Getting Started Guide

FortiPolicy 7.2.0

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/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

July 20, 2022
FortiPolicy 7.2.0 Getting Started Guide
64-720-775772-20220720

TABLE OF CONTENTS

Change log

Date	Change Description
July 20, 2022	Initial release

Overview

This guide provides a summary of the configuration required for FortiPolicy deployment in VMware ESXi environments. This guide covers both VMware infrastructure configuration and FortiPolicy configuration.

General workflow

Use this general workflow to set up ESXi for FortiPolicy installation, infrastructure discovery, and security configuration.

1. Review the requirements for your VMware environment before installing FortiPolicy.
   Refer to Requirements on page 7.
2. Perform or confirm the VMware ESXi configuration.
   Refer to Preparing the VMware ESXi environment on page 13.
3. Install FortiPolicy and log in.
   Refer to Installing FortiPolicy on page 17.
4. Configure FortiPolicy by importing the license file, creating a fabric connector, configuring data planes, and setting up Policy Generation.
   Refer to Configuring FortiPolicy on page 31.
5. Approve and deploy proposed applications and policies, microsegment workloads or segment application tiers, test policy rules and resolve violations, and enforce security policies.
   Refer to the *FortiPolicy Automated Policy Generation Guide*.

Requirements

Confirm that your ESXi environment meets FortiPolicy prerequisites and requirements before beginning the installation procedure. The following list contains all needed access privileges and requirements for deploying FortiPolicy into a VMware ESXi infrastructure. You can use the following as a checklist.

- Internet access. Outbound communication is required to allow the management plane to access FortiPolicy for software upgrades, licensing, and other features.
- Latest version of Google Chrome
- Access to the Fortinet InfoSite
- VMware vSphere 6.5 and higher for deploying FortiPolicy
- vCenter 6.x and above
- vCenter Server 6.0 or 6.5
- One IP address or fully qualified domain name (FQDN) for your vCenter server
- One ESXi host with 6.x and above
    - Network Time Protocol (NTP) enabled on ESXi hosts
    - vCenter credentials and user access are needed to deploy the FortiPolicy VM.
- Intel CPU, Sandy Bridge or later
- 86-100 GB memory
- 550-GB hard disk—thin provisioning
- One network interface with a static IP address
- One static IP address, a gateway, and a netmask to set up FortiPolicy
- A management network with DHCP. The management network must be reachable with the management VLAN.
- Laptop for client access (physical Ethernet preferred)
- One or more managed FortiSwitch units
    - Do NOT configure flow tracking on the connected FortiSwitch units.
- Root FortiGate device and any child FortiGate devices
    - For your critical business applications, you might want to monitor the security events for each application protected by FortiPolicy. To do so, enable the layer-7 security profiles in security policies for the applications:
        - Enable the deep-inspection security profile in FortiOS to show exploits in FortiPolicy.
        - Enable the application control security profile in FortiOS to show application ID events in FortiPolicy.
        - Enable the web filter security profile in FortiOS to show risky domains in FortiPolicy.
        - Enable the file filter security profile in FortiOS to show malware in FortiPolicy.

      To configure security profiles, see Security Profiles. To configure security policies, see NGFW policy.

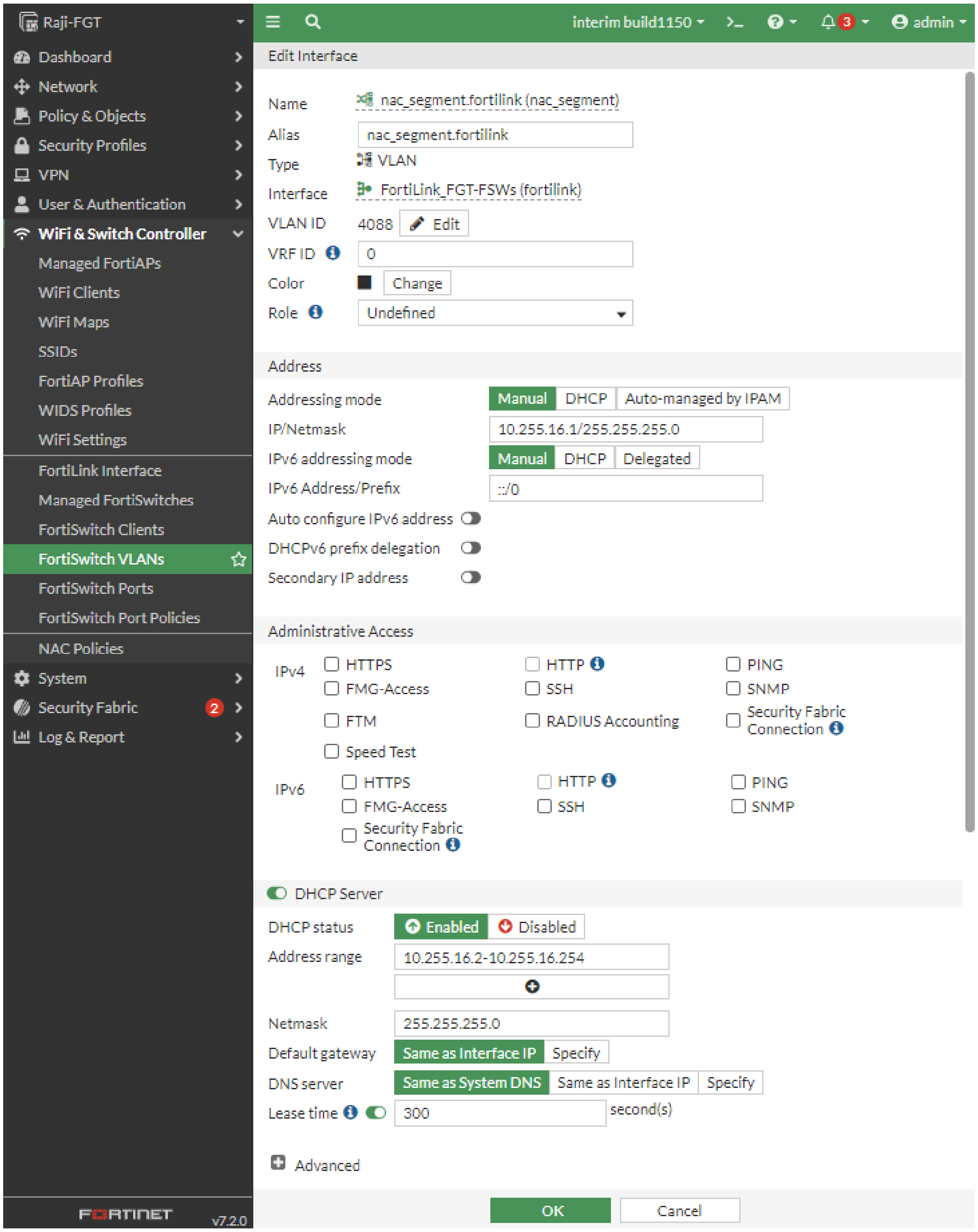
      After security profiles are configured in FortiOS and selected in security policies for the applications, go to *Workspace > Applications* in FortiPolicy (after it is installed and configured) and click on the *Risk* value to open the *Application Summary* page, where you can see all security events for the application in FortiPolicy.
    - The FortiGate management ports must have *Fabric Integration* selected, and the FortiGate devices must be reachable from FortiPolicy.

- The FortiGate devices cannot have a custom virtual domain (VDOM). Custom VDOMs prevent fabric integration.
- A NAC LAN segment must be configured on the physical FortiGate devices. You can use the default `nac_segment.fortilink` interface or create a new one.
- The FortiGate devices must have a FortiLink VLAN interface that can be used as a NAC LAN segment before configuring proxy Address Resolution Protocol (ARP). All workloads that you want FortiPolicy to inspect and generate policies for must be connected to the FortiLink VLAN interface on the FortiSwitch ports. The workloads must have an IP address from the FortiLink VLAN interface's DHCP range.

To configure the FortiLink VLAN interface in FortiOS:

i. Go to *WiFi & Switch Controller > FortiSwitch VLANs*.
ii. Select the FortiLink VLAN interface. The default FortiLink VLAN interface is `nac_segment.fortilink`.
iii. Click *Edit*.
iv. Make certain that the addressing mode is set to *Manual*.
v. Enable *DHCP Server* and click *Enabled* for the DHCP status.

vi. Enter the address range and netmask for the DHCP server.



Edit Interface

Name	nac_segment.fortilink (nac_segment)
Alias	nac_segment.fortilink
Type	VLAN
Interface	FortiLink_FGT-FSWs (fortilink)
VLAN ID	4088 Edit
VRF ID	0
Color	■ Change
Role	Undefined

Address

Addressing mode	[✓ Manual] DHCP Auto-managed by IPAM
IP/Netmask	10.255.16.1/255.255.255.0
IPv6 addressing mode	[✓ Manual] DHCP Delegated
IPv6 Address/Prefix	::/0
Auto configure IPv6 address	○
DHCPv6 prefix delegation	○
Secondary IP address	○

Administrative Access

IPv4 □ HTTPS □ HTTP □ PING □ FMG-Access □ SSH □ SNMP □ FTM □ RADIUS Accounting □ Security Fabric Connection □ Speed Test

IPv6 □ HTTPS □ HTTP □ PING □ FMG-Access □ SSH □ SNMP □ Security Fabric Connection

● DHCP Server

DHCP status	[✓ Enabled] Disabled
Address range	10.255.16.2-10.255.16.254
Netmask	255.255.255.0
Default gateway	[✓ Same as Interface IP] Specify
DNS server	[✓ Same as System DNS] Same as Interface IP Specify
Lease time ●	300 second(s)

Advanced

OK Cancel

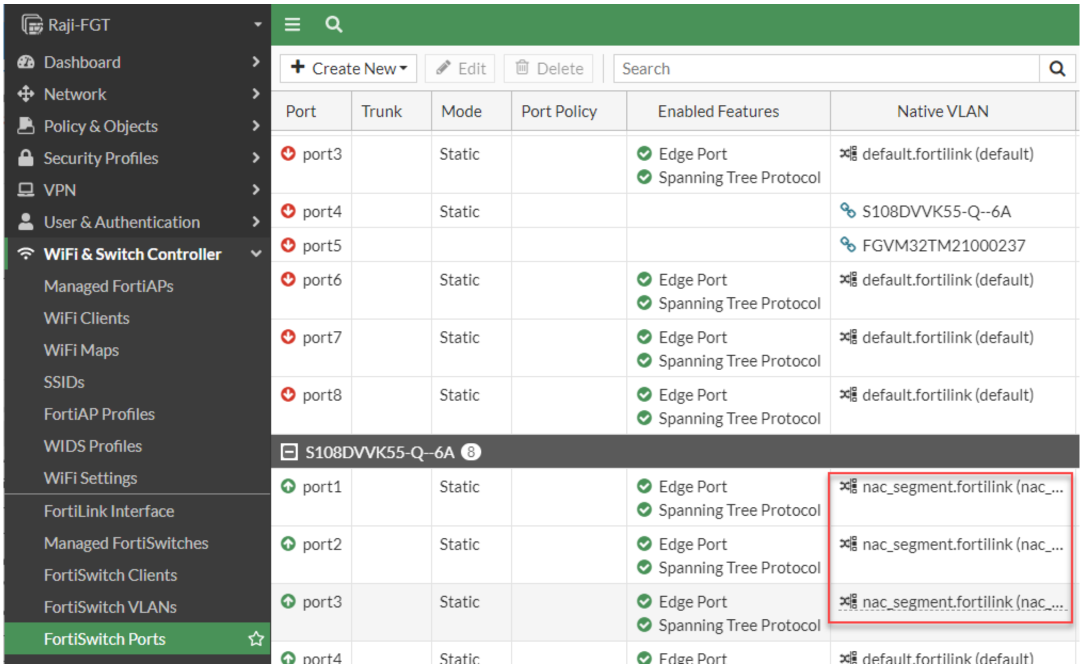
vii. Click *OK*.

viii. Go to *WiFi & Switch Controller > FortiSwitch Ports*.

ix. Hover over the *Native VLAN* column for one of the ports that should be used for the FortiLink VLAN and then click on the pencil to edit the native VLAN.

x. Select the FortiLink VLAN and then click *Apply*.

xi. Change the native VLAN to the FortiLink VLAN for each port connected to devices that need protection by FortiPolicy automatic policies.



Port	Trunk	Mode	Port Policy	Enabled Features	Native VLAN
port3		Static		Edge Port Spanning Tree Protocol	default.fortilink (default)
port4		Static			S108DVVK55-Q--6A
port5					FGVM32TM21000237
port6		Static		Edge Port Spanning Tree Protocol	default.fortilink (default)
port7		Static		Edge Port Spanning Tree Protocol	default.fortilink (default)
port8		Static		Edge Port Spanning Tree Protocol	default.fortilink (default)
S108DVVK55-Q--6A 8					
port1		Static		Edge Port Spanning Tree Protocol	nac_segment.fortilink (nac_...
port2		Static		Edge Port Spanning Tree Protocol	nac_segment.fortilink (nac_...
port3		Static		Edge Port Spanning Tree Protocol	nac_segment.fortilink (nac_...
port4		Static		Edge Port	default.fortilink (default)

- Use the CLI to configure the proxy ARP on the primary NAC segment interface on the FortiGate devices. For example:

```
config system proxy-arp
   edit 1
      set interface “nac_segment”
      set ip 10.255.13.2
      set end-ip 10.255.13.5
   next
end
```

Connectivity requirements

The following table lists the ESXi resource requirements.

FortiPolicy component	vCPU requirements	VM requirements
FortiPolicy management plane	10 vCPUs	1 VM

The following table lists the ports that FortiPolicy needs for communication through a firewall.

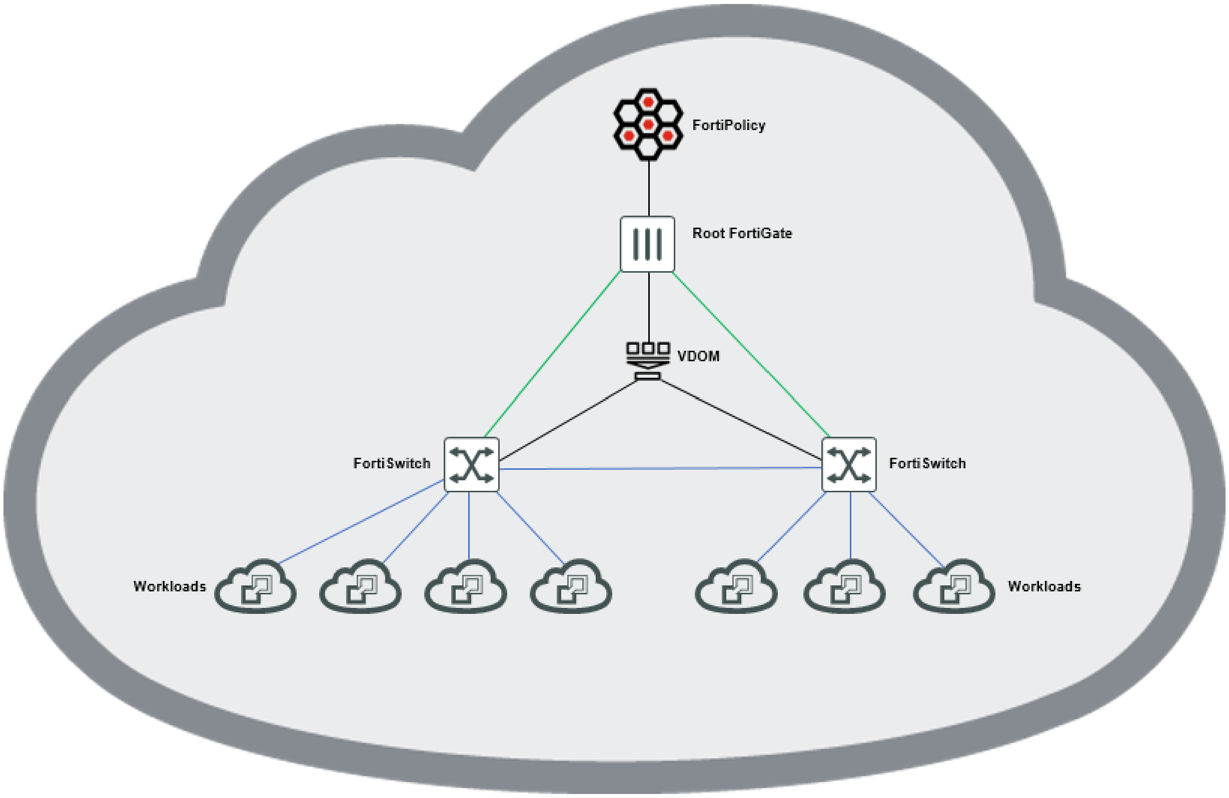
Service or program	Protocol	Incoming ports	Outgoing ports	Internal ports
SSHD	TCP	22		
DNS	TCP, UDP		53	
NTP	UDP		123 outbound queries to NTP servers from FortiPolicy	123 to FortiPolicy
Web access	TCP	80, 443		FortiPolicy port 5601
Connection between FortiPolicy and Security Fabric	TCP		8013 and 443	
Connection between FortiGate and FortiPolicy	UDP 4739	Syslog port for NetFlow	Syslog port for NetFlow	
For telemetry uploads to fortipolicy.fortinet.com	TCP	sxti.shieldx.com:443	sxti.shieldx.com:443	

The following table lists the required management ports.

Service or program	Protocol	Incoming ports	Outgoing ports	Internal ports
Web access	TCP	80		FortiPolicy port 5601
Web access	TCP	443		FortiPolicy port 5601

Deployment

The following figure shows the Fortinet Security Fabric for an east/west deployment.



Preparing the VMware ESXi environment

Use the following procedures to prepare the VMware ESXi environment before installing FortiPolicy:

1. Downloading the installation files for ESXi on page 13.
2. Selecting an ESXi host for FortiPolicy installation on page 14.
3. Setting up the management network in vSphere on page 16.

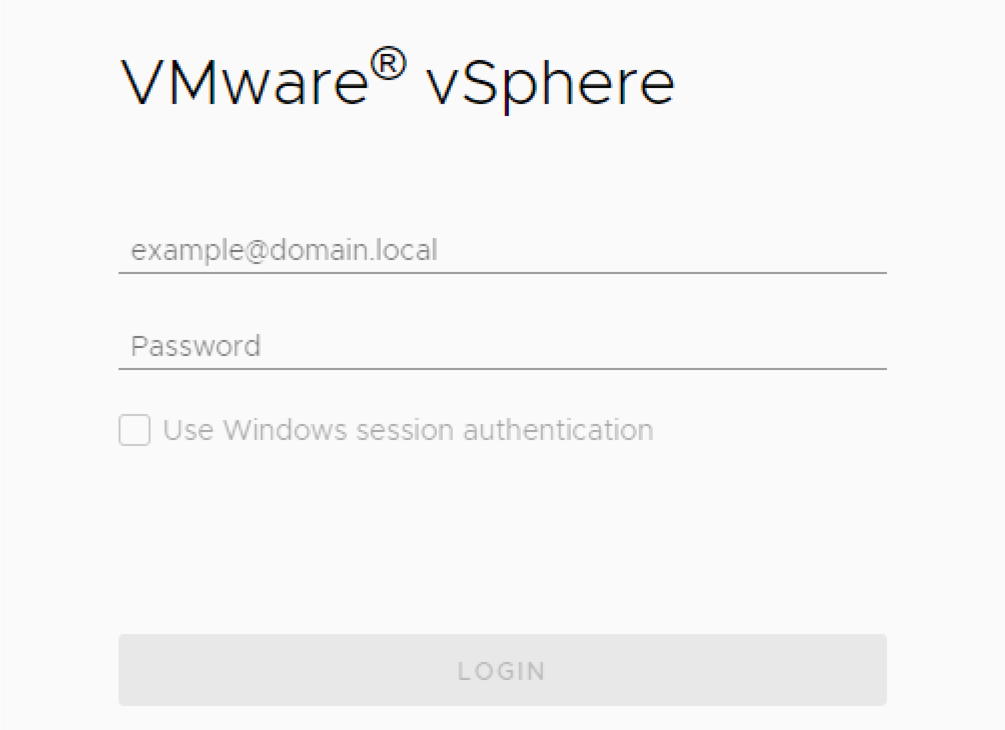
Downloading the installation files for ESXi

Download the following FortiPolicy installation file from the Fortinet InfoSite:

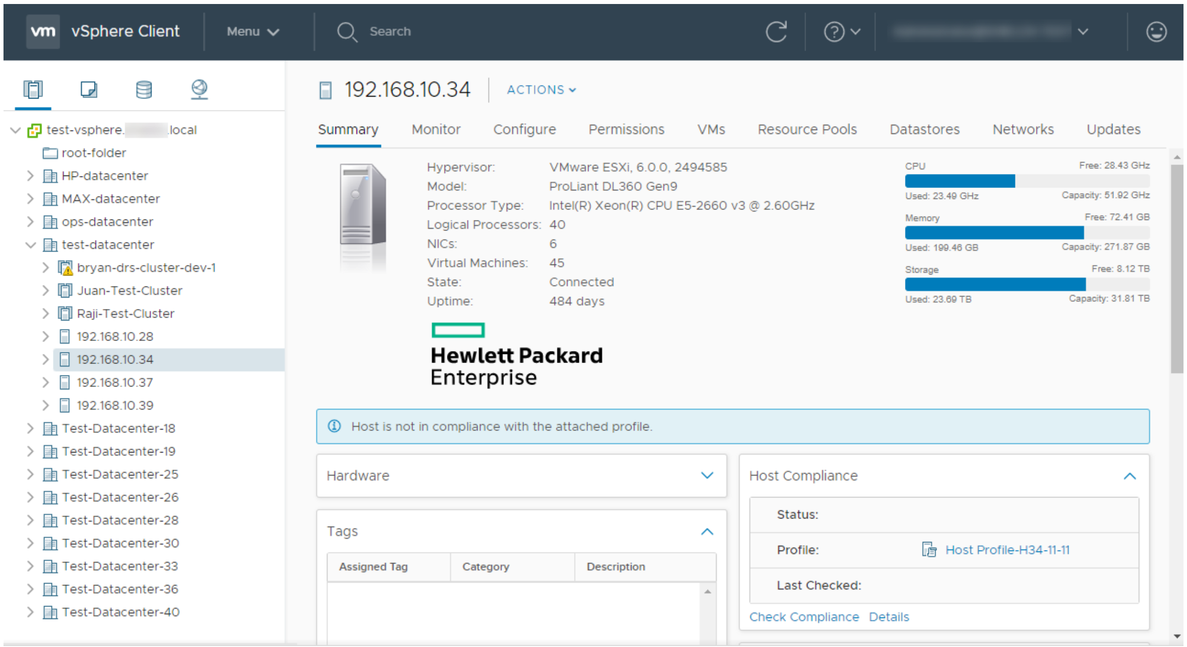
```
FortiPolicy-VM64-v7.2.0-buildxxxx-FORTINET.ova
```

Selecting an ESXi host for FortiPolicy installation

1. Log into your infrastructure using vSphere.
   These are the same credentials you will use to perform infrastructure discovery from the FortiPolicy console later on.



2. Select a host in your data center infrastructure where you will install FortiPolicy.



Hypervisor: VMware ESXi, 6.0.0, 2494585
Model: ProLiant DL360 Gen9
Processor Type: Intel(R) Xeon(R) CPU E5-2660 v3 @ 2.60GHz
Logical Processors: 40
NICs: 6
Virtual Machines: 45
State: Connected
Uptime: 484 days

CPU Free: 28.43 GHz
Used: 23.49 GHz Capacity: 51.92 GHz
Memory Free: 72.41 GB
Used: 199.46 GB Capacity: 271.87 GB
Storage Free: 8.12 TB
Used: 23.69 TB Capacity: 31.81 TB

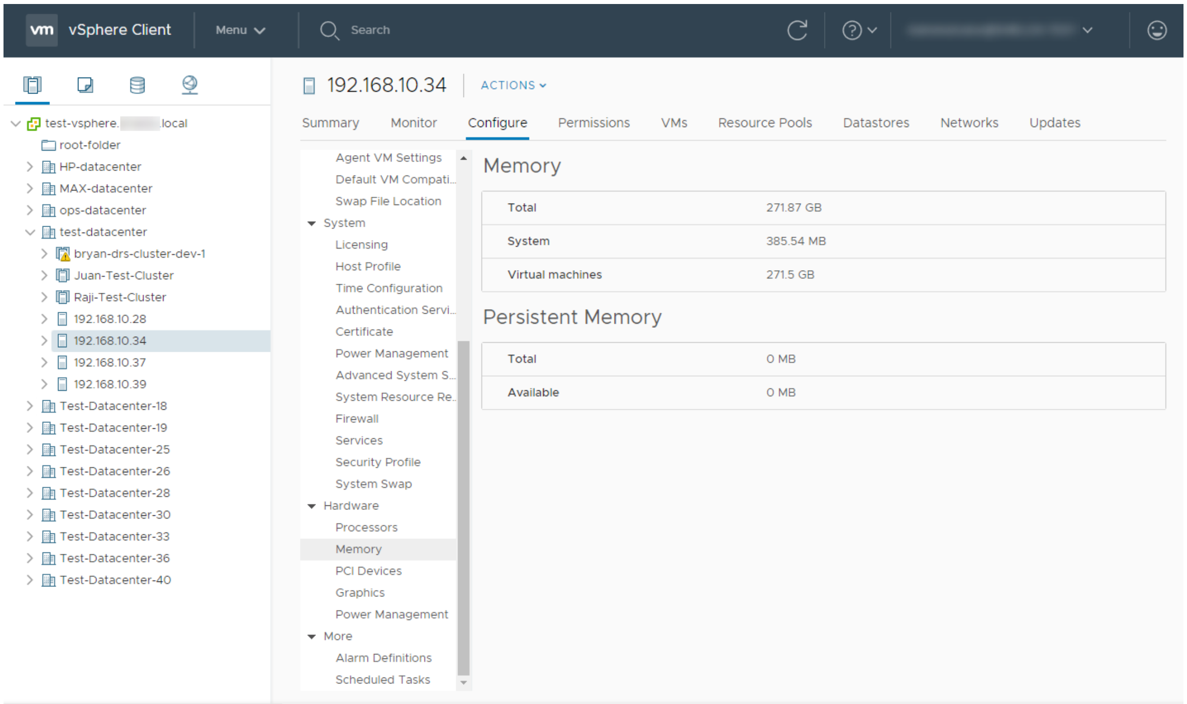
Host is not in compliance with the attached profile.

Assigned Tag	Category	Description

Status:
Profile: Host Profile-H34-11-11
Last Checked:

FortiPolicy provides NSX coexistence, where VMware NSX can be installed together with FortiPolicy in the same infrastructure.

3. Confirm that user privileges, memory, CPU, and core requirements are met on your selected host. Configure the host to meet requirements as necessary. See Requirements on page 7.



Memory

Total	271.87 GB
System	385.54 MB
Virtual machines	271.5 GB

Persistent Memory

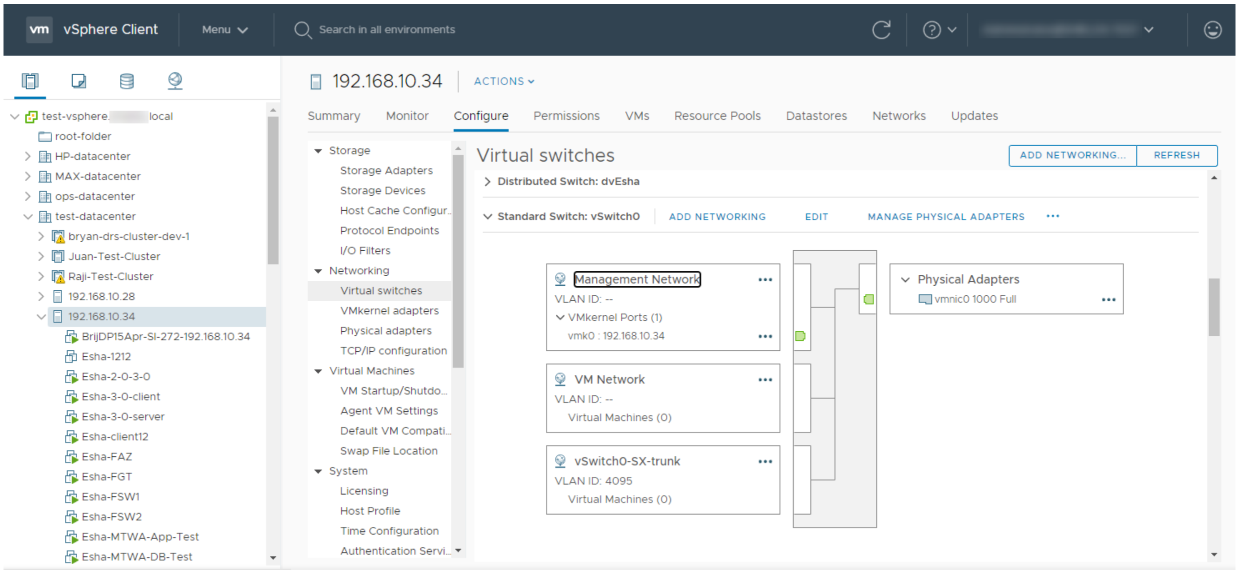
Total	0 MB
Available	0 MB

Setting up the management network in vSphere

The FortiPolicy management network configuration allows FortiPolicy to communicate between its management plane microservices, segments, and microsegments.

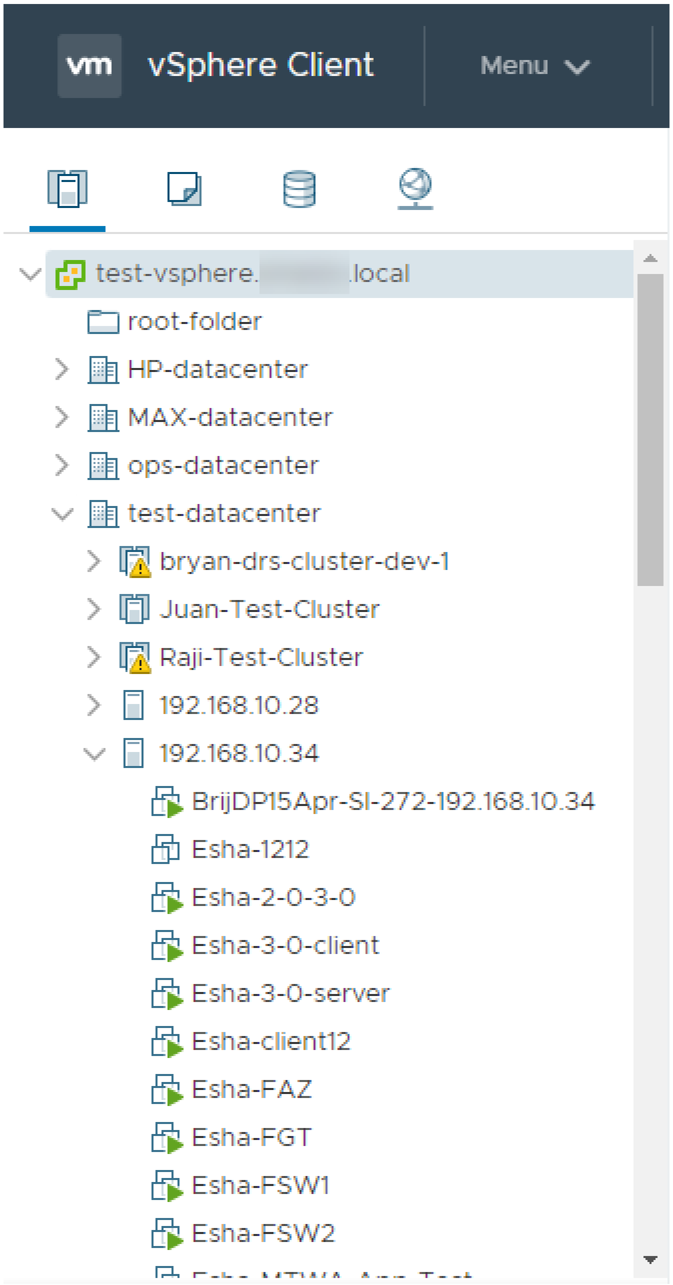
The management plane allows communication between FortiPolicy microservices and the management console and also connects to the outside world for software updates and so on.

If a management network already exists, FortiPolicy can use that but consider whether to use the existing network very carefully (do not use the kernel network, for example). You will need to specify which existing management network FortiPolicy should use. If no management network is already configured, you will need to set up a management network to be used by FortiPolicy on the selected host.



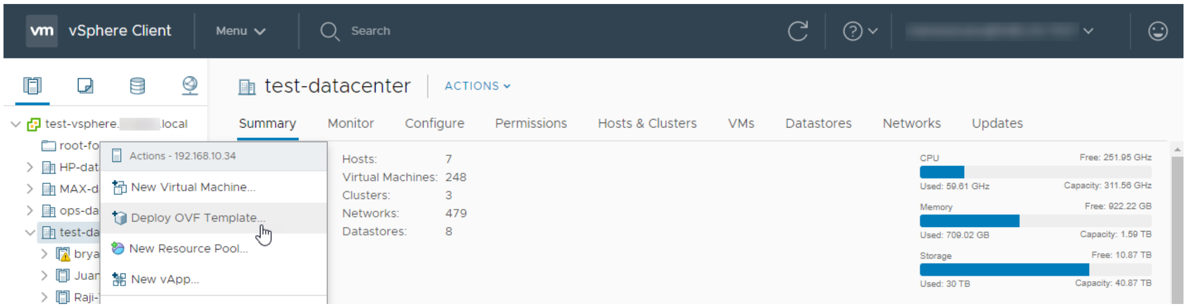
Installing FortiPolicy

1. Navigate to the host where FortiPolicy is to be installed.



test-vsphere.[redacted].local
root-folder
HP-datacenter
MAX-datacenter
ops-datacenter
test-datacenter
bryan-drs-cluster-dev-1
Juan-Test-Cluster
Raji-Test-Cluster
192.168.10.28
192.168.10.34
BrijDP15Apr-SI-272-192.168.10.34
Esha-1212
Esha-2-0-3-0
Esha-3-0-client
Esha-3-0-server
Esha-client12
Esha-FAZ
Esha-FGT
Esha-FSW1
Esha-FSW2

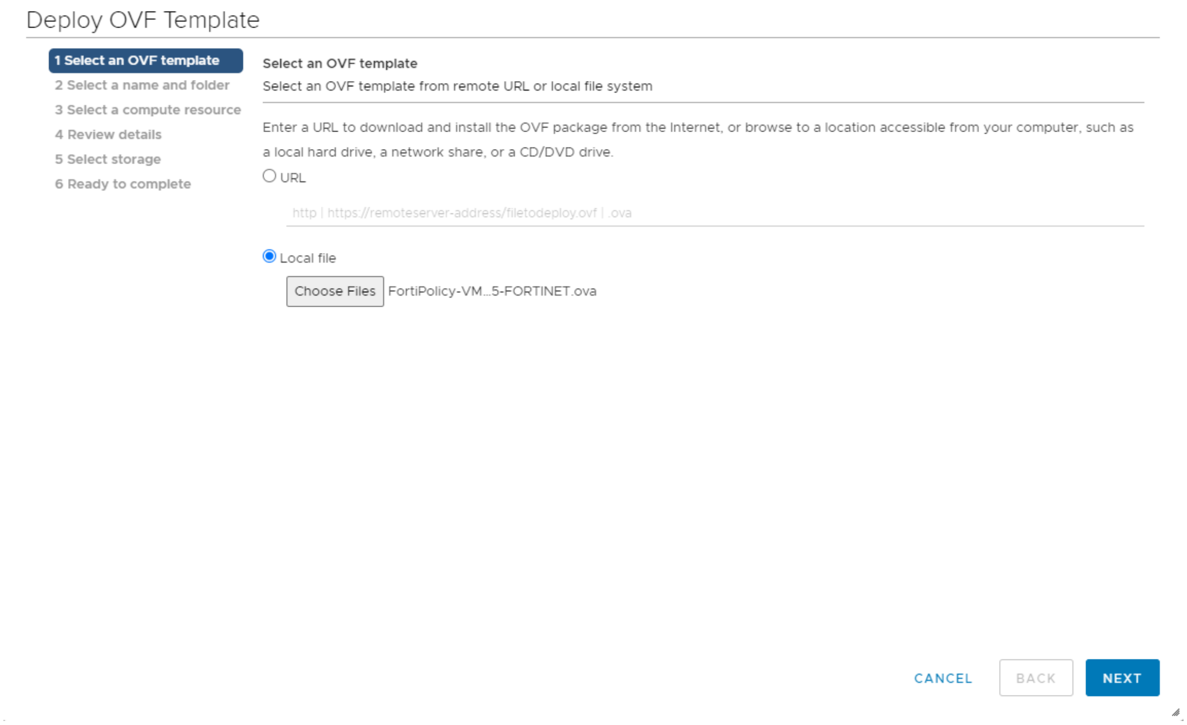
2. Right-click on the host and select *Deploy OVF Template*.



Hosts: 7
Virtual Machines: 248
Clusters: 3
Networks: 479
Datastores: 8

CPU Free: 251.95 GHz
Used: 59.61 GHz Capacity: 311.56 GHz
Memory Free: 922.22 GB
Used: 709.02 GB Capacity: 1.59 TB
Storage Free: 10.87 TB
Used: 30 TB Capacity: 40.87 TB

3. Locate and select the FortiPolicy OVA file and then click *NEXT*.



Deploy OVF Template

1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 Select storage
6 Ready to complete

Select an OVF template

Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

○ URL

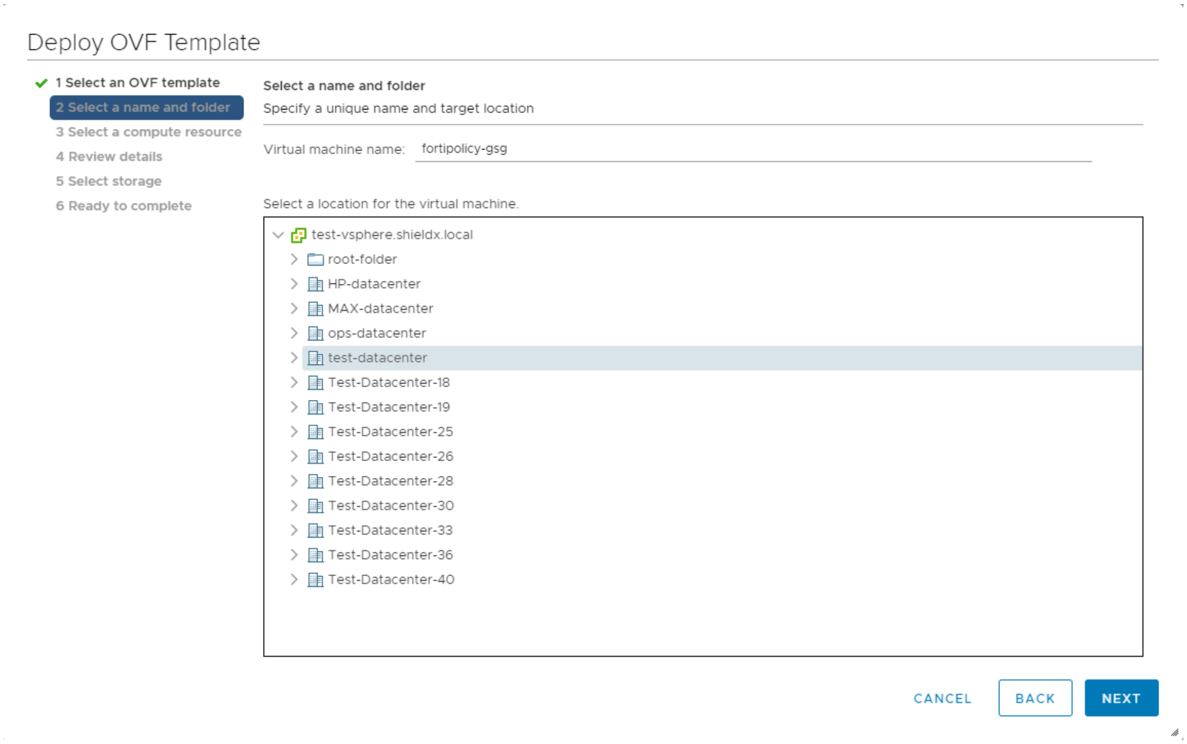
http | https://remoteserver-address/filetodeploy.ovf | .ova

● Local file

Choose Files FortiPolicy-VM...5-FORTINET.ova

CANCEL BACK NEXT

4. Name the FortiPolicy deployment and version in your specified data center location and then click *NEXT*.



Deploy OVF Template

✓ 1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 Select storage
6 Ready to complete

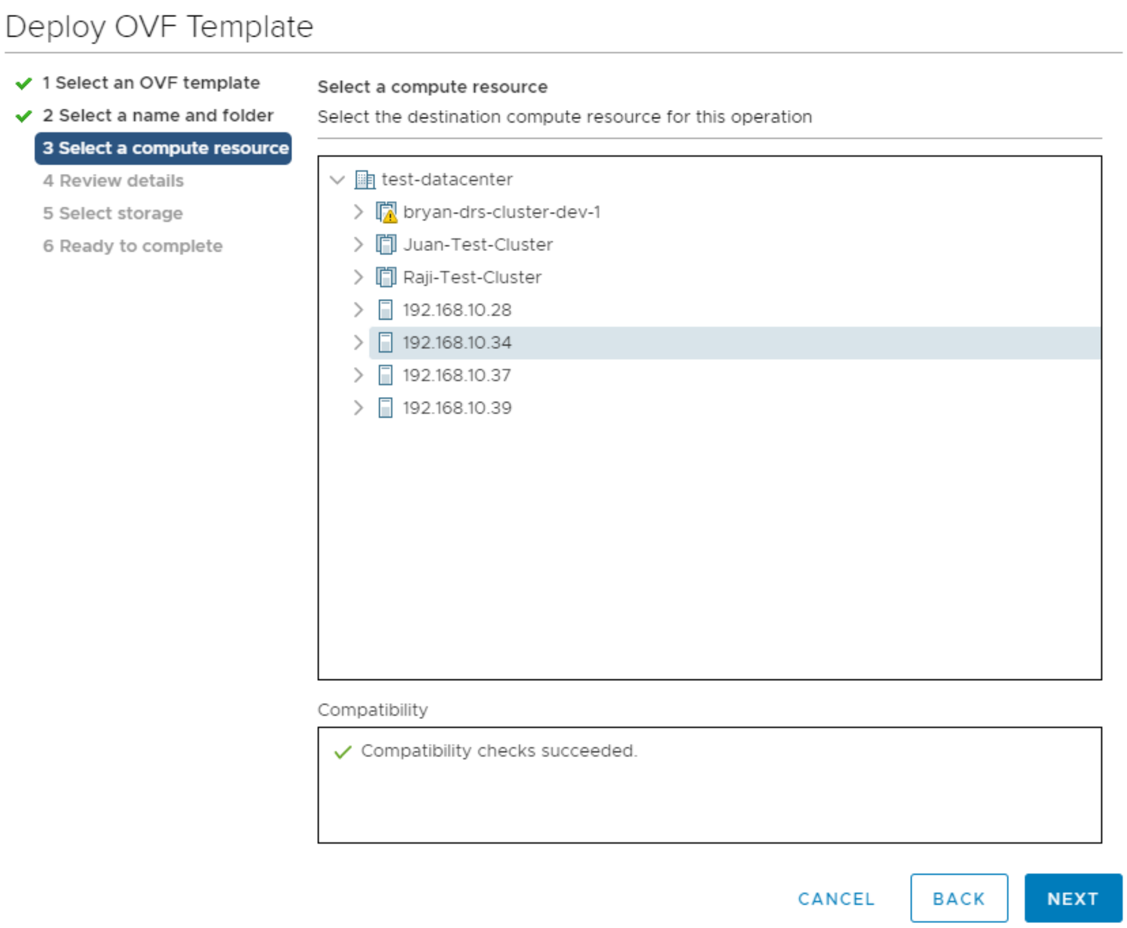
Select a name and folder

Specify a unique name and target location

Virtual machine name: fortipolicy-gsg

Select a location for the virtual machine.

5. Select a compute resource for the FortiPolicy files and then click *NEXT*.


Deploy OVF Template

✓ 1 Select an OVF template
✓ 2 Select a name and folder
3 Select a compute resource
4 Review details
5 Select storage
6 Ready to complete

Select a compute resource

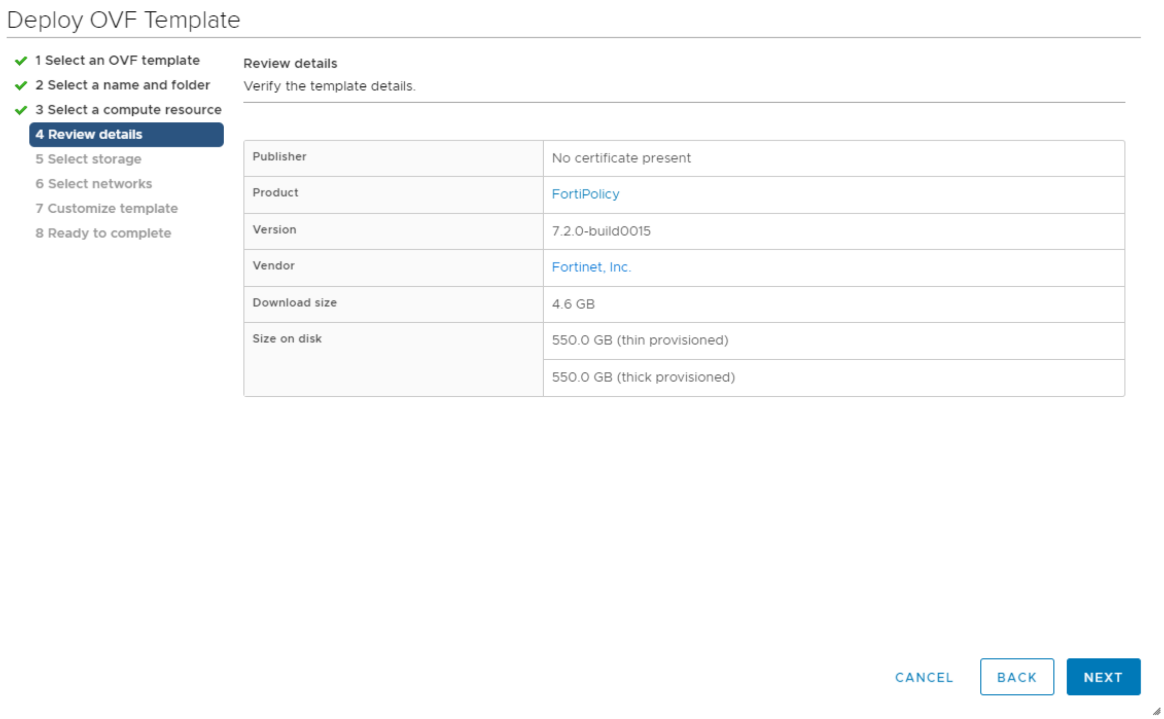
Select the destination compute resource for this operation

- test-datacenter
  - bryan-drs-cluster-dev-1
  - Juan-Test-Cluster
  - Raji-Test-Cluster
  - 192.168.10.28
  - 192.168.10.34
  - 192.168.10.37
  - 192.168.10.39

Compatibility

✓ Compatibility checks succeeded.

6. Review the details and then click *Next*.

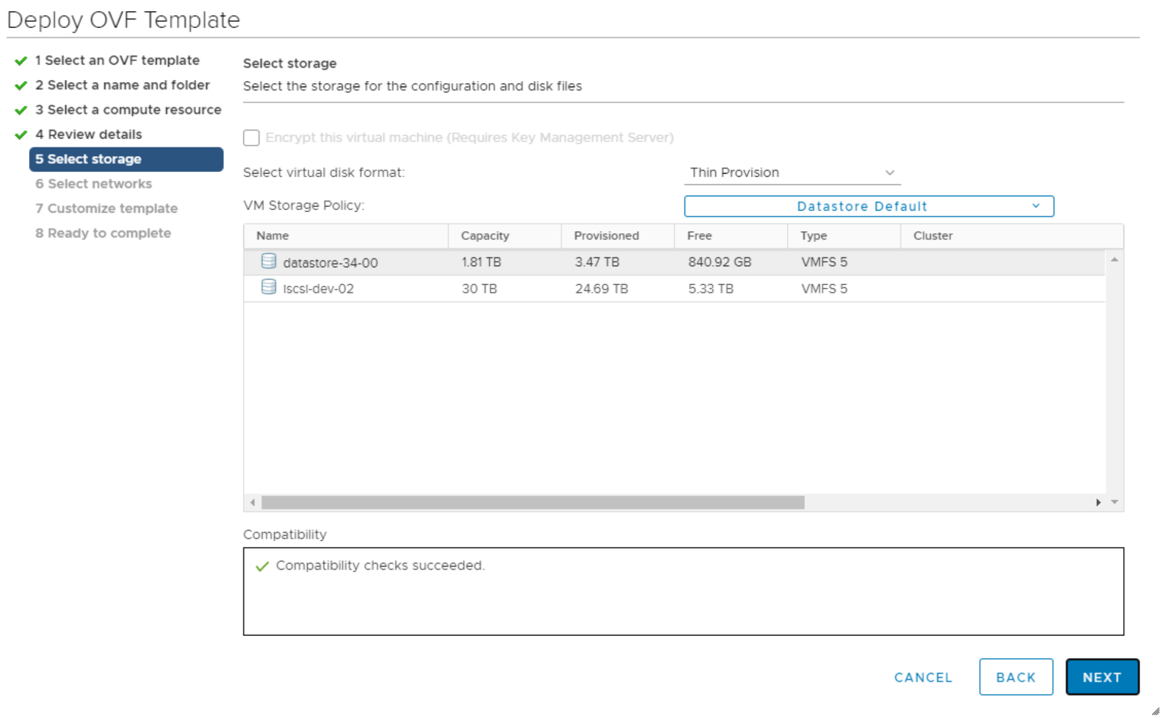


Review details

Verify the template details.

Publisher	No certificate present
Product	FortiPolicy
Version	7.2.0-build0015
Vendor	Fortinet, Inc.
Download size	4.6 GB
Size on disk	550.0 GB (thin provisioned)
	550.0 GB (thick provisioned)

7. Select the data store and virtual disk format and then click *Next*.



Select storage

Select the storage for the configuration and disk files

□ Encrypt this virtual machine (Requires Key Management Server)

Select virtual disk format: Thin Provision

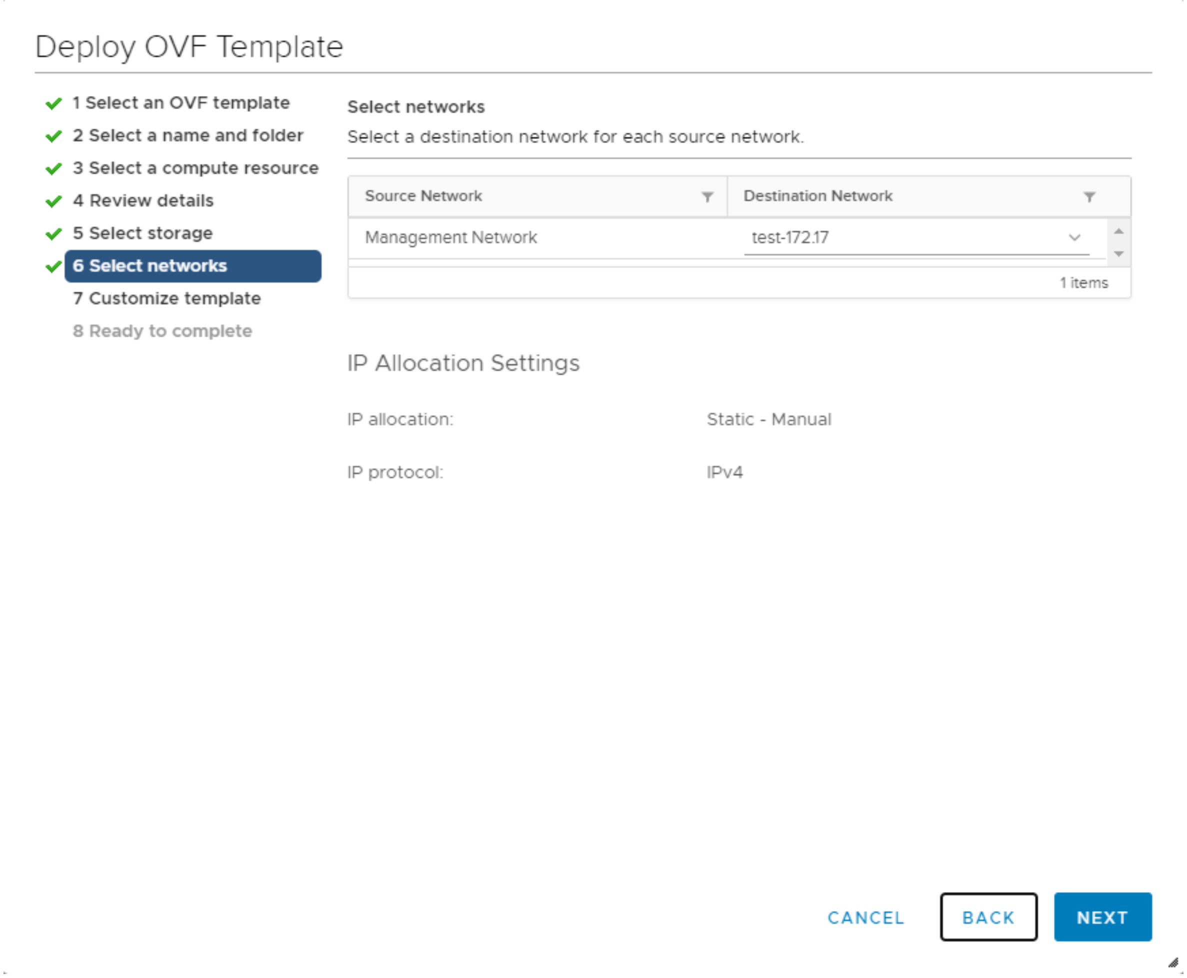
VM Storage Policy: Datastore Default

Name	Capacity	Provisioned	Free	Type	Cluster
datastore-34-00	1.81 TB	3.47 TB	840.92 GB	VMFS 5	
iscsi-dev-02	30 TB	24.69 TB	5.33 TB	VMFS 5	

Compatibility

✓ Compatibility checks succeeded.

8. Select the destination network and then click *NEXT*.



Deploy OVF Template

Select networks

Select a destination network for each source network.

Source Network	Destination Network
Management Network	test-172.17

1 items

IP Allocation Settings

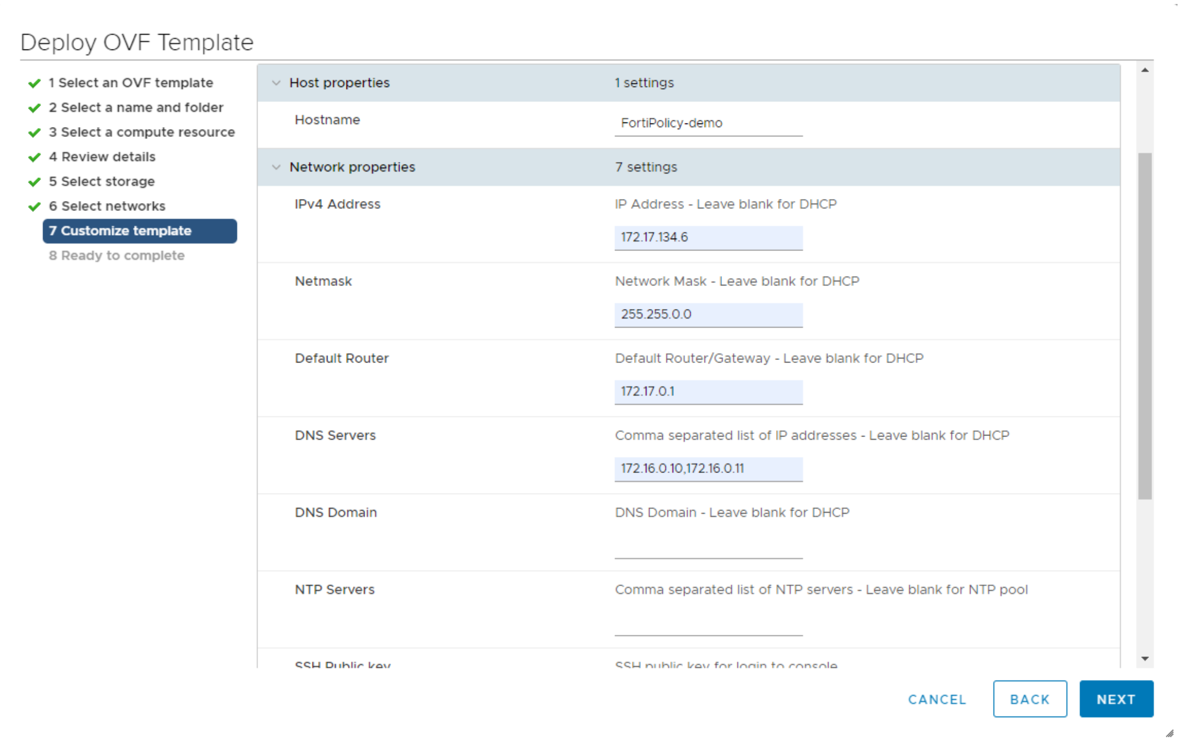
IP allocation: Static - Manual

IP protocol: IPv4

9. Fill out the following fields and then click *NEXT*.
   - *Hostname*—Enter the hostname.
   - *IPv4 Address*—Fortinet recommends a static IP address. Select from the set of IP addresses reserved for FortiPolicy.
   - *Netmask*—Enter the netmask.
   - *Default Router*—Enter the default router IP address.
   - *DNS Servers*—Enter the IP address of each DNS server.
   - *DNS Domain*—If you are using DHCP, leave this field blank.
   - *NTP Servers*—Enter the IP address of each NTP server. In the example, this field is blank because all hosts in this sample setup already have NTP set on them.
   - *SSH Public Key*—This field is not applicable to VMware deployments of FortiPolicy.

   No other configurations are required on this page.

   NOTE: FortiPolicy 7.2.0 supports different networks for management with isolated networks for each location.

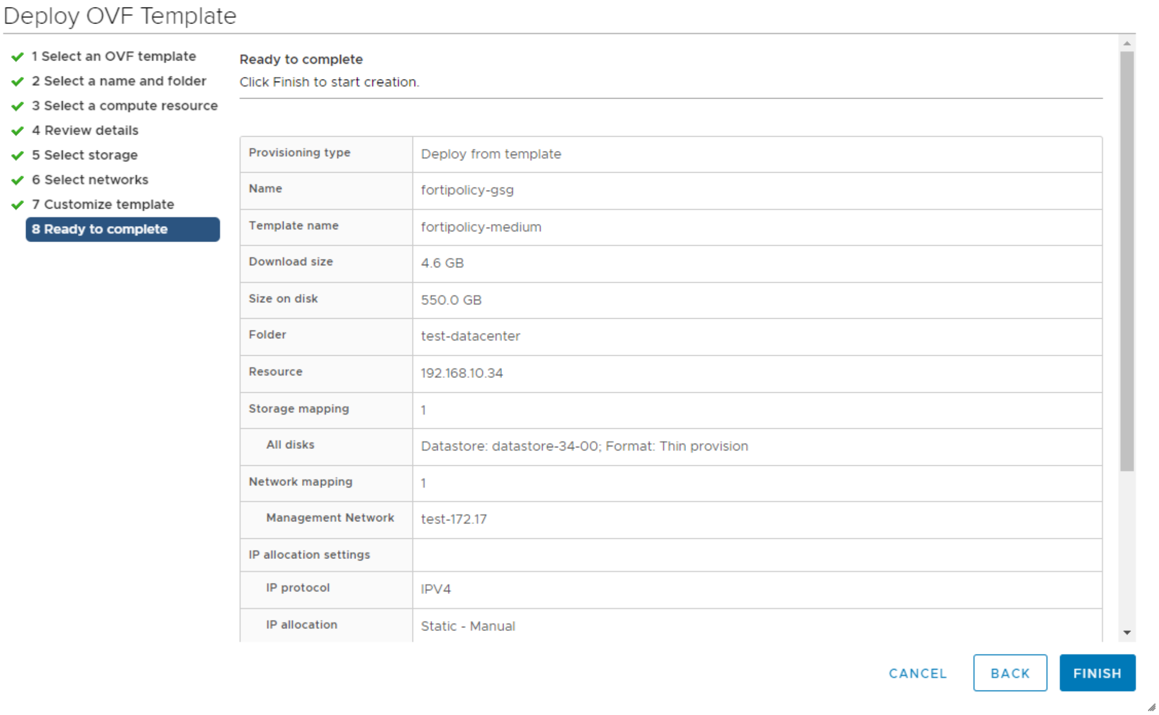


Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 Select storage
- ✓ 6 Select networks
- **7 Customize template**
- 8 Ready to complete

Host properties	1 settings
Hostname	FortiPolicy-demo
Network properties	7 settings
IPv4 Address	IP Address - Leave blank for DHCP 172.17.134.6
Netmask	Network Mask - Leave blank for DHCP 255.255.0.0
Default Router	Default Router/Gateway - Leave blank for DHCP 172.17.0.1
DNS Servers	Comma separated list of IP addresses - Leave blank for DHCP 172.16.0.10,172.16.0.11
DNS Domain	DNS Domain - Leave blank for DHCP
NTP Servers	Comma separated list of NTP servers - Leave blank for NTP pool
SSH Public key	SSH public key for login to console

10. Review the configuration and then click *FINISH*.



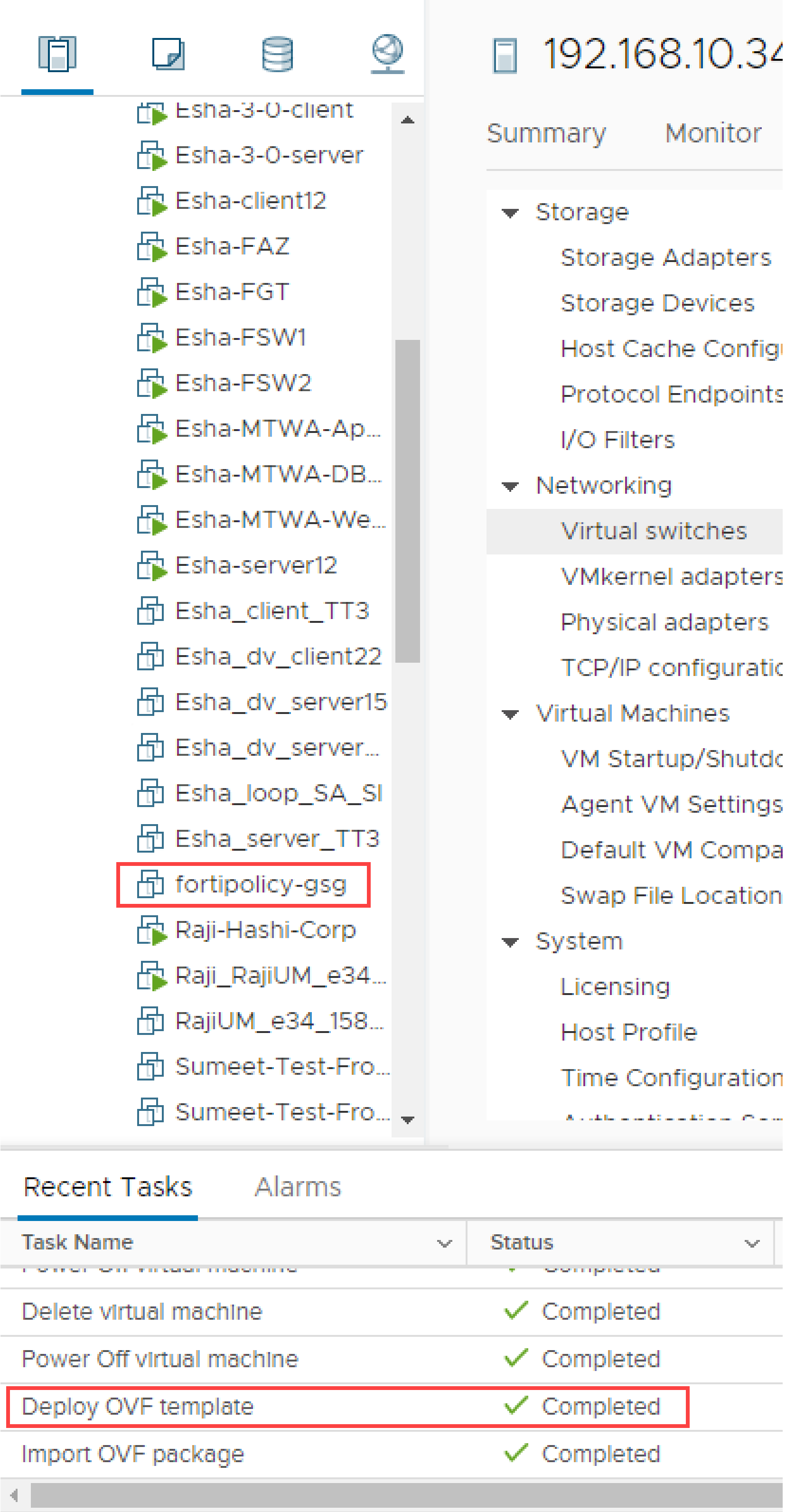
Deploy OVF Template

Ready to complete

Click Finish to start creation.

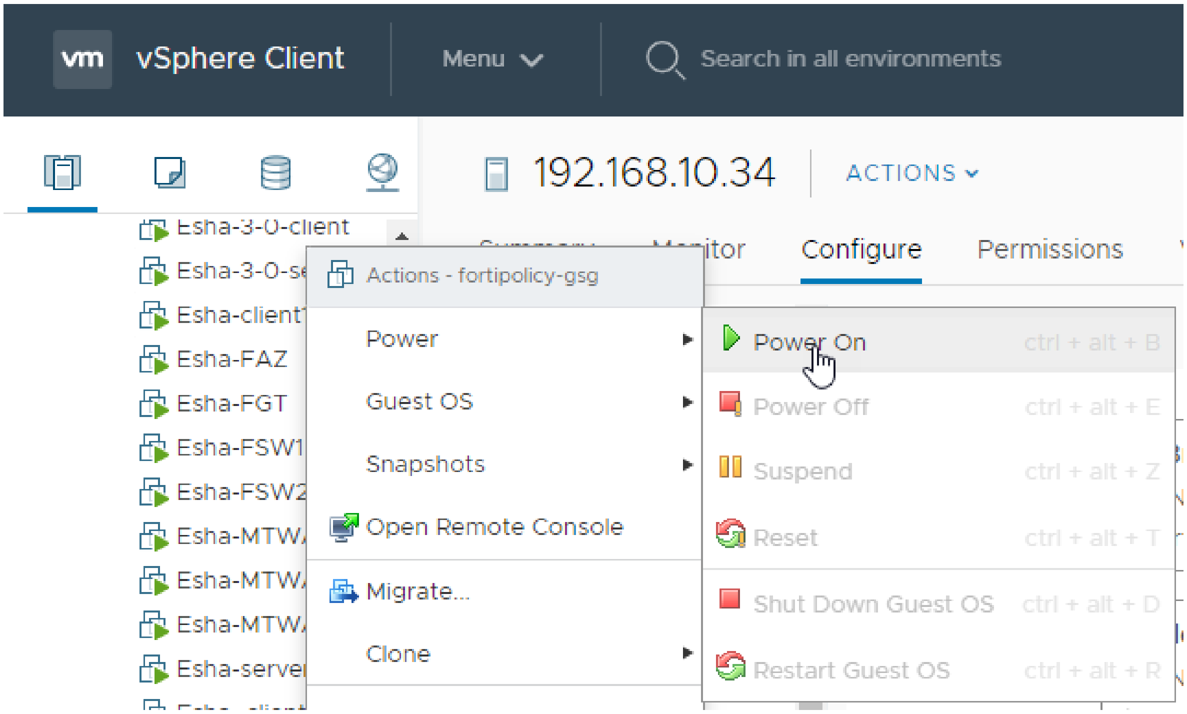
Provisioning type	Deploy from template
Name	fortipolicy-gsg
Template name	fortipolicy-medium
Download size	4.6 GB
Size on disk	550.0 GB
Folder	test-datacenter
Resource	192.168.10.34
Storage mapping	1
All disks	Datastore: datastore-34-00; Format: Thin provision
Network mapping	1
Management Network	test-172.17
IP allocation settings	
IP protocol	IPV4
IP allocation	Static - Manual

11. When the OVF template is deployed, the *Recent Tasks* pane displays *Completed*, and the new VM is listed in the *Hosts and Clusters* pane.

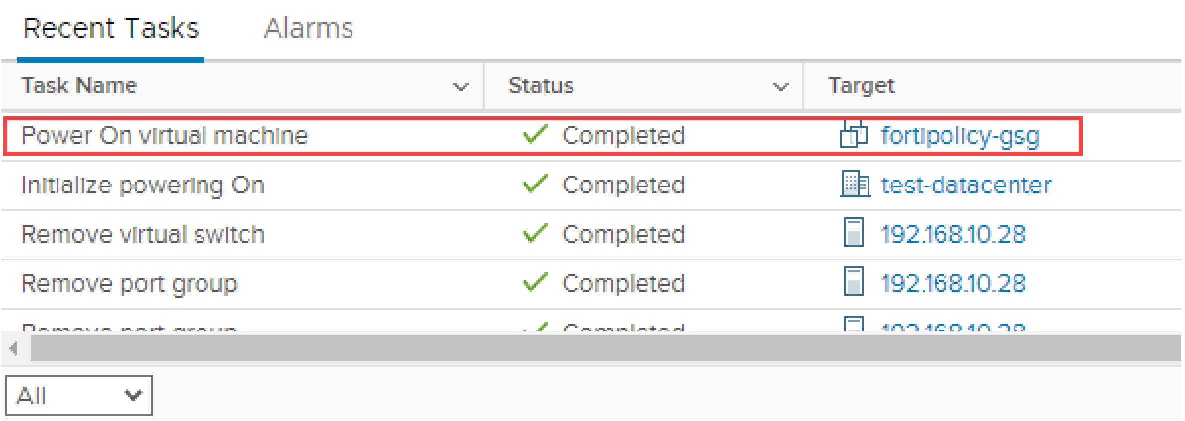


Task Name	Status
Delete virtual machine	✓ Completed
Power Off virtual machine	✓ Completed
Deploy OVF template	✓ Completed
Import OVF package	✓ Completed

12. Right-click on the name of the new VM and select *Power* > *Power On*.

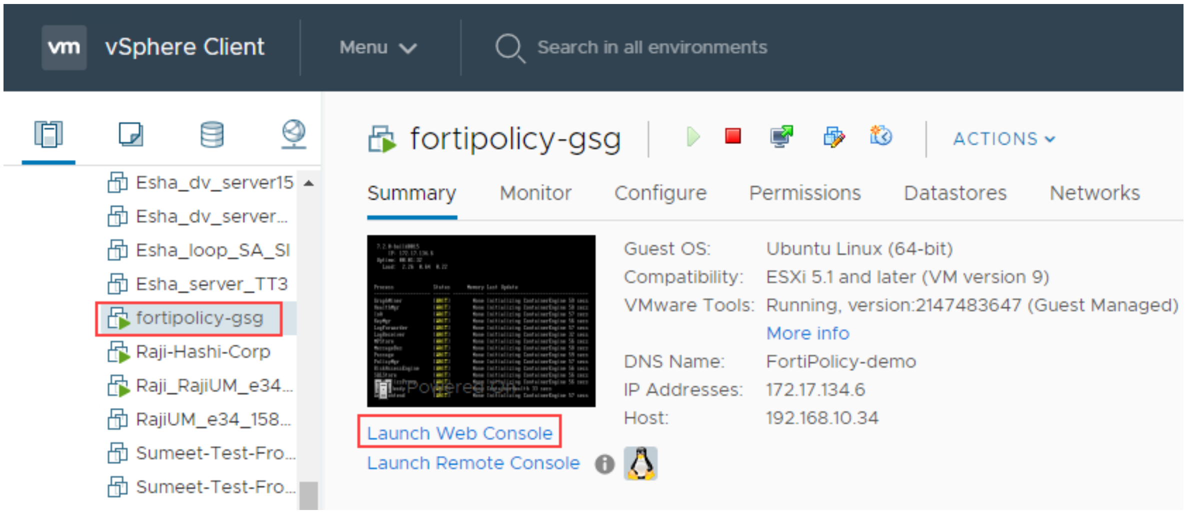


13. Check that the task has completed.



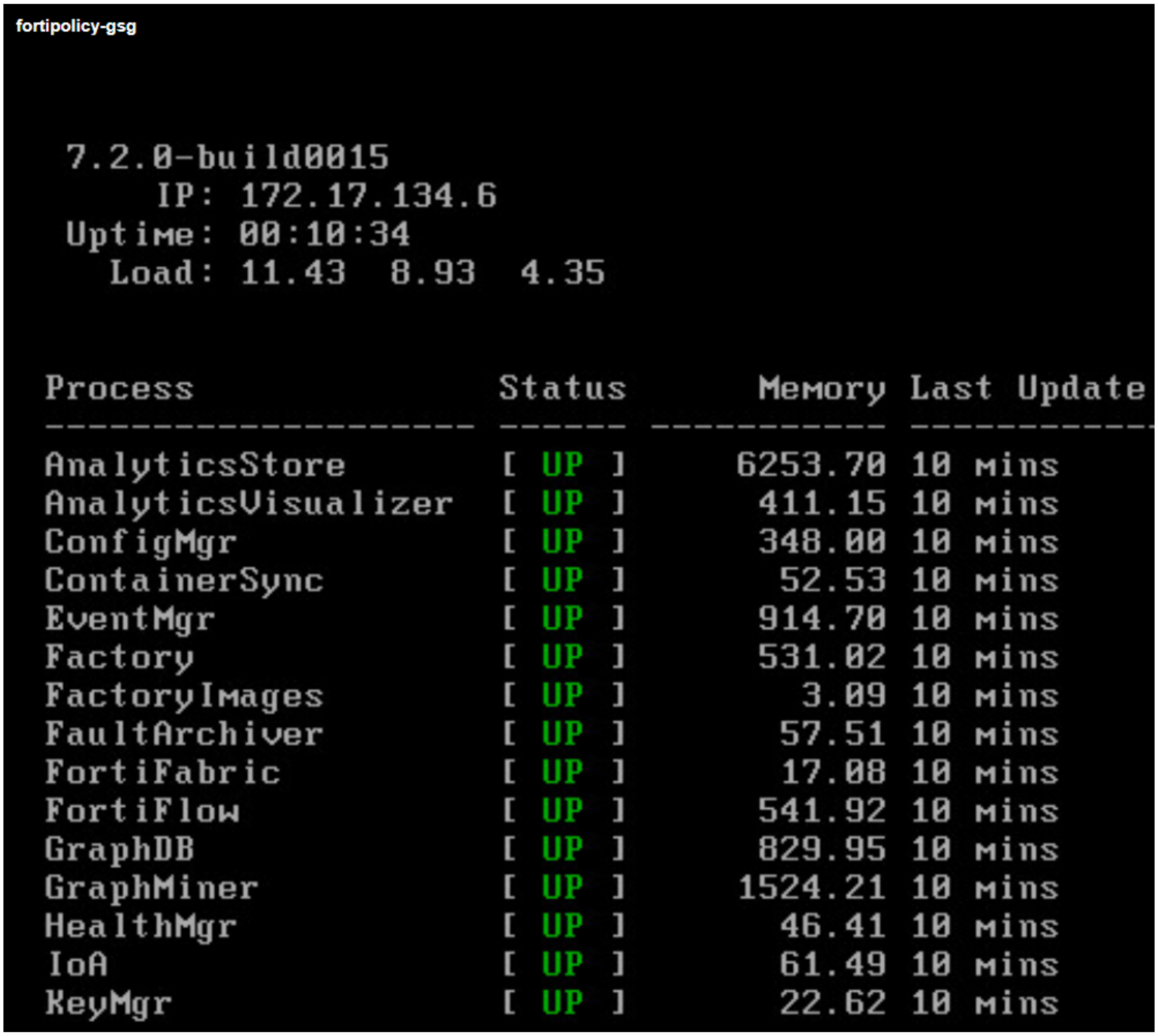
Task Name	Status	Target
Power On virtual machine	✓ Completed	fortipolicy-gsg
Initialize powering On	✓ Completed	test-datacenter
Remove virtual switch	✓ Completed	192.168.10.28
Remove port group	✓ Completed	192.168.10.28
Remove port group	✓ Completed	192.168.10.28

14. In the *Hosts and Clusters* tab, select your new VM and click *Launch Web Console*.



Guest OS: Ubuntu Linux (64-bit)
Compatibility: ESXi 5.1 and later (VM version 9)
VMware Tools: Running, version:2147483647 (Guest Managed)
DNS Name: FortiPolicy-demo
IP Addresses: 172.17.134.6
Host: 192.168.10.34

15. Check that all processes have a status of *UP*.



```
fortipolicy-gsg

 7.2.0-build0015
     IP: 172.17.134.6
 Uptime: 00:10:34
   Load: 11.43  8.93  4.35


Process               Status      Memory Last Update
--------------------- ------ ----------- -----------
AnalyticsStore        [ UP ]     6253.70 10 mins
AnalyticsVisualizer   [ UP ]      411.15 10 mins
ConfigMgr             [ UP ]      348.00 10 mins
ContainerSync         [ UP ]       52.53 10 mins
EventMgr              [ UP ]      914.70 10 mins
Factory               [ UP ]      531.02 10 mins
FactoryImages         [ UP ]        3.09 10 mins
FaultArchiver         [ UP ]       57.51 10 mins
FortiFabric           [ UP ]       17.08 10 mins
FortiFlow             [ UP ]      541.92 10 mins
GraphDB               [ UP ]      829.95 10 mins
GraphMiner            [ UP ]     1524.21 10 mins
HealthMgr             [ UP ]       46.41 10 mins
IoA                   [ UP ]       61.49 10 mins
KeyMgr                [ UP ]       22.62 10 mins
```

Initial login

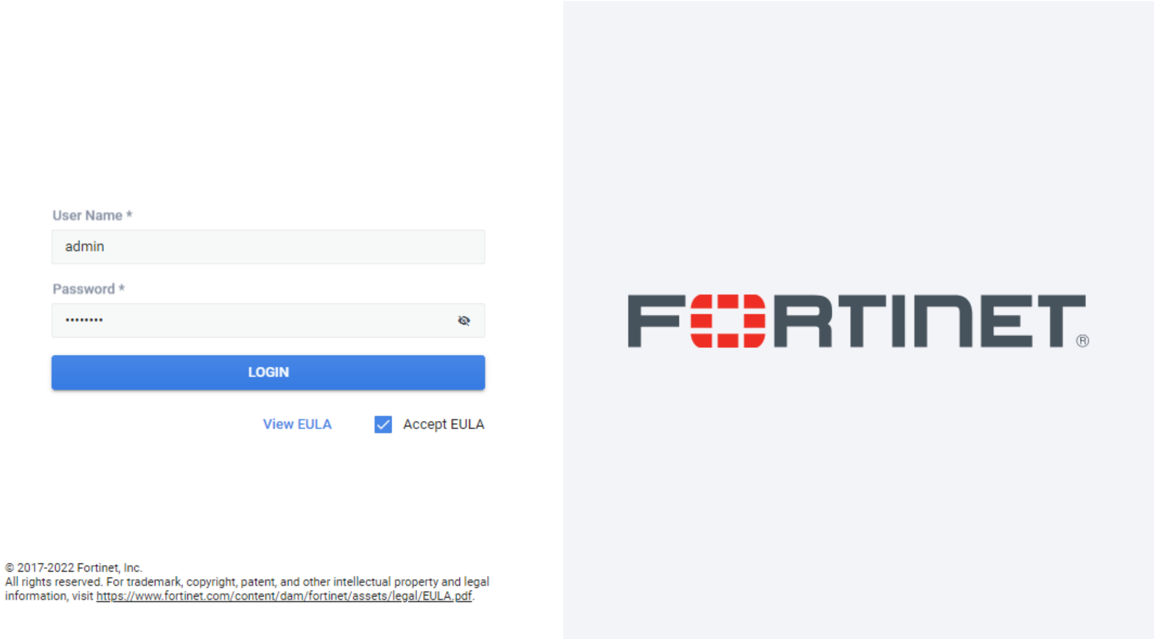
To launch the FortiPolicy console:

1. Enter the IP address in the browser address bar.

   The IP address was defined in Step 9.

   Fortinet recommends using Google Chrome.

2. In the User Name field, enter `admin`.
3. In the Password field, enter `fortinet`.
4. Select the *Accept EULA* checkbox.



User Name *: admin

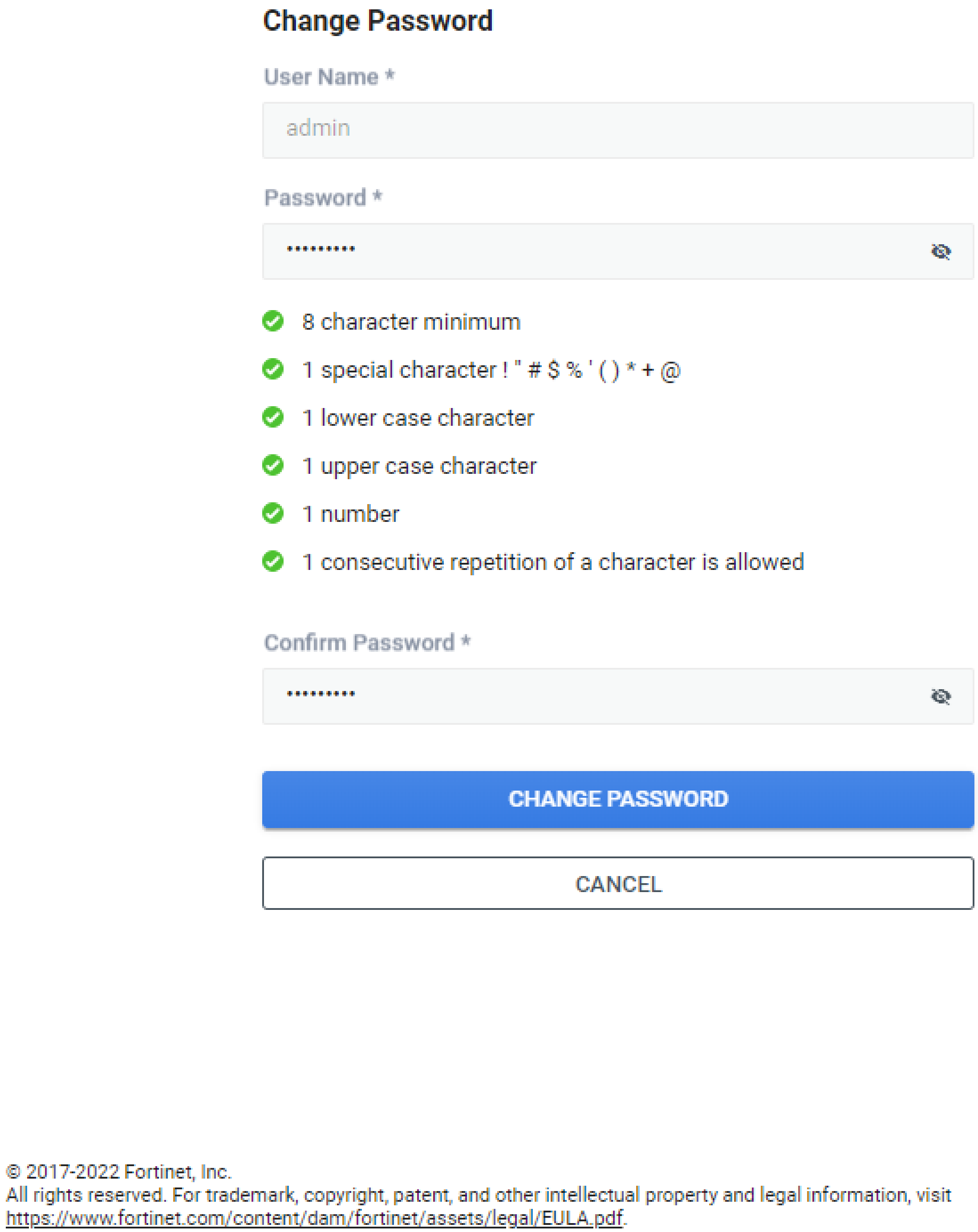
Password *: ••••••••

☑ Accept EULA

© 2017-2022 Fortinet, Inc.
All rights reserved. For trademark, copyright, patent, and other intellectual property and legal information, visit https://www.fortinet.com/content/dam/fortinet/assets/legal/EULA.pdf.

5. Click *LOGIN*.

6. Enter a new password and then enter the password a second time to confirm it.



Change Password

User Name *

admin

Password *

•••••••••

- ✓ 8 character minimum
- ✓ 1 special character ! " # $ % ' ( ) * + @
- ✓ 1 lower case character
- ✓ 1 upper case character
- ✓ 1 number
- ✓ 1 consecutive repetition of a character is allowed

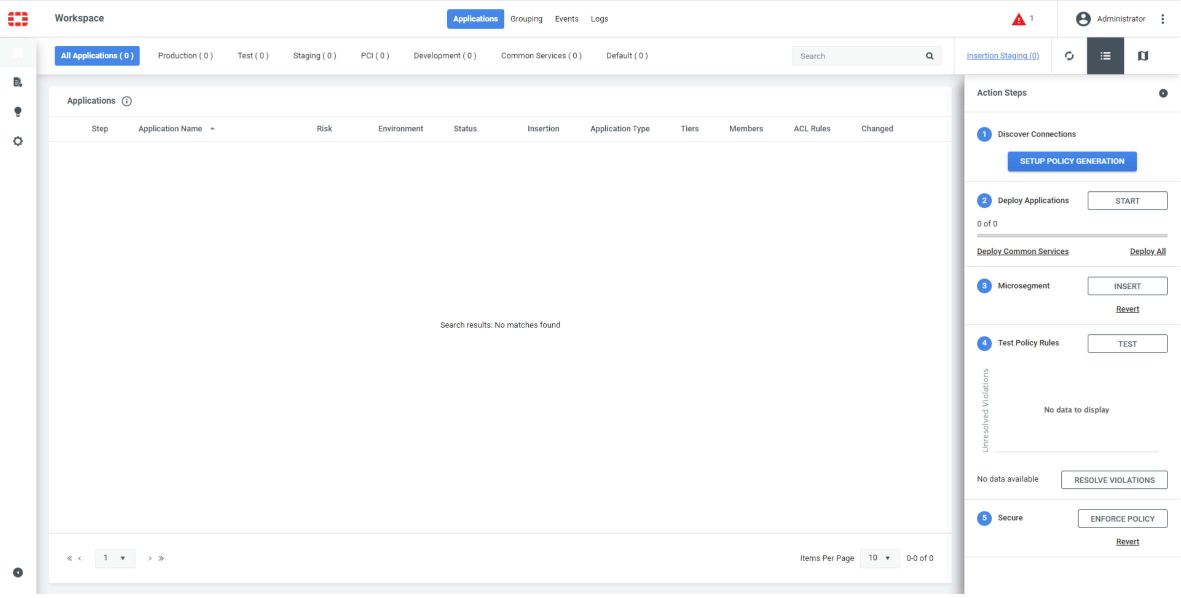
Confirm Password *

•••••••••

© 2017-2022 Fortinet, Inc.
All rights reserved. For trademark, copyright, patent, and other intellectual property and legal information, visit https://www.fortinet.com/content/dam/fortinet/assets/legal/EULA.pdf.

7. Click *CHANGE PASSWORD*.
8. In the *User Name* field, enter `admin`.
9. In the *Password* field, enter your new password.

10. Click *LOGIN*.



Search results: No matches found

After logging in, go to *Configuration* > *Users* and click the plus sign in the upper right corner to create a new user with the GlobalAdministrator role. After creating the new user, note the new credentials before you delete the `admin` user.

If you forget the new credentials, you will have to uninstall FortiPolicy and then re-install it.

Configuring FortiPolicy

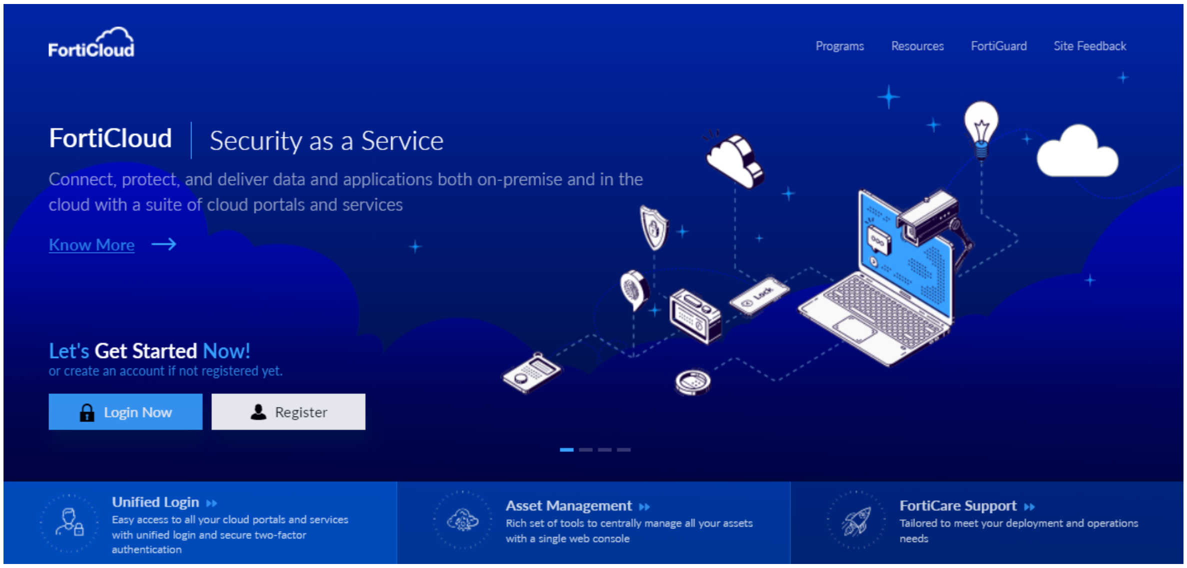
To configure FortiPolicy, complete the following procedures:

1. Importing the FortiPolicy license file on page 32
2. Creating a fabric connector on page 36
3. Configuring FortiPolicy data planes on page 44
4. Setting up Policy Generation on page 47

Importing the FortiPolicy license file

To import the FortiPolicy license file:

1. Go to FortiCloud and create a new account or log in with an existing account.



FortiCloud | Security as a Service

Connect, protect, and deliver data and applications both on-premise and in the cloud with a suite of cloud portals and services

Let's Get Started Now!

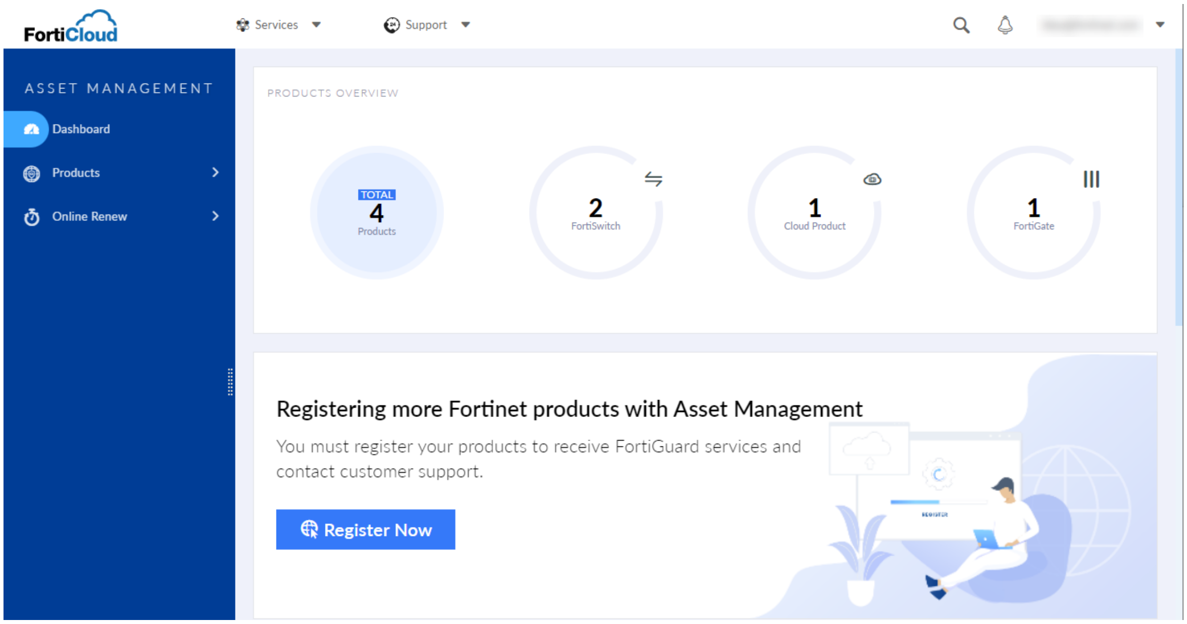
or create an account if not registered yet.

Unified Login: Easy access to all your cloud portals and services with unified login and secure two-factor authentication

Asset Management: Rich set of tools to centrally manage all your assets with a single web console

FortiCare Support: Tailored to meet your deployment and operations needs

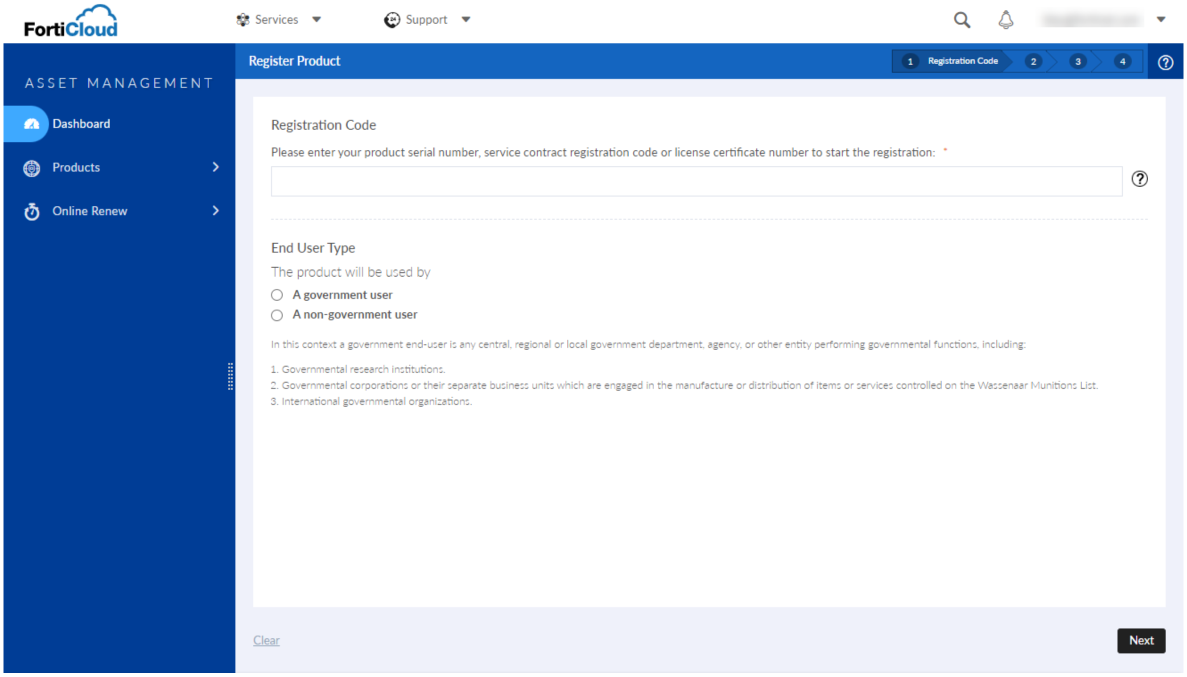
2. Go to *Asset Management* and click *Register Now* to start the registration process.



Registering more Fortinet products with Asset Management

You must register your products to receive FortiGuard services and contact customer support.

3. In the *Registration Code* field, enter the FortiPolicy UUID.



Registration Code

Please enter your product serial number, service contract registration code or license certificate number to start the registration: *

End User Type

The product will be used by

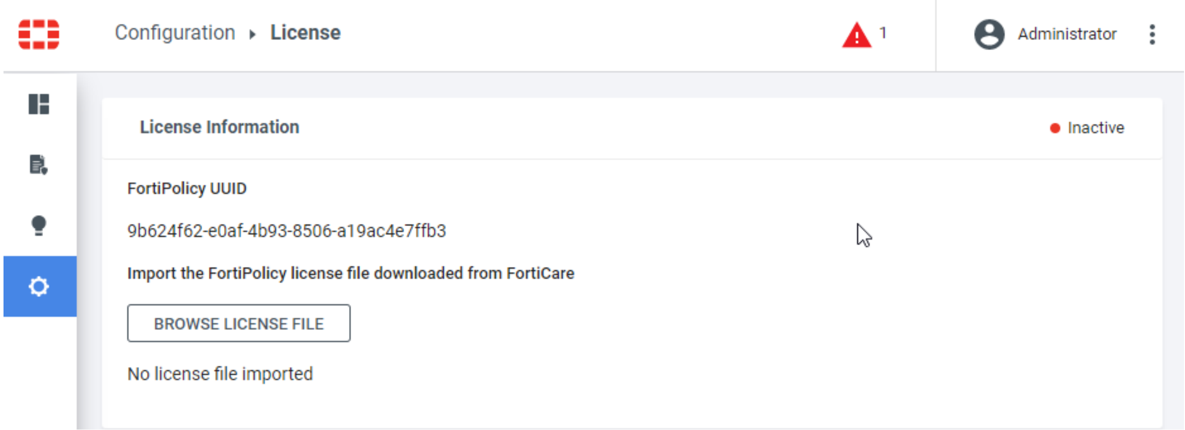
○ A government user

○ A non-government user

In this context a government end-user is any central, regional or local government department, agency, or other entity performing governmental functions, including:

1. Governmental research institutions.
2. Governmental corporations or their separate business units which are engaged in the manufacture or distribution of items or services controlled on the Wassenaar Munitions List.
3. International governmental organizations.

The FortiPolicy UUID is located in the *Configuration* > *License* page in FortiPolicy.



License Information ● Inactive

FortiPolicy UUID

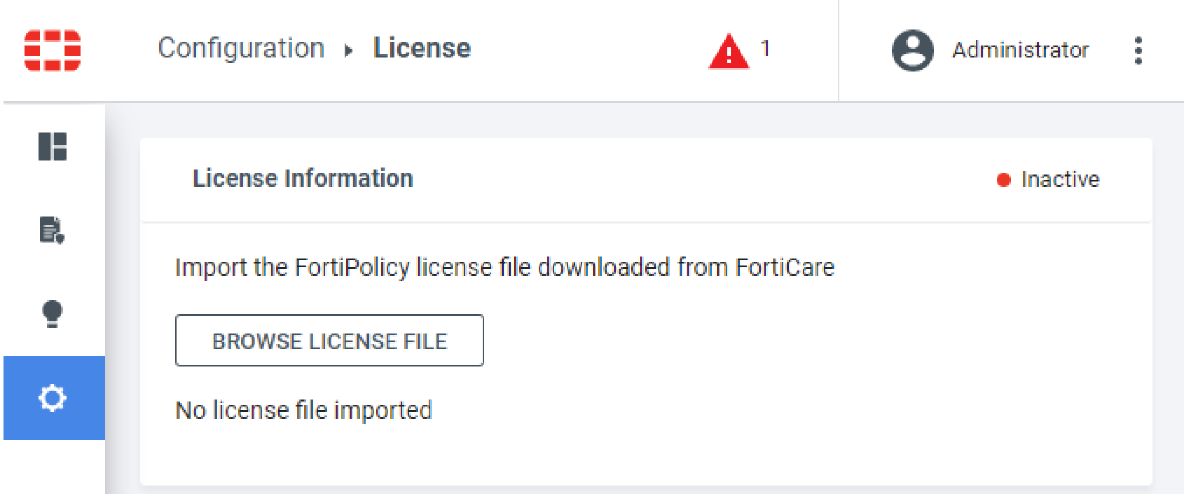
9b624f62-e0af-4b93-8506-a19ac4e7ffb3

Import the FortiPolicy license file downloaded from FortiCare

No license file imported

4. After you complete the registration process, go to *Products* > *Product List* in FortiCloud, click on the FortiPolicy serial number, and click *License File Download* to download your license file.

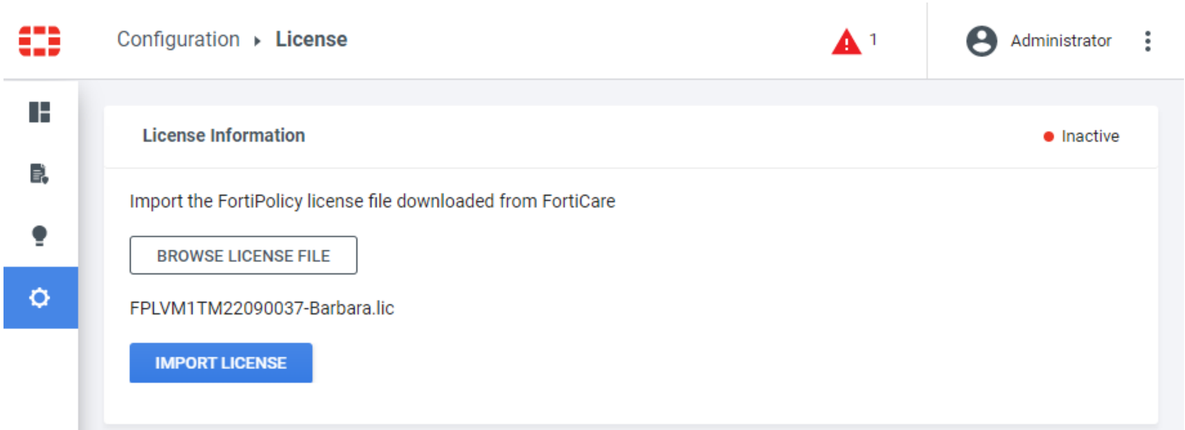
5. In FortiPolicy, go to *Configuration* > *License* and click *BROWSE LICENSE FILE*.



Import the FortiPolicy license file downloaded from FortiCare

No license file imported

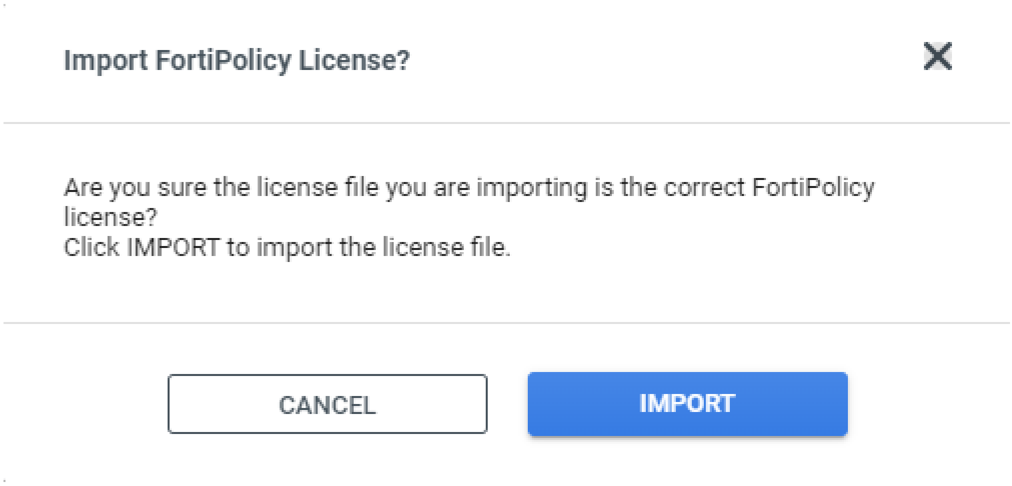
6. Select your FortiPolicy license file.



Import the FortiPolicy license file downloaded from FortiCare

FPLVM1TM22090037-Barbara.lic

7. Click *IMPORT LICENSE*.

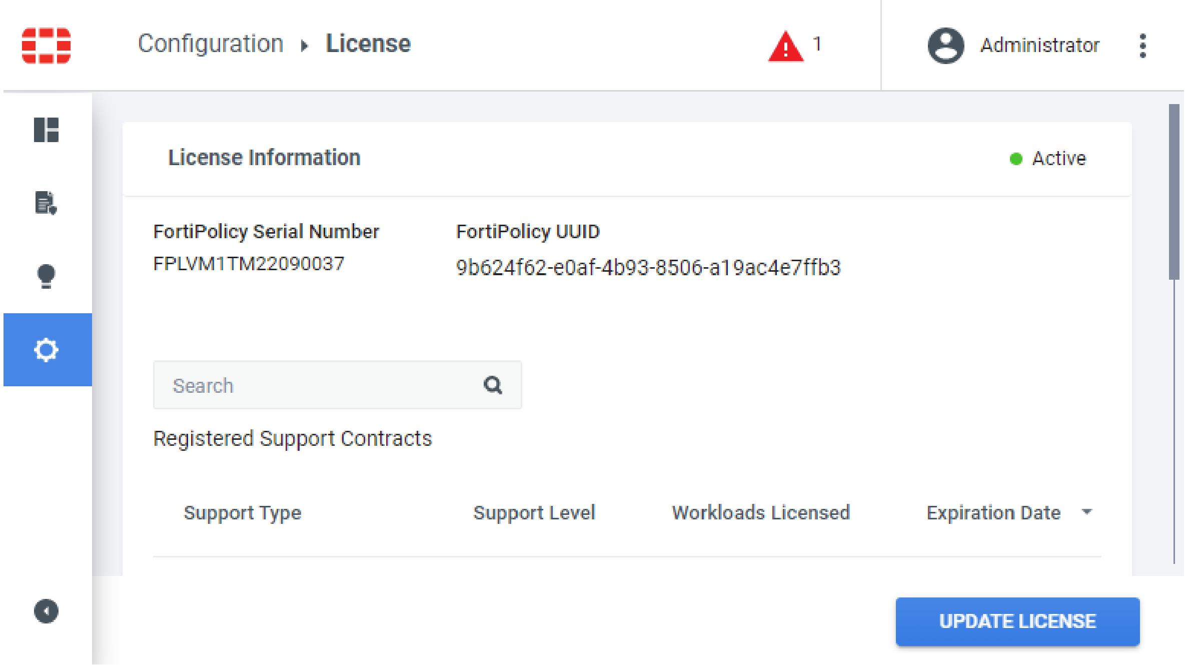


Import FortiPolicy License?

Are you sure the license file you are importing is the correct FortiPolicy license?
Click IMPORT to import the license file.

8. Click *IMPORT*.
9. Check that the status of the license is *Active*.

The *Registered Support Contracts* area is updated with all contracts that have been assigned to your license.



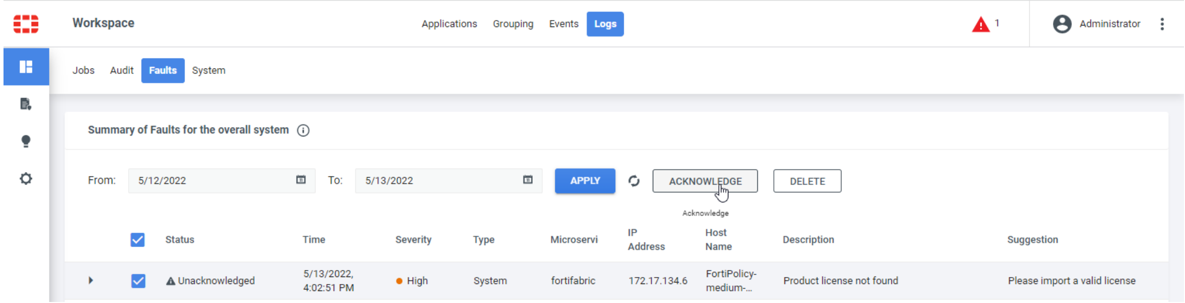
FortiPolicy Serial Number
FPLVM1TM22090037

FortiPolicy UUID
9b624f62-e0af-4b93-8506-a19ac4e7ffb3

Registered Support Contracts

Support Type	Support Level	Workloads Licensed	Expiration Date

If you see a red triangle on the right side of the header bar, click on it to see the system log message under *Workspace* > *Logs* > *Faults*. You can acknowledge the license fault and then ignore it.



Summary of Faults for the overall system

From: 5/12/2022 To: 5/13/2022

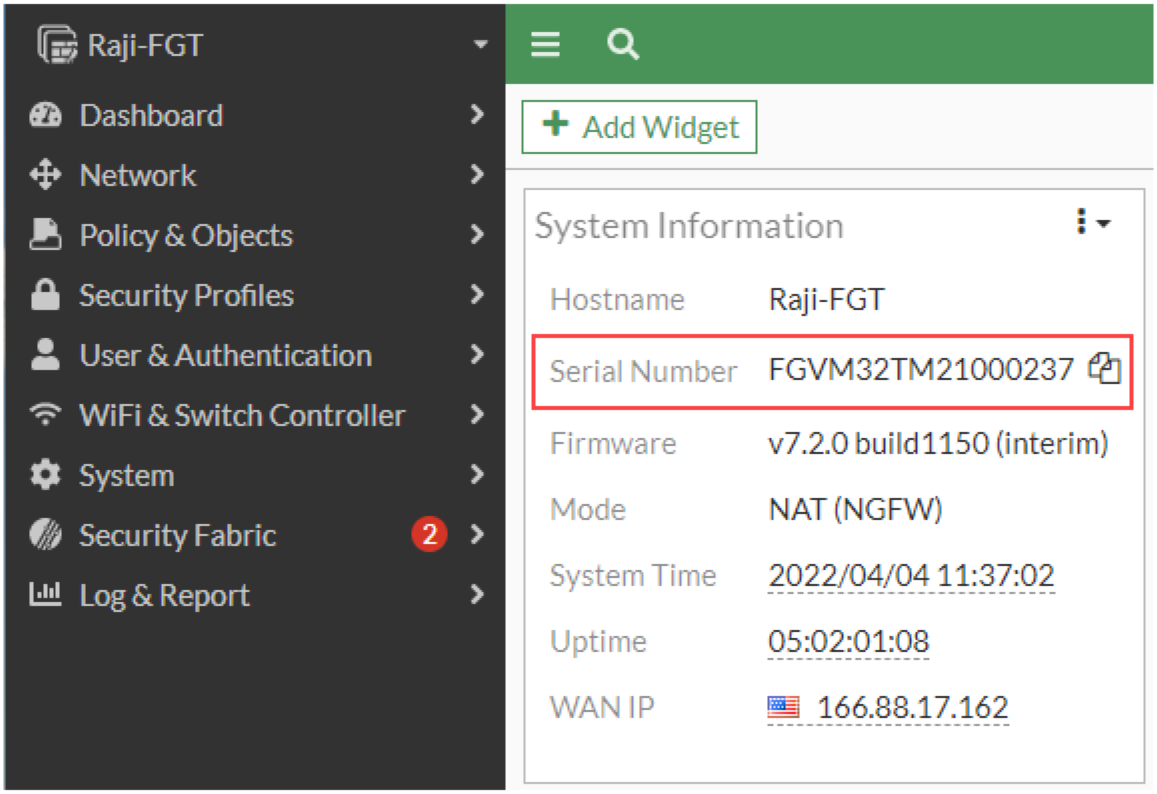
☑	Status	Time	Severity	Type	Microservi	IP Address	Host Name	Description	Suggestion
☑	Unacknowledged	5/13/2022, 4:02:51 PM	● High	System	fortifabric	172.17.134.6	FortiPolicy-medium-...	Product license not found	Please import a valid license

Creating a fabric connector

A fabric connector connects FortiPolicy to the root FortiGate device and everything connected to the root FortiGate device.

To create a fabric connector:

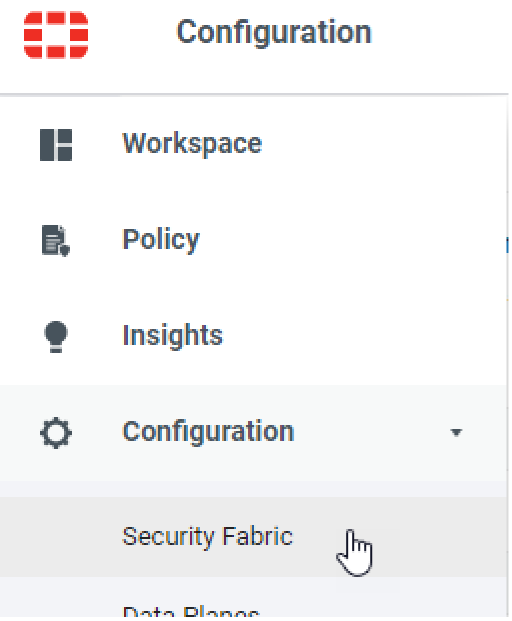
1. In the root FortiGate device, go to *Dashboard* > *Status* and copy the FortiGate serial number from the *System Information* widget.



System Information

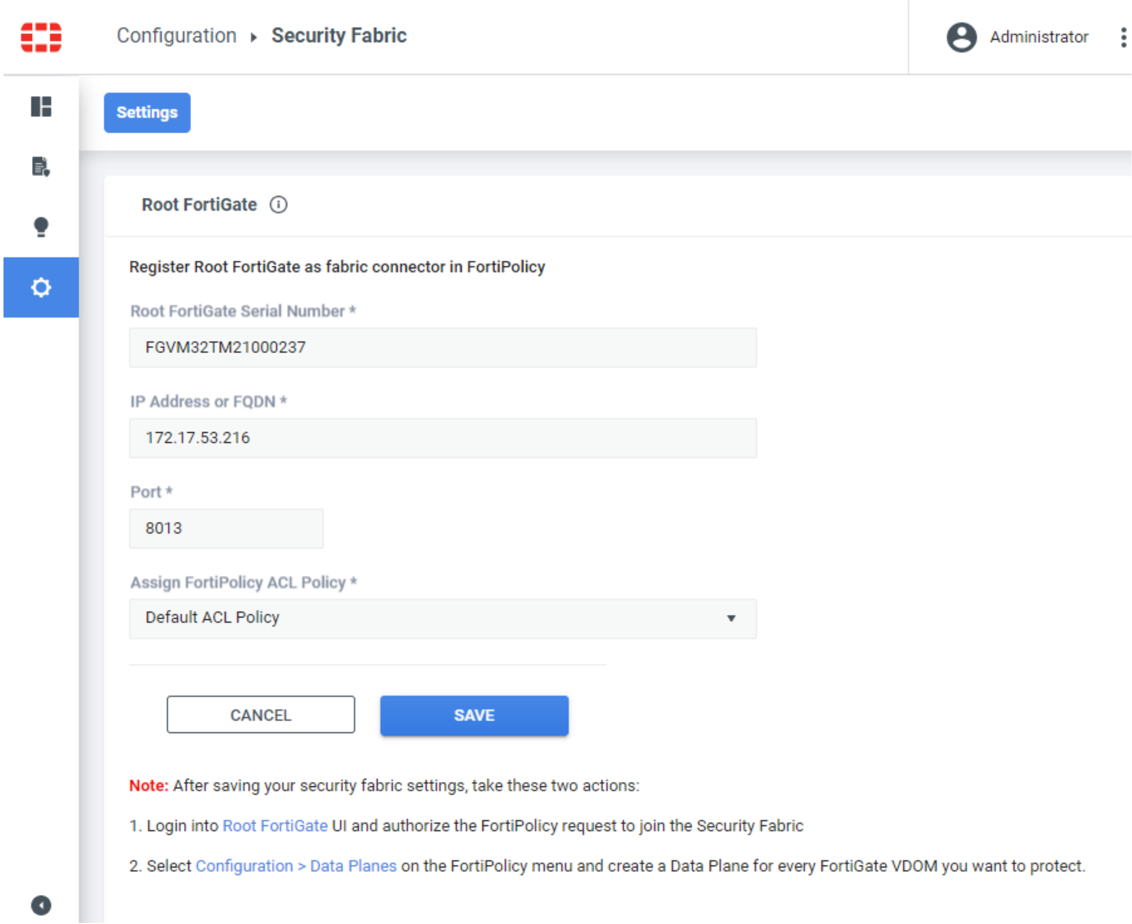
Hostname	Raji-FGT
Serial Number	FGVM32TM21000237
Firmware	v7.2.0 build1150 (interim)
Mode	NAT (NGFW)
System Time	2022/04/04 11:37:02
Uptime	05:02:01:08
WAN IP	166.88.17.162

2. In FortiPolicy, configure the Security Fabric.
   a. Go to *Configuration > Security Fabric*.



   b. In the *Root FortiGate Serial Number* field, enter the serial number for the root FortiGate device.
   c. In the *IP Address* field, enter the IP address of the root FortiGate device.
   d. By default, the *Port* field is set to `8013`.

e. In the *Assign FortiPolicy ACL Policy* dropdown list, select *Default ACL Policy*.



Register Root FortiGate as fabric connector in FortiPolicy

Root FortiGate Serial Number *: FGVM32TM21000237

IP Address or FQDN *: 172.17.53.216

Port *: 8013

Assign FortiPolicy ACL Policy *: Default ACL Policy

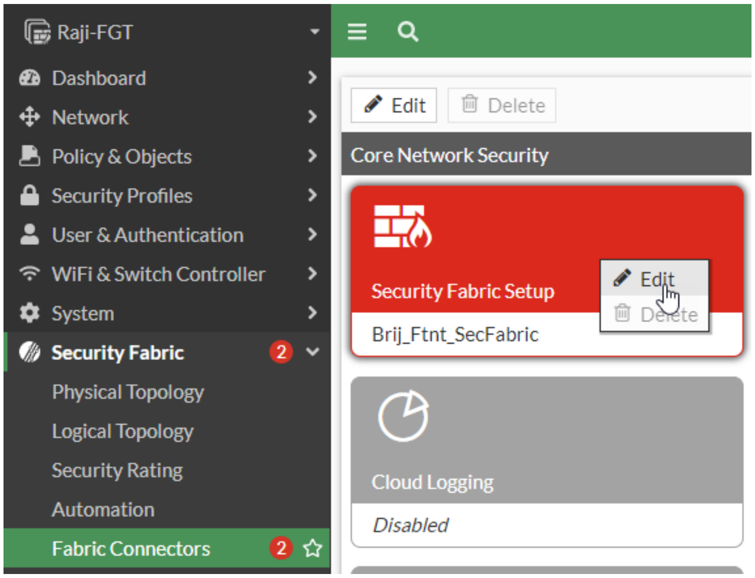
Note: After saving your security fabric settings, take these two actions:

1. Login into Root FortiGate UI and authorize the FortiPolicy request to join the Security Fabric

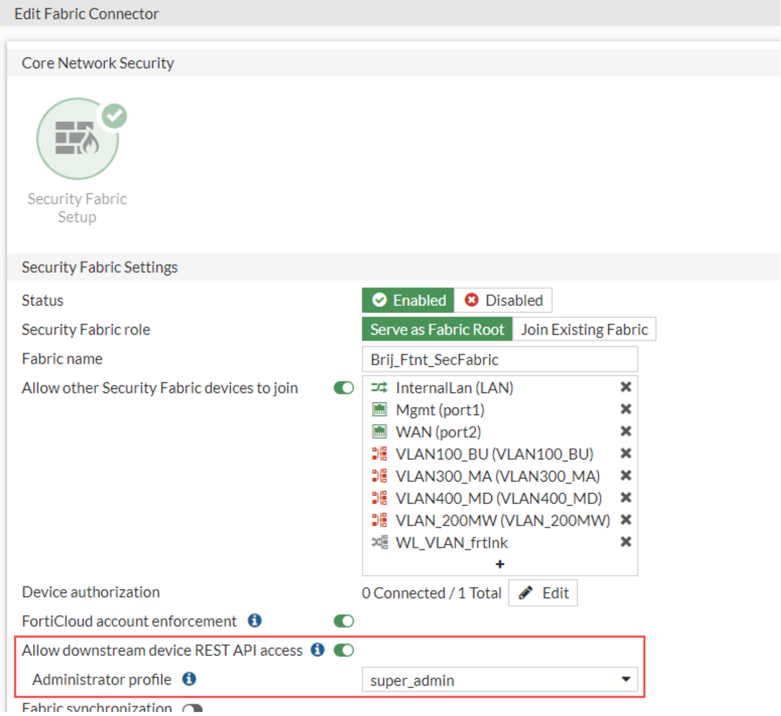
2. Select Configuration > Data Planes on the FortiPolicy menu and create a Data Plane for every FortiGate VDOM you want to protect.

f. Click *SAVE*.

3. Configure the settings in each FortiGate device (root FortiGate and child FortiGate devices) in the Security Fabric.
   a. Go to *Security Fabric > Fabric Connectors*, right-click *Security Fabric Setup*, and select *Edit*.



   b. Enable *Allow downstream device REST API Access*.
   c. From the *Administrator profile* dropdown list, select *super_admin*.

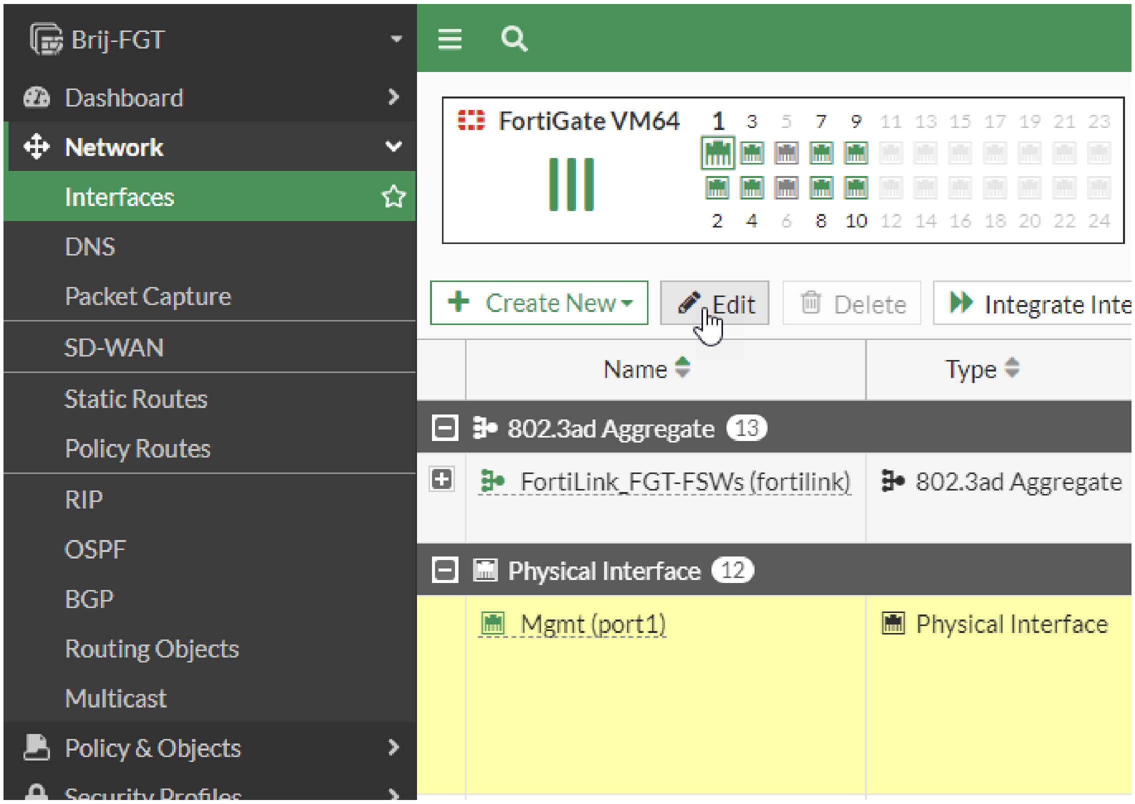


Security Fabric Settings

Status	Enabled / Disabled
Security Fabric role	Serve as Fabric Root / Join Existing Fabric
Fabric name	Brij_Ftnt_SecFabric
Allow other Security Fabric devices to join	InternalLan (LAN) Mgmt (port1) WAN (port2) VLAN100_BU (VLAN100_BU) VLAN300_MA (VLAN300_MA) VLAN400_MD (VLAN400_MD) VLAN_200MW (VLAN_200MW) WL_VLAN_frtlnk
Device authorization	0 Connected / 1 Total Edit
FortiCloud account enforcement	
Allow downstream device REST API access	
Administrator profile	super_admin
Fabric synchronization	

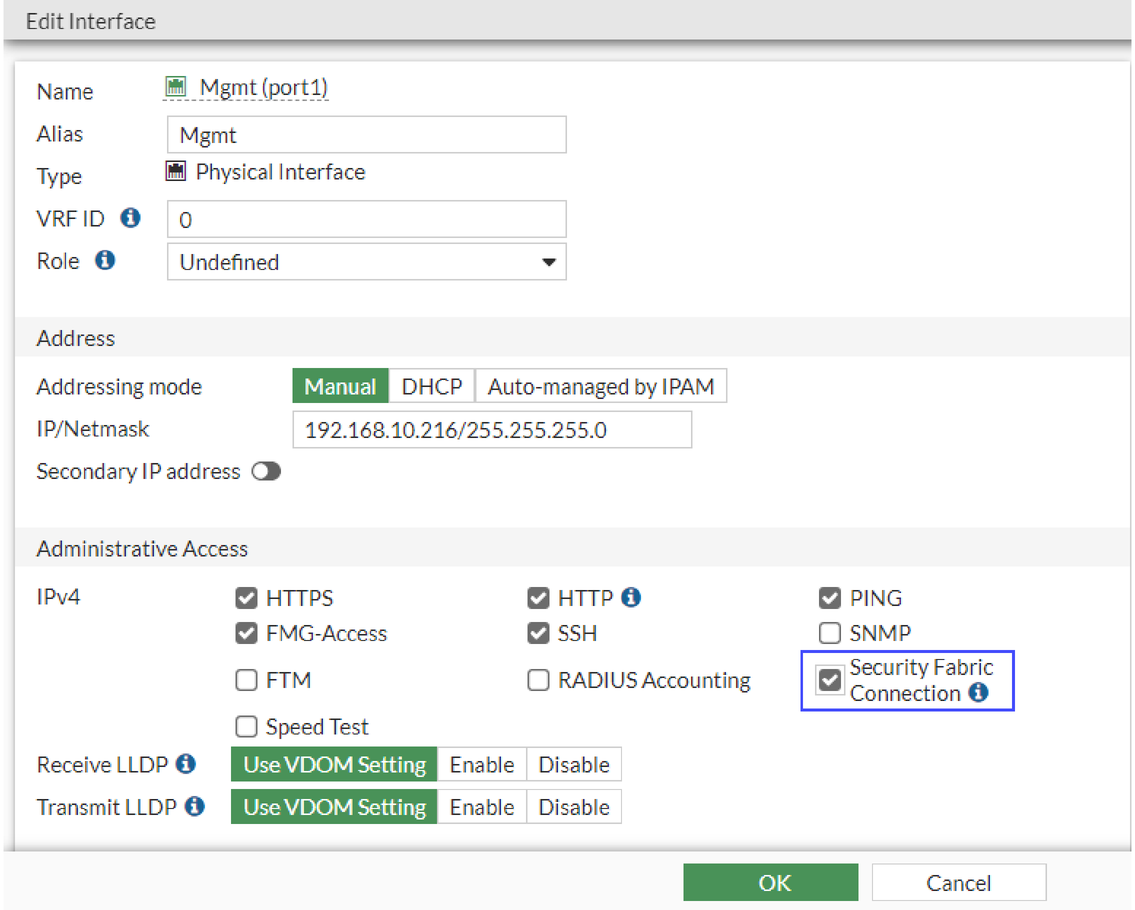
   d. Click *OK*.

4. In the root FortiGate device, configure the management port.
   a. Go to *Network* > *Interfaces*, select the *Mgmt* port, and click *Edit*.



Name	Type
802.3ad Aggregate 13	
FortiLink_FGT-FSWs (fortilink)	802.3ad Aggregate
Physical Interface 12	
Mgmt (port1)	Physical Interface

b. Select the *Security Fabric Connection* checkbox and then click *OK*.



Edit Interface

Name: Mgmt (port1)

Alias: Mgmt

Type: Physical Interface

VRF ID: 0

Role: Undefined

Address

Addressing mode: [✓ Manual] DHCP Auto-managed by IPAM

IP/Netmask: 192.168.10.216/255.255.255.0

Secondary IP address ○

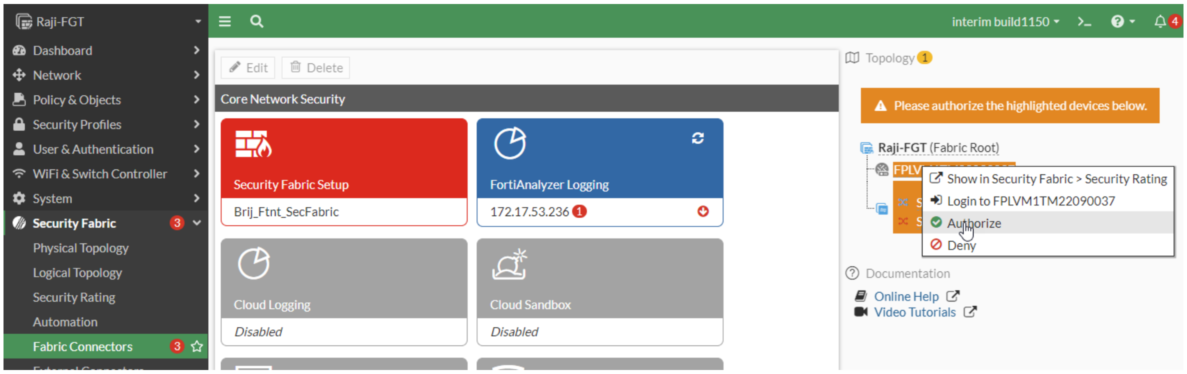
Administrative Access

IPv4:
☑ HTTPS ☑ HTTP ☑ PING
☑ FMG-Access ☑ SSH □ SNMP
□ FTM □ RADIUS Accounting ☑ Security Fabric Connection
□ Speed Test

Receive LLDP: [✓ Use VDOM Setting] Enable Disable

Transmit LLDP: [✓ Use VDOM Setting] Enable Disable

5. Go to *Security Fabric > Fabric Connectors*, click the highlighted FortiPolicy serial number, and select *Authorize*.



Core Network Security

Security Fabric Setup: Brij_Ftnt_SecFabric

FortiAnalyzer Logging: 172.17.53.236

Cloud Logging: *Disabled*

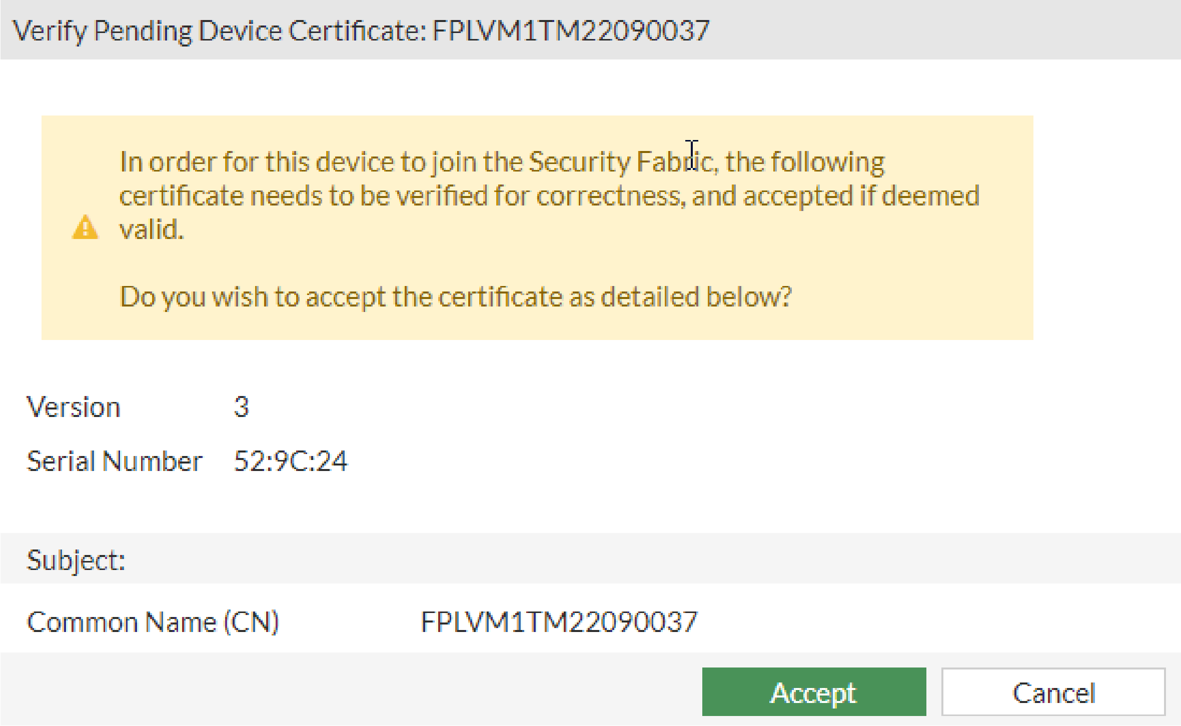
Cloud Sandbox: *Disabled*

Please authorize the highlighted devices below.

Raji-FGT (Fabric Root)

FPLV

6. In the *Verify Pending Device Certificate* pane, click *Accept*.



Verify Pending Device Certificate: FPLVM1TM22090037

In order for this device to join the Security Fabric, the following certificate needs to be verified for correctness, and accepted if deemed valid.

Do you wish to accept the certificate as detailed below?

Version	3
Serial Number	52:9C:24

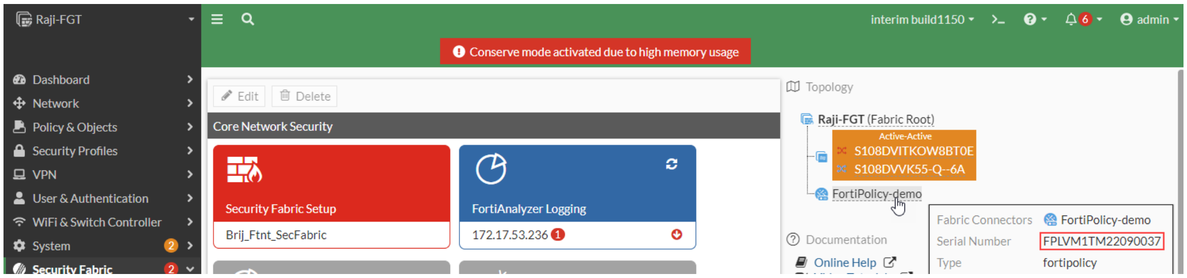
Subject:

Common Name (CN)	FPLVM1TM22090037

7. In the FortiOS CLI, click the *CLI Console* button at the top of the window and then enter the following commands on each FortiGate device that is part of the Security Fabric (root FortiGate and child FortiGate devices):

```
config system csf
   config fabric-connector
      edit <FortiPolicy_serial_number>
         set configuration-write-access enable
         set accprofile super_admin
      next
   end
end
```

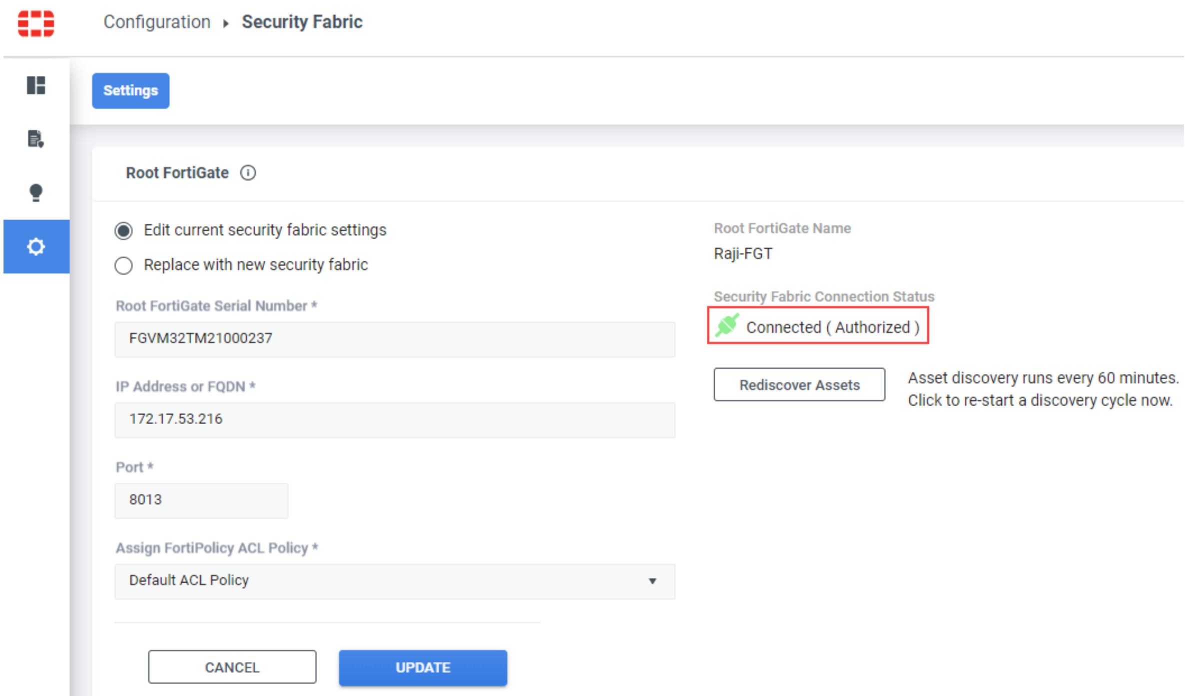
To find the FortiPolicy serial number, go to *Security Fabric > Fabric Connectors* and hover above the FortiPolicy device that you authorized, as shown in the following figure.



Conserve mode activated due to high memory usage

Fabric Connectors	FortiPolicy-demo
Serial Number	FPLVM1TM22090037
Type	fortipolicy

8. FortiPolicy now displays the status of the connector as *Connected (Authorized)*.



Root FortiGate ⓘ

● Edit current security fabric settings

○ Replace with new security fabric

Root FortiGate Serial Number *: FGVM32TM21000237

IP Address or FQDN *: 172.17.53.216

Port *: 8013

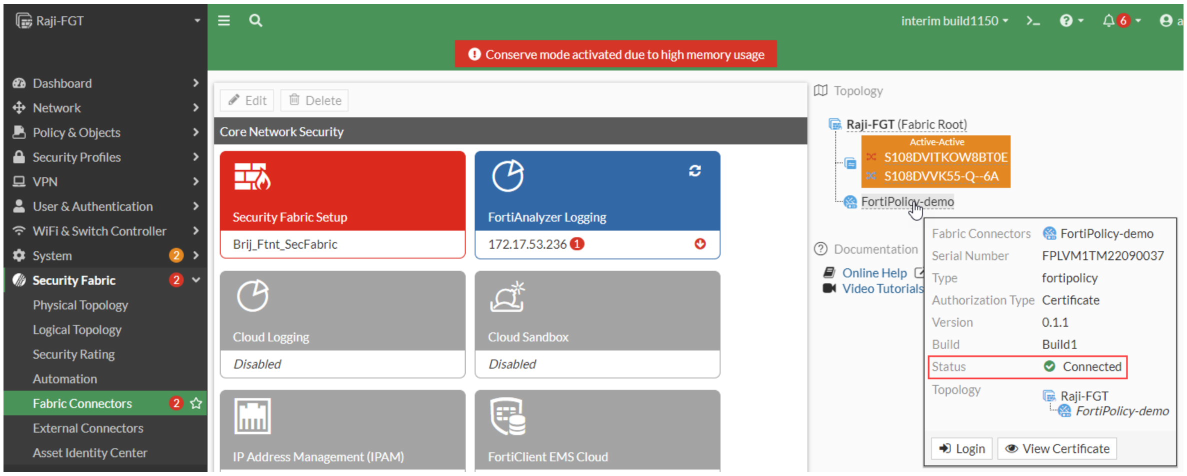
Assign FortiPolicy ACL Policy *: Default ACL Policy

Root FortiGate Name: Raji-FGT

Security Fabric Connection Status: Connected (Authorized)

Asset discovery runs every 60 minutes. Click to re-start a discovery cycle now.

9. In FortiOS, the status of the fabric connector is *Connected*.



Conserve mode activated due to high memory usage

Security Fabric Setup: Brij_Ftnt_SecFabric

FortiAnalyzer Logging: 172.17.53.236

Cloud Logging: *Disabled*

Cloud Sandbox: *Disabled*

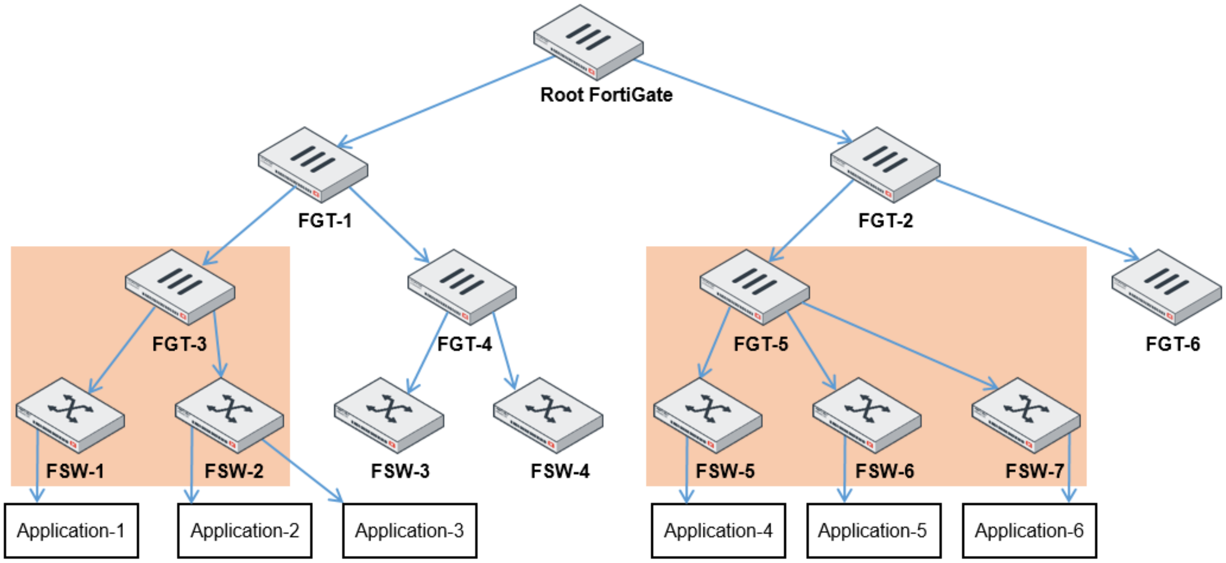
Raji-FGT (Fabric Root)
Active-Active
S108DVITKOW8BT0E
S108DVVK55-Q--6A
FortiPolicy-demo

Fabric Connectors	FortiPolicy-demo
Serial Number	FPLVM1TM22090037
Type	fortipolicy
Authorization Type	Certificate
Version	0.1.1
Build	Build1
Status	Connected
Topology	Raji-FGT *FortiPolicy-demo*

Configuring FortiPolicy data planes

You need to create a FortiPolicy data plane for each FortiGate device connected to application workloads that need to be secured. The workloads might be connected directly to the FortiGate device or might be connected to FortiSwitch units that are directly connected to the FortiGate device.

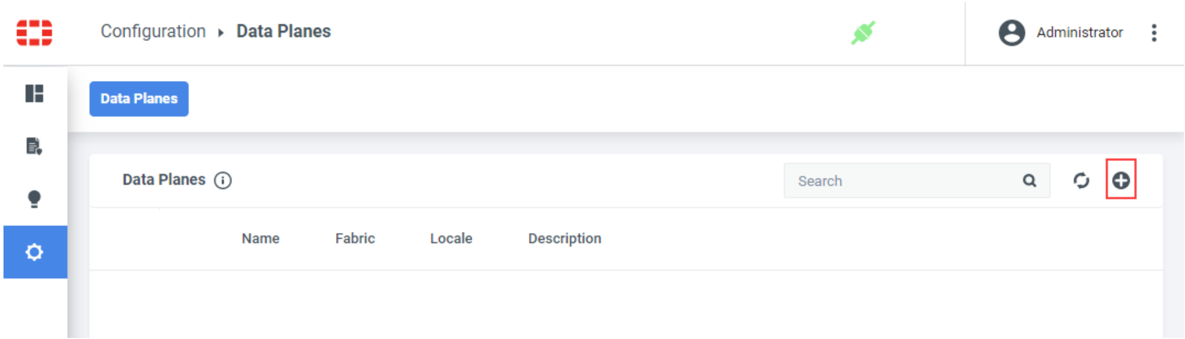
For example, in the following topology, you would create a data plane for FGT-3 to secure Application-1, Application-2, and Application-3. You would create a second data plane for FGT-5 to secure Application-4, Application-5, and Application-6.



The data planes determine which workloads Policy Generation will analyze. When you select the FortiGate device for a data plane, Policy Generation will examine the traffic logs from that FortiGate device and the netflows from the FortiSwitch units that are directly wired to the FortiGate device. Policy Generation will analyze the traffic for the workloads connected directly to the FortiGate device and FortiSwitch units.

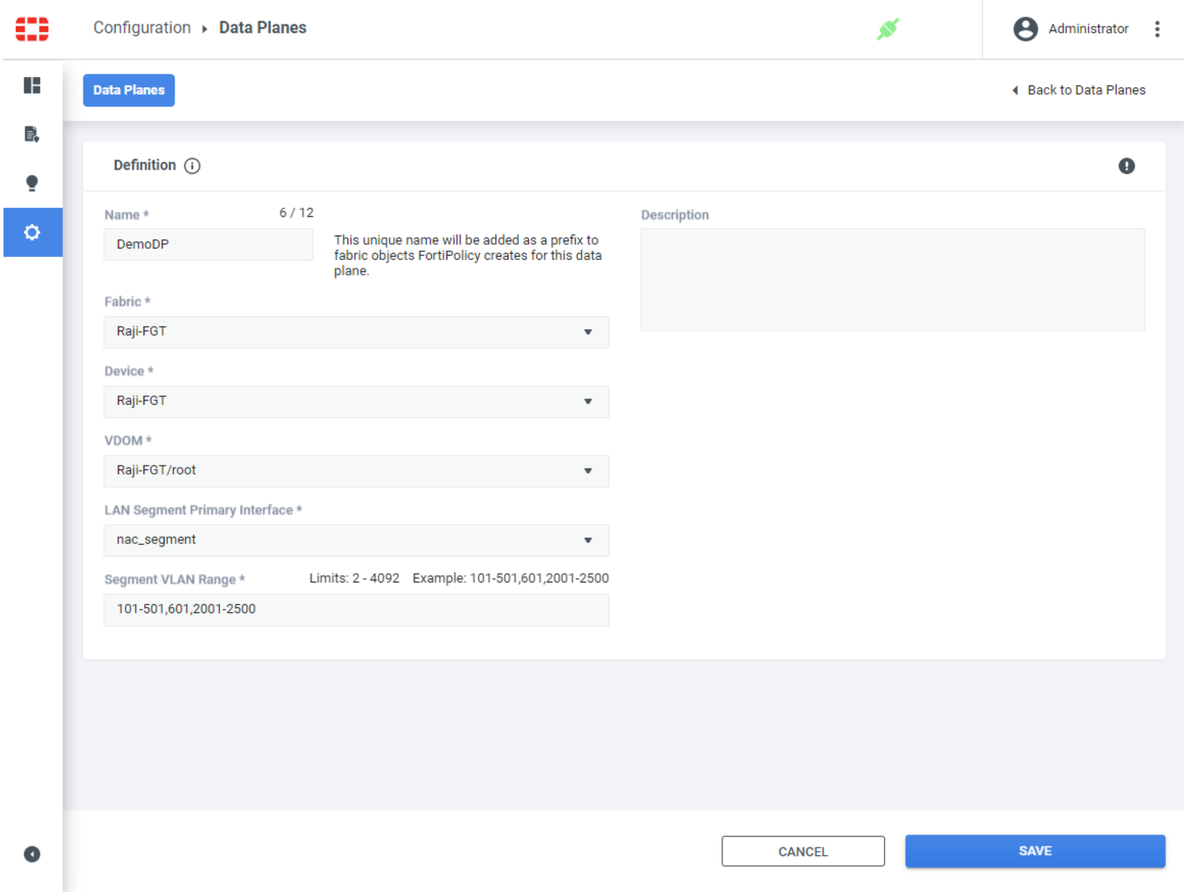
To create a data plane:

1. Go to *Configuration* > *Data Planes*.
2. Click the plus sign on the upper right corner of the *Data Planes* page.



3. In the *Name* field, enter a unique name for the new data plane.

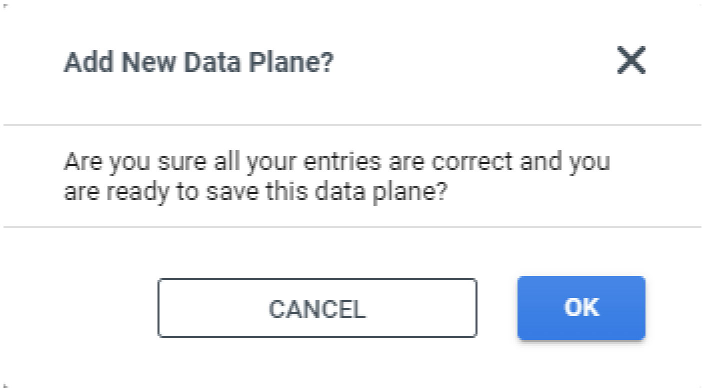
4. From the *Fabric* dropdown list, select the fabric connector that you created.
5. From the *Device* dropdown list, select the root FortiGate device.
6. From the *VDOM* dropdown list, select the VDOM.
7. From the *LAN Segment Primary Interface* dropdown list, select the LAN segment that you want to use as the primary interface. The default LAN segment is `nac_segment`.
8. In the *Segment VLAN Range* field, enter a range of VLAN IDs. If you are going to microsegment the workloads, each workload requires a separate VLAN.



Name * 6 / 12
DemoDP
This unique name will be added as a prefix to fabric objects FortiPolicy creates for this data plane.
Description
Fabric *
Raji-FGT
Device *
Raji-FGT
VDOM *
Raji-FGT/root
LAN Segment Primary Interface *
nac_segment
Segment VLAN Range * Limits: 2 - 4092 Example: 101-501,601,2001-2500
101-501,601,2001-2500

9. Click *SAVE*.

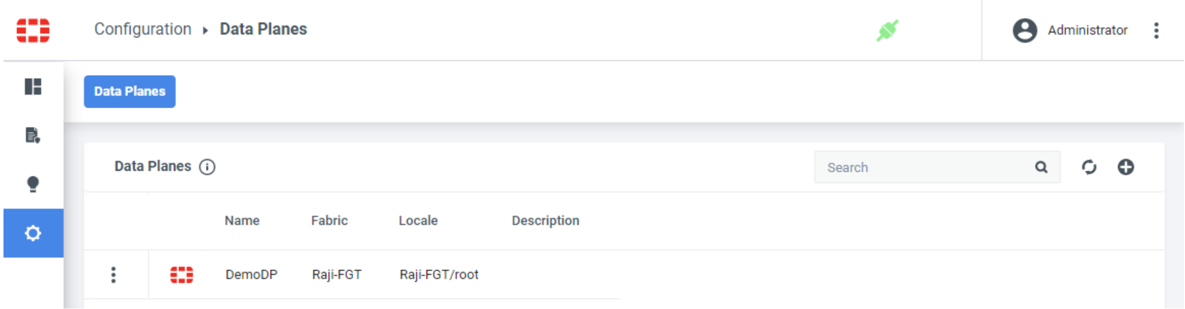
10. In the *Add New Data Plane?* dialog, click *OK*.



Add New Data Plane?

Are you sure all your entries are correct and you are ready to save this data plane?

The new data plane is listed in the *Data Planes* page.



Name	Fabric	Locale	Description
DemoDP	Raji-FGT	Raji-FGT/root	

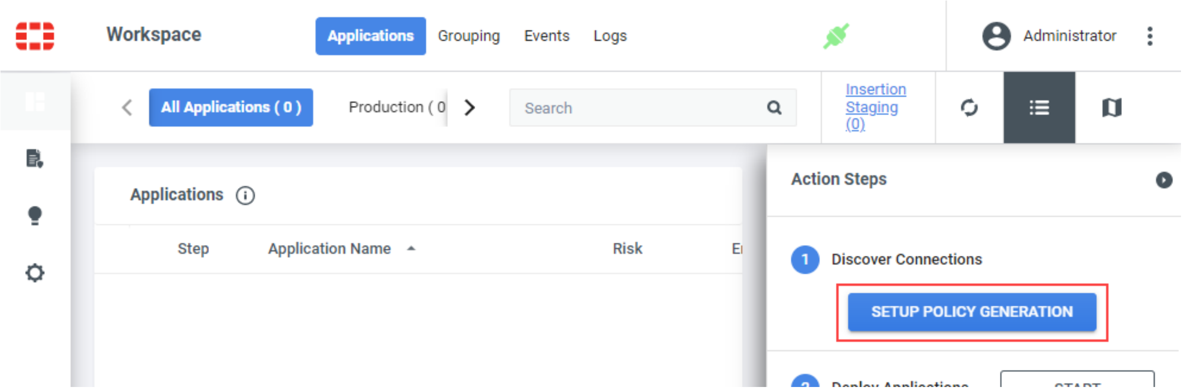
11. Repeat steps 2-10 for each FortiGate device connected to application workloads that need to be secured.

Setting up Policy Generation

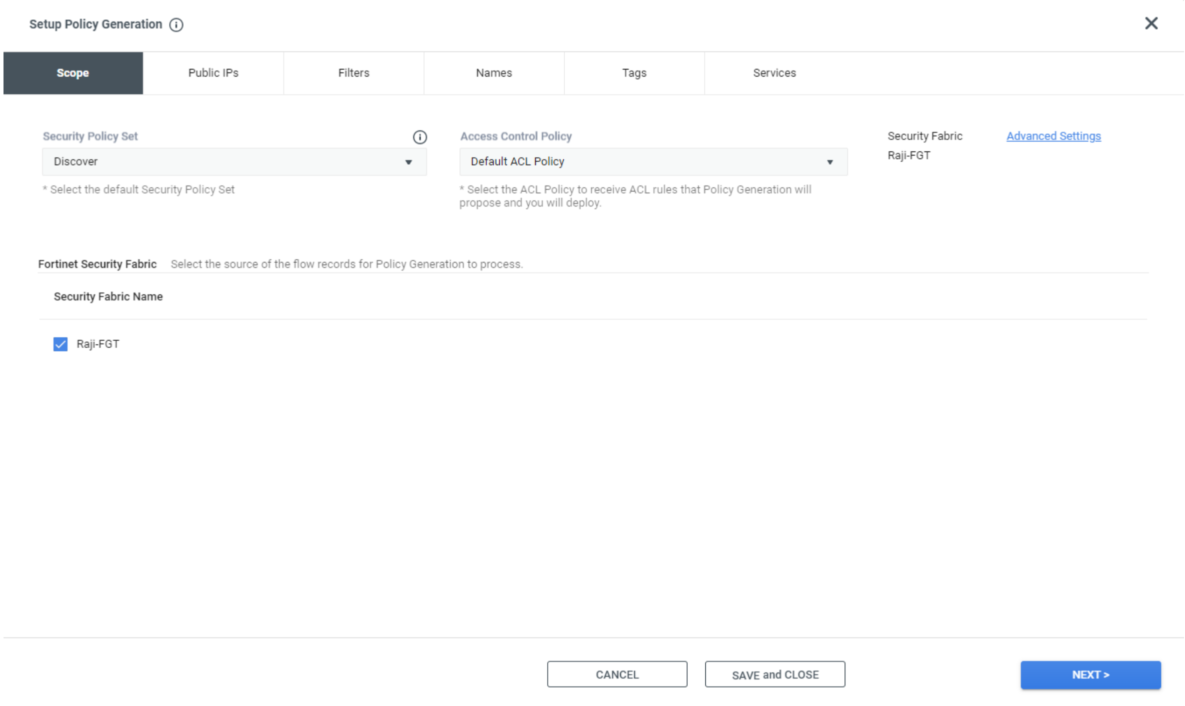
Automated Policy Generation provides the automated discovery of connections, tiers, applications, and network services.

To set up Policy Generation:

1. In FortiPolicy, go to *Workspace* > *Applications*.
2. In the *Action Steps* pane, click *SETUP POLICY GENERATION*.



3. For the *Security Policy Set* dropdown list, keep the default setting of *Discover*.
4. From the *Access Control Policy* dropdown list, select *Default ACL Policy*.
5. Select the checkbox for the Fortinet Security Fabric.



Security Policy Set: Discover

* Select the default Security Policy Set

Access Control Policy: Default ACL Policy

* Select the ACL Policy to receive ACL rules that Policy Generation will propose and you will deploy.

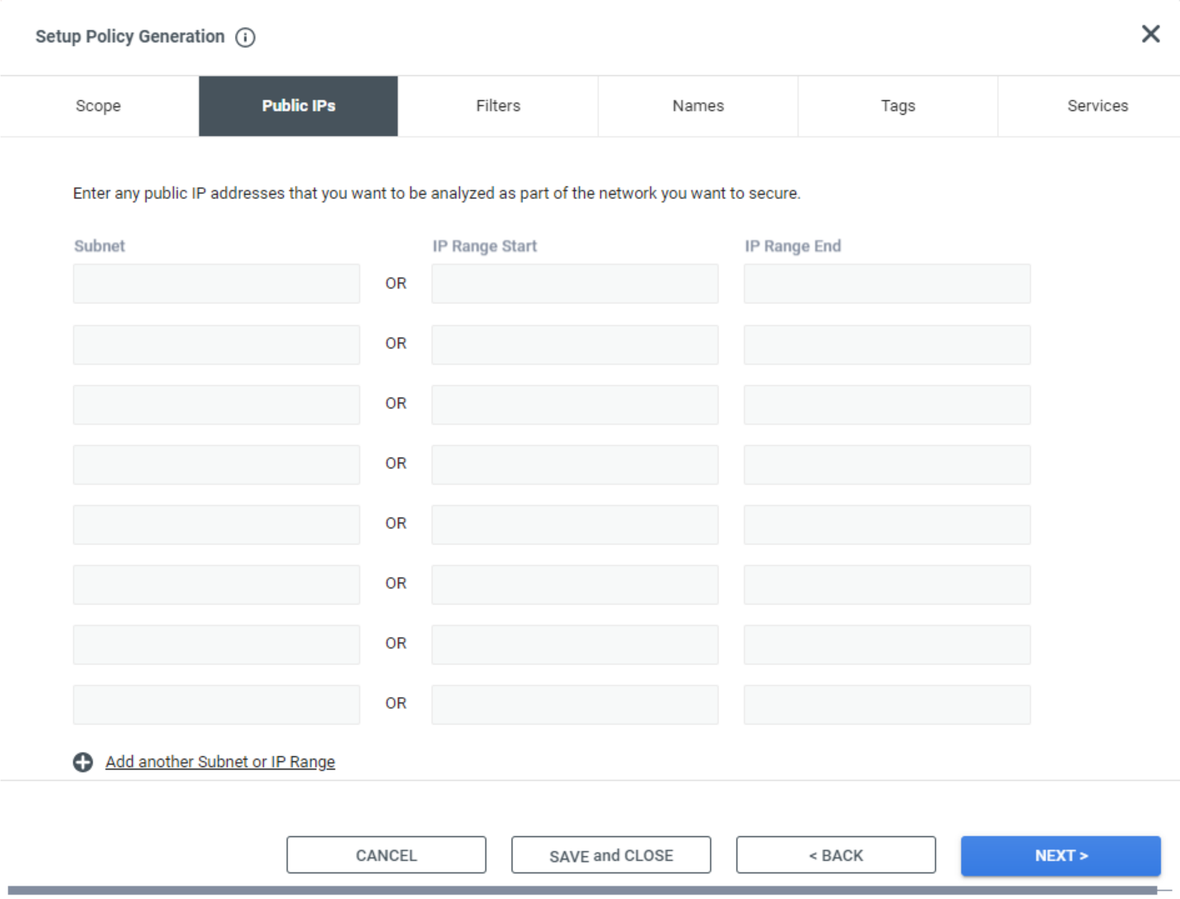
Security Fabric: Raji-FGT

Fortinet Security Fabric — Select the source of the flow records for Policy Generation to process.

Security Fabric Name
☑ Raji-FGT

6. Click *Next*.

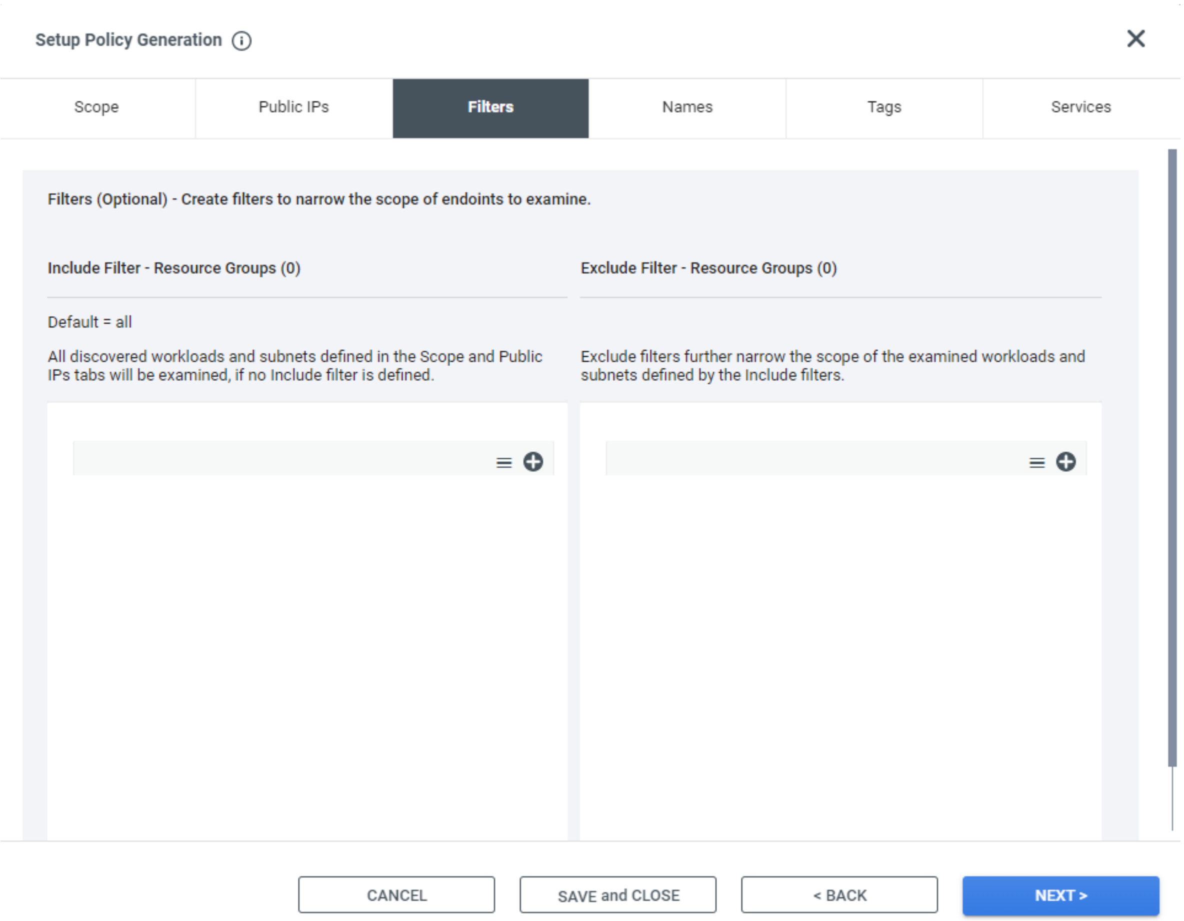
7. Enter any public IP addresses that you want to be analyzed as part of the network you are securing.



Enter any public IP addresses that you want to be analyzed as part of the network you want to secure.

8. Click *Next*.

9. If you do not want all workloads and subnets defined in the *Scope* and *Public IPs* tabs to be examined, create filters for which workloads and subnets to include and exclude.



Setup Policy Generation

Filters (Optional) - Create filters to narrow the scope of endoints to examine.

Include Filter - Resource Groups (0)

Default = all

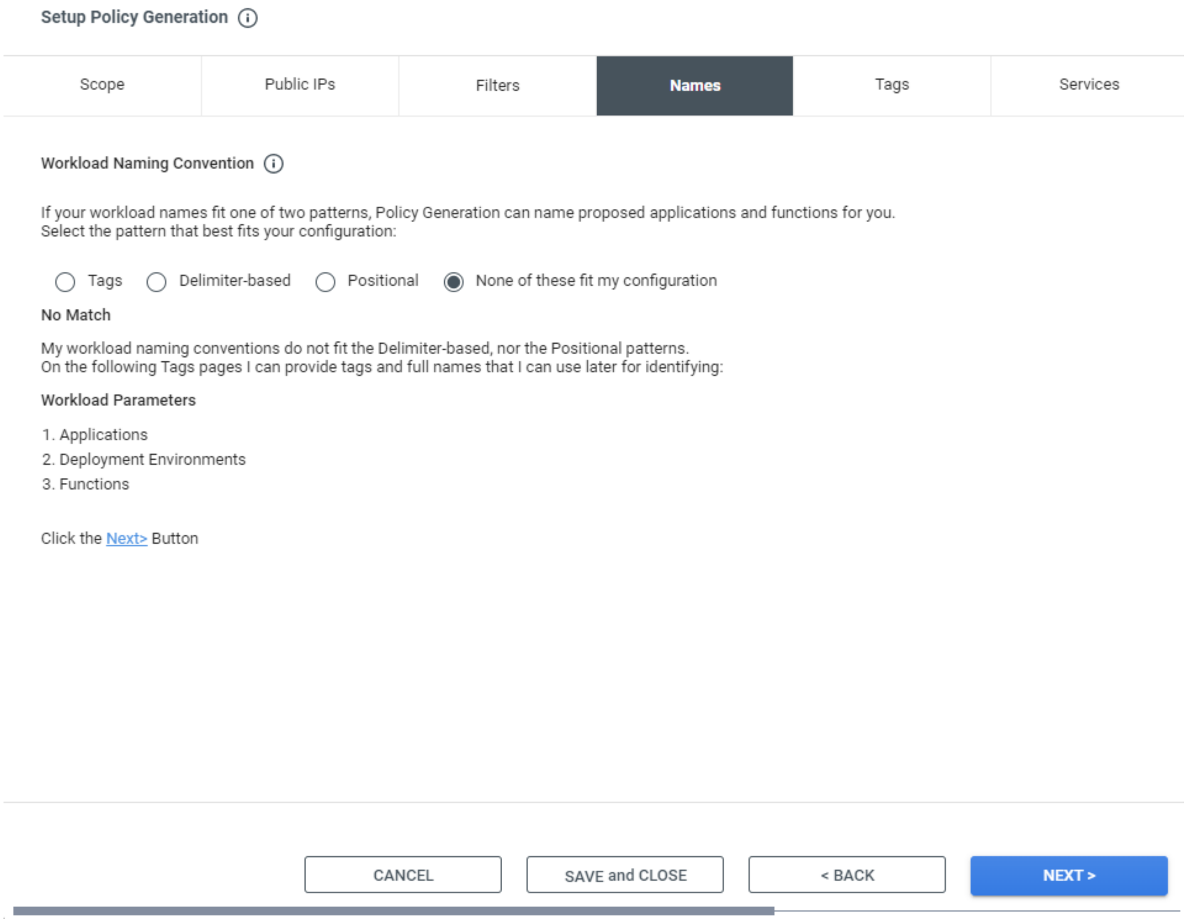
All discovered workloads and subnets defined in the Scope and Public IPs tabs will be examined, if no Include filter is defined.

Exclude Filter - Resource Groups (0)

Exclude filters further narrow the scope of the examined workloads and subnets defined by the Include filters.

10. Click *Next*.

11. Policy Generation will automatically examine the names of all workloads. If your workload naming convention follows the supported delimiter-based or positional format and contains any of the following data, Policy Generation can automatically label your applications, their tiers, and the sources and destinations in the policy rules. If your workload naming convention does not fit the supported formats or you want to manually name the proposed applications and tiers, select *None of these fit my configuration*.



Workload Naming Convention

If your workload names fit one of two patterns, Policy Generation can name proposed applications and functions for you.
Select the pattern that best fits your configuration:

○ Tags ○ Delimiter-based ○ Positional ● None of these fit my configuration

No Match

My workload naming conventions do not fit the Delimiter-based, nor the Positional patterns.
On the following Tags pages I can provide tags and full names that I can use later for identifying:

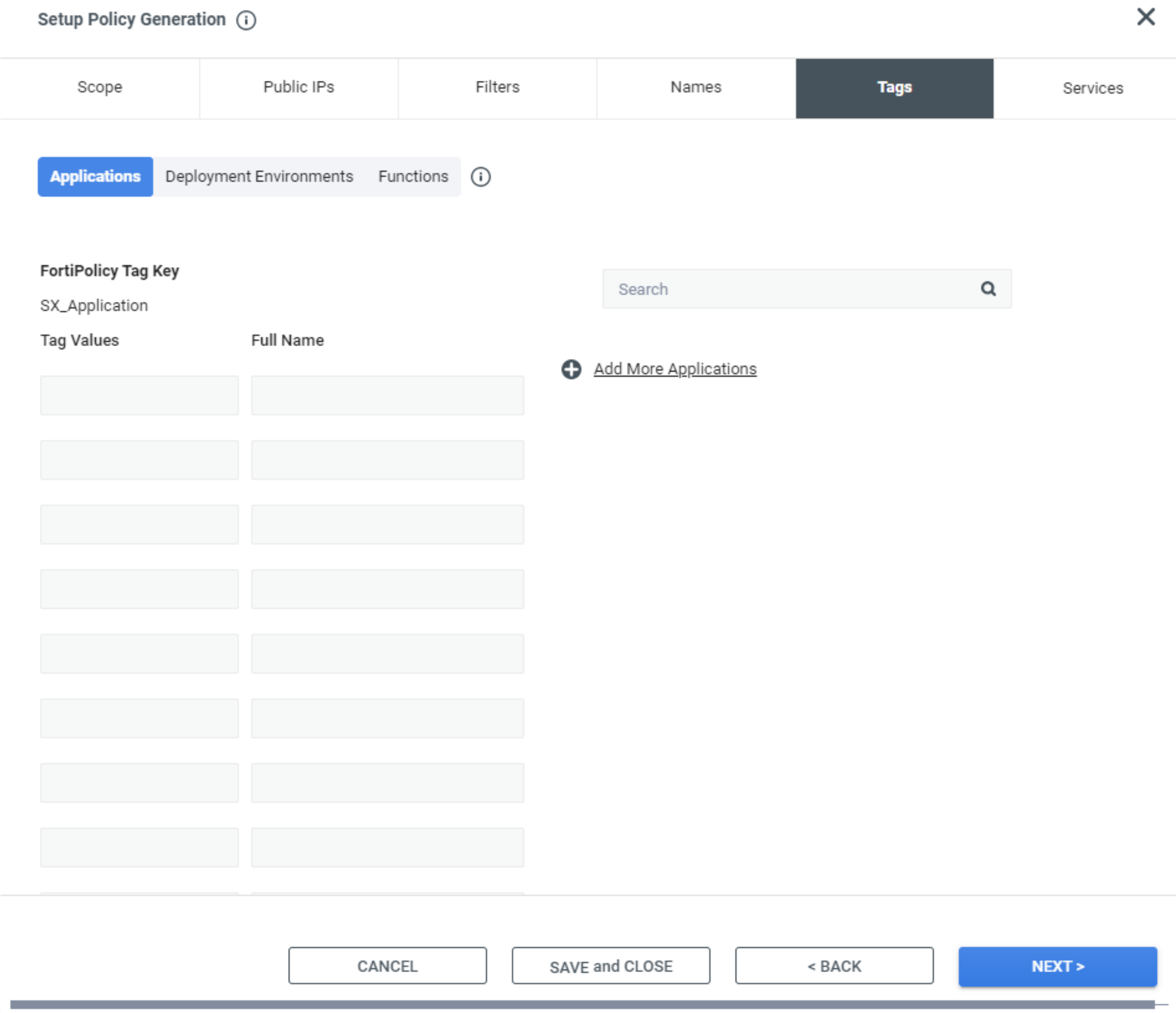
Workload Parameters

1. Applications
2. Deployment Environments
3. Functions

Click the Next> Button

12. Click *Next*.

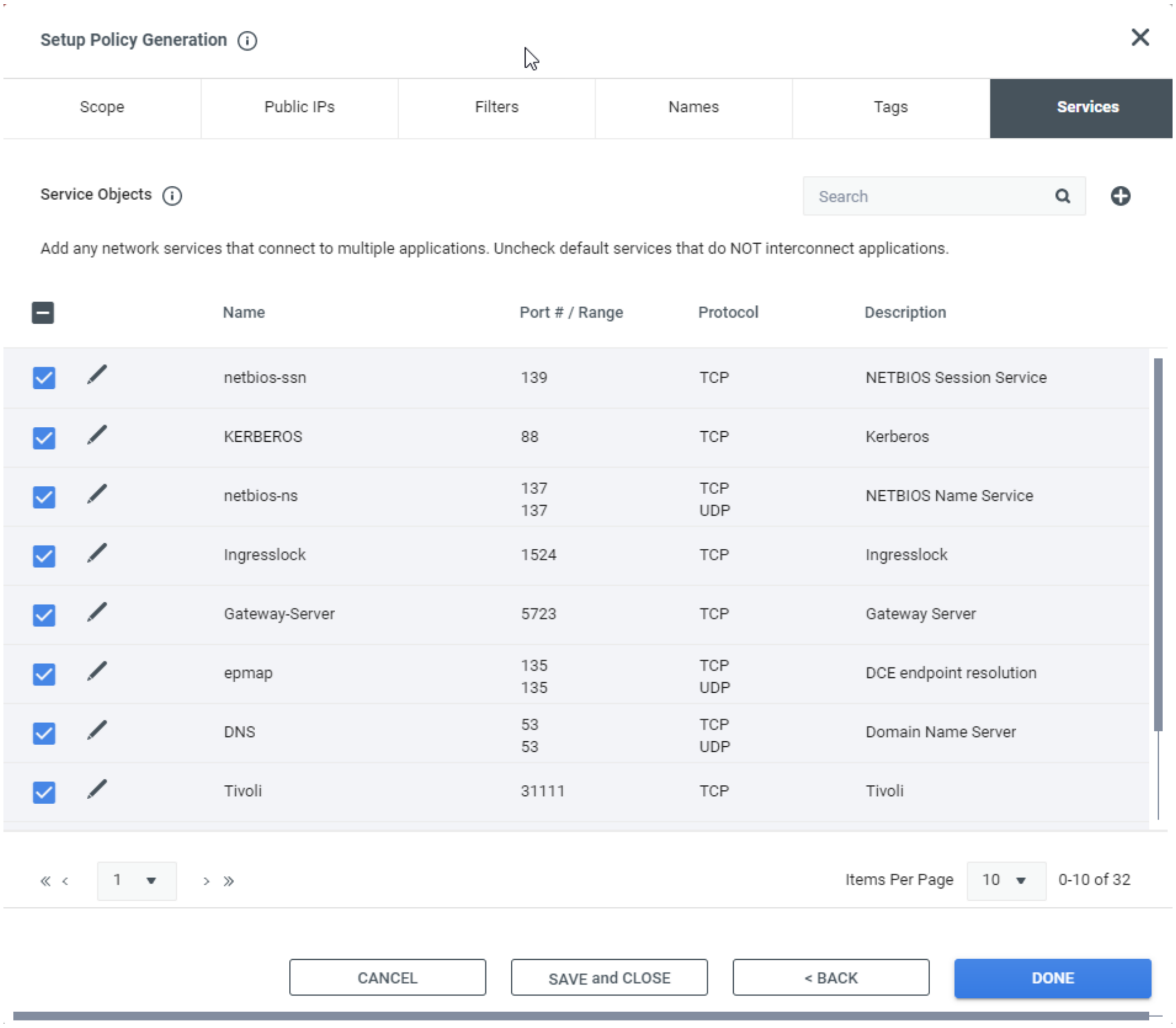
13. If you selected *Tags* on the *Names* tab, FortiPolicy derives tags from the workload naming convention used for existing applications, deployment environments, and tier functions. If you want to add more tags for applications, deployment environments, and tier functions, enter the value and full name for each tag.



14. Click *Next* to go through the three tag groups and then to the *Services* tab.

15. Review the list of standard network services that interconnect your workloads. Edit or add any services in your network that use nonstandard ports and protocols. Delete any services not used in your network.

Extremely important: An accurate list of network services allows FortiPolicy to identify all common network services and to distinguish between business application tiers and service tiers.



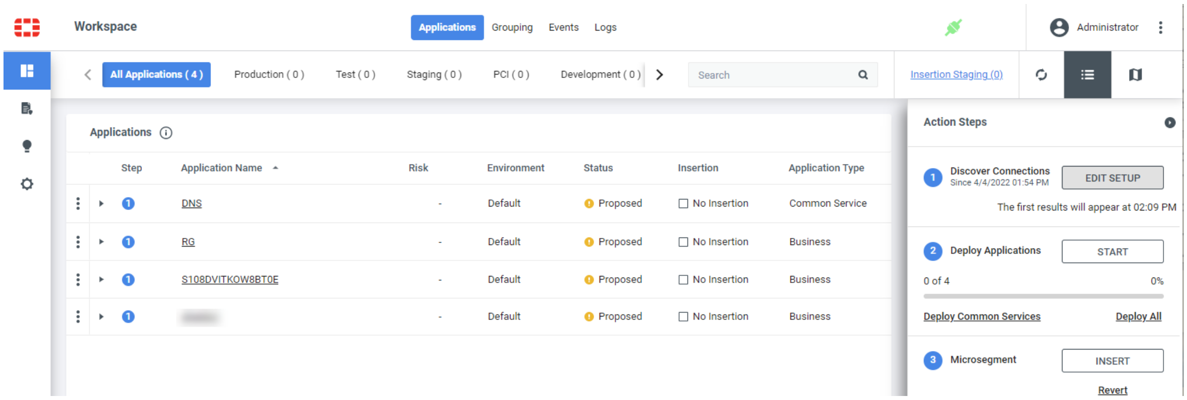
Service Objects

Add any network services that connect to multiple applications. Uncheck default services that do NOT interconnect applications.

⊟		Name	Port # / Range	Protocol	Description
☑	✎	netbios-ssn	139	TCP	NETBIOS Session Service
☑	✎	KERBEROS	88	TCP	Kerberos
☑	✎	netbios-ns	137 137	TCP UDP	NETBIOS Name Service
☑	✎	Ingresslock	1524	TCP	Ingresslock
☑	✎	Gateway-Server	5723	TCP	Gateway Server
☑	✎	epmap	135 135	TCP UDP	DCE endpoint resolution
☑	✎	DNS	53 53	TCP UDP	Domain Name Server
☑	✎	Tivoli	31111	TCP	Tivoli

16. Click *DONE*.

During Policy Generation, FortiPolicy gathers data on your network, learns its interconnections, and begins to propose security policies. The default connection discovery time is 2 hours. After additional analysis time, the proposed applications are listed in the *Applications* page.



Step	Application Name	Risk	Environment	Status	Insertion	Application Type
1	DNS	-	Default	Proposed	□ No Insertion	Common Service
1	RG	-	Default	Proposed	□ No Insertion	Business
1	S108DVITKOW8BT0E	-	Default	Proposed	□ No Insertion	Business
1	[redacted]	-	Default	Proposed	□ No Insertion	Business

1 Discover Connections
Since 4/4/2022 01:54 PM
The first results will appear at 02:09 PM

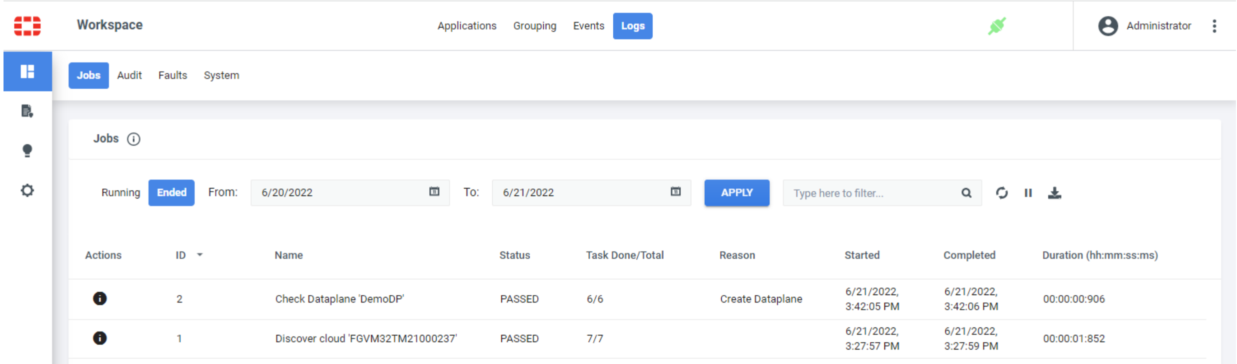
2 Deploy Applications
0 of 4 0%

3 Microsegment

For the next steps of FortiPolicy configuration, see the *FortiPolicy Automated Policy Generation Guide*.

Troubleshooting discovery

During discovery, you can view the real-time progression of infrastructure discovery events from the FortiPolicy *Workspace* > *Logs* > *Jobs* page and then troubleshoot any issues.



From: 6/20/2022 To: 6/21/2022

Actions	ID	Name	Status	Task Done/Total	Reason	Started	Completed	Duration (hh:mm:ss:ms)
i	2	Check Dataplane 'DemoDP'	PASSED	6/6	Create Dataplane	6/21/2022, 3:42:05 PM	6/21/2022, 3:42:06 PM	00:00:00:906
i	1	Discover cloud 'FGVM32TM21000237'	PASSED	7/7		6/21/2022, 3:27:57 PM	6/21/2022, 3:27:59 PM	00:00:01:852

Click the “i” information icon at the beginning of a Job row in the Jobs table to display any error details.

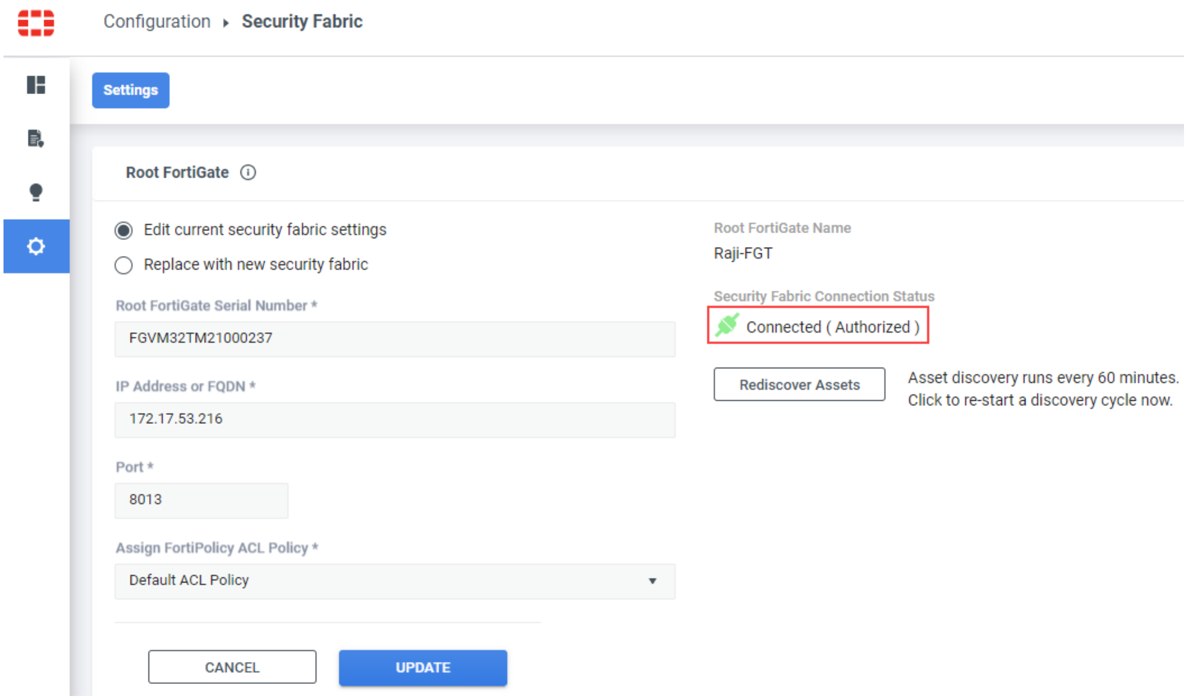
FortiPolicy discovers the data necessary for Policy Generation by connecting FortiPolicy data planes to the FortiGate and FortiSwitch devices in the Security Fabric. FortiPolicy discovers the Security Fabric endpoints and subscribes to the endpoints to receive traffic logs from the FortiGate devices and flow exports from the FortiSwitch units. FortiGate and FortiSwitch devices have a limit on the number of data collectors that can subscribe to receive this data (In FortiOS 7.0.x, the limit is four syslog data collectors for traffic logs and one data collector for flow export.). If FortiPolicy tries to subscribe to a device that is already at its subscription limit, data discovery will fail.

If connection discovery fails, FortiPolicy displays a red fault icon in the header bar, and the discovery status is shown as FAILED under the *Ended* tab on the *Workspace* > *Logs* > *Jobs* page. If connection discovery fails, FortiPolicy cannot get the necessary data to generate valid proposals. A common cause of discovery failure is that a device has reached its limit of subscribed clients.

To solve this problem, the FortiPolicy administrator must go to any oversubscribed FortiGate or FortiSwitch devices and remove an existing subscribed client. Then, the administrator can return to FortiPolicy, go to *Configuration* > *Data Planes*, click the vertical ellipsis menu at the left side of the page, and select *Sync* for each data plane to register it with its Fortinet devices. After synchronizing the data planes, the *Ended* tab on the *Jobs* page should show a status of PASSED for discovery.

You can also check the following settings if you are having trouble with connection discovery:

- Go to *Configuration* > *Security Fabric* and verify that the icon under Security Fabric Connection Status is green, which indicates that the connection is active.



Root FortiGate ⓘ

● Edit current security fabric settings
○ Replace with new security fabric

Root FortiGate Serial Number *: FGVM32TM21000237

IP Address or FQDN *: 172.17.53.216

Port *: 8013

Assign FortiPolicy ACL Policy *: Default ACL Policy

Root FortiGate Name: Raji-FGT

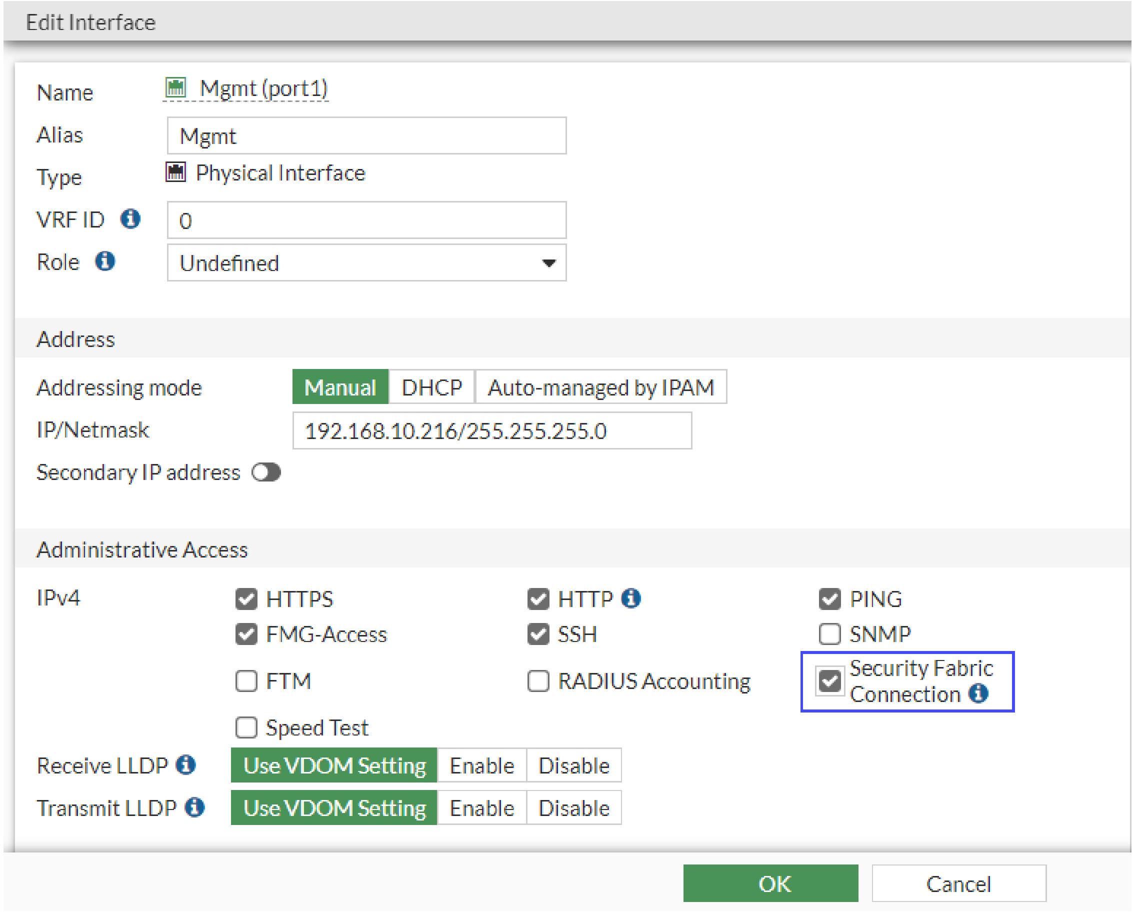
Security Fabric Connection Status: Connected (Authorized)

Asset discovery runs every 60 minutes. Click to re-start a discovery cycle now.

- Before you created the data planes, you needed to enable NetFlow on each FortiGate device where a data plane is created with the following commands:

```
config system csf
   config fabric-connector
      edit <FortiPolicy_serial_number>
         set configuration-write-access enable
         set accprofile super_admin
      next
   end
end
```

- Go to *Workspace* > *Logs* > *Jobs* and check for errors in discovering the Security Fabric.
  - If there are compatibility errors, make certain that you are using FortiOS 7.0.6.
  - In the root FortiGate device, go to *Network* > *Interfaces*, select the WAN port, and click *Edit*. Make certain that the *Security Fabric Connection* checkbox is selected.



Edit Interface

Name: Mgmt (port1)

Alias: Mgmt

Type: Physical Interface

VRF ID: 0

Role: Undefined

Address

Addressing mode: [✓ Manual] DHCP Auto-managed by IPAM

IP/Netmask: 192.168.10.216/255.255.255.0

Secondary IP address: ○

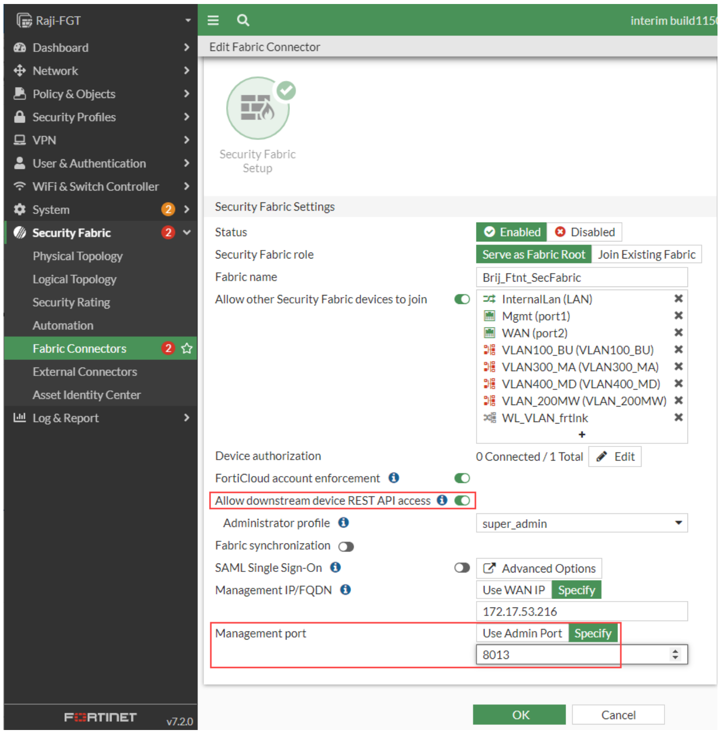
Administrative Access

IPv4:
☑ HTTPS ☑ HTTP ☑ PING
☑ FMG-Access ☑ SSH □ SNMP
□ FTM □ RADIUS Accounting ☑ Security Fabric Connection
□ Speed Test

Receive LLDP: [✓ Use VDOM Setting] Enable Disable

Transmit LLDP: [✓ Use VDOM Setting] Enable Disable

- Go to *Workspace* > *Logs* > *Jobs* and check for any errors from when you created the data planes.
  - For each FortiGate device in the Security Fabric, go to *Security Fabric* > *Fabric Connectors*, right-click *Security Fabric Setup*, and select *Edit*. Check that *Allow downstream device REST API access* is enabled and that the management port is set to 8013.



Edit Fabric Connector

Security Fabric Settings

Status	Enabled Disabled
Security Fabric role	Serve as Fabric Root Join Existing Fabric
Fabric name	Brij_Ftnt_SecFabric
Allow other Security Fabric devices to join	InternalLan (LAN) Mgmt (port1) WAN (port2) VLAN100_BU (VLAN100_BU) VLAN300_MA (VLAN300_MA) VLAN400_MD (VLAN400_MD) VLAN_200MW (VLAN_200MW) WL_VLAN_frtlnk +
Device authorization	0 Connected / 1 Total Edit
FortiCloud account enforcement	
Allow downstream device REST API access	
Administrator profile	super_admin
Fabric synchronization	
SAML Single Sign-On	Advanced Options
Management IP/FQDN	Use WAN IP Specify 172.17.53.216
Management port	Use Admin Port Specify 8013

  - Check that logs are enabled with the `set logtraffic` command under `config firewall policy` in the FortiOS CLI.
- Check that the proxy ARP was configured on the primary NAC segment interface on the FortiGate devices. For example:

```
config system proxy-arp
   edit 1
      set interface ”nac_segment”
      set ip 10.255.13.2
      set end-ip 10.255.13.5
   next
end
```

What to do next

Refer to the following FortiPolicy documentation for more information about the current release:

- *FortiPolicy Release Notes*
- *FortiPolicy Automated Policy Generation Guide*

FORTINET®

www.fortinet.com