful" user="admin" userfrom="jsconsole session_id=43750 adminprof="Super_User"
3	2019-01-18 21:06:07 log_id=0021030002 type=event subtype=objcfg pri=notice desc="cdb event log for object changed" user="admin" userfrom="GUI(10.2.0 VM64_root,checksum=2019-01-18 21:06:07-709174109()" adom="root" session_id=41291

4	2019-01-18 21:06:07 log_id=0021030002 type=event subtype=objcfg pri=notice desc="cdb event log for object changed" user="admin" userfrom="GUI(10.2.0
	1ba7-51e9-8b43-f9d866025b70,action=accept,auth-path=disable,auto-asic-offload=enable,block-notification=disable,captive-portal-exempt=disable,capture-p
	reverse=disable,diffservcode-forward=000000,diffservcode-rev=000000,disclaimer=disable,dscp-match=disable,dscp-negate=disable,dscp-value=000000,dsri=
	all,fixedport=disable,fsso=enable,inbound=disable,internet-service=disable,internet-service-negate=disable,internet-service-src=disable,internet-service-src-neg
	vip=disable,name=,nat=disable,natinbound=disable,natip=0.0.0.0 0.0.0.0,natoutbound=disable,np-acceleration=enable,ntlm=disable,ntlm-guest=disable,outbour
	bypass=disable,rsso=disable,rtp-nat=disable,scan-botnet-connections=disable,schedule=always,schedule-timeout=disable,send-deny-packet=disable,service=AL
	mirror=disable,status=enable,tcp-mss-receiver=0,tcp-mss-sender=0,tcp-session-without-syn=disable,timeout-send-rst=disable,utm-status=disable,vlan-cos-fwd
	opt=default,wccp=disable,webcache=disable,webcache-https=disable,wsso=enable" adom="root" session_id=41291

5	2019-01-18 21:05:46 log_id=0001010018 type=event subtype=system pri=information desc="User login/logout successful" user="admin" userfrom="GUI(10.2 adminprof="Super_User"
6	2019-01-18 21:05:11 log_id=0001010026 type=event subtype=system pri=notice desc="CLI execution info" user="admin" userfrom="jsconsole(10.2.0.250)" m path="system.global" objattr="" cli_act="add" cmd_from="cli"
7	2019-01-18 21:05:05 log_id=0001010018 type=event subtype=system pri=information desc="User login/logout successful" user="admin" userfrom="jsconsole session_id=28750 adminprof="Super_User"
8	2019-01-18 21:02:49 log_id=0001010032 type=event subtype=system pri=information desc="Adom locked/unlocked/switched" user="admin" userfrom="GUI(

- ADOM pre-empt lock takeover event logs are more clear. For example, if user 1 locks an ADOM, and user 2 takes over the ADOM, the event log shows *username* and *session ID* for workspace takeover log.



	Description	Message
nager event	Session manager event log	The session 53095 of the user 'ADMIN2' from jsconsole(192.168.1.110) is killed
nager event	User login/logout successful	user 'ADMIN2' with profile 'Super_User' login accepted from jsconsole(192.168.1.110)
nager event	Adom locked/unlocked/switched	The previous lock was removed from ADMIN1 (51909). User 'ADMIN2' locked adom (root) from 'GUI(192.168.1.110)'
nager event	Adom locked/unlocked/switched	User 'ADMIN2' (from 'GUI(192.168.1.110)') lock adom (root) success
nager event	Adom locked/unlocked/switched	User 'ADMIN1' (from 'GUI(192.168.1.110)') unlock adom (root) success
nager event	Adom locked/unlocked/switched	User 'ADMIN1' (from 'GUI(192.168.1.110)') lock adom (root) success
nager event	User login/logout successful	User 'ADMIN2' with profile 'Super_User' login accepted from GUI(192.168.1.110).
nager event	User login/logout successful	User 'ADMIN1' with profile 'Super_User' login accepted from GUI(192.168.1.110).
nager event	User login/logout successful	User 'admin' with profile 'Super_User' logout from GUI(192.168.1.110).
nager event	CLI execution info	path=system.admin.user,key=ADMIN2,act=edit,ssh-public-key1=(),ssh-public-key2=(),ssh-public-key3=()
nager event	CLI execution info	path=system.admin.user,key=ADMIN2,act=edit,
nager event	CLI execution info	path=system.admin.user:dashboard,key=ADMIN2:6,act=add,name=Alert Message Console,column=2,refresh

Usability

This section lists the new features added to FortiManager for usability.

List of new features:

- Consolidated Firewall Mode on page 100
- IPv6 Address Template on page 104
- Policy and Route Lookup on page 107
- Policy Blocks on page 109
- Promote Objects (LOCAL > GLOBAL) on page 114
- Address Icon/Tile View on page 116
- Device Manager Map View on page 118
- Clone Reverse Policy on page 122
- Admin Preference - Policy Package Cookie on page 123
- Promote Objects (LOCAL > GLOBAL) on page 114
- Upgrade Path Enforcement for Managed FortiGates on page 125

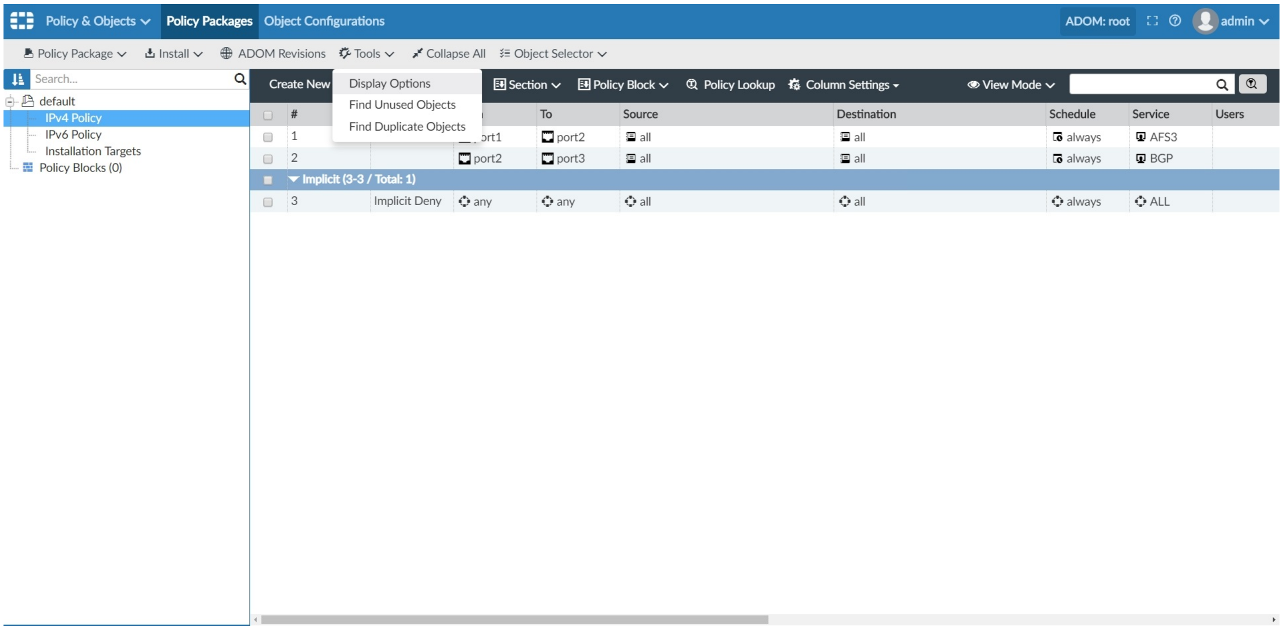
Consolidated Firewall Mode

Consolidated Firewall Mode allows administrators to create consolidated IPv4 and IPv6 policies from a single interface. This feature saves time in configuring two separate policies for IPv4 and IPv6.

See Create New Policy Packages.

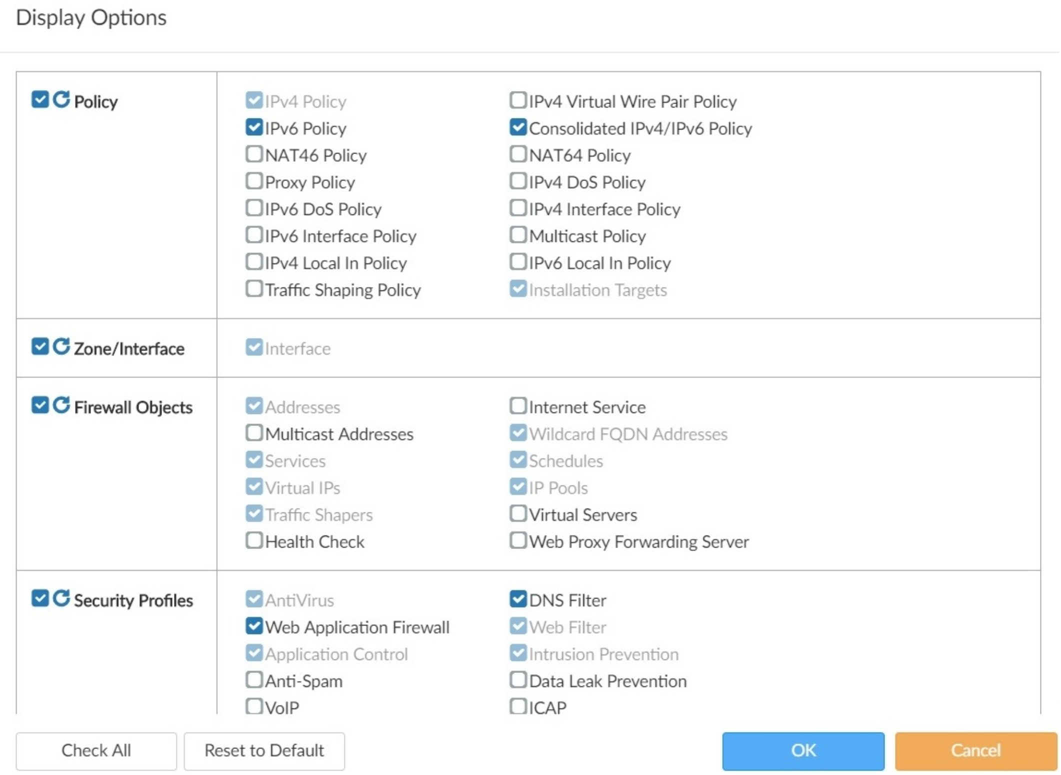
To create a Single Policy table for IPv4 and IPv6 policies:

1. Go to *Policy and Objects > Policy Packages*. Click *Tools* menu and select *Display Options*.



#			To	Source	Destination	Schedule	Service	Users
1		ort1	port2	all	all	always	AFS3	
2		port2	port3	all	all	always	BGP	
Implicit (3-3 / Total: 1)								
3	Implicit Deny	any	any	all	all	always	ALL	

2. In the Display Options screen, select *IPv4 Policy*, *IPv6 Policy*, and *Consolidated IPv4/IPv6 Policy*. Click *OK* to save.


Display Options

☑ Policy

☑ IPv4 Policy
☑ IPv6 Policy
☐ NAT46 Policy
☐ Proxy Policy
☐ IPv6 DoS Policy
☐ IPv6 Interface Policy
☐ IPv4 Local In Policy
☐ Traffic Shaping Policy
☐ IPv4 Virtual Wire Pair Policy
☑ Consolidated IPv4/IPv6 Policy
☐ NAT64 Policy
☐ IPv4 DoS Policy
☐ IPv4 Interface Policy
☐ Multicast Policy
☐ IPv6 Local In Policy
☑ Installation Targets

☑ Zone/Interface

☑ Interface

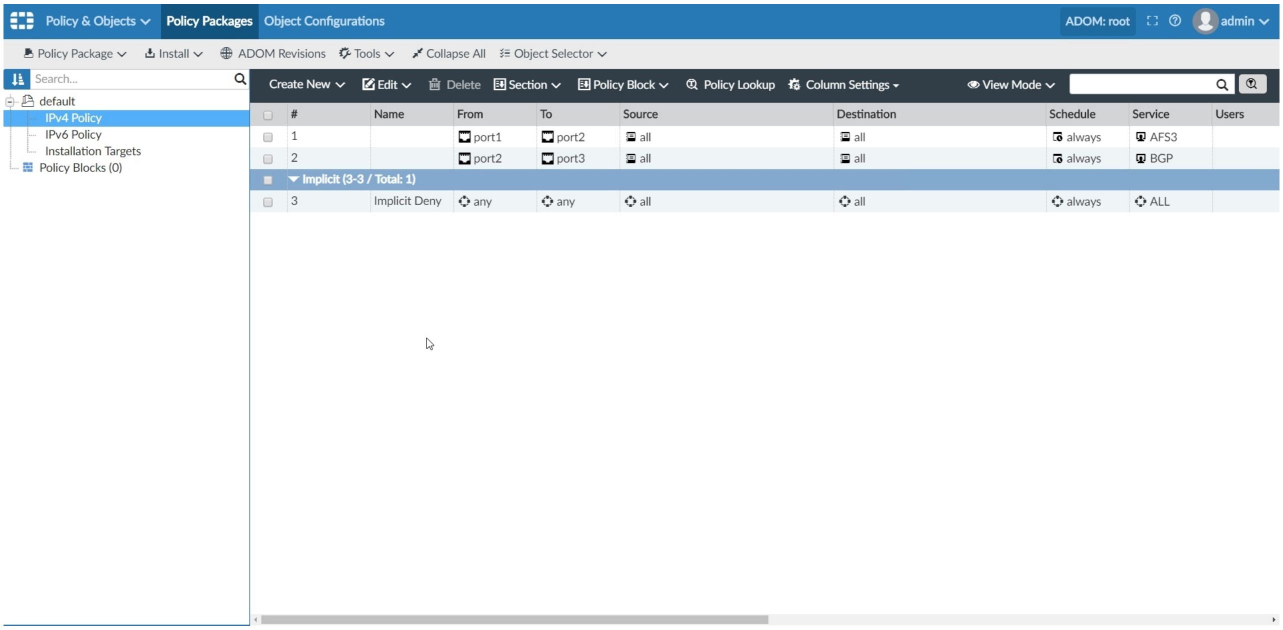
☑ Firewall Objects

☑ Addresses
☐ Multicast Addresses
☑ Services
☑ Virtual IPs
☑ Traffic Shapers
☐ Health Check
☐ Internet Service
☑ Wildcard FQDN Addresses
☑ Schedules
☑ IP Pools
☐ Virtual Servers
☐ Web Proxy Forwarding Server

☑ Security Profiles

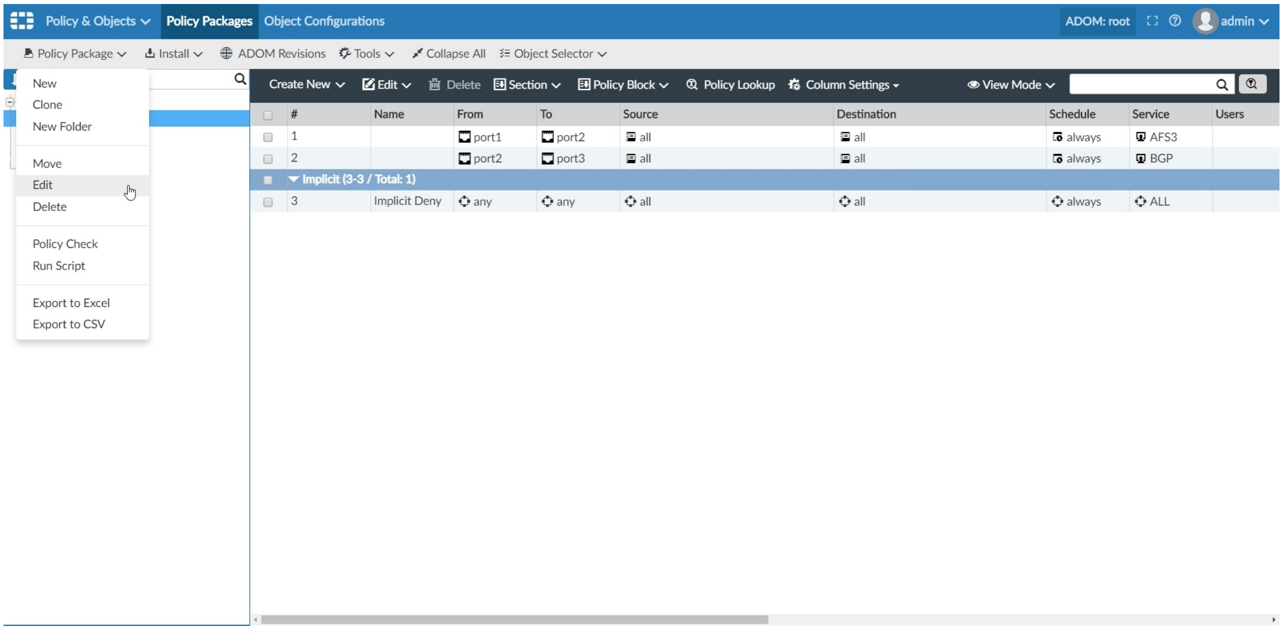
☑ AntiVirus
☑ Web Application Firewall
☑ Application Control
☐ Anti-Spam
☐ VoIP
☑ DNS Filter
☑ Web Filter
☑ Intrusion Prevention
☐ Data Leak Prevention
☐ ICAP

3. IPv4 and IPv6 policies are shown separately.



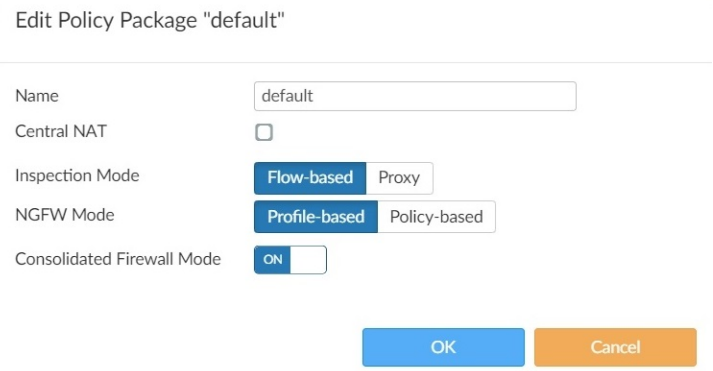
#	Name	From	To	Source	Destination	Schedule	Service	Users
1		port1	port2	all	all	always	AFS3	
2		port2	port3	all	all	always	BGP	
Implicit (3-3 / Total: 1)								
3	Implicit Deny	any	any	all	all	always	ALL	

4. Right-click the Policy Package and click *Edit*.



#	Name	From	To	Source	Destination	Schedule	Service	Users
1		port1	port2	all	all	always	AFS3	
2		port2	port3	all	all	always	BGP	
Implicit (3-3 / Total: 1)								
3	Implicit Deny	any	any	all	all	always	ALL	

5. Switch *Consolidated Firewall Mode* to *ON*. Click *OK*.



Edit Policy Package "default"

Name: default

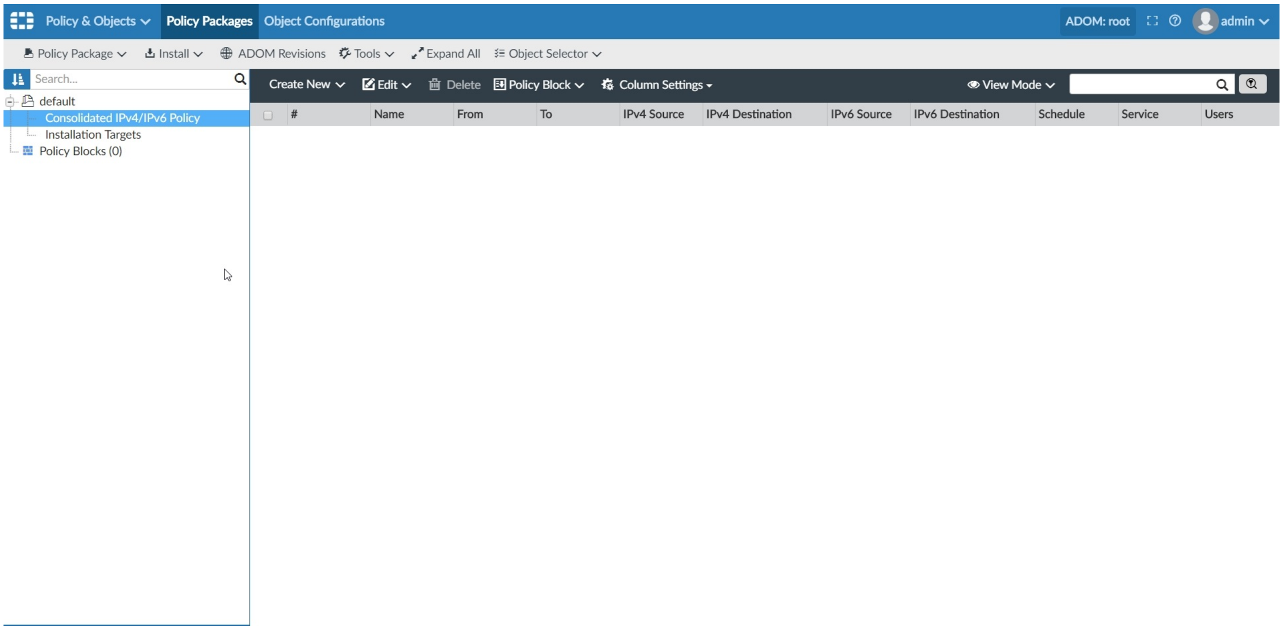
Central NAT: □

Inspection Mode: Flow-based | Proxy

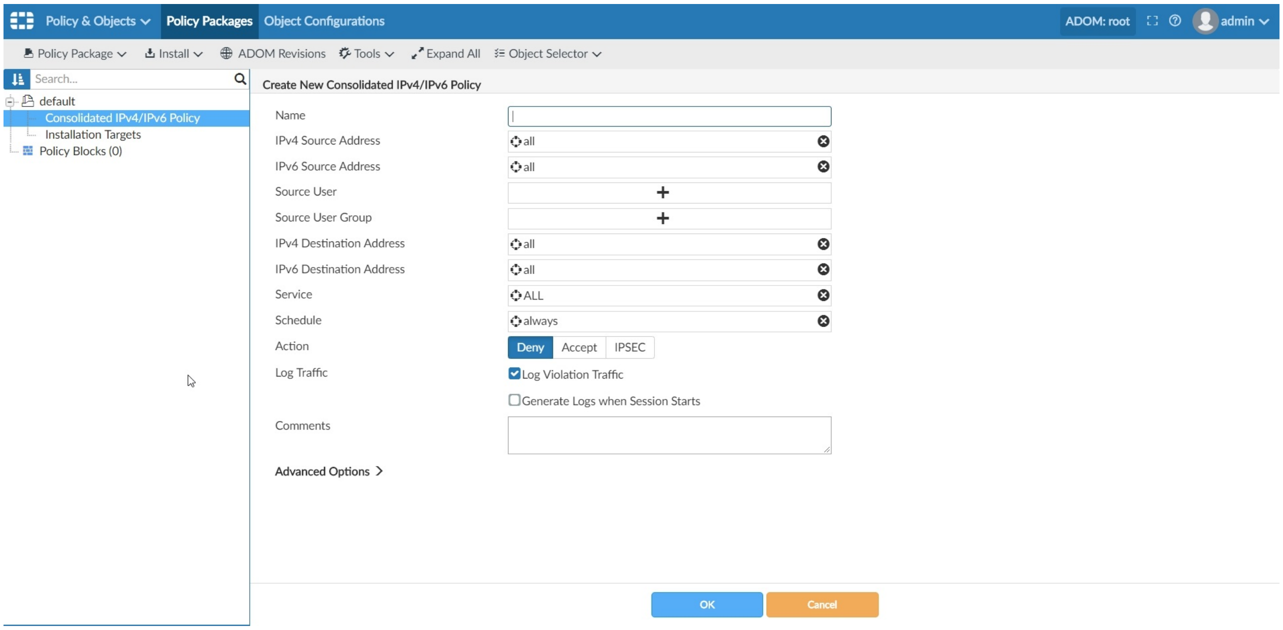
NGFW Mode: Profile-based | Policy-based

Consolidated Firewall Mode: ON

6. IPv4 and IPv6 policies are now shown together in *Consolidated IPv4/IPv6 Policy*.



7. Create a new policy. Both IPv4 and IPv6 are configurable in the same policy.



Create New Consolidated IPv4/IPv6 Policy

Name	
IPv4 Source Address	all
IPv6 Source Address	all
Source User	+
Source User Group	+
IPv4 Destination Address	all
IPv6 Destination Address	all
Service	ALL
Schedule	always
Action	Deny / Accept / IPSEC
Log Traffic	☑ Log Violation Traffic □ Generate Logs when Session Starts
Comments	

Advanced Options >

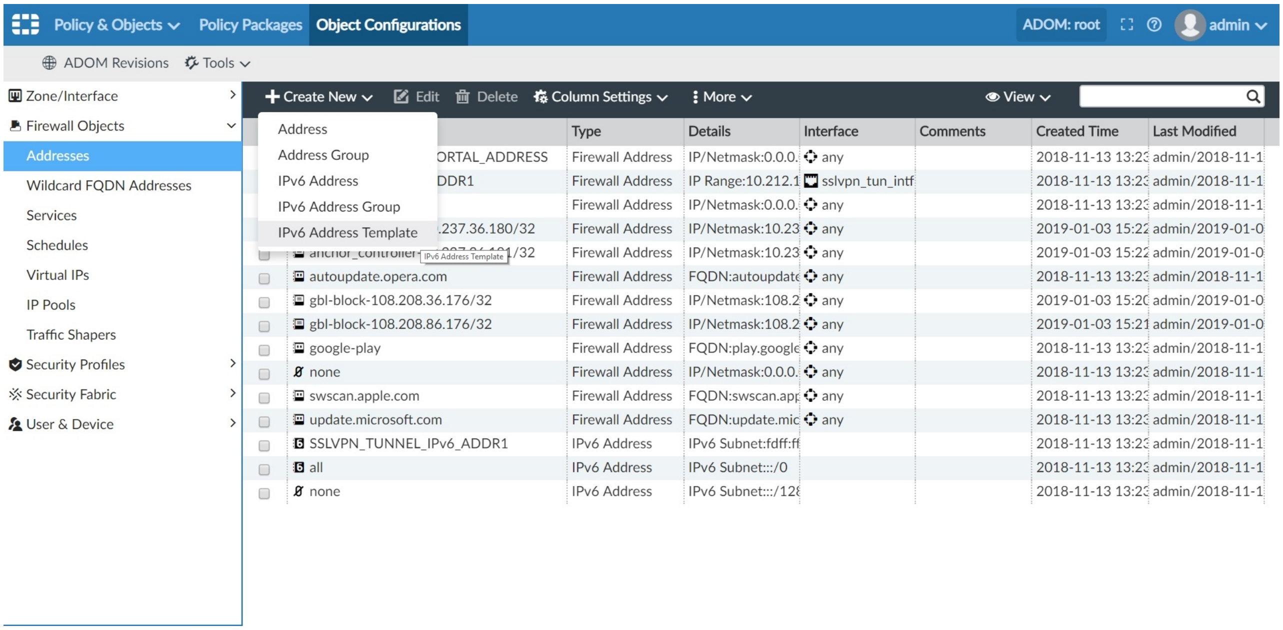
IPv6 Address Template

IPv6 Address Template allows administrators to create an IPv6 template with pre-defined parameters. The IPv6 Address Template can be reused while creating an IPv6 address. The IPv6 Address Template saves time since the predefined parameters in the template do not need to be entered while creating each IPv6 address.

See IPv6 Address Template.

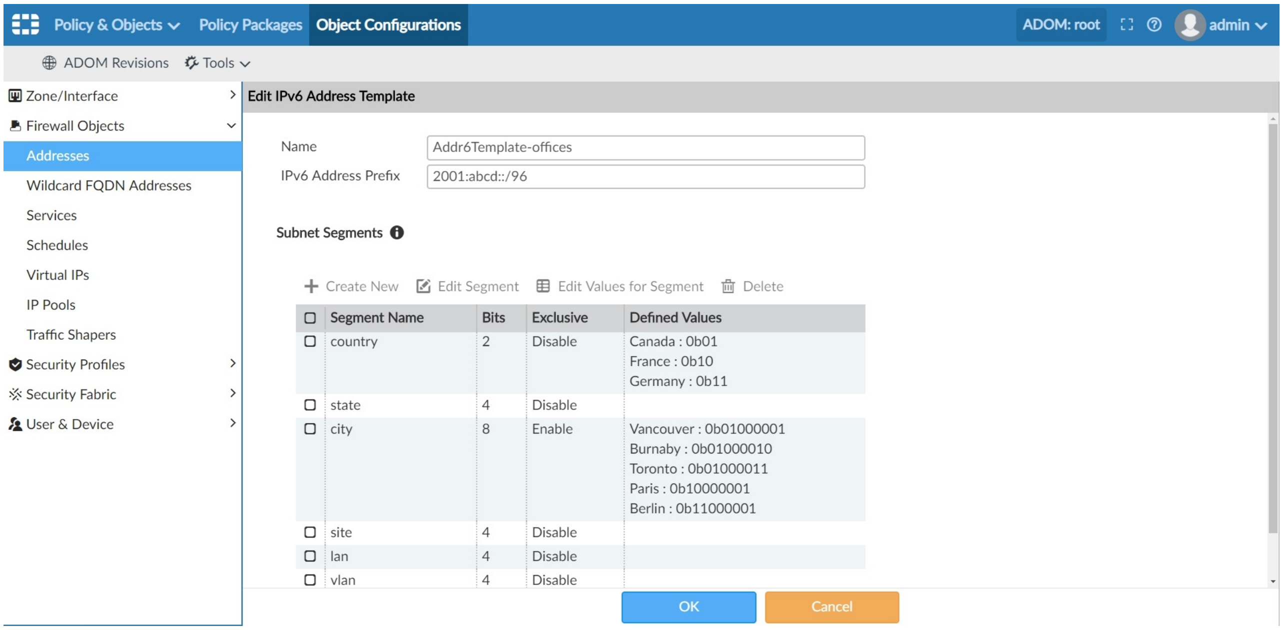
Creating an IPv6 Template

1. Go to *Policy & Objects* > *Object Configuration*. Click *Addresses*. Click *Create New* > *IPv6 Address Template*.



	Type	Details	Interface	Comments	Created Time	Last Modified
ORTAL_ADDRESS	Firewall Address	IP/Netmask:0.0.0.	any		2018-11-13 13:23	admin/2018-11-1
DDR1	Firewall Address	IP Range:10.212.1	sslvpn_tun_intf		2018-11-13 13:23	admin/2018-11-1
	Firewall Address	IP/Netmask:0.0.0.	any		2018-11-13 13:23	admin/2018-11-1
.237.36.180/32	Firewall Address	IP/Netmask:10.23	any		2019-01-03 15:22	admin/2019-01-0
anchor_controller- 1/32	Firewall Address	IP/Netmask:10.23	any		2019-01-03 15:22	admin/2019-01-0
autoupdate.opera.com	Firewall Address	FQDN:autoupdate	any		2018-11-13 13:23	admin/2018-11-1
gbl-block-108.208.36.176/32	Firewall Address	IP/Netmask:108.2	any		2019-01-03 15:20	admin/2019-01-0
gbl-block-108.208.86.176/32	Firewall Address	IP/Netmask:108.2	any		2019-01-03 15:21	admin/2019-01-0
google-play	Firewall Address	FQDN:play.google	any		2018-11-13 13:23	admin/2018-11-1
none	Firewall Address	IP/Netmask:0.0.0.	any		2018-11-13 13:23	admin/2018-11-1
swscan.apple.com	Firewall Address	FQDN:swscan.app	any		2018-11-13 13:23	admin/2018-11-1
update.microsoft.com	Firewall Address	FQDN:update.mic	any		2018-11-13 13:23	admin/2018-11-1
SSLVPN_TUNNEL_IPv6_ADDR1	IPv6 Address	IPv6 Subnet:fdff:ff			2018-11-13 13:23	admin/2018-11-1
all	IPv6 Address	IPv6 Subnet:::/0			2018-11-13 13:23	admin/2018-11-1
none	IPv6 Address	IPv6 Subnet:::/128			2018-11-13 13:23	admin/2018-11-1

2. Define the IPv6 address template. If *Exclusive* set to *Enable*, at least 1 segment value must be defined.

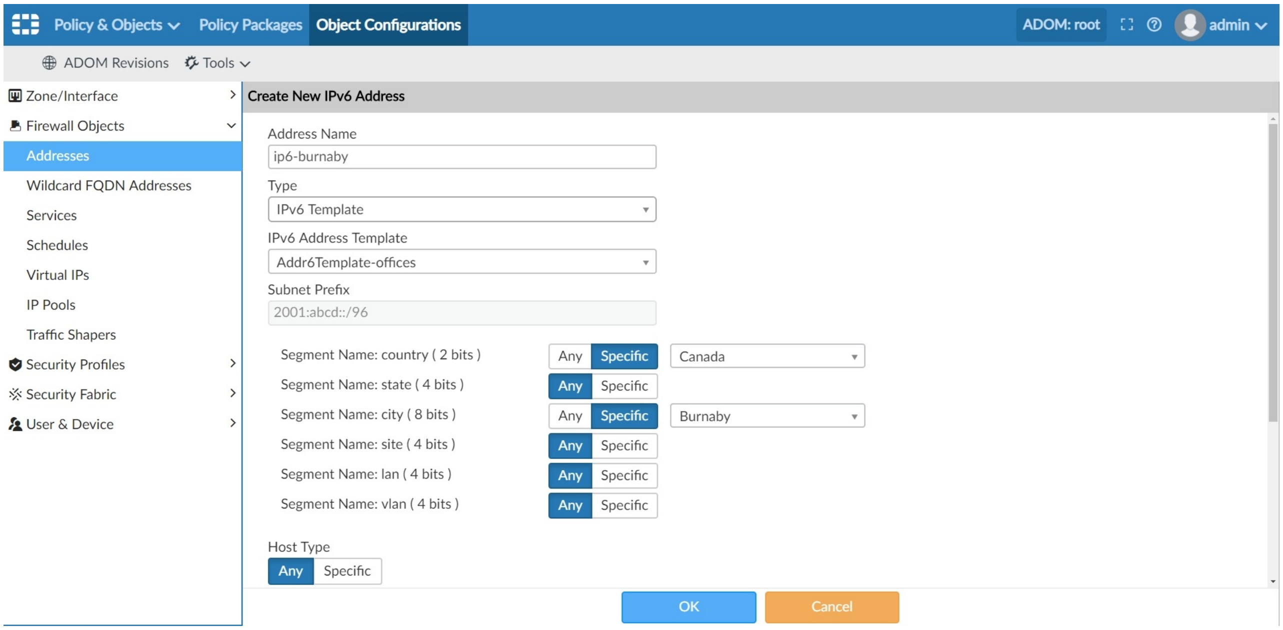


Edit IPv6 Address Template

Name	Addr6Template-offices
IPv6 Address Prefix	2001:abcd::/96

□	Segment Name	Bits	Exclusive	Defined Values
□	country	2	Disable	Canada : 0b01 France : 0b10 Germany : 0b11
□	state	4	Disable	
□	city	8	Enable	Vancouver : 0b01000001 Burnaby : 0b01000010 Toronto : 0b01000011 Paris : 0b10000001 Berlin : 0b11000001
□	site	4	Disable	
□	lan	4	Disable	
□	vlan	4	Disable	

3. Create an IPv6 address that uses the template. If *Specific* is selected, defined segment values are available for selection from the drop-down list, which simplifies what the administrator has to enter and pick human readable values. The administrator may also select *Any* without specifying a value.



Create New IPv6 Address

Address Name: ip6-burnaby

Type: IPv6 Template

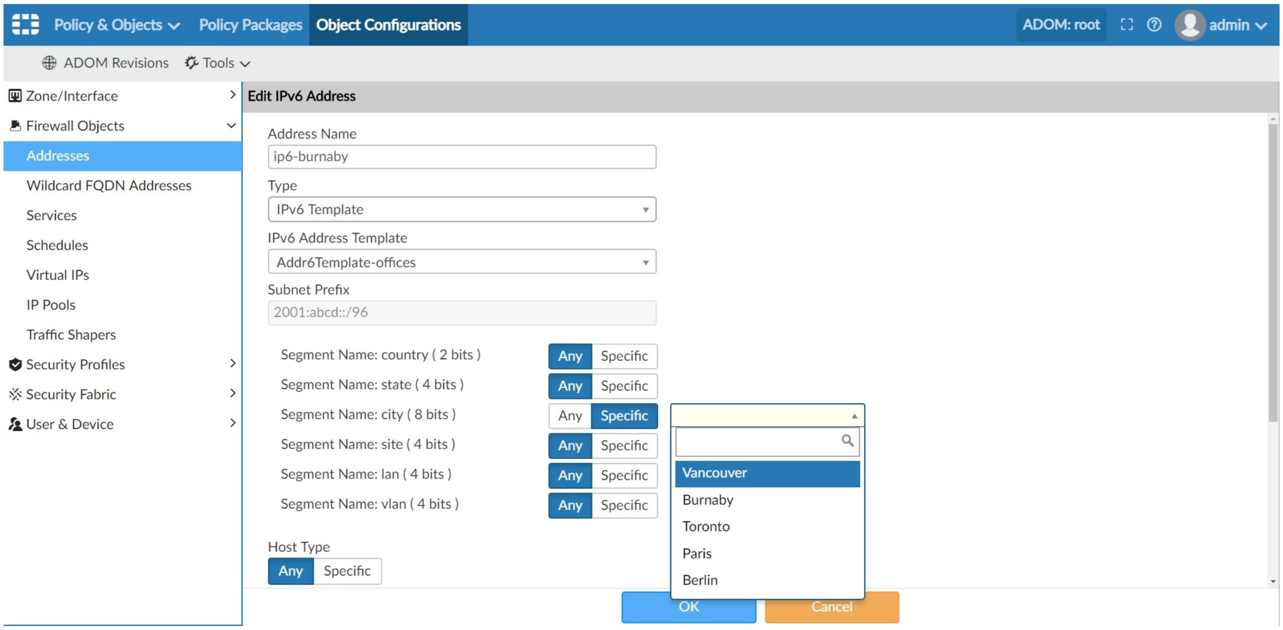
IPv6 Address Template: Addr6Template-offices

Subnet Prefix: 2001:abcd::/96

Segment Name: country (2 bits)	Specific	Canada
Segment Name: state (4 bits)	Any	
Segment Name: city (8 bits)	Specific	Burnaby
Segment Name: site (4 bits)	Any	
Segment Name: lan (4 bits)	Any	
Segment Name: vlan (4 bits)	Any	

Host Type: Any

4. Set *Host Type* as *Any* for wildcard. or specify a host. A standard IPv6 address can be divided into three parts: [IPv6 network prefix] + [subnet segments] + [host address].



Edit IPv6 Address

Address Name: ip6-burnaby

Type: IPv6 Template

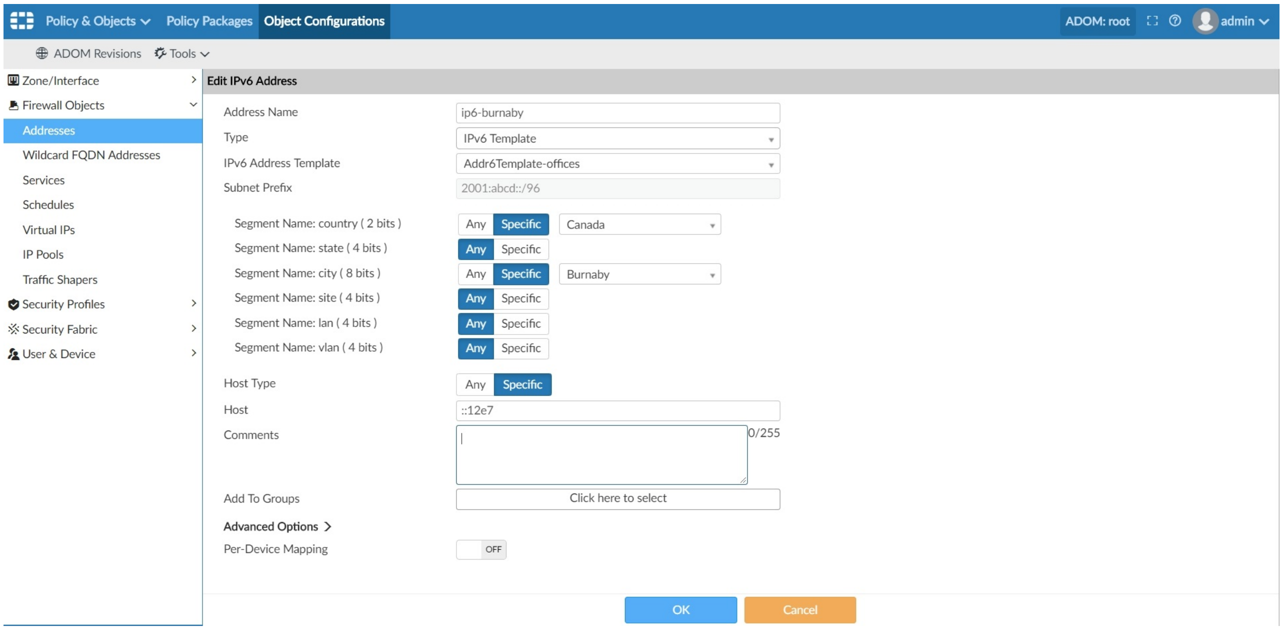
IPv6 Address Template: Addr6Template-offices

Subnet Prefix: 2001:abcd::/96

Segment Name: country (2 bits)	Any
Segment Name: state (4 bits)	Any
Segment Name: city (8 bits)	Specific
Segment Name: site (4 bits)	Any
Segment Name: lan (4 bits)	Any
Segment Name: vlan (4 bits)	Any

Host Type: Any

5. After selecting the IPv6 address template, and configuring the other settings, click *OK*.



Edit IPv6 Address

Address Name	ip6-burnaby
Type	IPv6 Template
IPv6 Address Template	Addr6Template-offices
Subnet Prefix	2001:abcd::/96
Segment Name: country (2 bits)	Any [✓ Specific] Canada
Segment Name: state (4 bits)	[✓ Any] Specific
Segment Name: city (8 bits)	Any [✓ Specific] Burnaby
Segment Name: site (4 bits)	[✓ Any] Specific
Segment Name: lan (4 bits)	[✓ Any] Specific
Segment Name: vlan (4 bits)	[✓ Any] Specific
Host Type	Any [✓ Specific]
Host	::12e7
Comments	0/255
Add To Groups	Click here to select
Advanced Options >	
Per-Device Mapping	OFF

OK Cancel

Policy and Route Lookup

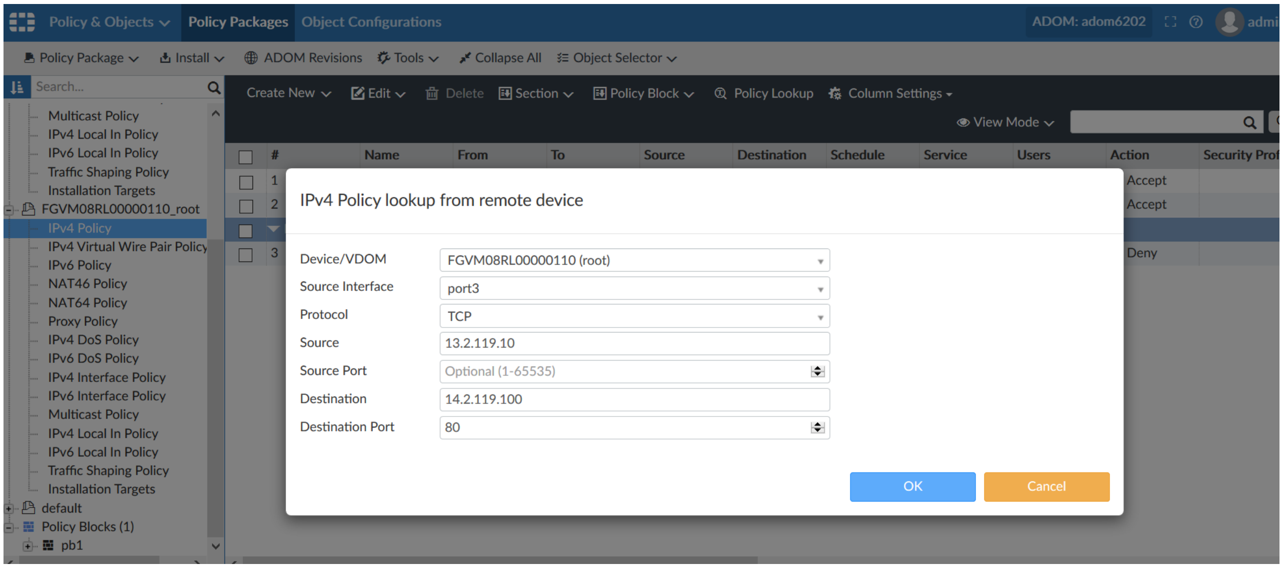
Policy Lookup allows administrators to search for policies on a FortiGate device (or VDOM) based on certain input parameters. The input parameters simulate a packet received on FortiGate, and return the matching policy that would be triggered for it. This feature helps administrators troubleshoot issues and test new policies that they are creating.

Route Lookup allows administrators to similarly test a routing decision by specifying similar types of input parameters. Both policy routing and normal routing are consulted for the decision.

The policy and route lookup features are both invoked using the FortiGate API, as they require the real-time state of the FortiGate.

Policy Lookup

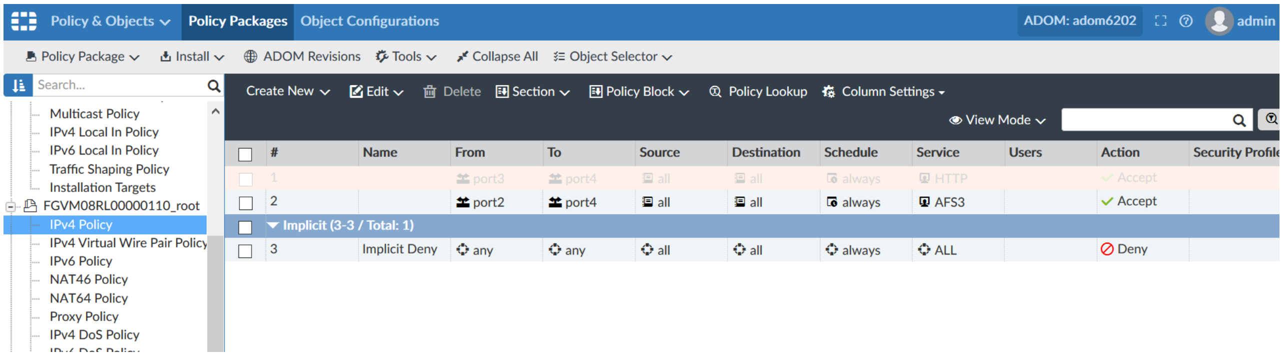
1. Go to *Policy & Objects* > *Policy Packages*.
2. In the tree menu, select a policy package then a policy type, such as *IPv4 Policy*.
3. Click *Policy Lookup* in the toolbar.
   The *IPv4 Policy lookup from remote device* dialog box opens.



IPv4 Policy lookup from remote device

Device/VDOM	FGVM08RL00000110 (root)
Source Interface	port3
Protocol	TCP
Source	13.2.119.10
Source Port	Optional (1-65535)
Destination	14.2.119.100
Destination Port	80

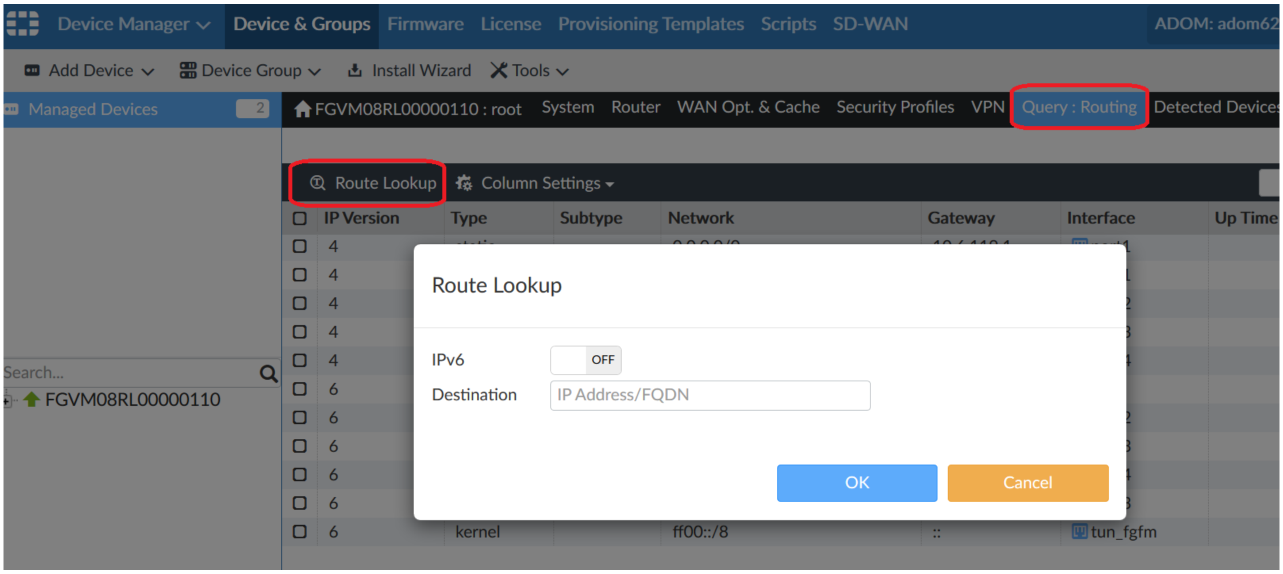
4. Fill in the required information, then click *OK*.
   The matching policy entry, learned from the remote FortiGate, will be highlighted in the policy list.



#	Name	From	To	Source	Destination	Schedule	Service	Users	Action	Security Profile
1		port3	port4	all	all	always	HTTP		Accept	
2		port2	port4	all	all	always	AFS3		Accept	
Implicit (3-3 / Total: 1)										
3	Implicit Deny	any	any	all	all	always	ALL		Deny	

Route Lookup

1. Go to *Device Manager*, and open a synchronized, managed device.
2. Go to *Query > Routing*.
3. Click *Route Lookup* in the toolbar.
   The *Route Lookup* dialog box opens.



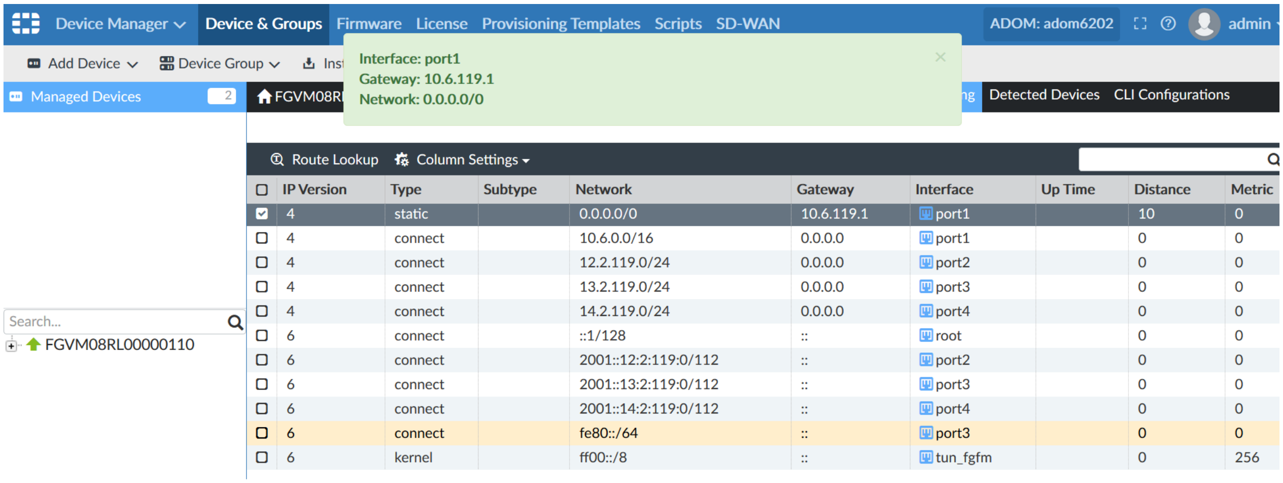
Route Lookup

IPv6 OFF

Destination IP Address/FQDN

OK Cancel

4. Select IPv4 or IPv6, enter the destination address, then click *OK*.
A pop-up will show the show the route information from the FortiGate, and the route will be highlighted in the routing table.



Interface: port1
Gateway: 10.6.119.1
Network: 0.0.0.0/0

□	IP Version	Type	Subtype	Network	Gateway	Interface	Up Time	Distance	Metric
☑	4	static		0.0.0.0/0	10.6.119.1	port1		10	0
□	4	connect		10.6.0.0/16	0.0.0.0	port1		0	0
□	4	connect		12.2.119.0/24	0.0.0.0	port2		0	0
□	4	connect		13.2.119.0/24	0.0.0.0	port3		0	0
□	4	connect		14.2.119.0/24	0.0.0.0	port4		0	0
□	6	connect		::1/128	::	root		0	0
□	6	connect		2001::12:2:119:0/112	::	port2		0	0
□	6	connect		2001::13:2:119:0/112	::	port3		0	0
□	6	connect		2001::14:2:119:0/112	::	port4		0	0
□	6	connect		fe80::/64	::	port3		0	0
□	6	kernel		ff00::/8	::	tun_fgfm		0	256

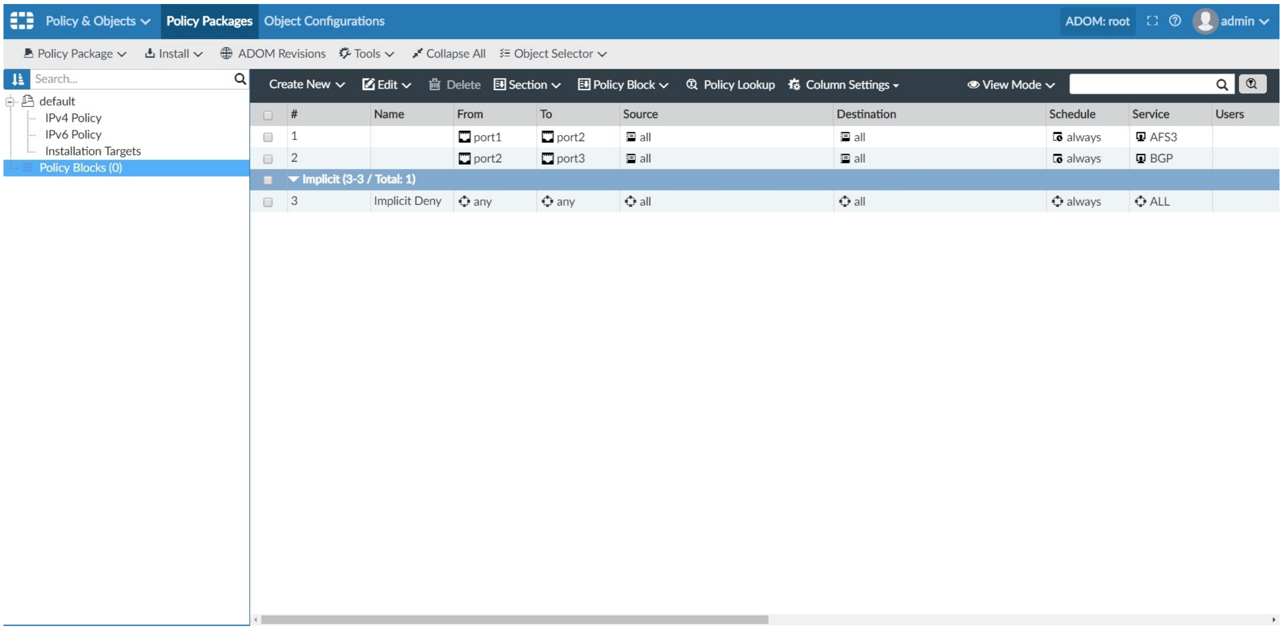
Policy Blocks

Policy Blocks are created to store multiple policies. Policy Blocks can be appended to a Policy Package. When creating a Policy Package, the administrator does not need to add one policy at a time. By appending a Policy Block to a Policy Package, the administrator can ensure that all policies in the Policy Block are added to the policy package together.

See Creating Policy Blocks.

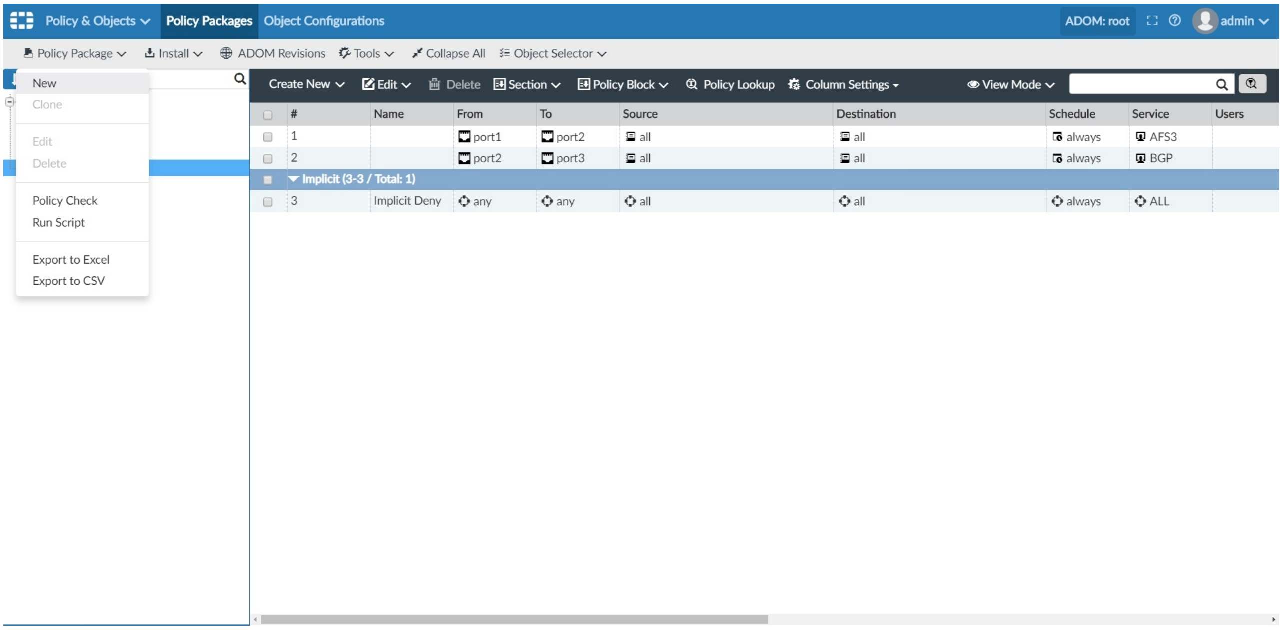
To create Policy Blocks:

1. Go to *Policy Packages* and select *Policy Blocks*.



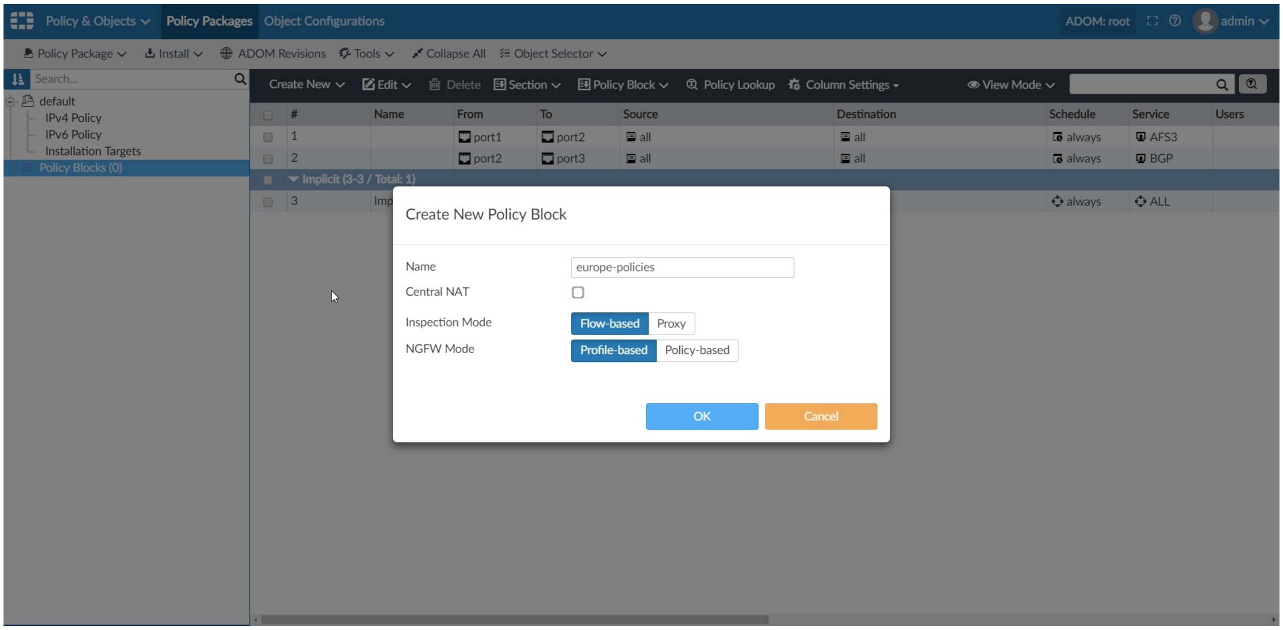
#	Name	From	To	Source	Destination	Schedule	Service	Users
1		port1	port2	all	all	always	AFS3	
2		port2	port3	all	all	always	BGP	
Implicit (3-3 / Total: 1)								
3	Implicit Deny	any	any	all	all	always	ALL	

2. Expand the *Policy Package* menu and click *New*.



#	Name	From	To	Source	Destination	Schedule	Service	Users
1		port1	port2	all	all	always	AFS3	
2		port2	port3	all	all	always	BGP	
Implicit (3-3 / Total: 1)								
3	Implicit Deny	any	any	all	all	always	ALL	

3. Specify a name and configure other settings. Click *OK* to save.



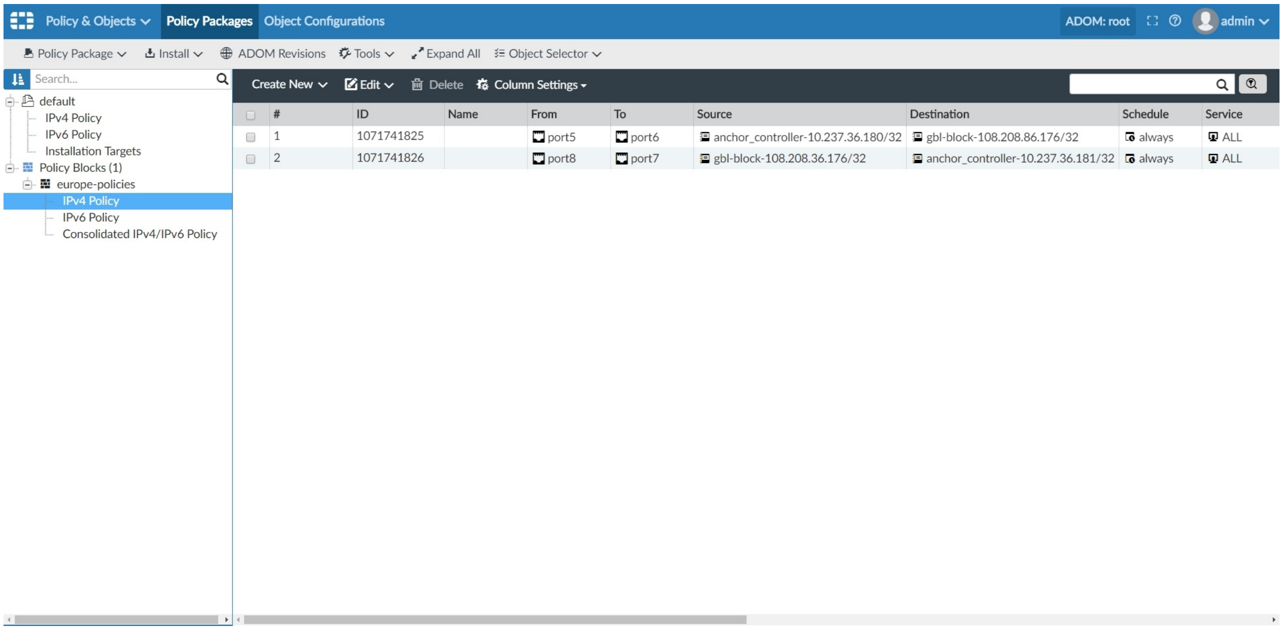
Create New Policy Block

Name	europe-policies
Central NAT	□
Inspection Mode	[✓ Flow-based] Proxy
NGFW Mode	[✓ Profile-based] Policy-based

OK Cancel

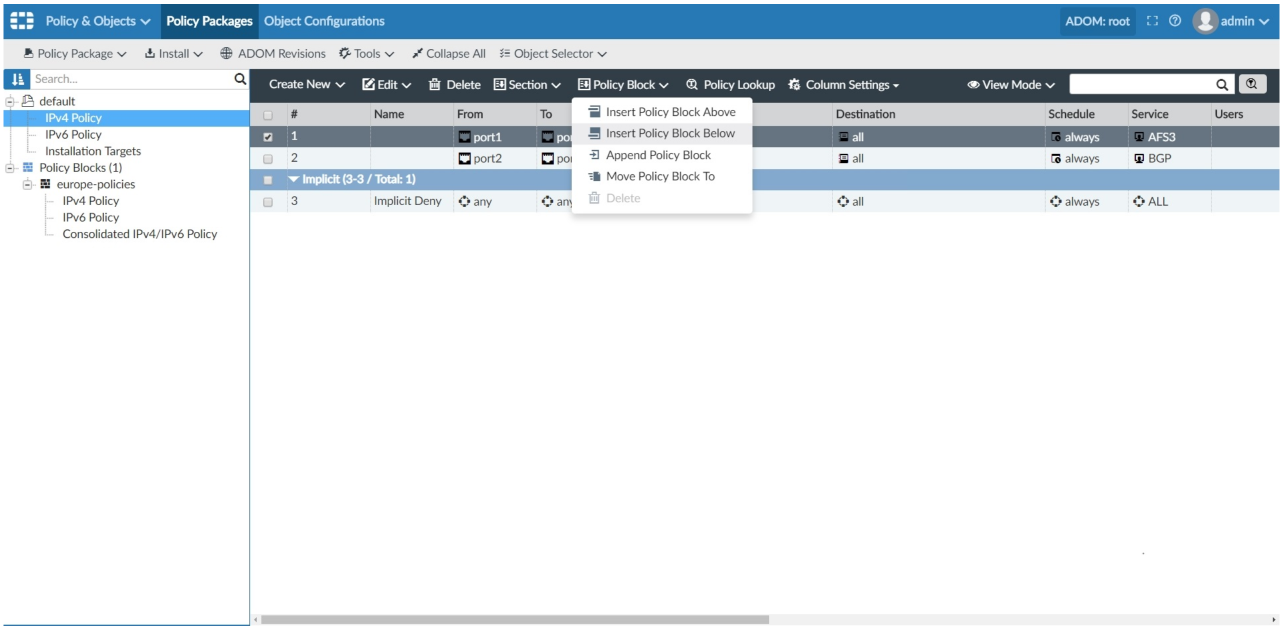
#	Name	From	To	Source	Destination	Schedule	Service	Users
1		port1	port2	all	all	always	AFS3	
2		port2	port3	all	all	always	BGP	
Implicit (3-3 / Total: 1)								
3	Imp					always	ALL	

4. Create a few policies in the new Policy Block. Policy ID in policy block is in a special defined range, similar to the Global header and footer policies.



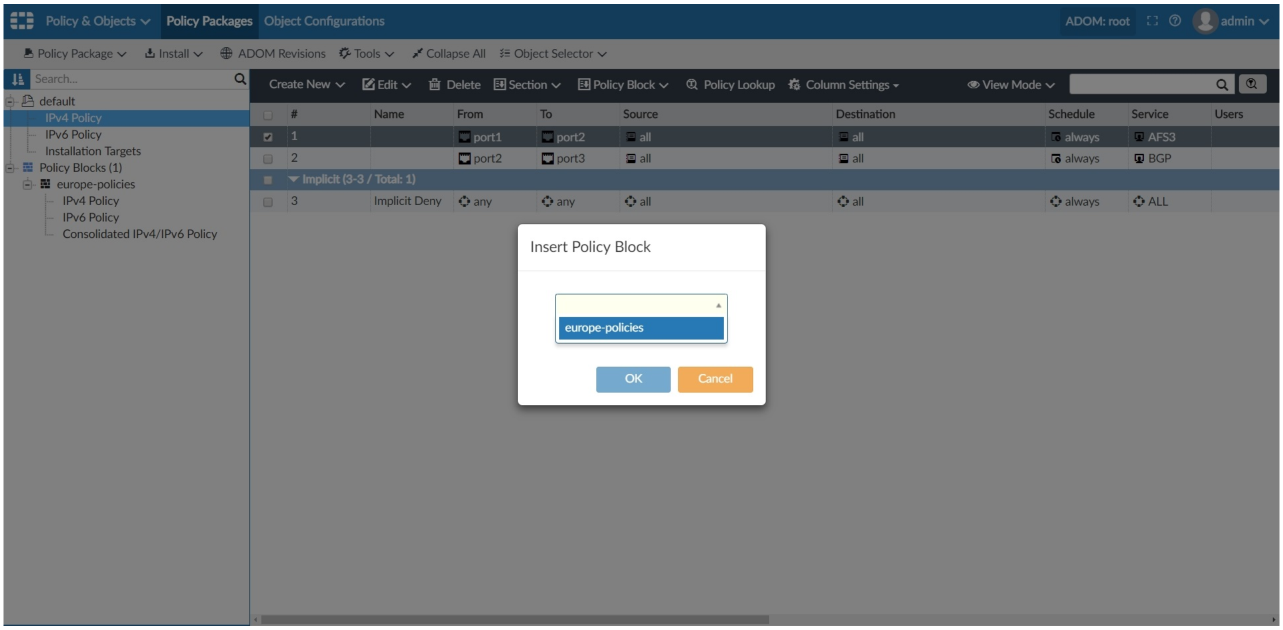
#	ID	Name	From	To	Source	Destination	Schedule	Service
1	1071741825		port5	port6	anchor_controller-10.237.36.180/32	gbl-block-108.208.86.176/32	always	ALL
2	1071741826		port8	port7	gbl-block-108.208.36.176/32	anchor_controller-10.237.36.181/32	always	ALL

5. Select a policy and click *Policy Block > Insert Policy Block Below*.



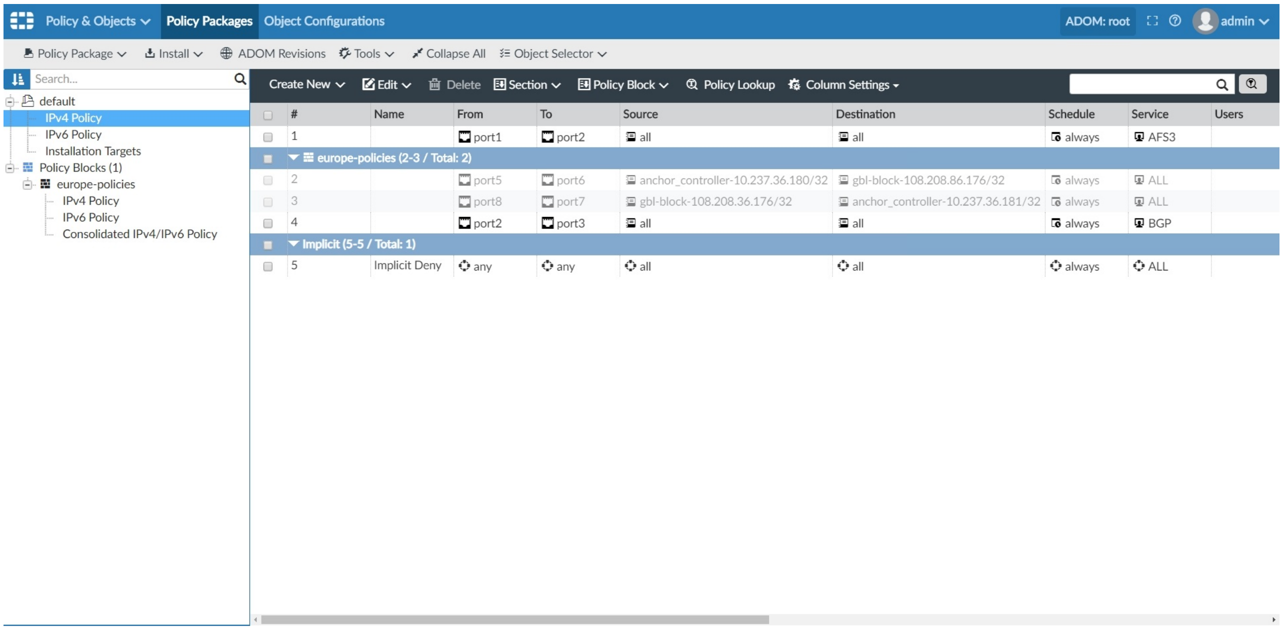
□	#	Name	From	To	Destination	Schedule	Service	Users
☑	1		port1	po	all	always	AFS3	
□	2		port2	po	all	always	BGP	
□	Implicit (3-3 / Total: 1)							
□	3	Implicit Deny	any	any	all	always	ALL	

6. Select the *Policy Block* to insert. Click *OK*.



□	#	Name	From	To	Source	Destination	Schedule	Service	Users
☑	1		port1	port2	all	all	always	AFS3	
□	2		port2	port3	all	all	always	BGP	
□	Implicit (3-3 / Total: 1)								
□	3	Implicit Deny	any	any	all	all	always	ALL	

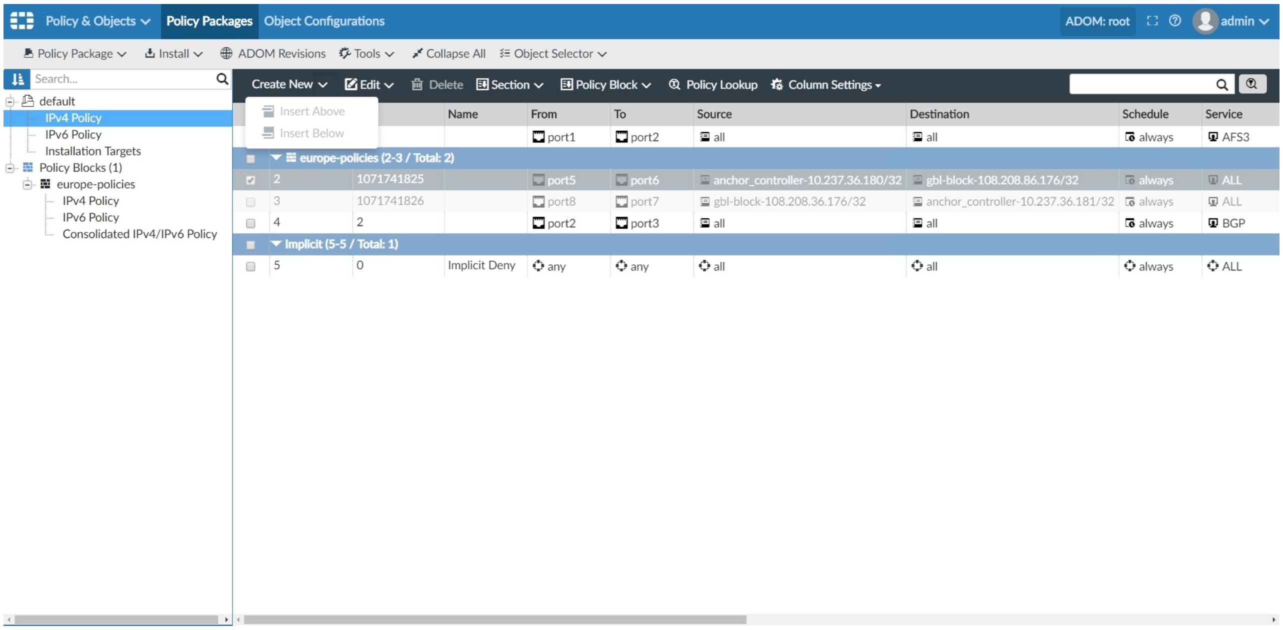
7. The Policy Block is inserted into the package.



☐	#	Name	From	To	Source	Destination	Schedule	Service	Users
☐	1		port1	port2	all	all	always	AFS3	
☐	europe-policies (2-3 / Total: 2)								
☐	2		port5	port6	anchor_controller-10.237.36.180/32	gbl-block-108.208.86.176/32	always	ALL	
☐	3		port8	port7	gbl-block-108.208.36.176/32	anchor_controller-10.237.36.181/32	always	ALL	
☐	4		port2	port3	all	all	always	BGP	
☐	Implicit (5-5 / Total: 1)								
☐	5	Implicit Deny	any	any	all	all	always	ALL	

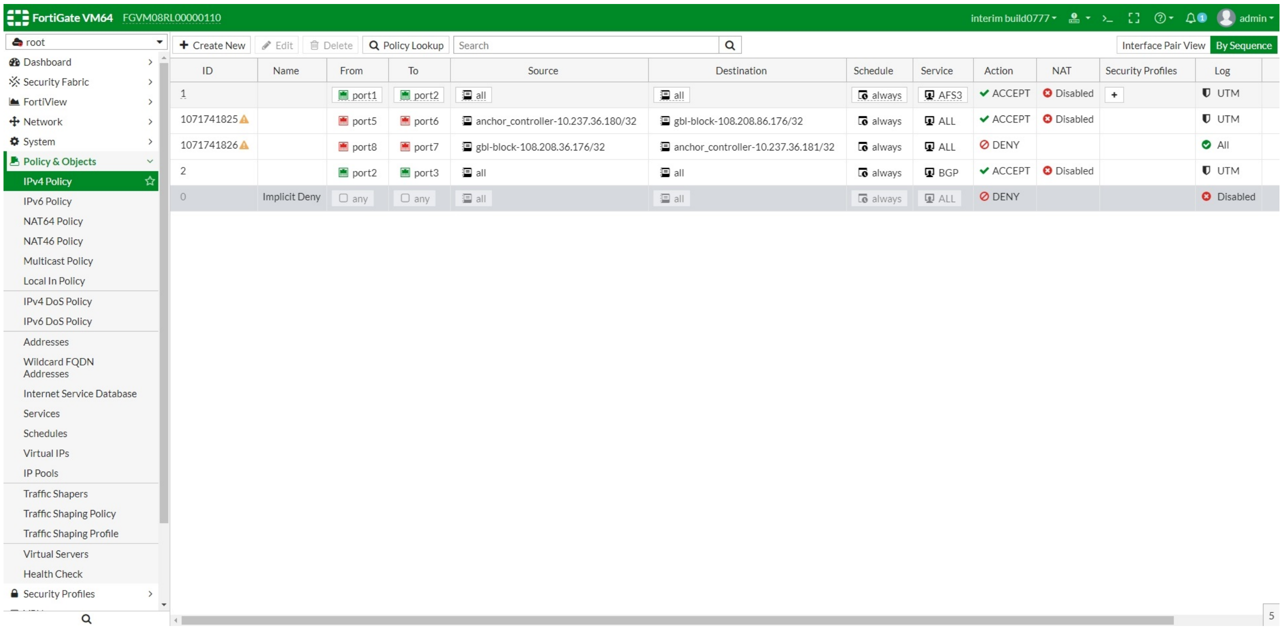
Important information about Policy Blocks

- A Policy Block can be added or removed from a Policy Package. But an individual policy in a Policy Block cannot be added, edited or deleted in a policy package. When a policy is selected, relevant menu items are grayed out.



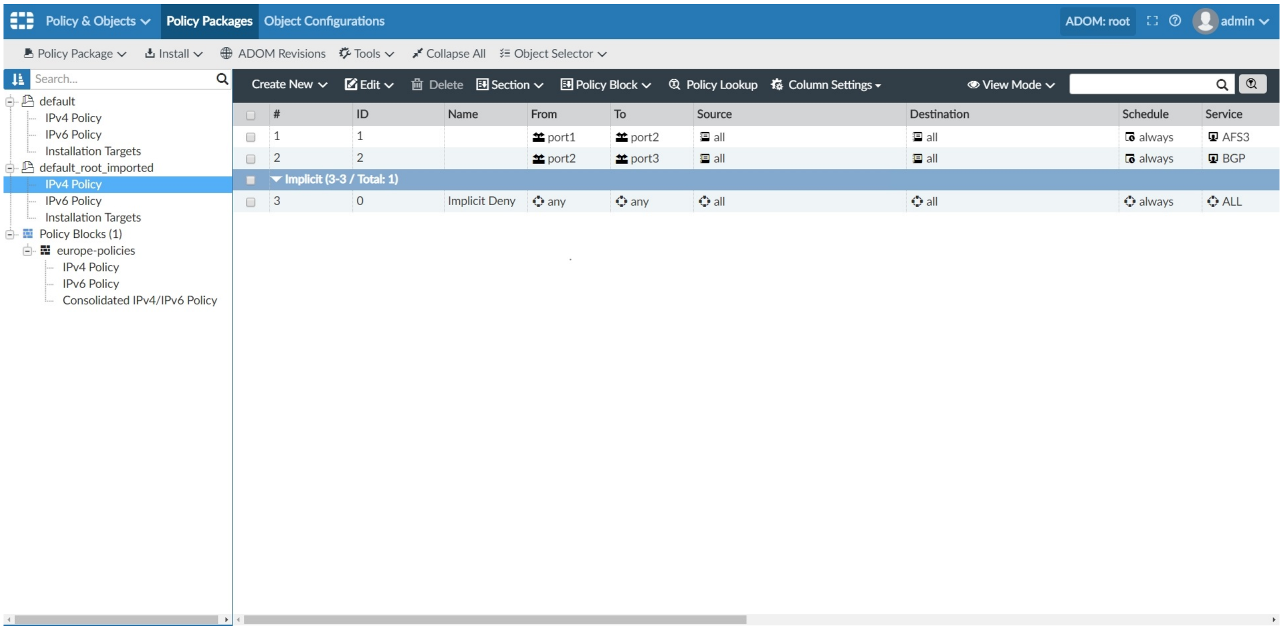
			Name	From	To	Source	Destination	Schedule	Service
				port1	port2	all	all	always	AFS3
☐	europe-policies (2-3 / Total: 2)								
☑	2	1071741825		port5	port6	anchor_controller-10.237.36.180/32	gbl-block-108.208.86.176/32	always	ALL
☐	3	1071741826		port8	port7	gbl-block-108.208.36.176/32	anchor_controller-10.237.36.181/32	always	ALL
☐	4	2		port2	port3	all	all	always	BGP
☐	Implicit (5-5 / Total: 1)								
☐	5	0	Implicit Deny	any	any	all	all	always	ALL

- The policy block is for FortiManager only. It is not installed to FortiGate. FortiGate shows individual policies only.



ID	Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log
1		port1	port2	all	all	always	AFS3	✓ ACCEPT	Disabled	+	UTM
1071741825		port5	port6	anchor_controller-10.237.36.180/32	gbl-block-108.208.86.176/32	always	ALL	✓ ACCEPT	Disabled		UTM
1071741826		port8	port7	gbl-block-108.208.36.176/32	anchor_controller-10.237.36.181/32	always	ALL	DENY			All
2		port2	port3	all	all	always	BGP	✓ ACCEPT	Disabled		UTM
0	Implicit Deny	any	any	all	all	always	ALL	DENY			Disabled

- When importing a FortiGate to a policy package, Policy Blocks are not imported. In this example, only two policies are imported to FortiManager.



	#	ID	Name	From	To	Source	Destination	Schedule	Service
□	1	1		port1	port2	all	all	always	AFS3
□	2	2		port2	port3	all	all	always	BGP
□	Implicit (3-3 / Total: 1)								
□	3	0	Implicit Deny	any	any	all	all	always	ALL

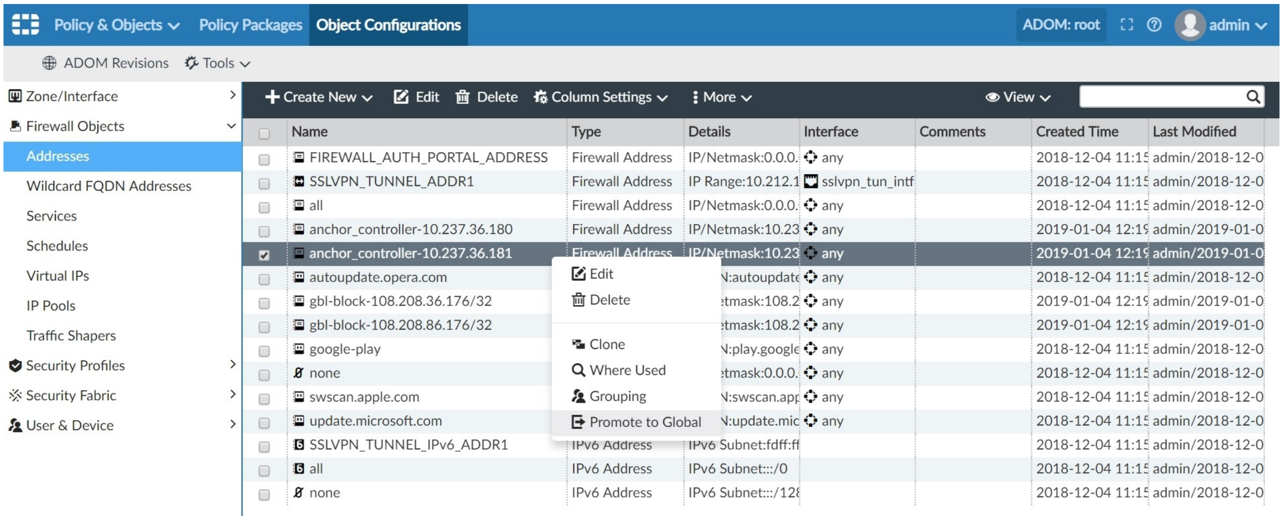
Promote Objects (LOCAL > GLOBAL)

Administrators can promote an object from an ADOM to Global Database. This can be an object imported from a FortiGate device or created on FortiManager. Once the object is promoted to the Global Database, it can be reused by other ADOMs and need not be re-created.

See Promoting Objects to Global Database.

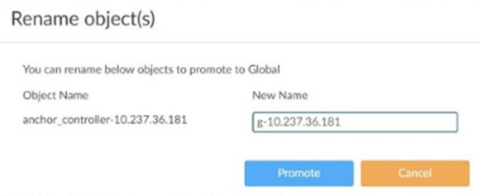
To promote objects from ADOM to Global Database:

1. Go to *Policy and Objects* > *Object Configurations*.
2. Right-click an object and click *Promote to Global*.



□	Name	Type	Details	Interface	Comments	Created Time	Last Modified
□	FIREWALL_AUTH_PORTAL_ADDRESS	Firewall Address	IP/Netmask:0.0.0.	any		2018-12-04 11:15	admin/2018-12-0
□	SSLVPN_TUNNEL_ADDR1	Firewall Address	IP Range:10.212.1	sslvpn_tun_intf		2018-12-04 11:15	admin/2018-12-0
□	all	Firewall Address	IP/Netmask:0.0.0.	any		2018-12-04 11:15	admin/2018-12-0
□	anchor_controller-10.237.36.180	Firewall Address	IP/Netmask:10.23	any		2019-01-04 12:19	admin/2019-01-0
☑	anchor_controller-10.237.36.181	Firewall Address	IP/Netmask:10.23	any		2019-01-04 12:19	admin/2019-01-0
□	autoupdate.opera.com		N:autoupdate	any		2018-12-04 11:15	admin/2018-12-0
□	gbl-block-108.208.36.176/32		etmask:108.2	any		2019-01-04 12:19	admin/2019-01-0
□	gbl-block-108.208.86.176/32		etmask:108.2	any		2019-01-04 12:19	admin/2019-01-0
□	google-play		N:play.google	any		2018-12-04 11:15	admin/2018-12-0
□	none		etmask:0.0.0.	any		2018-12-04 11:15	admin/2018-12-0
□	swscan.apple.com		N:swscan.app	any		2018-12-04 11:15	admin/2018-12-0
□	update.microsoft.com		N:update.mic	any		2018-12-04 11:15	admin/2018-12-0
□	SSLVPN_TUNNEL_IPv6_ADDR1	IPv6 Address	IPv6 Subnet:fdff:ff			2018-12-04 11:15	admin/2018-12-0
□	all	IPv6 Address	IPv6 Subnet:::/0			2018-12-04 11:15	admin/2018-12-0
□	none	IPv6 Address	IPv6 Subnet:::/128			2018-12-04 11:15	admin/2018-12-0

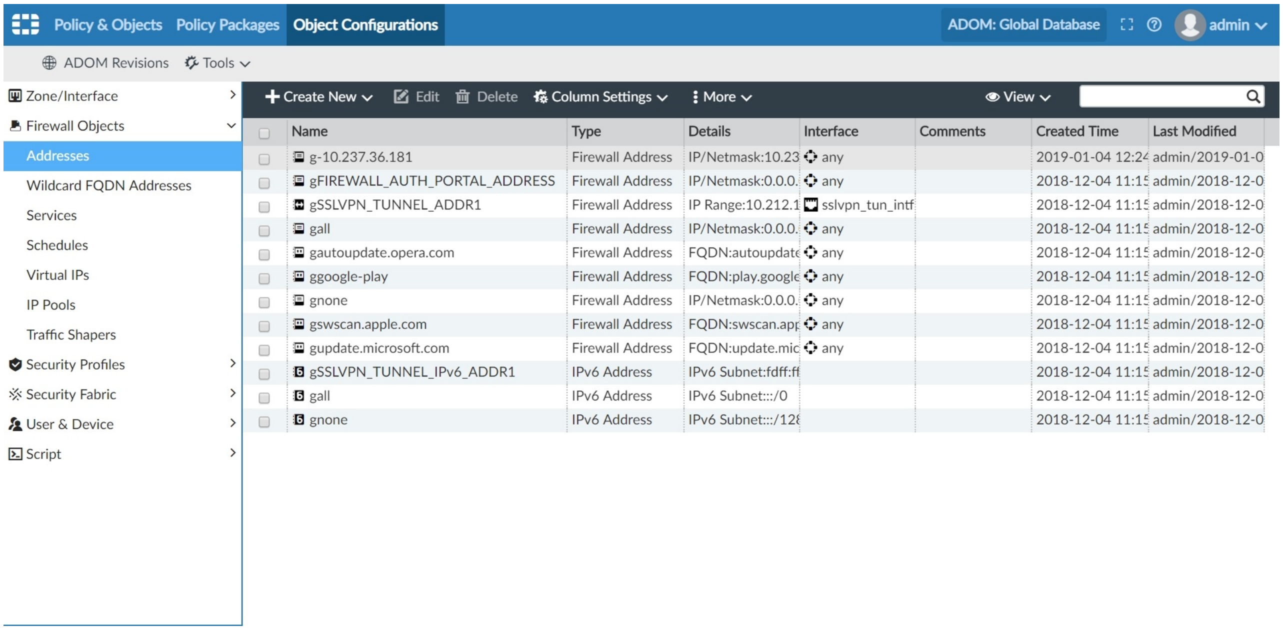
3. Specify a new name in the *Rename object(s)* dialog. If you do not specify a new name, the object will be promoted with the same name which may create a conflict if the Global database already contains an object with the same name.
4. Click *Promote*. The object is now promoted to the Global Database.



You can rename below objects to promote to Global

Object Name	New Name
anchor_controller-10.237.36.181	g-10.237.36.181

5. Switch the ADOM to *Global Database* to verify the promoted object.



□	Name	Type	Details	Interface	Comments	Created Time	Last Modified
□	g-10.237.36.181	Firewall Address	IP/Netmask:10.23	any		2019-01-04 12:24	admin/2019-01-0
□	gFIREWALL_AUTH_PORTAL_ADDRESS	Firewall Address	IP/Netmask:0.0.0.	any		2018-12-04 11:15	admin/2018-12-0
□	gSSLVPN_TUNNEL_ADDR1	Firewall Address	IP Range:10.212.1	sslvpn_tun_intf		2018-12-04 11:15	admin/2018-12-0
□	gall	Firewall Address	IP/Netmask:0.0.0.	any		2018-12-04 11:15	admin/2018-12-0
□	gautoupdate.opera.com	Firewall Address	FQDN:autoupdate	any		2018-12-04 11:15	admin/2018-12-0
□	ggoogle-play	Firewall Address	FQDN:play.google	any		2018-12-04 11:15	admin/2018-12-0
□	gnone	Firewall Address	IP/Netmask:0.0.0.	any		2018-12-04 11:15	admin/2018-12-0
□	gswscan.apple.com	Firewall Address	FQDN:swscan.app	any		2018-12-04 11:15	admin/2018-12-0
□	gupdate.microsoft.com	Firewall Address	FQDN:update.mic	any		2018-12-04 11:15	admin/2018-12-0
□	gSSLVPN_TUNNEL_IPv6_ADDR1	IPv6 Address	IPv6 Subnet:fdff:ff			2018-12-04 11:15	admin/2018-12-0
□	gall	IPv6 Address	IPv6 Subnet:::/0			2018-12-04 11:15	admin/2018-12-0
□	gnone	IPv6 Address	IPv6 Subnet:::/128			2018-12-04 11:15	admin/2018-12-0

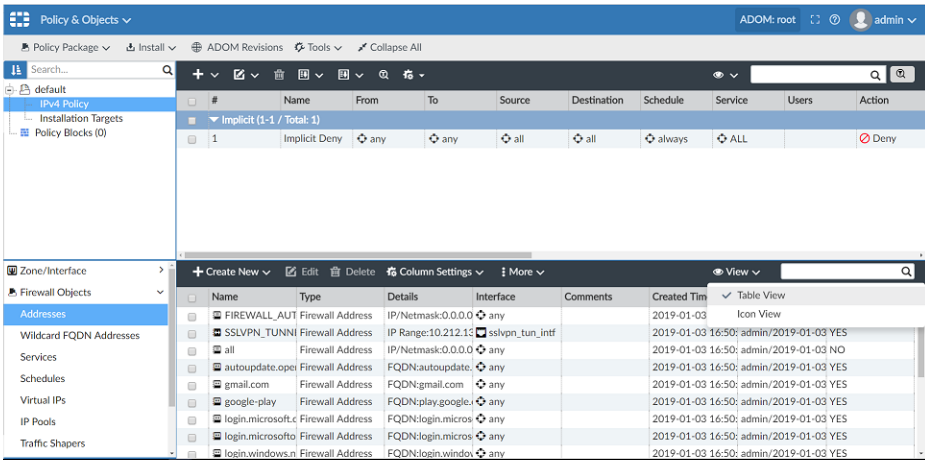
Address Icon/Tile View

View the objects as Icons or in a table format. This provides a better visual presentation of objects in a user-defined format.

See Search Objects.

Improvements in Icon or Table view

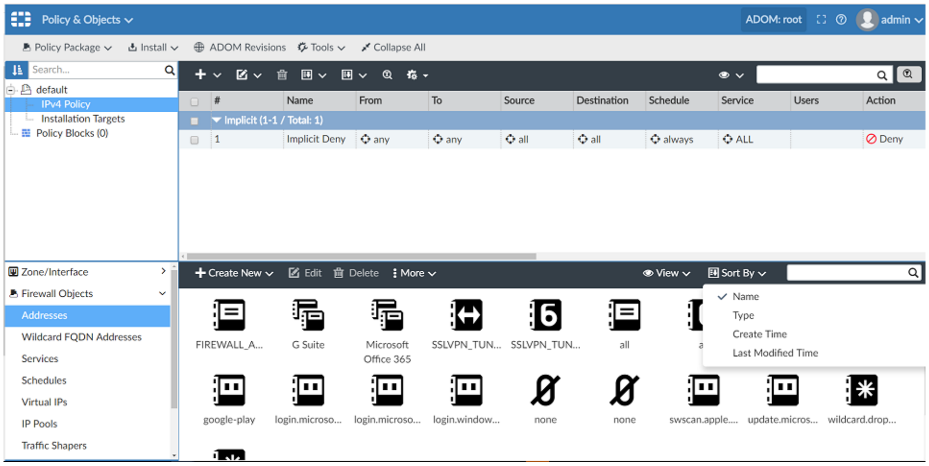
- Switch between views - select *View* > *Icon View* or *View* > *Table View* to switch between views.



#	Name	From	To	Source	Destination	Schedule	Service	Users	Action
Implicit (1-1 / Total: 1)									
1	Implicit Deny	any	any	all	all	always	ALL		Deny

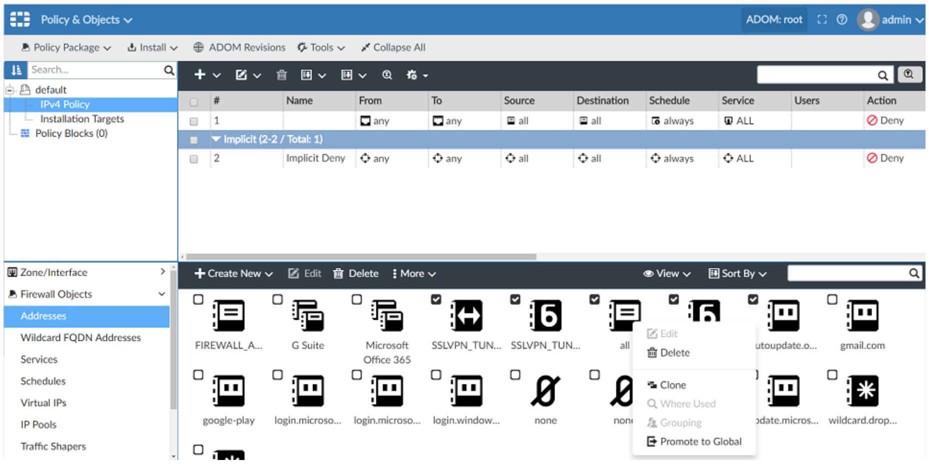
Name	Type	Details	Interface	Comments	Created Tim		
FIREWALL_AUT	Firewall Address	IP/Netmask:0.0.0.0	any		2019-01-03		
SSLVPN_TUNNI	Firewall Address	IP Range:10.212.13	sslvpn_tun_intf		2019-01-03 16:50:	admin/2019-01-03	YES
all	Firewall Address	IP/Netmask:0.0.0.0	any		2019-01-03 16:50:	admin/2019-01-03	NO
autoupdate.opei	Firewall Address	FQDN:autoupdate.	any		2019-01-03 16:50:	admin/2019-01-03	YES
gmail.com	Firewall Address	FQDN:gmail.com	any		2019-01-03 16:50:	admin/2019-01-03	YES
google-play	Firewall Address	FQDN:play.google.c	any		2019-01-03 16:50:	admin/2019-01-03	YES
login.microsoft.c	Firewall Address	FQDN:login.micros	any		2019-01-03 16:50:	admin/2019-01-03	YES
login.microsofto	Firewall Address	FQDN:login.micros	any		2019-01-03 16:50:	admin/2019-01-03	YES
login.windows.n	Firewall Address	FQDN:login.windov	any		2019-01-03 16:50:	admin/2019-01-03	YES

- Sort by Menu - sort by Name, Type, Create Time, and Last Modified Time



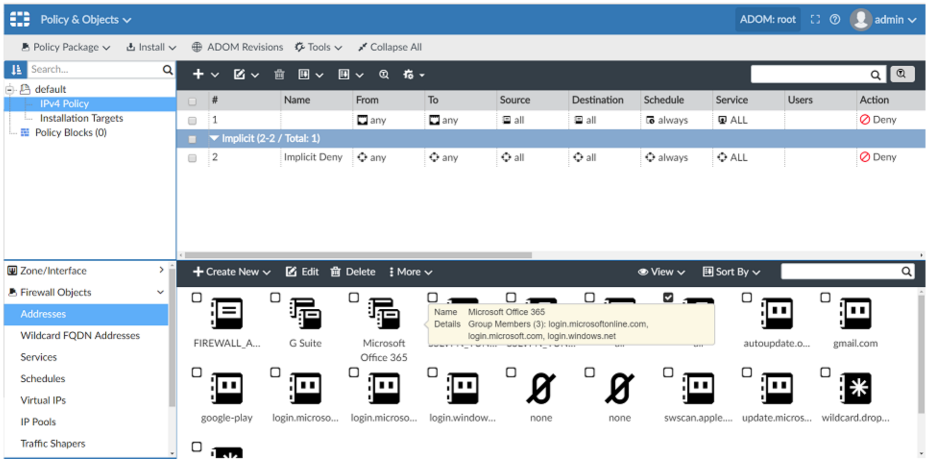
#	Name	From	To	Source	Destination	Schedule	Service	Users	Action
Implicit (1-1 / Total: 1)									
1	Implicit Deny	any	any	all	all	always	ALL		Deny

- Select multiple objects - select multiple objects to *Promote to Global*, *Clone* or *Delete* the objects.



#	Name	From	To	Source	Destination	Schedule	Service	Users	Action
1		any	any	all	all	always	ALL		Deny
Implicit (2-2 / Total: 1)									
2	Implicit Deny	any	any	all	all	always	ALL		Deny

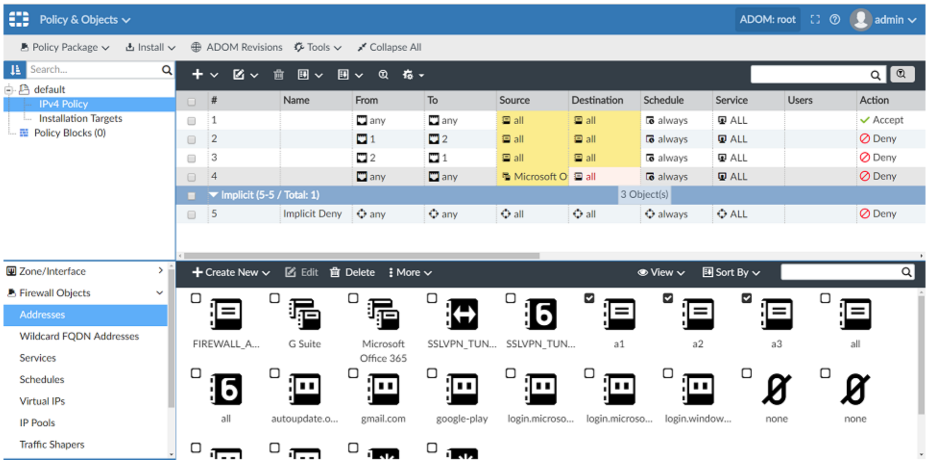
- Tool-tip - mouse-over the object for more information about the object.



#	Name	From	To	Source	Destination	Schedule	Service	Users	Action
1		any	any	all	all	always	ALL		Deny
Implicit (2-2 / Total: 1)									
2	Implicit Deny	any	any	all	all	always	ALL		Deny

Name Microsoft Office 365
Details Group Members (3): login.microsoftonline.com, login.microsoft.com, login.windows.net

- Drag and drop - drag and drop single or multiple objects into the policy in dual pane display mode.



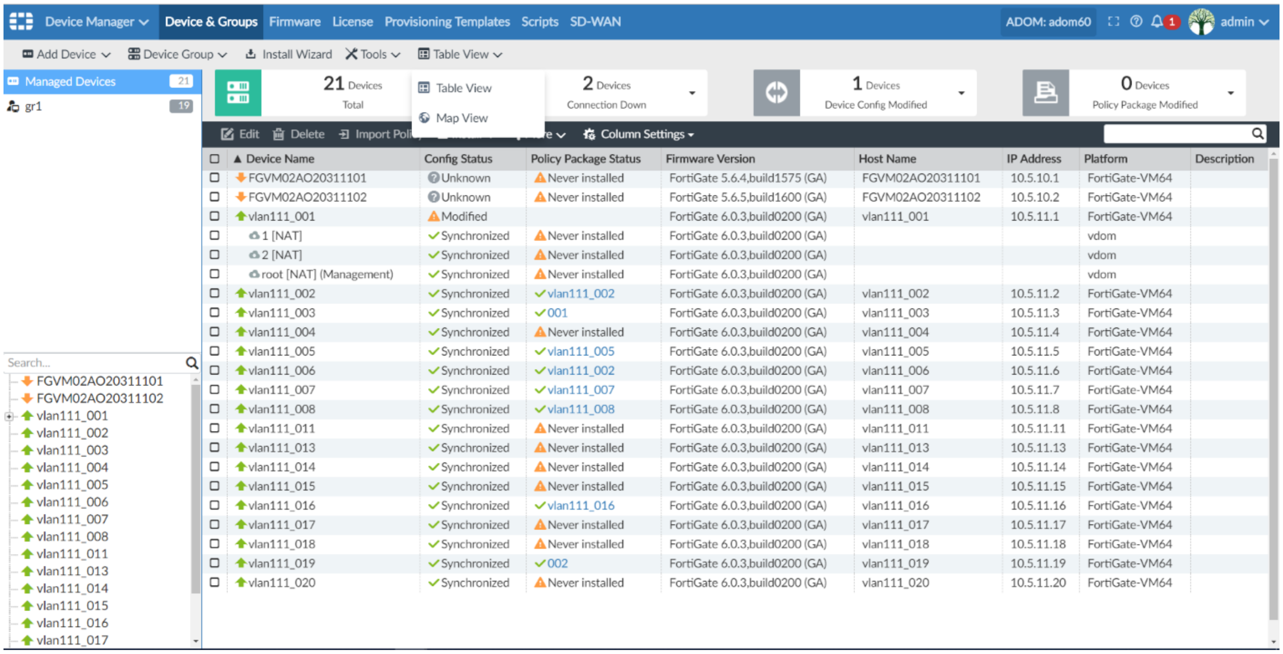
#	Name	From	To	Source	Destination	Schedule	Service	Users	Action
1		any	any	all	all	always	ALL		Accept
2		1	2	all	all	always	ALL		Deny
3		2	1	all	all	always	ALL		Deny
4		any	any	Microsoft O	all	always	ALL		Deny
Implicit (5-5 / Total: 1)									
5	Implicit Deny	any	any	all	all	always	ALL		Deny

Device Manager Map View

Automatically view the location of FortiGate devices on Google Maps. Manually configure the location of the FortiGate from FortiManager. Perform various actions directly from the Map View.

Map View feature

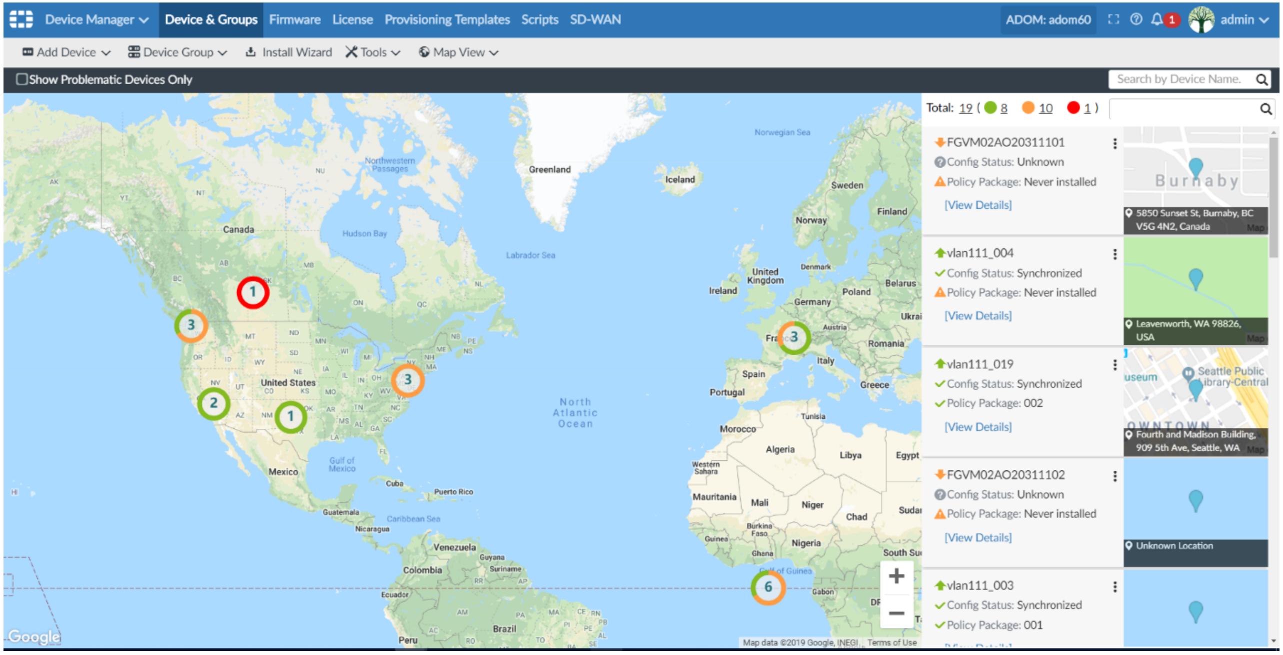
1. Go to Device Manager and select *Map View* from the menu options.



□	▲ Device Name	Config Status	Policy Package Status	Firmware Version	Host Name	IP Address	Platform	Description
□	FGVM02AO20311101	Unknown	Never installed	FortiGate 5.6.4,build1575 (GA)	FGVM02AO20311101	10.5.10.1	FortiGate-VM64	
□	FGVM02AO20311102	Unknown	Never installed	FortiGate 5.6.5,build1600 (GA)	FGVM02AO20311102	10.5.10.2	FortiGate-VM64	
□	vlan111_001	Modified		FortiGate 6.0.3,build0200 (GA)	vlan111_001	10.5.11.1	FortiGate-VM64	
□	1 [NAT]	✓Synchronized	Never installed	FortiGate 6.0.3,build0200 (GA)			vdom	
□	2 [NAT]	✓Synchronized	Never installed	FortiGate 6.0.3,build0200 (GA)			vdom	
□	root [NAT] (Management)	✓Synchronized	Never installed	FortiGate 6.0.3,build0200 (GA)			vdom	
□	vlan111_002	✓Synchronized	✓vlan111_002	FortiGate 6.0.3,build0200 (GA)	vlan111_002	10.5.11.2	FortiGate-VM64	
□	vlan111_003	✓Synchronized	✓001	FortiGate 6.0.3,build0200 (GA)	vlan111_003	10.5.11.3	FortiGate-VM64	
□	vlan111_004	✓Synchronized	Never installed	FortiGate 6.0.3,build0200 (GA)	vlan111_004	10.5.11.4	FortiGate-VM64	
□	vlan111_005	✓Synchronized	✓vlan111_005	FortiGate 6.0.3,build0200 (GA)	vlan111_005	10.5.11.5	FortiGate-VM64	
□	vlan111_006	✓Synchronized	✓vlan111_002	FortiGate 6.0.3,build0200 (GA)	vlan111_006	10.5.11.6	FortiGate-VM64	
□	vlan111_007	✓Synchronized	✓vlan111_007	FortiGate 6.0.3,build0200 (GA)	vlan111_007	10.5.11.7	FortiGate-VM64	
□	vlan111_008	✓Synchronized	✓vlan111_008	FortiGate 6.0.3,build0200 (GA)	vlan111_008	10.5.11.8	FortiGate-VM64	
□	vlan111_011	✓Synchronized	Never installed	FortiGate 6.0.3,build0200 (GA)	vlan111_011	10.5.11.11	FortiGate-VM64	
□	vlan111_013	✓Synchronized	Never installed	FortiGate 6.0.3,build0200 (GA)	vlan111_013	10.5.11.13	FortiGate-VM64	
□	vlan111_014	✓Synchronized	Never installed	FortiGate 6.0.3,build0200 (GA)	vlan111_014	10.5.11.14	FortiGate-VM64	
□	vlan111_015	✓Synchronized	Never installed	FortiGate 6.0.3,build0200 (GA)	vlan111_015	10.5.11.15	FortiGate-VM64	
□	vlan111_016	✓Synchronized	✓vlan111_016	FortiGate 6.0.3,build0200 (GA)	vlan111_016	10.5.11.16	FortiGate-VM64	
□	vlan111_017	✓Synchronized	Never installed	FortiGate 6.0.3,build0200 (GA)	vlan111_017	10.5.11.17	FortiGate-VM64	
□	vlan111_018	✓Synchronized	Never installed	FortiGate 6.0.3,build0200 (GA)	vlan111_018	10.5.11.18	FortiGate-VM64	
□	vlan111_019	✓Synchronized	✓002	FortiGate 6.0.3,build0200 (GA)	vlan111_019	10.5.11.19	FortiGate-VM64	
□	vlan111_020	✓Synchronized	Never installed	FortiGate 6.0.3,build0200 (GA)	vlan111_020	10.5.11.20	FortiGate-VM64	

2. Map view shows device location on Google Maps and a combined status in Green, Orange, and Red colors.
   - Green - Shows devices are healthy. The policy package configuration and device configuration are in sync.
   - Orange - Shows a warning status. The device configuration status or policy package configuration status is *Out of Sync*. Or, there is no policy imported or no policy package installed.

- Red - Shows an error status. Copy has failed, installation has failed or device connection is down.



Total: 19 (● 8 ● 10 ● 1)

FGVM02AO20311101
Config Status: Unknown
Policy Package: Never installed
[View Details]
5850 Sunset St, Burnaby, BC V5G 4N2, Canada

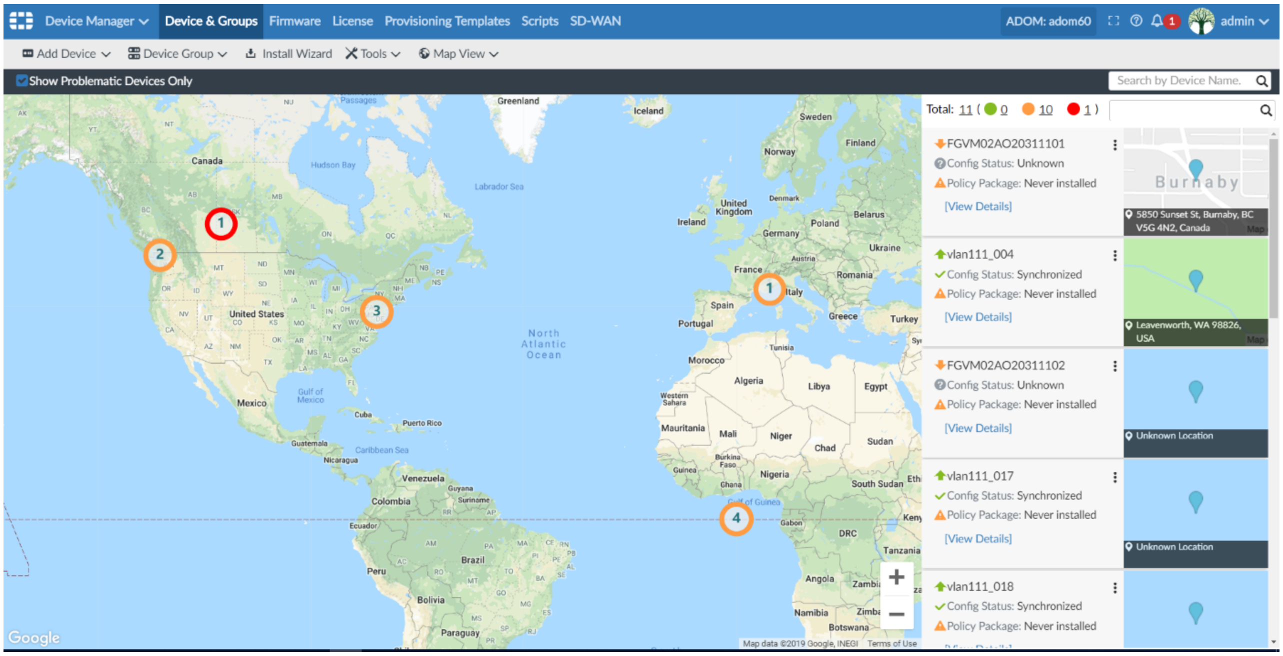
vlan111_004
Config Status: Synchronized
Policy Package: Never installed
[View Details]
Leavenworth, WA 98826, USA

vlan111_019
Config Status: Synchronized
Policy Package: 002
[View Details]
Fourth and Madison Building, 909 5th Ave, Seattle, WA

FGVM02AO20311102
Config Status: Unknown
Policy Package: Never installed
[View Details]
Unknown Location

vlan111_003
Config Status: Synchronized
Policy Package: 001

3. Select *Show Problematic Devices Only* to filter devices on the map and show it on the right pane with *Orange* or *Red* status.



Total: 11 (● 0 ● 10 ● 1)

FGVM02AO20311101
Config Status: Unknown
Policy Package: Never installed
[View Details]
5850 Sunset St, Burnaby, BC V5G 4N2, Canada

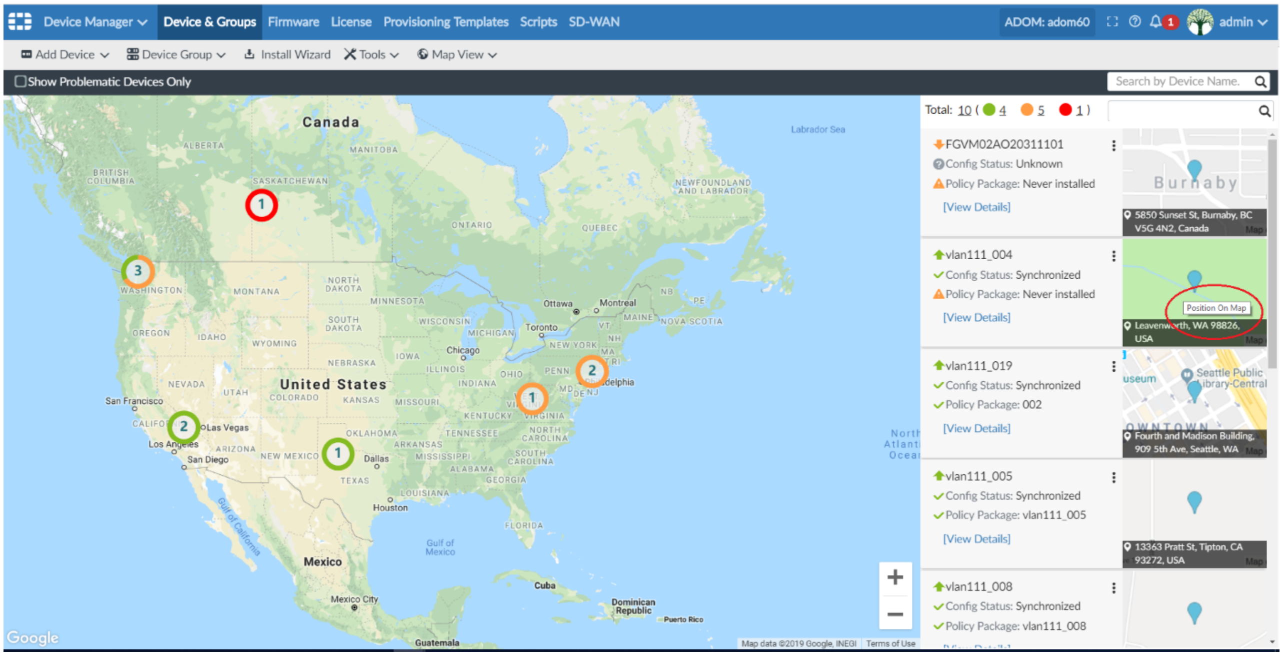
vlan111_004
Config Status: Synchronized
Policy Package: Never installed
[View Details]
Leavenworth, WA 98826, USA

FGVM02AO20311102
Config Status: Unknown
Policy Package: Never installed
[View Details]
Unknown Location

vlan111_017
Config Status: Synchronized
Policy Package: Never installed
[View Details]
Unknown Location

vlan111_018
Config Status: Synchronized
Policy Package: Never installed

4. To manually position a device, click the device shown on the smaller map on the right pane.



Total: 10 (● 4 ● 5 ● 1)

FGVM02AO20311101
Config Status: Unknown
Policy Package: Never installed
[View Details]
5850 Sunset St, Burnaby, BC V5G 4N2, Canada

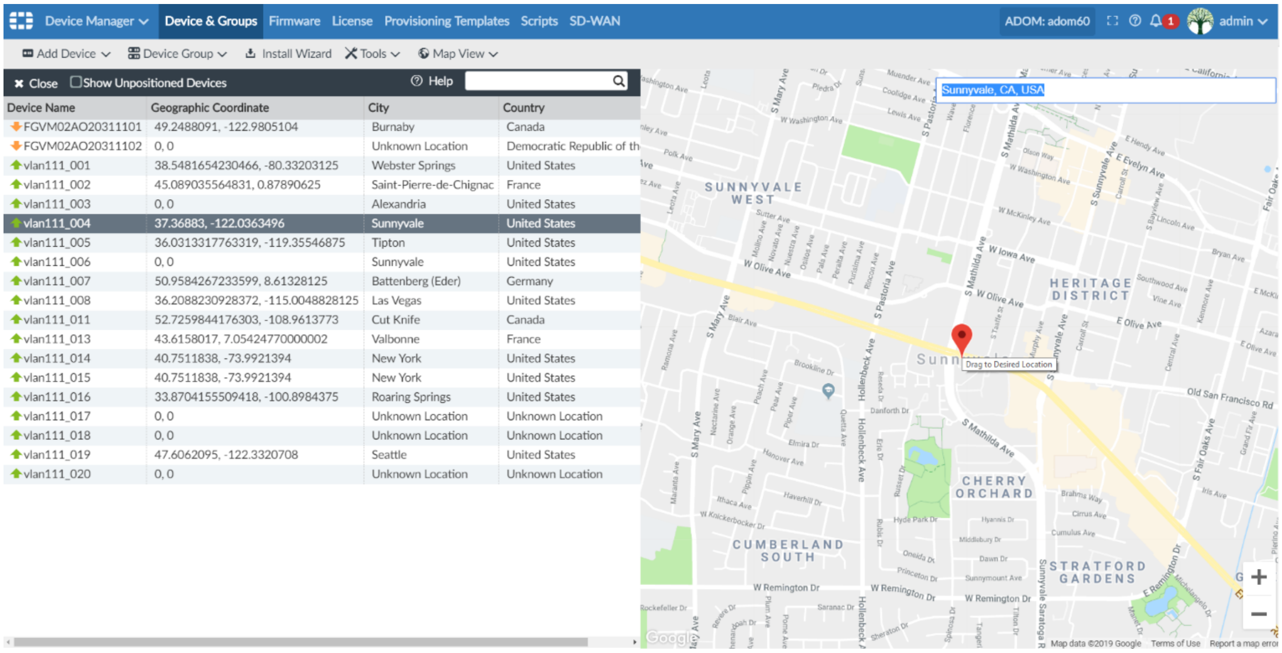
vlan111_004
Config Status: Synchronized
Policy Package: Never installed
[View Details]
Leavenworth, WA 98826, USA

vlan111_019
Config Status: Synchronized
Policy Package: 002
[View Details]
Fourth and Madison Building, 909 5th Ave, Seattle, WA

vlan111_005
Config Status: Synchronized
Policy Package: vlan111_005
[View Details]
13363 Pratt St, Tipton, CA 93272, USA

vlan111_008
Config Status: Synchronized
Policy Package: vlan111_008

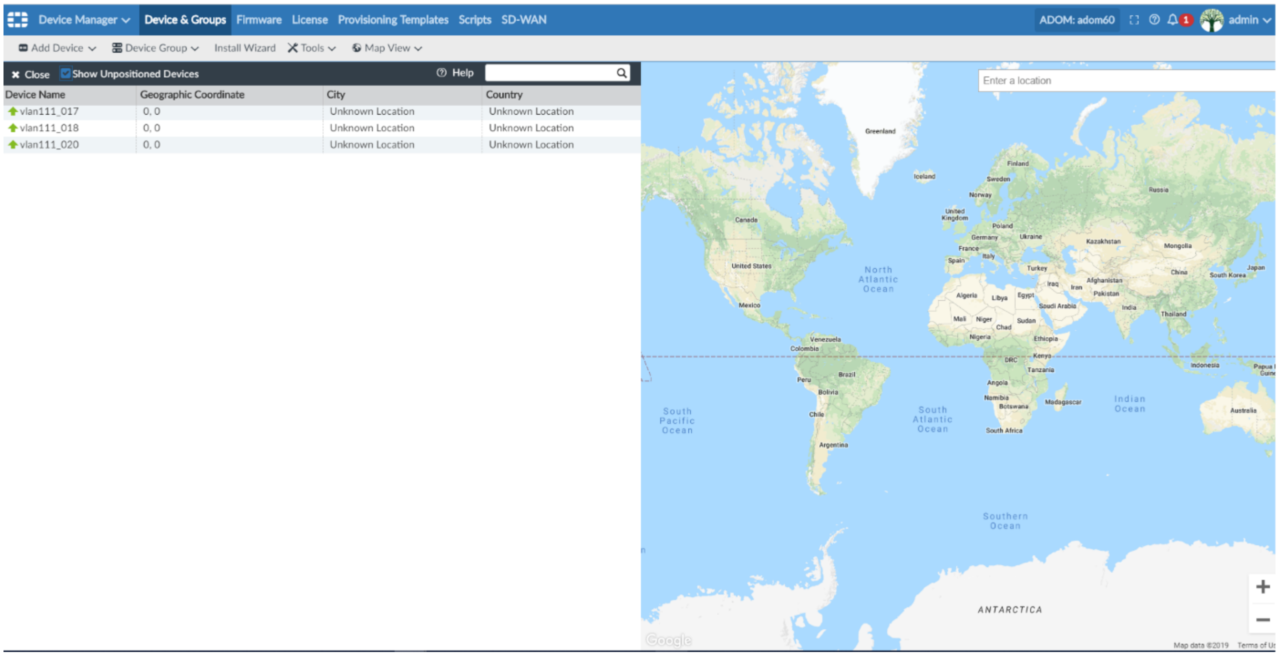
5. Enter the location of the device manually. You can also drag the device to the accurate position.



Sunnyvale, CA, USA

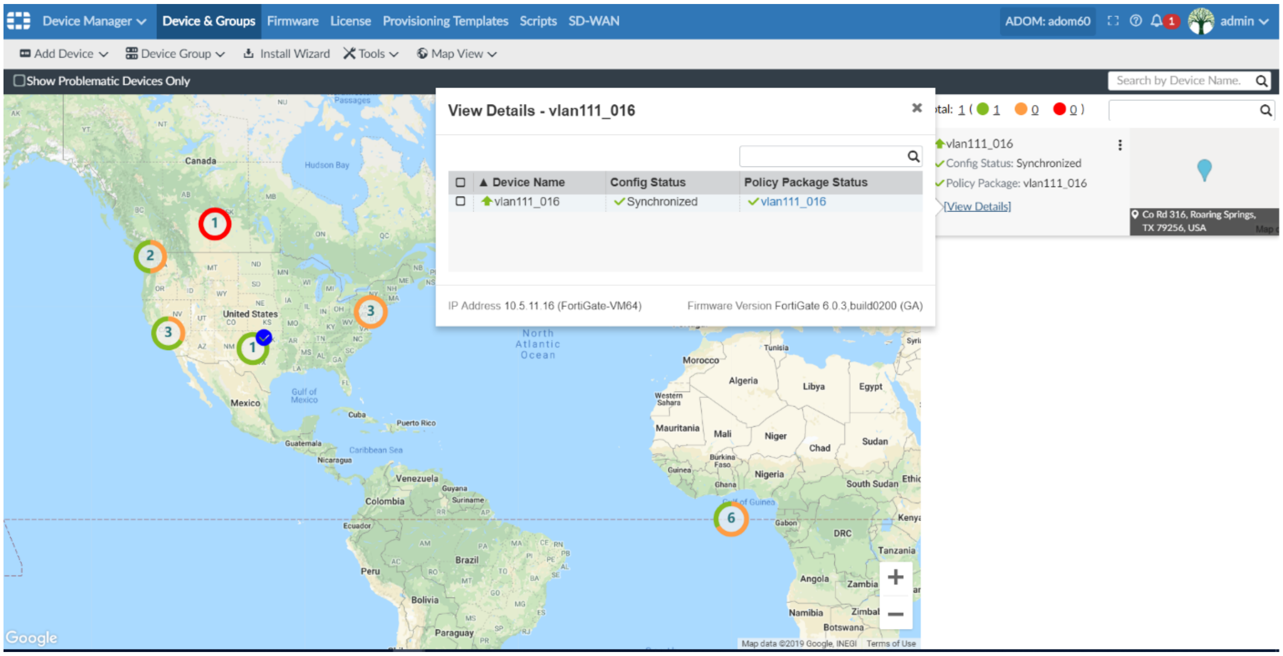
Device Name	Geographic Coordinate	City	Country
FGVM02AO20311101	49.2488091, -122.9805104	Burnaby	Canada
FGVM02AO20311102	0, 0	Unknown Location	Democratic Republic of th
vlan111_001	38.5481654230466, -80.33203125	Webster Springs	United States
vlan111_002	45.089035564831, 0.87890625	Saint-Pierre-de-Chignac	France
vlan111_003	0, 0	Alexandria	United States
vlan111_004	37.36883, -122.0363496	Sunnyvale	United States
vlan111_005	36.0313317763319, -119.35546875	Tipton	United States
vlan111_006	0, 0	Sunnyvale	United States
vlan111_007	50.9584267233599, 8.61328125	Battenberg (Eder)	Germany
vlan111_008	36.2088230928372, -115.0048828125	Las Vegas	United States
vlan111_011	52.7259844176303, -108.9613773	Cut Knife	Canada
vlan111_013	43.6158017, 7.05424770000002	Valbonne	France
vlan111_014	40.7511838, -73.9921394	New York	United States
vlan111_015	40.7511838, -73.9921394	New York	United States
vlan111_016	33.8704155509418, -100.8984375	Roaring Springs	United States
vlan111_017	0, 0	Unknown Location	Unknown Location
vlan111_018	0, 0	Unknown Location	Unknown Location
vlan111_019	47.6062095, -122.3320708	Seattle	United States
vlan111_020	0, 0	Unknown Location	Unknown Location

6. Click *Show Unpositioned Devices* to filter devices that do not have any location.



Device Name	Geographic Coordinate	City	Country
vlan111_017	0, 0	Unknown Location	Unknown Location
vlan111_018	0, 0	Unknown Location	Unknown Location
vlan111_020	0, 0	Unknown Location	Unknown Location

7. Click *View Details* for the device to show device configuration status and policy package status.



View Details - vlan111_016

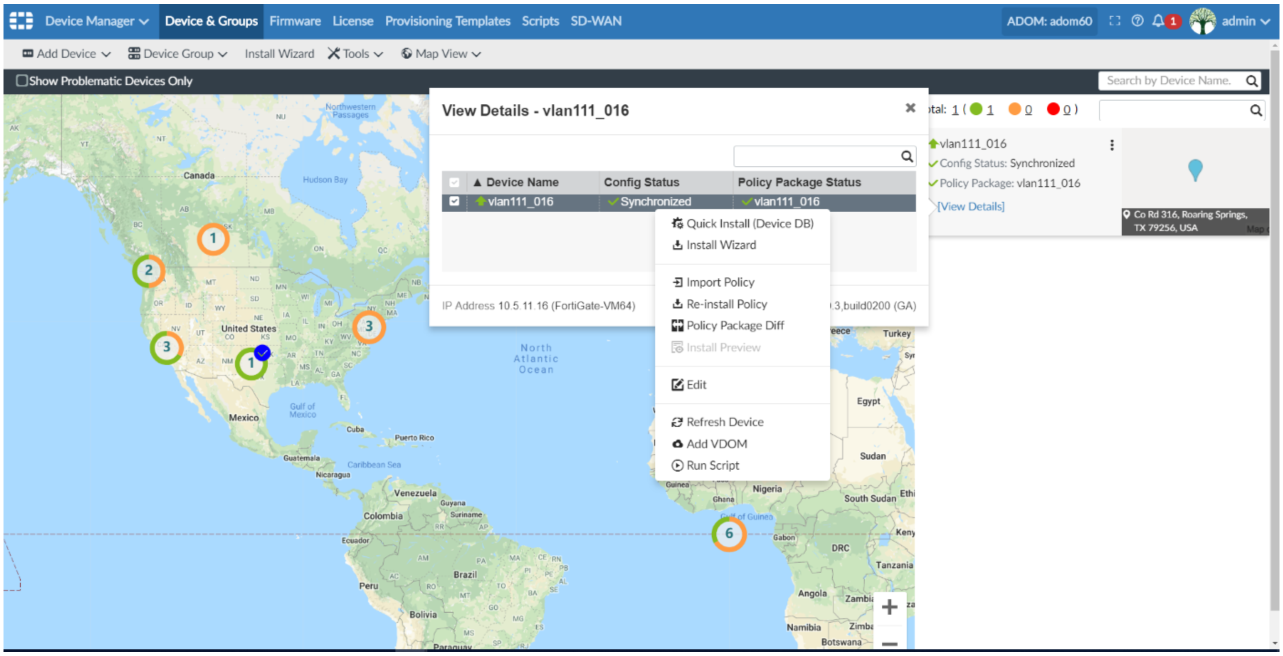
☐	▲ Device Name	Config Status	Policy Package Status
☐	vlan111_016	✓ Synchronized	✓ vlan111_016

IP Address 10.5.11.16 (FortiGate-VM64)   Firmware Version FortiGate 6.0.3,build0200 (GA)

vlan111_016
✓ Config Status: Synchronized
✓ Policy Package: vlan111_016
[View Details]

Co Rd 316, Roaring Springs, TX 79256, USA

8. Right-click the device menu to run various operations such as Quick Install, Install Wizard, Import Policy, Re-install Policy, Policy Package Diff, Edit, Refresh Device, Add VDOM, and Run Script.



View Details - vlan111_016

Device Name	Config Status	Policy Package Status
vlan111_016	Synchronized	vlan111_016

IP Address 10.5.11.16 (FortiGate-VM64)

3,build0200 (GA)

vlan111_016
Config Status: Synchronized
Policy Package: vlan111_016

Co Rd 316, Roaring Springs, TX 79256, USA

Clone Reverse Policy

Administrators can now clone a policy in such a way that the *Incoming Interface* and *Outgoing Interface* are switched in the newly cloned policy. The *Source Address* and *Destination Address* are also switched in the newly cloned policy.

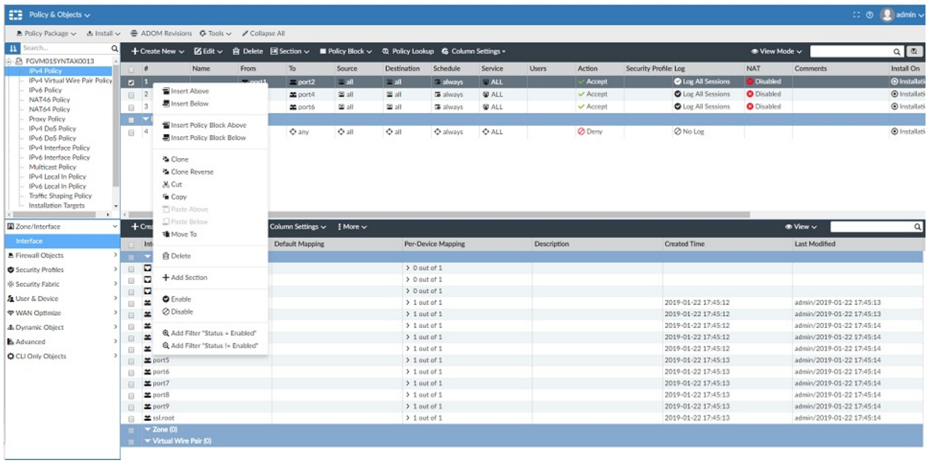
For example, if a policy is configured with the *Incoming Interface* as *port1* and the *Outgoing Interface* as *port2*, cloning the policy with *Clone Reverse* automatically sets the *Incoming Interface* as *port2* and *Outgoing Interface* as *port1*.

If a policy is configured with the *Source Address* as *update.microsoft.com* and the *Destination Address* as *all*, cloning the policy with Clone Reverse automatically sets the *Source Address* as *all* and *Destination Address* as *update.microsoft.com*.

The original policy remains unchanged.

To Clone Reverse a Policy:

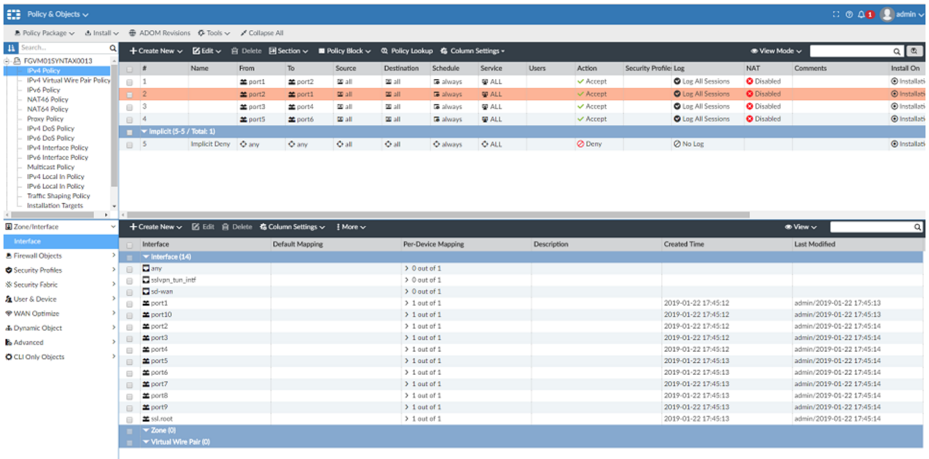
1. Select a policy and select *Clone Reverse* from the *Edit* menu.



#	Name	From	To	Source	Destination	Schedule	Service	Users	Action	Security Profile	Log	NAT	Comments	Install On
1		port1	port2	all	all	always	ALL		Accept		Log All Sessions	Disabled		Installati
2			port4	all	all	always	ALL		Accept		Log All Sessions	Disabled		Installati
3			port6	all	all	always	ALL		Accept		Log All Sessions	Disabled		Installati
4			any	all	all	always	ALL		Deny		No Log			Installati

Int	Default Mapping	Per-Device Mapping	Description	Created Time	Last Modified
		0 out of 1			
		0 out of 1			
		0 out of 1			
		1 out of 1		2019-01-22 17:45:12	admin/2019-01-22 17:45:13
		1 out of 1		2019-01-22 17:45:12	admin/2019-01-22 17:45:13
		1 out of 1		2019-01-22 17:45:12	admin/2019-01-22 17:45:14
		1 out of 1		2019-01-22 17:45:12	admin/2019-01-22 17:45:14
		1 out of 1		2019-01-22 17:45:12	admin/2019-01-22 17:45:14
port5		1 out of 1		2019-01-22 17:45:13	admin/2019-01-22 17:45:14
port6		1 out of 1		2019-01-22 17:45:13	admin/2019-01-22 17:45:14
port7		1 out of 1		2019-01-22 17:45:13	admin/2019-01-22 17:45:14
port8		1 out of 1		2019-01-22 17:45:13	admin/2019-01-22 17:45:14
port9		1 out of 1		2019-01-22 17:45:13	admin/2019-01-22 17:45:14
ssl.root		1 out of 1		2019-01-22 17:45:13	admin/2019-01-22 17:45:14
Zone (0)					
Virtual Wire Pair (0)					

2. The policy is cloned with the *Incoming Interface* and *Outgoing Interface* switched with each other. The *Source* and *Destination* are also switched with each other.



#	Name	From	To	Source	Destination	Schedule	Service	Users	Action	Security Profile	Log	NAT	Comments	Install On
1		port1	port2	all	all	always	ALL		Accept		Log All Sessions	Disabled		Installati
2		port2	port1	all	all	always	ALL		Accept		Log All Sessions	Disabled		Installati
3		port3	port4	all	all	always	ALL		Accept		Log All Sessions	Disabled		Installati
4		port5	port6	all	all	always	ALL		Accept		Log All Sessions	Disabled		Installati
Implicit (5-5 / Total: 1)														
5	Implicit Deny	any	any	all	all	always	ALL		Deny		No Log			Installati

Interface	Default Mapping	Per-Device Mapping	Description	Created Time	Last Modified
Interface (14)					
any		0 out of 1			
sslvpn_tun_intf		0 out of 1			
sd-wan		0 out of 1			
port1		1 out of 1		2019-01-22 17:45:12	admin/2019-01-22 17:45:13
port10		1 out of 1		2019-01-22 17:45:12	admin/2019-01-22 17:45:13
port2		1 out of 1		2019-01-22 17:45:12	admin/2019-01-22 17:45:14
port3		1 out of 1		2019-01-22 17:45:12	admin/2019-01-22 17:45:14
port4		1 out of 1		2019-01-22 17:45:12	admin/2019-01-22 17:45:14
port5		1 out of 1		2019-01-22 17:45:13	admin/2019-01-22 17:45:14
port6		1 out of 1		2019-01-22 17:45:13	admin/2019-01-22 17:45:14
port7		1 out of 1		2019-01-22 17:45:13	admin/2019-01-22 17:45:14
port8		1 out of 1		2019-01-22 17:45:13	admin/2019-01-22 17:45:14
port9		1 out of 1		2019-01-22 17:45:13	admin/2019-01-22 17:45:14
ssl.root		1 out of 1		2019-01-22 17:45:13	admin/2019-01-22 17:45:14
Zone (0)					
Virtual Wire Pair (0)					

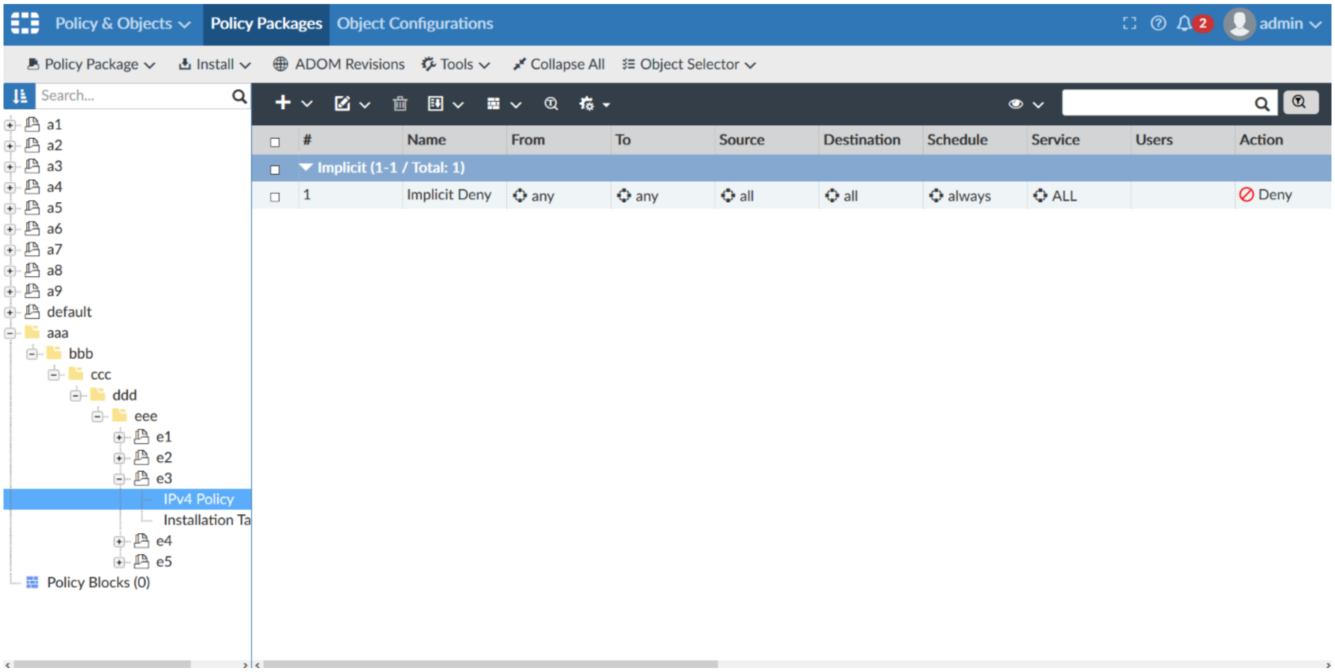
Admin Preference - Policy Package Cookie

In previous releases, when an administrator opened a Policy Package and logged out, the default view was shown on the *Policy Packages* page on logging in. The administrator had to navigate to the same Policy Package again upon logging in. When an administrator opened an Object and logged out, the default view was shown on the *Object Configurations* page upon logging in. The administrator had to navigate to the Object again upon logging in.

In this release, the Policy Package and Object opened by the administrator is remembered by FortiManager.

Last opened Policy Package

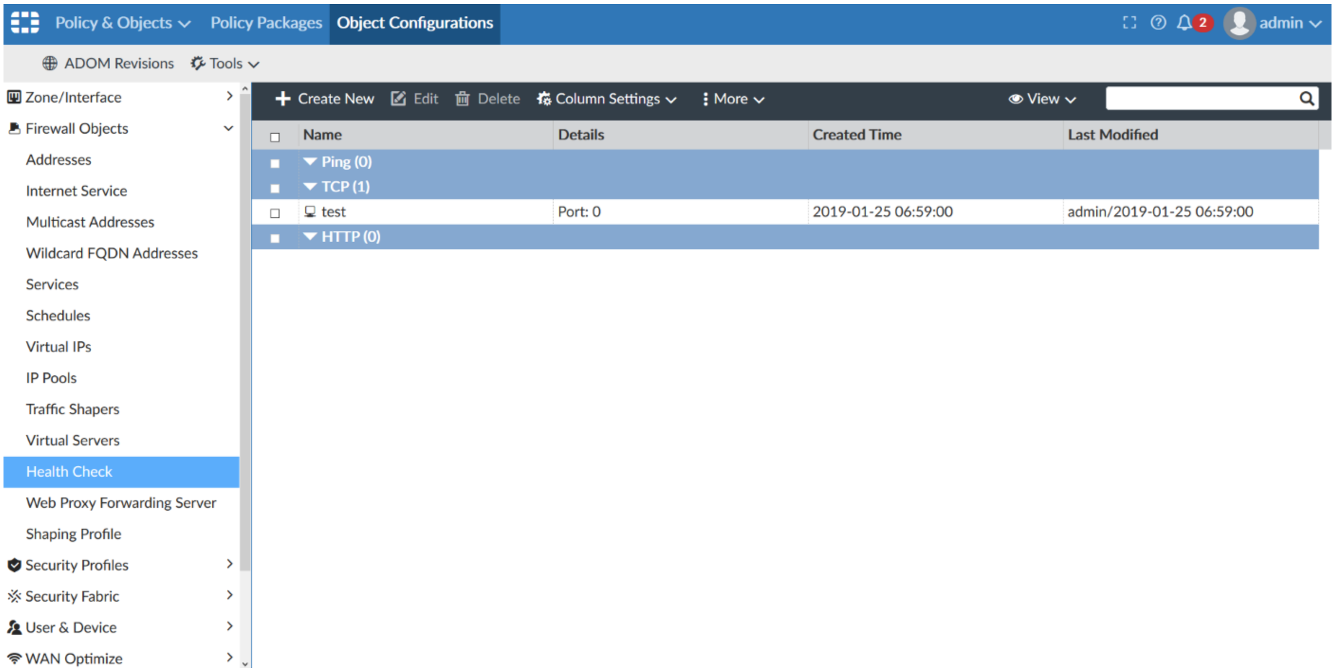
The last opened Policy Package is shown upon logging in.



#	Name	From	To	Source	Destination	Schedule	Service	Users	Action
Implicit (1-1 / Total: 1)									
1	Implicit Deny	any	any	all	all	always	ALL		Deny

Last opened Object

The last opened Object is shown upon logging in.



Name	Details	Created Time	Last Modified
Ping (0)			
TCP (1)			
test	Port: 0	2019-01-25 06:59:00	admin/2019-01-25 06:59:00
HTTP (0)			

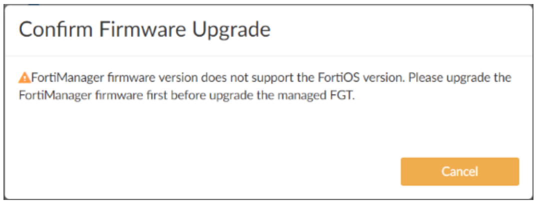
Upgrade Path Enforcement for Managed FortiGates

In earlier versions of FortiManager, when upgrading FortiGate devices to a higher version than FortiManager, there was no check and the upgrade process would be completed. Managing higher version FortiOS devices with lower version of FortiManager caused issues.

This release includes multiple usability improvements to guide the administrator towards a successful upgrade.

Warning when upgrading to a higher version of FortiOS than FortiManager

When trying to upgrade FortiOS devices to a version higher than FortiManager, the upgrade process is blocked and the following warning is shown to the administrator:



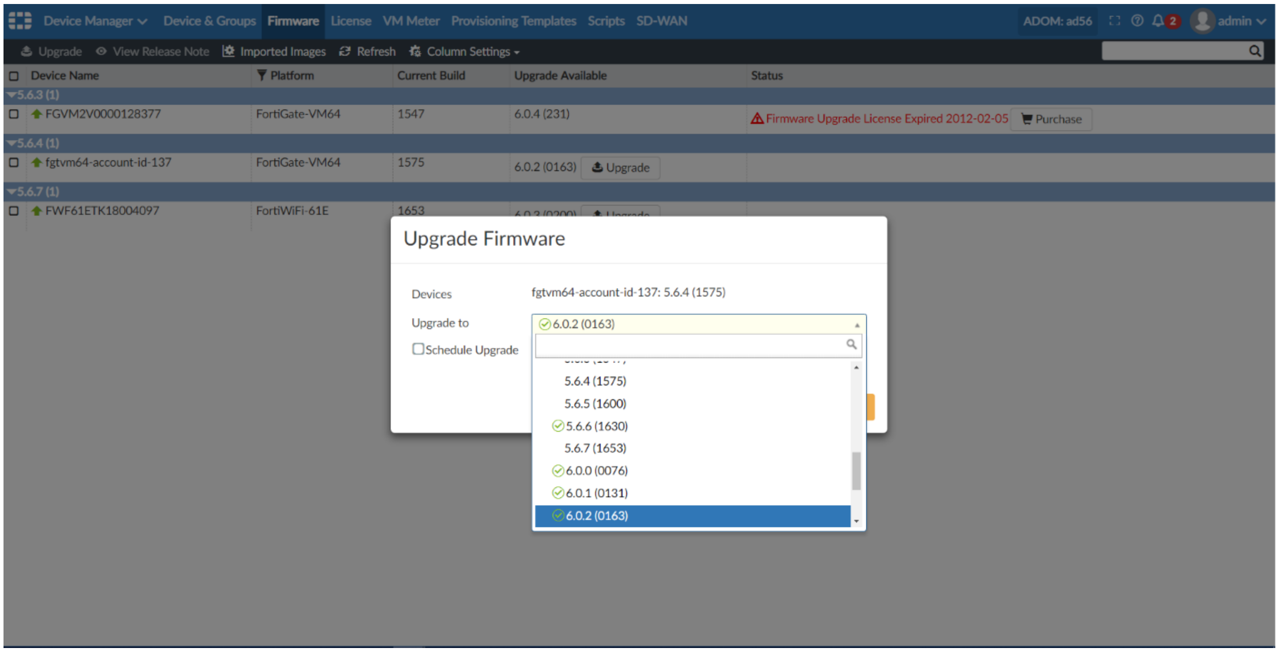
Confirm Firmware Upgrade

⚠FortiManager firmware version does not support the FortiOS version. Please upgrade the FortiManager firmware first before upgrade the managed FGT.

Upgrading Multiple FortiGate devices with the Recommended Upgrade Path

This version improves the upgrade process by providing useful warnings and options to take a recommended upgrade path:

- Go to *Device Manager* > *Firmware*, select multiple FortiGate devices and click *Upgrade*. The versions available in the upgrade path are shown by a green check mark.



Device Name	Platform	Current Build	Upgrade Available	Status
5.6.3 (1)				
FGVM2V0000128377	FortiGate-VM64	1547	6.0.4 (231)	⚠Firmware Upgrade License Expired 2012-02-05 Purchase
5.6.4 (1)				
fgtvm64-account-id-137	FortiGate-VM64	1575	6.0.2 (0163) Upgrade	
5.6.7 (1)				
FWF61ETK18004097	FortiWiFi-61E	1653	6.0.3 (0200) Upgrade	

Upgrade Firmware

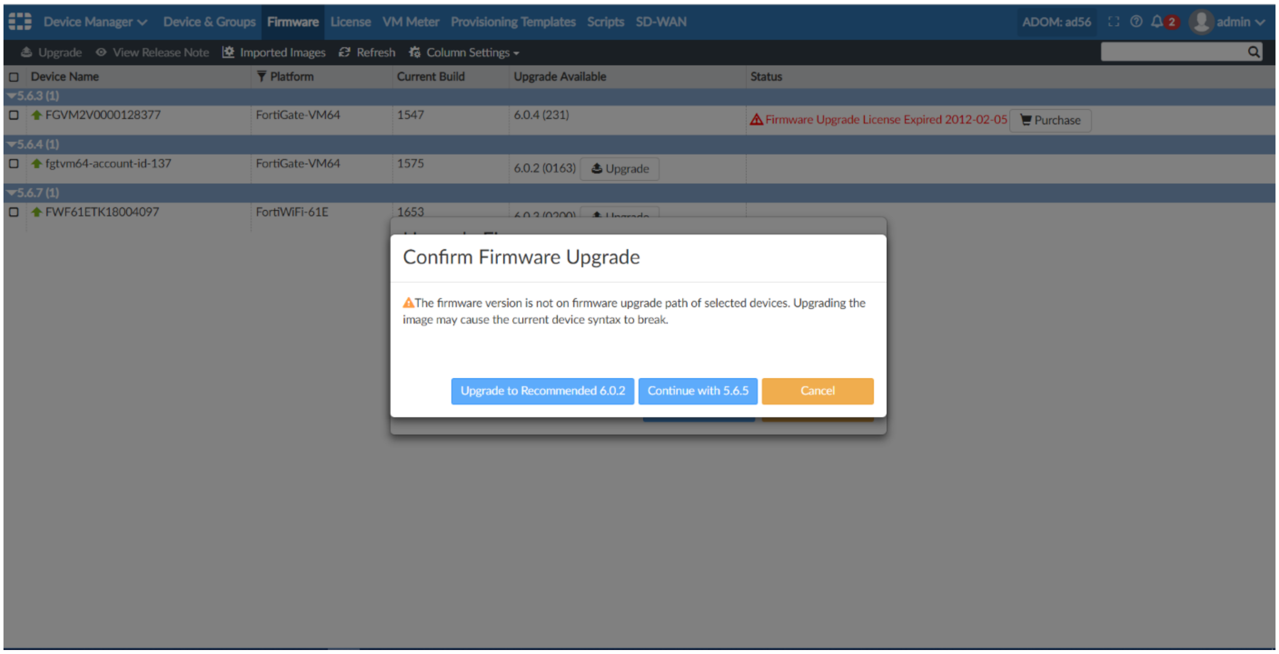
Devices fgtvm64-account-id-137: 5.6.4 (1575)

Upgrade to ✓6.0.2 (0163)

□Schedule Upgrade

5.6.4 (1575)
5.6.5 (1600)
✓5.6.6 (1630)
5.6.7 (1653)
✓6.0.0 (0076)
✓6.0.1 (0131)
✓6.0.2 (0163)

- When upgrading, the administrator is presented with an option to upgrade as per the recommended upgrade path or continue with the selected version.

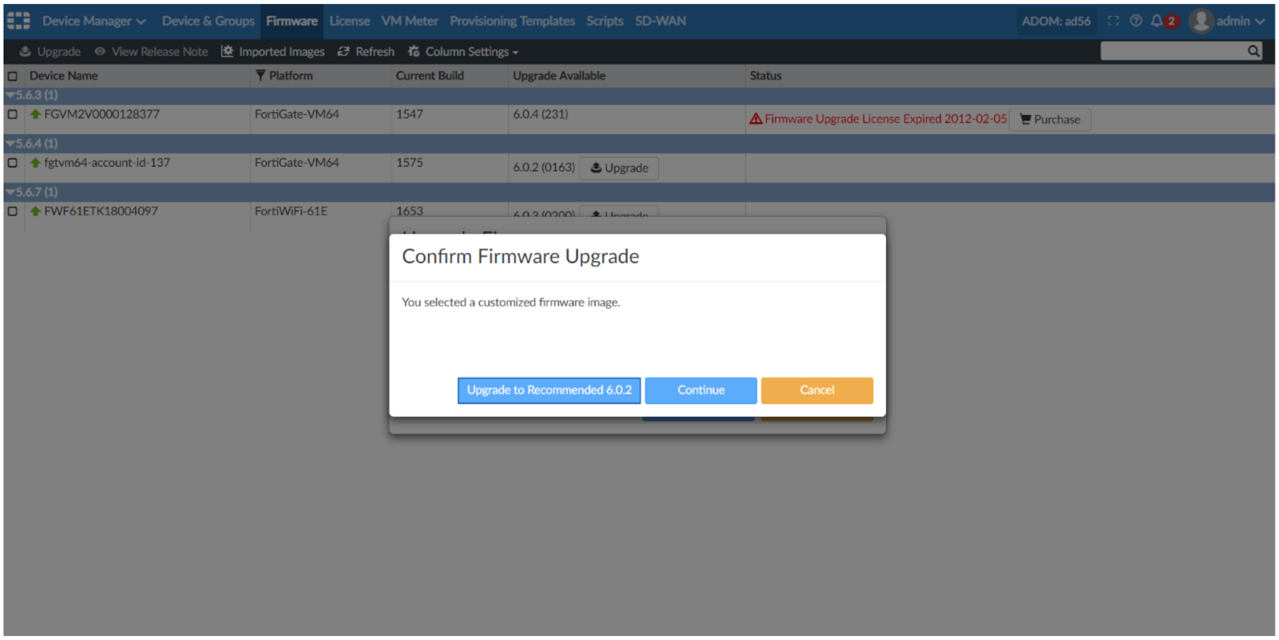


Device Name	Platform	Current Build	Upgrade Available	Status
5.6.3 (1)				
FGVM2V0000128377	FortiGate-VM64	1547	6.0.4 (231)	Firmware Upgrade License Expired 2012-02-05 Purchase
5.6.4 (1)				
fgtvm64-account-id-137	FortiGate-VM64	1575	6.0.2 (0163) Upgrade	
5.6.7 (1)				
FWF61ETK18004097	FortiWiFi-61E	1653	6.0.2 (0200) Upgrade	

Confirm Firmware Upgrade

The firmware version is not on firmware upgrade path of selected devices. Upgrading the image may cause the current device syntax to break.

- If the administrator selects a customized image, a warning is shown with an option to upgrade as per the recommended upgrade path or to continue with the selected customized image.



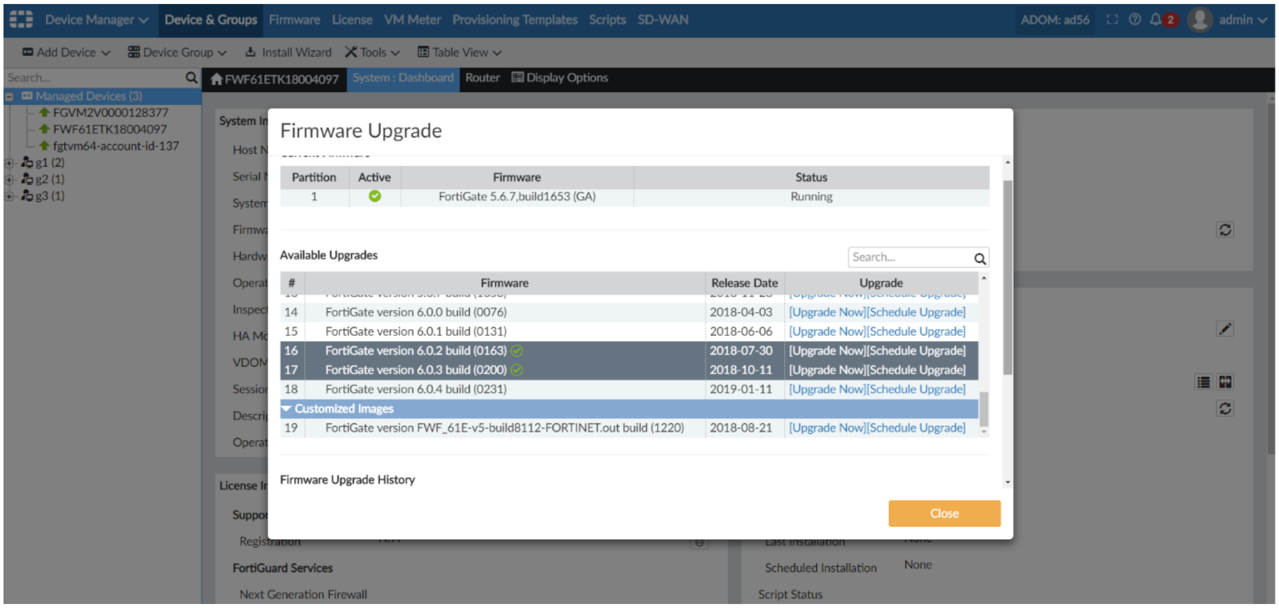
Device Name	Platform	Current Build	Upgrade Available	Status
5.6.3 (1)				
FGVM2V0000128377	FortiGate-VM64	1547	6.0.4 (231)	Firmware Upgrade License Expired 2012-02-05 Purchase
5.6.4 (1)				
fgtvm64-account-id-137	FortiGate-VM64	1575	6.0.2 (0163) Upgrade	
5.6.7 (1)				
FWF61ETK18004097	FortiWiFi-61E	1653	6.0.2 (0200) Upgrade	

Confirm Firmware Upgrade

You selected a customized firmware image.

Upgrading FortiGate Devices Individually with the Recommended Upgrade Path

- Go to *Device Manager* > *[Device Name]* > *System Information* widget. Click the *Firmware Version* update icon. The recommended upgrade is shown with a green check mark.



Firmware Upgrade

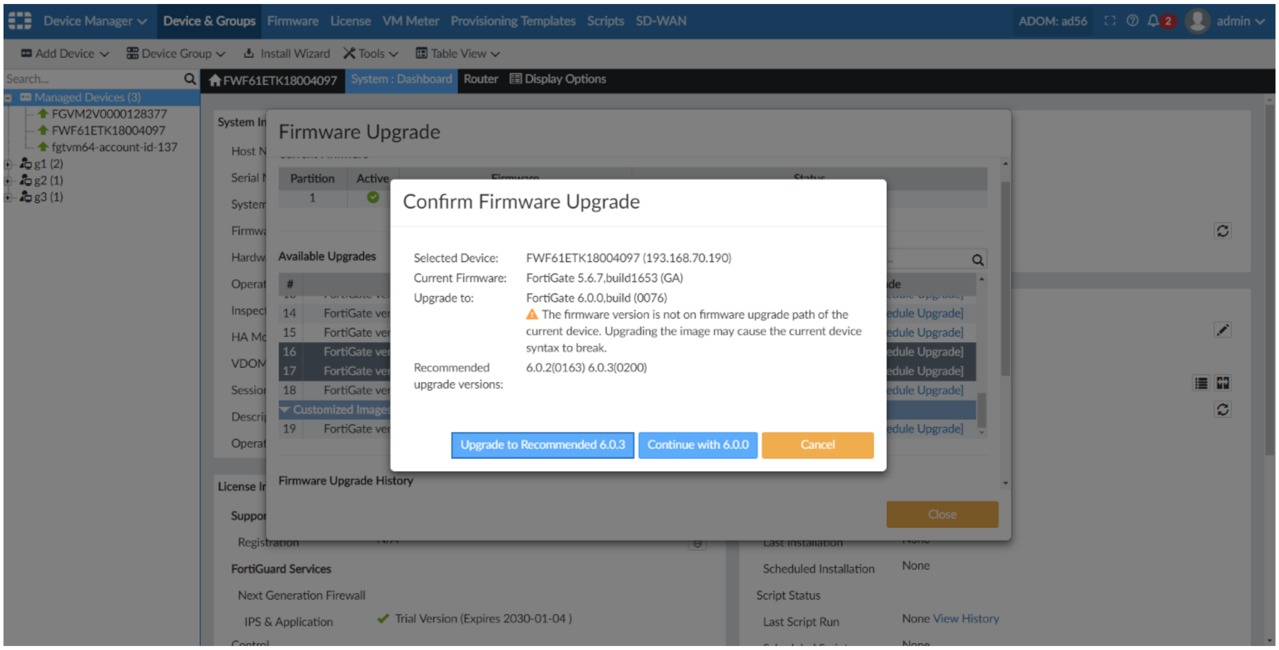
Partition	Active	Firmware	Status
1	✓	FortiGate 5.6.7,build1653 (GA)	Running

Available Upgrades

#	Firmware	Release Date	Upgrade
14	FortiGate version 6.0.0 build (0076)	2018-04-03	[Upgrade Now][Schedule Upgrade]
15	FortiGate version 6.0.1 build (0131)	2018-06-06	[Upgrade Now][Schedule Upgrade]
16	FortiGate version 6.0.2 build (0163) ✓	2018-07-30	[Upgrade Now][Schedule Upgrade]
17	FortiGate version 6.0.3 build (0200) ✓	2018-10-11	[Upgrade Now][Schedule Upgrade]
18	FortiGate version 6.0.4 build (0231)	2019-01-11	[Upgrade Now][Schedule Upgrade]
Customized Images			
19	FortiGate version FWF_61E-v5-build8112-FORTINET.out build (1220)	2018-08-21	[Upgrade Now][Schedule Upgrade]

Firmware Upgrade History

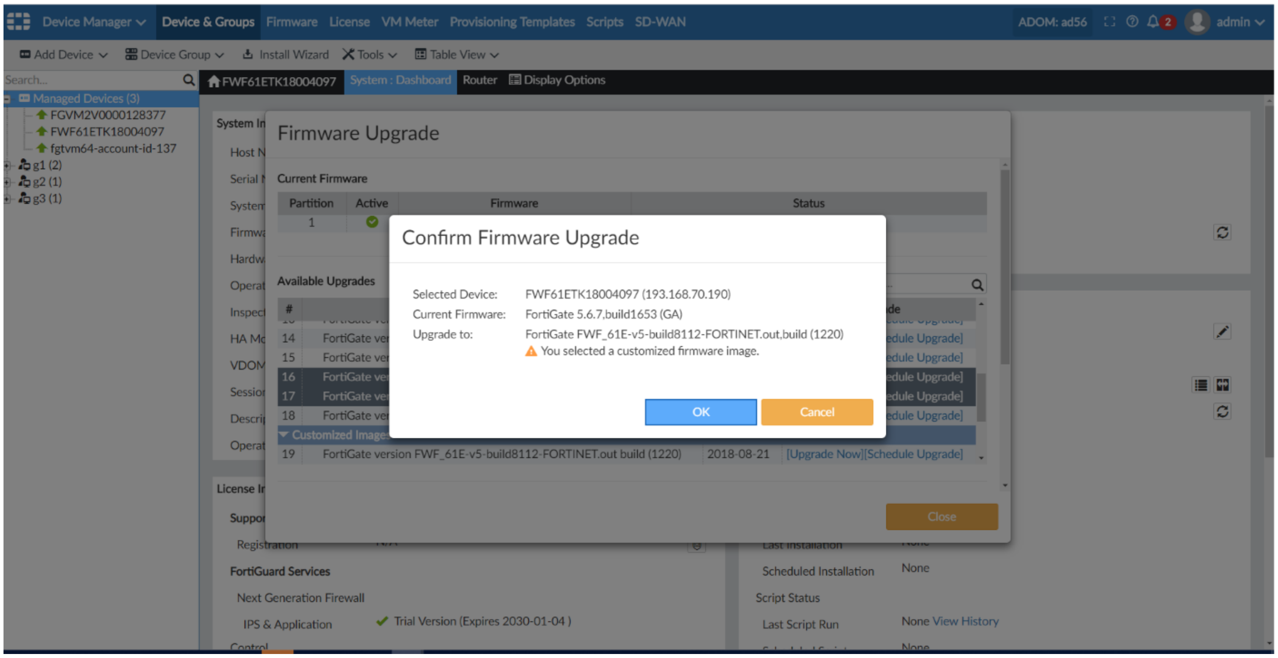
- Selecting a firmware that is not on the upgrade path shows a warning with an option to upgrade as per the recommended upgrade path.



Confirm Firmware Upgrade

Selected Device: FWF61ETK18004097 (193.168.70.190)
Current Firmware: FortiGate 5.6.7,build1653 (GA)
Upgrade to: FortiGate 6.0.0,build (0076)
⚠ The firmware version is not on firmware upgrade path of the current device. Upgrading the image may cause the current device syntax to break.
Recommended upgrade versions: 6.0.2(0163) 6.0.3(0200)

- Upgrading to a customized firmware image shows a warning asking the administrator to confirm the action.



Confirm Firmware Upgrade

Selected Device: FWF61ETK18004097 (193.168.70.190)
Current Firmware: FortiGate 5.6.7,build1653 (GA)
Upgrade to: FortiGate FWF_61E-v5-build8112-FORTINET.out,build (1220)
⚠ You selected a customized firmware image.

OK Cancel

#			
19	FortiGate version FWF_61E-v5-build8112-FORTINET.out build (1220)	2018-08-21	[Upgrade Now][Schedule Upgrade]

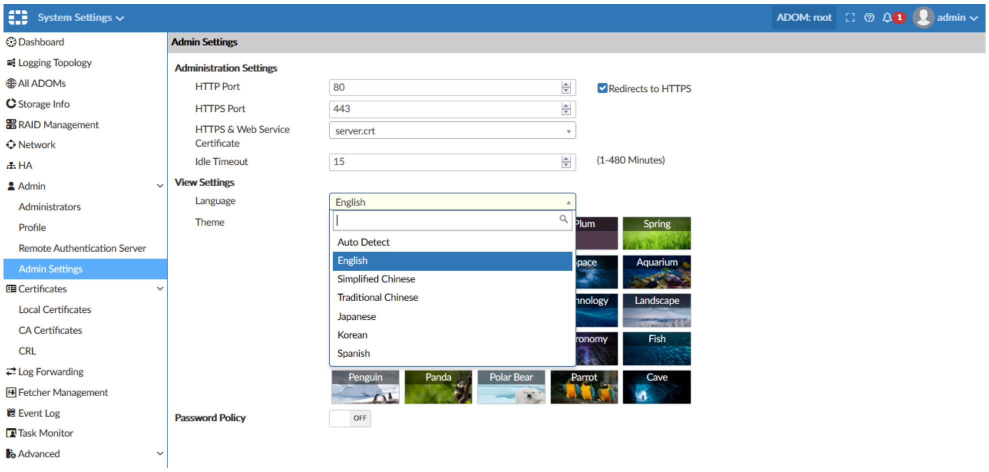
Spanish UI

The FortiAnalyzer and FortiManager user interface now supports Spanish in addition to the previously supported English, Simplified Chinese, Traditional Chinese, Korean, and Japanese.

Set user interface language preferences

To set the UI language to Spanish:

1. Go to *System Settings* > *Admin* > *Admin Settings*.
2. In *View Settings*, select *Spanish* in the *Language* drop-down.



Admin Settings

Administration Settings

HTTP Port: 80 ☑ Redirects to HTTPS
HTTPS Port: 443
HTTPS & Web Service Certificate: server.crt
Idle Timeout: 15 (1-480 Minutes)

View Settings

Language: English
Theme

Auto Detect
English
Simplified Chinese
Traditional Chinese
Japanese
Korean
Spanish

Password Policy: OFF

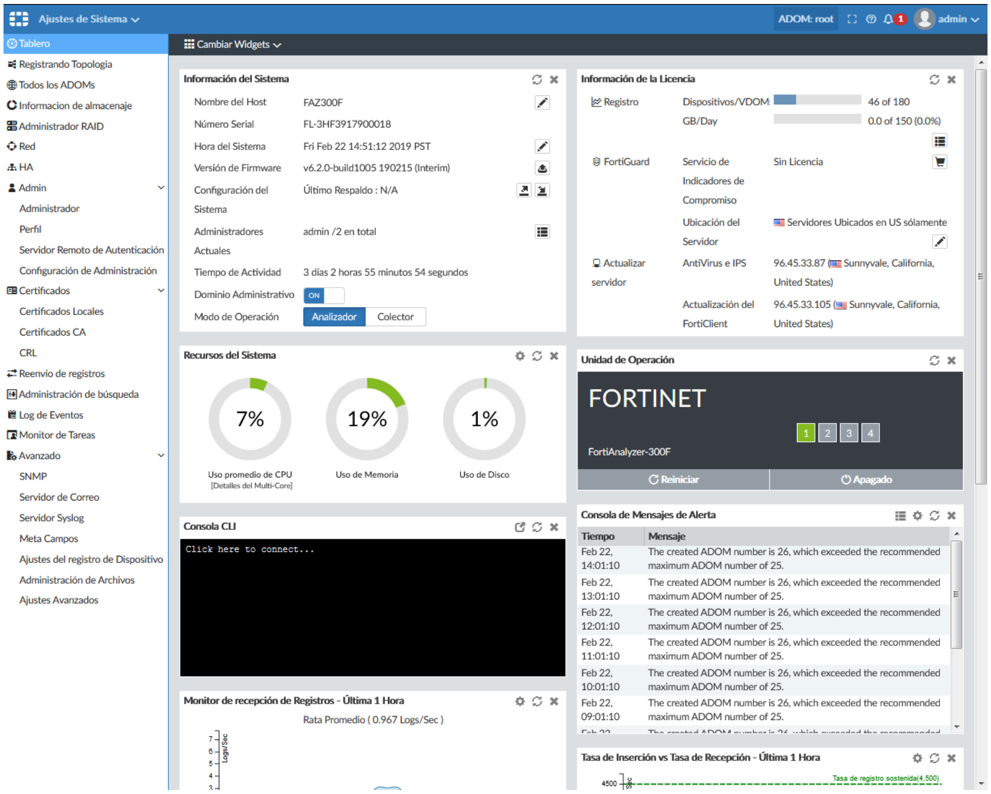
3. Select *Apply*.

To set the UI language to Spanish in the CLI:

```
FAZ300F # config system admin setting
(setting)# set webadmin_language ?
 auto_detect               Automatically detect language.
 english                   English.
 japanese                  Japanese.
 korean                    Korean.
 simplified_chinese        Simplified Chinese.
 spanish                   Spanish.
 traditional_chinese       Traditional Chinese.

(setting)# set webadmin_language spanish
```

Spanish user interface examples

- System Settings



Información del Sistema

Nombre del Host FAZ300F
Número Serial FL-3HF3917900018
Hora del Sistema Fri Feb 22 14:51:12 2019 PST
Versión de Firmware v6.2.0-build1005 190215 (Interim)
Configuración del Sistema Último Respaldo : N/A
Administradores Actuales admin /2 en total
Tiempo de Actividad 3 días 2 horas 55 minutos 54 segundos
Dominio Administrativo ON
Modo de Operación Analizador Colector

Información de la Licencia

Registro Dispositivos/VDOM: 46 of 180
GB/Day 0.0 of 150 (0.0%)
FortiGuard Servicio de Indicadores de Compromiso Sin Licencia
Ubicación del Servidor Servidores Ubicados en US sólamente
Actualizar servidor AntiVirus e IPS 96.45.33.87 (Sunnyvale, California, United States)
Actualización del FortiClient 96.45.33.105 (Sunnyvale, California, United States)

Recursos del Sistema

Unidad de Operación

Consola CLI

```
Click here to connect...
```

Consola de Mensajes de Alerta

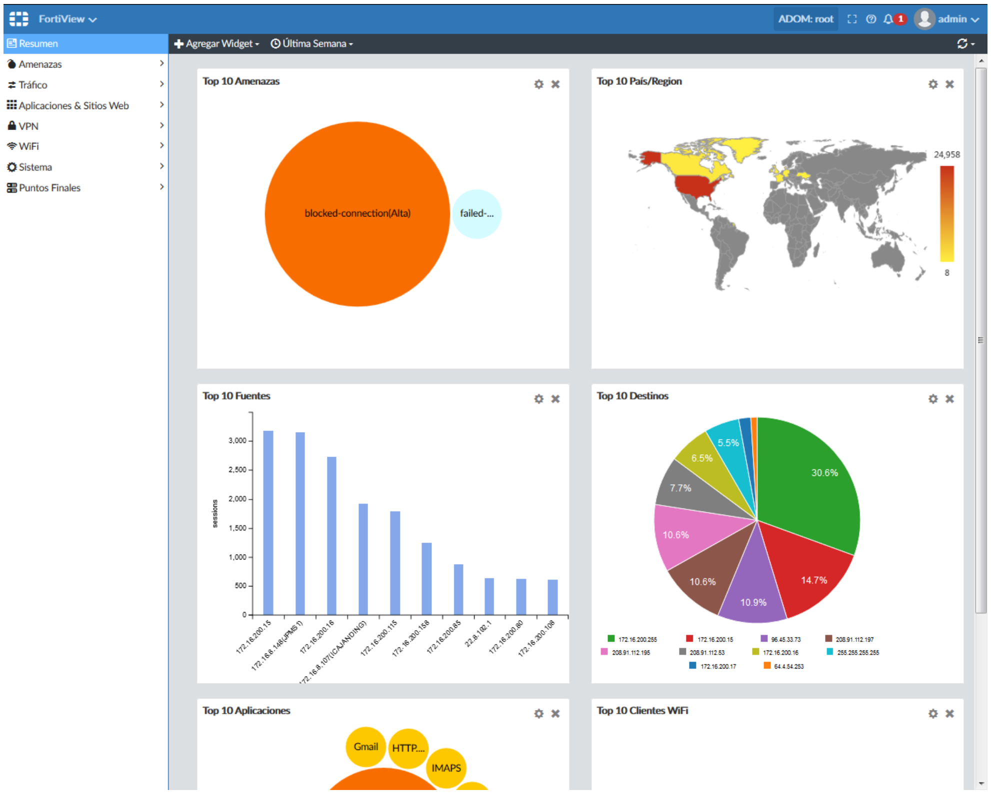
Tiempo	Mensaje
Feb 22, 14:01:10	The created ADOM number is 26, which exceeded the recommended maximum ADOM number of 25.
Feb 22, 13:01:10	The created ADOM number is 26, which exceeded the recommended maximum ADOM number of 25.
Feb 22, 12:01:10	The created ADOM number is 26, which exceeded the recommended maximum ADOM number of 25.
Feb 22, 11:01:10	The created ADOM number is 26, which exceeded the recommended maximum ADOM number of 25.
Feb 22, 10:01:10	The created ADOM number is 26, which exceeded the recommended maximum ADOM number of 25.
Feb 22, 09:01:10	The created ADOM number is 26, which exceeded the recommended maximum ADOM number of 25.

Monitor de recepción de Registros - Última 1 Hora

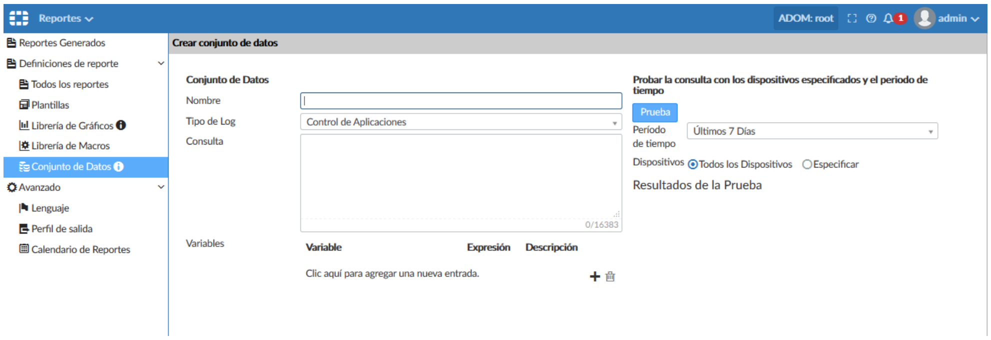
Rata Promedio (0.967 Logs/Sec)

Tasa de Inserción vs Tasa de Recepción - Última 1 Hora

- FortiView



- Reports



Crear conjunto de datos

Conjunto de Datos

Nombre

Tipo de Log: Control de Aplicaciones

Consulta

0/16383

Variables

Variable | Expresión | Descripción

Probar la consulta con los dispositivos especificados y el periodo de tiempo

Período de tiempo: Últimos 7 Días

Dispositivos ● Todos los Dispositivos ○ Especificar

Resultados de la Prueba

Other

This section lists other new features added to FortiManager.

List of new features:

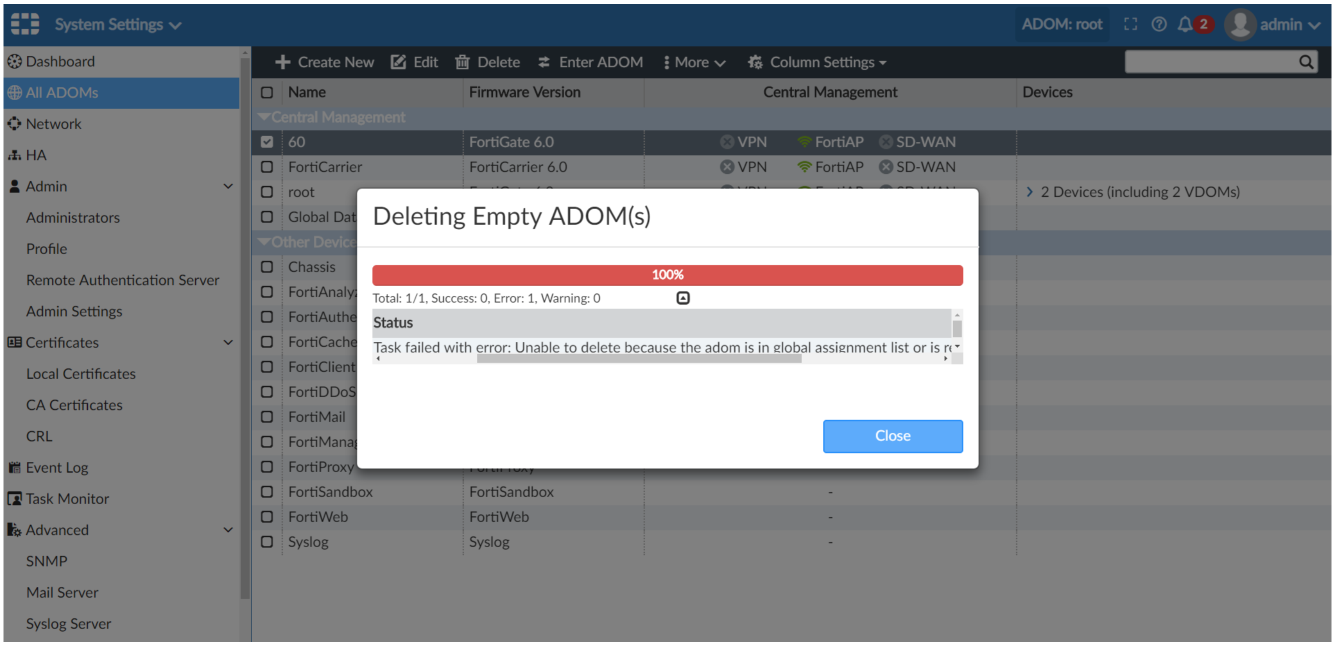
Delete Empty ADOMs

Empty ADOMs can now be deleted without un-assigning the Policy Packages assigned to the ADOM. Empty ADOMs can also be deleted without having to remove them from administrator's accounts. Once FortiGate devices are removed and the ADOM is empty, the ADOM can be deleted immediately.

See Deleting ADOMs.

Deleting ADOMs in earlier versions

Deleting an ADOM after removing FortiGate devices resulted in a message *Unable to delete because the adom is in global assignment list or is referenced by a defined admin account*. The ADOM may still be referenced by administrator accounts or global policy packages, and the references may be not easy to be find and remove. The following message was shown in earlier versions:



Name	Firmware Version	Central Management	Devices
Central Management			
☑ 60	FortiGate 6.0	VPN FortiAP SD-WAN	
□ FortiCarrier	FortiCarrier 6.0	VPN FortiAP SD-WAN	
□ root			2 Devices (including 2 VDOMs)
□ Global Dat			
Other Devic			
□ Chassis			
□ FortiAnaly			
□ FortiAuthe			
□ FortiCache			
□ FortiClient			
□ FortiDDoS			
□ FortiMail			
□ FortiManag			
□ FortiProxy			
□ FortiSandbox	FortiSandbox	-	
□ FortiWeb	FortiWeb	-	
□ Syslog	Syslog	-	

Deleting Empty ADOM(s)

100%

Total: 1/1, Success: 0, Error: 1, Warning: 0

Status

Task failed with error: Unable to delete because the adom is in global assignment list or is r

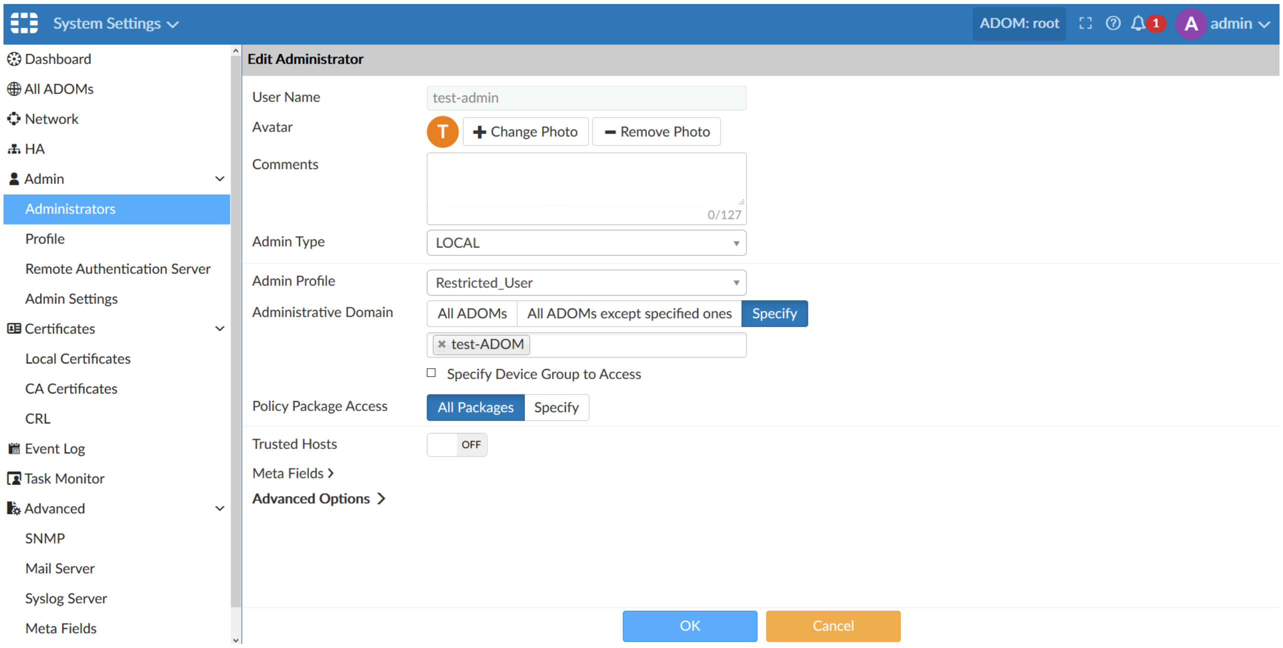
Close

Improvement in deleting ADOMs

The process of deleting ADOMs has been improved in this release. The administrator must remove all FortiGate devices from the ADOM. While deleting the ADOM, the references to administrator accounts and global policy packages will be shown and you can delete the ADOM without removing the listed references. The references to administrator accounts and global policy packages will be removed when deleting the ADOM.

To delete ADOMs:

1. Create a *test-ADOM* and reference it in the user *test-admin*.



Edit Administrator

User Name: test-admin

Avatar: T — Change Photo — Remove Photo

Comments: 0/127

Admin Type: LOCAL

Admin Profile: Restricted_User

Administrative Domain: All ADOMs | All ADOMs except specified ones | Specify (selected)

test-ADOM

□ Specify Device Group to Access

Policy Package Access: All Packages (selected) | Specify

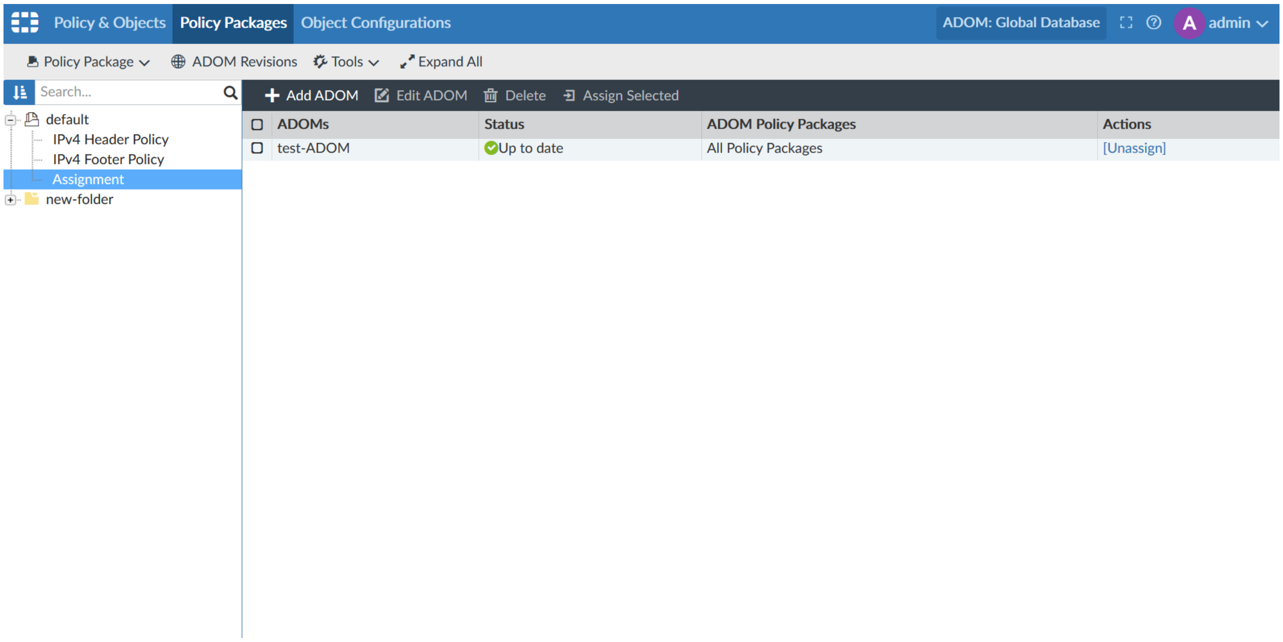
Trusted Hosts: OFF

Meta Fields >

Advanced Options >

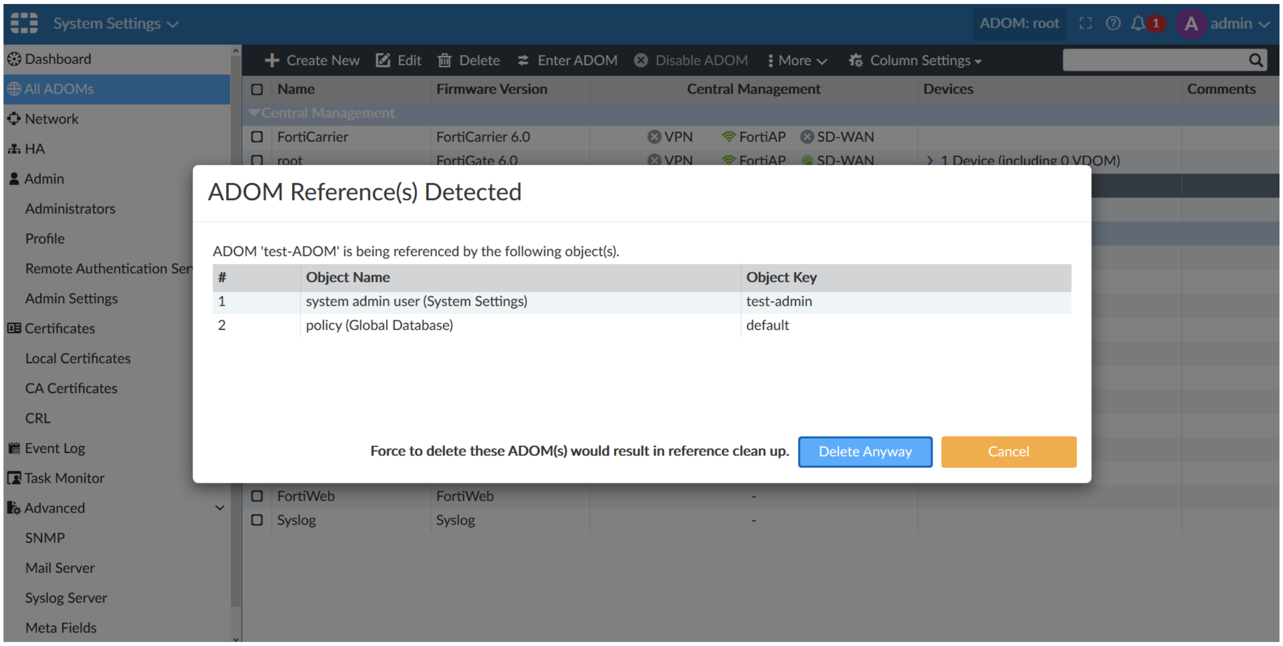
OK Cancel

2. Use the ADOM in Global Database assignment.



ADOMs	Status	ADOM Policy Packages	Actions
test-ADOM	Up to date	All Policy Packages	[Unassign]

3. Delete the ADOM. The following message is shown.



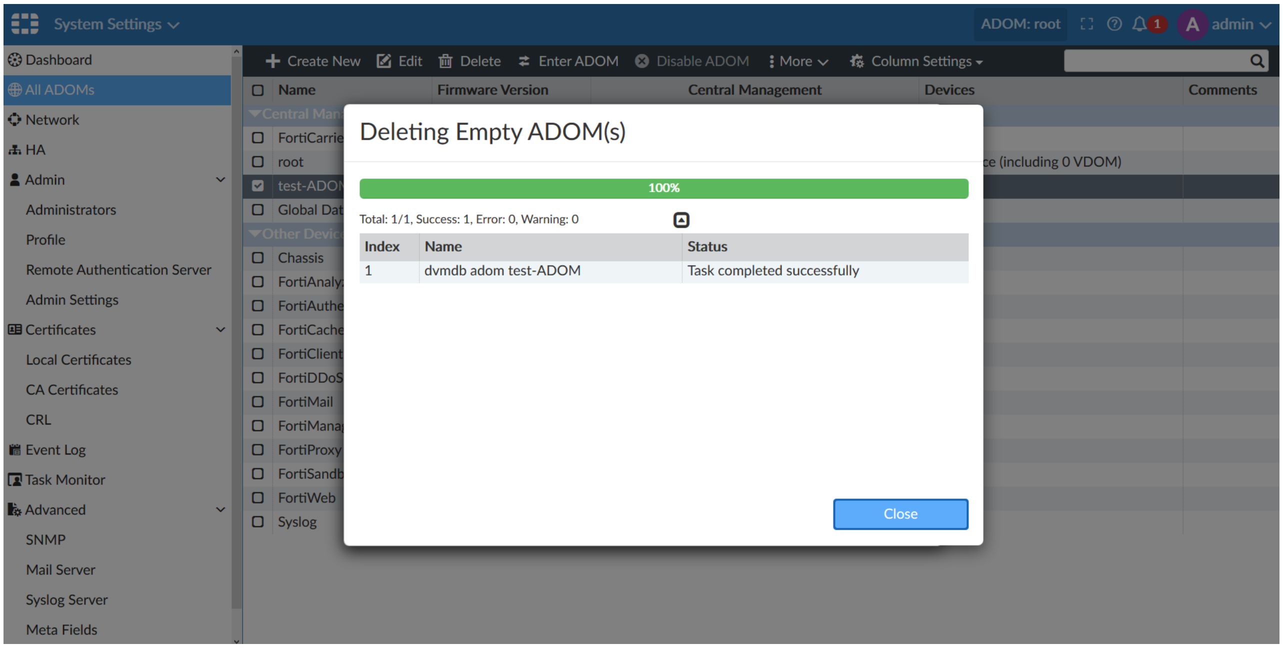
ADOM Reference(s) Detected

ADOM 'test-ADOM' is being referenced by the following object(s).

#	Object Name	Object Key
1	system admin user (System Settings)	test-admin
2	policy (Global Database)	default

Force to delete these ADOM(s) would result in reference clean up.

4. Click *Delete Anyway* to automatically remove the reference and delete the ADOM.



Deleting Empty ADOM(s)

100%

Total: 1/1, Success: 1, Error: 0, Warning: 0

Index	Name	Status
1	dvmdb adom test-ADOM	Task completed successfully

Telnet Removed

Telnet has been removed as a communication method in FortiManager for administrative access. Removing Telnet enhances the security since Telnet is not secure.

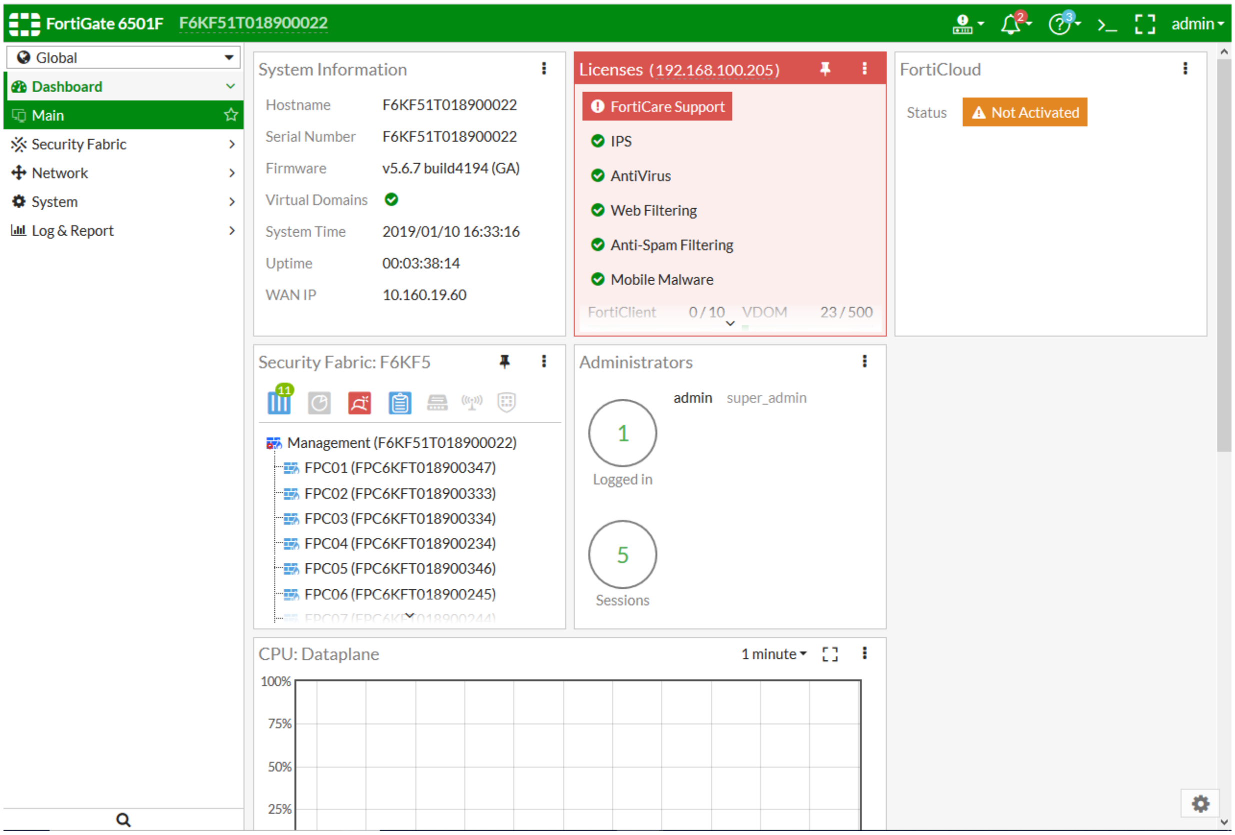
See Changing Administrative Access.

6000/7000-series UI Updates

FortiGate 6000 and 7000 series running FortiOS 5.6 and earlier do not support Security Fabric features with external devices. Earlier versions of FortiManager showed FortiGate 6000 and 7000 series running ForitOS 5.6 and earlier as Security Fabric devices which caused confusion. In FortiManager 6.2, these devices are correctly shown as non-Security Fabric FortiGate devices.

Displaying FortiGate 6000 and 7000 FortiManager

- FortiGate 6000 running FortiOS 5.6.7



FortiGate 6501F F6KF51T018900022 admin

Global

Dashboard

Main

Security Fabric

Network

System

Log & Report

System Information

Hostname	F6KF51T018900022
Serial Number	F6KF51T018900022
Firmware	v5.6.7 build4194 (GA)
Virtual Domains	✓
System Time	2019/01/10 16:33:16
Uptime	00:03:38:14
WAN IP	10.160.19.60

Licenses (192.168.100.205)

- FortiCare Support
- ✓ IPS
- ✓ AntiVirus
- ✓ Web Filtering
- ✓ Anti-Spam Filtering
- ✓ Mobile Malware

FortiClient 0 / 10 VDOM 23 / 500

FortiCloud

Status: Not Activated

Security Fabric: F6KF5

Management (F6KF51T018900022)
- FPC01 (FPC6KFT018900347)
- FPC02 (FPC6KFT018900333)
- FPC03 (FPC6KFT018900334)
- FPC04 (FPC6KFT018900234)
- FPC05 (FPC6KFT018900346)
- FPC06 (FPC6KFT018900245)
- FPC07 (FPC6KFT018900244)

Administrators

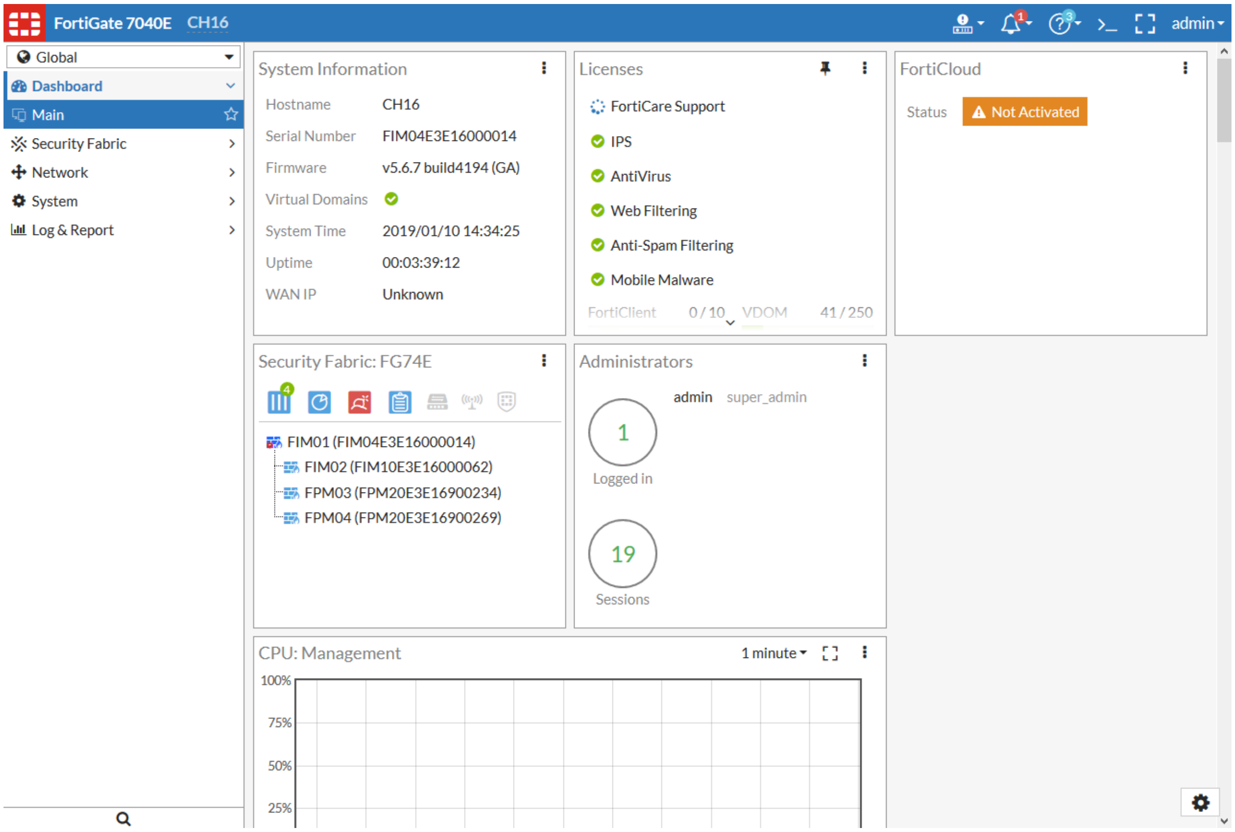
admin super_admin

1 Logged in

5 Sessions

CPU: Dataplane 1 minute

- FortiGate 7000 running FortiOS 5.6.7



System Information

Hostname CH16
Serial Number FIM04E3E16000014
Firmware v5.6.7 build4194 (GA)
Virtual Domains ✓
System Time 2019/01/10 14:34:25
Uptime 00:03:39:12
WAN IP Unknown

Licenses

FortiCare Support
✓ IPS
✓ AntiVirus
✓ Web Filtering
✓ Anti-Spam Filtering
✓ Mobile Malware
FortiClient 0 / 10 VDOM 41 / 250

FortiCloud

Status ⚠ Not Activated

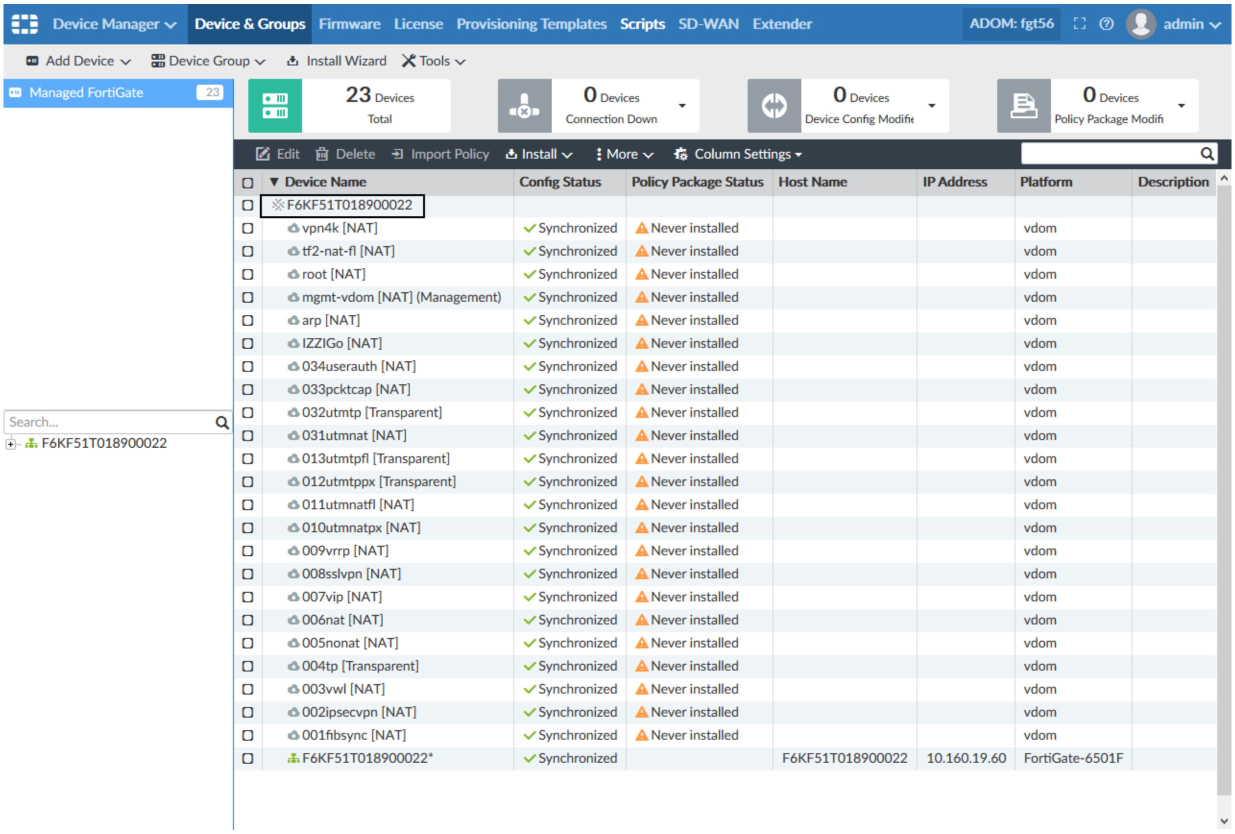
Security Fabric: FG74E

FIM01 (FIM04E3E16000014)
FIM02 (FIM10E3E16000062)
FPM03 (FPM20E3E16900234)
FPM04 (FPM20E3E16900269)

Administrators

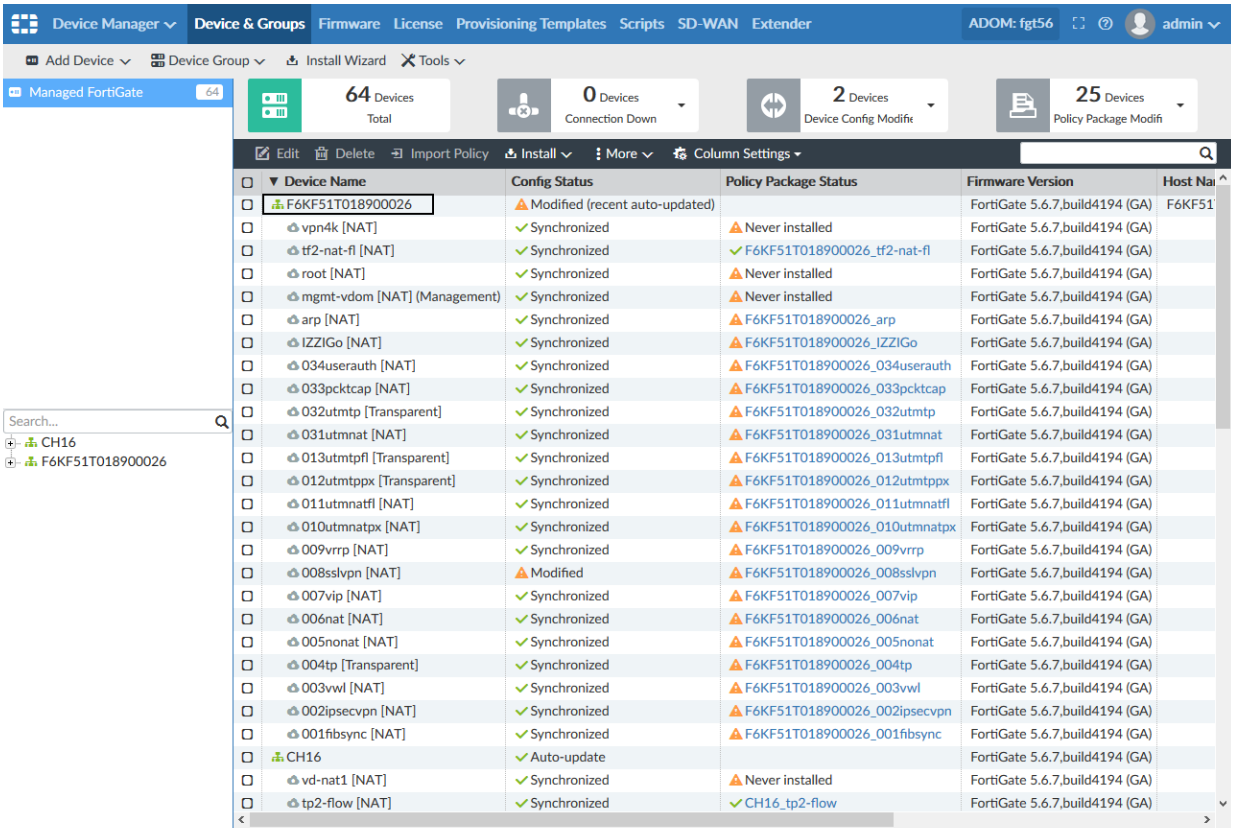
admin super_admin
1 Logged in
19 Sessions

- Earlier versions of FortiManager showed the Security Fabric tag in the *Device Name* column.



□	Device Name	Config Status	Policy Package Status	Host Name	IP Address	Platform	Description
□	F6KF51T018900022						
□	vpn4k [NAT]	✓ Synchronized	Never installed			vdom	
□	tf2-nat-fl [NAT]	✓ Synchronized	Never installed			vdom	
□	root [NAT]	✓ Synchronized	Never installed			vdom	
□	mgmt-vdom [NAT] (Management)	✓ Synchronized	Never installed			vdom	
□	arp [NAT]	✓ Synchronized	Never installed			vdom	
□	IZZIGo [NAT]	✓ Synchronized	Never installed			vdom	
□	034userauth [NAT]	✓ Synchronized	Never installed			vdom	
□	033pcktcap [NAT]	✓ Synchronized	Never installed			vdom	
□	032utmtp [Transparent]	✓ Synchronized	Never installed			vdom	
□	031utmnat [NAT]	✓ Synchronized	Never installed			vdom	
□	013utmtpfl [Transparent]	✓ Synchronized	Never installed			vdom	
□	012utmtppx [Transparent]	✓ Synchronized	Never installed			vdom	
□	011utmnatfl [NAT]	✓ Synchronized	Never installed			vdom	
□	010utmnatpx [NAT]	✓ Synchronized	Never installed			vdom	
□	009vrrp [NAT]	✓ Synchronized	Never installed			vdom	
□	008sslvpn [NAT]	✓ Synchronized	Never installed			vdom	
□	007vip [NAT]	✓ Synchronized	Never installed			vdom	
□	006nat [NAT]	✓ Synchronized	Never installed			vdom	
□	005nonat [NAT]	✓ Synchronized	Never installed			vdom	
□	004tp [Transparent]	✓ Synchronized	Never installed			vdom	
□	003vwl [NAT]	✓ Synchronized	Never installed			vdom	
□	002ipsecvpn [NAT]	✓ Synchronized	Never installed			vdom	
□	001fibsync [NAT]	✓ Synchronized	Never installed			vdom	
□	F6KF51T018900022*	✓ Synchronized		F6KF51T018900022	10.160.19.60	FortiGate-6501F	

- FortiManager 6.2 correctly shows FortiGate 6000 and FortiGate 7000 running FortiOS 5.6 or earlier as regular FortiGate devices.



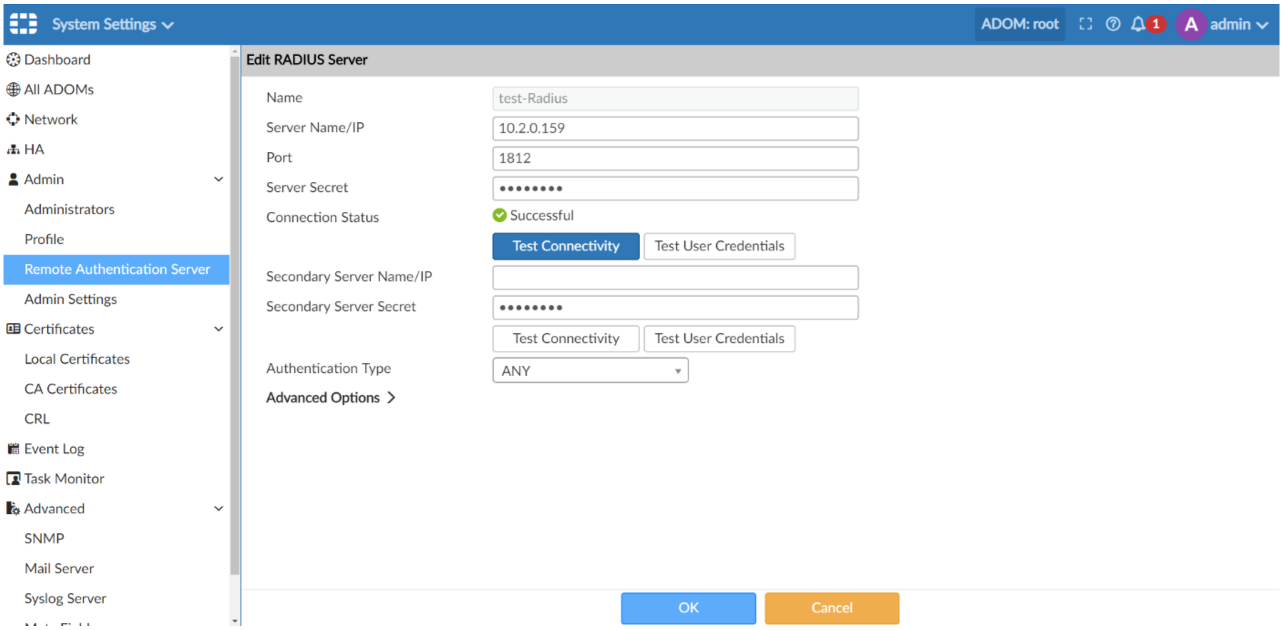
□	Device Name	Config Status	Policy Package Status	Firmware Version	Host Na
□	F6KF51T018900026	⚠ Modified (recent auto-updated)		FortiGate 5.6.7,build4194 (GA)	F6KF51
□	vpn4k [NAT]	✓ Synchronized	⚠ Never installed	FortiGate 5.6.7,build4194 (GA)	
□	tf2-nat-fl [NAT]	✓ Synchronized	✓ F6KF51T018900026_tf2-nat-fl	FortiGate 5.6.7,build4194 (GA)	
□	root [NAT]	✓ Synchronized	⚠ Never installed	FortiGate 5.6.7,build4194 (GA)	
□	mgmt-vdom [NAT] (Management)	✓ Synchronized	⚠ Never installed	FortiGate 5.6.7,build4194 (GA)	
□	arp [NAT]	✓ Synchronized	⚠ F6KF51T018900026_arp	FortiGate 5.6.7,build4194 (GA)	
□	IZZIGo [NAT]	✓ Synchronized	⚠ F6KF51T018900026_IZZIGo	FortiGate 5.6.7,build4194 (GA)	
□	034userauth [NAT]	✓ Synchronized	⚠ F6KF51T018900026_034userauth	FortiGate 5.6.7,build4194 (GA)	
□	033pcktcap [NAT]	✓ Synchronized	⚠ F6KF51T018900026_033pcktcap	FortiGate 5.6.7,build4194 (GA)	
□	032utmtp [Transparent]	✓ Synchronized	⚠ F6KF51T018900026_032utmtp	FortiGate 5.6.7,build4194 (GA)	
□	031utmnat [NAT]	✓ Synchronized	⚠ F6KF51T018900026_031utmnat	FortiGate 5.6.7,build4194 (GA)	
□	013utmtpfl [Transparent]	✓ Synchronized	⚠ F6KF51T018900026_013utmtpfl	FortiGate 5.6.7,build4194 (GA)	
□	012utmtppx [Transparent]	✓ Synchronized	⚠ F6KF51T018900026_012utmtppx	FortiGate 5.6.7,build4194 (GA)	
□	011utmnatfl [NAT]	✓ Synchronized	⚠ F6KF51T018900026_011utmnatfl	FortiGate 5.6.7,build4194 (GA)	
□	010utmnatpx [NAT]	✓ Synchronized	⚠ F6KF51T018900026_010utmnatpx	FortiGate 5.6.7,build4194 (GA)	
□	009vrrp [NAT]	✓ Synchronized	⚠ F6KF51T018900026_009vrrp	FortiGate 5.6.7,build4194 (GA)	
□	008sslvpn [NAT]	⚠ Modified	⚠ F6KF51T018900026_008sslvpn	FortiGate 5.6.7,build4194 (GA)	
□	007vip [NAT]	✓ Synchronized	⚠ F6KF51T018900026_007vip	FortiGate 5.6.7,build4194 (GA)	
□	006nat [NAT]	✓ Synchronized	⚠ F6KF51T018900026_006nat	FortiGate 5.6.7,build4194 (GA)	
□	005nonat [NAT]	✓ Synchronized	⚠ F6KF51T018900026_005nonat	FortiGate 5.6.7,build4194 (GA)	
□	004tp [Transparent]	✓ Synchronized	⚠ F6KF51T018900026_004tp	FortiGate 5.6.7,build4194 (GA)	
□	003vwl [NAT]	✓ Synchronized	⚠ F6KF51T018900026_003vwl	FortiGate 5.6.7,build4194 (GA)	
□	002ipsecvpn [NAT]	✓ Synchronized	⚠ F6KF51T018900026_002ipsecvpn	FortiGate 5.6.7,build4194 (GA)	
□	001fibsync [NAT]	✓ Synchronized	⚠ F6KF51T018900026_001fibsync	FortiGate 5.6.7,build4194 (GA)	
□	CH16	✓ Auto-update		FortiGate 5.6.7,build4194 (GA)	
□	vd-nat1 [NAT]	✓ Synchronized	⚠ Never installed	FortiGate 5.6.7,build4194 (GA)	
□	tp2-flow [NAT]	✓ Synchronized	✓ CH16_tp2-flow	FortiGate 5.6.7,build4194 (GA)	

Improve RADIUS Setup

The FortiManager RADIUS setup now includes the Test Connectivity and Test User Credentials options. The *Administrators* > *Advanced Options* now include Admin Profile Override and other minor usability improvements.

List of Improvements

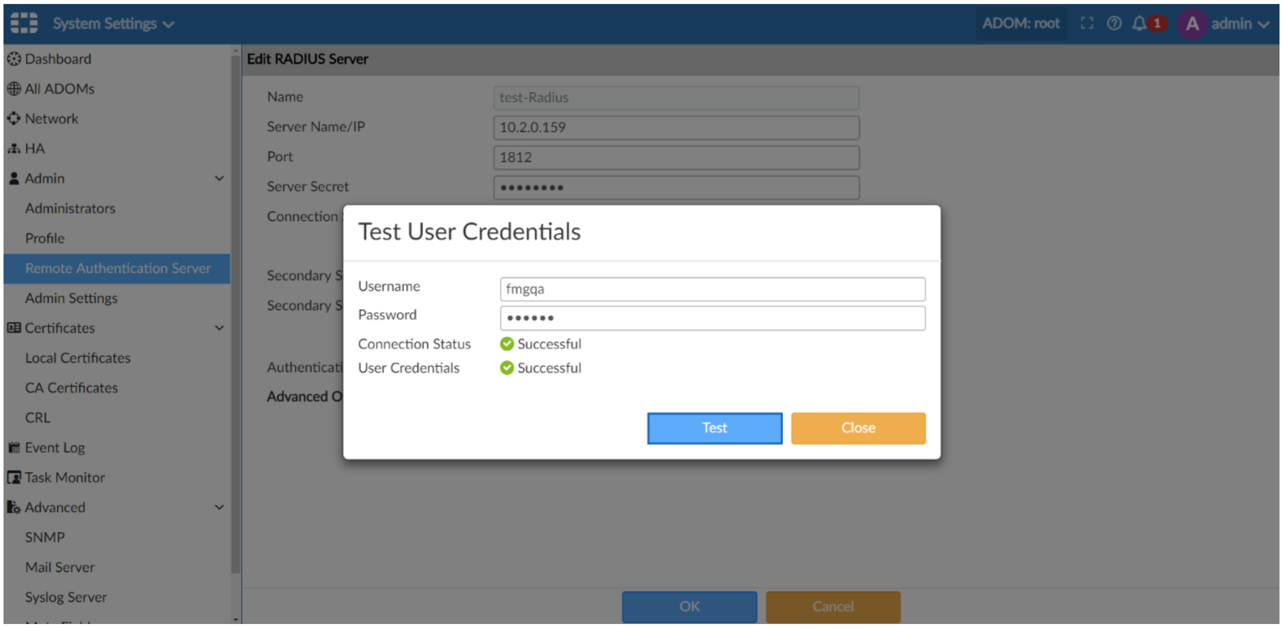
- RADIUS Configuration now includes *Test Connectivity* and *Test User Credentials* buttons.



Edit RADIUS Server

Name	test-Radius
Server Name/IP	10.2.0.159
Port	1812
Server Secret	••••••••
Connection Status	Successful
Secondary Server Name/IP	
Secondary Server Secret	••••••••
Authentication Type	ANY

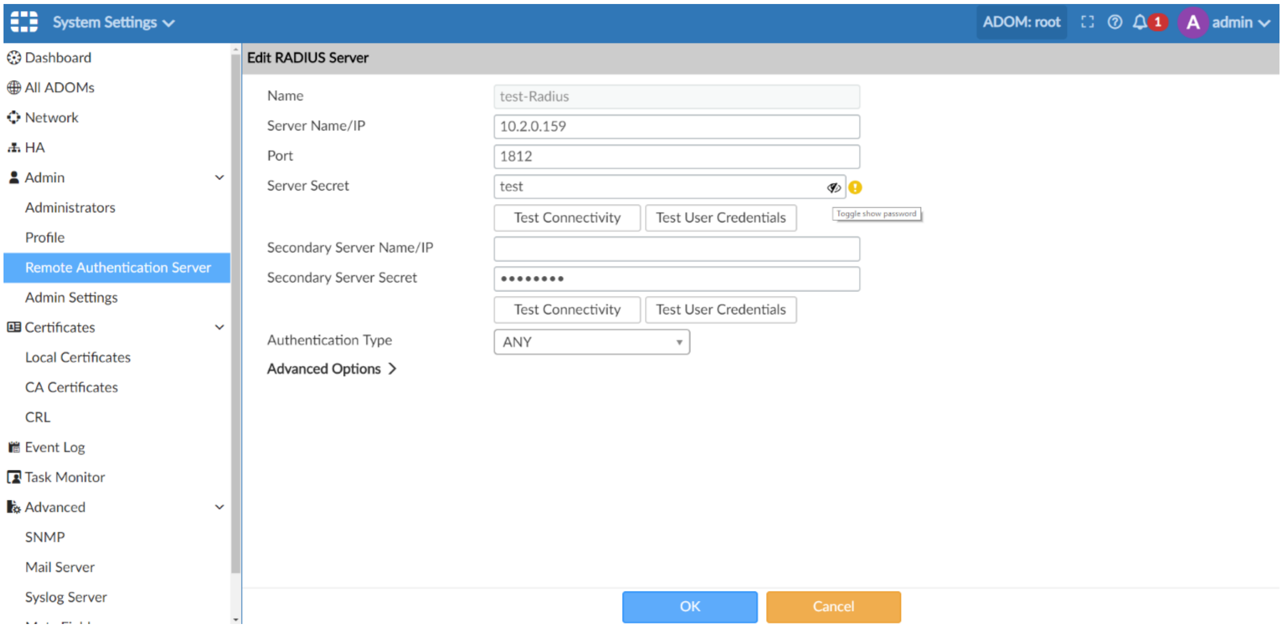
- *Test User Credentials* shows success or failure.



Test User Credentials

Username	fmgqa
Password	••••••
Connection Status	Successful
User Credentials	Successful

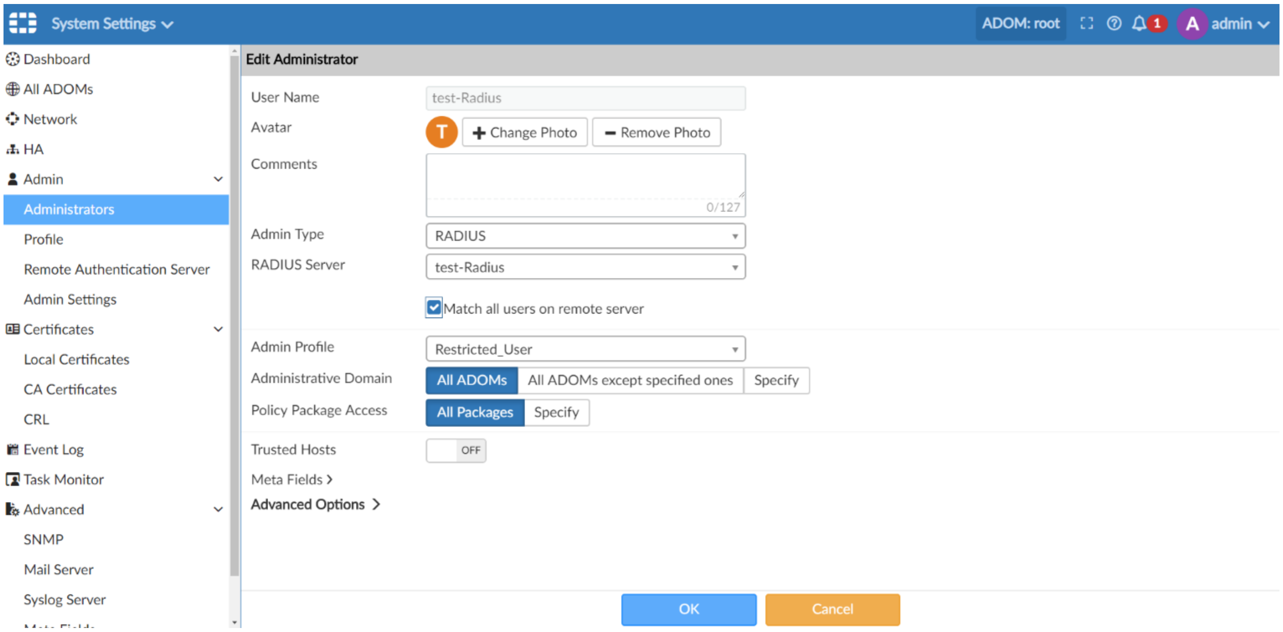
- Eye icon added to show or hide the Server Secret.



Edit RADIUS Server

Name	test-Radius
Server Name/IP	10.2.0.159
Port	1812
Server Secret	test
Secondary Server Name/IP	
Secondary Server Secret	••••••••
Authentication Type	ANY

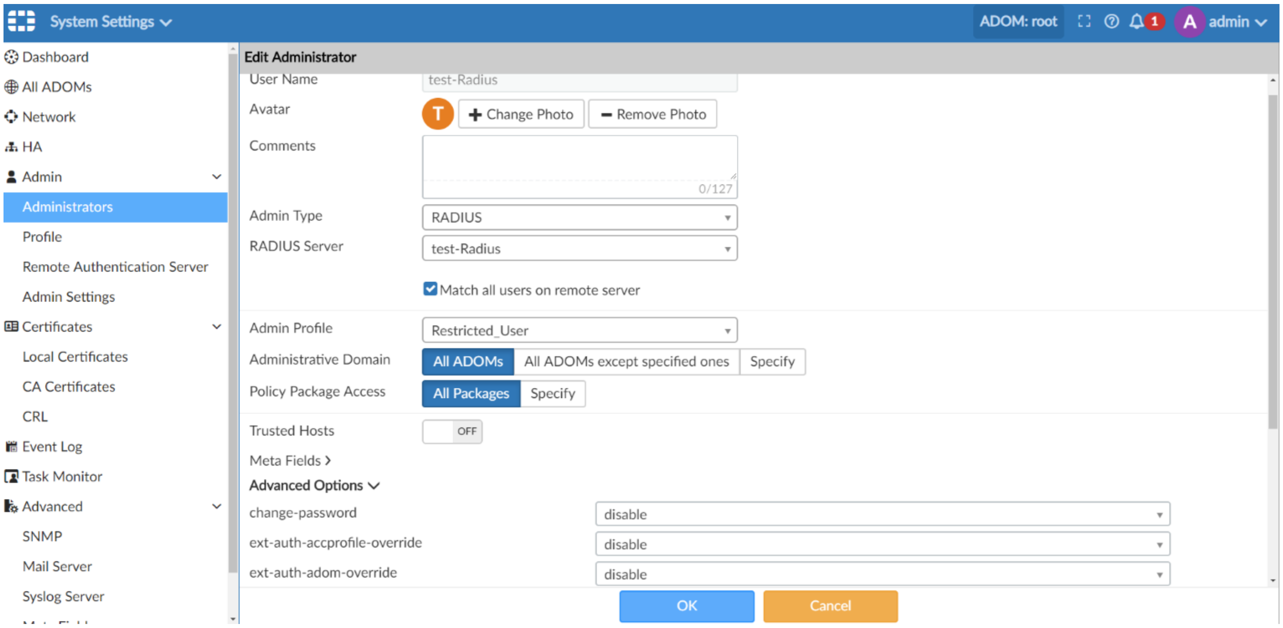
- Wildcard option changed to *Match all users on remote server* in GUI.



Edit Administrator

User Name	test-Radius
Avatar	T
Comments	
Admin Type	RADIUS
RADIUS Server	test-Radius
	☑ Match all users on remote server
Admin Profile	Restricted_User
Administrative Domain	All ADOMs
Policy Package Access	All Packages
Trusted Hosts	OFF

- Go to *System Settings* > *Administrators* > *Advanced Options* to add admin profile override configuration.



Edit Administrator

User Name: test-Radius

Avatar: T

Comments: 0/127

Admin Type: RADIUS

RADIUS Server: test-Radius

☑ Match all users on remote server

Admin Profile: Restricted_User

Administrative Domain: All ADOMs | All ADOMs except specified ones | Specify

Policy Package Access: All Packages | Specify

Trusted Hosts: OFF

change-password: disable

ext-auth-accprofile-override: disable

ext-auth-adom-override: disable

- Wildcard and override feature can also be configured via CLI.

```
config system admin user
   edit "Radius"
      set adom "all_adoms"
      set policy-package "all_policy_packages"
      set user_type radius
      set radius_server "test-Radius"
      set wildcard enable
      set ext-auth-accprofile-override enable
      set ext-auth-adom-override enable
   next
end
```

Support for FortiOS VM Directly Connecting to FortiGuard

In previous releases, FortiOS-VM (FortiMeter) instances needed to get services from FortiManager that facilitated updates by tracking service entitlements based on serial numbers starting with FOSVM1. However, if the FortiOS-VM connected directly to Fortinet Distribution Network (FDN), updates were not available since FDN was not aware of serial numbers with prefix FOSVM1.

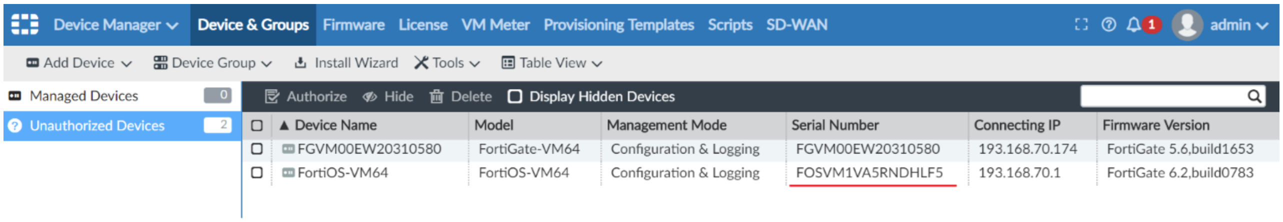
In the current release, the serial number prefix FOSVM2 was added to FortiOS-VM. When the FortiOS-VM connected directly to FDN, it is now able to receive the updates.

The same serial number will have two different prefixes depending on the situation:

- FortiOS-VM sends the serial numbers with prefix FOSVM2 to FortiManager or FortiGuard for updates and rating service. FOSVM2 is not visible on the FortiManager GUI.
- FortiOS-VM sends the serial numbers with prefix FOSVM1 to FortiManager for management. FOSVM1 is shown on the FortiManager GUI.

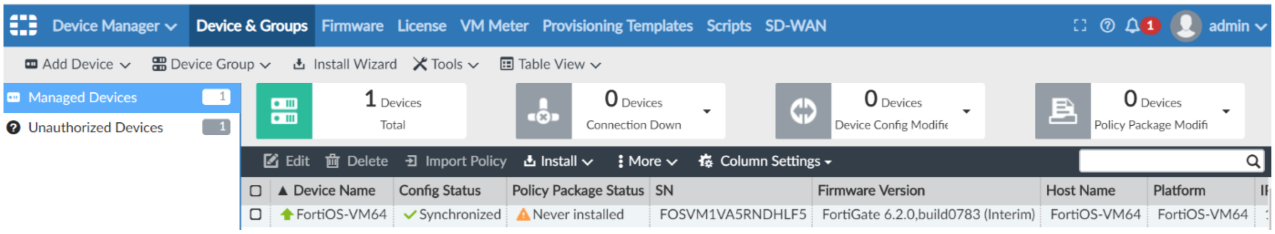
FortiGate Serial Numbers shown in FortiManager

- FortiOS-VM in FortiManager *Unauthorized Devices* list with the serial number prefix FOSVM1



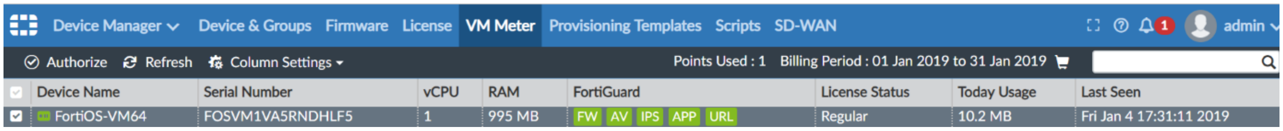
☐	▲ Device Name	Model	Management Mode	Serial Number	Connecting IP	Firmware Version
☐	FGVM00EW20310580	FortiGate-VM64	Configuration & Logging	FGVM00EW20310580	193.168.70.174	FortiGate 5.6,build1653
☐	FortiOS-VM64	FortiOS-VM64	Configuration & Logging	FOSVM1VA5RNDHLF5	193.168.70.1	FortiGate 6.2,build0783

- Authorized FortiOS-VM in FortiManager



☐	▲ Device Name	Config Status	Policy Package Status	SN	Firmware Version	Host Name	Platform
☐	FortiOS-VM64	✓ Synchronized	⚠ Never installed	FOSVM1VA5RNDHLF5	FortiGate 6.2.0,build0783 (Interim)	FortiOS-VM64	FortiOS-VM64

- Authorize FortiGuard service to FortiOS-VM. FortiManager checks service license with serial number prefix FOSVM1 while providing service to FOSVM2.



Points Used : 1 Billing Period : 01 Jan 2019 to 31 Jan 2019

☐	Device Name	Serial Number	vCPU	RAM	FortiGuard	License Status	Today Usage	Last Seen
☑	FortiOS-VM64	FOSVM1VA5RNDHLF5	1	995 MB	FW AV IPS APP URL	Regular	10.2 MB	Fri Jan 4 17:31:11 2019

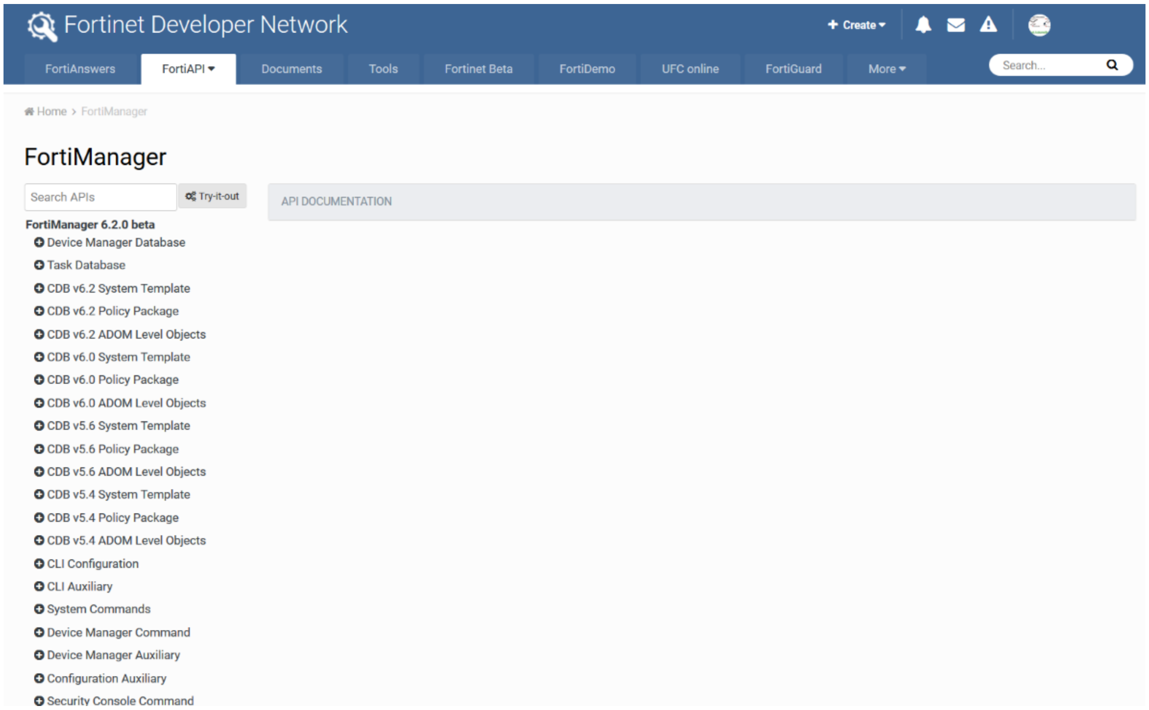
Swagger support for FNDN API Tool

A new Swagger API viewer is added to FNDN, with *try it out* feature enabling dev-ops developers to quickly review, test and monitor changes to REST API across versions.

To use the FNDN API tool:

1. Log on to *fndn.fortinet.net*.
2. Click the *FortiAPI* tab.

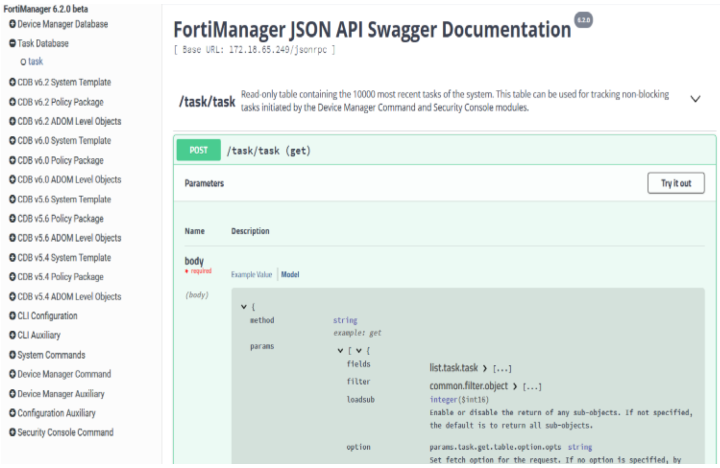
3. Click *FortiManager*.



FortiManager

FortiManager 6.2.0 beta
- Device Manager Database
- Task Database
- CDB v6.2 System Template
- CDB v6.2 Policy Package
- CDB v6.2 ADOM Level Objects
- CDB v6.0 System Template
- CDB v6.0 Policy Package
- CDB v6.0 ADOM Level Objects
- CDB v5.6 System Template
- CDB v5.6 Policy Package
- CDB v5.6 ADOM Level Objects
- CDB v5.4 System Template
- CDB v5.4 Policy Package
- CDB v5.4 ADOM Level Objects
- CLI Configuration
- CLI Auxiliary
- System Commands
- Device Manager Command
- Device Manager Auxiliary
- Configuration Auxiliary
- Security Console Command

4. To get the detailed JSON API information, click any URL. For example, click the *task* URL.



FortiManager JSON API Swagger Documentation

[Base URL: 172.18.65.249/jsonrpc]

/task/task Read-only table containing the 10000 most recent tasks of the system. This table can be used for tracking non-blocking tasks initiated by the Device Manager Command and Security Console modules.

/task/task (get)

Parameters

Name	Description
body * required *(body)*	

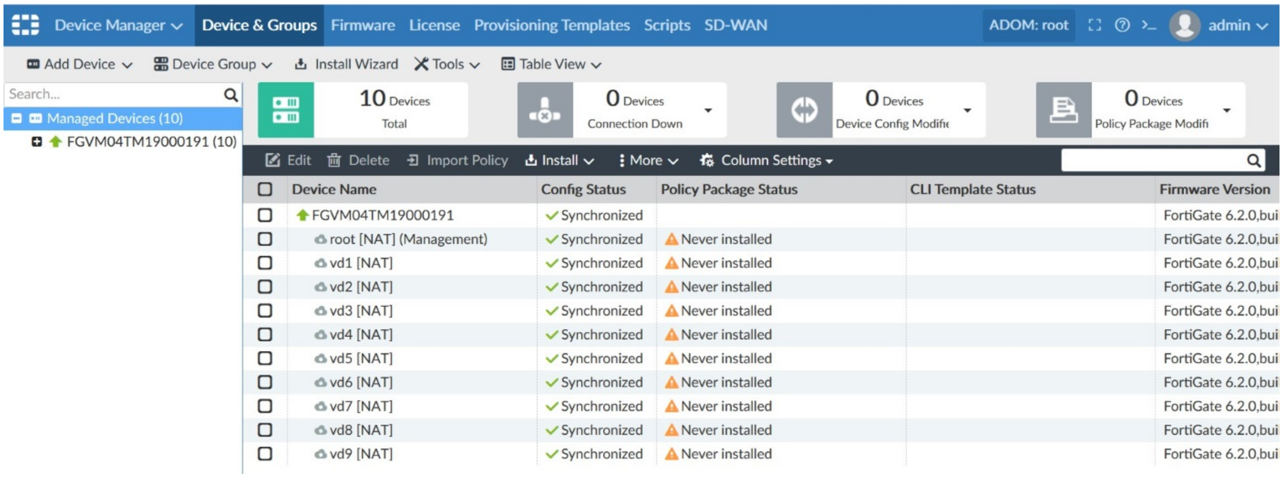
```
{
  method          string
                  example: get
  params          [ {
     fields            list.task.task > [...]
     filter            common.filter.object > [...]
     loadsub           integer($int16)
                       Enable or disable the return of any sub-objects. If not specified,
                       the default is to return all sub-objects.

     option            params.task.get.table.option.opts  string
                       Set fetch option for the request. If no option is specified, by
```

License for FortiGates with FortiManager Cloud Entitlement

When a FortiGate contains the FortiManager Cloud license entitlement (from 360 Protection Bundle or a la carte SKU purchase), it will not count towards the license of FortiManager.

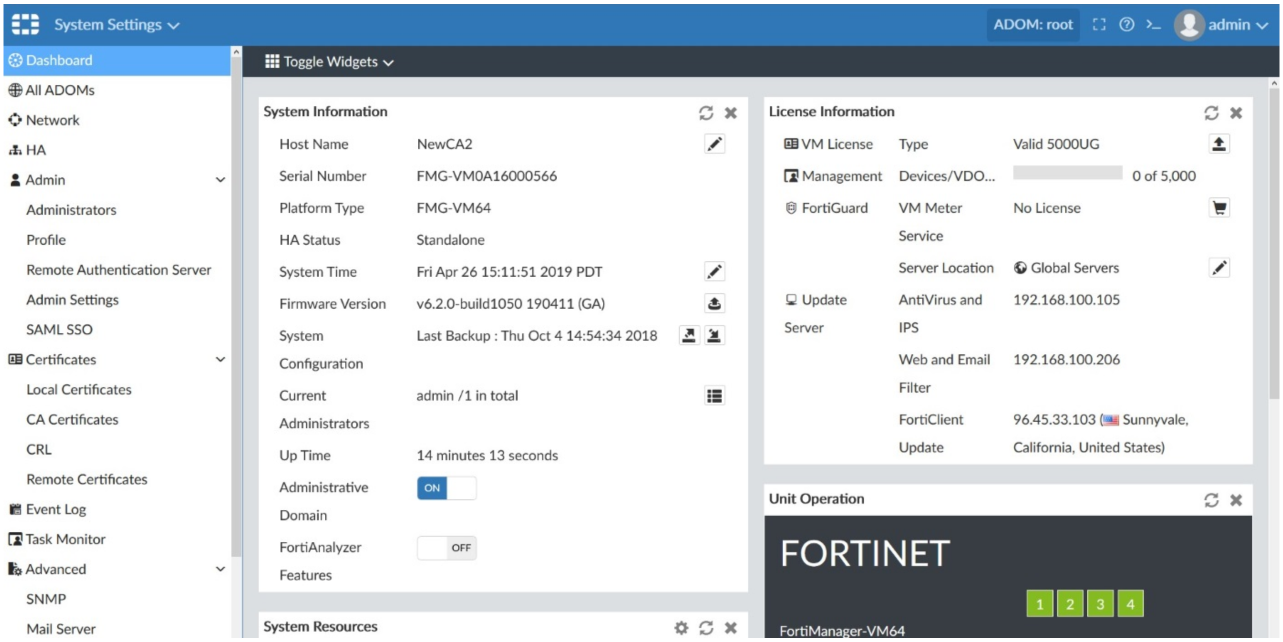
To view the license count via GUI:

1. Add a FortiGate with 10 VDOMs to FortiManager.



Device Name	Config Status	Policy Package Status	CLI Template Status	Firmware Version
FGVM04TM19000191	✓ Synchronized			FortiGate 6.2.0,bui
root [NAT] (Management)	✓ Synchronized	⚠ Never installed		FortiGate 6.2.0,bui
vd1 [NAT]	✓ Synchronized	⚠ Never installed		FortiGate 6.2.0,bui
vd2 [NAT]	✓ Synchronized	⚠ Never installed		FortiGate 6.2.0,bui
vd3 [NAT]	✓ Synchronized	⚠ Never installed		FortiGate 6.2.0,bui
vd4 [NAT]	✓ Synchronized	⚠ Never installed		FortiGate 6.2.0,bui
vd5 [NAT]	✓ Synchronized	⚠ Never installed		FortiGate 6.2.0,bui
vd6 [NAT]	✓ Synchronized	⚠ Never installed		FortiGate 6.2.0,bui
vd7 [NAT]	✓ Synchronized	⚠ Never installed		FortiGate 6.2.0,bui
vd8 [NAT]	✓ Synchronized	⚠ Never installed		FortiGate 6.2.0,bui
vd9 [NAT]	✓ Synchronized	⚠ Never installed		FortiGate 6.2.0,bui

The Device Manager shows the count as 10. However, the total license count is not increased.



System Information

Host Name	NewCA2
Serial Number	FMG-VM0A16000566
Platform Type	FMG-VM64
HA Status	Standalone
System Time	Fri Apr 26 15:11:51 2019 PDT
Firmware Version	v6.2.0-build1050 190411 (GA)
System Configuration	Last Backup : Thu Oct 4 14:54:34 2018
Current Administrators	admin /1 in total
Up Time	14 minutes 13 seconds
Administrative Domain	ON
FortiAnalyzer Features	OFF

License Information

VM License	Type	Valid 5000UG
Management	Devices/VDO...	0 of 5,000
FortiGuard	VM Meter Service	No License
	Server Location	Global Servers
Update Server	AntiVirus and IPS	192.168.100.105
	Web and Email Filter	192.168.100.206
	FortiClient Update	96.45.33.103 (Sunnyvale, California, United States)

To check the license count via CLI:

1. Run the command `diagnose fmupdate dbcontract fds FGVM04TM19000191`
   The following output is shown:

```
FGVM04TM19000191 [SERIAL_NO]
                                  AccountID: fmgclouduser001@mail.com
                                  Industry:  Technology
                                  Company:   fortinet
                                  Contract:  13
                                  AVDB-1-06-20200125
                                  AVEN-1-06-20200125
                                  ENHN-1-10-20200125
```

```
                                       FGSA-1-06-20200125
                                       FMGC-1-06-20200204
                                       FMWR-1-06-20200125
                                       FRVS-1-06-20200125
                                       FURL-1-06-20200125
                                       ISSS-1-06-20200125
                                       NIDS-1-06-20200125
                                       SPAM-1-06-20200125
                                       SPRT-1-10-20200125
                                       ZHVO-1-06-20200125
                                       Contract Raw Data:
                               Contract=AVDB-1-06-20200125:0:1:1:0*AVEN-1-06-20200125:0:1:1:0*ENHN-1-10
20200125:0:1:1:0*FGSA-1-06-20200125:0:1:1:0*FMGC-1-06-20200204:0:1:1:0*FMWR-1-06-
20200125:0:1:1:0*FRVS-1-06-20200125:0:1:1:0*FURL-1-06-20200125:0:1:1:0*ISSS-1-06-
20200125:0:1:1:0*NIDS-1-06-20200125:0:1:1:0*SPAM-1-06-20200125:0:1:1:0*SPRT-1-10-
20200125:0:1:1:0*ZHVO-1-06-
20200125:0:1:1:0|AccountID=fmgclouduser001@mail.com|Industry=Technology|Company=fortinet|Us
erID=876051
```