Administration Guide

FortiPolicy 7.2.2

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

February 10, 2023
FortiPolicy 7.2.2 Administration Guide
64-722-0808206-20230210

TABLE OF CONTENTS

Change log

Date	Change description
February 10, 2023	Initial release

Preface

This section covers the following topics:

- Overview on page 6
- Documentation conventions on page 6
- Related documentation on page 7
- Obtaining more information on page 7
- Technical support on page 8

Overview

FortiPolicy is the first containerized security platform that implements and automates security orchestration with full-flow inspection and segmented and microsegmented policy enforcement while auto-scaling to accommodate infrastructure changes and multi-terabit traffic flows.

This manual describes how FortiPolicy facilitates application security using the Fortinet Security Fabric.

This manual is prepared for data center infrastructure administrators, network virtualization administrators, information technology (IT) managers, network security experts, data center security administrators, and cybersecurity analysts.

This manual is organized as follows:

- Introduction on page 9 describes security threats in a Security Fabric, followed by the FortiPolicy technology solutions and detailed software component overviews.
- Getting started on page 12 explains how to initially install the FortiPolicy software to get started with continuous Security Fabric monitoring.
- Setting up your workspace on page 63 describes how to set up your applications, configure resource groups, specify segmentation and microsegmentation, and view events and logs.
- Customizing policies on page 100 describes how to create access control list (ACL) rules and policies, allowlists, blocklists, and custom URL categories.
- Insights into FortiPolicy on page 104 covers how to view FortiPolicy workloads, detections, assets, and operations.
- FortiPolicy configuration on page 108 describes how to configure the Security Fabric, create data planes, set up servers and certificates, improve your system health, perform system maintenance, and obtain reports.

Documentation conventions

This manual uses the following conventions for typographically representing terms and procedures.

Convention	Meaning	Example
italics	Denotes the name of GUI elements.	Enter a unique name in the *Name* field.
Courier font	Coding examples and text to be entered at a command prompt or Web UI field.	Enter the following path: `z:\vsphere-remote\datacenter`
Click	Click the left mouse button.	Click *Deploy* to save your configuration and deploy the virtual chassis.
Double-click	Double-click the left mouse button.	Double-click the tagged *WORKLOAD* icon to display its IP address.
Right-click	Click the right mouse button.	Right-click the icon to display related details.

Related documentation

The following FortiPolicy documents supplement this manual:

- *FortiPolicy Release Notes* describe the latest release of the FortiPolicy software including caveats, open issues, and new features.
- *FortiPolicy Getting Started Guide* describes how to install and initially configure the FortiPolicy software in VMware environments. FortiPolicy becomes self-orchestrating immediately following initial configuration and virtual chassis deployment.
- *FortiPolicy Automated Policy Generation Guide* describes how to secure your environment by allowing FortiPolicy to automate discovery, analysis, and organization of all connections and workloads into application groups for you, with proposed security policy recommendations for connections between those groups, including custom policies.
- *FortiPolicy CLI Reference* describes the commands that make up the command-line interface (CLI) for FortiPolicy.

Obtaining more information

To obtain more information about FortiPolicy, refer to the following sources:

- Fortinet website—General information about the company and products
- Fortinet Support Community—Technical tips, Fortinet Forum, and Knowledge Base
- Fortinet Document Library—Administration guides, reference manuals, and release information

Technical support

For technical support, contact Fortinet as follows:

- Email support@fortinet.com
- Call:
  + 1 408 898 3205 (Worldwide)
  +1 877 345 3834 (USA & Canada)
- Visit the Fortinet Customer Support Portal (login required) at:
  http://www.fortinet.com/support/

Introduction

This section introduces FortiPolicy and provides an overview of how FortiPolicy facilitates application security using the Fortinet Security Fabric.

This section covers the following topics:

- Intent-based cybersecurity on page 9
- FortiPolicy microservices-based adaptive security on page 9
- Primary components and containerized microservices on page 10
- FortiPolicy management plane on page 11

Intent-based cybersecurity

The cybersecurity landscape is filled with threats. Networks of all types face challenges in the visibility and understanding of appropriate communications verses possible threats. The need to implement important zero-trust concepts such as “least privilege” segmentation and microsegmentation policies is paramount in limiting the impact of possible breaches to the network. Network administrators require tools that enable them to automate and enforce intent-based cybersecurity.

FortiPolicy delivers comprehensive and consistent controls to protect on-premises data centers and OT environments, their applications, and their data. It leverages agentless machine-learning (ML) technology, and, through the Fortinet Security Fabric, enforces intention with a set of comprehensive controls including microsegmentation, firewalling, and more.

This powerful, agentless, ML platform enhances the microsegmentation and intent-based networking segmentation capabilities of the Security Fabric. It enables end-to-end visibility and connection-mapping of north-south and east-west traffic flows for on-premises data centers. FortiPolicy then applies ML to provide context to these workflows, enabling it to suggest security policies to the Security Fabric.

Data-center administrators are then able to learn relationships among workloads and applications and make decisions to allow or block that communication. These machine-learning-enabled policies can be automated, which reduces complexity and improves efficiency in their implementation. This process of discovery, security, and automation offers a truly adaptive solution to protect your most sensitive assets. FortiPolicy meshes seamlessly into the Security Fabric and is integrated into all layers of the infrastructure.

FortiPolicy microservices-based adaptive security

FortiPolicy software-defined security is deployed into your Security Fabric. FortiPolicy provides uniquely intelligent and extremely high levels of automated security policy orchestration. These data-aware services discover and monitor entire infrastructure network topologies, protocols, applications, security policies, and active workloads, and they can protect active workloads across your Security Fabric.

By providing complete, centralized visibility into your fabric, FortiPolicy software-based security delivers the next generation of data center protection.

FortiPolicy enables organizations to natively, automatically segment and secure workloads at scale. It provides visibility, policy management, and enforcement at scale. Organizations can implement on-demand security policies, based on the following:

- Microsegmentation: Application-aware access control; security enforcement between workloads even on the same subnet
- Flows: East/west

Primary components and containerized microservices

The following table lists the primary components and containerized microservices in FortiPolicy, including usage descriptions and links to more detailed information.

Software component or microservice	Usage
FortiPolicy software	FortiPolicy software OVF (VMware)
Continuous discovery	Following initial discovery with a simple Infrastructure Connector configuration, FortiPolicy's continuous discovery continues to identify all changes throughout your Security Fabric. The FortiPolicy factory then automatically updates protections for all infrastructure objects that FortiPolicy is configured to protect. FortiPolicy technology also visualizes the continuous discovery results in a map view (available from the FortiPolicy maps).
Connection discovery	The automated FortiPolicy policy generation secures your environments by allowing FortiPolicy to automate discovery, analysis and organization of all connections and workloads into application groups, for you, with security policy recommendations for connections between those groups. Connection discovery is distinct from FortiPolicy's infrastructure-assets discovery/continuous discovery technologies. Following FortiPolicy connection discovery, FortiPolicy proposes security groupings of applications with suggested ACLs for implementation between proposed application groups—with policy granularity to the level of the tier. You can verify, modify, and test grouping, policy proposals, and compliance before deploying and enforcing security policies with microsegmentation.
FortiPolicy fabric connector	The FortiPolicy fabric connector connects to a Security Fabric for fabric provisioning information exchange and security orchestration as part of FortiPolicy continuous discovery and continuous monitoring.
FortiPolicy resource group	A collection of workloads or networks, proposed by FortiPolicy, that share identical security requirements. Also sometimes referred to as an application tier. The automated policy generation feature proposes application tiers as sources and destinations in its proposed ACL rules.

Software component or microservice	Usage
FortiPolicy data plane	The data plane is where security policy is enforced. The scope of a data plane is to observe and propose policies specific to a VDOM.
Automated Policy Generation	FortiPolicy option that allows FortiPolicy to automate discovery, analysis, and organization of all connections and workloads in your infrastructures into application groups, for you, with security policy recommendations for connections between those groups.
FortiPolicy access control (ACL)	Access control policy is an ordered set of rules that govern the ability of workloads to make connections. FortiPolicy provides dynamic grouping of ACLs for granular security of segments and microsegments. Assigning an ACL policy to a fabric connector is required; this allows you to create ACLs between workloads in different data planes.

FortiPolicy management plane

The management plane is needed for communicating between FortiPolicy services and the management console, and to connect to the outside world for software updates and so on.

No ACLs are allowed on the FortiPolicy management network.

Getting started

This section describes FortiPolicy requirements for VMware and how to get started installing FortiPolicy for continuous monitoring and microservice protection.

This section covers the following topics:

- Before you begin on page 12
- FortiPolicy deployment scenario on page 12
- Installation and setup requirements on page 13
- Installing FortiPolicy on page 18
- Initial login on page 29
- Navigating the FortiPolicy menus on page 31
- Configuring FortiPolicy on page 32
- Troubleshooting discovery on page 54
- FortiPolicy CLI on page 57
- Using the FortiPolicy REST API on page 58

Before you begin

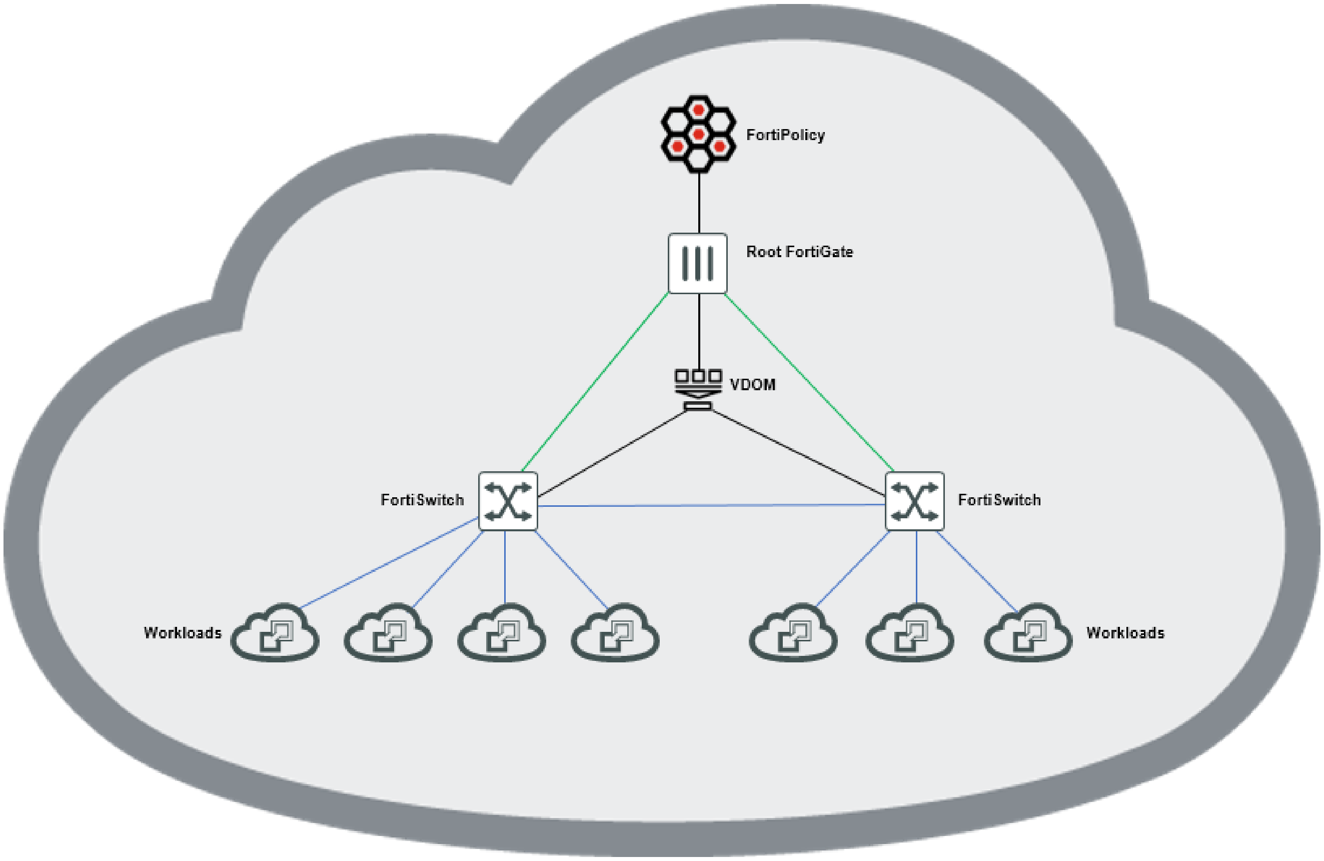
Before installing FortiPolicy:

- Read the *FortiPolicy Release Notes* for the current release.
- Review the requirements for your VMware environment before installing FortiPolicy.
  Refer to Installation and setup requirements on page 13.

A change of IP address for the FortiPolicy console is not supported in this release.

FortiPolicy deployment scenario

The FortiPolicy virtual chassis, all associated data planes, and all integrated microservices and security controls can be deployed in the Fortinet Security Fabric for an east/west deployment.



Installation and setup requirements

This section identifies the system requirements for installing FortiPolicy.

General requirements

Confirm that your ESX environment meets FortiPolicy prerequisites and requirements before beginning an installation procedure. The following list displays 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 the FortiPolicy cloud for software upgrades, licensing, and other features.
- Latest version of Google Chrome
- Access to Fortinet Support
- 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.

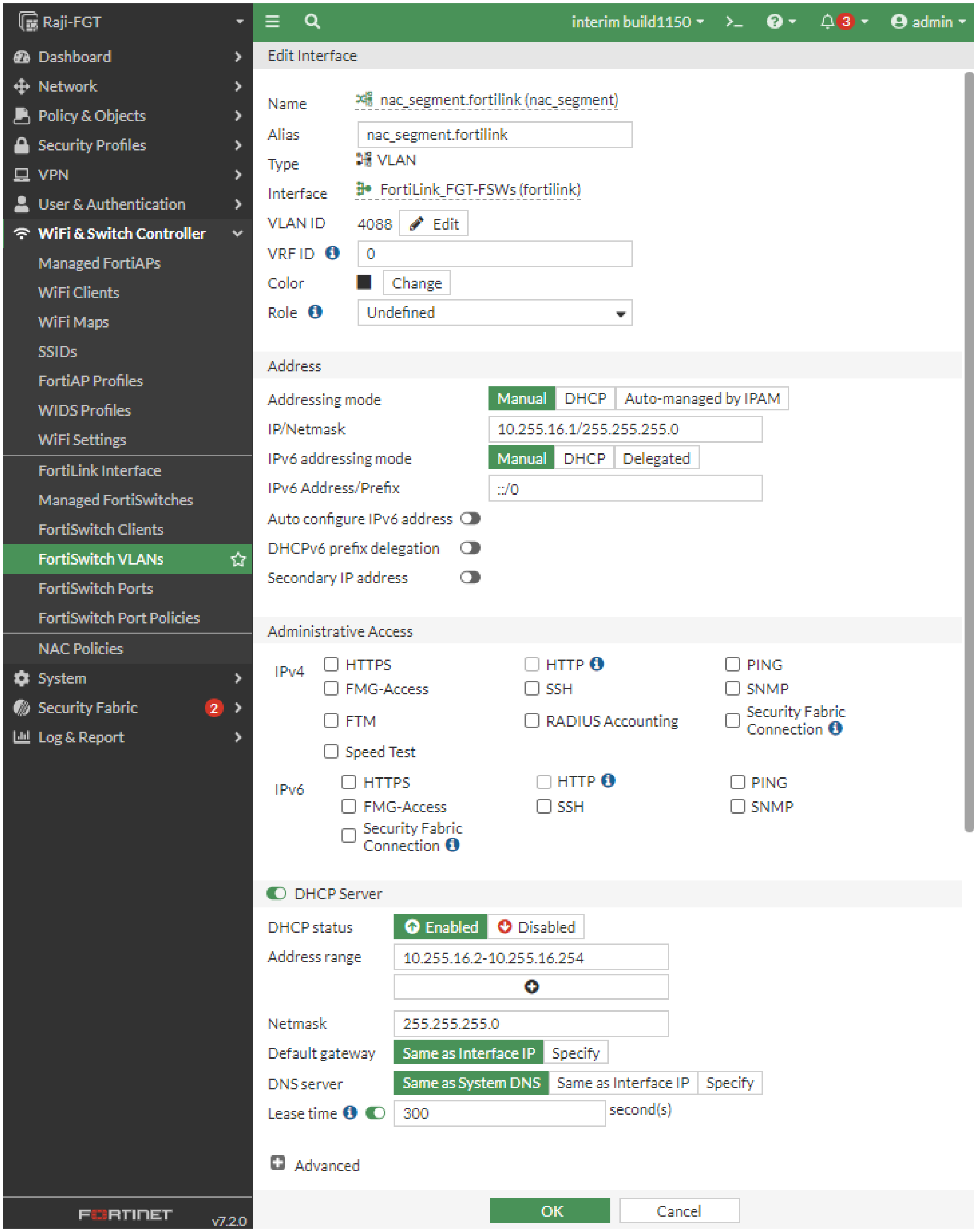
    To configure security profiles, see Security Profiles. To configure security policies, see NGFW policy.

    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 port must have *Fabric Integration* selected, and the FortiGate device must be reachable from FortiPolicy.
  - The FortiGate device cannot have a custom virtual domain (VDOM). Custom VDOMs prevent fabric integration.
  - A NAC LAN segment must be configured on a physical FortiGate device. You can use the default `nac_segment.fortilink` interface or create a new one.
  - The FortiGate device 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

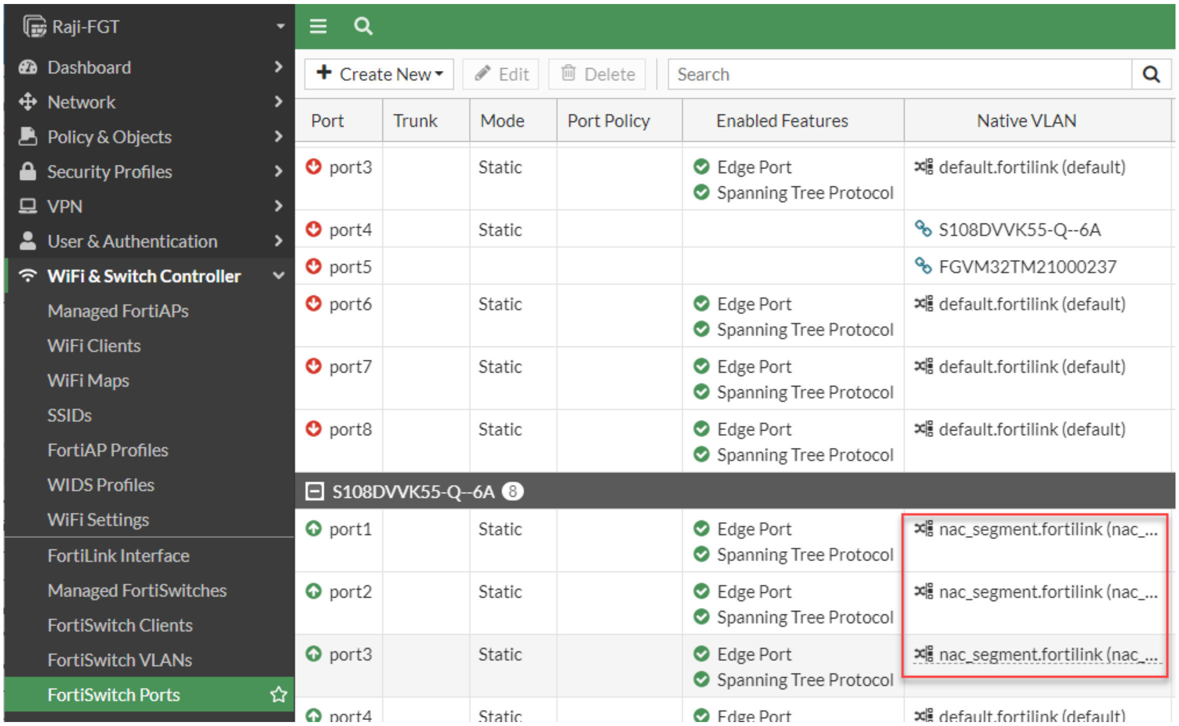
vii. Click *OK*.

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; 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 device. 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 ESX 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		

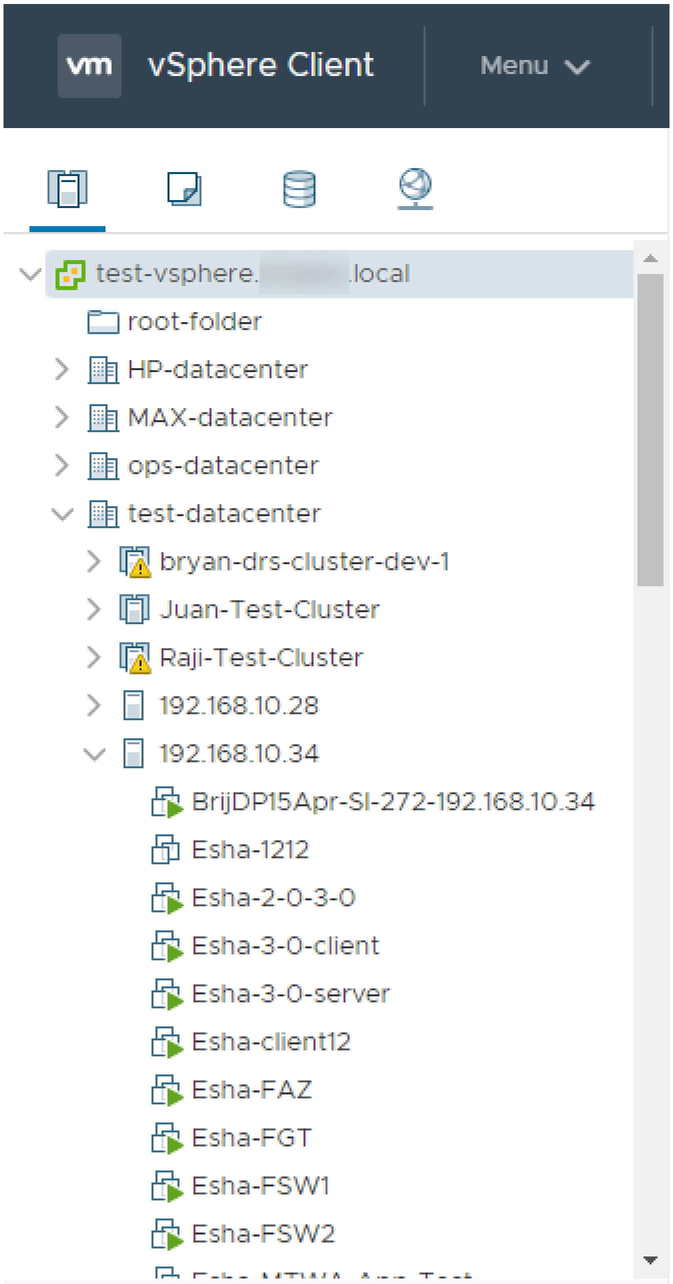
Service or program	Protocol	Incoming ports	Outgoing ports	Internal ports
DNS	TCP, UDP		53	
NTP	UDP		123 outbound queries to NTP servers from FortiPolicy	123 to FortiPolicy
Web access	UDP	80, 443		FortiPolicy port 5601
Connection between FortiPolicy and Security Fabric	TCP		8013 and 443	
Connection between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

The following table lists the required management ports.

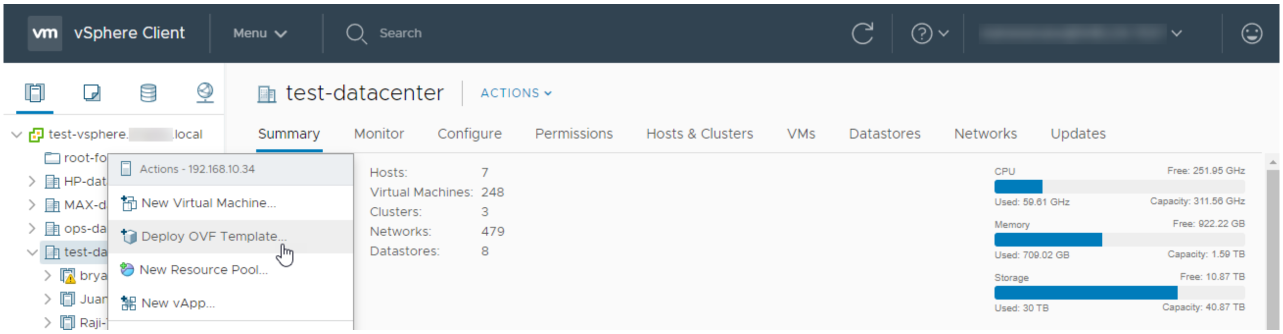
Service or program	Protocol	Incoming ports	Outgoing ports	Internal ports
Web access	TCP	80		FortiPolicy port 5601
Web access	TCP	443		FortiPolicy port 5601

Installing FortiPolicy

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



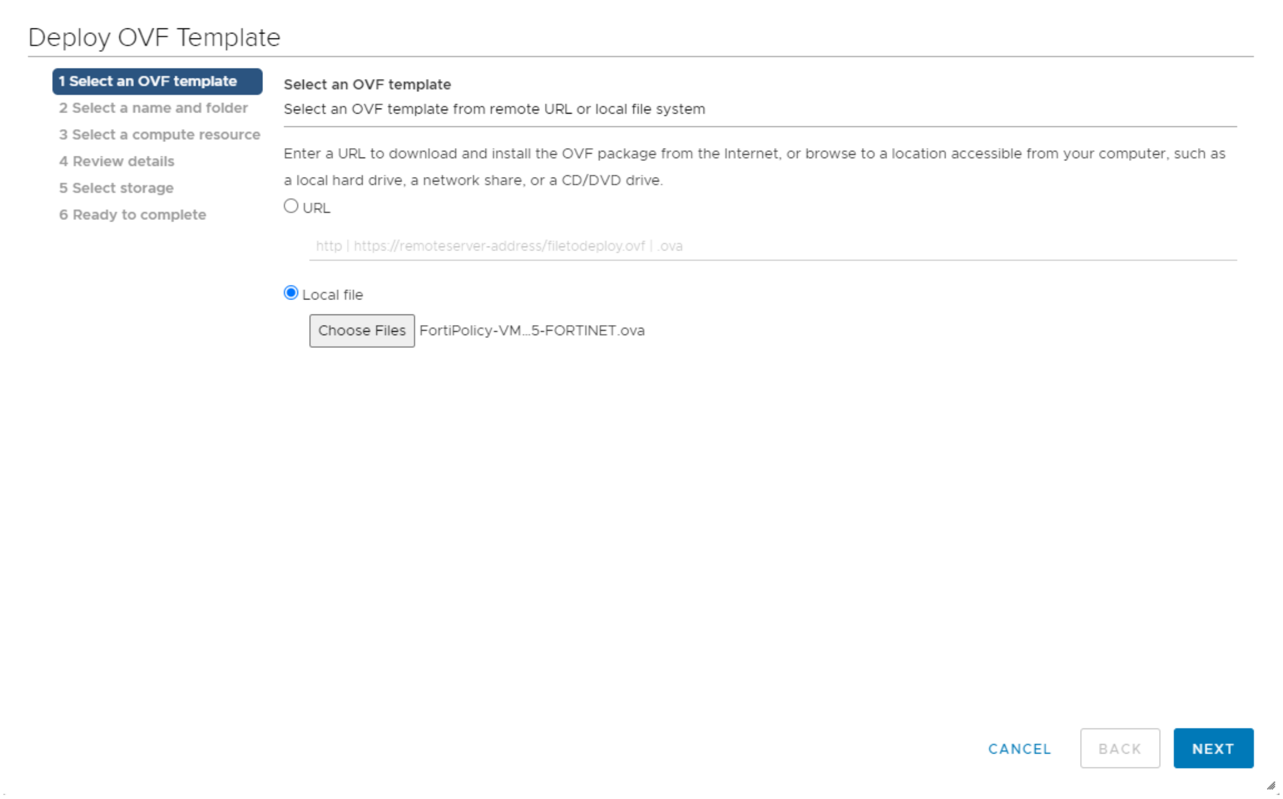
2. Right-click on the host and select *Deploy OVF Template*.



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*.



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.

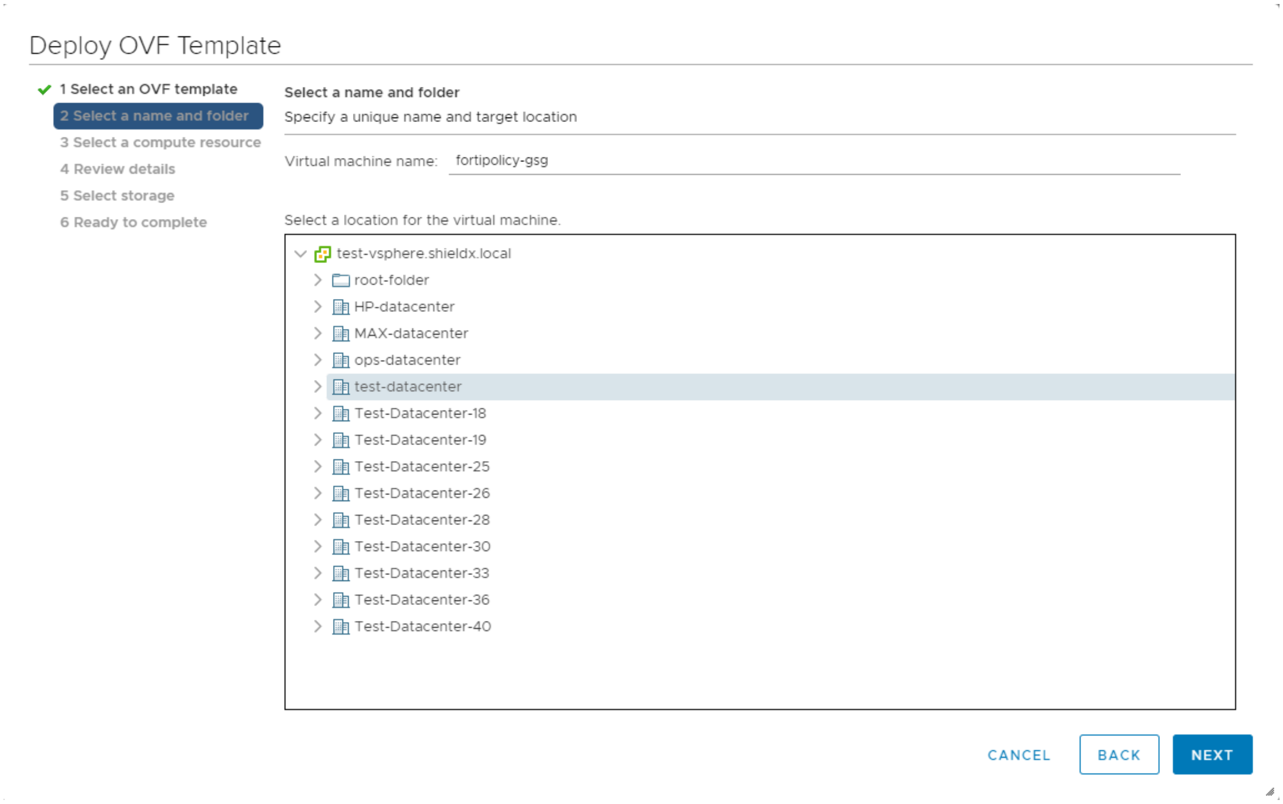
○ URL

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

● Local file

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

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



Deploy OVF Template

Select a name and folder

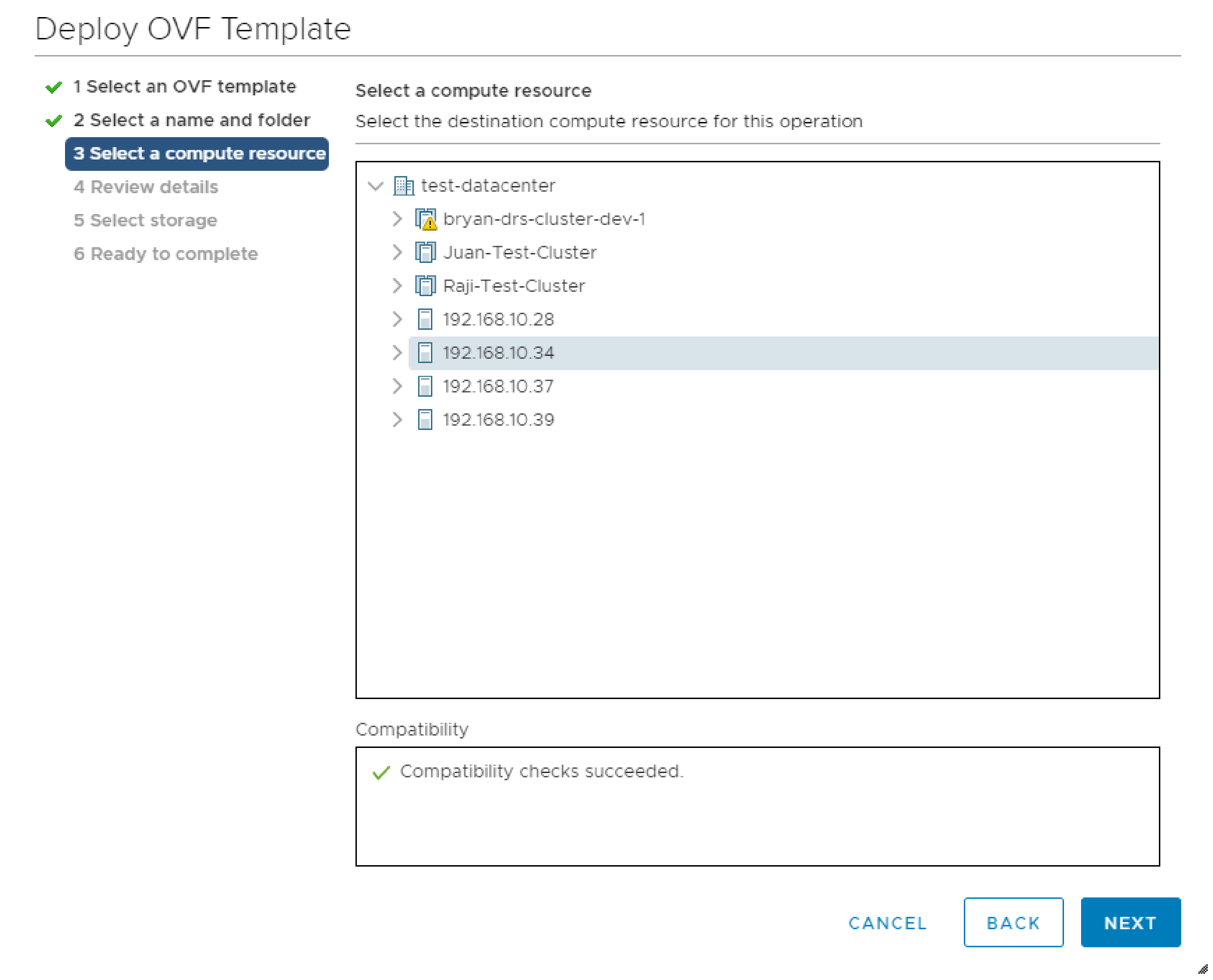
Specify a unique name and target location

Virtual machine name: fortipolicy-gsg

Select a location for the virtual machine.

- test-vsphere.shieldx.local
  - root-folder
  - HP-datacenter
  - MAX-datacenter
  - ops-datacenter
  - test-datacenter
  - Test-Datacenter-18
  - Test-Datacenter-19
  - Test-Datacenter-25
  - Test-Datacenter-26
  - Test-Datacenter-28
  - Test-Datacenter-30
  - Test-Datacenter-33
  - Test-Datacenter-36
  - Test-Datacenter-40

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

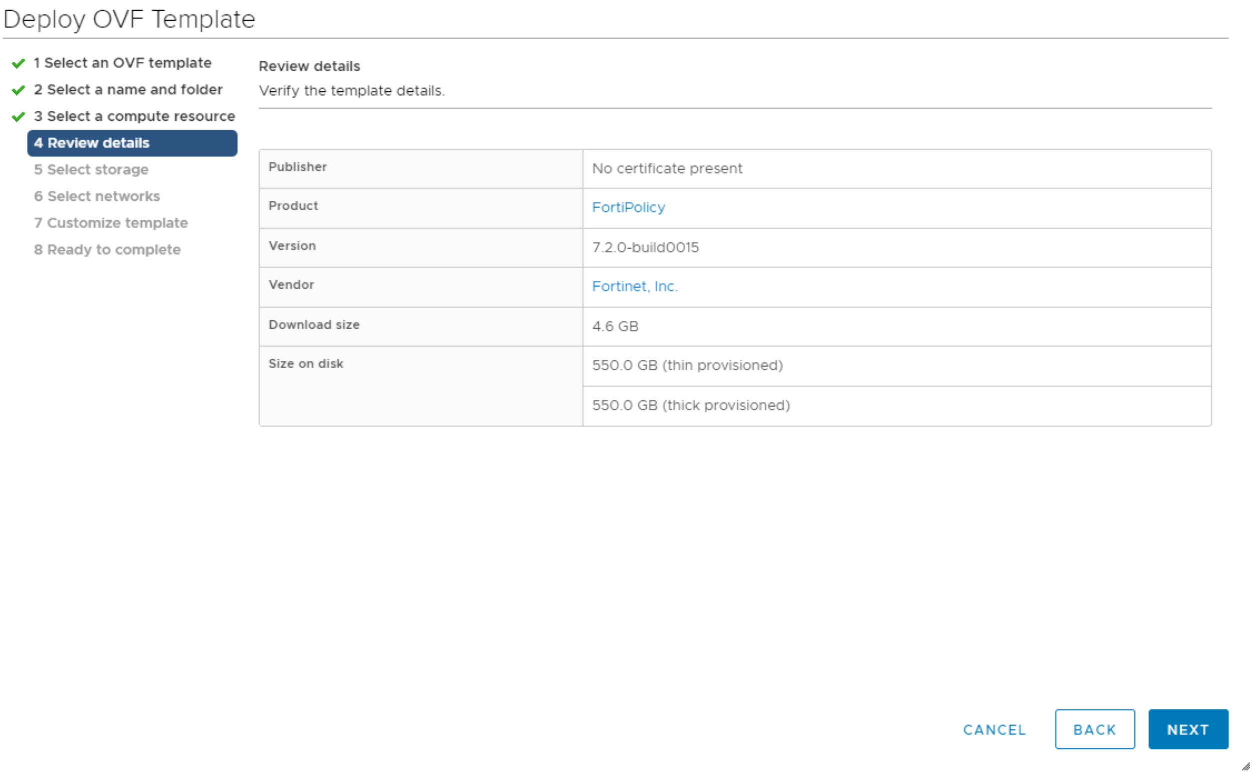
Select a compute resource
Select the destination compute resource for this operation

- 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*.

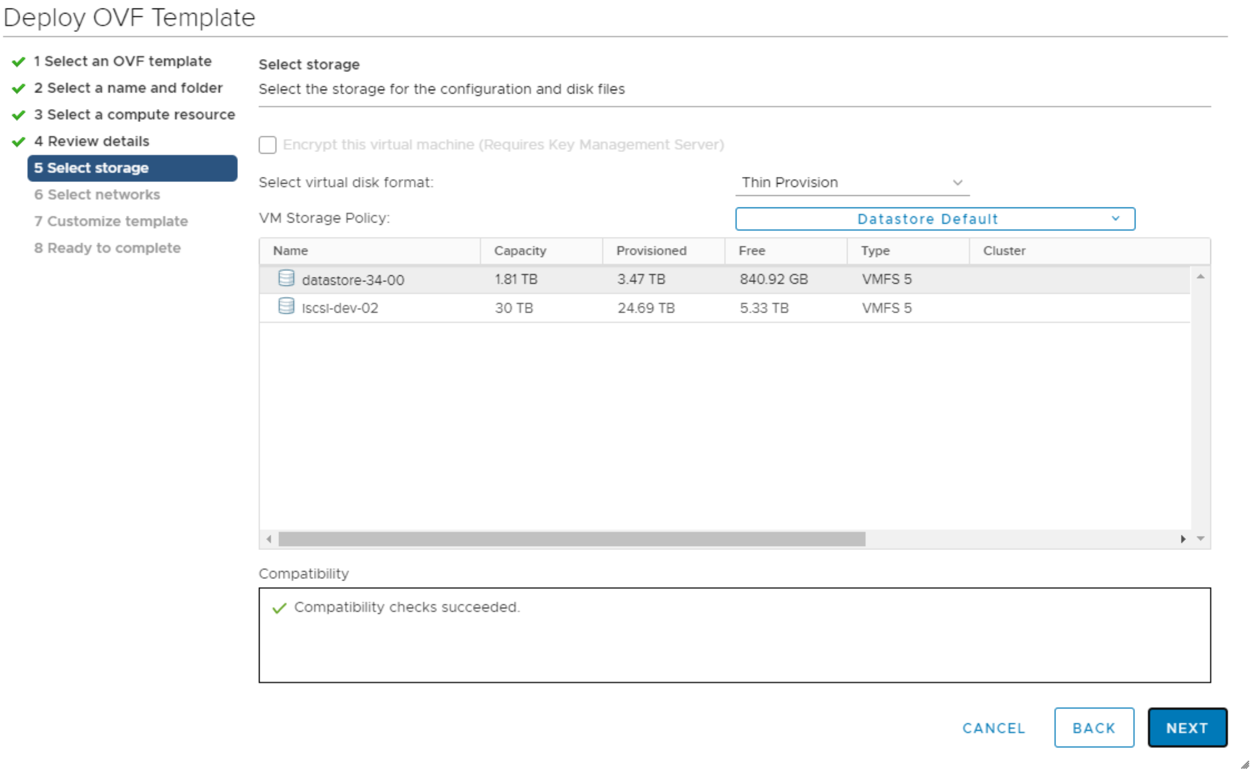


Review details

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

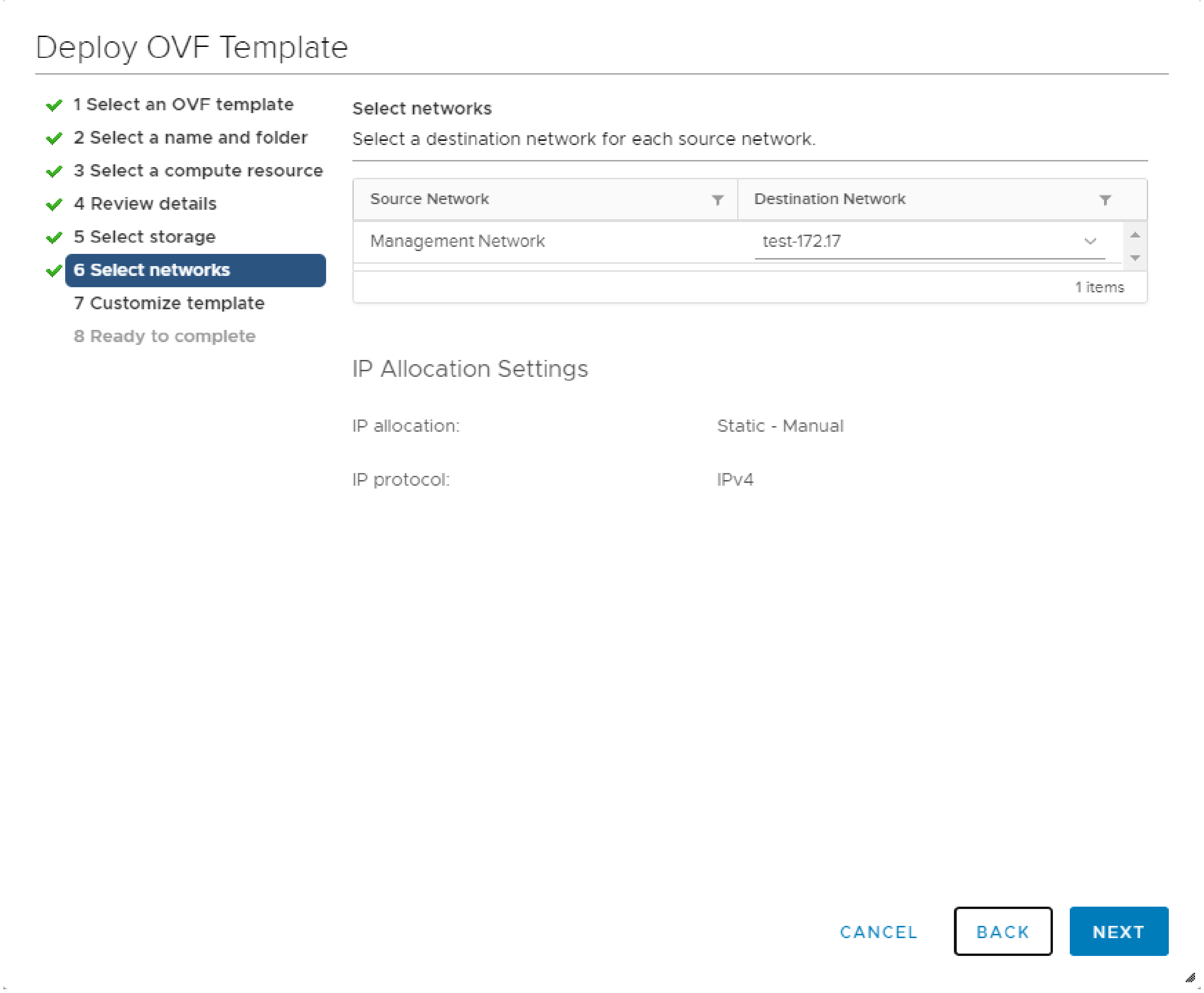
VM Storage Policy: Datastore Default

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

- ✓ 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

Select networks

Select a destination network for each source network.

Source Network	Destination Network
Management Network	test-172.17

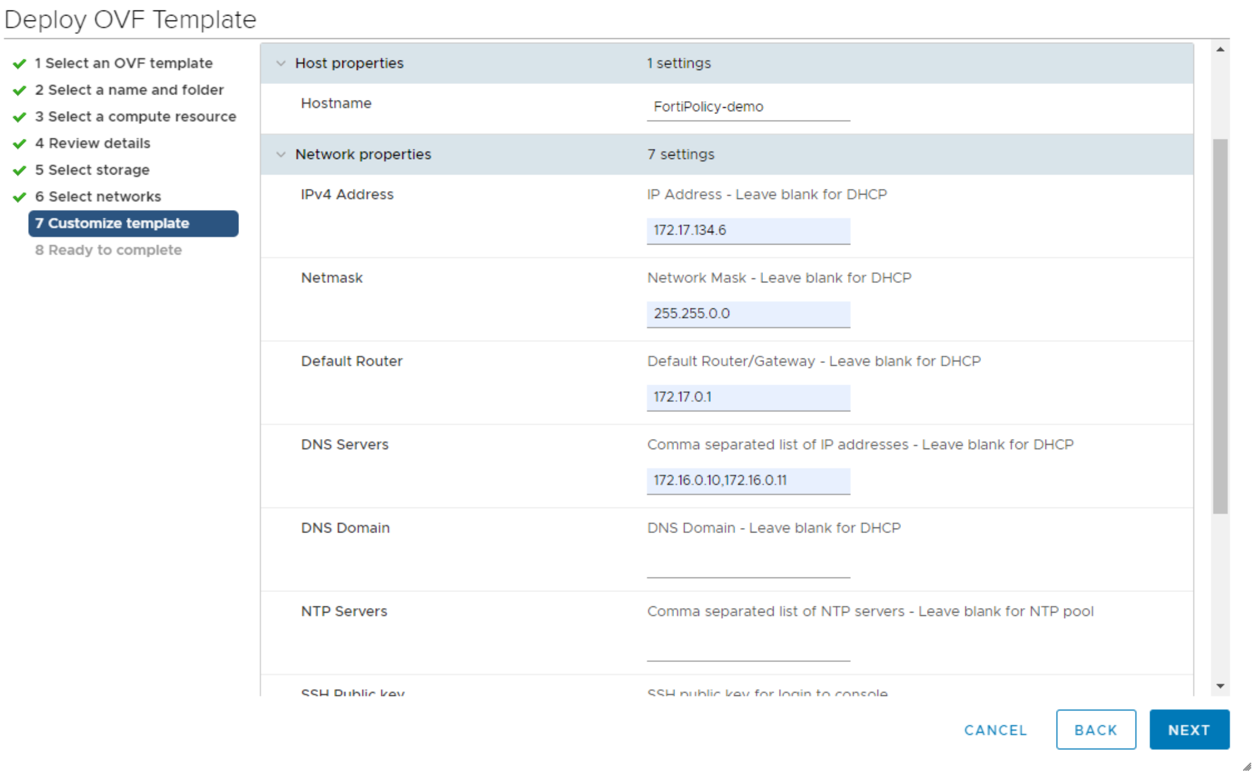
1 items

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.

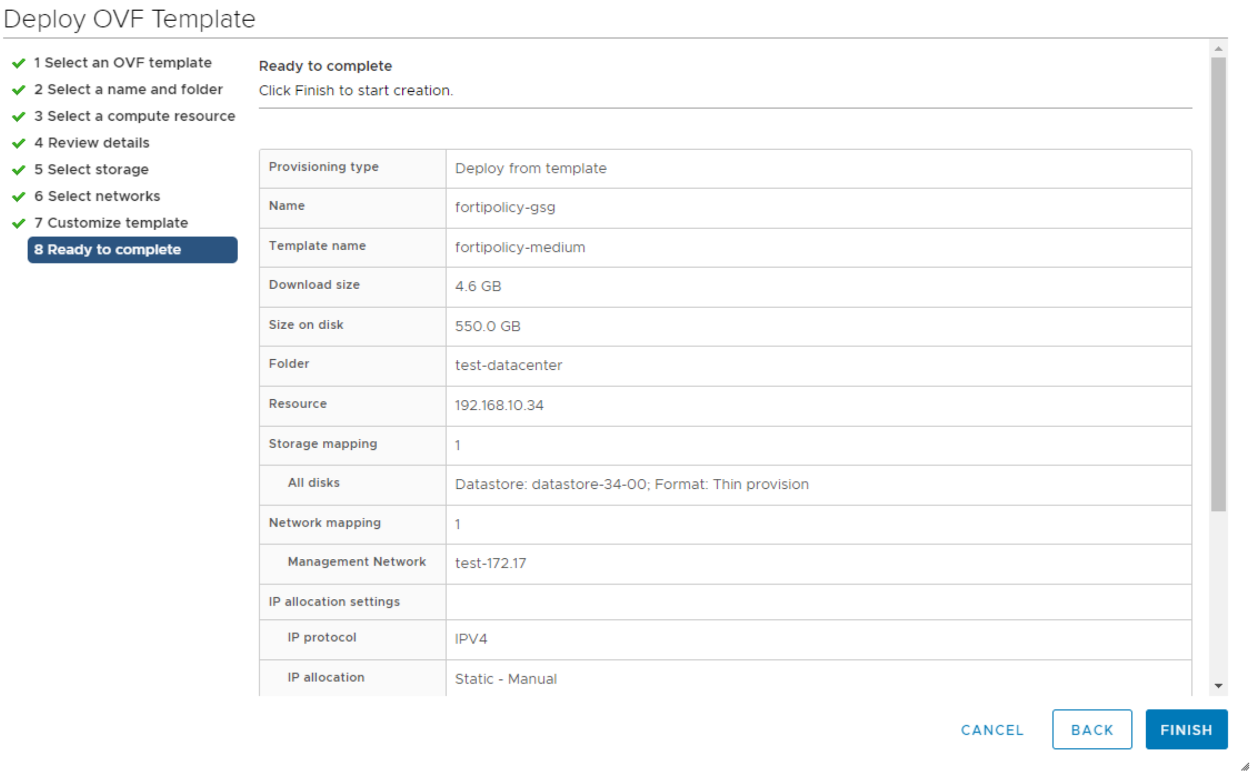
   No other configurations are required on this page.



Deploy OVF Template

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

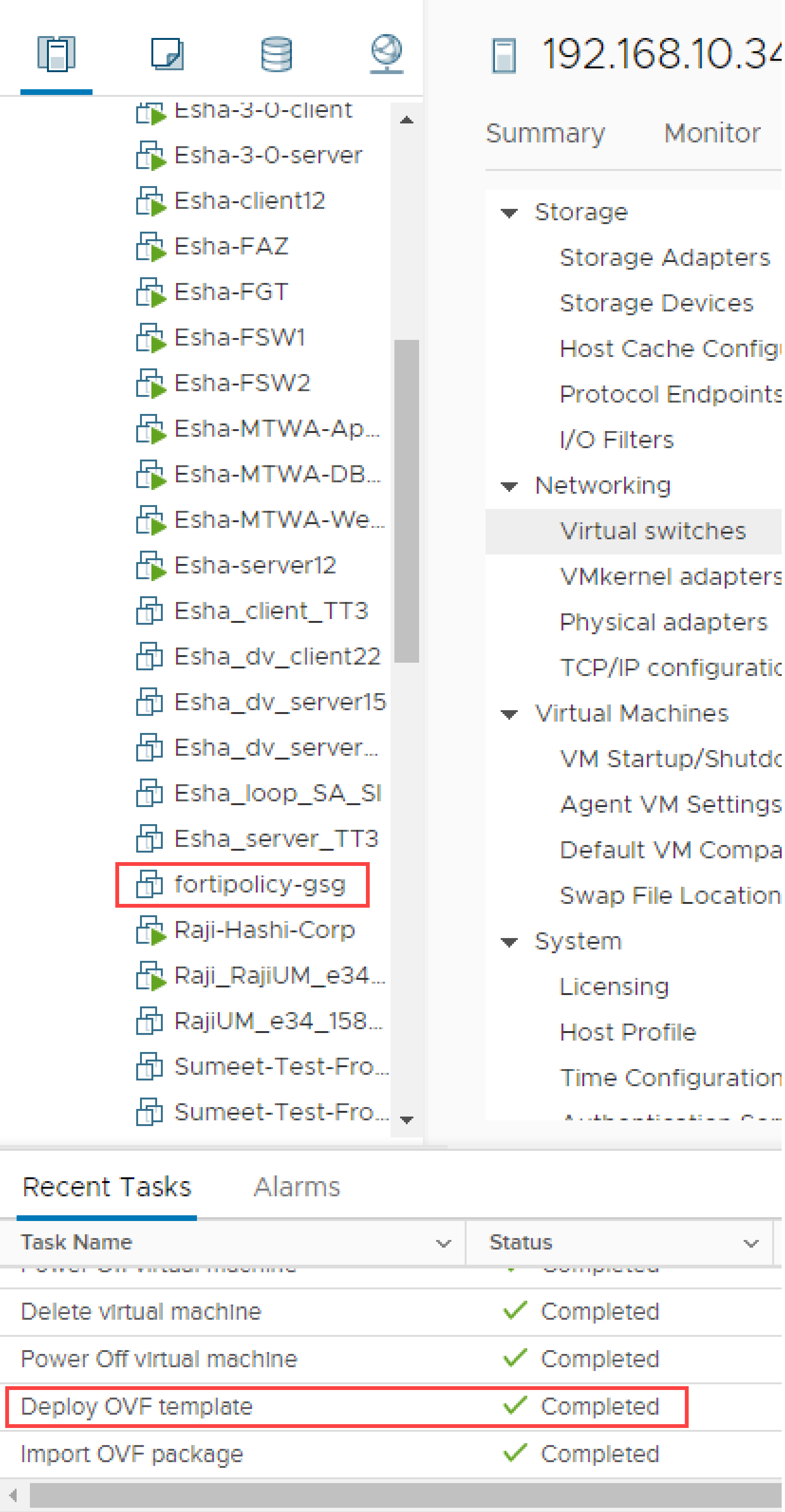
- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 Select storage
- ✓ 6 Select networks
- ✓ 7 Customize template
- 8 Ready to complete

Ready to complete

Click Finish to start creation.

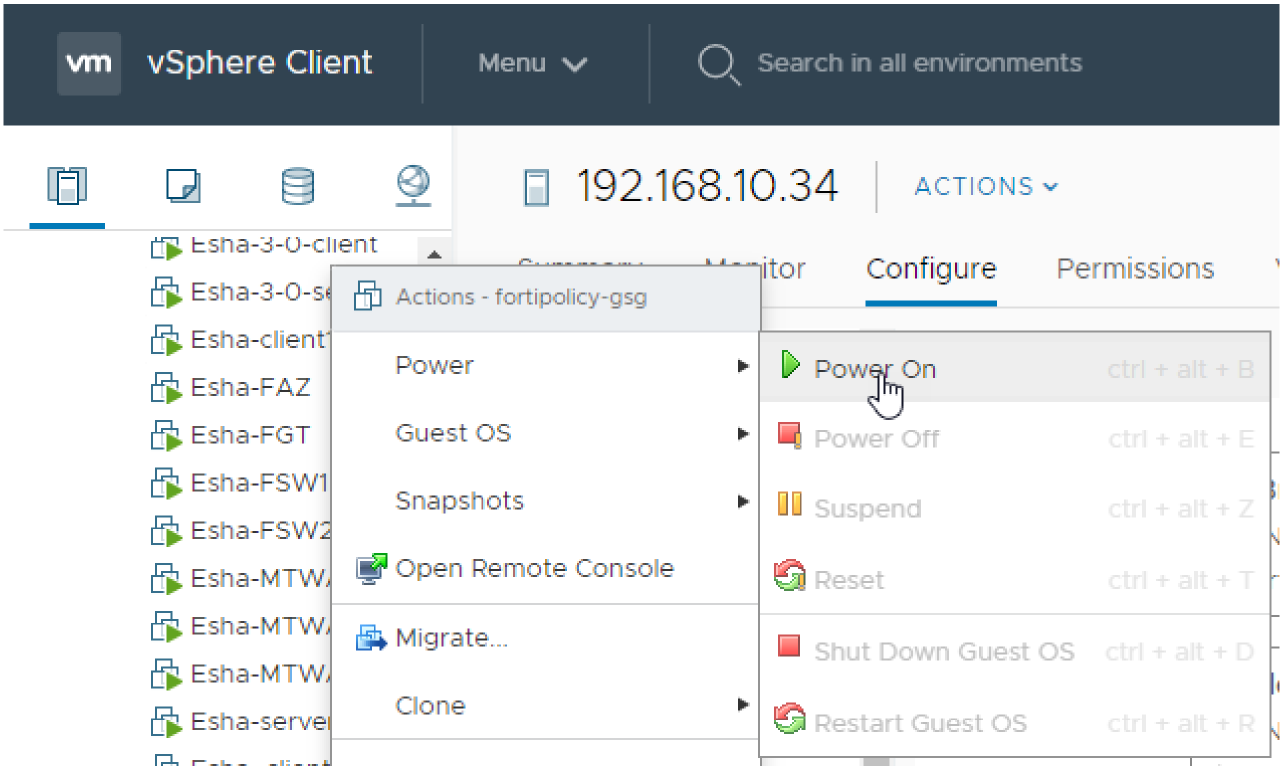
Provisioning type	Deploy from template
Name	fortipolicy-gsg
Template name	fortipolicy-medium
Download size	4.6 GB
Size on disk	550.0 GB
Folder	test-datacenter
Resource	192.168.10.34
Storage mapping	1
All disks	Datastore: datastore-34-00; Format: Thin provision
Network mapping	1
Management Network	test-172.17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

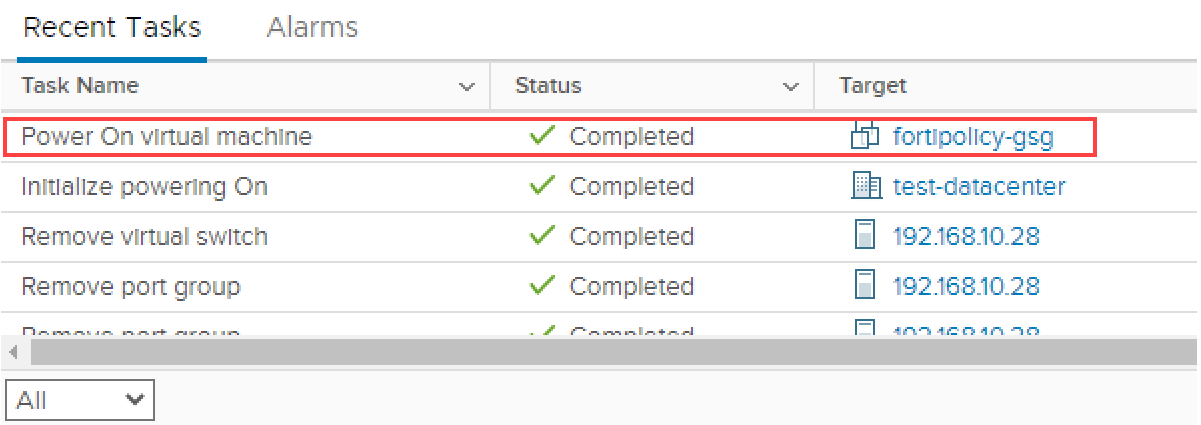


Task Name	Status
Power Off virtual machine	✓ Completed
Delete virtual machine	✓ Completed
Power Off virtual machine	✓ Completed
Deploy OVF template	✓ Completed
Import OVF package	✓ Completed

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

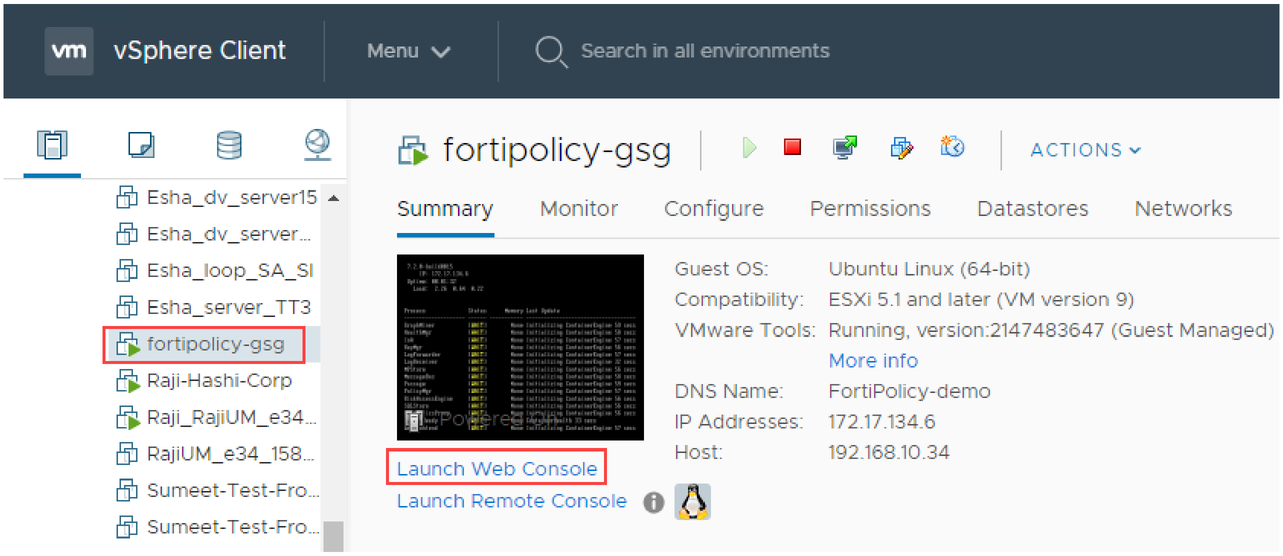


13. Check that the task has completed.



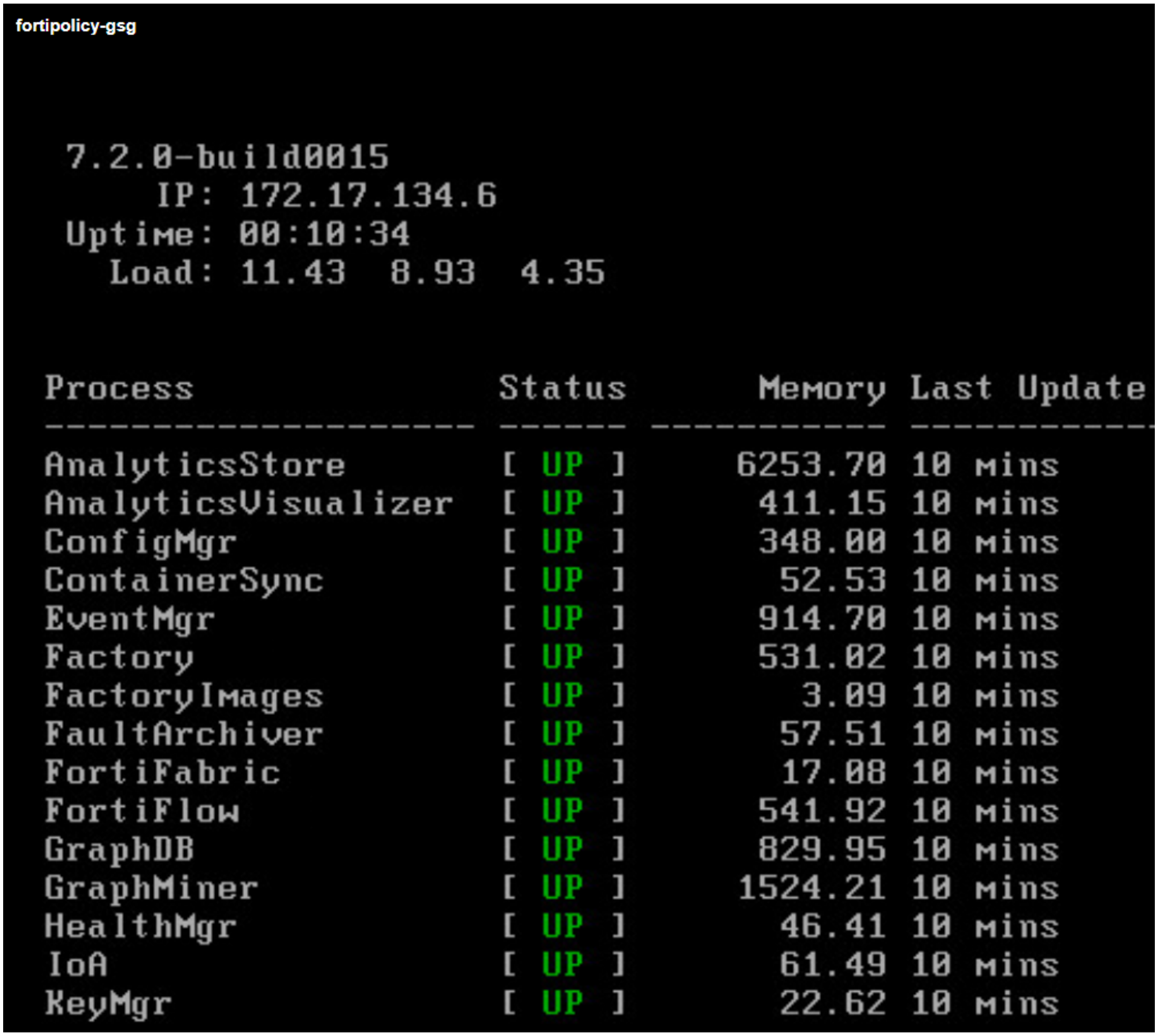
Task Name	Status	Target
Power On virtual machine	✓ Completed	fortipolicy-gsg
Initialize powering On	✓ Completed	test-datacenter
Remove virtual switch	✓ Completed	192.168.10.28
Remove port group	✓ Completed	192.168.10.28
Remove port group	✓ Completed	192.168.10.28

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)
More info
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
```

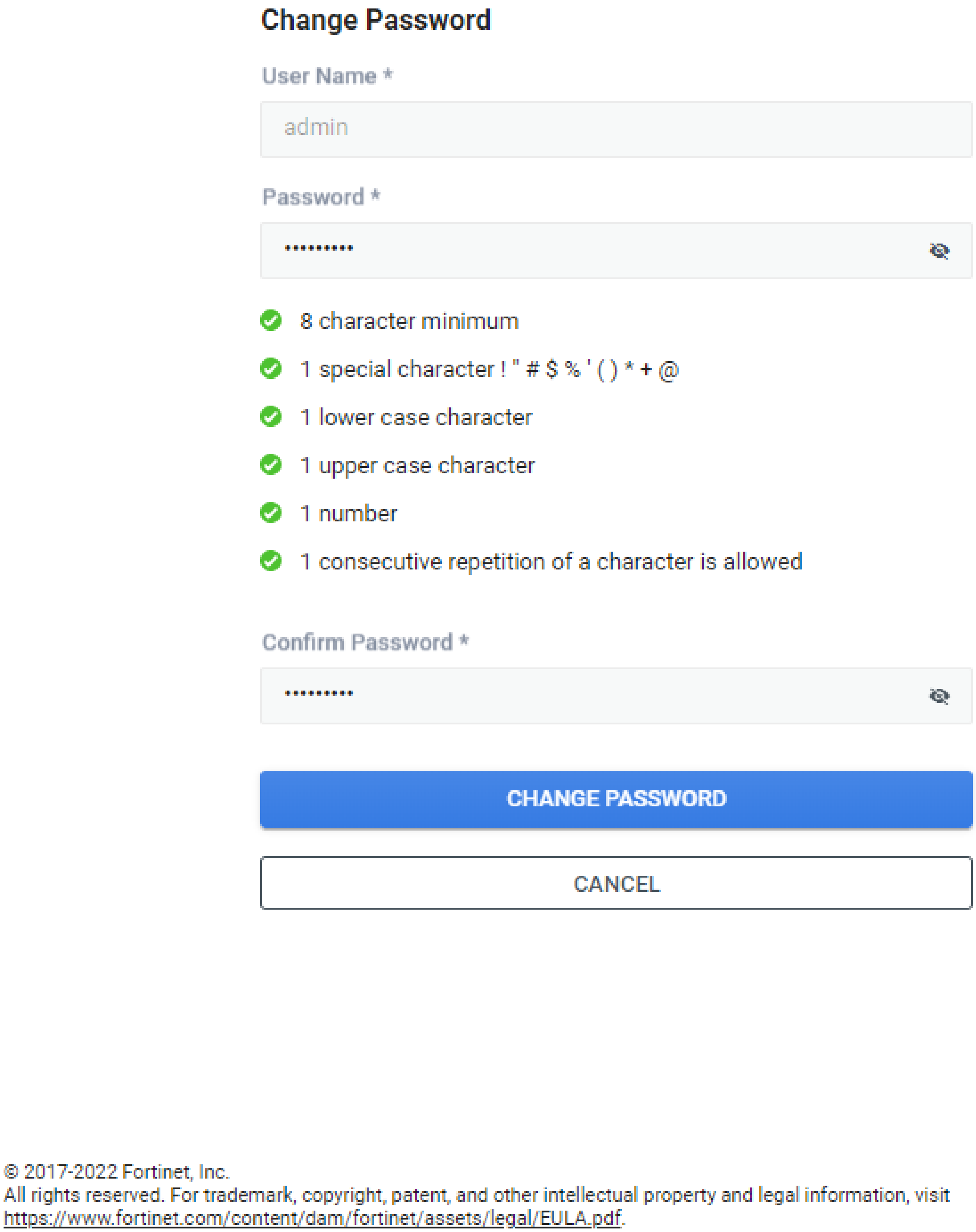
Initial login

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. Click *LOGIN*.
5. 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.

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

9. Click *LOGIN*.

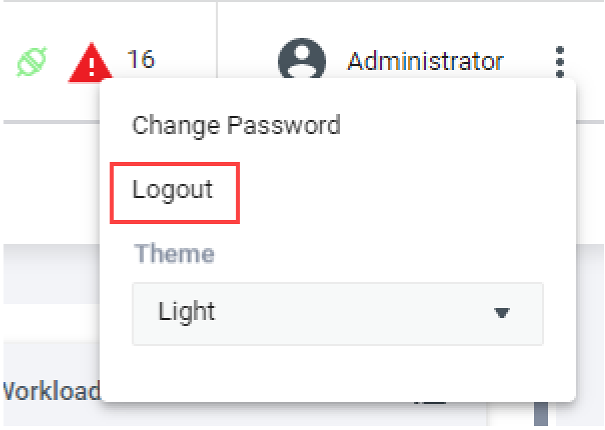
After logging in, go to *Configuration* > *Users* and click the plus sign in the upper right corner to create a new user with the GlobalAdministrator role. After creating the new user, you can delete the `admin` user.

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

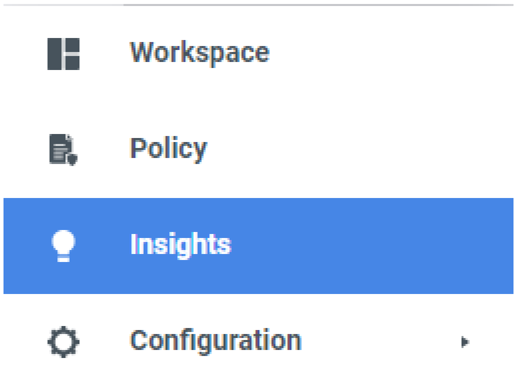
Navigating the FortiPolicy menus

To navigate the FortiPolicy menu, click the icons in the left pane or the tabs at the top of the window.

Click the menu button in the top right corner to log out of the current FortiPolicy console session.



The FortiPolicy menu in the left pane contains the following options:



- *Workspace*—Set up applications and resource groups, as well as review events and logs.
- *Policy*—Lists available access control list (ACL) policies and allows you to add ACL rules and policies, clone policies, delete policies, and export policies.
- *Insights*—Allows you to quickly scan workloads, detections, and operations and offers maps of assets and attacks.
- *Configuration*—Allows you to configure the Security Fabric, add data planes, change your system setup, import certificates, add users, set up notifications, update the software, update your license, and generate reports.

Configuring FortiPolicy

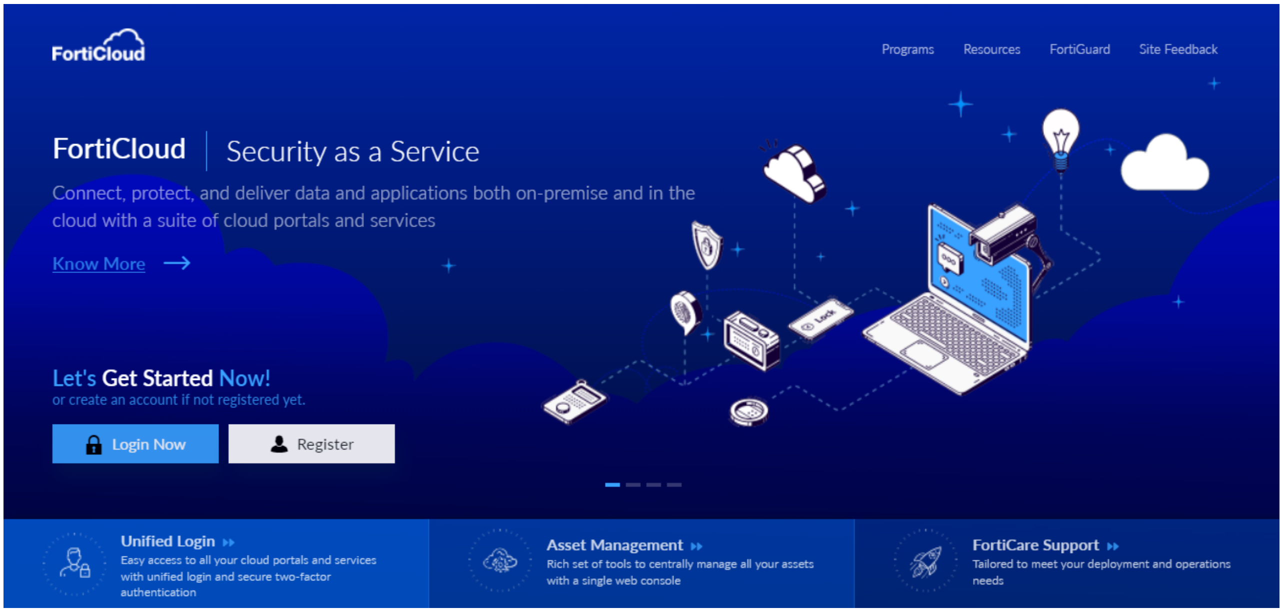
To configure FortiPolicy, complete the following procedures:

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

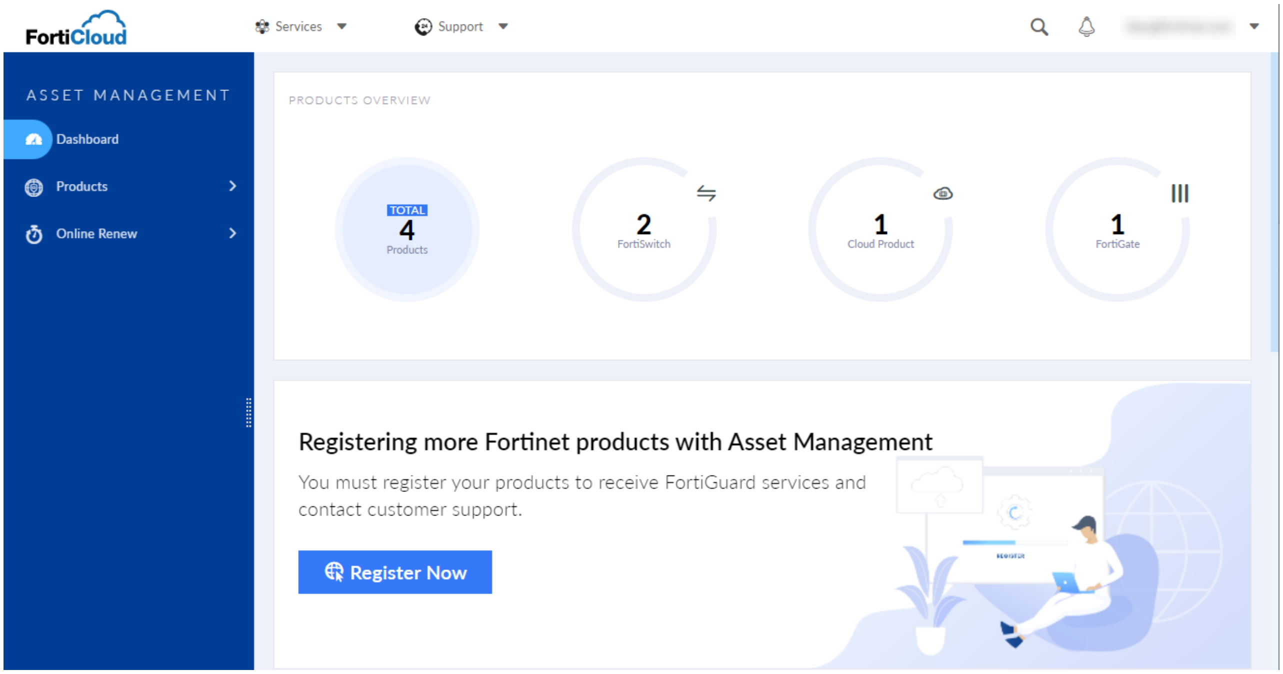
Importing the FortiPolicy license file

To import the FortiPolicy license file:

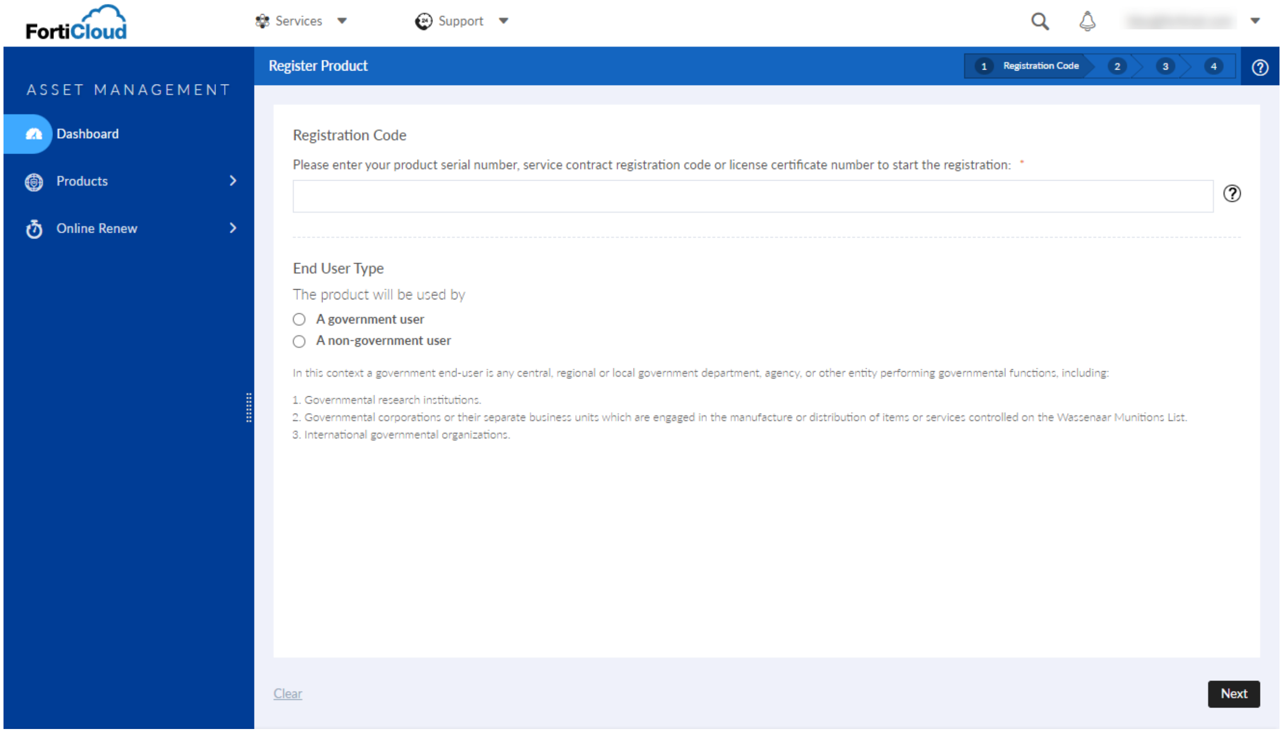
1. Go to FortiCloud and create a new account or log in with an existing account.


FortiCloud
Programs
Resources
FortiGuard
Site Feedback
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
Know More
Let's Get Started Now!
or create an account if not registered yet.
Login Now
Register
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.



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

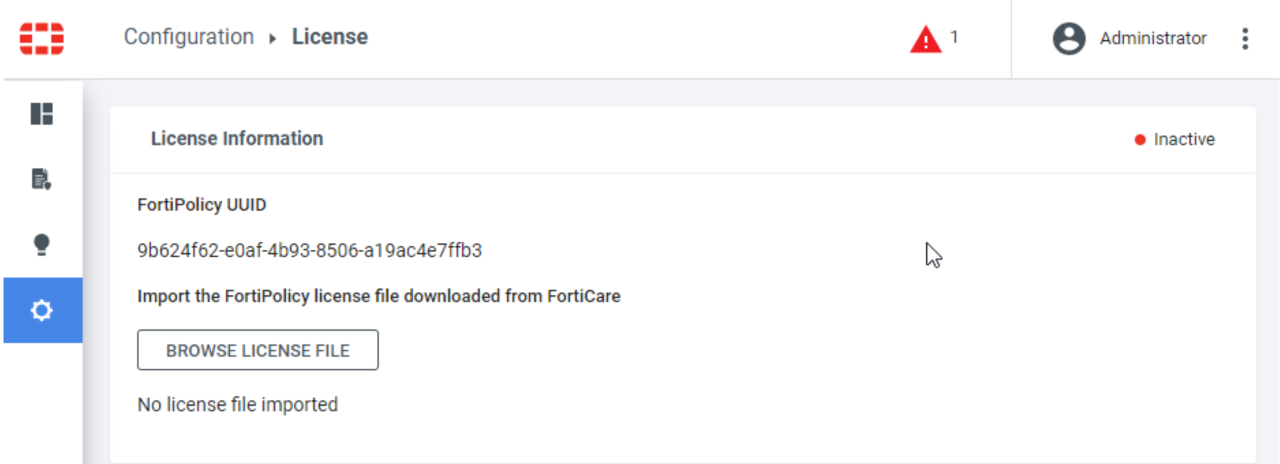
○ A government user

○ 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.



FortiPolicy UUID

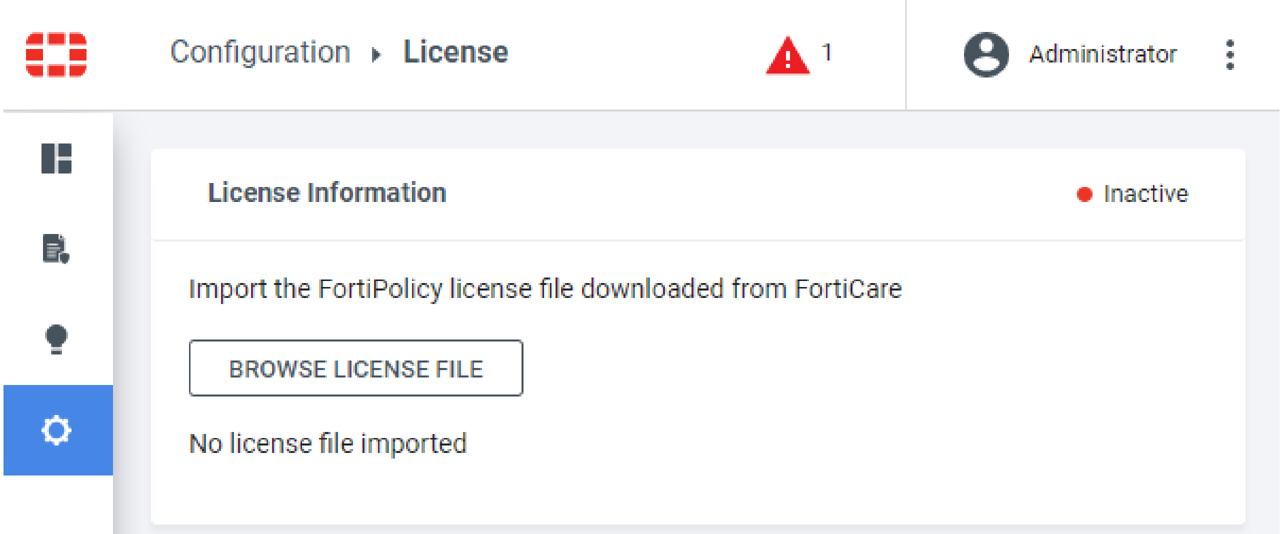
9b624f62-e0af-4b93-8506-a19ac4e7ffb3

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.

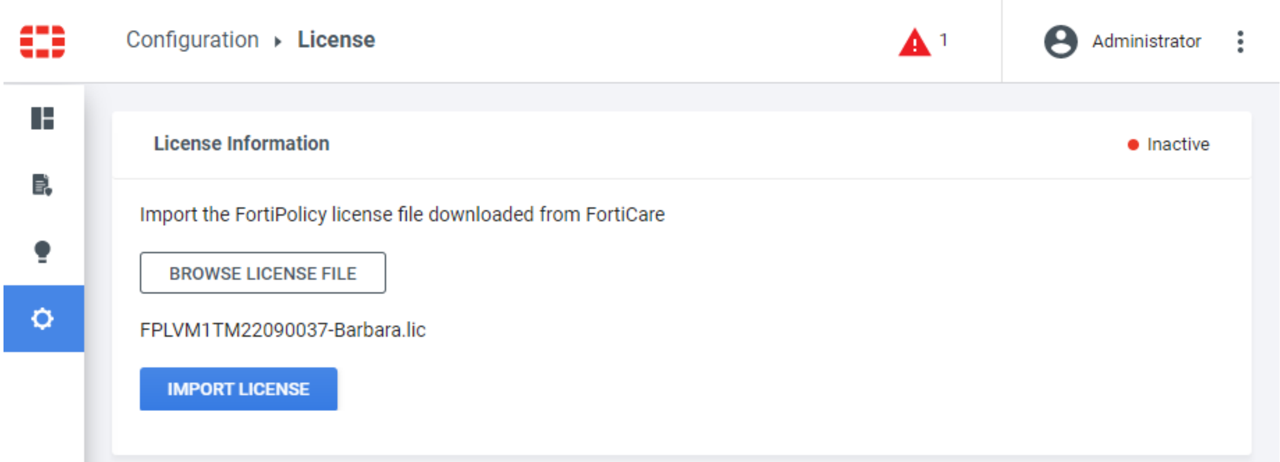
5. In FortiPolicy, go to *Configuration* > *License* and click *BROWSE LICENSE FILE*.



Import the FortiPolicy license file downloaded from FortiCare

No license file imported

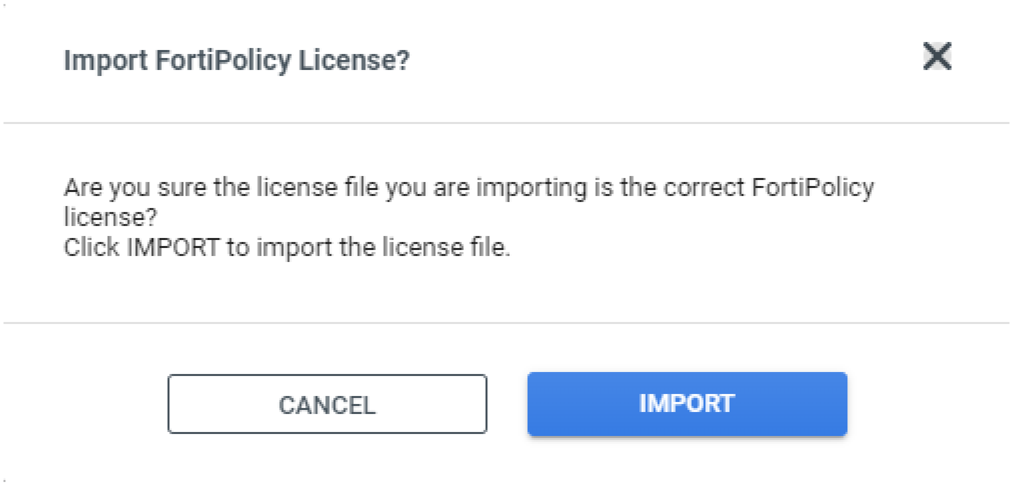
6. Select your FortiPolicy license file.



Import the FortiPolicy license file downloaded from FortiCare

FPLVM1TM22090037-Barbara.lic

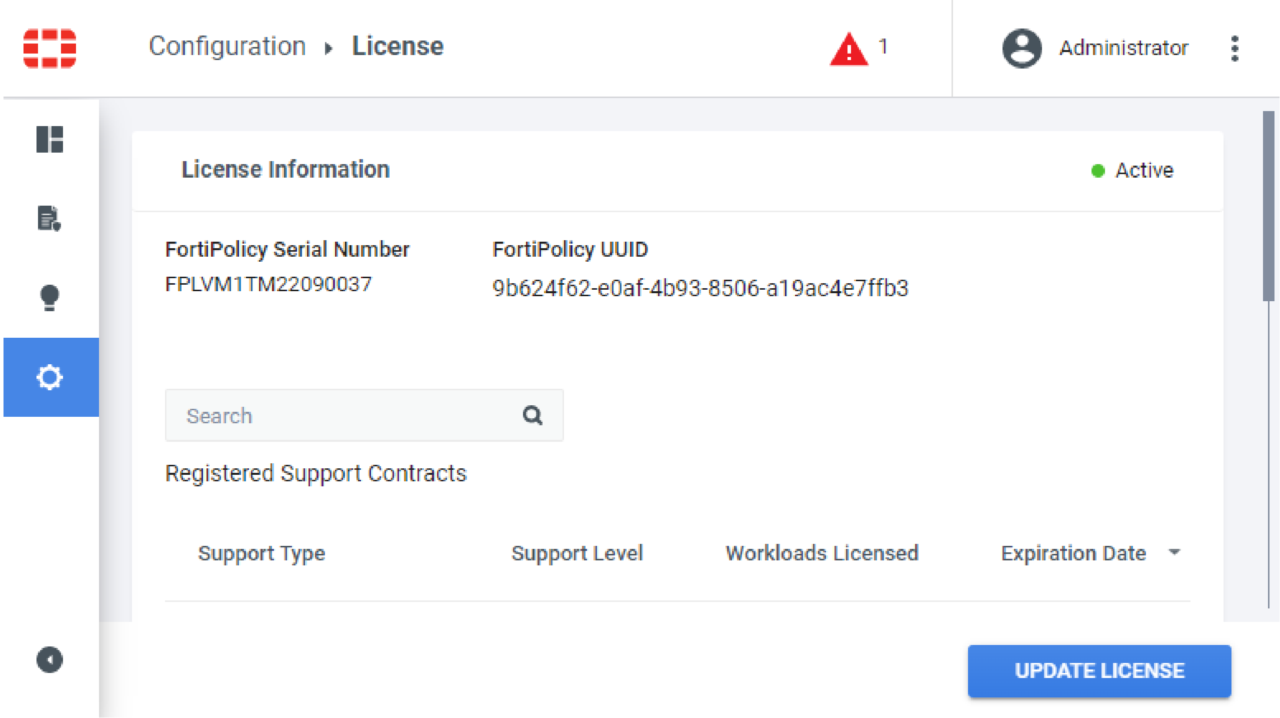
7. Click *IMPORT LICENSE*.



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.



License Information ● Active

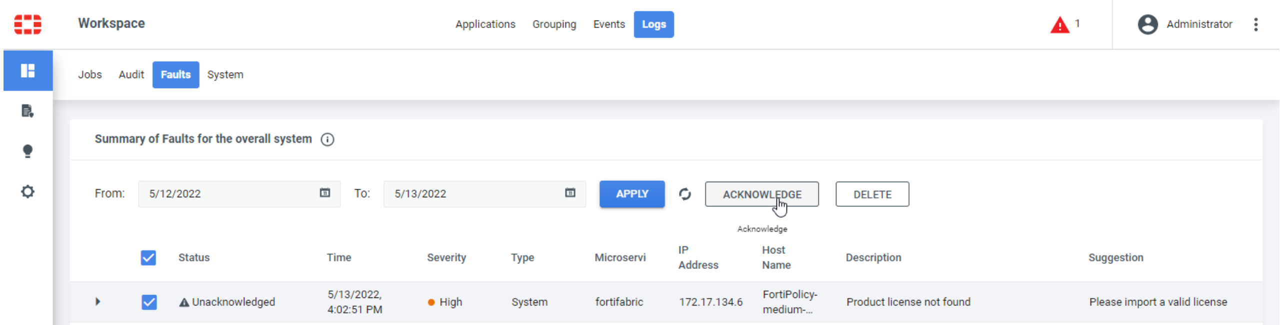
FortiPolicy Serial Number: FPLVM1TM22090037

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 fault and then ignore it.



Summary of Faults for the overall system

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

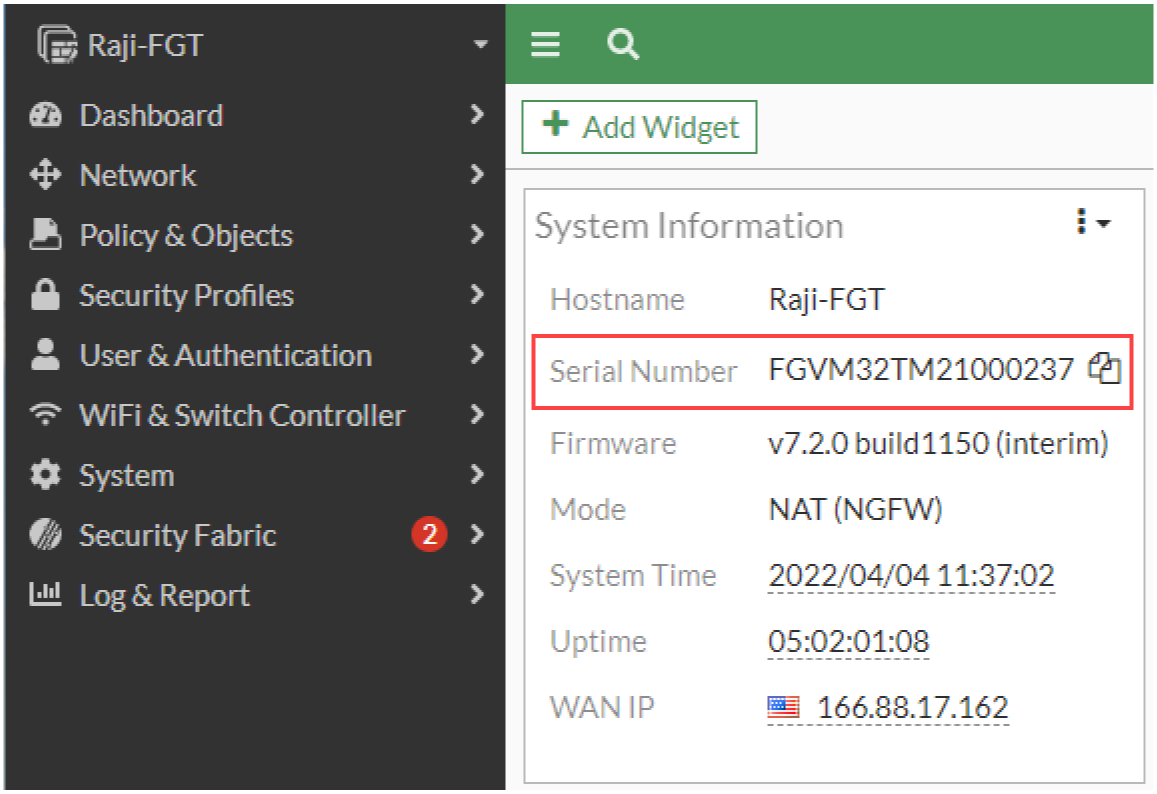
☑	Status	Time	Severity	Type	Microservi	IP Address	Host Name	Description	Suggestion
☑	Unacknowledged	5/13/2022, 4:02:51 PM	● High	System	fortifabric	172.17.134.6	FortiPolicy-medium-...	Product license not found	Please import a valid license

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.

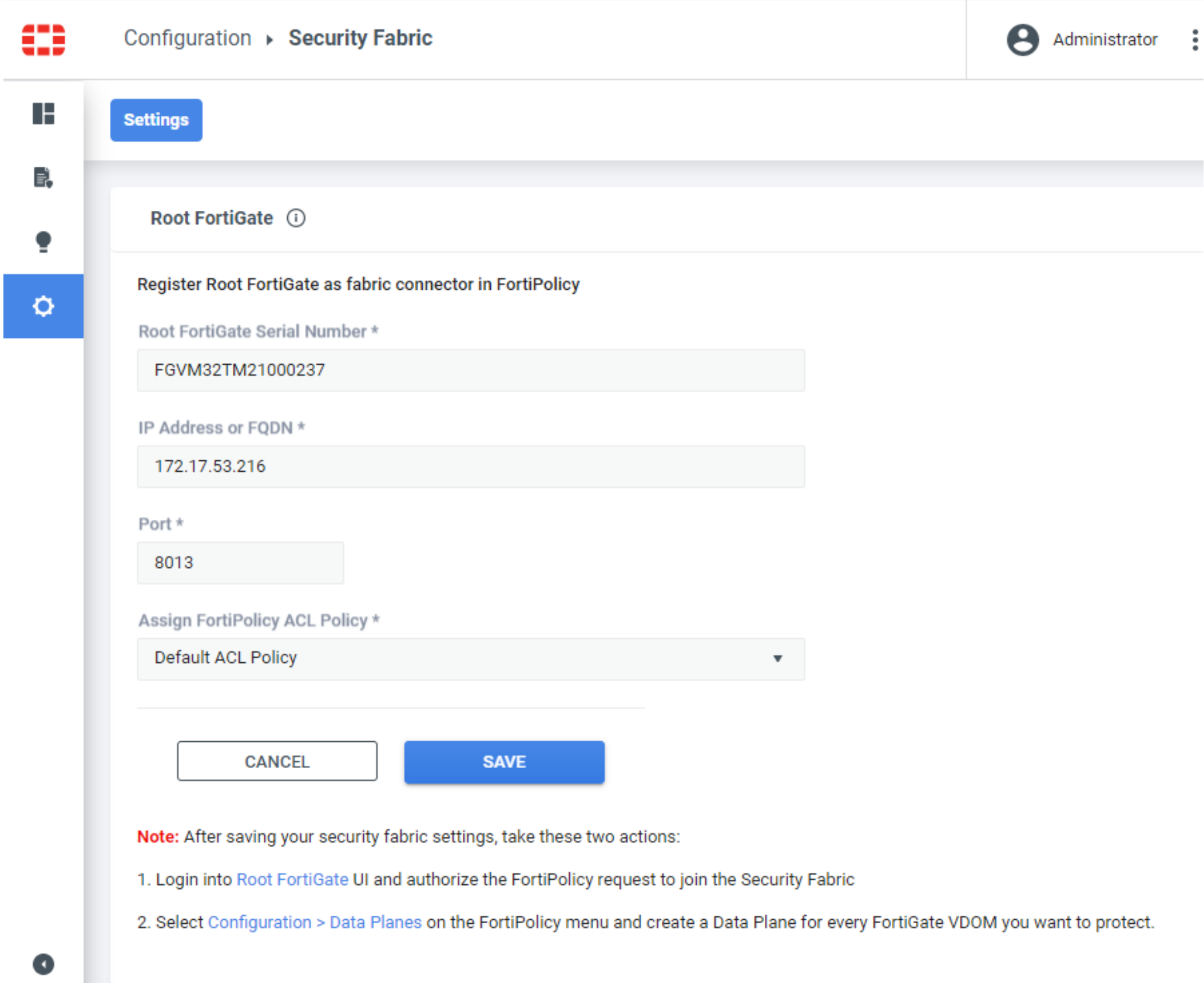


System Information

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:

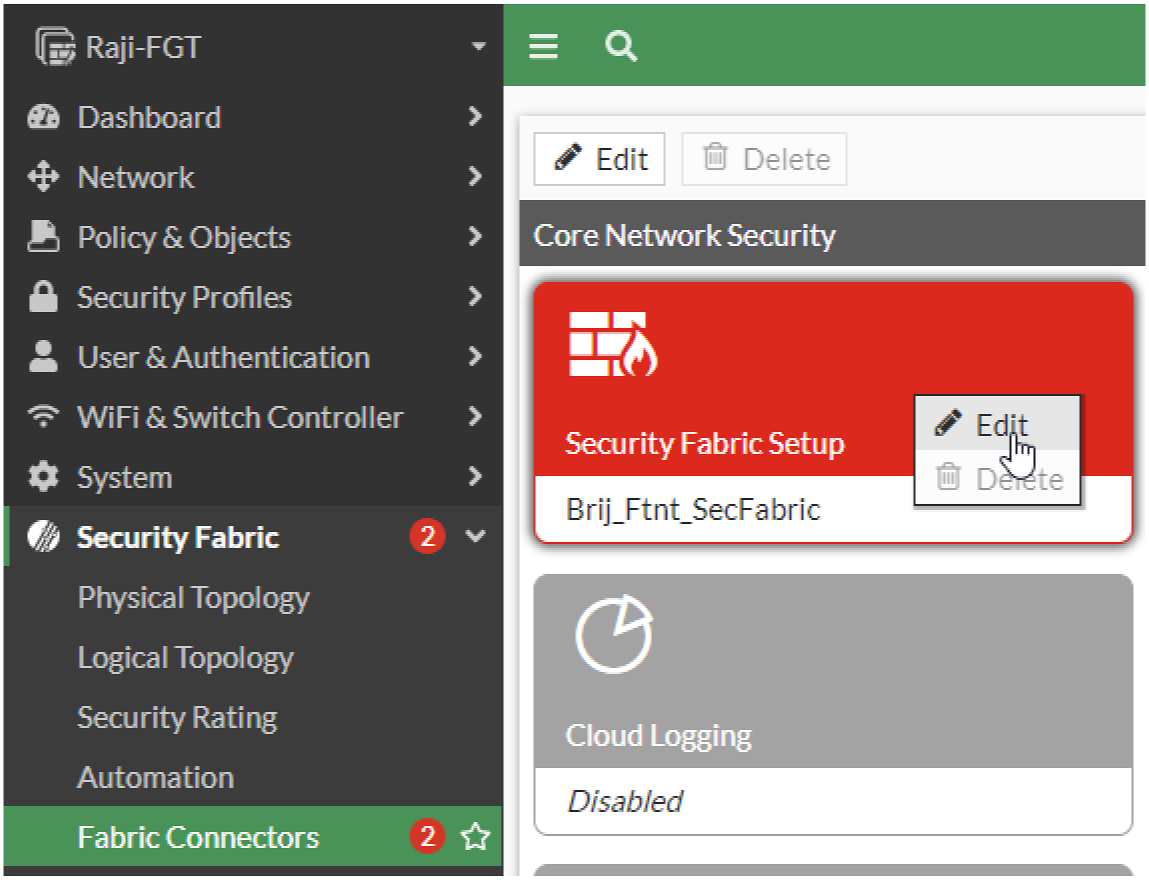
1. Login into Root FortiGate UI and authorize the FortiPolicy request to join the Security Fabric

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*.

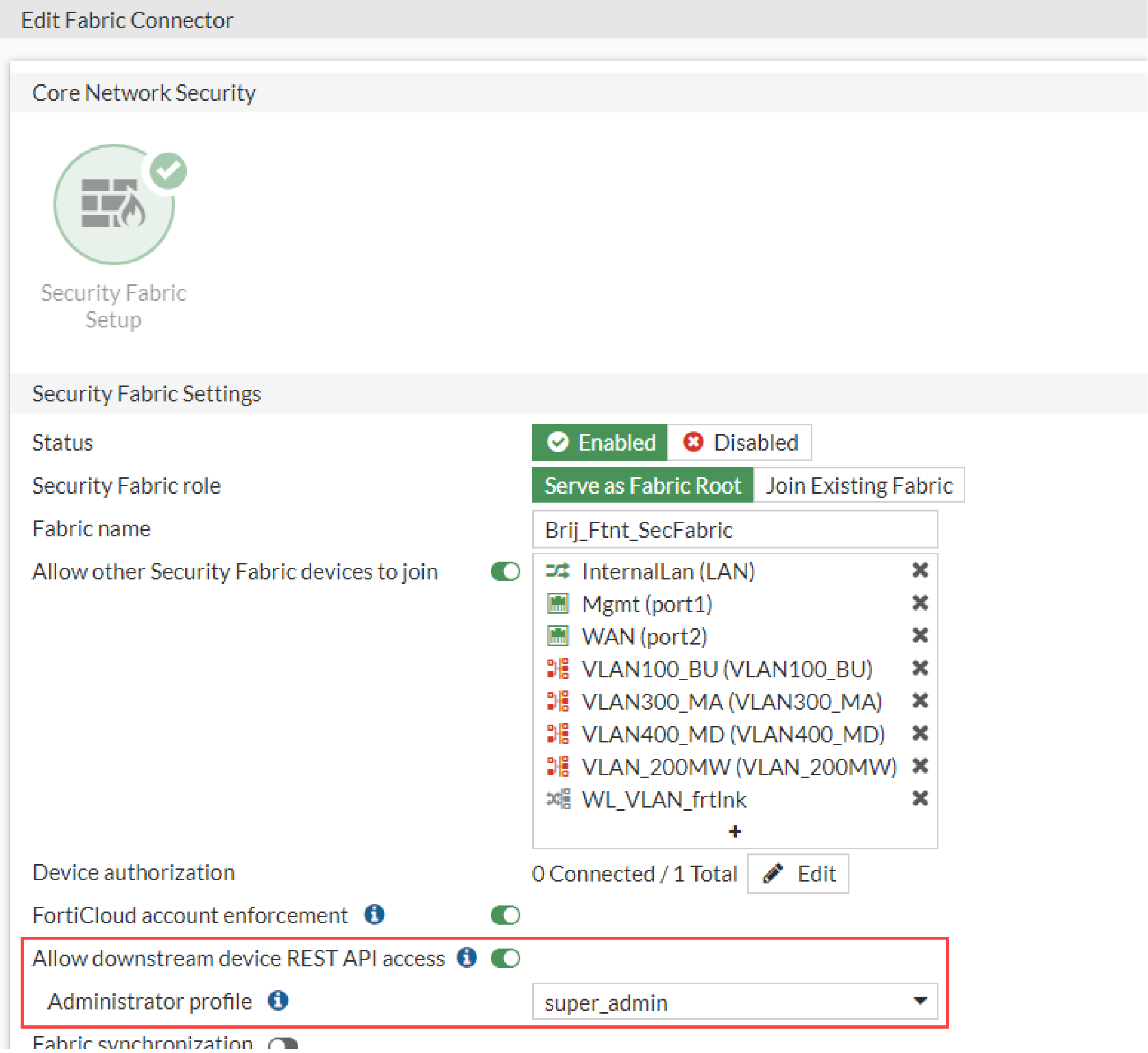
3. Configure the settings in each FortiGate device (root FortiGate and child FortiGate devices) in the Security Fabric.

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*.



Edit Fabric Connector

Core Network Security

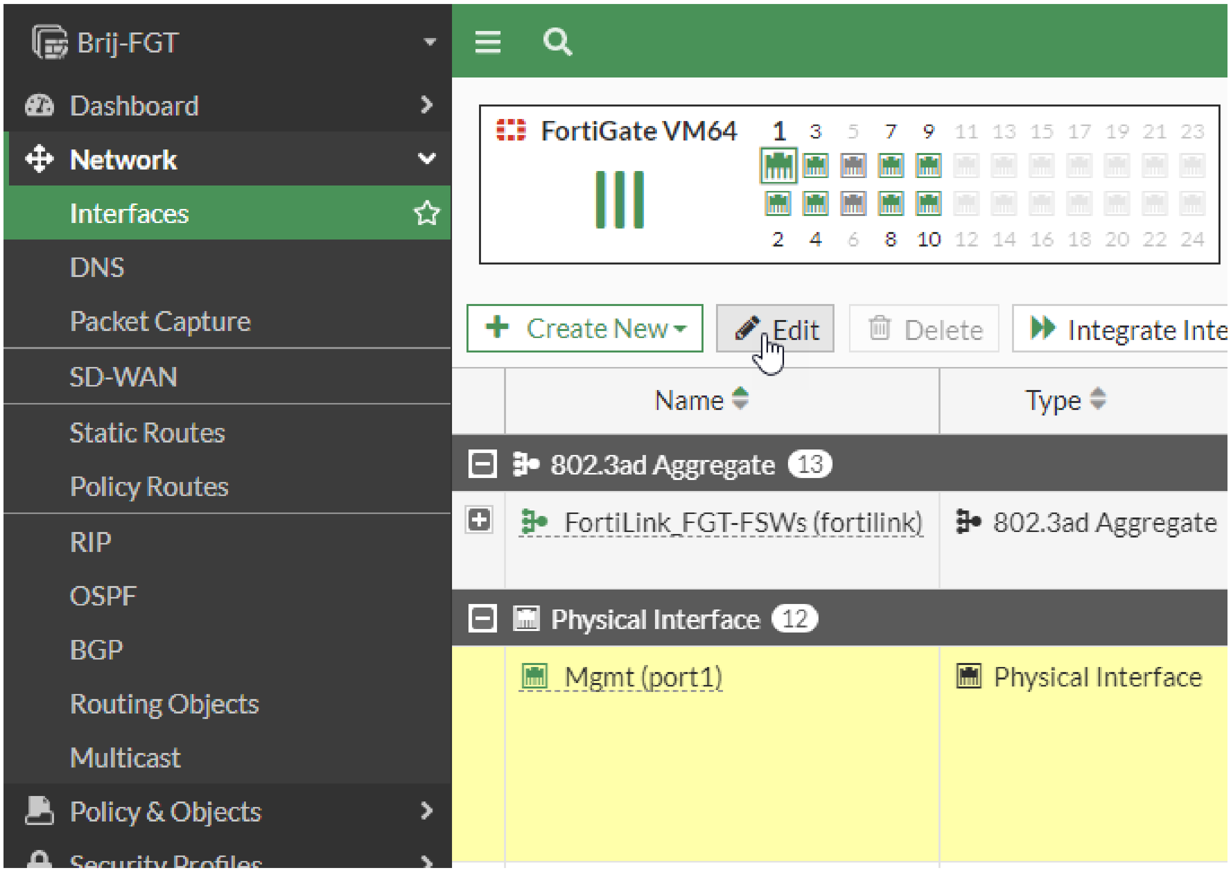
Security Fabric Settings

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 ℹ ●	
Allow downstream device REST API access ℹ ●	
Administrator profile ℹ	super_admin ▾
Fabric synchronization ○	

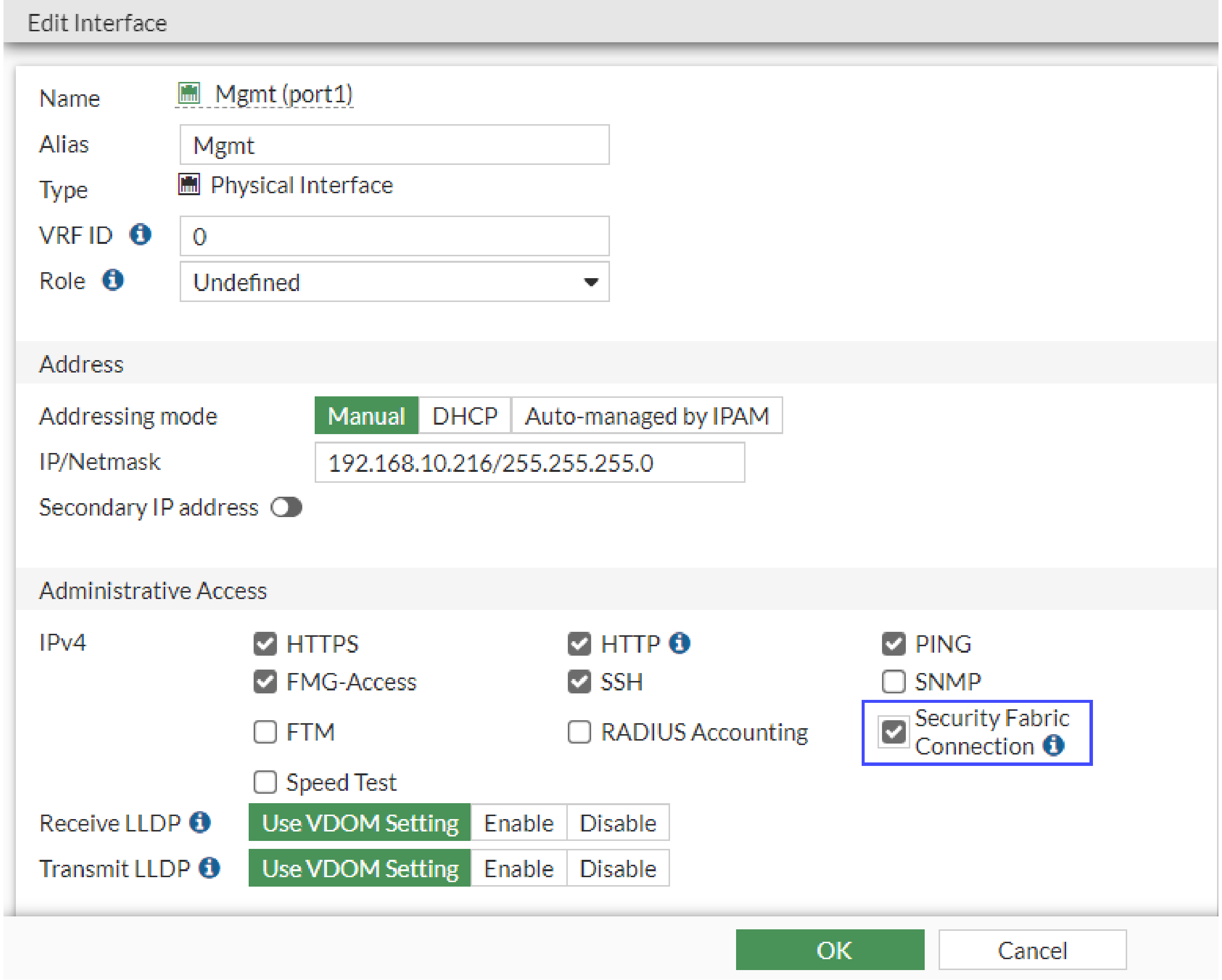
d. Click *OK*.

4. In the root FortiGate device, configure the management port.

a. Go to *Network* > *Interfaces*, select the *Mgmt* port, and click *Edit*.



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 ○

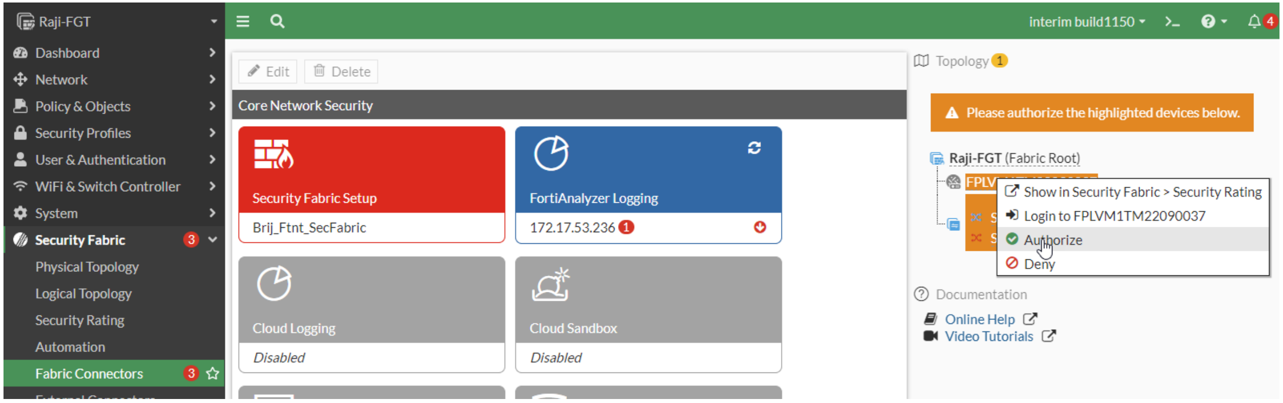
Administrative Access

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

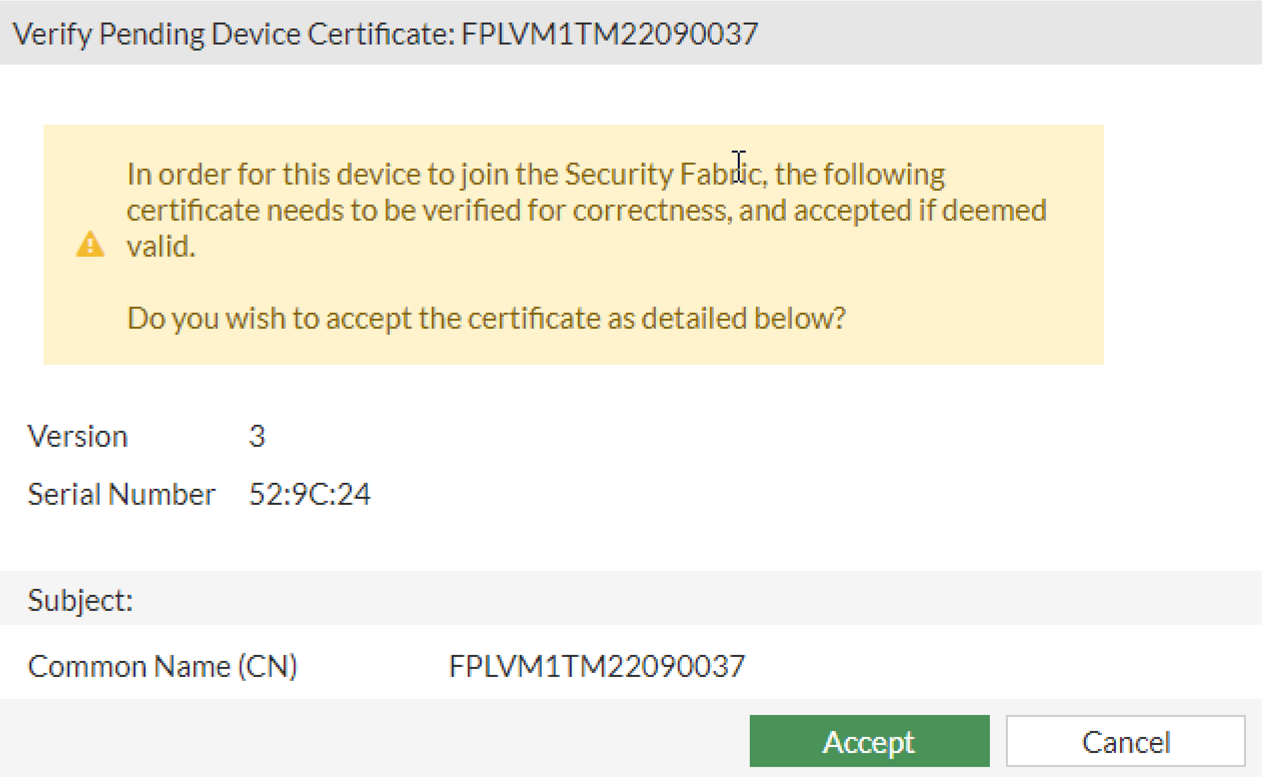
Receive LLDP: [✓ Use VDOM Setting] Enable Disable
Transmit LLDP: [✓ Use VDOM Setting] Enable Disable

OK Cancel

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



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

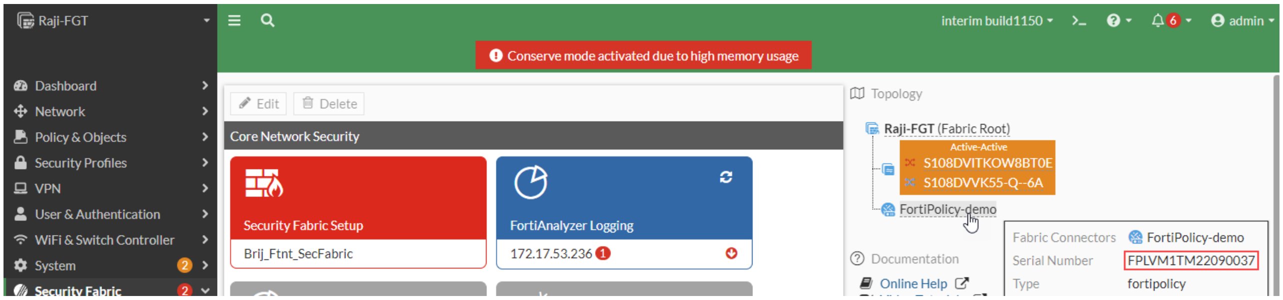
Subject:

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):

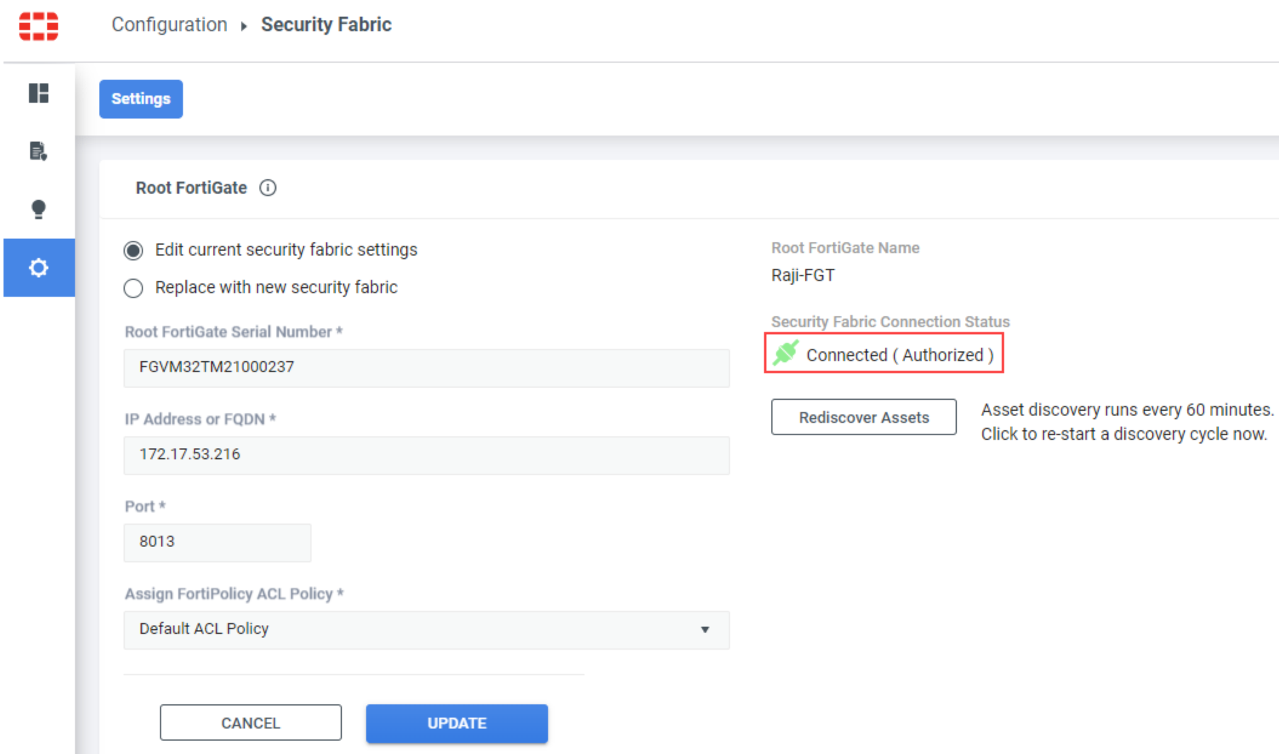
```
config system csf
   config fabric-connector
      edit <FortiPolicy_serial_number>
         set configuration-write-access enable
         set accprofile super_admin
      next
   end
end
```

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



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

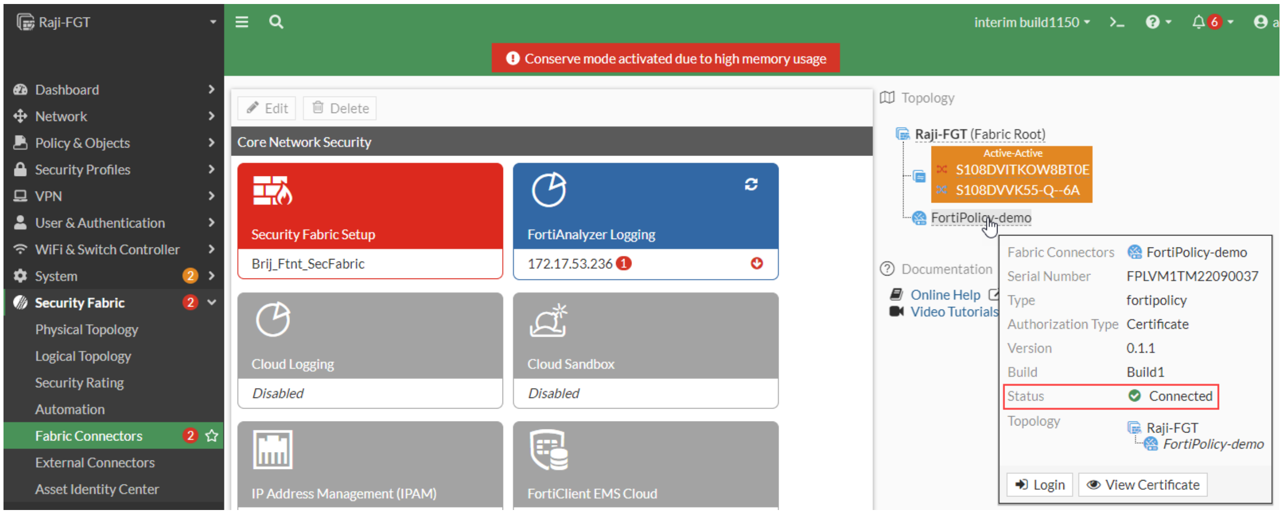
Assign FortiPolicy ACL Policy * Default ACL Policy

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 1

Cloud Logging: *Disabled*

Cloud Sandbox: *Disabled*

Raji-FGT (Fabric Root)

Active-Active

S108DVITKOW8BT0E

S108DVVK55-Q--6A

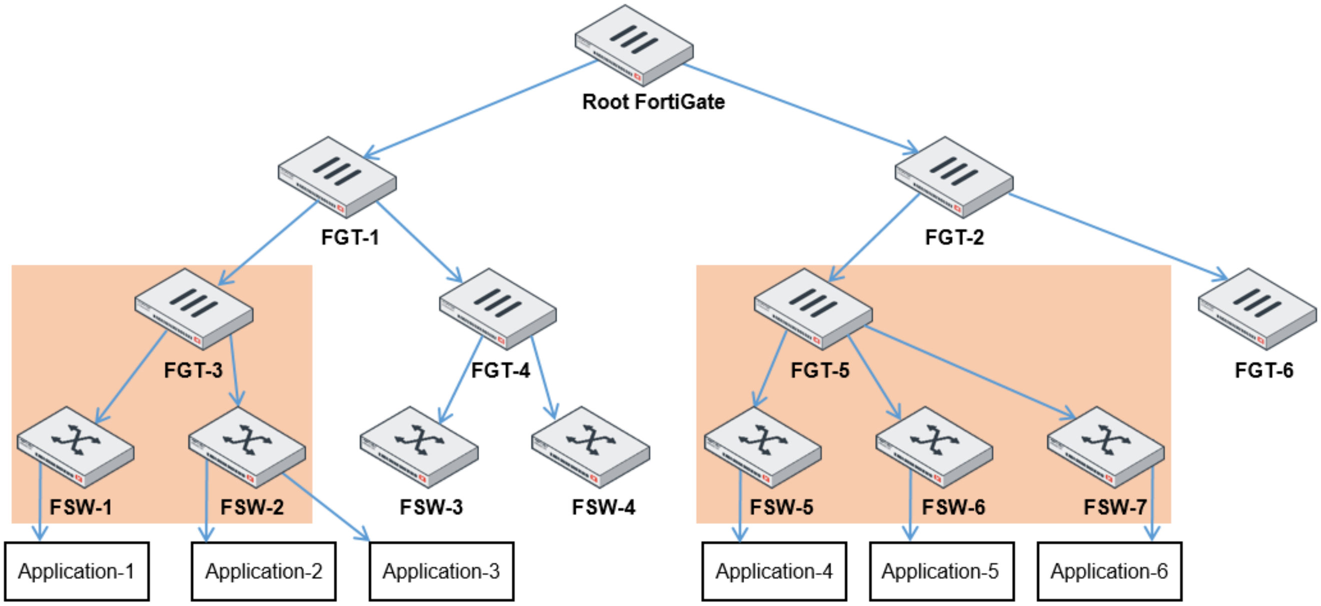
FortiPolicy-demo

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 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.

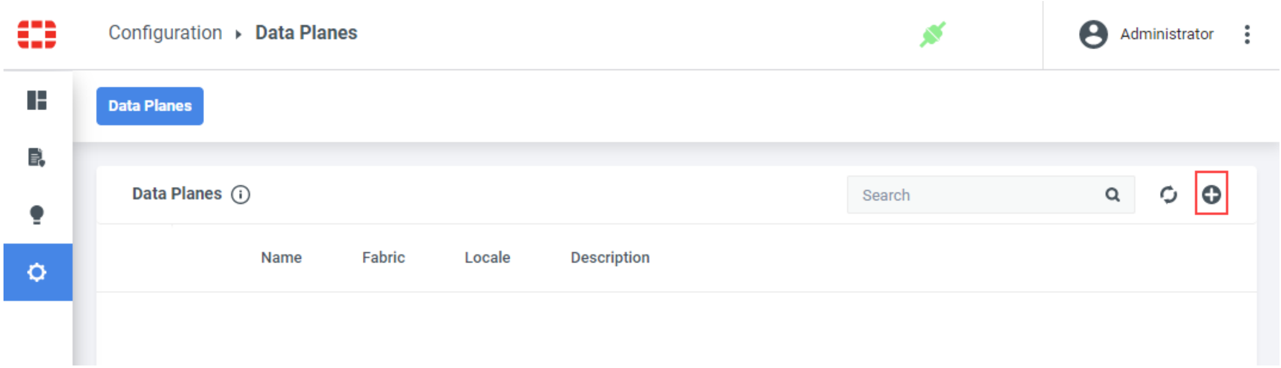
For example, in the following topology, you would create a data plane for FGT-3 to secure Application-1, Application-2, and Application-3. You would create a second data plane for FGT-5 to secure Application-4, Application-5, and Application-6.



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:

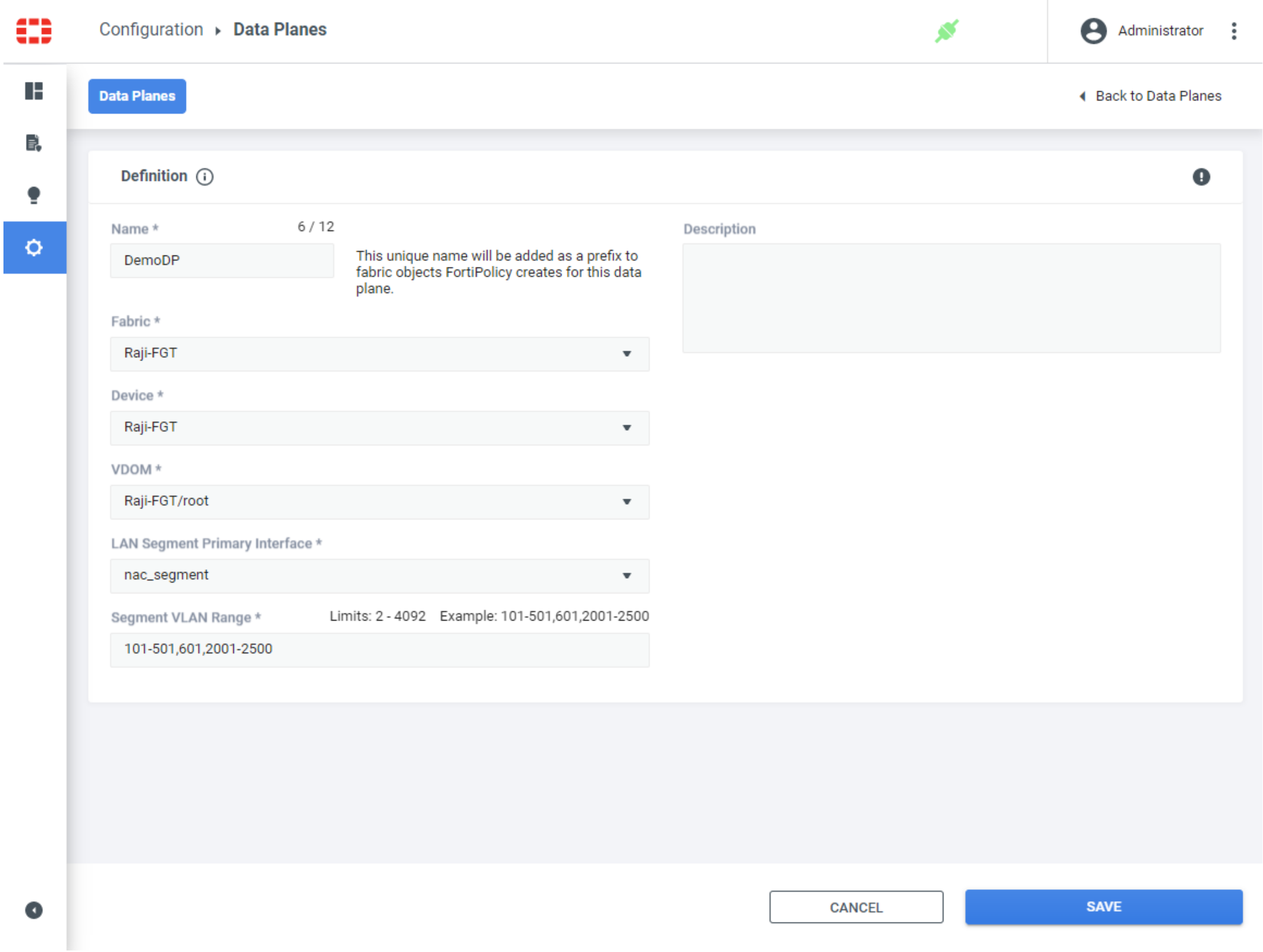
1. Go to *Configuration* > *Data Planes*.
2. Click the plus sign on the upper right corner of the *Data Planes* page.



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

   This unique name will be added as a prefix to all fabric objects that FortiPolicy creates for this 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

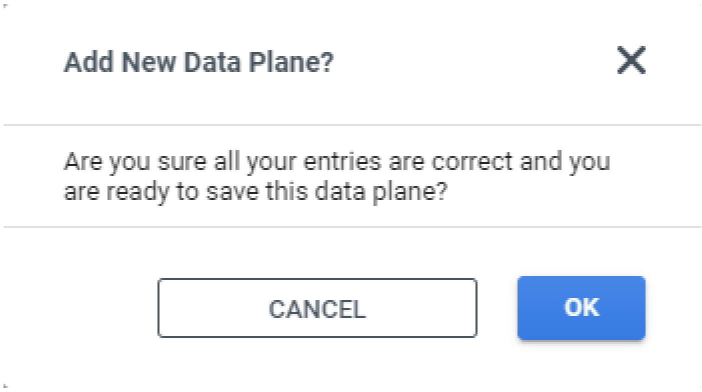
VDOM *
Raji-FGT/root

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*.

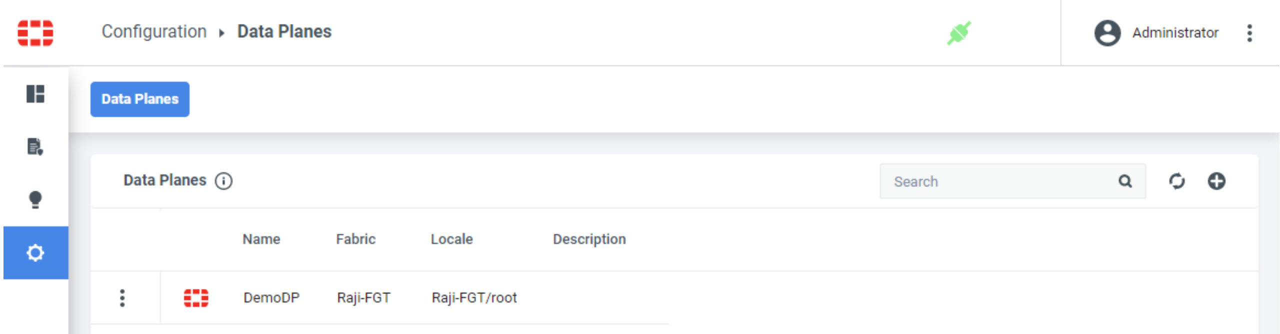
10. In the *Add New Data Plane?* dialog, click *OK*.



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	

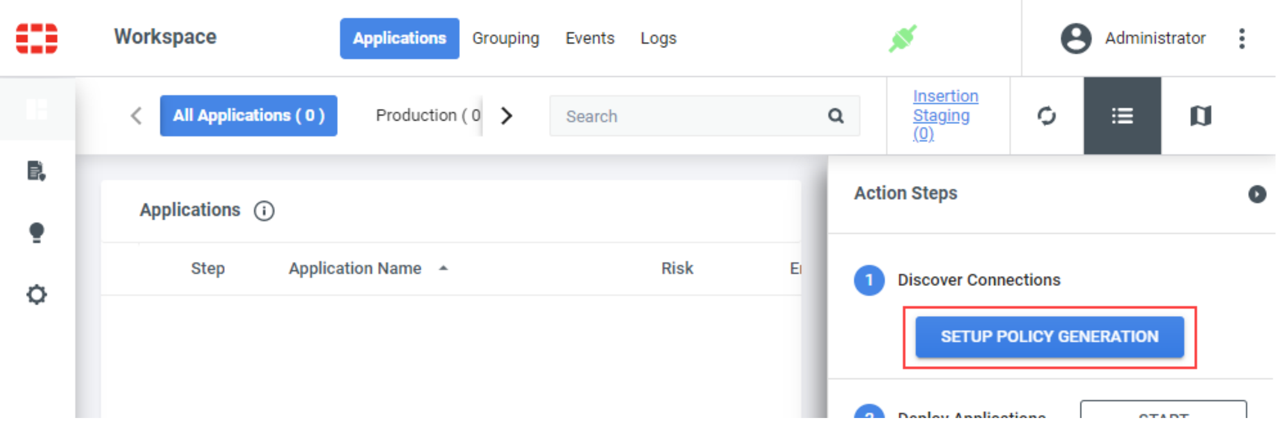
11. Repeat steps 2-10 for each FortiGate device connected to application workloads that need to be secured.

Setting up Policy Generation

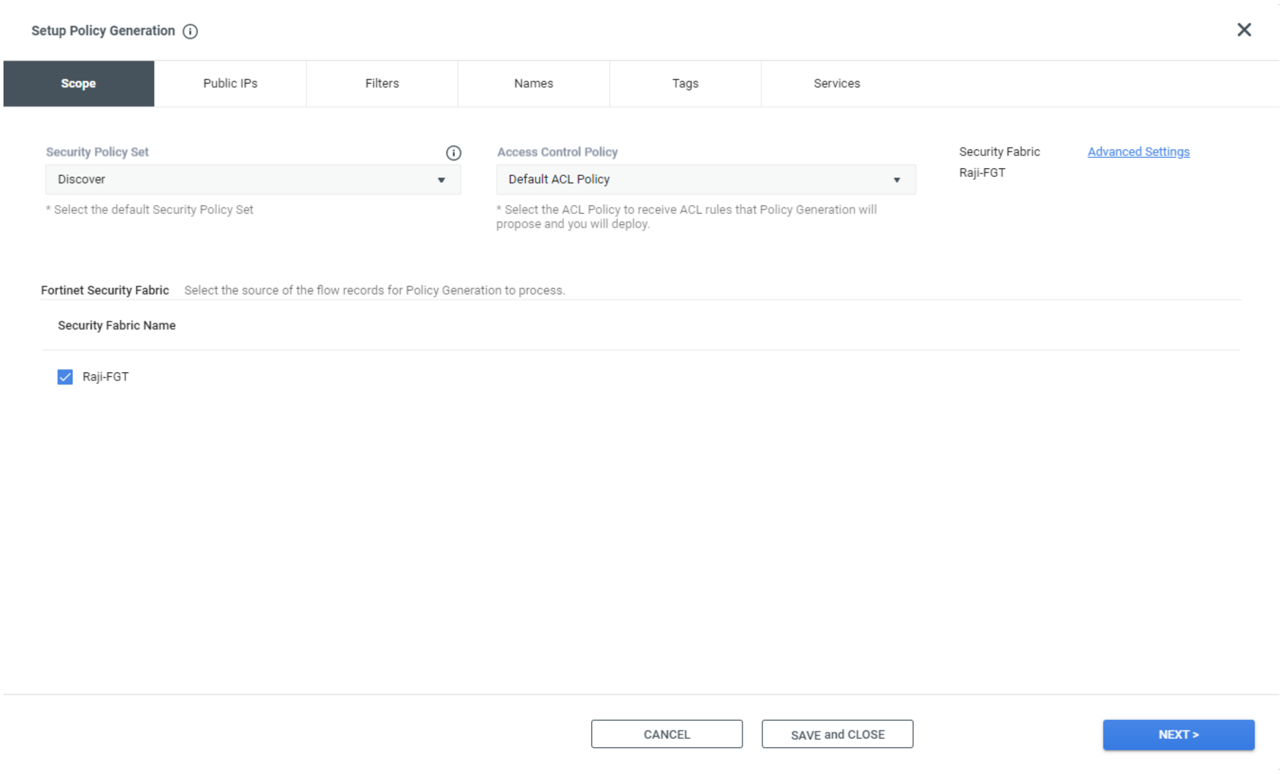
Automated Policy Generation provides the automated discovery of connections, tiers, applications, and network services.

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.



Setup Policy Generation

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.

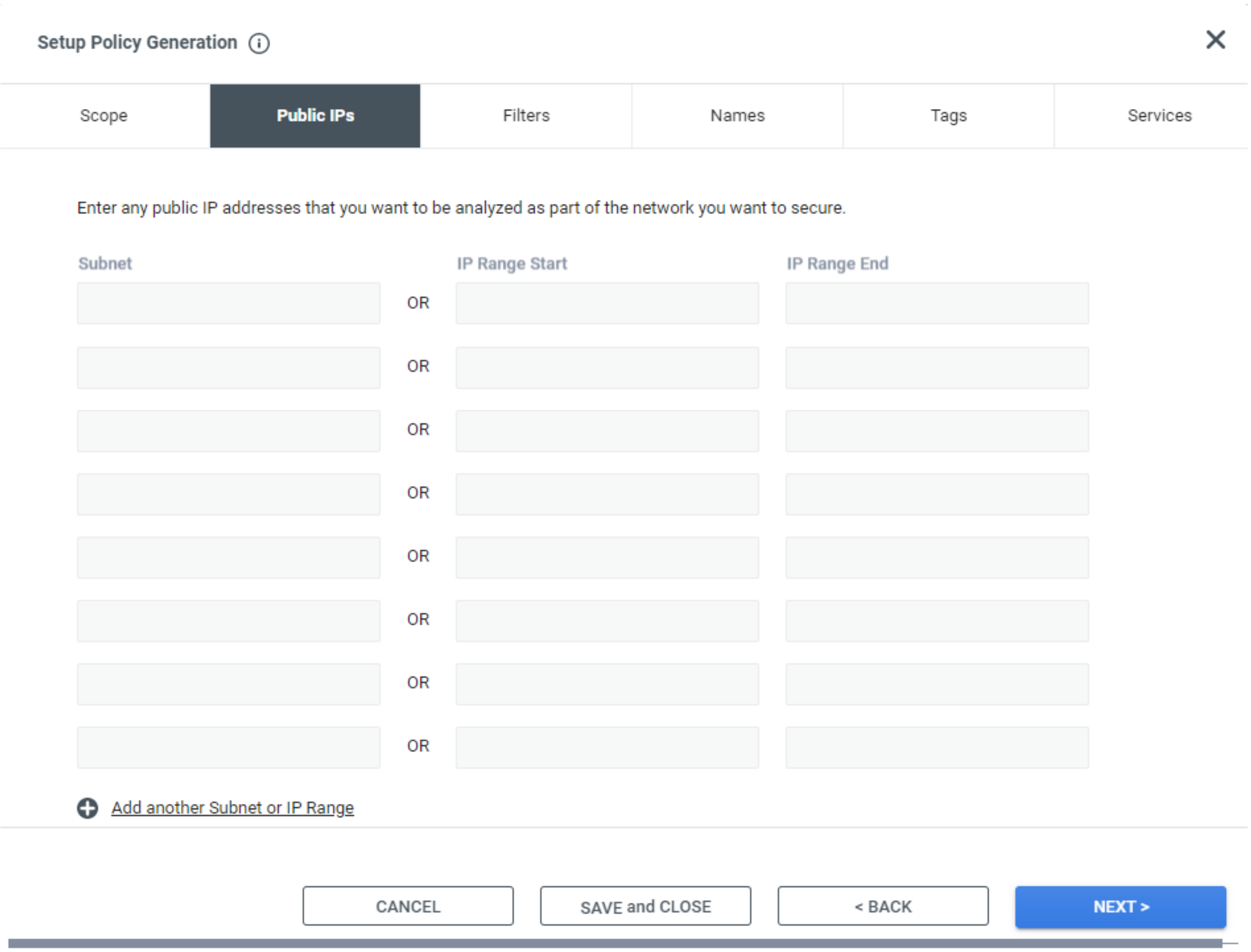
Security Fabric: Raji-FGT

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

Security Fabric Name
☑ Raji-FGT

6. Click *Next*.

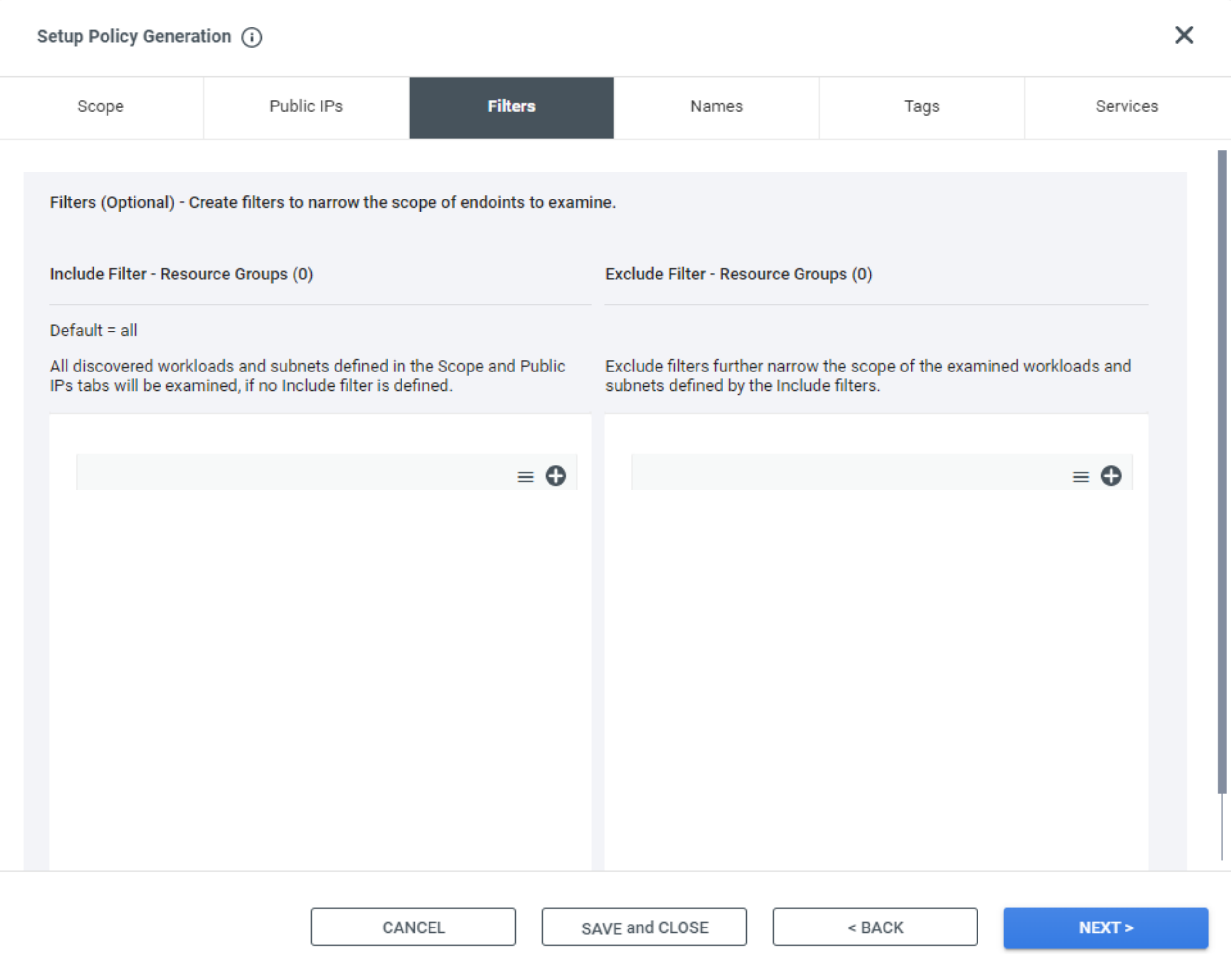
7. Enter any public IP addresses that you want to be analyzed as part of the network you are securing.



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.



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

Include Filter - Resource Groups (0)

Default = all

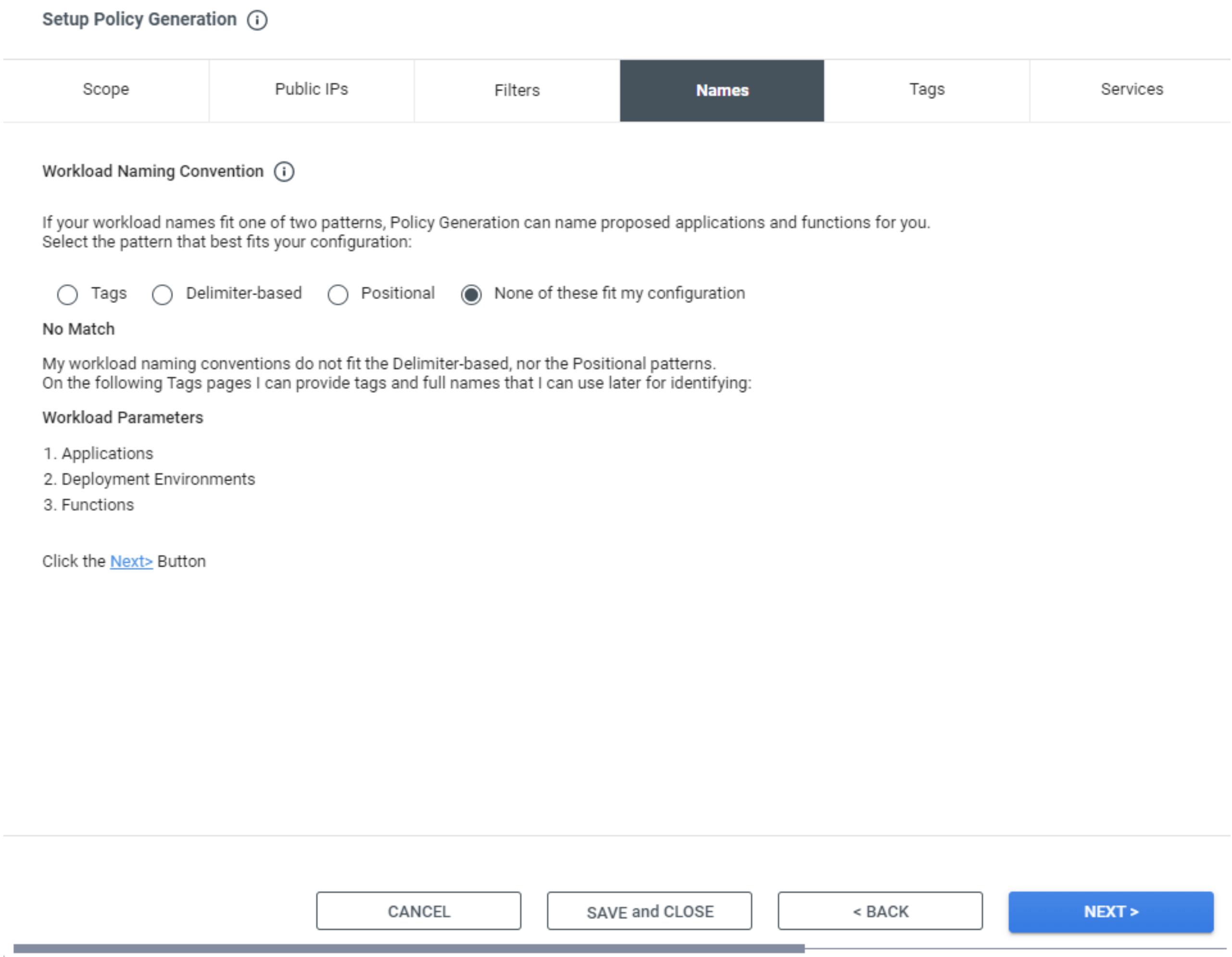
All discovered workloads and subnets defined in the Scope and Public IPs tabs will be examined, if no Include filter is defined.

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:

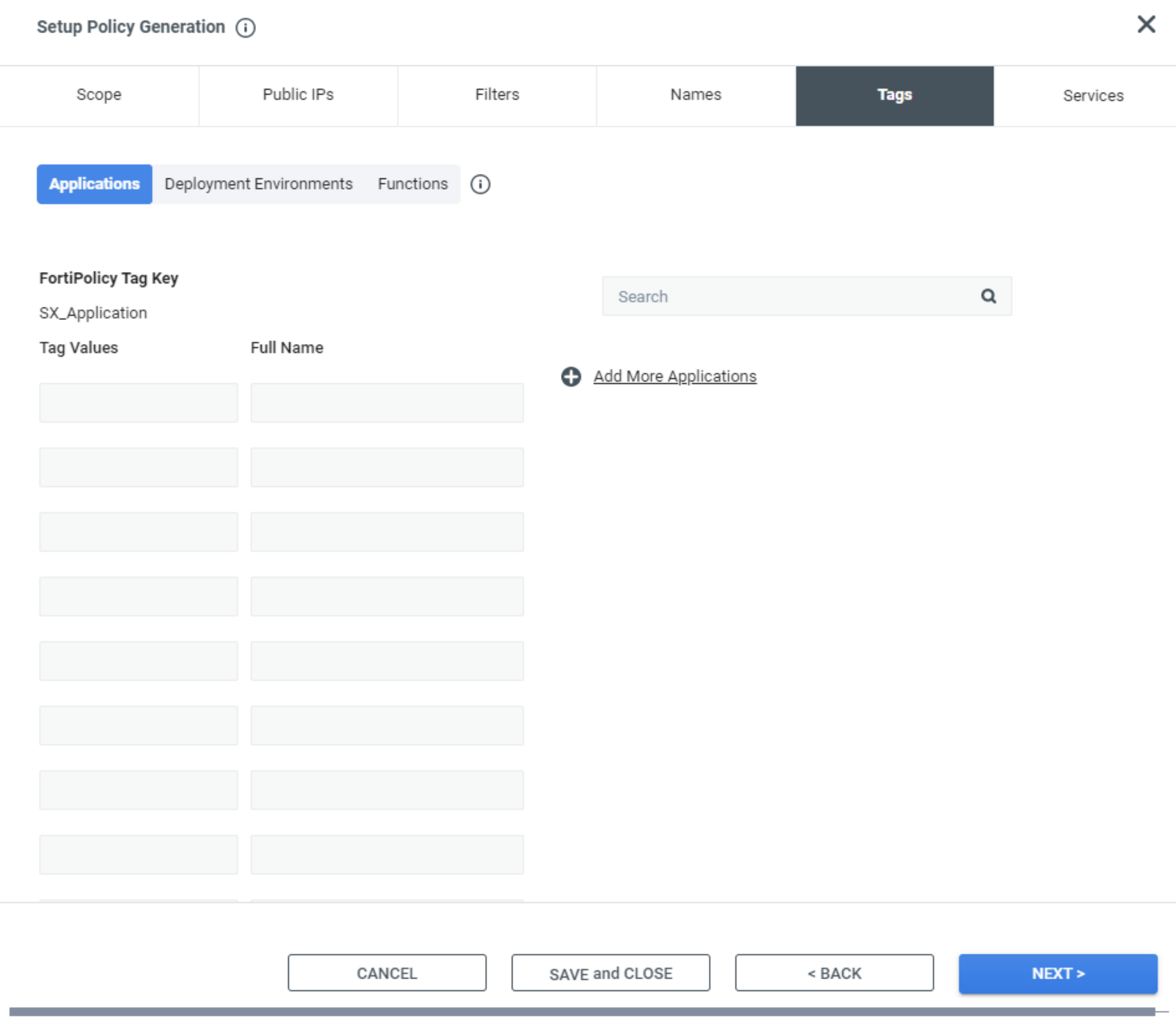
Workload Parameters

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.



FortiPolicy Tag Key

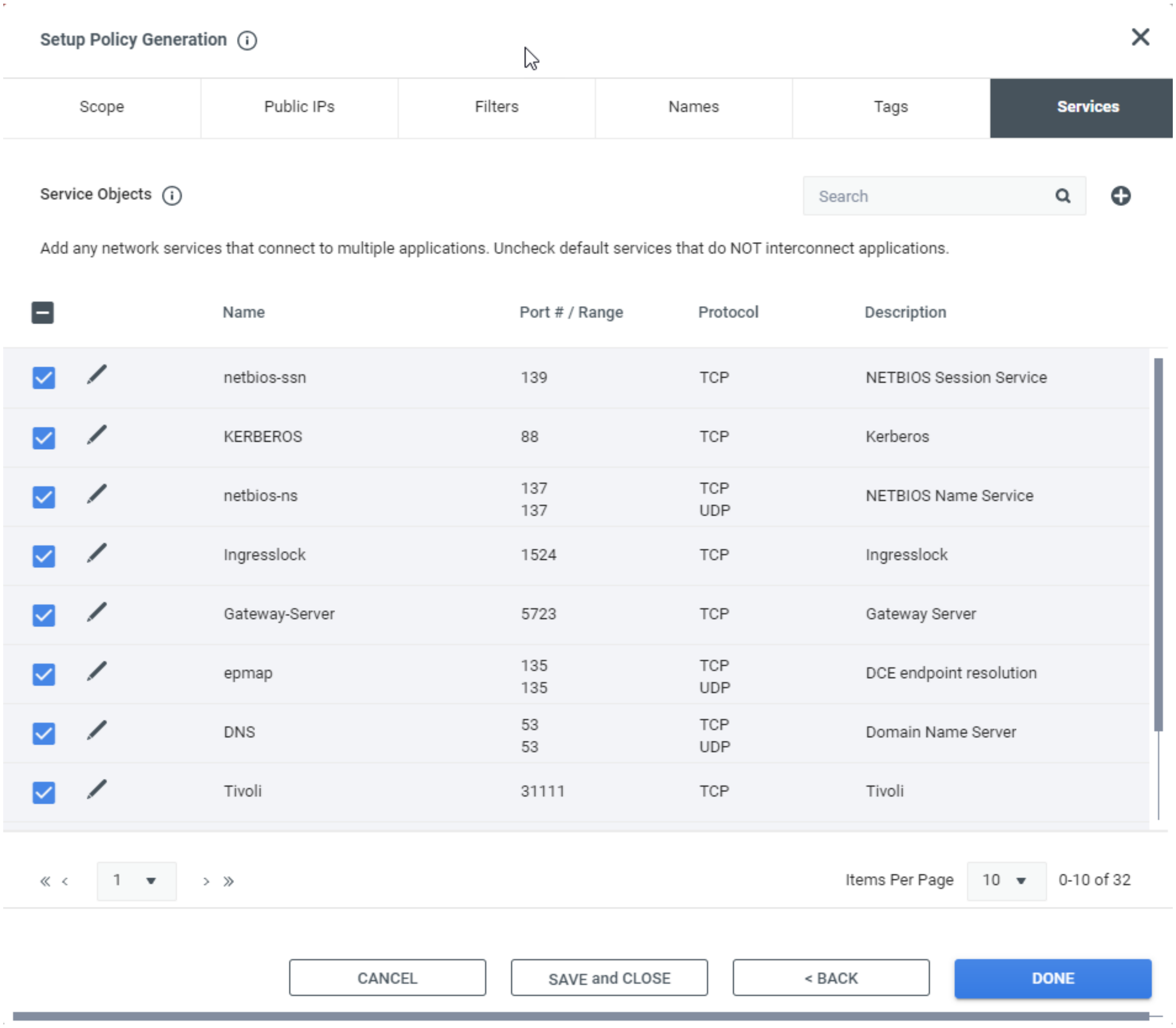
SX_Application

Tag Values	Full Name

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.

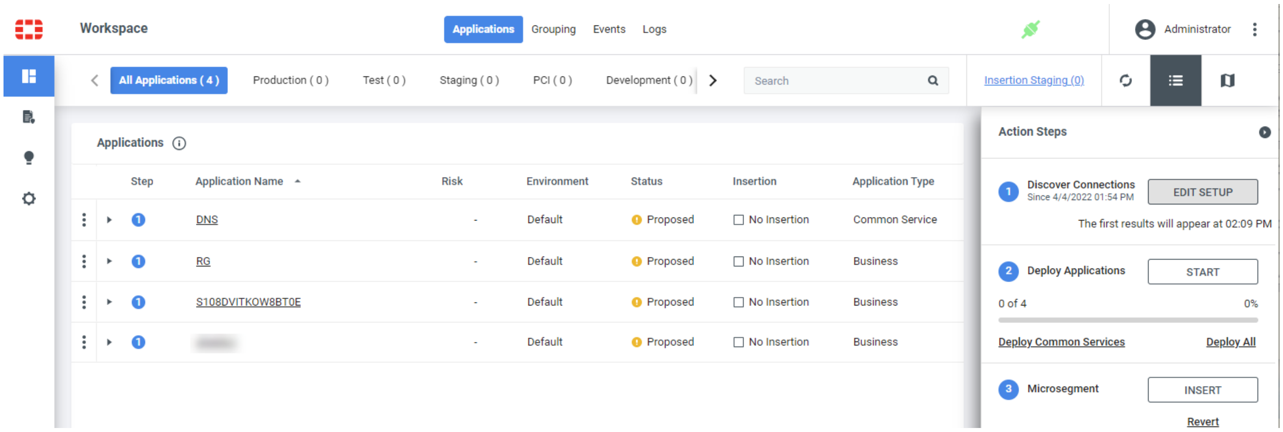


Add any network services that connect to multiple applications. Uncheck default services that do NOT interconnect applications.

▬		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

Action Steps

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

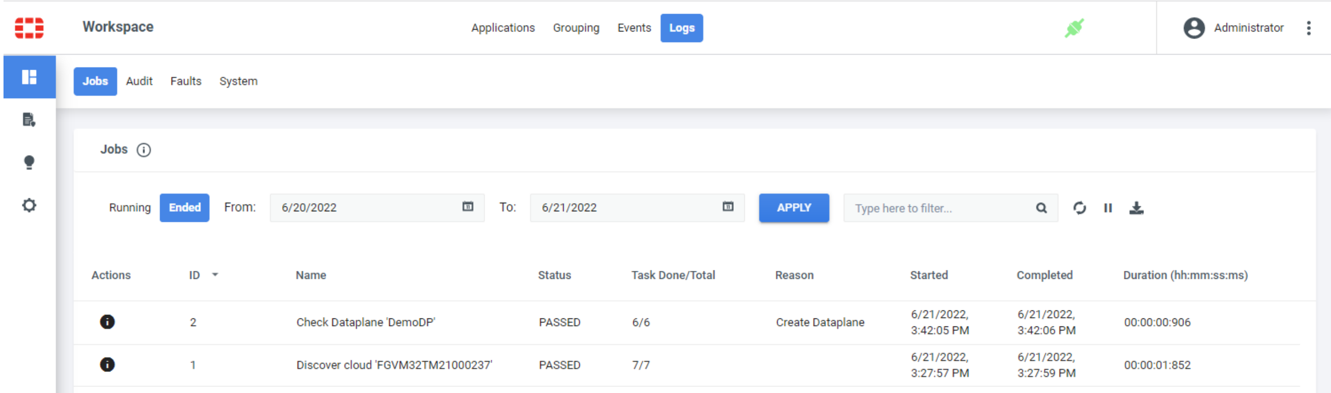
2 Deploy Applications
START
0 of 4 0%
Deploy Common Services
Deploy All

3 Microsegment
INSERT
Revert

Refer to Automated policy generation on page 65 to complete the action steps.

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.

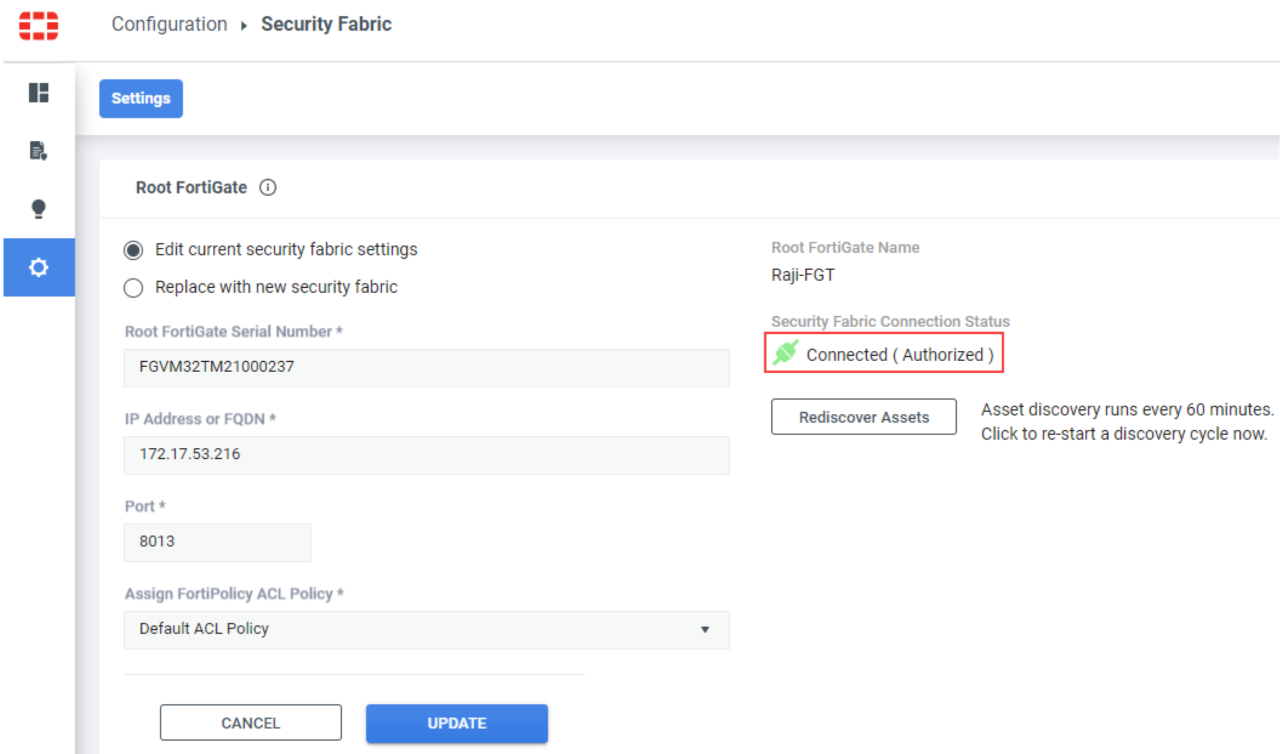
FortiPolicy discovers the data necessary for Policy Generation by connecting FortiPolicy data planes to the FortiGate and FortiSwitch devices in the Security Fabric. FortiPolicy discovers the Security Fabric endpoints and subscribes to the endpoints to receive traffic logs from the FortiGate devices 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.



● 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

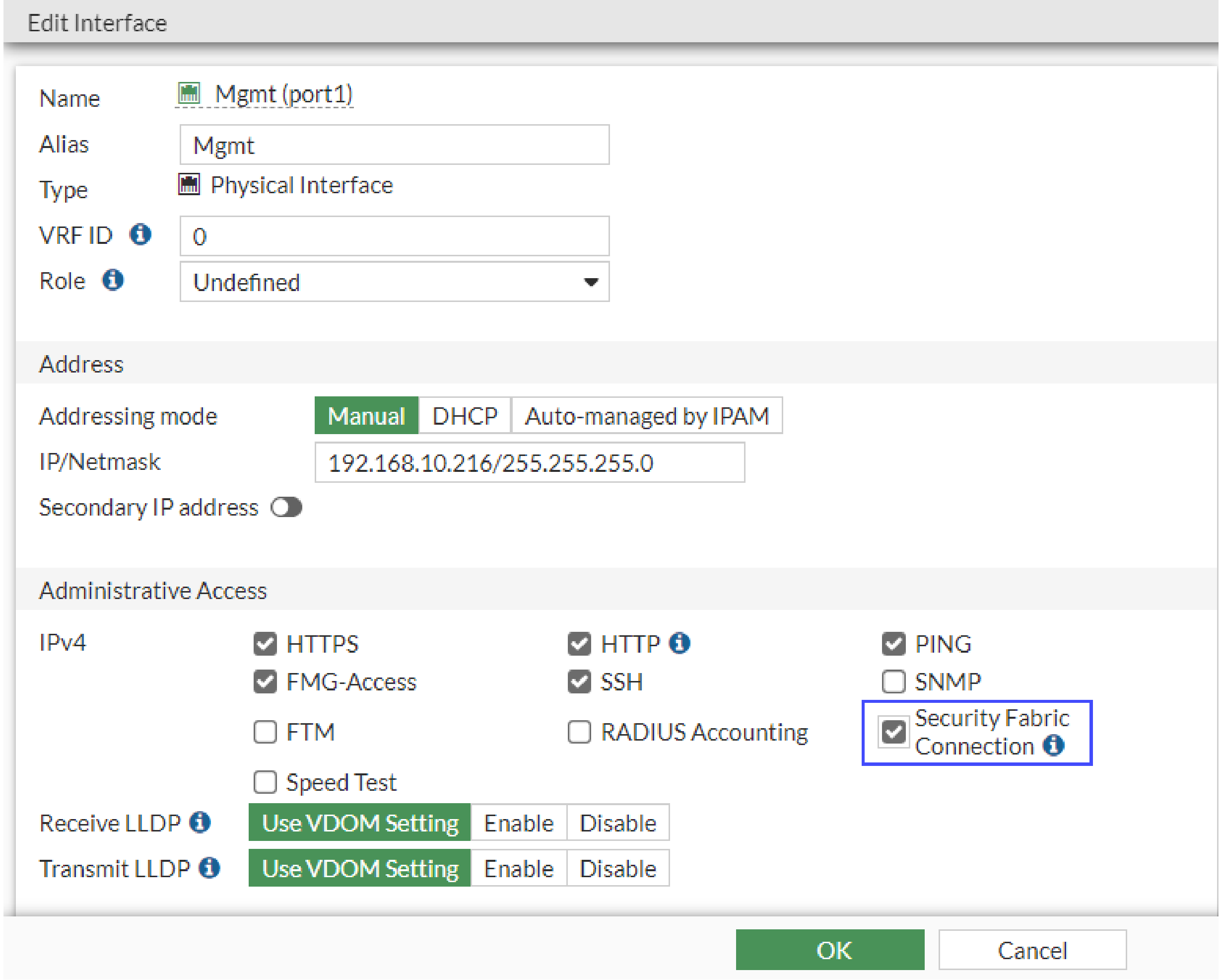
Security Fabric Connection Status
Connected (Authorized)

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 (Manual selected)

IP/Netmask: 192.168.10.216/255.255.255.0

Secondary IP address: off

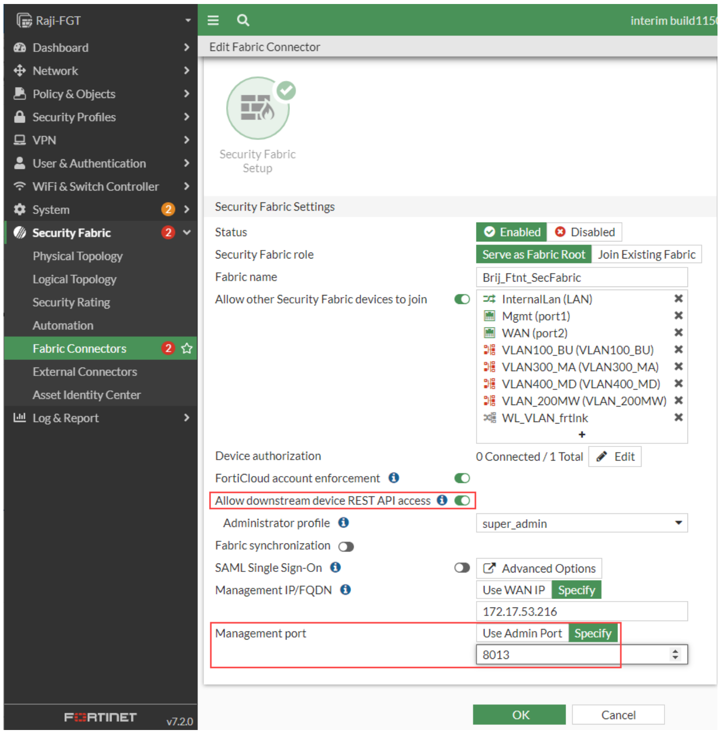
Administrative Access

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

Receive LLDP: Use VDOM Setting | Enable | Disable (Use VDOM Setting selected)

Transmit LLDP: Use VDOM Setting | Enable | Disable (Use VDOM Setting selected)

- 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
```

FortiPolicy CLI

The CLI provides a set of commands used to configure and display status for the FortiPolicy software system and its microservices components.

1. Use SSH to log in to the FortiPolicy CLI with your user name and password.
2. To display the full set of available CLI commands, enter `?`.

```
FortiPolicy-medium-demo>
        delete       Delete system configuration
        enable       Enable new view etc
```

```
exit        Logout of the current CLI session
help        Display an overview of the CLI syntax
history     Display the current session's command line history
ping        Send messages to network hosts
reboot      Reboot the system.
resize      Resize console to terminal size
restart     Restart services
set         Set system configuration
shell       Drop to restricted shell.
show        Show system configuration
ssh         Connect to remote CLI sessions
test        Test commands etc
traceroute  Print the route packets trace to network host
```

3. To enable a FortiPolicy support session:

```
FortiPolicy-medium-demo> set support enabled
Version              : 3
Shared Secret        : 002IRSZ4SNU2FBMZ8VG3FRWDF5VP9
One-Time Password(s) : 00246753839 00214000114 00294672571 00248811433 00267257933

FortiPolicy-medium-demo> show support keys
Version              : 3
Shared Secret        : 002IRSZ4SNU2FBMZ8VG3FRWDF5VP9
One-Time Password(s) : 00246753839 00214000114 00294672571 00248811433 00267257933
```

Using the FortiPolicy REST API

You can use the FortiPolicy Representational State Transfer (REST) API endpoints to interact with the FortiPolicy microservices.

The REST API enables FortiPolicy users to securely connect to FortiPolicy software deployed in a virtualized environment, from which remote procedure calls (RPC) using cURL and JSON can be executed.

The FortiPolicy REST API uses HTTP authentication to manage authentication between a client and FortiPolicy software.

The FortiPolicy REST API supports GET, DELETE, PUT and POST requests:

- Use GET requests to submit RPC commands.
- Use POST requests to create new resources and PUT requests to update them.
- Retrieve infrastructure and security policy information in JSON format.
- Retrieve operational data in JSON format.

FortiPolicy HTTP-based APIs can be used to obtain threat, system management data, software-defined security policy configurations and microservices events.

As part of the FortiPolicy REST API, an AnalyticsStore microservice component is included for querying all ElasticSearch events/error logs per customer environment, generated, logged and indexed by FortiPolicy microservices. The FortiPolicy AnalyticsStore holds all the data that drives the FortiPolicy Analytics and Correlation Dashboards. It is one of the microservices deployed on a single instance FortiPolicy VM. When the FortiPolicy management system scales out to accommodate an infrastructure’s changes and resource demands, three different Analytics Store VMs are deployed to form a “cluster.” This means each VM of the AnalyticsStore microservice is aware of the presence of the other VMs in the cluster and can exchange information and track the health of the other instances of the cluster.

After creating and assigning tags, the tag-based groups are identified in the FortiPolicy console with a tag icon and available for ACL and security policy assignments from the Security Orchestration grouping pages. Up to 50 tags are supported by the FortiPolicy management console. In an upcoming release of the product, tags can be applied across infrastructure types in cloud environments.

Python-based tagging tool

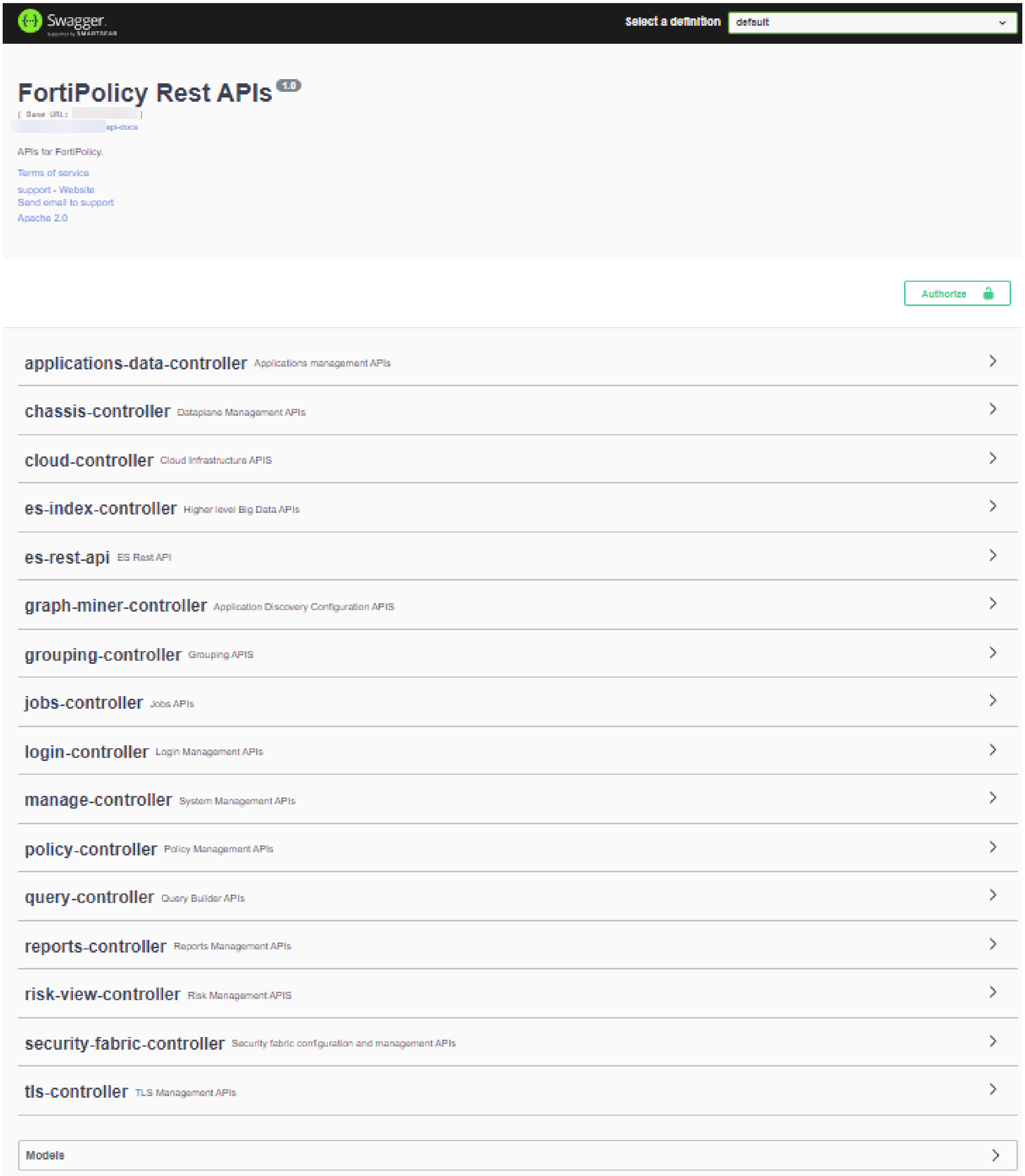
An (optional) tagging tool (Python script) is also available to expedite security group tag creation and assignment. The tagging tool locates and includes the workload ID in the creation command and assignment commands for you, and can handle multiple tags with an AND condition, so it can be a faster option than issuing API calls for customers preferring Python scripting. Request the script from technical support.

FortiPolicy REST API endpoints

FortiPolicy REST API endpoints are organized by software components. All REST API endpoints are listed at:

```
https://<FortiPolicy_IP_address>/swagger-ui/index.html
```

The FortiPolicy REST APIs main page lists the REST API categories:



FortiPolicy Rest APIs 1.0

[Base URL: [redacted]]
[redacted]api-docs

APIs for FortiPolicy.

Terms of service

support - Website
Send email to support
Apache 2.0

applications-data-controller Applications management APIs

chassis-controller Dataplane Management APIs

cloud-controller Cloud Infrastructure APIS

es-index-controller Higher level Big Data APIs

es-rest-api ES Rest API

graph-miner-controller Application Discovery Configuration APIS

grouping-controller Grouping APIS

jobs-controller Jobs APIs

login-controller Login Management APIs

manage-controller System Management APIs

policy-controller Policy Management APIs

query-controller Query Builder APIs

reports-controller Reports Management APIs

risk-view-controller Risk Management APIS

security-fabric-controller Security fabric configuration and management APIs

tls-controller TLS Management APIs

Models

Click on a category to expand it, click on an endpoint to expand it, click *Try it out*, enter any required parameters, and then click *Execute*.

The FortiPolicy API uses HTTP authentication to manage authentication between a client and the FortiPolicy software and microservices. An authorized user account must exist before accessing the FortiPolicy API. The client must include the user account name and password to generate an API KEY for accessing the online FortiPolicy API facility.

Generating an API key

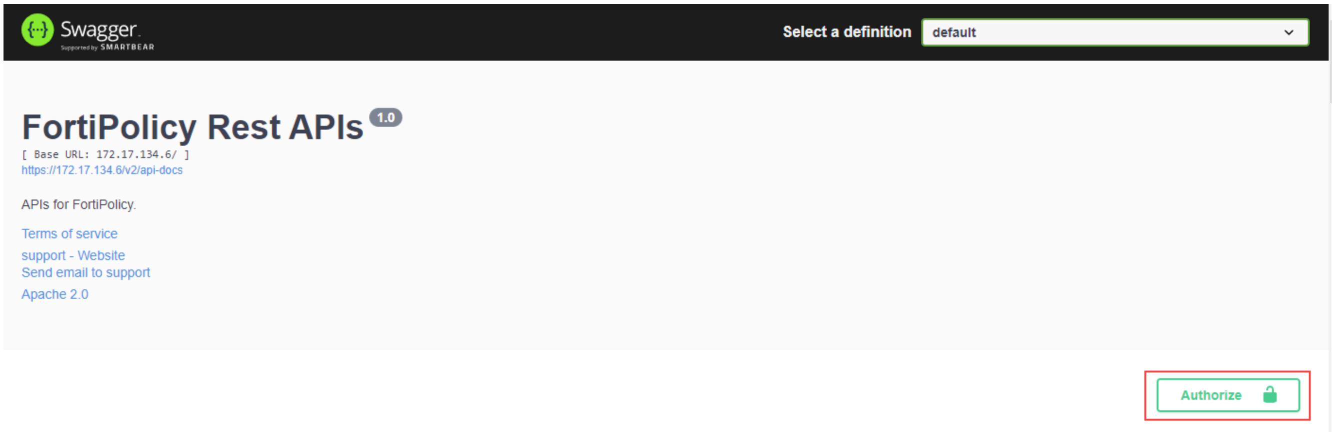
An API key required for access to the FortiPolicy REST API set.

To generate an API key, execute the following cURL command with the login password and user name, as well as the IP address of the FortiPolicy management console. Click *Authorize*, copy the generated API key (token) into the *Value* field, and then click *Authorize*.

```
curl -I -H 'X-Password: <Loginpwd>' -H 'X-Username: <loginUsername>' -XPOST
https://<FortiPolicy_IP_address>/shieldxapi
```

For example:

```
curl -I -H "x-Password: admin" -H "X-Username: admin" -XPOST https://12.6.3.5/shieldxapi
```



FortiPolicy Rest APIs 1.0

[Base URL: 172.17.134.6/]

https://172.17.134.6/v2/api-docs

APIs for FortiPolicy.

In some cases, the single quote in the cURL command may need to be changed to a double quote, depending on a specific operating system’s handling of cURL.

API categories per software component

Software Component	API Category
applications-data-controller	Applications management API endpoints
chassis-controller	Data plane management API endpoints
cloud-controller	Cloud infrastructure API endpoints
es-index-controller	Higher level big data API endpoints

Software Component	API Category
es-rest-api	Elastic Search API endpoints
graph-miner-controller	Application discovery configuration API endpoints
grouping-controller	Grouping API endpoints
jobs-controller	Jobs API endpoints
login-controller	Login management API endpoints
manage-controller	System management API endpoints
policy-controller	Policy management API endpoints
query-controller	Query builder API endpoints
reports-controller	Reports management API endpoints
risk-view-controller	Risk management API endpoints
security-fabric-controller	Security Fabric configuration and management API endpoints
tls-controller	TLS management API endpoints

FortiPolicy API request properties

All FortiPolicy HTTP API requests have the following base URL:

```
HTTP_scheme://<FortiPolicy_IP_address>/shieldxapi/v2/<API>/params
```

For example:

```
"https://10.1.1.1/shieldxapi/v2/deployspec"
```

Each JSON response always contains a “status” field. An “error_msg” includes a string describing the error.

Authentication is with the session API key. API keys are generated with the following cURL command:

```
curl -I -H 'X-Password: <Login_pwd>' -H 'X-Username: <login_Username>'-XPOST
https://<FortiPolicy_IP_address>/shieldxapi
```

In some cases, the single quote in the cURL command may need to be changed to a double quote, depending on a specific operating system’s handling of cURL.

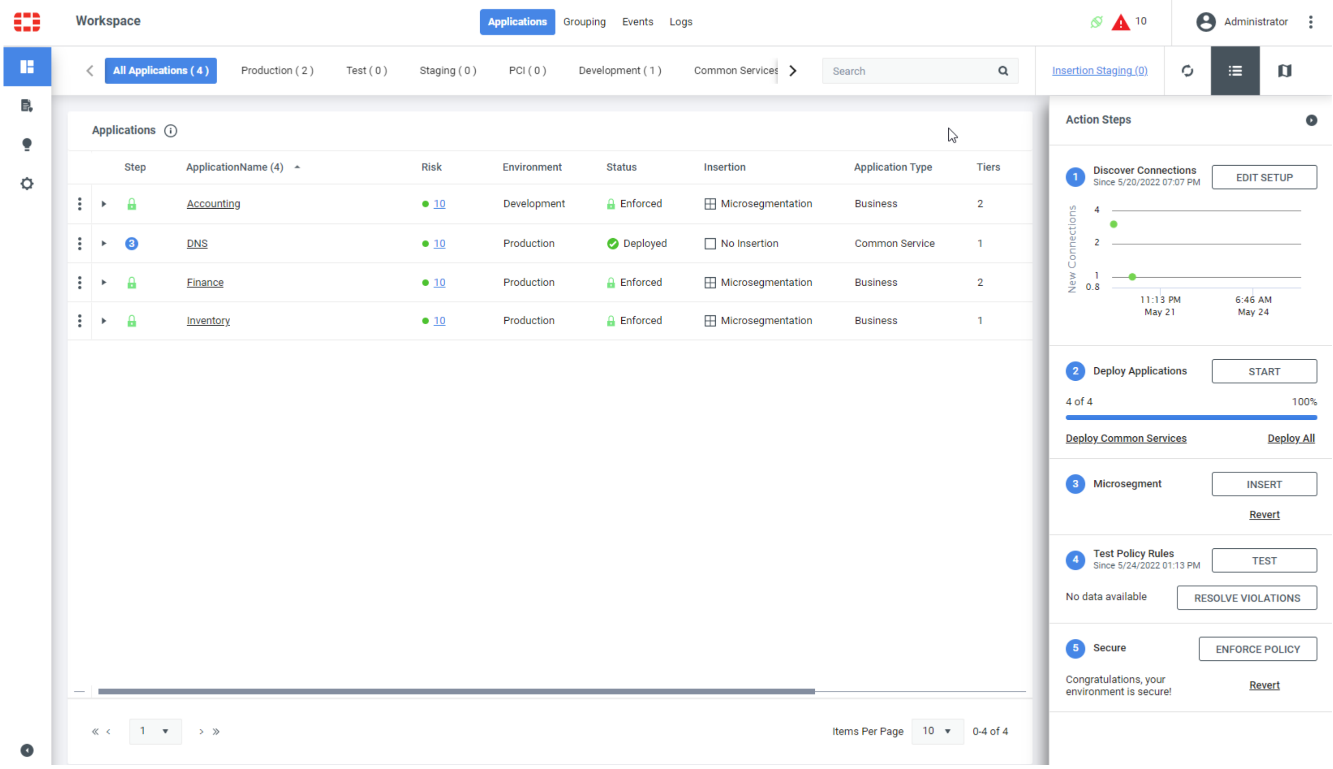
Setting up your workspace

The *Workspace* pages allow you to set up your applications, configure resource groups, specify segmentation and microsegmentation, and view events and logs.

There are four tabs under *Workspace*:

- Applications on page 63
- Grouping on page 89
- Events on page 94
- Logs on page 95

Applications



Step	ApplicationName (4)	Risk	Environment	Status	Insertion	Application Type	Tiers
	Accounting	● 10	Development	Enforced	Microsegmentation	Business	2
3	DNS	● 10	Production	Deployed	No Insertion	Common Service	1
	Finance	● 10	Production	Enforced	Microsegmentation	Business	2
	Inventory	● 10	Production	Enforced	Microsegmentation	Business	1

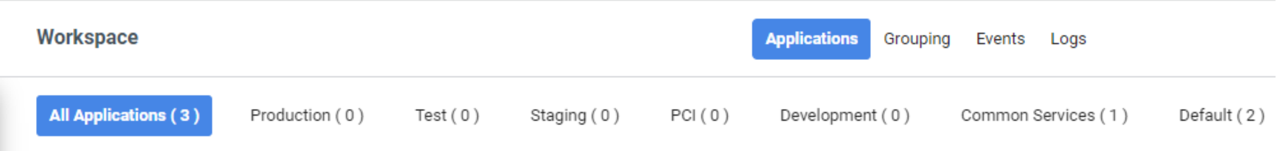
The *Applications* page contains the following:

- *Actions Steps* panel for automated policy generation

  The *Action Steps* panel on the right side of the page lists the five action steps to process raw, unsecured workloads into applications in a fully microsegmented Security Fabric. See Automated policy generation on page 65.
- Tabs

  The tabs are for *All Applications*, *Common Services*, *Default*, and the deployment environments that you specify in the Policy Generation wizard. The default deployment environments are *Production*, *Development*, *Test*, *Staging*, and *PCI*. Click on a tab to select which applications or services to display. Each tab has two views:

- Applications table
- Applications Topology Map



Policy Generation populates these tabs with proposed applications. When you set up Policy Generation, you had an opportunity to provide data that might help the system identify what deployment environment a workload serves. If that data is not available, Policy Generation chooses the Default environment.

- *Insertion Staging* link

  Insertion staging is described in Insertion staging on page 81.
- Buttons
  - *Applications Table* button

    Click *Applications Table* to see applications in a tabular format.
  - *Applications Topology Map* button

    Click *Applications Topology Map* to see applications in a graphical format.
  - *Refresh* button

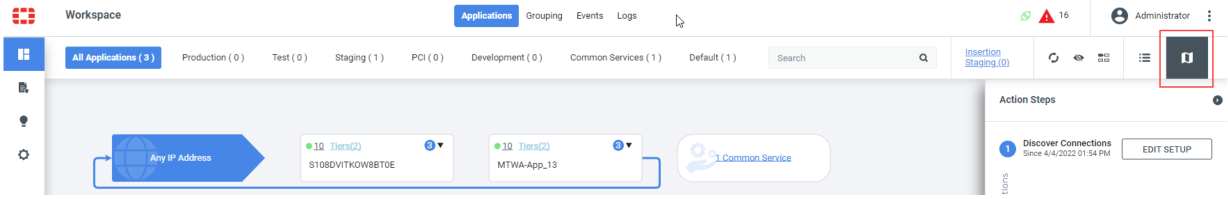
    Click *Refresh* to view the most recent results.
  - *Toggle Connections/Hide All Connections* button

    When you are in the Application Topology Map, click *Toggle Connections/Hide All Connections* to show or hide the connections between applications.
  - *Show All Applications/Hide Applications* button

    When you are in the Applications Topology Map, click *Show All Applications* to see all applications. Click *Hide Applications* to see only applications that are connected to the currently selected application.
- Applications in tabular or graphical format
  - Applications tables

    The Applications tables display details of all the proposed, approved, and deployed applications in each tab. Each application has a summary row that can be opened to show summary details of each tier in the proposed application. If, on the FortiGate device, you enabled layer-7 discovery in the ACL rules that are providing flow data, then there will be a risk score for each application and tier. Click on the numeric score link to display risk and vulnerability data if it is available. Clicking the vertical ellipsis on the far left of each table row displays the actions that can be taken on each application, based on its deployment status.
  - Applications Topology Map

    The Applications Topology Map lets you easily see which applications are connected to other applications. Click the *Applications Topology Map* icon in the upper right corner of the *Applications* page for the Applications Topology Map. Select a connection between two applications to view the proposed ACL rules that connect them.



Each application rectangle in the topology has a tier count link and number indicating its stage in the process. Next to the number is a dropdown arrow, which displays the proposal's status and the menu of actions that can be taken on each proposal, appropriate for its deployment status.

Click on the application name in the Applications table or Tier Count links in the Applications Topology Map to display the *Applications Details* page with details on each tier and connection in the application. See Applications Details page on page 87.

When you first visit the *Applications* page, no applications are shown. Complete Step 1: Discover connections on page 66 to discover and display available applications.

Automated policy generation

Connecting FortiPolicy to your Security Fabric automatically loads data on all the fabric's workloads into FortiPolicy. This can be confirmed on the *Insights* > *Workloads* dashboard and the *Insights* > *Maps* views.

Configuring Policy Generation initiates a deeper process of discovery and analysis of all those workloads connections, which will automatically present you with a complete security policy proposal. The Action Steps then guide you through the process of reviewing, editing, approving, deploying, microsegmenting, testing, and enforcing security policies on your Security Fabric.

Policy Generation groups workloads into applications, application tiers, and deployment environments, like production and development, so that the sources and destinations in your deployed ACL rules are easily identified with the functions and roles they enable in your network.

Policy Generation uses machine learning to do the following:

- Discover all connections between your workloads and identify the functions of all the workloads and their interconnections.
- Group discovered workloads into proposed applications and application tiers and propose tags for the workloads:
  - Tier functions
  - Deployment environments
  - Application names
- Provide risk scores for workloads, tiers, and applications to help you see what is most at risk.
- Propose access control list (ACL) rules that permit observed traffic between tiers.
- Help you to systematically review, edit, approve, and deploy each proposal.
- Help you to microsegment or segment workloads in preparation for enforcing policy rules.
- Test the deployment on actual traffic for a second review and edit.
- Add a security tag to the application workloads to enforce policy and permit only traffic allowed by your ACL rules.

The following are required for automated Policy Generation:

- FortiPolicy installation

  See Installing FortiPolicy on page 18.
- FortiPolicy license

  See Importing the FortiPolicy license file on page 32.
- Security Fabric

  Add a fabric connector to the root FortiGate device of your Security Fabric and authorize the connection between FortiPolicy and the FortiGate device. See Creating a fabric connector on page 36.
- Layer-7 data

From the root FortiGate device, enable layer-7 discovery on existing ACL rules that are providing flow data .FortiPolicy displays the fabric workloads on the *Workspace > Assets Map* page and lists them for discovery. FortiPolicy then proposes allow rules that allow specific data to flow from one specific place to another. Data that is not allowed by any rule is blocked.

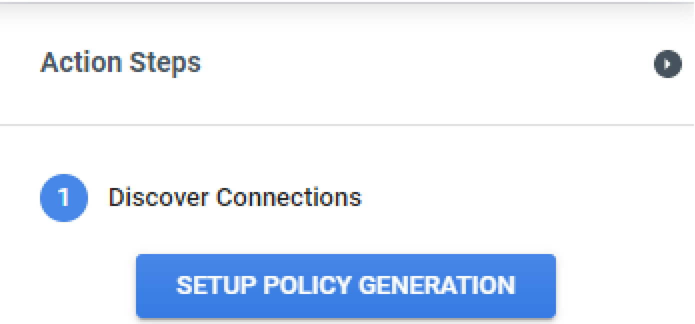
- Data planes
  Create a data plane for each FortiGate device with connected workloads that you want to secure. See Configuring data planes on page 44.

There are five Policy Generation steps in the *Action Steps* panel to process raw, unsecured workloads into applications in a fully microsegmented Security Fabric:

- Step 1: Discover connections on page 66
- Step 2: Deploy applications on page 75
- Step 3: Microsegment on page 80
- Step 4: Test policy rules on page 83
- Step 5: Secure on page 85

Steps 3 through 5 require that the security rules are deployed to the Security Fabric.

Step 1: Discover connections



Click *SETUP POLICY GENERATION* in the *Action Steps* panel on the right side of the *Workspace > Applications* page to open the configuration wizard to set the automated processes in motion. Fill out the forms on the tabs and refer to the help provided on each page. Click *DONE* in Setup Policy Generation to begin connection discovery. See Connection discovery on page 74.

Policy Generation will discover all the traffic between all the workloads and endpoints in the network. Using that data, Policy Generation will automatically organize your workloads into proposed applications, application tiers, and ACL rules. The more you complete on the setup page form, the more work Policy Generation can do for you. The six tabs let you specify the following:

- Scope tab on page 67
  Specify where to look for connections and how to process the data.
- Public IPs tab on page 68
  Enter public IP addresses that are to be analyzed as part of your internal private network scope.
- Filters tab on page 69

Add logical rules to limit the scope specified in the *Scope* and *Public IPs* tabs.

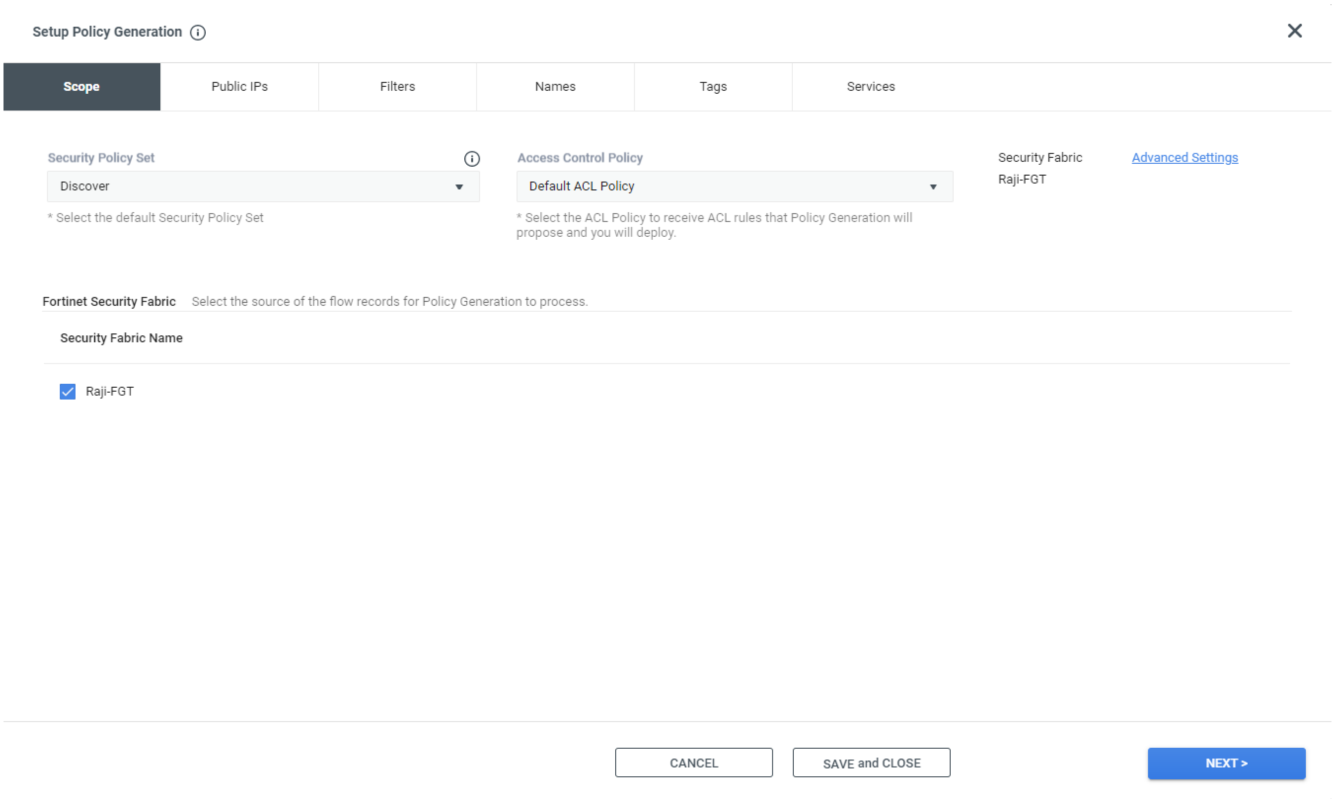
- Names tab on page 70

  Specify your workload naming convention, so the system can name applications, tiers, and deployment environments for you.
- Tags tab on page 71

  Specify how to name applications, application tiers, and deployment environments and how to tag workloads.
- Services tab on page 73

  Check the names of common network service applications that support networks and the ports and protocols they use. Identifying network services is crucial to deriving the optimal set of business applications.

Scope tab



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

In this tab, you specify from where and how Policy Generation should gather data on the connections with and between workloads and where to store the policy rules that will result from your review and deployment of the automated policy proposals.

1. In the *Security Policy Set* dropdown list, keep the default setting of *Discover* for automated policy generation.
2. In the *Access Control Policy* dropdown list, select the policy table in which you want to store the ACL rules. Select one of the following:
   - The same ACL policy you assigned to the Security Fabric. Usually this is the *Default ACL Policy*.

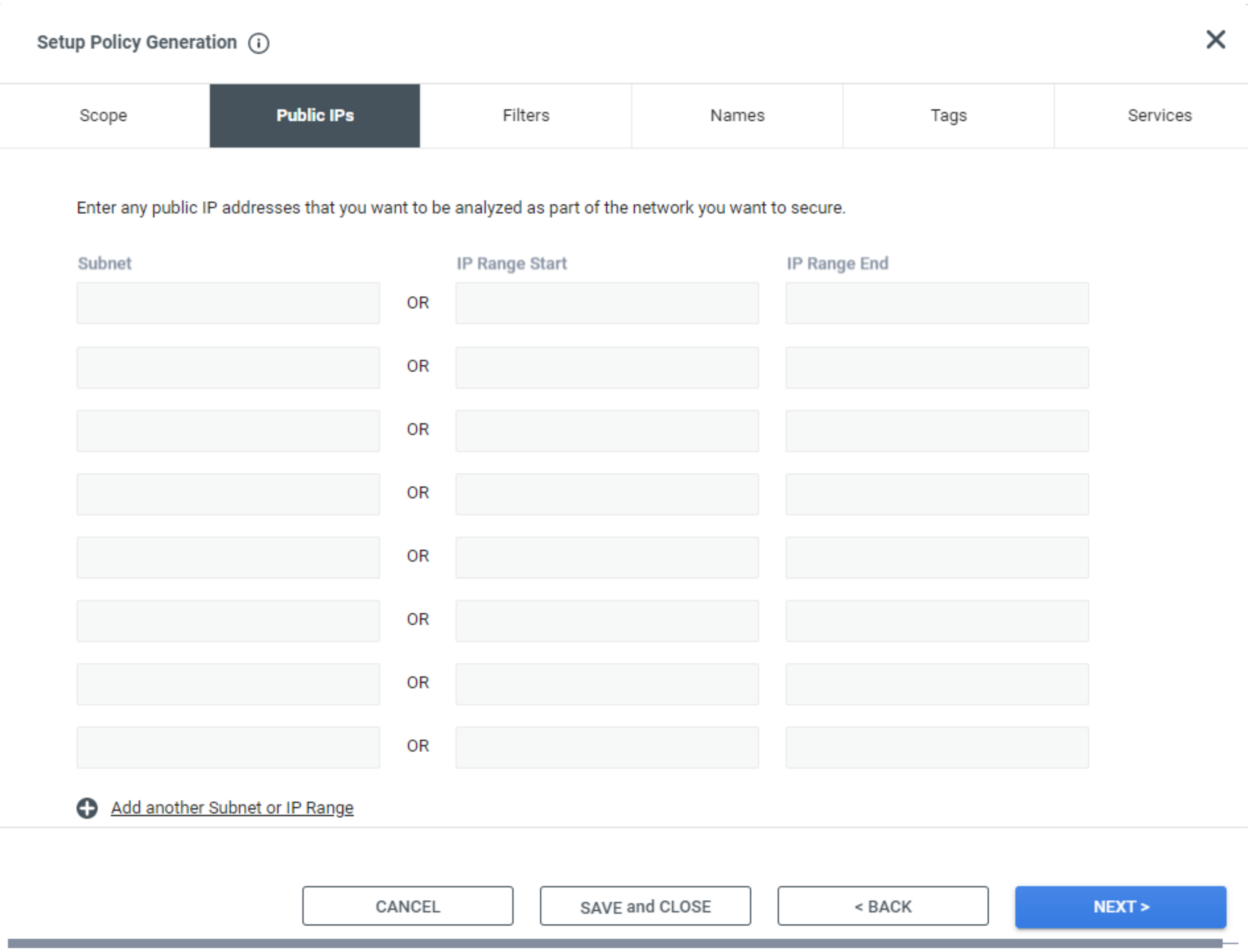
     The name of the Security Fabric is displayed to the right of the *Access Control Policy* dropdown list. When you deploy an application, its ACL rules are copied to the selected policy and immediately deployed to the root FortiGate device and its appropriate Security Fabric VDOMs.
   - A different ACL policy from the one you assigned to the Security Fabric.

To create an ACL policy, see Access control on page 100. If the ACL policy is not tied to the Security Fabric, no fabric name is displayed to the right of the *Access Control Policy* dropdown list. You can deploy ACL rules to the new ACL policy, but those rules will NOT be forwarded to the Security Fabric until you associate the new ACL policy with the Security Fabric on the *Configurations* > *Security Fabric* page.

3. Under *Security Fabric Name*, select the checkbox for the Fortinet Security Fabric. This allows Policy Generation to gather data from the Security Fabric.
4. If Fortinet Support asks you to change the default settings, click *Advanced Settings*.

   See Advanced settings on page 86.
5. Click *NEXT*.

Public IPs tab



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

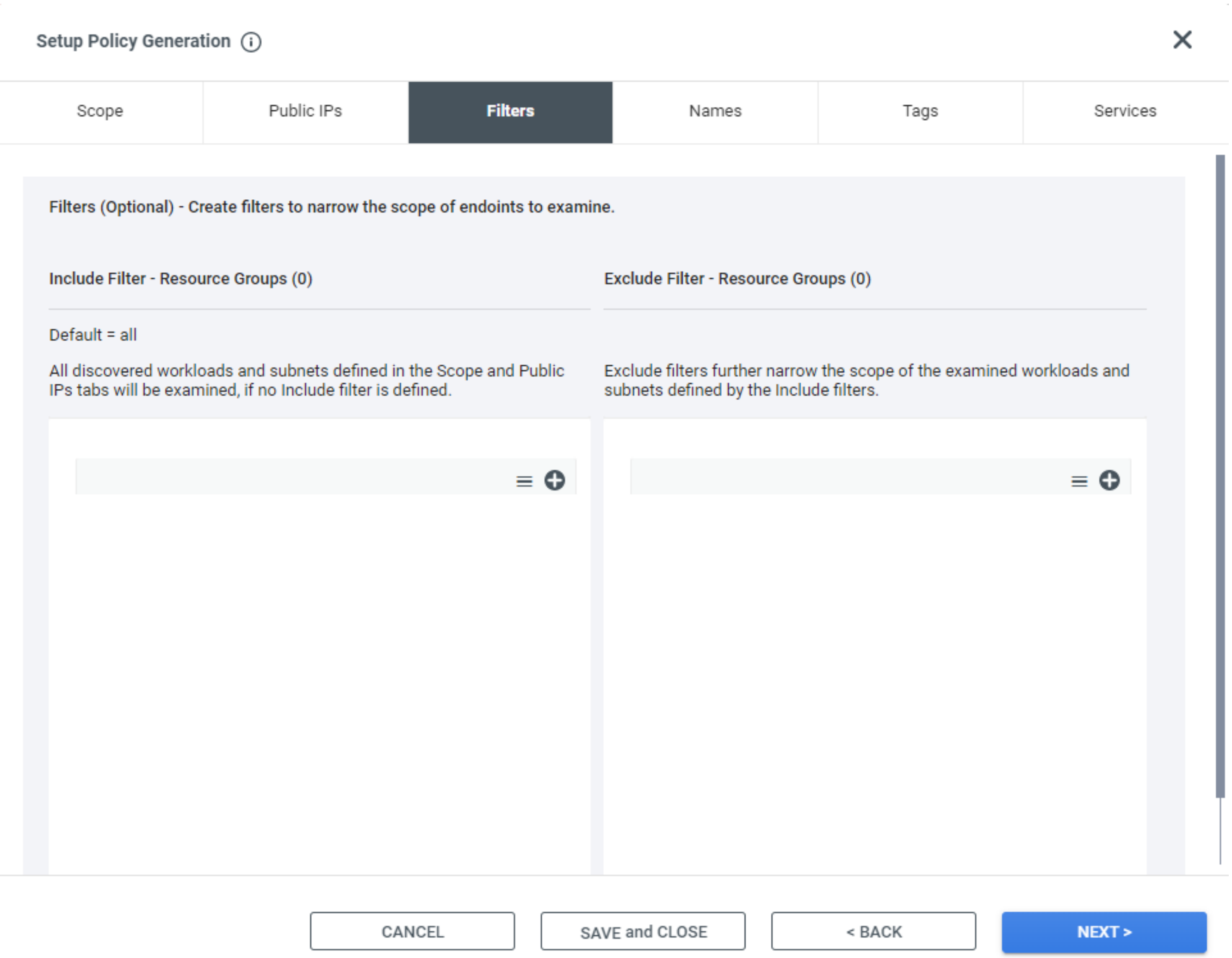
Enter any public IP addresses that you want to be analyzed as part of the network you want to secure.

If Policy Generation observes a public IP address that you entered, Policy Generation will propose an application tier that is specifically defined by that public IP address.

If Policy Generation observes a public IP address that you have NOT entered to be analyzed as part of the network you want to secure, Policy Generation will propose a generic, all-inclusive tier with the universal IP range of 0.0.0.0/0. The specific observed public IP address will be listed in the tier details as observed, but the tier definition will include all IP addresses, public and private.

When you are finished, click *NEXT*.

Filters tab



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.

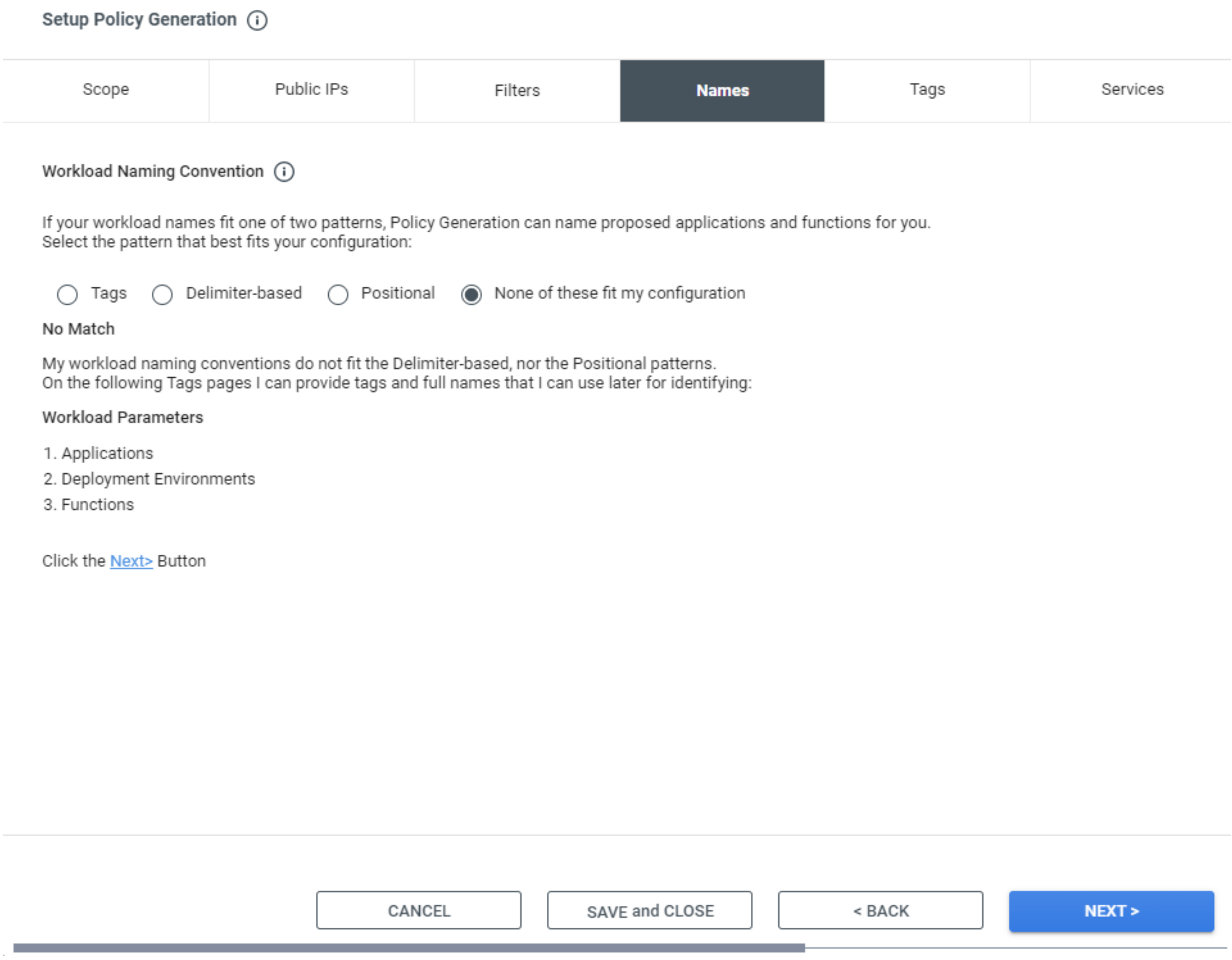
Policy Generation will examine all workloads defined on the *Scope* and *Public IPs* tabs unless you add one or more filters.

Add include filters to specify which of the defined workloads and subnets to examine. Include filters narrow the scope.

Add exclude filters to specify which of the defined or included workloads and subnets already specified should NOT be examined. Exclude filters also narrow the scope.

When you are finished, click *NEXT*.

Names tab



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

Policy Generation proposes names for application workload tiers based on the following:

- Application name, such as CRM or Accounting
- Deployment environment, such as Production, Development, or Testing
- Tier function, such as Web, Database, or Application Logic

If applicable, select one of the two naming convention patterns that best fits your workload-naming configuration:

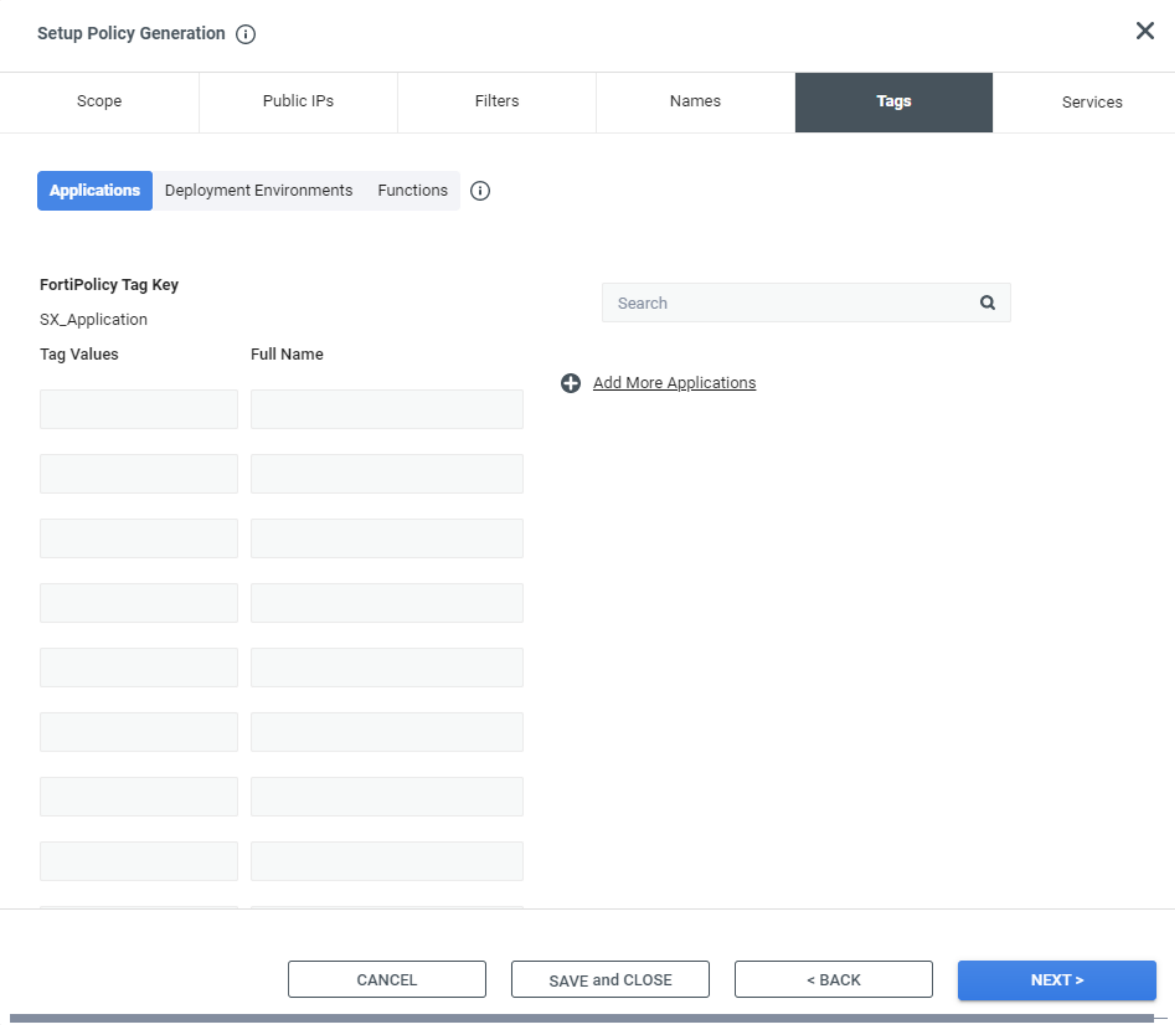
- *Delimiter-based*: This common naming convention format allows codes of different lengths for each value by inserting a delimiter like _ underscore or . period between code sections.
- *Positional*: This common naming convention format allows codes of a set length for each of its values.

FortiGate devices do not currently support a native tagging system.

If your workload names do not provide any of these three data values in a pattern that Policy Generation can read, then select *None of these fit my configuration*.

When finished, click *NEXT*.

Tags tab



Setup Policy Generation ⓘ

Scope	Public IPs	Filters	Names	Tags	Services

Applications | Deployment Environments | Functions ⓘ

FortiPolicy Tag Key

SX_Application

Tag Values | Full Name

Policy Generation uses its own key/value tags to identify the workloads as members of the following:

- Applications
- Tiers
- Deployment environments

There are three sub-tabs, one for each of these three categories of data.

Each tier is typically defined by a set of three workload tags. For example:

Tag Key	Values	Full Name
SX_ Application	Acnt	Accounting Software

Tag Key	Values	Full Name
SX_ Application	Inv	Inventory Management
SX_ Environment	Prod	Production
SX_ Environment	Test	Test
SX_Environment	Dev	Development
SX_Tier	Web	Web
SX_Tier	Logic	Business Logic
SX_Tier	DB	Database

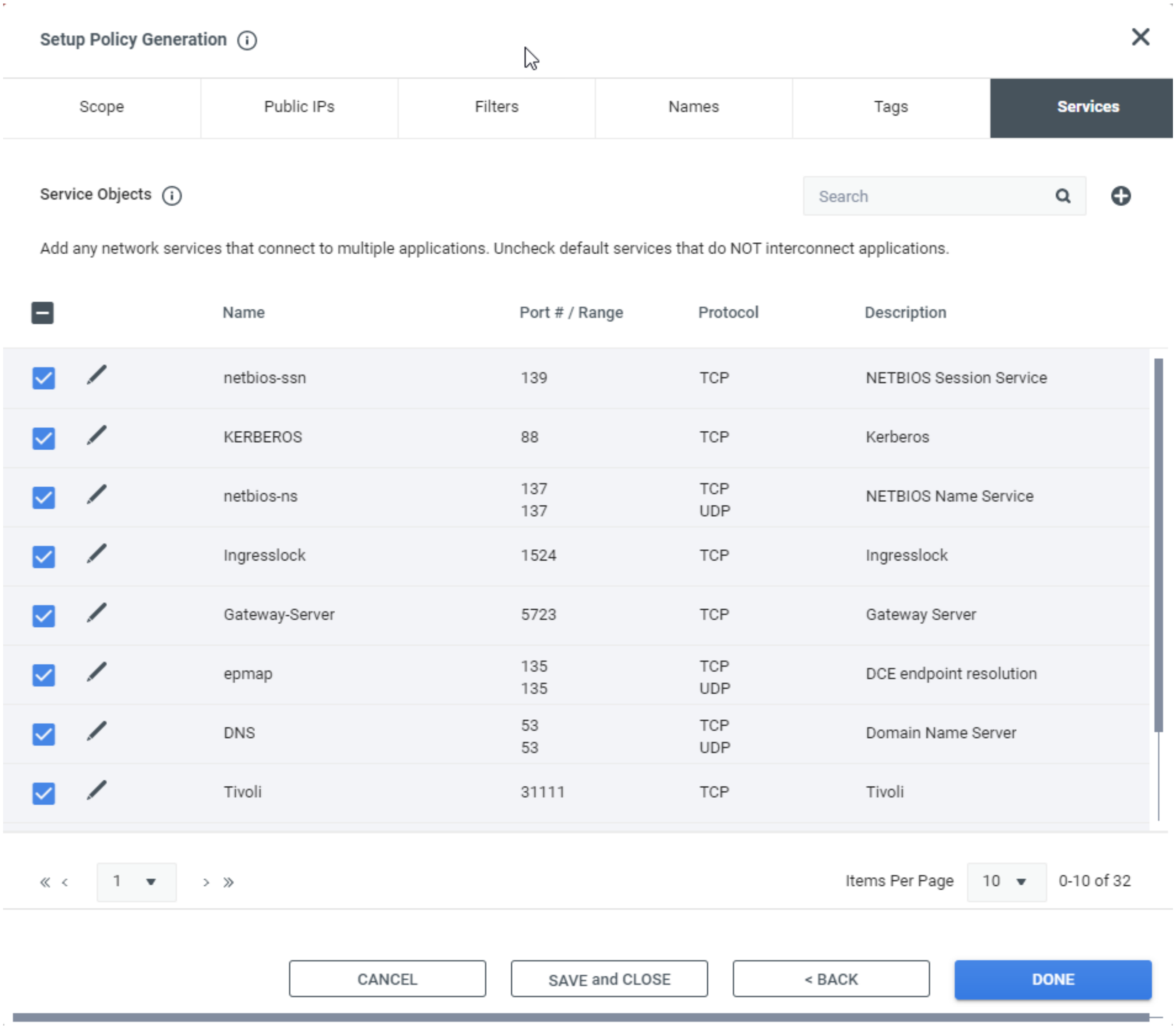
If your naming convention provided Policy Generation with application name data, you will see the values for all your applications pre-populated in double columns on the first of the three sub-tabs. All you might want to do is edit the full names for each of the tag values. If you do, the full names will be used in dropdowns and table labels instead of the typical brief names. If all your users are comfortable using the strings in your naming convention, you do not need to change anything.

For any data that cannot be derived from your naming convention, manually enter the tag values and full names you will use to identify your applications, deployment environments, and functions.

Many companies have so many applications that some users will not know all the application tag values. You can help those users by supplying full names as well as briefer tag values.

When you are finished, click *NEXT*.

Services tab



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

It is vitally important to help Policy Generation identify all common network service applications, like DNS and NTP, that tend to interconnect all the Business Application tiers in your environment.

The Services tab presents a list of many of the most common network services with their standard names, ports, and protocols. If your network uses nonstandard ports and protocols for any of the listed services, you need to edit each such service to include all its ports and protocols.

Add any custom services in your network that are not already on the standard list.

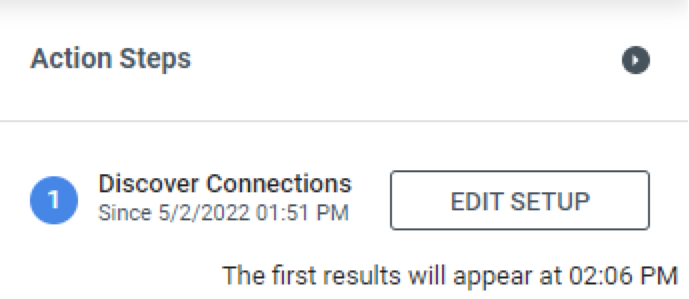
Updating the information on this tab allows Policy Generation to better distinguish between the following:

- Business application tiers that connect within a business application or to other business applications
- Service tiers that connect to each other and to most of the business application tiers

When you have completed the six tabs in the Setup Policy Generation wizard, click *DONE* to submit your input, close the wizard, and return to the *Applications* page, where you will see that connection discovery has started.

Connection discovery

When you click *DONE* in the Setup Policy Generation wizard, connection discovery begins. Step 1: Discover Connections shows the time and date connection discovery started. A status message displays the time when the first discovery cycle will complete, but it might take longer for the first data point to appear on the chart.

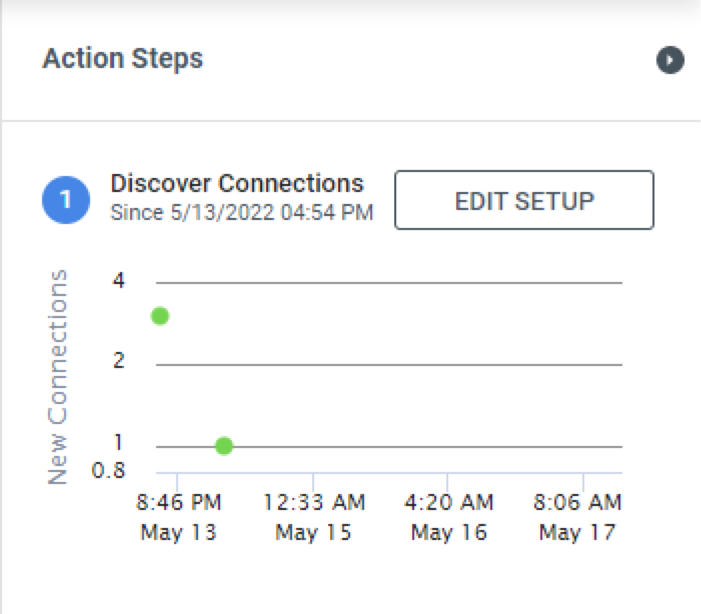


Action Steps

1 Discover Connections
Since 5/2/2022 01:51 PM

The first results will appear at 02:06 PM

Connection data is displayed in the New Connections graph in Step 1 after each 2-hour discovery cycle, plus computation time. Even after just the initial discovery cycle, Policy Generation will begin proposing applications and policies.



Action Steps

1 Discover Connections
Since 5/13/2022 04:54 PM

Do not approve or deploy applications at this point. Let Policy Generation discover all network connections and propose applications and ACL policy rules.

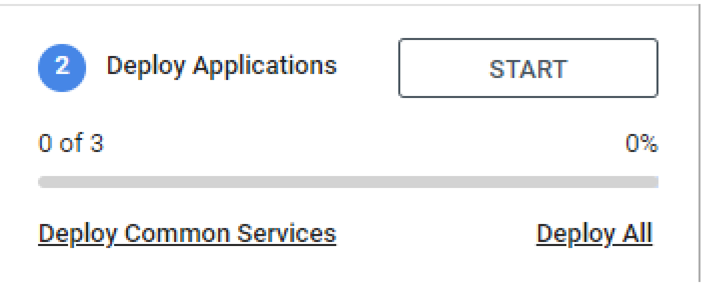
Most connections are discovered in the first cycle. Some connections, however, will take longer, for example, if your backup only runs on Sunday night. Let the discovery process run until all the allowed connections have occurred. The graph adds a data point every 2 hours until there are no more new connections discovered. At 0, Policy Generation is not seeing any new connections. Wait until there are several consecutive updates at 0.

When the graph stabilizes at 0, you can move to Step 2: Deploy Applications.

If there are rare connections that might not take place until the distant future, you can manually add them later.

Step 2: Deploy applications

In Action Step 2: Deploy Applications, click *START*.



The deployment wizard displays the *Application Details* page and walks you through the deployment of the following:

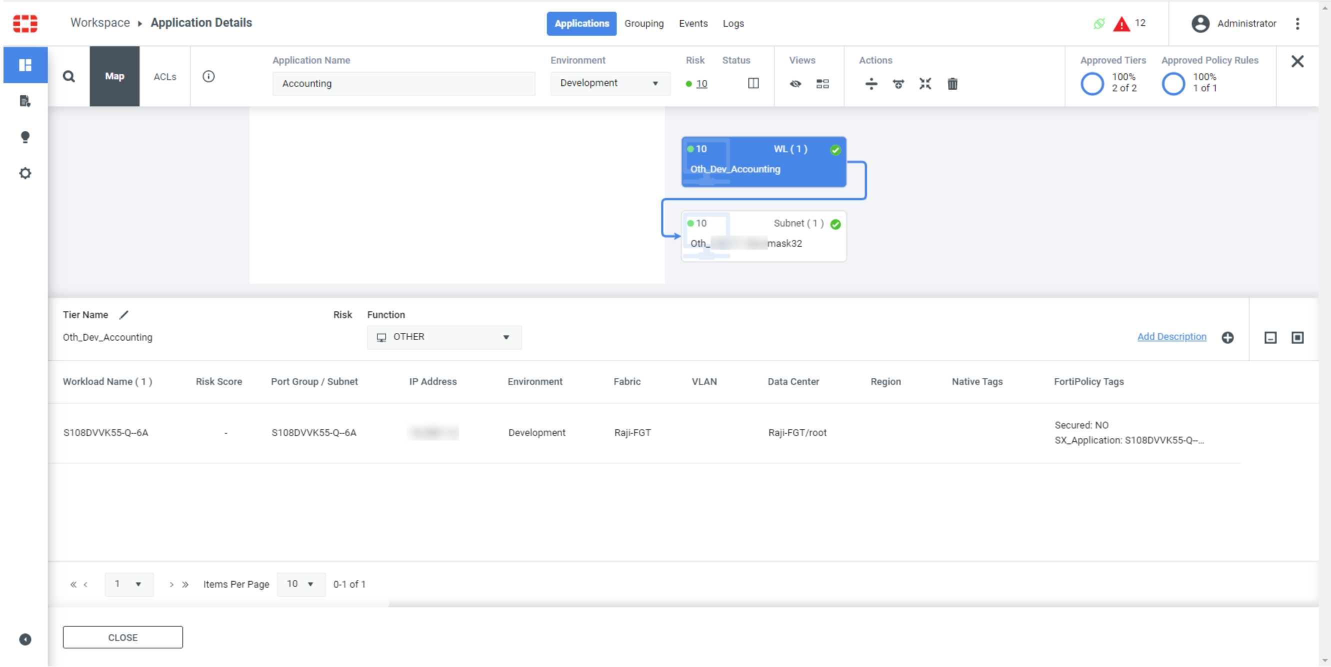
- *Common network services*

  Review, edit as needed, approve, and deploy all the proposed common network service applications (such as DNS and NTP) before approving and deploying proposed business applications. A business application cannot be deployed until its common services are deployed. While reviewing a business application, the wizard can deploy needed common services when necessary, but in the middle of reviewing a business application, you will lose the ability to carefully review and edit those services that are not already deployed.

  The wizard displays the *Application Details* page for each common service. The page allows you to examine, edit, approve, and deploy each proposed common service application. Follow the on-screen help to process the proposal and deploy the rules you approve to the root FortiGate device’s Security Fabric.
- *Business applications* After you deploy all the common services, the wizard displays the first business application. At this point, you have two options:
  - Follow the wizard.

    Let the wizard walk you through deploying the proposed business applications, just as it did for the common service applications. The *Application Details* page lets you examine, edit, approve, and deploy the proposed business application, just as you did with the common service applications. Follow the on-screen help to process the proposal and deploy the rules you approve to the root FortiGate and its Security Fabric.
  - Make your own choices.

    To decide for yourself which business applications you want to secure first, close the *Application Details* page. The system will return you to the All Applications table showing you all proposed business applications and deployed common service applications.



Application Name: Accounting

Environment: Development

Risk: ● 10

Status

Approved Tiers: 100% 2 of 2

Approved Policy Rules: 100% 1 of 1

Tier Name: Oth_Dev_Accounting

Risk

Function: OTHER

Workload Name (1)	Risk Score	Port Group / Subnet	IP Address	Environment	Fabric	VLAN	Data Center	Region	Native Tags	FortiPolicy Tags
S108DVVK55-Q--6A	-	S108DVVK55-Q--6A	[redacted]	Development	Raji-FGT		Raji-FGT/root			Secured: NO SX_Application: S108DVVK55-Q-...

« ‹ 1 › » Items Per Page 10 0-1 of 1

Common network services

For common network services, you can make the following changes:

- Edit the name of the service tier.

  Usually the data you provided on the *Services* tab of the Policy Generation Setup wizard is enough for the system to accurately identify your network service application names, but you might want to edit them in ways that conform to your liking and needs. You can edit the name of the service tier as needed.
- Select the deployment environment.

  By default, all proposals are assigned to the Default environment, unless you were able to provide naming guidance in the Policy Generation Setup wizard. You might have some applications in your Production environment and other instances of the same applications that serve your other environments, such as Test and Development. You will need to determine what deployment environment each proposed application belongs in. If you have common services that support multiple environments, you might decide to leave them in the Default environment or create a special deployment environment for these shared resources: Go to *Applications* > *Edit Setup* > *Tags* > *Deployment Environments* to create new deployment environment names that can then be selected from the dropdown list on the *Application Details* pages.
- View the function.

  Each service tier is assigned the Service function by default. You do not need to change this function.
- Approve the tier members.

  A tier can be composed of a single server, a server cluster, or a set of independent servers or clusters. Review the proposed tier members. Do they have the same security requirements and do all indeed provide the service identified in the Application Name? You might decide to delete a member from one tier and add it to another tier in another application. When you are happy with the Application Name, Deployment Environment, Tier Function, Tier Name, and membership, click *Approve Tier* in the lower right corner. The wizard will automatically advance to the next tier to be reviewed or to the first connection to be reviewed.
- Approve the ACL rules.

If the service has connections to other deployed common services, the deployment wizard allows you to approve each connection's ACL rules before deploying a service application. Review the ACL rule and edit if necessary. When you are happy with the connection, click *Approve Policy* in the lower right corner.

When all application tiers and connections are approved, you will see the Approval Complete message, giving you the choice to deploy the application now or later. For the best security, service applications must be deployed before you deploy your business applications. If you are ready to deploy now without further levels of review, then click *DEPLOY RULES NOW*. The system checks to see if you edited the Application Name and Deployment Environment from Policy Generation's initial proposal. If you did not make any edits, you will get a chance to make any last changes.

Deploying the proposal will prevent further editing of the proposal as a whole and send the rules to the Security Fabric.

When you deploy any application, the workloads in that application are tagged with the following FortiPolicy tags based on the choices you approved and deployed:

- Application Name tag
- Deployment Environment tag
- Tier Function tag
- Secure tag

  The Secure tag defaults to “No” but is switched to “Yes” when you choose to secure the application.

If your process requires additional review, then click *DEPLOY LATER*. Reviewers can select fully approved common service applications from the Applications tables or topologies. To follow the best security practices, you will need to complete all service application policy reviews and deploy your service applications before approving and deploying any business applications. When you return to a fully approved service *Application Details* page, you will see the *DEPLOY RULES* button in the lower right corner. Click *DEPLOY RULES* to deploy the application and return to the *Applications* page.

Business applications

For business applications, you can do the following:

- Choose an application to secure.

  Search and sort the application table or search and scan the Application Topology Map to find the business application you want to secure next.

  You might want to search for workload names or IP addresses that you know belong to a specific application. Click the application name in the application table or click the tier count link in the Application Topology Map to open the *Application Details* page.
- Approve and deploy.

  The *Application Details* page lets you examine, edit, approve, and deploy the proposed business application, just as you did with the common service applications. Follow the on-screen help to process the proposal and deploy the rules you approve to the root FortiGate device and its Security Fabric.
- Approve and save.

  The *Application Details* page supports an alternate workflow if you want to have multiple reviews before deploying rules to your Security Fabric. When the last of all the proposed tiers and ACL rules are approved, you are given the choice to deploy now or save and deploy later. If you choose to deploy later, your work will be saved, and others can review your work. When the application has passed the requisite reviews, you or another authorized user can deploy the application to the Security Fabric.
- Approve and deploy to an alternate ACL table.

  There is an alternate workflow: If, on the *Scope* tab of the Setup Policy Generation wizard, you selected an alternate access control policy that was not assigned to the Security Fabric on the *Configuration* > *Security Fabric* page, then each time you deploy an application, its rules are saved to the alternate ACL policy table and not to the Security Fabric. This gives you and your team the opportunity to review the whole ACL table. When the whole alternate table has been reviewed and accepted, you can then associate the alternate ACL with the Security Fabric and deploy the ACL rules to the Security Fabric.

For business applications, you can make the following changes:

- Edit the name of the business application.

  If you were able to provide application naming convention data, Policy Generation will have named the Business Applications for you. If not, Policy Generation will create a unique name based on the longest common prefix among all the workloads of the application. Be sure to examine the tier workloads or subnets and the ACL rules to confirm or edit the application name. You can select any tier rectangle or connection line to view the details of each as you determine which application you are looking at. By default, FortiPolicy shows only the connections for the selected tier and hides all the other connections. To show all the connections at once, select the Toggle Connections icon under Views.
- Divide combined proposals.

  If you have business applications that communicate with each other, Policy Generation might not be able to accurately separate them into unique proposals. If you find that a proposal contains the tiers of two or more applications, then select the Assign Tiers icon under Actions and assign tiers to different applications, thus dividing the proposal into two or more proposals. Then approve and deploy each of the new proposals.
- Select the deployment environment.

  Confirm or edit the proposed environment. Usually, you do not want to leave business applications in the Default environment. You will need to determine what deployment environment each application belongs in. Sort them into Production, Development, Test, and so on.
- Review the tier function.

  Confirm or edit the proposed tier function. Policy Generation will propose the tier function, based on the application components, ports, and protocols used by the tier: Web, Business Logic, Database, Other, Service, or External. Examine the workloads in the tier to confirm the function of the tier. To select a different tier function, pick from the dropdown list in the Tier Members Table header. In some cases, you might have more than one tier with the same tier function in an application. The system will automatically add a digit to the end of the tier function to be sure that each tier is uniquely identified.
- Edit the tier name.

  Each tier rectangle in the map displays the tier name. By default, workload tier names are a concatenation of the Tier Function tag, the Deployment Environment tag, and the Application Name tag. As you edit any of these individual values, those edits are automatically applied to the workload tier names. Subnet tier names are a concatenation of the tier function and the first subnet. The tier names are shown as sources and destinations in proposed ACL rules. This makes it easy to read the rules and understand what is allowed to talk to what. Tier names are also displayed on the Tier Members Table header bar together with an edit icon. If you want to give a different name to some tiers, select the edit icon.

  NOTE: If you manually edit a tier’s name, the system keeps that name and ceases its automatic naming behavior if you later change the application name, environment, and/or function.
- Add a description.

  On the far right of the Tier Members Table, you can click *Add Description* if you want to add notes about the tier. Such notes can be helpful when you are first trying to identify which of your applications is being proposed. Your notes might also be helpful when reading the rules in the *Policy > Access Control* table.
- Review the proposed workloads.

  Confirm, add, or delete the proposed workloads. Confirm that they all have the same function and have the same security policy requirements. By definition, a tier is a set of members that all share an identical set of security requirements. If necessary, you can remove any workloads that do not belong in the tier by selecting the Delete icon. To add any workloads that should be in the group but are not, find the workloads you want and delete them from their current tiers. Then select the Add icon at the upper right in the table header and select the workloads you want to add.

- Review the proposed subnets.

  Confirm, add, edit, or delete the proposed subnets in the tier. Confirm that they all have the same function and have the same security policy requirements. If necessary, you can remove any subnets that do not belong in the tier by selecting the Delete icon. To edit a subnet, select the Edit icon. Click *Add Subnet* as needed to add subnets.
- Approve the tier.

  To keep track of which tiers you have reviewed and approved, when you agree with the workloads or subnets in the tier and the tier function, click *Approve Tier*. The approved tier's status icon will change from a yellow exclamation to a black-and-white check mark. The deployment wizard will automatically advance to select the next tier in the application. Repeat the approval steps for each tier. When all tiers are approved, they will all be marked with a black-and-white check mark, and the deployment wizard takes you to the first connection that needs to be approved.
- Approve the ACL rules.

  Confirm or edit the ACL rules that make up the first connection. ACLs can only be confirmed after the tiers on both ends of the connection are approved. You will see that a connection and the tiers on both sides are selected in pink. Review the tiers' ACL rules in the table below the application map graphic. Either confirm or edit them so that they allow the traffic you want to permit between the two tiers. You can delete a connection by deleting all its ACL rules.
- Add connections.

  In the rare case that a connection between tiers of an application is missing, you can add a connection. On the application map, select the two tiers that you want to connect (Select one tier, press the *Shift* key, and select the second tier). Then select the Add Connection icon under Actions. The system will draw a new connection between the two tiers and present you with an ACL rule that you can edit.
- Merge tiers.

  If Policy Generation has proposed two separate tiers but you think of them as one tier with the same security requirements, then you can merge two tiers of the same type, workload, or subnet. Select one tier, press the *Shift* key, and select the second tier. Then select the Merge Tiers icon under Actions. The two tiers are merged into one and share a combined set of ACL rules. Now review and approve the new tier.
- Delete tiers.

  If you find that a tier does not belong in a proposal, you can use the Assign Tiers feature to assign it to another proposal, or you can delete that tier by selecting the tier and then selecting the Delete Tier icon under Actions. Deleting a workload tier will temporarily free up its workloads, allowing them to be added to other tiers. In the next discovery cycle, Policy Generation will propose application tiers for any freed workloads or subnets.
- Review the Common Services object.

  All common network services that support the functions of the tiers in the business application are grouped into a single Common Services object, displayed in the far-right column of the application map, under the header *External*. These are service applications that are external to the business application, but necessary for its participation in the network. In the preferred workflow, these common services will already be deployed when you are reviewing your business applications. The approval process will not automatically review these service applications. You may select the Common Services object to see a list of the service applications that support this business application.
- Review external tiers.

  In the first and sixth columns of the six-column application map, you might see External Tiers. These are tiers that seem to connect to the proposed business application from the Internet or from other applications. The Any IP Address tier at the top left is a subnet tier, representing any workload or IP address that is outside the network that Policy Generation examined and might represent the Internet or addresses not identified as part of a proposed application. The Tier Member table displays the actual IP addresses that have been detected. Determine what external object exists at these IP addresses and then note the address and description of that object in the tier's *Description* field. You can leave the broad tier definition of all IP addresses, 0.0.0.0/0, or, for each application, you can edit this subnet to fit the address ranges you want to allow.

Any other external tiers in the first column are members of other proposed applications that are sources, only connecting to web tiers of the current proposed application. In the sixth column, below the Common Services object, you might see external tiers from other proposed applications that are sources and/or destinations that connect to other tiers in the current proposed application. To deploy the current application with all its proposed ACL rules, these external tiers must also be reviewed, approved, and deployed.

When all application tiers and connections are approved, you will see the Approval Complete message, giving you the choice to deploy the application now or later. If you are ready to deploy now without anyone else's review, then click *DEPLOY RULES NOW*. Deploying the proposal will prevent further editing of the proposal and will send the rules to the FortiGate device or the alternate policy table if so configured. The rules will be deployed to the specific FortiGate device on which the tier workloads were found. The deployed rules can be seen in FortiOS under *Policy and Objects*. All FortiPolicy-created artifacts can be identified from the comment “FortiPolicy created.”

If you are still using the deployment wizard, the next proposed business application will appear, or you can select the next business application you want to approve and deploy from the Applications table or topology.

If necessary, you can change deployed ACL rules and deployed tiers:

- In FortiPolicy, all deployed rules can be viewed in the *Policy > Access Control* page. New ACL rules can be added, and deployed ACL rules cab be deleted. Although it may appear like you can edit them, you cannot directly edit deployed policy ACL rules in the *Policy > Access Control* table. There is this workaround:

  a. Duplicate the rule you want to change.

  b. Edit the duplicate.

  c. Delete the original rule.

  d. Click *SAVE*.

  The original rule will be deleted from, and the new rule will be added to, all the right VDOMs.

- The easiest way to edit deployed applications is to delete the application by selecting *Delete* from the application's action menu. This will remove all the ACLs and tiers, freeing up all the workload and subnet members of the application. Policy Generation will discover all the connections and propose the application again. Wait until all the connections have been discovered. Then go through the application approval process again. While approving tiers and ACLs, it is relatively easy to edit the proposals, editing, adding, or subtracting workloads, subnets, and ACL rules as you like. After editing the application, deploy it again.

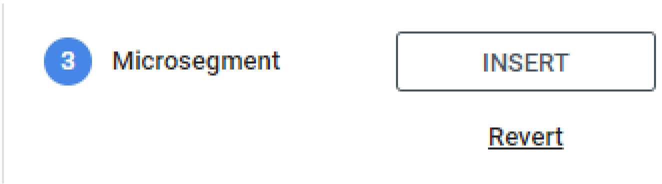
  However, you might want to edit the membership of one tier while the application remains deployed and secure.

  To edit subnet tier members, copy the tier name from the Applications table or from the *Application Details* page. On the *Groupings* page, search for the tier name. From the tier's action menu on the right side of the table row, click *Edit*. On the resulting *Edit Resource Group* page, you can now add, remove, or edits the subnets and then click *SAVE*. The system will automatically deploy the changes tier definitions to the right VDOMs.

Although it is NOT best security practice, for demonstration purposes, you can skip the careful review and approval of each proposed detail and deploy a proposal quickly by selecting the small dropdown arrow in the bottom right corner of the *Application Details* page and then clicking *DEPLOY RULES*.

Step 3: Microsegment

Insertion is the process of configuring the Security Fabric to monitor and regulate an application's traffic. It requires that the ACL rules are deployed to the Security Fabric. Insertion is a prerequisite for the next two action steps (Step 4: Test Policy Rules and Step 5: Secure).



FortiPolicy applies two types of insertion that are facilitated using the FortiGate device’s LAN segment feature:

- Microsegment

  Microsegment essentially puts a firewall around every workload, even those on the same subnet or in the same application tier. All traffic is now monitored and controlled by a FortiGate device. When later enforced, the rules that you have deployed will govern what workloads can talk to each other and what traffic will be blocked. Microsegmentation is more secure than segmentation, but your system's performance will be slower because more traffic is being examined.

  To microsegment a workload, go to *Workspace > Applications*, click the vertical ellipsis at the left end of an application row, and select *Microsegment*. If you click *INSERT* in Step 3 of the *Action Steps* panel, all deployed business applications and common services applications that have not been segmented are microsegmented.
- Segment

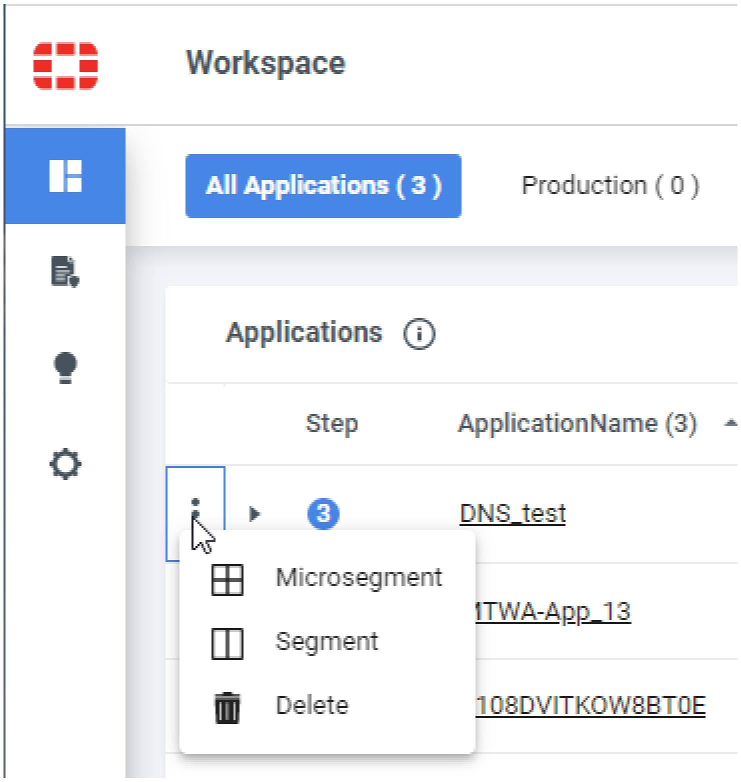
  Segmentation puts a firewall around every application tier. When the security policies are enforced on the FortiGate device, the FortiGate device monitors and controls all traffic between tiers. Traffic within tiers is not controlled by the FortiGate device. Segmentation is less secure than microsegmentation, but your system will perform better. To segment an application tier, go to *Workspace > Applications*, click the vertical ellipsis at the left end of an application row, and select *Segment*.

You might want to wait before inserting deployed applications to allow team members to review your work.

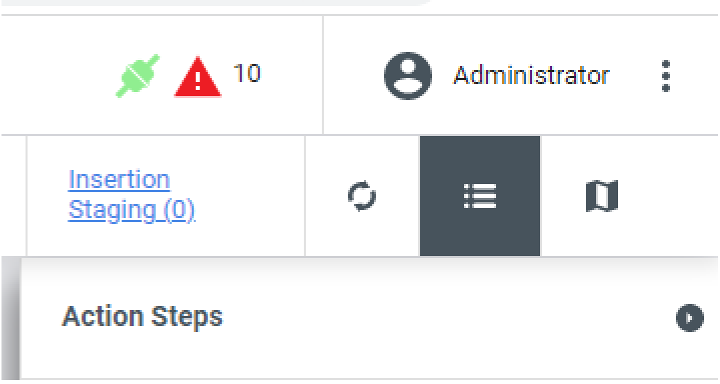
Insertion staging

Insertion Staging allows you to queue one or more deployed applications for insertion. You can queue some applications to microsegment and others to segment. Later you can batch insert the applications in the queue, while leaving others to be inserted later.

To queue an individual deployed application for insertion, click to open the application’s action menu from the application’s table or topology. Then click the insertion type you want from the action menu: *Microsegment* or *Segment*.



Each time you select an insertion type for a deployed application, the system will increment the *Insertion Staging* link near the top right of the *Applications* page. This indicates that the application has been placed into the Insertion Staging queue. You can view the queue at any time by clicking the *Insertion Staging* link. The Insertion Staging queue is located at *Workspace* > *Grouping* > *Insertion Staging*.



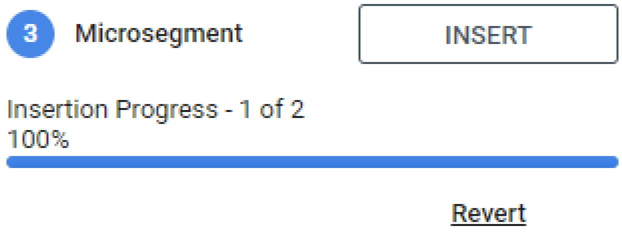
Applications placed into Insertion Staging are queued to be segmented or microsegmented, whichever you chose.

To be selective, click *COMMIT ALL CHANGES* on the *Insertion Staging* page. This executes all the segmentations and microsegmentations that you specified. Deployed applications that have not been queued are not segmented or microsegmented.

To microsegment in bulk, click *INSERT* at Action Step 3: Microsegment. This will do the following:

- Segment or microsegment all applications sitting in the Insertion Staging queue, if any.
- Microsegment all deployed applications that are not inserted and not in the Insertion Staging queue.

The Insertion Progress bar in Step 3: Microsegment tracks insertions. You can also track insertions from the *Workspace > Logs > Jobs* page.



3 Microsegment

Insertion Progress - 1 of 2
100%

If you want to remove insertion for one application, open that application's action menu on the applications table or topology and click *Revert Insertion*. If the application has been enforced, click *Revert Insertion & Enforcement*. This will place the application into Insertion Staging. Click *COMMIT ALL CHANGES* on the *Insertion Staging* page to complete the process of reverting insertion for individually selected applications.

If you want to remove all types of insertion for all deployed and inserted applications, click *Revert* at Step 3: Microsegment. This will revert all applications to the not inserted state, including any individual applications in the Insertion Staging queue.

Step 4: Test policy rules

Now you can test your ACL rules that have been deployed to and inserted on the Security Fabric against live traffic on your fabric, without blocking any traffic until you want to enforce them. Testing will flag any traffic that does not conform to your rules. You can then review these rule "violations" and select one of the following:

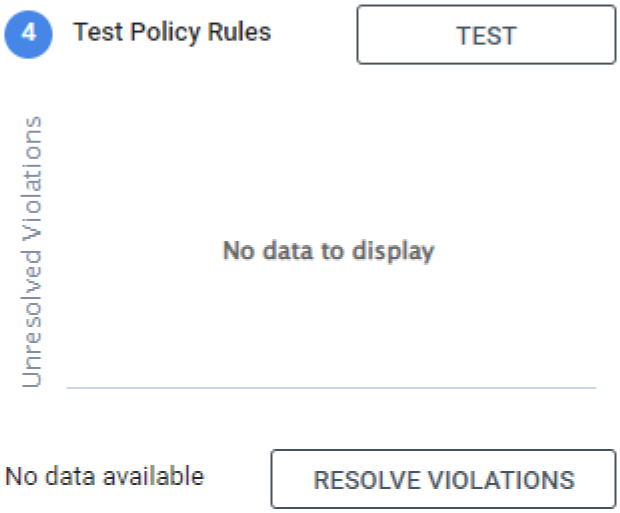
- *Acknowledged as violations*

  This is suspect traffic that you will want to block when you secure your application. This traffic violates your rules, and you do not want to allow it.
- *Acknowledged as legitimate*

  This is valid traffic that either was not detected during connection discovering at Step 1: Discover Connections or that you might have edited out while approving and deploying the application. Now that you are testing against live traffic, you recognize that you should allow this traffic by adding an ACL rule.

You can test all deployed and inserted applications in bulk or be selective about which applications to test when.

To test all deployed and inserted applications, click *TEST* in Action Step 4: Test Policy Rules.



To test only selected deployed and inserted applications, select the applications' action menu on the Applications table or topology. Click *Test ACL Rules* for each application to test.

When application testing starts, the first start time is displayed under the Action Step 4: Test Policy Rules. When the testing system starts, it processes packets against the rule table. All unsecured traffic is allowed to pass. Packets for which there are no rules are:

- Recorded as violation events
- Summarized into unique violation types every hour
- Displayed in the Unresolved Violations chart every 5 minutes

Click *RESOLVE VIOLATIONS* to view a *Unique Violations* page with a table row for each unique violation. Follow the on-screen help on this page to determine if you want to add an ACL rule to allow this traffic or just acknowledge that you want to block such traffic when you enforce security at Action Step 5: Secure.

Resolve violations

Policy Generation compares all packets transmitted since the last time the policy table changed with all the ACL rules for deployed and inserted applications. All packets that match an ACL rule will be set to allow the connection. All packets that do not match an ACL rule will also be allowed. However, they will be logged as a violation of the deployed ACL rules. Multiple packets that are from the same source to the same destination with the same port and protocol will be logged as a single unique violation. Every 5 minutes, the Unresolved Violations chart will record the total number of unique unresolved violations that occurred in that 5-minute period.

The Acknowledged progress bar at the top of the table shows you how many of the unique violations have been acknowledged.

Each row in the chart presents a summary of one unique violation:

- *Start* is the detection time of the first packet from the source to the destination, using the protocol and destination port.
- The *Hit Count* is the number of times that this same connection was detected.
- Click the Events icon to display the *Violation Events Details* page listing all the identical violation events over time.

To allow a connection and resolve a unique violation by adding an allow rule, click the Add Rule icon to bring up a the *Add ACL Rule* dialog. This displays a proposed allow rule preconfigured to match the violation. You can make notes in the *Description* field at the end of the rule. Click *SAVE* to create the new rule. Creating the new rule in this way will automatically check the *Acknowledged* checkbox for the unique violation and increment the Acknowledged progress bar.

To block a connection from the *Resolve Violations* dialog, check the *Acknowledged* checkbox for that row on the Unique Violations table. No rule is created. When you later secure the application, this violation will be blocked.

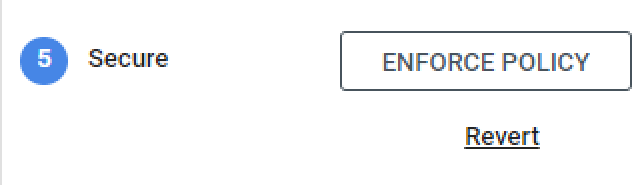
To block many connections, use the Select All checkbox at the top of the page. You can then deselect any rows you do not want to block, click the Add Rule icon to bring up a the *Add ACL Rule* dialog for each row you want to allow, and then click *SAVE*.

When all the violations are resolved and new ones are no longer appearing, you can click *END TESTING* to stop testing and proceed to Step 5: Secure.

If you want to resume testing later, you can do so from the Applications table or topology by selecting *Test ACL Rules* from the action menu for each application to test.

Step 5: Secure

You can now enforce all deployed and inserted ACL rules, or you can choose to only enforce the rules for selected applications.



To enforce ACL rules for one deployed and inserted application at a time:

1. In the Applications table or topology, click the application’s action menu.
2. Click *Enforce ACL Rules*.

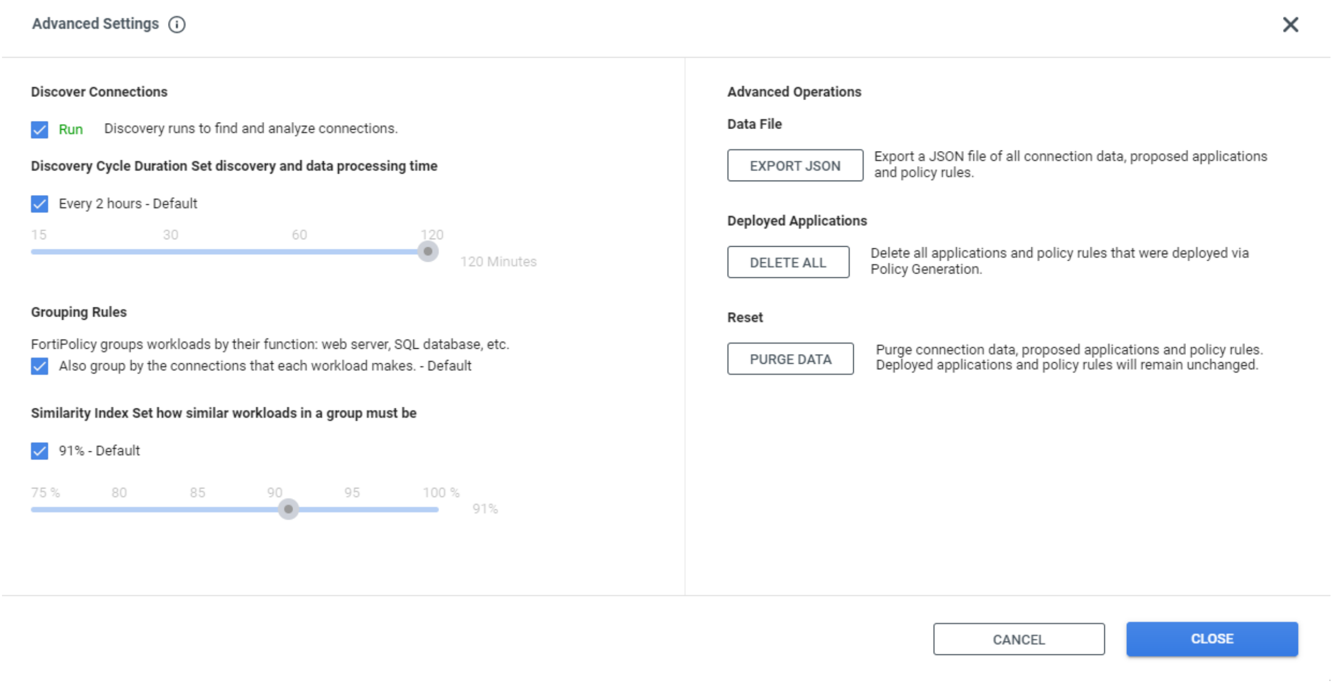
   That application is now secure.
3. If at any time you want to stop enforcing a single application’s ACL rules, click *Revert Enforcement* from the application’s action menu.

To enforce all ACL rules for all deployed and inserted applications:

1. Click *ENFORCE POLICY* at Action Step 5: Secure.

   All your applications are now secure.
2. If at any time you want to stop enforcing all applications’ ACL rules, click *Revert* at Action Step 5: Secure.

Advanced settings



Advanced Settings ⓘ

Discover Connections

☑ Run Discovery runs to find and analyze connections.

Discovery Cycle Duration Set discovery and data processing time

☑ Every 2 hours - Default

Grouping Rules

FortiPolicy groups workloads by their function: web server, SQL database, etc.

☑ Also group by the connections that each workload makes. - Default

Similarity Index Set how similar workloads in a group must be

☑ 91% - Default

Advanced Operations

Data File

EXPORT JSON Export a JSON file of all connection data, proposed applications and policy rules.

Deployed Applications

DELETE ALL Delete all applications and policy rules that were deployed via Policy Generation.

Reset

PURGE DATA Purge connection data, proposed applications and policy rules. Deployed applications and policy rules will remain unchanged.

The following advanced settings are available:

- By default, the *Run* checkbox is selected.

  If you anticipate network disruptions or you want to stop Policy Generation from learning for a period, you can manually stop discovery.

  ### To manually stop connection discovery:

  a. Clear the *RUN* checkbox.
  b. Click *YES* in the *Turn Off Application Discovery* dialog.
  c. Click *CLOSE* in the Advanced Settings dialog.
  d. Click *SAVE and CLOSE* in the Policy Generation wizard.
- By default, the *Every 2 hours - Default* checkbox is selected.

  Policy Generation needs this time to listen to all the workload-to-workload connections. Then it learns from analyzing the data and makes its proposals. Typically, you should let Policy Generation run through many two-hour cycles until it is no longer discovering many new unique connections. However, sometimes for demonstration purposes, an advanced user might shorten the discovery cycle. If you want a shorter discovery period, clear the *Every 2 hours - Default* checkbox and move the slider.
- By default, the *Also group by the connections that each workload makes. - Default* checkbox is selected.

  The default setting groups workloads by function and by connections. In this way, the system can distinguish between the different types of tiers and the different applications.

  Some users only want to group certain types of assets, such as databases. To group your workloads into functional groups, clear the *Also group by the connections that each workload makes – Default* checkbox.
- By default, the *91% - Default* checkbox is selected.

If this setting creates groups that include many workloads that should not be included, clear the checkbox and set the similarity setting a little higher.

If this setting creates groups that do not include all the workloads they should, clear the checkbox and set the similarity setting a little lower.

You can make these adjustments during or after connection discovery. Proposals are recomputed at the end of the next discovery cycle.

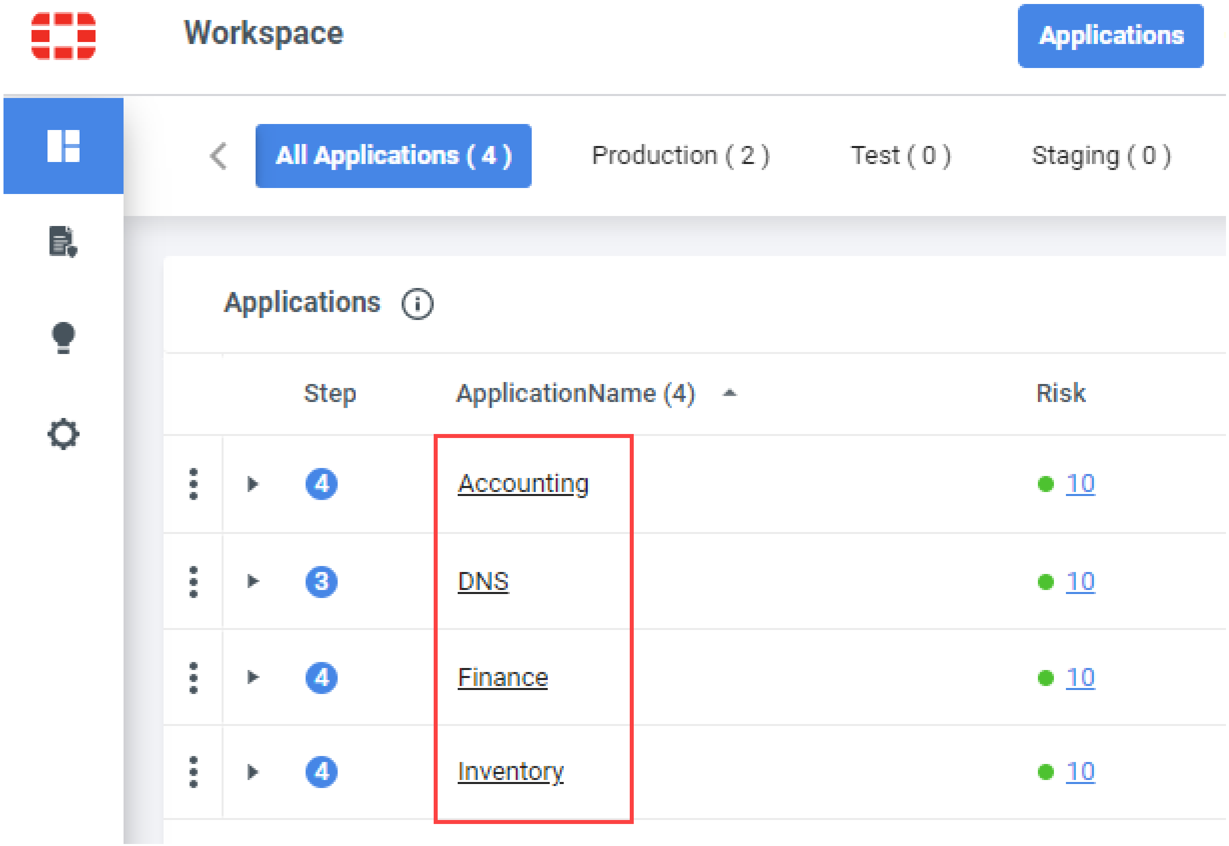
If you have started to verify and implement applications and decide that you need to change this setting, you can click *DELETE ALL*. You can delete individual deployed applications that you are not happy with from the Applications table. Then adjust the similarity index. The next data analysis will continue at the new similarity setting.

- Click *EXPORT JSON* to download a file of all the connections and proposal data that Policy Generation has accumulated. Fortinet Technical Support might request this information for troubleshooting.
- Click *DELETE ALL* to remove all the applications that were deployed to the FortiGate device using Policy Generation in case you want to start over again. This action will take effect after you click *YES* in the confirmation dialog.
- Click *PURGE DATA* to delete existing connection data, proposed applications, and policy rules. Deployed applications are not affected. The *RUN* checkbox will be selected. This action will take effect after you click *YES* in the confirmation dialog.

Applications Details page

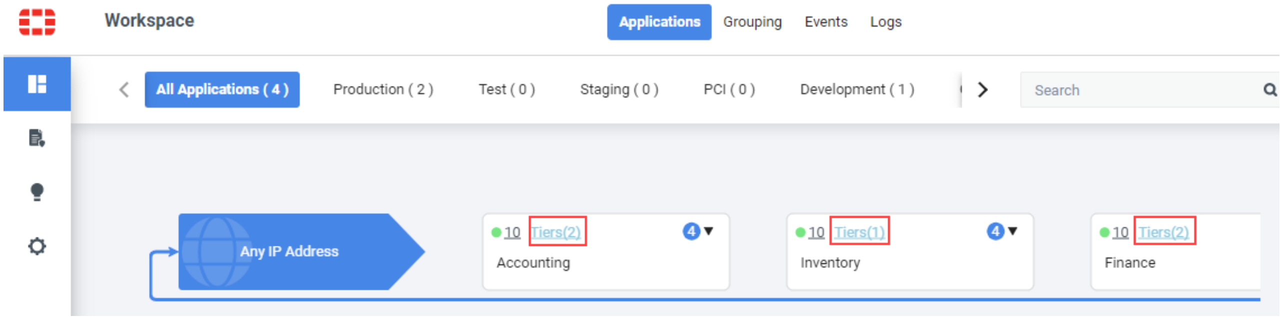
To open the *Applications Details* page, go to *Workspace* > *Applications* and do one of the following actions:

- Click on the application name in the Applications table.



Step	ApplicationName (4)	Risk
4	Accounting	● 10
3	DNS	● 10
4	Finance	● 10
4	Inventory	● 10

- Click *Tiers* in the Application Topology Map.



The *Applications Details* page has four main sections:

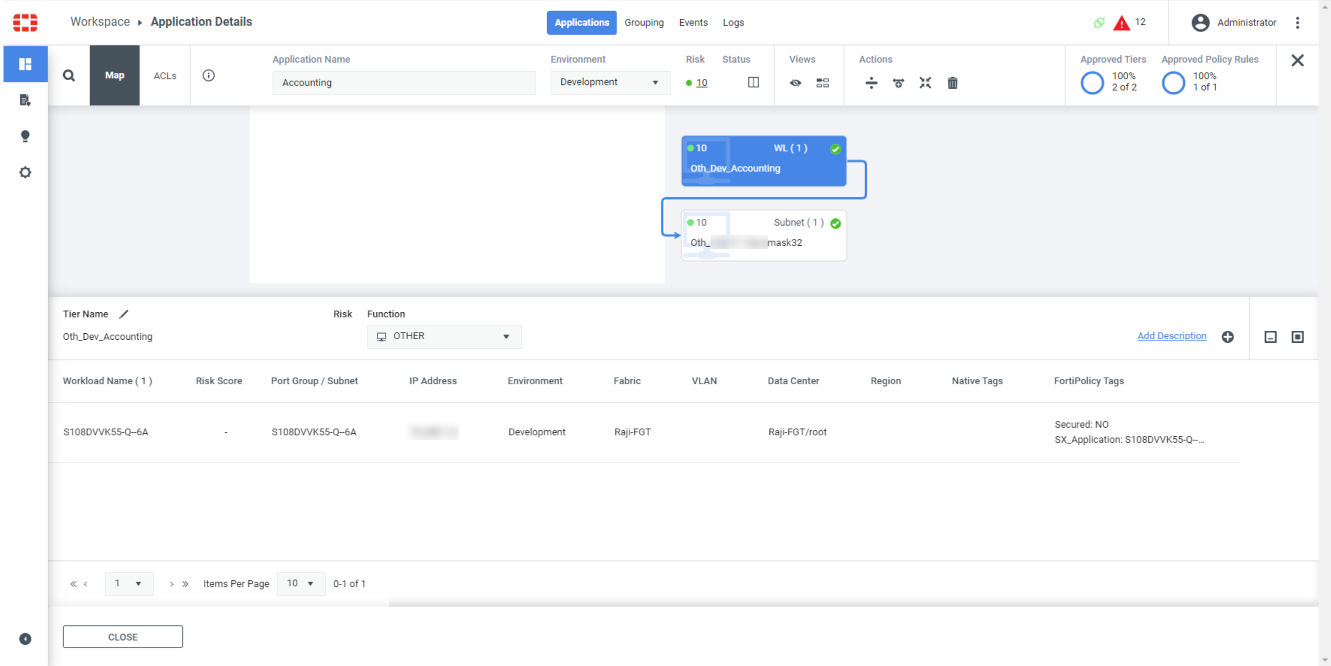
- Header bar

  The header bar has the application name, environment, risk score, status, Views buttons, Actions buttons, number and percentage of approved tiers, number and percentage of approved policy rules.
- Map view

  By default, the Map view is shown when you open the *Applications Detail* page. The Map view shows the proposed tiers and connections.
- Members table

  The members table lists the workloads, subnets, or ACL rules of the object selected in the Map view.
- ACLs view

  Click *ACLs* in the header bar to switch from Map View to ACLs view. The ACLs view lists the proposed ACL rules for the application.



Application Name: Accounting

Environment: Development

Risk: 10

Approved Tiers: 100% 2 of 2

Approved Policy Rules: 100% 1 of 1

Tier Name: Oth_Dev_Accounting

Function: OTHER

Workload Name (1)	Risk Score	Port Group / Subnet	IP Address	Environment	Fabric	VLAN	Data Center	Region	Native Tags	FortiPolicy Tags
S108DVVK55-Q--6A	-	S108DVVK55-Q--6A	[redacted]	Development	Raji-FGT		Raji-FGT/root			Secured: NO SX_Application: S108DVVK55-Q-...

« ‹ 1 › » Items Per Page 10 0-1 of 1

The Actions buttons allow you to do the following:

- Divide combined proposals

  If you have business applications that communicate with each other, Policy Generation might not be able to accurately separate them into unique proposals. If a proposal contains the tiers of two or more applications, then select the *Assign Tiers* icon in the Actions buttons area and assign the tiers to different applications, thus dividing the proposal into two or more proposals. Then approve and deploy each of the new proposals.
- Merge proposals
- Add a connection between selected tiers

  If a connection between tiers of an application is missing, you can add a connection. On the application map, select a tier, then press the Shift key and select another tier. Then click the *Add a Connection* icon in the Actions buttons area. FortiPolicy draws a new connection between the two tiers and presents you with an ACL rule that you can edit.
- Merge two selected tiers of the same member type

  If Policy Generation has proposed two separate tiers but you want them to be one tier with the same security requirements, then you can select two tiers of the same type, workload, or subnet. Select one tier, press the Shift key, and select another tier. Then select the *Merge Two Selected Tiers* icon in the Actions buttons area. The two tiers are merged into one and share a combined set of ACL rules. Now review and approve the new tier.
- Delete selected tier

  If a tier does not belong in a proposal, you can use the Assign Tiers feature described above to assign it to another proposal. Or you can delete that tier by selecting the tier and then selecting the *Delete Tier* icon in the Actions buttons area. Deleting a workload tier will temporarily free up its workloads, allowing them to be added to other tiers. In the next discovery cycle, Policy Generation will propose application tiers for any freed workloads or subnets.

Grouping

The *Grouping* page has two tabs:

- Groups on page 89

  The goal of grouping is to collect infrastructure workloads that share similar security requirements into defined groups.
- Insertion staging on page 93

  FortiPolicy organizes all grouping configurations in the *Insertion Staging* tab for you. When you click *COMMIT ALL CHANGES*, the insertion changes are deployed to the data planes, and segmentation or microsegmentation takes place.

Groups

Resource groups are discovered workloads or subnets with members selected according to their shared or similar security requirements. When workloads enter or leave your environment, the resource groups are automatically updated to reflect the changes.

You can use resource groups as sources and destinations in ACL rules or as filters in Setup Policy Generation.

Deployed application tiers are also resource groups, and they too will appear in the Resource Groups table. Tiers can also respond dynamically to changes in the workload members of your Security Fabric. If new workloads appear and you have used FortiPolicy API endpoints to tag those workloads, they will automatically join any existing tiers with that tag set, and the tier's ACL rules will be applied to the new workload tier members.

There are two types of resource groups:

- Dynamic resource groups
  When FortiPolicy discovers a workload that meets a resource group membership rule, FortiPolicy will dynamically segment or microsegment the port group, thus protecting the workloads.
- Static resource groups
  The FortiPolicy administrator determines where and when to perform segmentation and microsegmentation.

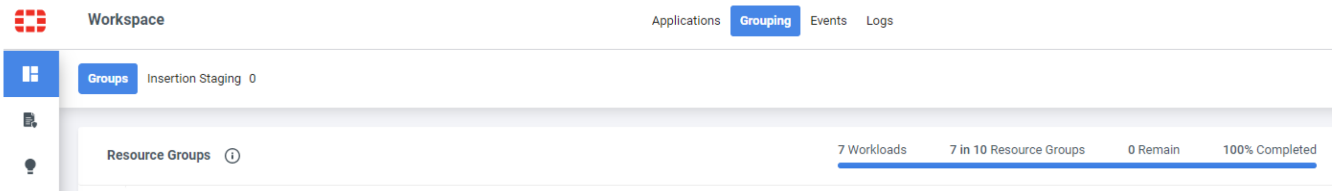
The two types of resource groups can be combined as necessary. For example: an administrator can set up FortiPolicy to perform continuous monitoring and dynamic insertions in inline microsegmentation mode for every resource group, except for a specified set of networks that are configured with *No Insertion*.

Microsegmentation, segmentation, and ACL rules are defined per resource group.

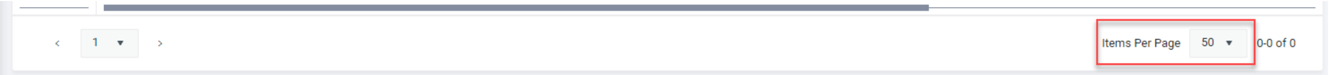
Security controls (threat prevention, malware, and URL filtering) are collected into security policy sets and then applied to resource groups after grouping and insertion. ACL rules are applied to resource groups; security policy sets are bound to resource groups; and the security policy sets are enacted during segmentation and microsegmentation in a deployed data plane.

You can create a new resource group or edit, copy, or delete existing resource groups.

FortiPolicy provides a dynamic accounting of all workloads discovered in the infrastructure. As resource group assignments are configured, you can track your progress using this accounting bar at the top of the page.

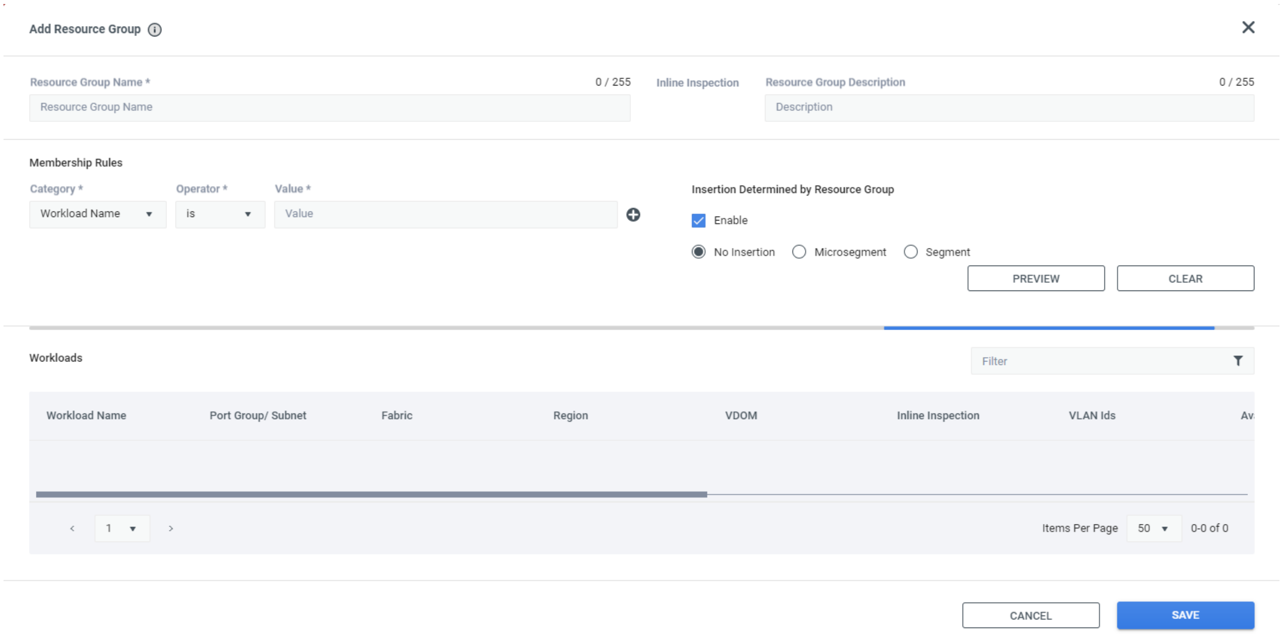


All workloads from all infrastructures are displayed when the *Groups* page loads. By default, 50 rows are displayed. To adjust the number of rows displayed, select the number of rows from the *Items Per Page* dropdown list at the bottom of the *Groups* page.



To create a dynamic resource group:

1. Go to *Workspace* > *Grouping* > *Groups*.
2. Click the + icon in the upper right corner of the *Groups* page.
3. In the *Add Resource Group* dialog, enter a name and description for the new group.



Add Resource Group

Resource Group Name * 0 / 255 Resource Group Name

Inline Inspection

Resource Group Description 0 / 255 Description

Membership Rules

Category * Workload Name ▾ Operator * is ▾ Value * Value

Insertion Determined by Resource Group

☑ Enable

● No Insertion ○ Microsegment ○ Segment

Workloads

Workload Name	Port Group/ Subnet	Fabric	Region	VDOM	Inline Inspection	VLAN Ids	Av

Items Per Page 50 ▾ 0-0 of 0

The name and description might describe the role of this group as a particular tier of a production instance of a particular application in your network. Enter a name that will help you choose this resource group when you are creating ACL rules.

4. Use the *Membership Rules* options to create logical filters to define groups of workloads or IP addresses. The membership of resource groups is not static. When there are changes in your environment, membership is adjusted automatically, based on your rules.

   Use the *Category* filter to select one of the following categories:

   - *Workload Name*

     Select this category if you want to explicitly create a static list the workloads in the resource group or if your naming convention corresponds to the security-related roles of each workload.
   - *Port Group/Subnet*

     Select this category if all workloads on a port group perform exactly the same role.
   - *Subnet*

     Select this category if you are specifying endpoints outside the examined network, and no Workloads table is presented.
   - *FortiPolicy Tag*

     This category is not supported in FortiPolicy 7.2.0.
   - *Native Tag*

     This category is not supported in FortiPolicy 7.2.0.

5. Select an operator and enter a value:
   - *is* specifies matching the exact name
   - *contains* specifies matching all names with the entered value in any position
   - *begins with* specifies matching all names that begin with the entered value

6. Create as many rules as you need to define all the members of the resource group.

   Click the plus sign in the *Membership Rules* area to create another filter setting rule.

7. Select the *Enable* checkbox to select the type of insertion and then click *Microsegment*, *Segment*, or *No Insertion*.

   See Segmentation versus microsegmentation on page 92 for details.

8. Click *PREVIEW* to see if your rules return all the current members of the resource group you are defining. Edit the rules as necessary and click *PREVIEW* again until you are satisfied. If new members that meet these rules arise in the future, they will automatically be included in the resource group and will automatically receive the configurations and protections you have assigned to the group.
9. Click *SAVE*.

   Any resource group with Segment or Microsegment insertion is sent to the *Insertion Staging* page to await your further insertion action. View the configured resource groups in the *Insertion Staging* page and then commit the insertion changes by clicking *COMMIT ALL CHANGES*.

To create a static resource group:

1. Go to *Workspace* > *Grouping* > *Groups* page, click the vertical ellipsis in one of the rows, and select *Edit*.
2. Enter the values in the fields for the members of the resource group.
3. Click the plus sign to add another row.
4. Click *SAVE*.

Segmentation versus microsegmentation

Insertion is the process of configuring the Security Fabric to monitor and regulate an application’s traffic. You have three insertion choices:

- *Segment*—Segmentation puts a firewall around an application tier or resource group. When the security policies are enforced on the FortiGate device, the FortiGate device monitors and controls all traffic among tiers. Traffic within tiers is not monitored or controlled by the FortiGate device. Segmentation is less secure than microsegmentation, but your system will perform better.
- *Microsegment*—Microsegmentation secures each workload, even workloads on the same subnet or in the same application tier or resource group. When the security policies are enforced on the FortiGate device, the FortiGate device monitors and controls all traffic among workloads. Microsegmentation is more secure than segmentation, but your system's performance will be slower because more traffic is being examined.
- *No Insertion*—This setting prevents segmentation and microsegmentation on the workloads within the resource group. The *No Insertion* option is the default insertion setting for a new resource group.

Subnet service applications are a special case. If you use an outside service for DNS, NTP, and so on, Policy Generation will propose these services as applications with tiers that are only IP addresses on one or more subnets and not as workloads within your managed network. These subnet service applications can be approved and deployed, but they cannot be segmented, microsegmented, tested, or secured. They are only secured to the extent that the workload tiers they connect to directly are segmented, microsegmented, tested, and secured. After they are deployed, they are marked as stage 3, and there are no further actions to take on them in FortiPolicy, except to view their details and delete them if you are no longer using them.

If any case should arise where the insertion type of one resource group overlaps with other types, the setting with the first priority prevails and determines the insertion type for that port group.

Priority	Description
First	Microsegmentation has the first priority.

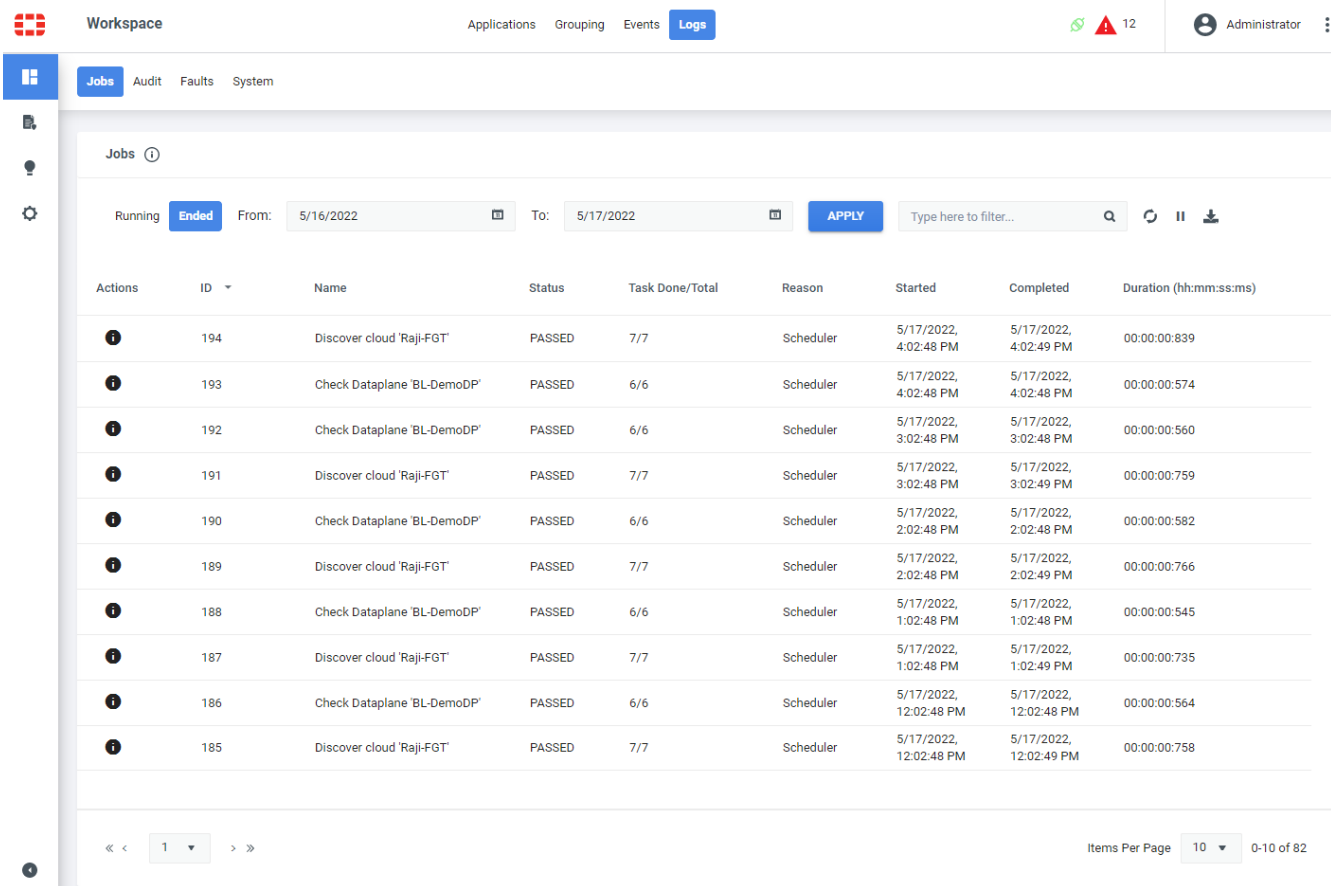
Priority	Description
Second	Segmentation has the second priority.
Third	*No Insertion* has the third priority and applies when no other insertion mode preempts it.

When you create resource groups, the object itself is created immediately. However, any insertion actions specified are saved into Insertion Staging so that you can carefully review network changes and pick when you want to commit batch processing of those changes.

Troubleshooting: Job tracking

To see the real-time progress of a job, go to *Workspace* > *Logs* > *Jobs* and click *Running*.

To see jobs that have completed, go to *Workspace* > *Logs* > *Jobs* and click *Ended*.



Actions	ID	Name	Status	Task Done/Total	Reason	Started	Completed	Duration (hh:mm:ss:ms)
●	194	Discover cloud 'Raji-FGT'	PASSED	7/7	Scheduler	5/17/2022, 4:02:48 PM	5/17/2022, 4:02:49 PM	00:00:00:839
●	193	Check Dataplane 'BL-DemoDP'	PASSED	6/6	Scheduler	5/17/2022, 4:02:48 PM	5/17/2022, 4:02:48 PM	00:00:00:574
●	192	Check Dataplane 'BL-DemoDP'	PASSED	6/6	Scheduler	5/17/2022, 3:02:48 PM	5/17/2022, 3:02:48 PM	00:00:00:560
●	191	Discover cloud 'Raji-FGT'	PASSED	7/7	Scheduler	5/17/2022, 3:02:48 PM	5/17/2022, 3:02:49 PM	00:00:00:759
●	190	Check Dataplane 'BL-DemoDP'	PASSED	6/6	Scheduler	5/17/2022, 2:02:48 PM	5/17/2022, 2:02:48 PM	00:00:00:582
●	189	Discover cloud 'Raji-FGT'	PASSED	7/7	Scheduler	5/17/2022, 2:02:48 PM	5/17/2022, 2:02:49 PM	00:00:00:766
●	188	Check Dataplane 'BL-DemoDP'	PASSED	6/6	Scheduler	5/17/2022, 1:02:48 PM	5/17/2022, 1:02:48 PM	00:00:00:545
●	187	Discover cloud 'Raji-FGT'	PASSED	7/7	Scheduler	5/17/2022, 1:02:48 PM	5/17/2022, 1:02:49 PM	00:00:00:735
●	186	Check Dataplane 'BL-DemoDP'	PASSED	6/6	Scheduler	5/17/2022, 12:02:48 PM	5/17/2022, 12:02:48 PM	00:00:00:564
●	185	Discover cloud 'Raji-FGT'	PASSED	7/7	Scheduler	5/17/2022, 12:02:48 PM	5/17/2022, 12:02:49 PM	00:00:00:758

Insertion staging

After reviewing all insertion actions, click *COMMIT ALL CHANGES*. This will queue multiple jobs to run, which will configure each affected data plane to support the insertion actions you have specified.

After the data planes are configured, they will automatically respond dynamically to changes in your Security Fabric and enforce your security policy assignments.

Events

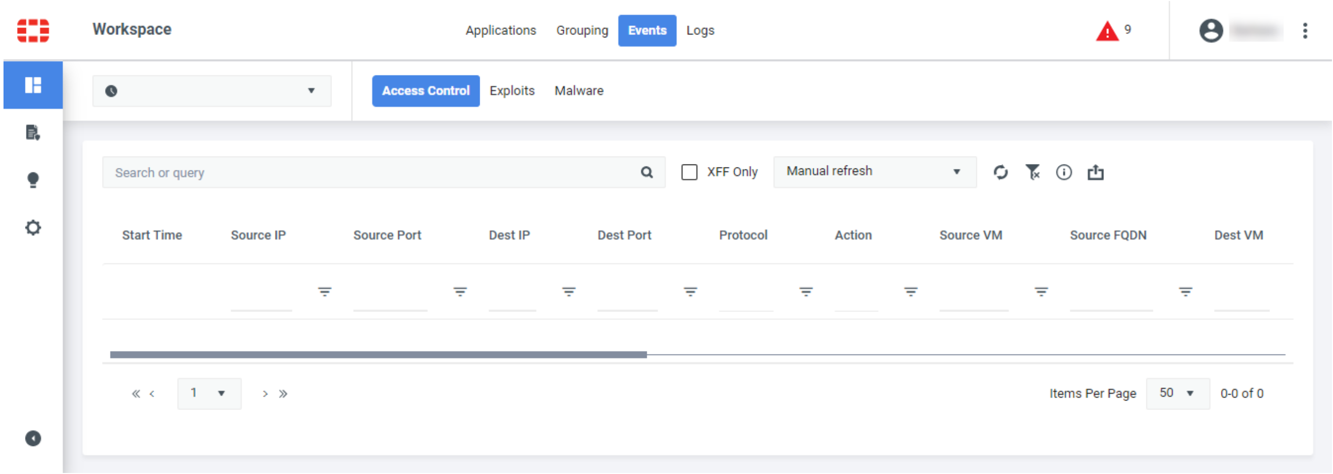
The *Events* page has three tabs:

- Access control, exploits, and malware on page 94

Access control, exploits, and malware

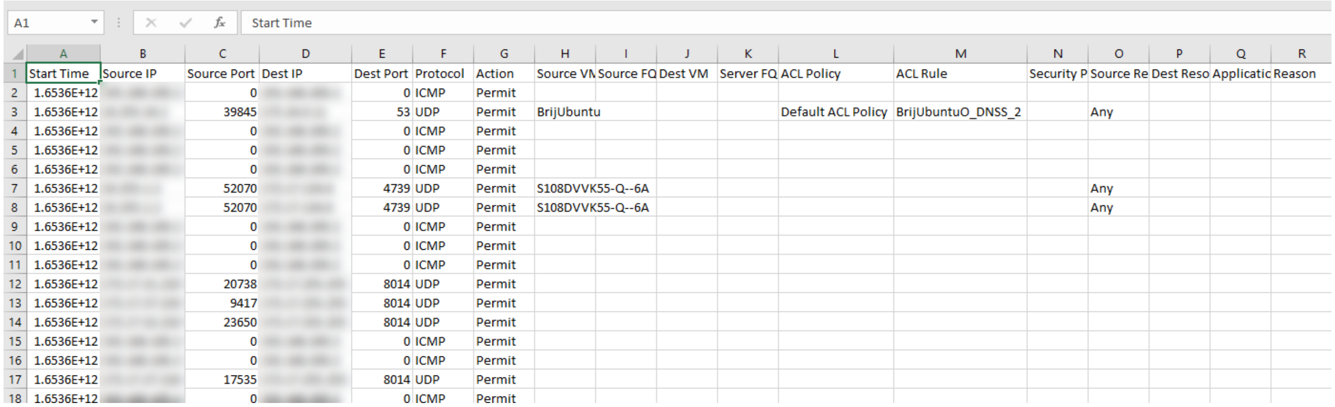
Use the event correlation explorer (ECE) to create tables or graphs that display correlated FortiPolicy event analysis data. You can also export generated analysis data for reporting.

Go to *Workspace* > *Events* to access the event correlation explorer.



After creating and populating a table with selected filters (or selected "attributes" for graph displays), arrange the columns and sort the column data, as needed. After setting the table criteria, click the export icon at the top of the page to export the analysis results.

An example of exported analysis data is shown in the following figure.



A1 Start Time

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
1	Start Time	Source IP	Source Port	Dest IP	Dest Port	Protocol	Action	Source VM	Source FQ	Dest VM	Server FQ	ACL Policy	ACL Rule	Security P	Source Re	Dest Reso	Applicatic	Reason
2	1.6536E+12	[redacted]	0	[redacted]	0	ICMP	Permit											
3	1.6536E+12	[redacted]	39845	[redacted]	53	UDP	Permit	BrijUbuntu				Default ACL Policy	BrijUbuntuO_DNSS_2		Any			
4	1.6536E+12	[redacted]	0	[redacted]	0	ICMP	Permit											
5	1.6536E+12	[redacted]	0	[redacted]	0	ICMP	Permit											
6	1.6536E+12	[redacted]	0	[redacted]	0	ICMP	Permit											
7	1.6536E+12	[redacted]	52070	[redacted]	4739	UDP	Permit	S108DVVK55-Q--6A							Any			
8	1.6536E+12	[redacted]	52070	[redacted]	4739	UDP	Permit	S108DVVK55-Q--6A							Any			
9	1.6536E+12	[redacted]	0	[redacted]	0	ICMP	Permit											
10	1.6536E+12	[redacted]	0	[redacted]	0	ICMP	Permit											
11	1.6536E+12	[redacted]	0	[redacted]	0	ICMP	Permit											
12	1.6536E+12	[redacted]	20738	[redacted]	8014	UDP	Permit											
13	1.6536E+12	[redacted]	9417	[redacted]	8014	UDP	Permit											
14	1.6536E+12	[redacted]	23650	[redacted]	8014	UDP	Permit											
15	1.6536E+12	[redacted]	0	[redacted]	0	ICMP	Permit											
16	1.6536E+12	[redacted]	0	[redacted]	0	ICMP	Permit											
17	1.6536E+12	[redacted]	17535	[redacted]	8014	UDP	Permit											
18	1.6536E+12	[redacted]	0	[redacted]	0	ICMP	Permit											

The event correlation explorer analyzes access control, exploit, and malware events.

ECE is the primary tool for viewing ACL instances and ACL events.

To use the ECE:

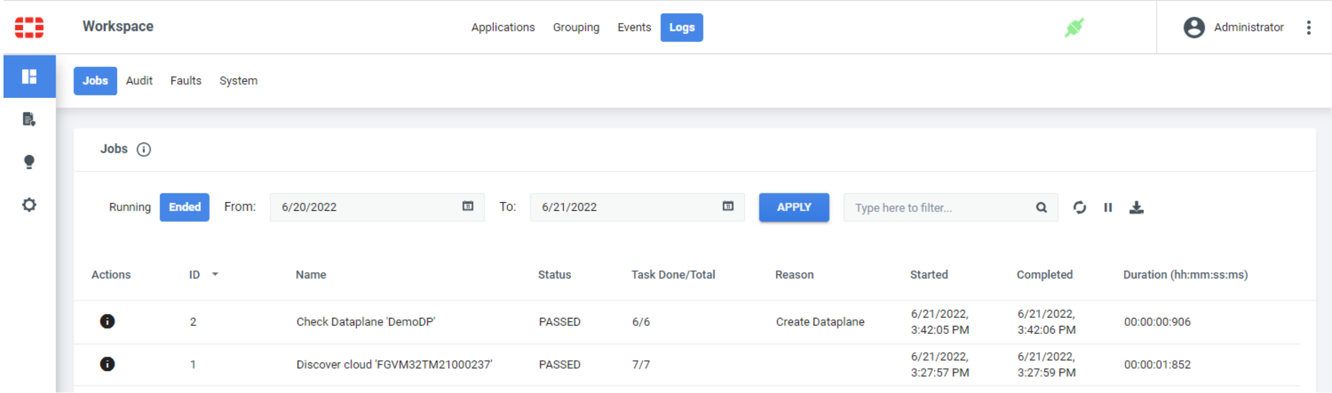
1. Go to *Workspace* > *Events*.
2. Select the type of events to analyze: *Access Control*, *Exploits*, or *Malware*.
3. Set a time period to analyze: *Last Hour*, *Last 2 Hours*, *Last 24 Hours*, *Last 7 Days*, or *Last 30 Days*.
4. Click each column heading to sort the data in ascending or descending order.
5. Click the filter icon under the column heading to filter the data in that column.
6. Click the Refresh icon to update the table data.
7. Click the Clear All Filters icon to show all events.
8. Click the Export Data icon to export the analysis results as a comma-separated values (CSV) file.

Logs

Go to *Workspace* > *Logs* to view the four types of logs:

- Jobs log on page 96
- Audit log on page 96
- Faults log on page 97
- System logs on page 98

Jobs log



Actions	ID	Name	Status	Task Done/Total	Reason	Started	Completed	Duration (hh:mm:ss:ms)
●	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
●	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

The Jobs log provides real-time insight into deployment and insertion processes and progress. The Jobs facility executes operational system and security tasks in a certain order, either sequential or in parallel, and these executions are displayed on the FortiPolicy Jobs log so users can track whether a job passed or failed.

While the Jobs tracking tool assists an administrator with confirmation that a job passed, there is no need for an administrator to be concerned about the job content unless there is a job event that requires investigation.

To investigate Job details, click the “i” icon at the beginning of each Job row. Use the *Tasks* page to identify where an issue might have occurred and the possible cause.

To stop a running job, click the pause icon above the Jobs table.

FortiPolicy does not interpret errors produced by third parties such as VMware. Whenever those vendors produce an error, that error is displayed in the Jobs table exactly as relayed. Corrective action by the user requires the user first interpret the failure in the context of the infrastructure named and the task attempted, which is typically suggested in the task name itself.

Audit log

The Audit log records all configuration changes generated by a user, including configuration events that take place with the FortiPolicy API and CLI.

The FortiPolicy administrator determines which users can view audit records based on role assignment. By default, access to the Audit log is denied to everyone except those with the GlobalAdministrator role. No user can purge or modify an Audit log in any way. See Users on page 127 to specify which users can access the audit log.

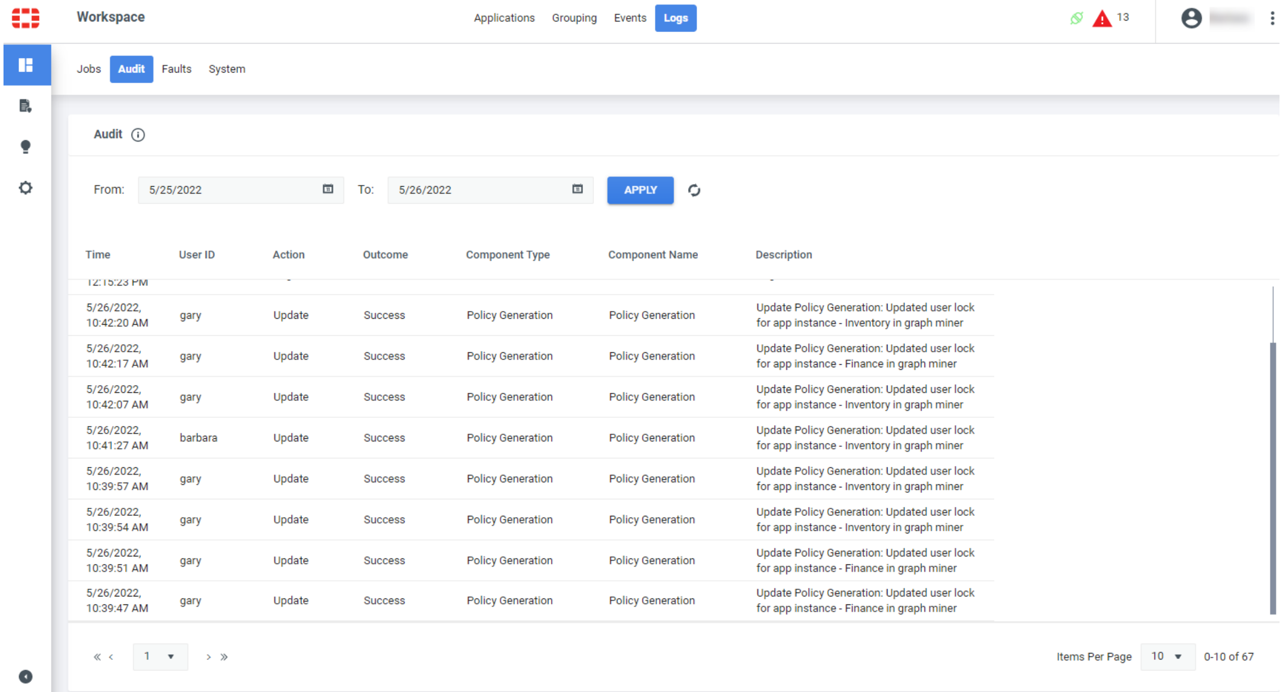
The following table lists the information in each record in the Audit log.

Audit Log Data	Example
Time	Date and time for the action
User ID	User name
Action	Update, Login, Add, Logout, Edit

Audit Log Data	Example
Outcome	Success or Failure
Component type	The part of the system acted on by the user, for example, Policy Generation.
Component name	Name of the component
Description	More information about the action

To filter and search the audit log:

1. Go to *Workspace* > *Logs* > *Audit*.



From: 5/25/2022 To: 5/26/2022

Time	User ID	Action	Outcome	Component Type	Component Name	Description
12:15:23 PM						
5/26/2022, 10:42:20 AM	gary	Update	Success	Policy Generation	Policy Generation	Update Policy Generation: Updated user lock for app instance - Inventory in graph miner
5/26/2022, 10:42:17 AM	gary	Update	Success	Policy Generation	Policy Generation	Update Policy Generation: Updated user lock for app instance - Finance in graph miner
5/26/2022, 10:42:07 AM	gary	Update	Success	Policy Generation	Policy Generation	Update Policy Generation: Updated user lock for app instance - Inventory in graph miner
5/26/2022, 10:41:27 AM	barbara	Update	Success	Policy Generation	Policy Generation	Update Policy Generation: Updated user lock for app instance - Inventory in graph miner
5/26/2022, 10:39:57 AM	gary	Update	Success	Policy Generation	Policy Generation	Update Policy Generation: Updated user lock for app instance - Inventory in graph miner
5/26/2022, 10:39:54 AM	gary	Update	Success	Policy Generation	Policy Generation	Update Policy Generation: Updated user lock for app instance - Inventory in graph miner
5/26/2022, 10:39:51 AM	gary	Update	Success	Policy Generation	Policy Generation	Update Policy Generation: Updated user lock for app instance - Finance in graph miner
5/26/2022, 10:39:47 AM	gary	Update	Success	Policy Generation	Policy Generation	Update Policy Generation: Updated user lock for app instance - Finance in graph miner

Items Per Page 10 0-10 of 67

2. Filter by a time interval by selecting the *From* date and *To* date and then clicking *APPLY*.
3. You can click on the column headings to change the sort order.

Audit log records are archived automatically. A FortiPolicy administrator can configure how long to save Audit log records. By default, Audit log records are saved for 7 years.

Faults log

The FortiPolicy Faults log records exceptions, system errors, faults, and related issues that arise during FortiPolicy operations. A fault will stay in the Faults log until an administrator acknowledges it or deletes it.

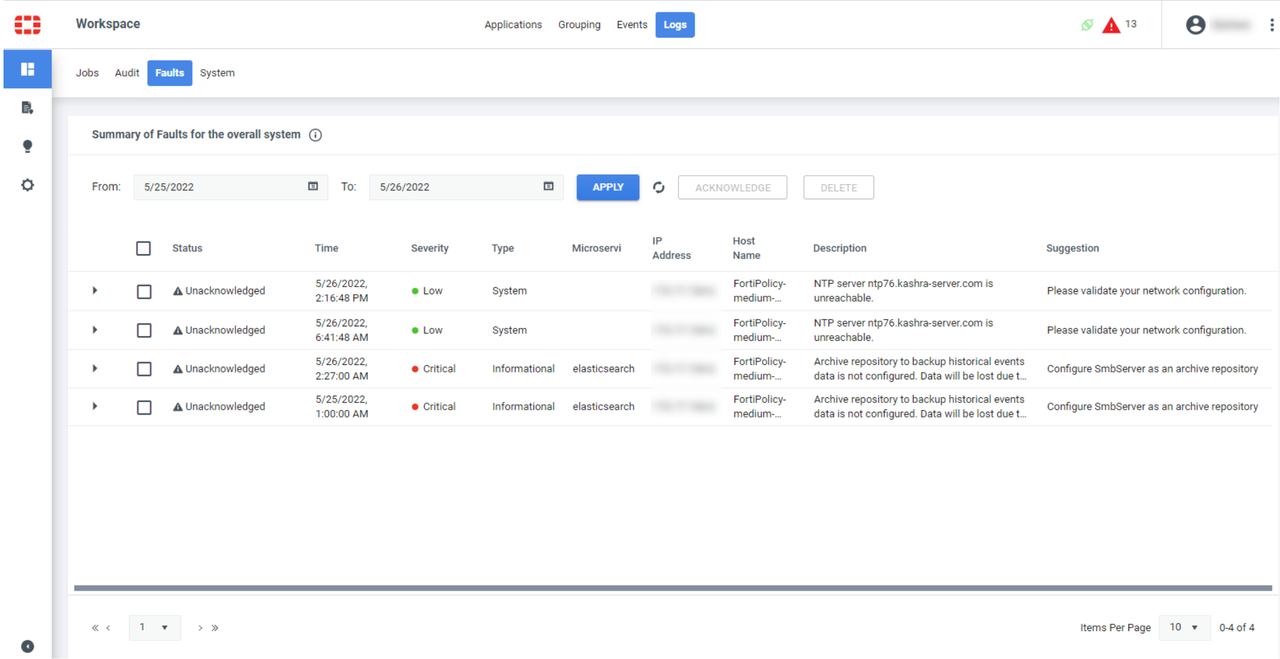
Use the Faults log page to view and search for specific faults, based on date, time, or search string, such as microservice or description.

All fault entries are initially displayed as *Unacknowledged* (that is, not yet examined or investigated). After you mark a fault as *Acknowledged*, the fault appears as acknowledged to all users.

The number of unacknowledged faults is displayed in the header bar at the top of every FortiPolicy page so that an administrator is alerted to new faults.

To filter and search the Faults log:

1. Go to *Workspace* > *Logs* > *Faults*.



Summary of Faults for the overall system

From: 5/25/2022 To: 5/26/2022 APPLY ACKNOWLEDGE DELETE

	□	Status	Time	Severity	Type	Microservi	IP Address	Host Name	Description	Suggestion
▸	□	⚠ Unacknowledged	5/26/2022, 2:16:48 PM	● Low	System		[redacted]	FortiPolicy-medium-...	NTP server ntp76.kashra-server.com is unreachable.	Please validate your network configuration.
▸	□	⚠ Unacknowledged	5/26/2022, 6:41:48 AM	● Low	System		[redacted]	FortiPolicy-medium-...	NTP server ntp76.kashra-server.com is unreachable.	Please validate your network configuration.
▸	□	⚠ Unacknowledged	5/26/2022, 2:27:00 AM	● Critical	Informational	elasticsearch	[redacted]	FortiPolicy-medium-...	Archive repository to backup historical events data is not configured. Data will be lost due t...	Configure SmbServer as an archive repository
▸	□	⚠ Unacknowledged	5/25/2022, 1:00:00 AM	● Critical	Informational	elasticsearch	[redacted]	FortiPolicy-medium-...	Archive repository to backup historical events data is not configured. Data will be lost due t...	Configure SmbServer as an archive repository

« ‹ 1 › » Items Per Page 10 0-4 of 4

2. Filter by a time interval by selecting the *From* date and *To* date and then clicking *APPLY*.
3. You can click on the column headings to change the sort order.
4. To expand a fault row to display more information, click the arrow at the beginning of the row.
5. To acknowledge an Unacknowledged fault, expand the row, select the fault, and click *ACKNOWLEDGE* above the table.

   Acknowledging a fault updates the Unacknowledged Faults icon at the top of all FortiPolicy pages.
6. To delete a fault, select the fault and click *DELETE* above the table.

The Audit log creates a record of the User ID of each individual that marks a fault as acknowledged.

Email notification of faults is available.

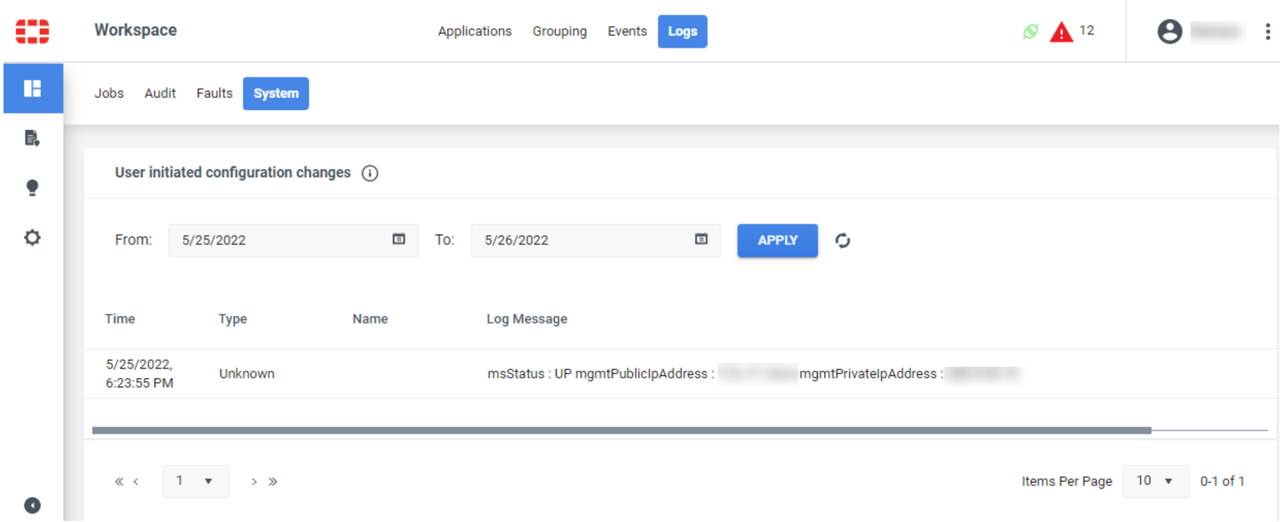
System logs

View and filter the following information in the FortiPolicy System log.

System Log Data	Example
Time	Date and time of the user-initiated configuration change
Type	Type of microservice, for example, DPI, SI, or TLS
Name	Name of the microservice
Log Message	Message logged for a user-initiated configuration change

To filter and search a system log:

1. Go to *Workspace* > *Logs* > *System*.



User initiated configuration changes

From: 5/25/2022 To: 5/26/2022 APPLY

Time	Type	Name	Log Message
5/25/2022, 6:23:55 PM	Unknown		msStatus : UP mgmtPublicIpAddress : [redacted] mgmtPrivateIpAddress : [redacted]

2. Filter by a time interval by selecting the *From* date and *To* date and then clicking *APPLY*.
3. You can click on the column headings to change the sort order.

Customizing policies

Use the *Policy* page to create access control lists (ACLs) .

The *Policy* page has two tabs:

- Access control on page 100
- Security on page 1

Access control

The ACL policy uses an ordered set of ACL rules that specify precedence and the behavior of object groups to which workloads can connect, as well as the applications used during the connection. The ACL policy is assigned to the Security Fabric.

Microsegmentation is essentially security policy applied on a per workload basis.

FortiPolicy ACL policy rules are defined with selectors and response actions. Multiple values can be specified within a selector using OR semantics. For example, an ACL policy can be applied to a Data Center App Tier object group to allow connections to a database tier and subnets.

Policy Generation proposes ACL policies with an “implicit deny all” rule at the end. All proposed rules are permit (allow) rules. Any packet for which there is not an explicit permit rule is denied. The following table shows a sample ACL rule ordering.

Rule order	Rule name	Enabled	Description	Service or AppID	Action
1	Allow DB Tier	Yes	Database rule	MySQL400LJ	Permit
2	Allow AllToThree	Yes	Access to DHCP, DNS, and so on	TCP	Permit
3	Allow AllToTwo	Yes	Two available to all	UDP	Permit
4	Implicit DenyAll	Yes	Default	Any	Deny

Configuring ACL policies

A FortiPolicy ACL policy is an ordered set of rules that govern the ability of workloads to make connections. The ACL policy is assigned to the Security Fabric. An ACL policy’s ordered set of ACL rules specify a hierarchy of precedence and behavior applied to resource groups to which workloads can connect (permit a connection or deny a connection), including access to the applications or protocols used during the connection, as part of FortiPolicy continuous monitoring and inspection.

ACLs are part of every Security Fabric configuration. This requirement allows you to create ACLs between workloads in different data planes. In fact, you control which ACL is applied to a resource group from inside an ACL policy rule set.

ACL policies in FortiPolicy are defined with selectors and response actions. For example, an ACL policy can be applied to a Data Center Web Tier resource group to PERMIT connections to an Application Tier and external IP addresses.

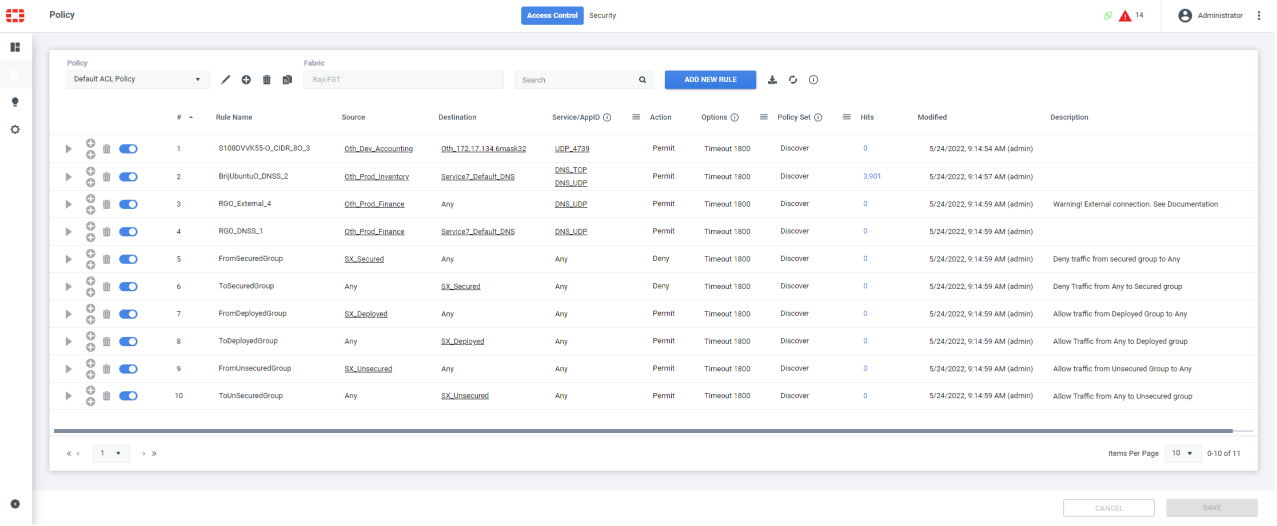
You can configure access control reporting that includes options to schedule and generate monthly or quarterly audit report(s). Configure report generation for either default or custom ACLs, as needed. Go to *Configuration* > *Reports* > *Access Control Rules* to configure. You will need the path to a location on an SMB server to generate the report.

From the *Policy* > *Access Control* page, you can create a new ACL policy and new ACL rules, or you can edit the Default ACL Policy and add rules to customize it.

Do NOT edit deployed ACL rules in FortiPolicy. Edit deployed ACL rules in the FortiGates' Access Control tables.

To create a new ACL policy and ACL rules:

1. Go to *Policy* > *Access Control*.
   The rules in the Default ACL Policy are displayed by default in the table. If there are other ACL policies configured, you can select them from the *Policy* dropdown list.

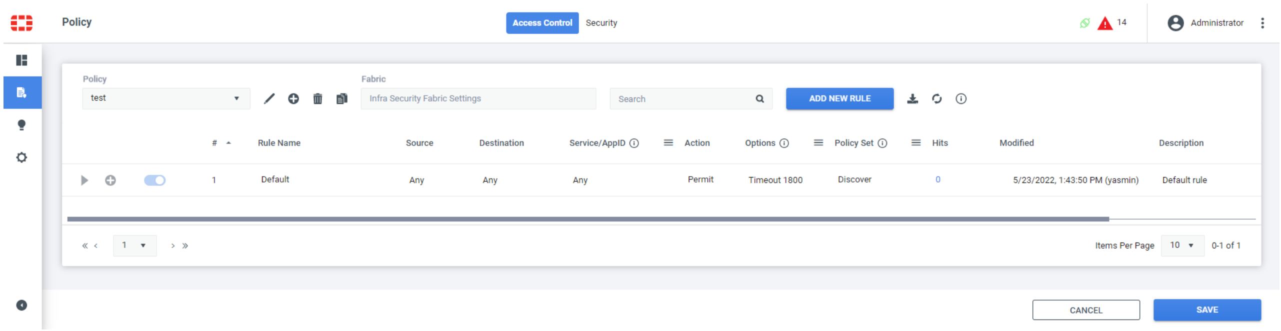


Policy: Default ACL Policy
Fabric: Raji-FGT
Search

#	Rule Name	Source	Destination	Service/AppID	Action	Options	Policy Set	Hits	Modified	Description
1	S108DVVK55-O_CIDR_80_3	Oth_Dev_Accounting	Oth_172.17.134.6mask32	UDP_4739	Permit	Timeout 1800	Discover	0	5/24/2022, 9:14:54 AM (admin)	
2	BrijUbuntuO_DNSS_2	Oth_Prod_Inventory	Service7_Default_DNS	DNS_TCP DNS_UDP	Permit	Timeout 1800	Discover	3,901	5/24/2022, 9:14:57 AM (admin)	
3	RGO_External_4	Oth_Prod_Finance	Any	DNS_UDP	Permit	Timeout 1800	Discover	0	5/24/2022, 9:14:59 AM (admin)	Warning! External connection. See Documentation
4	RGO_DNSS_1	Oth_Prod_Finance	Service7_Default_DNS	DNS_UDP	Permit	Timeout 1800	Discover	0	5/24/2022, 9:14:59 AM (admin)	
5	FromSecuredGroup	SX_Secured	Any	Any	Deny	Timeout 1800	Discover	0	5/24/2022, 9:14:59 AM (admin)	Deny traffic from secured group to Any
6	ToSecuredGroup	Any	SX_Secured	Any	Deny	Timeout 1800	Discover	0	5/24/2022, 9:14:59 AM (admin)	Deny Traffic from Any to Secured group
7	FromDeployedGroup	SX_Deployed	Any	Any	Permit	Timeout 1800	Discover	0	5/24/2022, 9:14:59 AM (admin)	Allow traffic from Deployed Group to Any
8	ToDeployedGroup	Any	SX_Deployed	Any	Permit	Timeout 1800	Discover	0	5/24/2022, 9:14:59 AM (admin)	Allow Traffic from Any to Deployed group
9	FromUnsecuredGroup	SX_Unsecured	Any	Any	Permit	Timeout 1800	Discover	0	5/24/2022, 9:14:59 AM (admin)	Allow traffic from Unsecured Group to Any
10	ToUnSecuredGroup	Any	SX_Unsecured	Any	Permit	Timeout 1800	Discover	0	5/24/2022, 9:14:59 AM (admin)	Allow Traffic from Any to Unsecured group

« ‹ 1 › »
Items Per Page 10 0-10 of 11

2. To create a new ACL policy, click the + icon, enter a name for the new policy, and click *SAVE*.



Policy: test

Fabric: Infra Security Fabric Settings

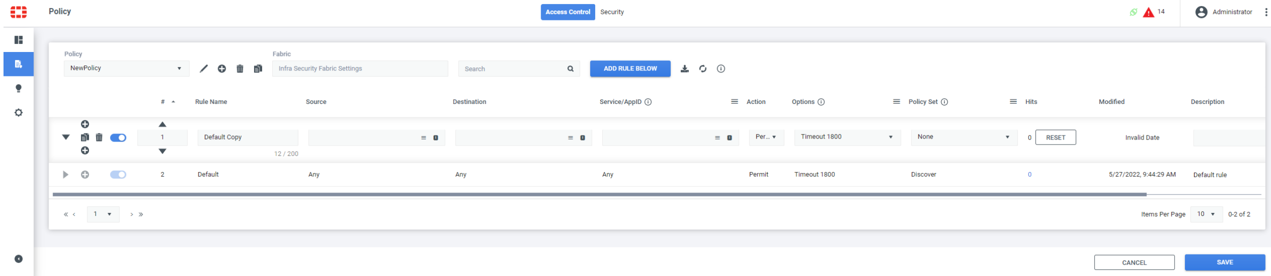
#	Rule Name	Source	Destination	Service/AppID	Action	Options	Policy Set	Hits	Modified	Description
1	Default	Any	Any	Any	Permit	Timeout 1800	Discover	0	5/23/2022, 1:43:50 PM (yasmin)	Default rule

Items Per Page 10 0-1 of 1

The new ACL policy is created with a baseline rule that permits all connections from any source resource group to any destination resource group. By default, the baseline rule is enabled. The baseline rule has initial precedence, but all new rules build on this rule and, in turn, take precedence in the order hierarchy. Check the settings of the baseline rule and be sure that you want it to permit all connections. This is the catch-all rule that is executed last in the rule set (after all other rules are executed per policy).

To edit the baseline ACL rule, click the arrow at the beginning of the row to expand it. You can change the action, options, and policy set.

3. To add a new ACL rule to the policy selected in the *Policy* dropdown list, click *ADD NEW RULE* in the top right of the page.



Policy: NewPolicy

Fabric: Infra Security Fabric Settings

#	Rule Name	Source	Destination	Service/AppID	Action	Options	Policy Set	Hits	Modified	Description
1	Default Copy 12 / 200				Per...	Timeout 1800	None	0	Invalid Date	
2	Default	Any	Any	Any	Permit	Timeout 1800	Discover	0	5/27/2022, 9:44:29 AM	Default rule

Items Per Page 10 0-2 of 2

4. Enter a unique rule name.
5. In the *Source* column for the new rule, click the Browse Groups icon to identify the source resource groups to monitor. Click *NEW GROUP* to create a new resource group. Select the resource groups and then click *SAVE*.
6. In the *Destination* column for the new rule, click the Browse Groups icon to identify the destination resource groups. The ACL rule will apply to the connection between the source resource groups and the destination resource groups. Click *NEW GROUP* to create a new resource group. Select the resource groups and then click *SAVE*.
7. In the *Service/AppID* column for the new rule, click the Browse Groups icon to select services and AppIDs that the ACL rule will affect. Click *NEW SERVICE* to create a new service. When you are done, click *SAVE*.
8. In the *Action* column for the new row, select *Permit*, *Drop*, or *Deny*. This action applies to the services and AppIDs that you selected.
9. In the *Options* column for the new row, you can enable *SysLog* and *Timeout*.
   - Enable *SysLog* if you want to capture events related to the ACL rule on the Syslog server. To configure a Syslog server, see Syslog on page 114.
   - Enable *Timeout* to limit the length of a session and then enter the number of seconds that the session will last before it times out.

   After selecting the options you want, click *DONE*.

10. In the *Policy Set* column for the new rule, select *Discover*, *All Inclusive*, or *Testing*.

    The following are the default SPSs:

    - *All Inclusive*—This is a preconfigured security policy set containing the All Threats threat-prevention policy, the Default URL Filtering Policy, and the WithSXCloud Malware Policy. The All Inclusive SPS contains all threats and all application protections.
    - *Discover*—This SPS contains the AppVisibility threat-prevention policy, but no threat rules are enabled, and no Malware policy or URL Filtering policy is associated with this SPS.
    - *Testing*—This SPS is tuned for optimized performance and includes the WithSXCloud malware policy and the Common Threats threat-prevention policy.
11. In the *Hits* column for the new rule, click *RESET* if you want to clear this counter.
12. In the Description column for the new rule, enter a description of the rule.
13. Click *SAVE* in the lower right of the page to save the ACL rule configuration.

    The new rule is added to the rules table for this policy, above the default rule. Use the up and down arrows to move the rule up or down and change its precedence.
14. Click *ADD NEW RULE* to create another rule. If you have a rule selected, click *ADD RULE BELOW*. Continue creating rules until all access conditions are defined for this ACL policy.

ACL rules and precedence

The order of ACL rules maters because it indicates the precedence of the ACL rules. FortiPolicy uses ACL rule precedence to resolve group membership and conflicts during segmentation and microsegmentation.

The default baseline ACL rule is a “catch-all” rule that contains otherwise unclassified workloads or IPs in rule assignments. This allows large parts of a data center or cloud to be referenced, without having to create many separate rules, but only when all members of the catch-all rule share security requirements.

The last rule in the ordered list (i.e., the rule with the lowest precedence) is the “catch-all” rule, which matches every workload that has not been specified by one of the preceding rules. N

ACL policy configuration strategies

The ACL policy is attached to the Security Fabric.

- ACL rules are written for the client, so begin by creating a list of which clients can initiate a connection.
- Set up rules using the outcome approach. Using the client-side approach, FortiPolicy is more aligned with the outcome.
- ACL rules with ACL policy assignments are executed in order.
- For ACL, each rule would have its own ACL policy; for example: the web tier of an application should only connect to the application tier. An application tier should never connect to a database tier, and so on. For database tiers, a database rule generally declares that the database cannot connect to anyone and will only permit incoming connections.

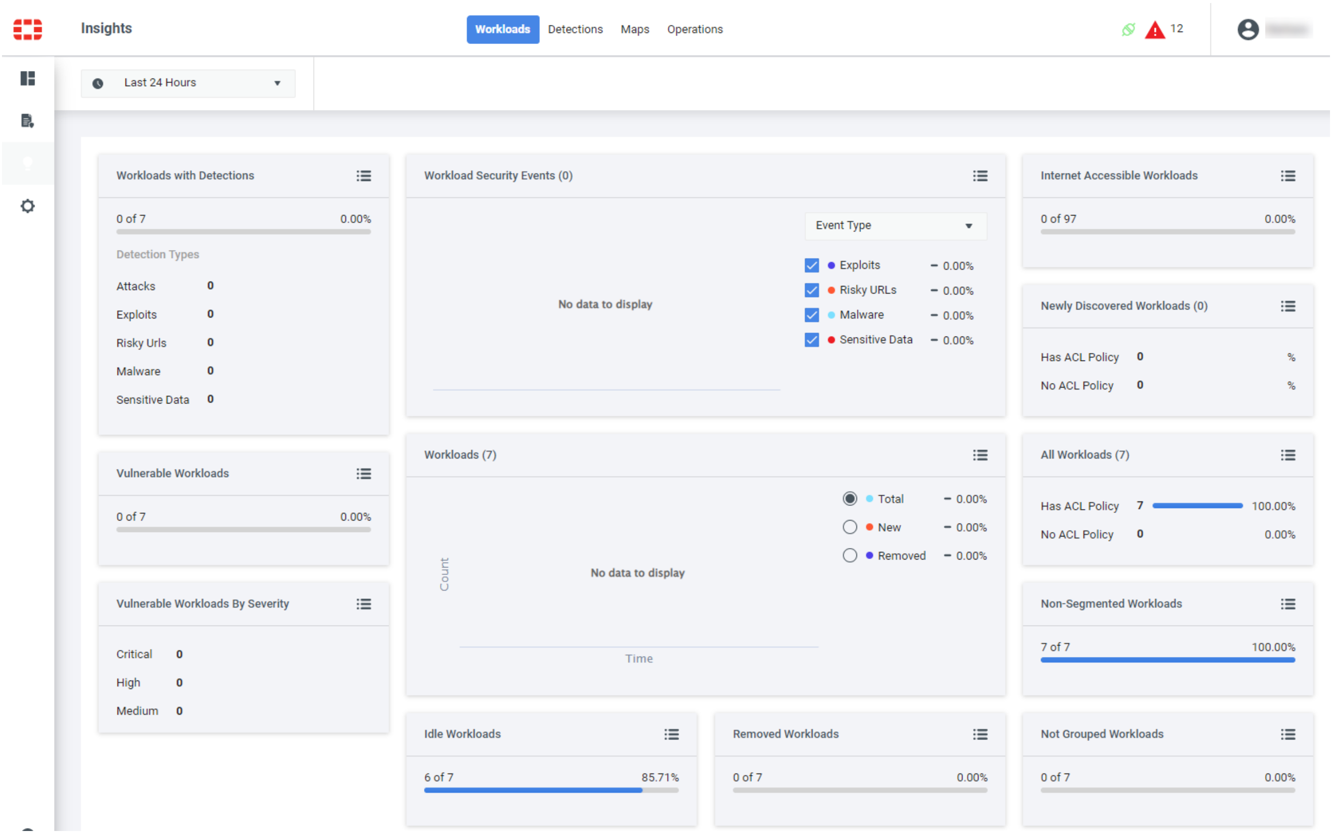
Insights into FortiPolicy

Use the Insights page how to view FortiPolicy workloads, detections, attacks, assets, and operations.

The *Insights* page has four tabs:

- Workloads on page 104
- Detections on page 105
- Maps on page 105
- Operations on page 107

Workloads



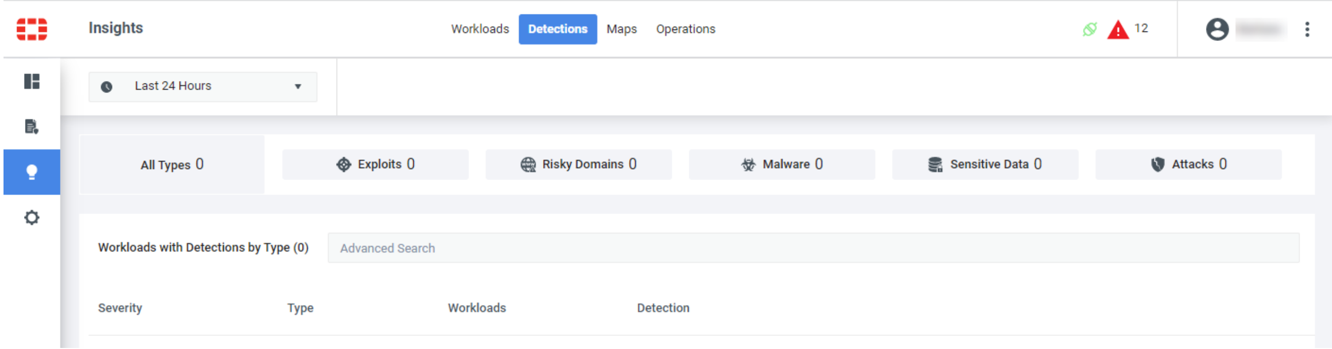
The *Workloads* page displays the following widgets:

- Workloads with Detections
- Workload Security Events
- Internet Accessible Workloads
- Newly Discovered Workloads
- Vulnerable Workloads

- Workloads
- All Workloads
- Vulnerable Workloads by Severity
- Non-Segmented Workloads
- Idle Workloads
- Removed Workloads
- Not Grouped Workloads

At the top of the *Workloads* page, you can select the time period to display results for: *Last Hour*, *Last 2 Hours*, *Last 24 Hours*, *Last 7 Days*, or *Last 30 Days*.

Detections



The *Detections* page shows the number of workloads with exploits, risky domains, malware, or sensitive data.

At the top of the *Detections* page, you can select the time period to display results for: *Last Hour*, *Last 2 Hours*, *Last 24 Hours*, *Last 7 Days*, or *Last 30 Days*.

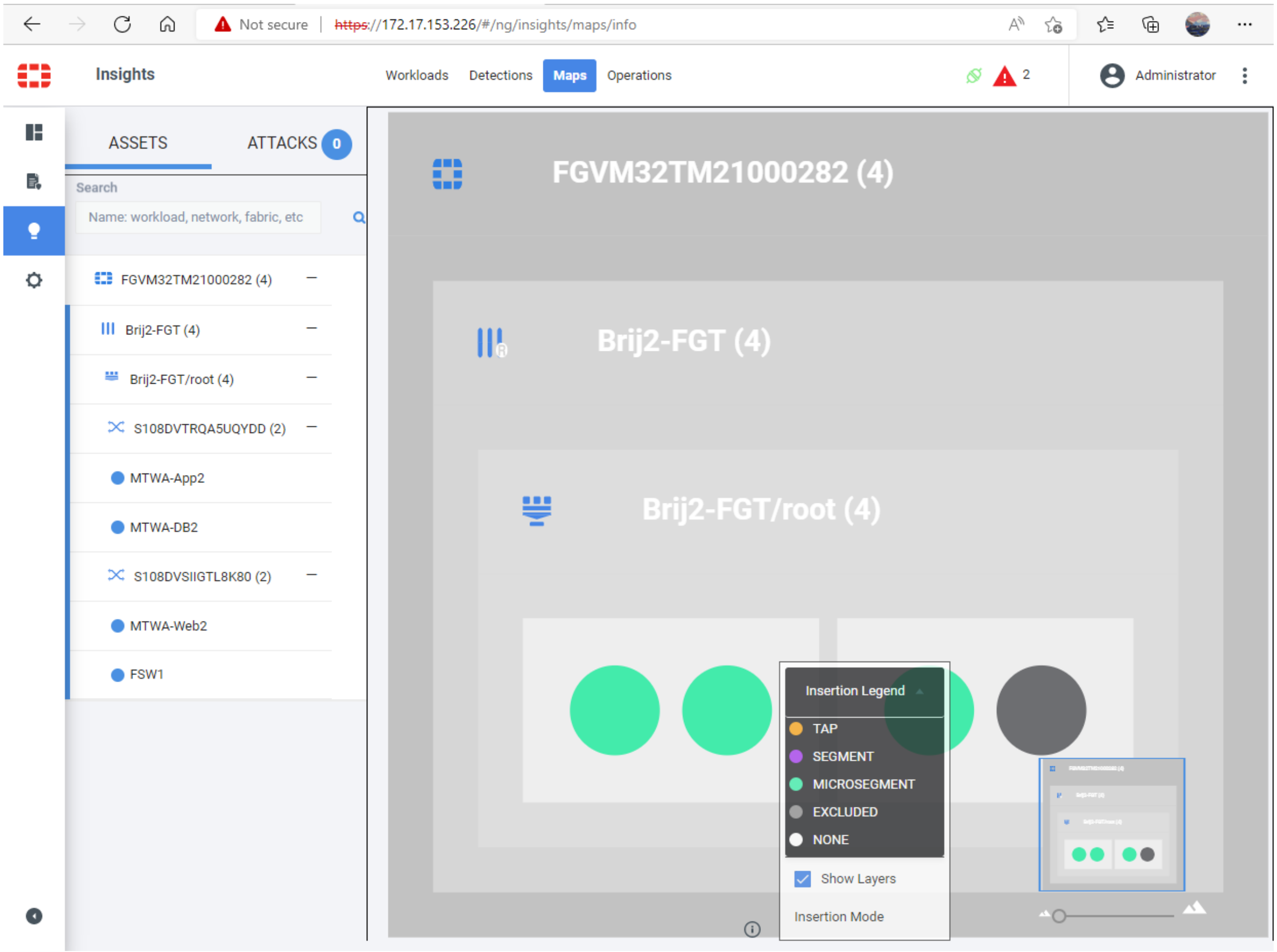
The Attacks data is not currently available.

Maps

The *Maps* page displays the Assets map.

The Attacks map is not supported in this release.

A simple fabric connector configuration connects to your Security Fabric with its workloads and allows FortiPolicy to immediately perform initial discovery of all network objects and assets in your infrastructures. After initial discovery, FortiPolicy performs continuous discovery, in perpetuity. All discovered assets in the Security Fabric are visualized in the Assets map.



The *ASSETS* tab provides both lists and visualizations of all discovered assets resulting from FortiPolicy continuous discovery of the Security Fabric. Lists are expandable; click the + symbol to expand a list segment; click the minus symbol to hide list segments. Use the *Search* field to find assets by name and display associated details. Expand the lists to drill deep into Security Fabric assets.

The expandable list uses a distinct mapping structure and hierarchy per infrastructure. As you click the map list to expand it, the visualization to the right displays the structures and embedded hierarchy correspondingly:

Security Fabric > FortiGate > VDOM > FortiSwitch > Workload port

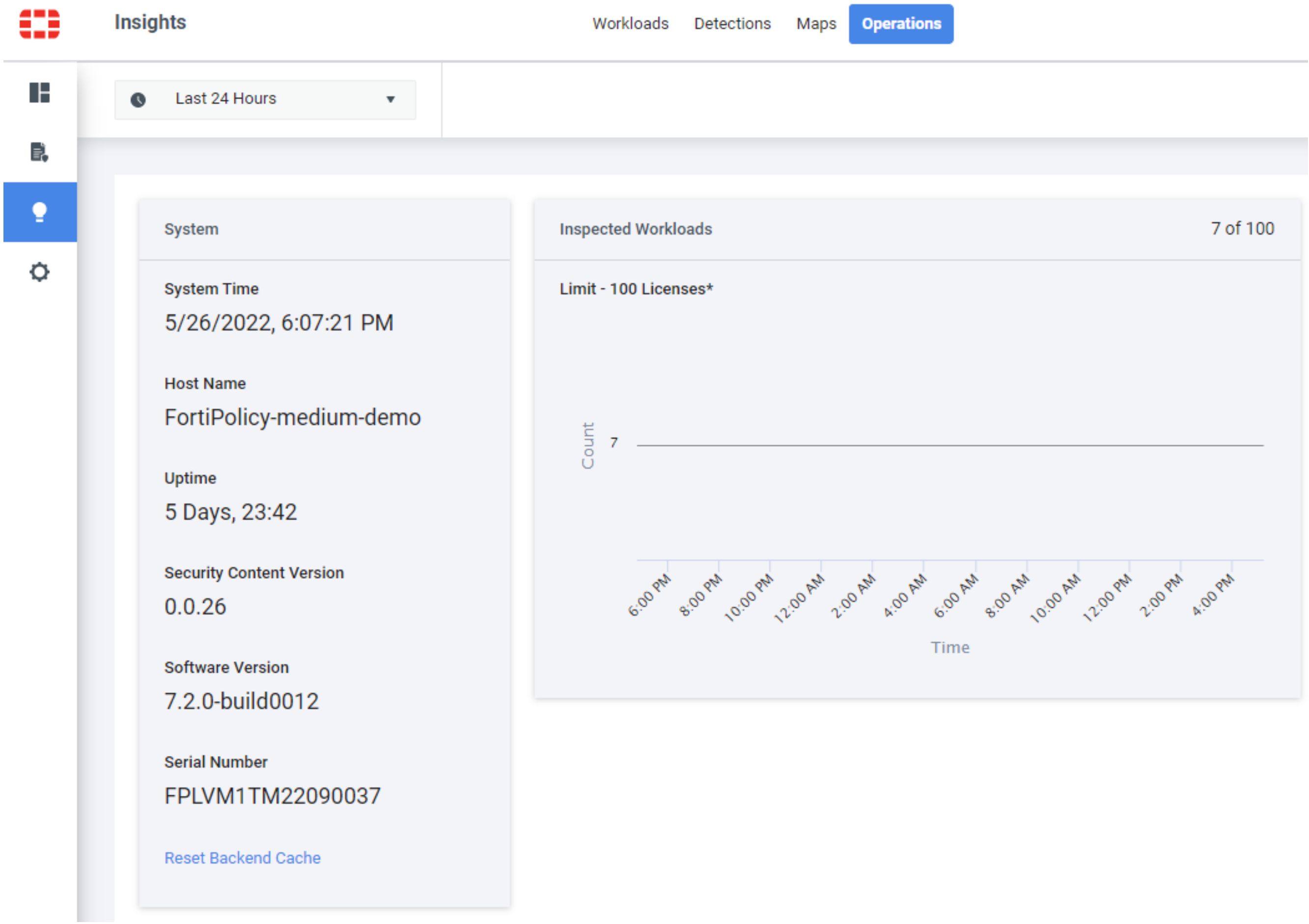
To use the Assets map:

- In the map visualizations area, click any entity to display more information.
- The solid white circles in the visualization displays always represent workload ports.

  Most workloads have exactly one port, which means the number of circles represent the number of workloads most of the time. However, there are cases called multi-homed, where a workload might have multiple ports. These different ports of the same workload can be dispersed over other switches on the map. So sometimes the number of circles shown might be larger than the number of actual workloads. The numbers shown in the upper right of each structure indicates the actual, total number of ports in that level of the hierarchy. When a multi-homed workload is selected on the Assets tree, all ports of that workload are highlighted on the map. A double-click on a workload port or structure automatically pans and zooms the view to center on that object.

- Clicking on any structure or entity, such as a VDOM or a circle workload port, displays a *Properties* window on the right side of the screen. Workload port properties include a list of all ports per workload.
- Hover your mouse over any entity to reveal a quick tooltip display of its name and other identifiers.
- Use the zoom slider on the lower right to adjust the display.
- Select the *Show Layers* checkbox to display the color-coded heat map for insertion modes. When layers are enabled, workloads are overlaid by the color code for their current insertion mode: orange for TAP mode; purple for SEGMENT mode; green for MICROSEGMENT mode; gray for EXCLUDED; and white for NO INSERTION.
- Drag the view finder box area on the lower right to select a specific area for display.

Operations



System

System Time
5/26/2022, 6:07:21 PM

Host Name
FortiPolicy-medium-demo

Uptime
5 Days, 23:42

Security Content Version
0.0.26

Software Version
7.2.0-build0012

Serial Number
FPLVM1TM22090037

The *Operations* page displays information about your system and inspected workloads relative to licensed workloads.

At the top of the *Operations* page, you can select the time period to display results for: *Last Hour*, *Last 2 Hours*, *Last 24 Hours*, *Last 7 Days*, or *Last 30 Days*.

FortiPolicy configuration

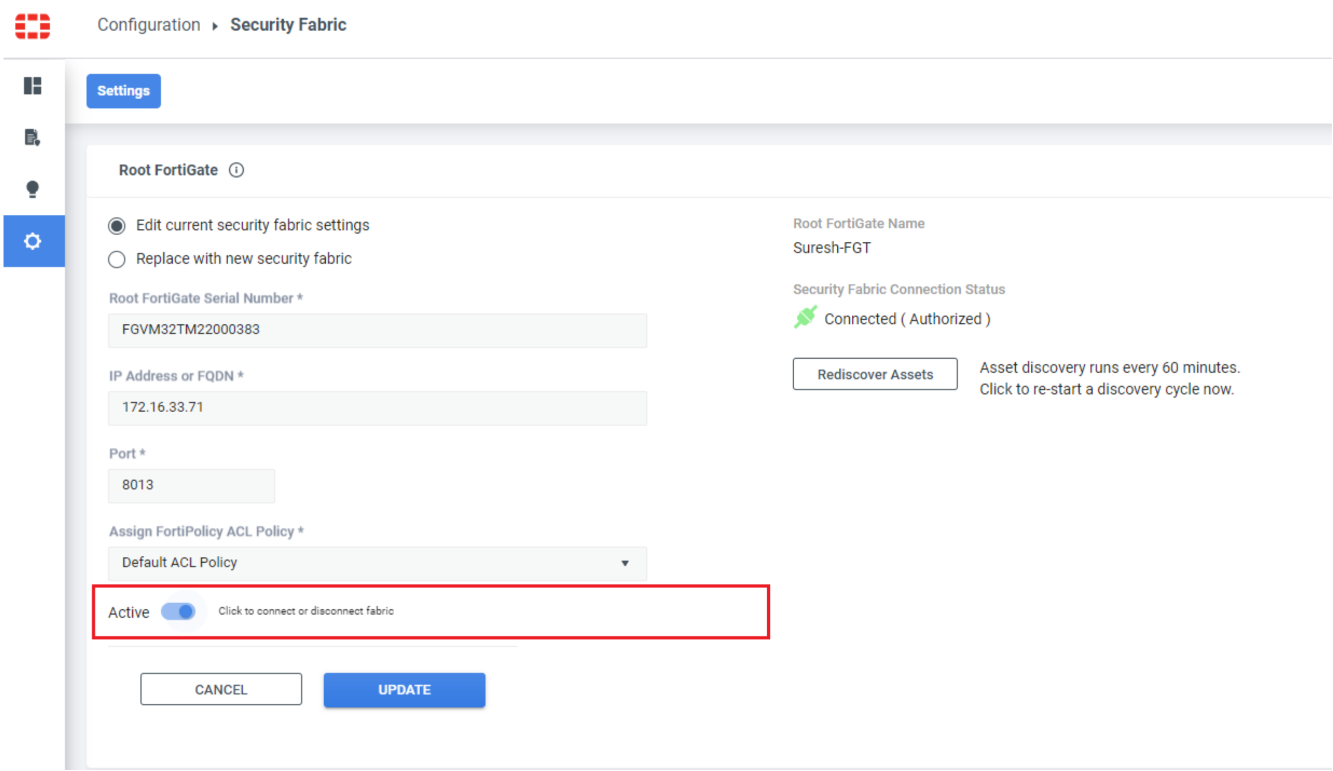
The *Configuration* menu allows you to configure the Security Fabric, create data planes, set up servers and certificates, improve your system health, perform system maintenance, and obtain reports.

This section covers the following topics:

Security Fabric

Connecting FortiPolicy to your Security Fabric automatically loads data on all the fabric's workloads into FortiPolicy. This can be confirmed on the *Insights* > *Workloads* dashboard and the *Insights* > *Maps* view.

The *Configuration* > *Security Fabric* page allows you to edit your current Security Fabric settings or replace your current settings with a new Security Fabric.



Configuration ▸ Security Fabric

Settings

Root FortiGate ⓘ

● Edit current security fabric settings

○ Replace with new security fabric

Root FortiGate Serial Number *: FGVM32TM22000383

IP Address or FQDN *: 172.16.33.71

Port *: 8013

Assign FortiPolicy ACL Policy *: Default ACL Policy

Active — Click to connect or disconnect fabric

Root FortiGate Name: Suresh-FGT

Security Fabric Connection Status: Connected (Authorized)

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

Editing your current Security Fabric settings

1. Go to *Configuration > Security Fabric*.
2. Click *Edit current security fabric settings*.
3. Make any necessary changes.
4. Click *UPDATE*.

Replacing your Security Fabric

Each FortiPolicy installation is licensed to analyze one Security Fabric. If you are removing FortiPolicy from one Security Fabric to analyze another Security Fabric, you need to remove the FortiPolicy configurations from the first Security Fabric. If you have completed the Action Steps in *Workspace > Applications*, do the following before replacing your Security Fabric with a different one:

1. Go to *Workspace > Applications*.
2. In the *Action Steps* panel, click *Revert* in Step 5: Security to stop enforcing the policy rules.
3. Click *Revert* in Step 3: Microsegment to remove segmentation and microsegmentation.
4. Click *EDIT SETUP* in Step 1: Discover Connections.
5. Click *Advanced Settings*.
6. Click *DELETE ALL* to delete all applications and policy rules.
7. Click *PURGE DATA* to delete connection data, proposed applications, and policy rules.
8. Click *CLOSE* to leave the *Advanced Settings* dialog.

9. Click *SAVE and CLOSE* to leave the Setup Policy Generation wizard.
10. Go to *Configuration* > *Data Planes*.
11. Click the vertical ellipsis menu and select *Delete* for each data plane.

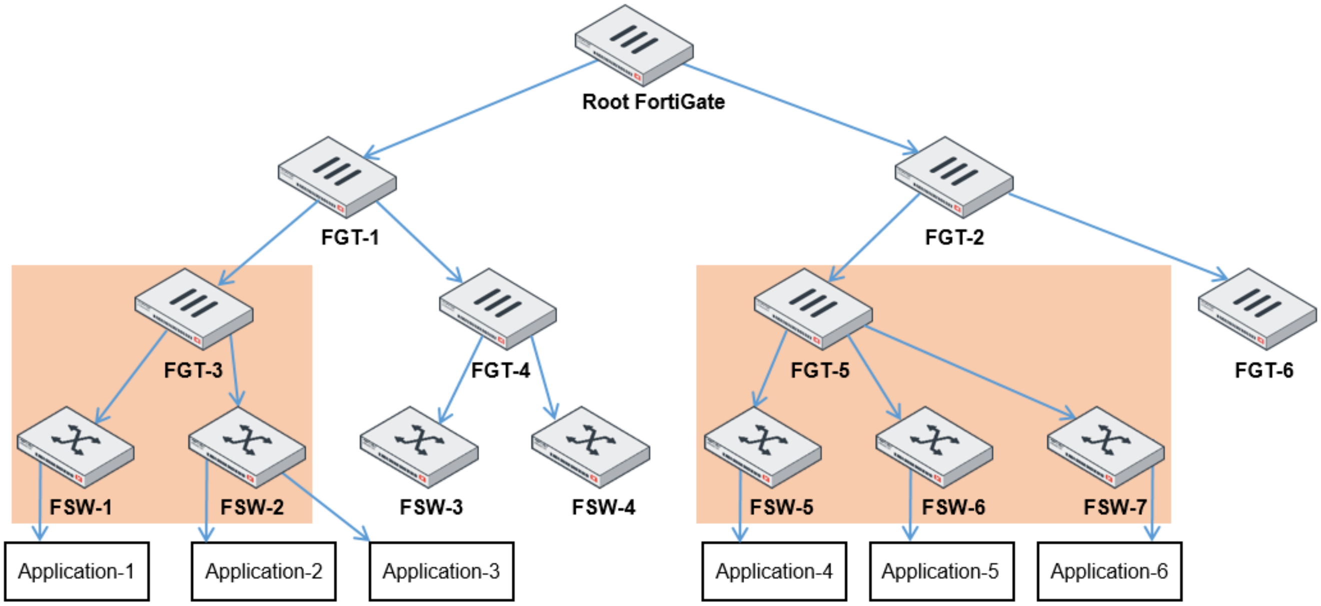
To replace the Security Fabric:

1. Go to *Configuration* > *Security Fabric*.
2. Click *Replace with new security fabric*.
3. In the *Serial Number* field, enter the serial number for the new root FortiGate device.
   The FortiGate serial number is displayed in the *System Information* widget on the *Dashboard* > *Status* page of your FortiGate device.
4. In the *IP Address* field, enter the IP address of the new root FortiGate device.
5. By default, the *Port* field is set to `8013`.
6. In the *Assign FortiPolicy ACL Policy* dropdown list, select a customized ACL policy or select *Default ACL Policy* if you have not created your own ACL policy.
7. Click *UPDATE*.

After replacing the Security Fabric, you need to authorize FortiPolicy on the root FortiGate device and create a data plane for every FortiGate device that you want to protect.

Data planes

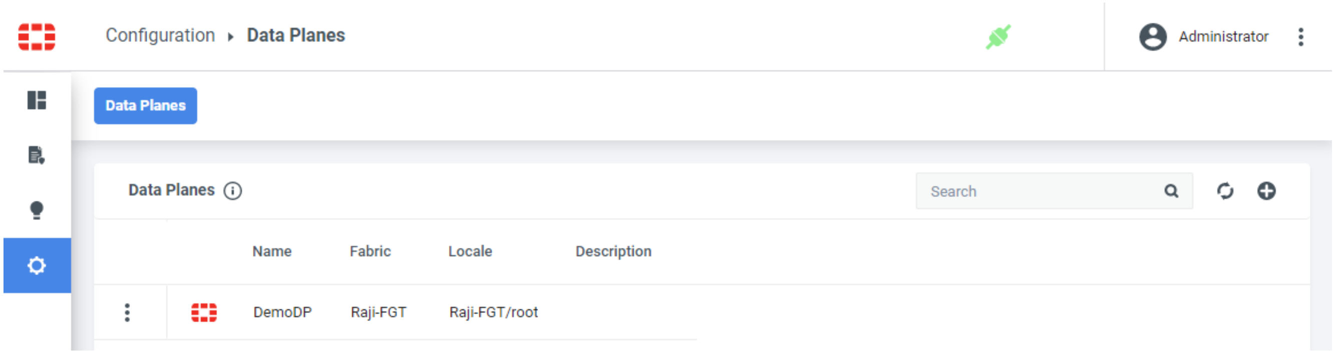
You need to create a data plane for each FortiGate device with applications under it that need to be secured. For example, in the following topology, you would create a data plane for FGT-3 to secure Application-1, Application-2, and Application-3. You would create a second data plane for FGT-5 to secure Application-4, Application-5, and Application-6.



The data plane determines what the Policy Generation wizard can analyze and what the proposed rules can secure. When you select the FortiGate device for the data plane, the Policy Generation wizard will examine the traffic logs from that FortiGate device and the netflows from the FortiSwitch units that are directly wired to the FortiGate device. The Policy Generation wizard will analyze the traffic for the workloads connected directly to the FortiGate device or FortiSwitch units.

A data plane is deployed only when resource groups are moved from Insertion Staging to a formal COMMIT.

Go to *Configuration* > *Data Planes* to view available data planes or to create data planes.



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

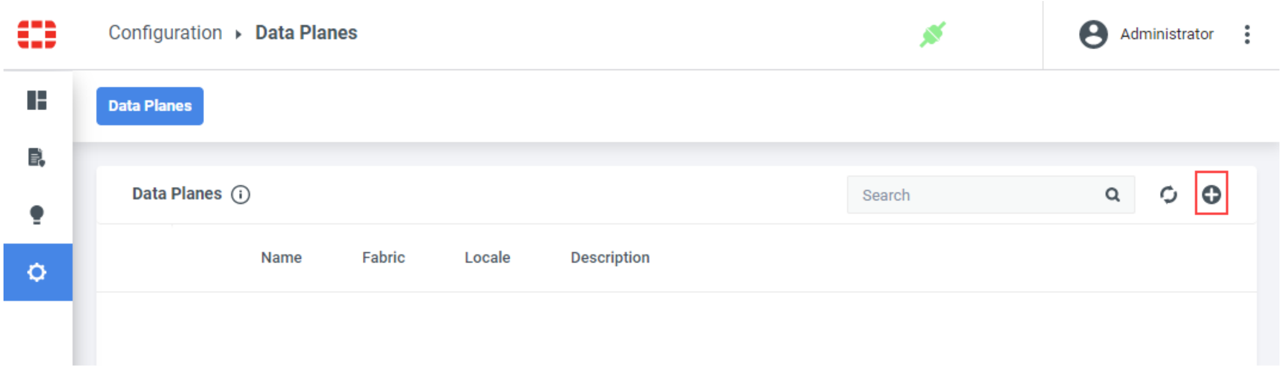
If there are no rows displayed in the *Data Planes* page, no data planes have been created.

Click the vertical ellipsis at the start of each row to edit, synchronize, redeploy, or delete data plane configurations. When you click *Edit*, you can edit the details for the configuration.

Creating a data plane

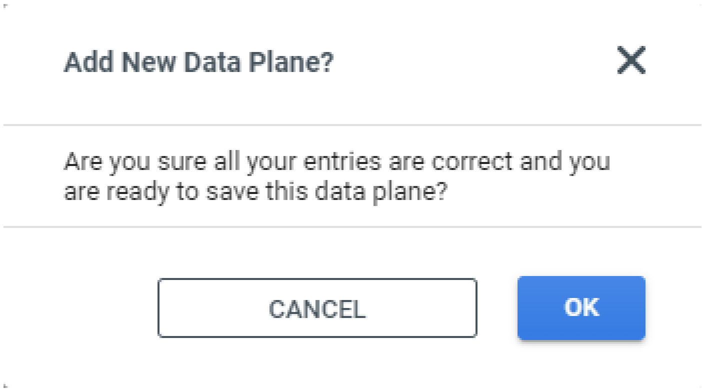
To create a data plane:

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 deployment.
4. From the *Fabric* dropdown list, select a fabric connector.
5. From the *Device* dropdown list, select the root FortiGate device.

6. From the *VDOM* dropdown list, select the root virtual domain (VDOM) of the root FortiGate device.
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.
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.

11. Repeat steps 2-10 for each FortiGate device with applications under it that need to be secured.

Synchronizing or redeploying a data plane

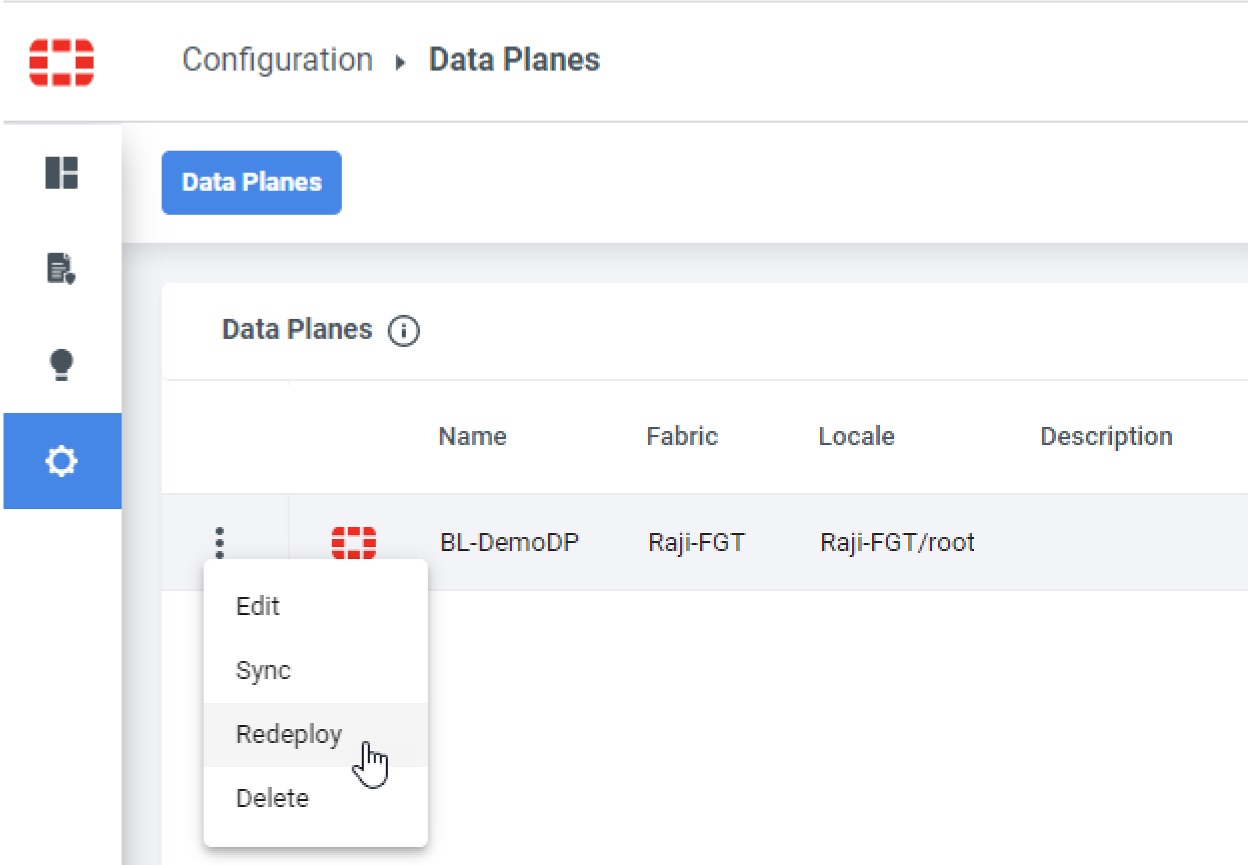
Go to *Configuration* > *Data Planes* to synchronize or redeploy an established data plane:

- Synchronize the data plane if you want to correct something in your deployment; perhaps creating a data plane failed because there was a “Jobs” error that had to be resolved.
- Redeploy the data plane if you want to pick up a new data path image.

If a data plane deployment fails, go to *Workspace* > *Logs* > *Jobs* to troubleshoot and resolve the issue and then return to the *Data Planes* page and select *Sync* from the vertical ellipse menu. In the confirmation dialog, click *YES*.

To redeploy a data plane:

1. Go to the *Configuration* > *Data Planes* page.
2. Click the vertical ellipsis at the start of the row and select *Redeploy*.
3. In the confirmation dialog, click *YES*.



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

Deployment (or redeployment) of a data plane is performed within seconds.

A message is displayed on the banner on the *Data Planes* page when redeployment starts, is processing, and is complete.

To synchronize a data plane:

1. Go to the *Configuration* > *Deployments* > *Data Planes* page.
2. Click the vertical ellipsis at the start of the row and select *Sync*.
3. In the confirmation dialog, click *YES*.

Deleting a data plane

To delete a data plane:

1. Go to the *Configuration* > *Data Planes* page.
2. Click the vertical ellipsis at the start of the row and select *Delete*.
3. In the confirmation dialog, click *YES*.

If you delete a data plane and then re-create it too quickly, the application tiers might use the previous data plane identifier during automated policy generation. Deploying an application tier that uses the previous data plane identifier causes a FortiPolicy error (no free VLAN identifiers are available).

To work around this error:

1. Go to *Workspace* > *Applications*.
2. Click *EDIT SETUP* in Step 1: Discover Connections.
3. Click *Advanced Settings*.
4. Click *PURGE DATA* to delete connection data, proposed applications, and proposed policy rules.
5. Click *CLOSE* to leave the *Advanced Settings* dialog.
6. Set up automated policy generation and let it run for one discovery cycle (from 15 minutes to 2 hours).

Setup

The *Setup* page contains five tabs:

- Servers on page 114
- Authentication on page 118
- Certificates on page 121
- Backup on page 124
- Telemetry on page 127

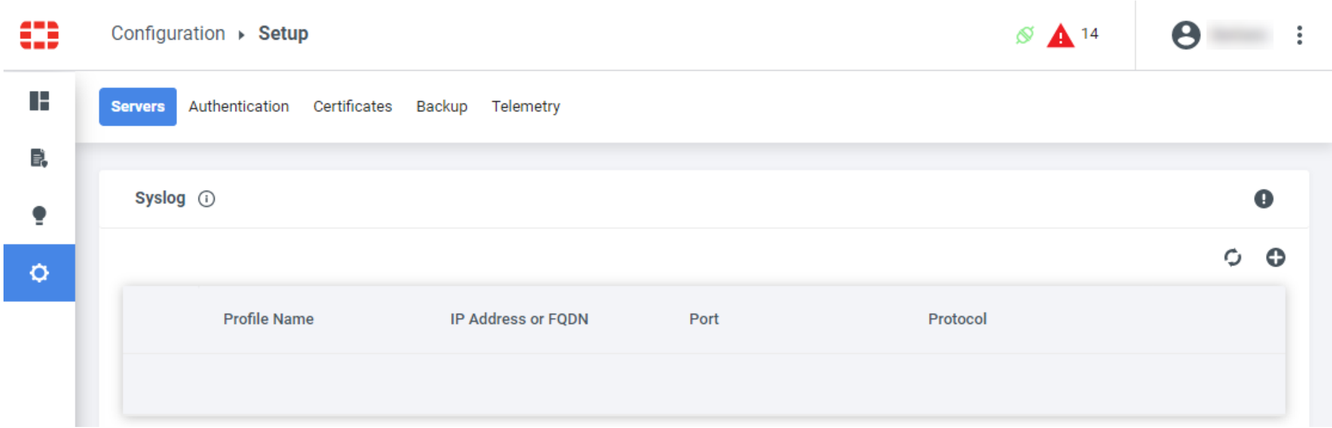
Servers

The *Servers* page allow you to configure the following:

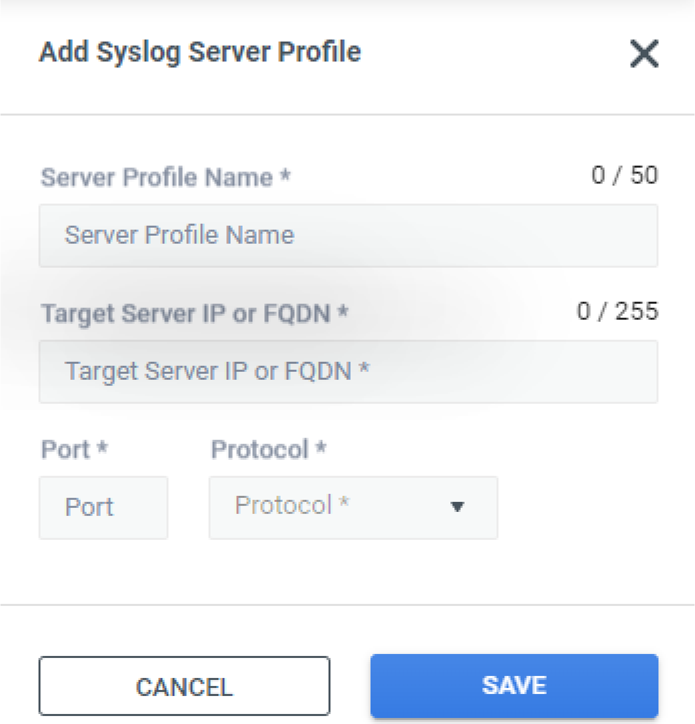
- Syslog on page 114
- SMTP on page 115
- SMB on page 116
- Management proxy on page 117
- NTP on page 118
- Remote packet capture on page 1
- FortiSandbox on page 1

Syslog

Go to the *Syslog* section of the *Configuration* > *Setup* > *Servers* page to create a Syslog server profile.



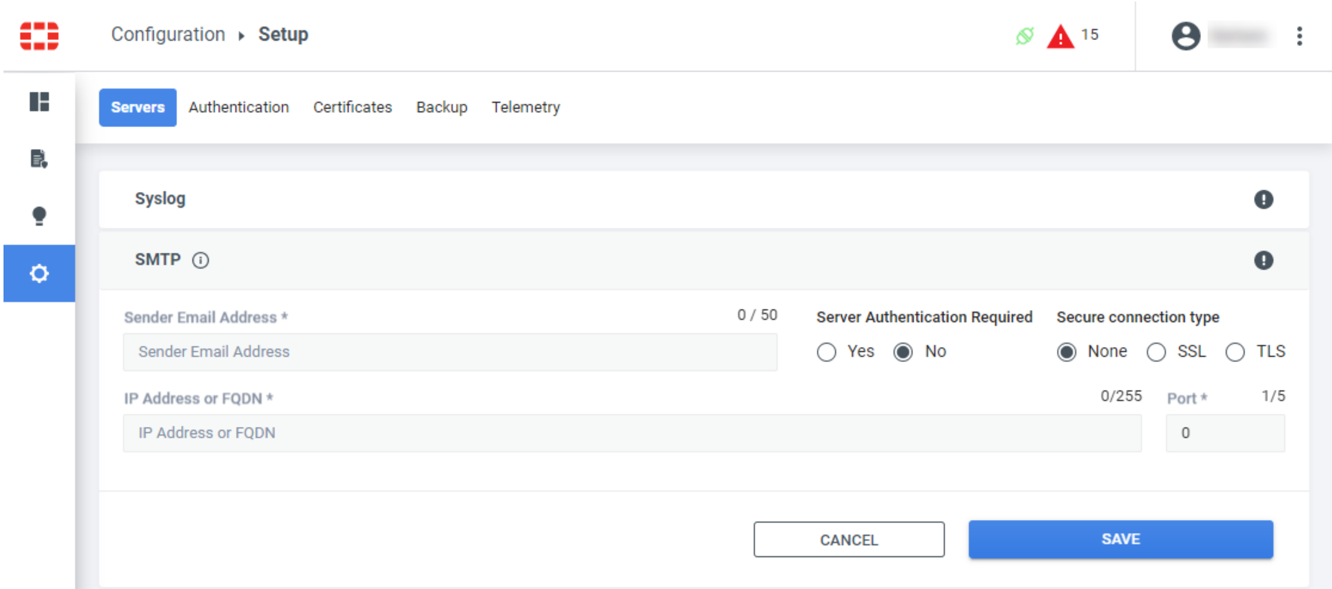
1. Click the + icon in the upper right side of the *Syslog* section to open the *Add Syslog Server Profile* panel.



2. Enter a name for the Syslog server profile.
3. Enter the target server IP address or fully qualified domain name.
4. Enter the server port number.
5. Enter the protocol configured for the server, either *TCP* or *UDP*.
6. Click *Save* to create the profile.

SMTP

Go to the *SMTP* section of the *Configuration* > *Setup* > *Servers* page to configure an SMTP server.



Sender Email Address * 0 / 50: Sender Email Address

Server Authentication Required: ○ Yes ● No

Secure connection type: ● None ○ SSL ○ TLS

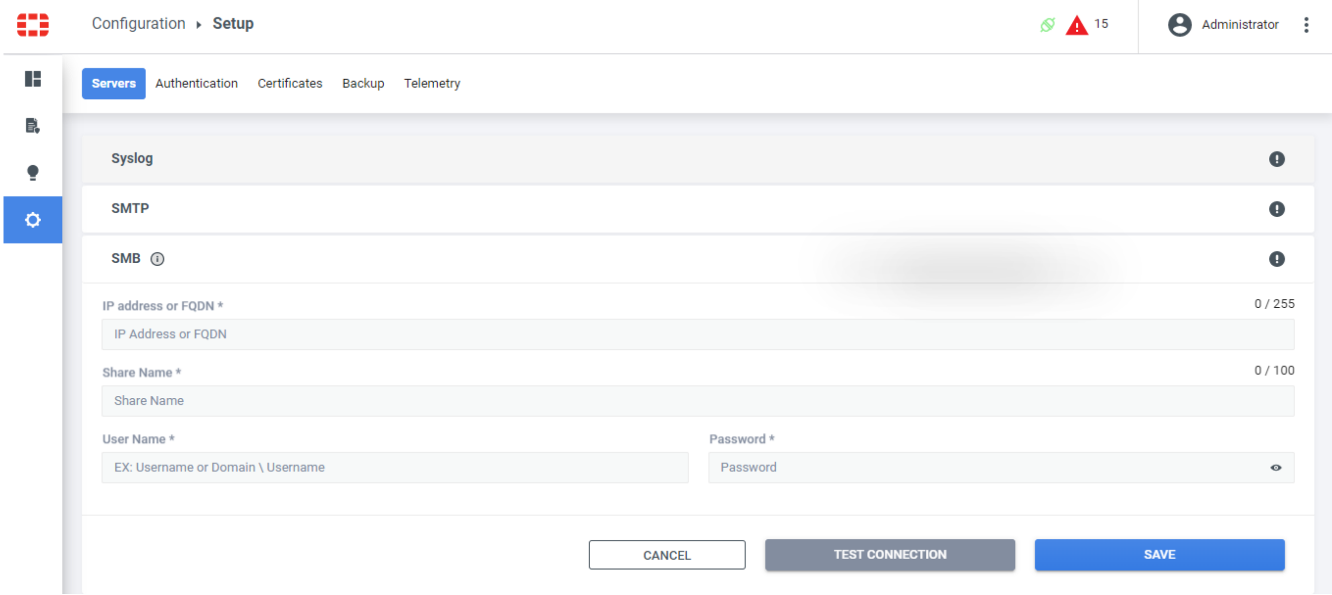
IP Address or FQDN * 0/255: IP Address or FQDN

Port * 1/5: 0

1. Enter the email address for the sender.
2. Enter the IP address or fully qualified domain name for the SMTP server.
3. If server authentication is required, click *Yes* and enter the user name and password for the SMTP server.
4. Select whether the connection to the server will be with SSL, TLS, or neither.
5. Enter the port number that the SMTP server will use.
6. Click *Save* to save the configuration.

SMB

Go to the *SMB* section of the *Configuration* > *Setup* > *Servers* page to configure an SMB server.



IP address or FQDN * 0 / 255: IP Address or FQDN

Share Name * 0 / 100: Share Name

User Name *: EX: Username or Domain \ Username

Password *: Password

1. Enter the IP address or fully qualified domain name for the SMB server.
2. Enter the share name for the SMB server.
3. Enter the user name and password to access the SMB server.
4. Click *Test Connection* to verify connectivity.
5. Click *Save* to save the configuration.

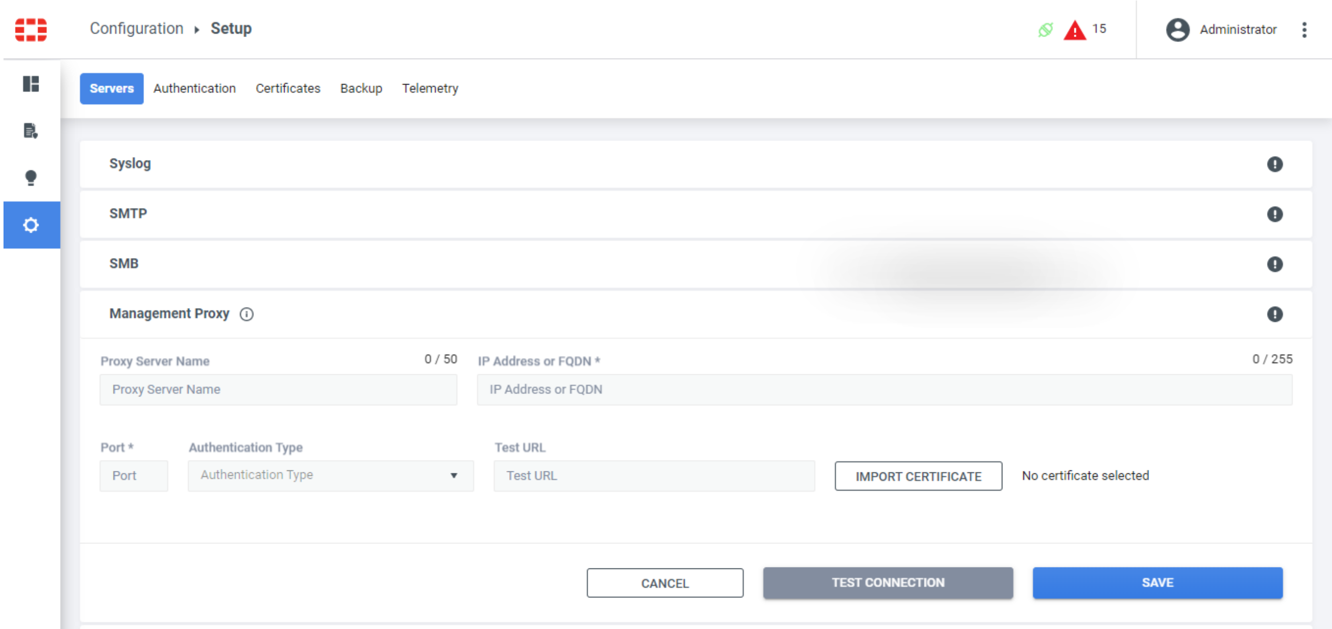
An SMB server must be configured and operational to perform a backup.

Management proxy

If you use a proxy server to control access to the Internet, the proxy server is used by the FortiPolicy management plane. Currently, proxy server integration supports FortiPolicy license imports, log uploads, Elasticsearch data uploads, and software upgrades.

When there is no proxy server configuration, traffic is routed directly from the FortiPolicy management platform to the Internet.

Enable and configure proxy settings from the *Management Proxy* section of the *Configuration* > *Setup* > *Servers* page.



To configure a new proxy server:

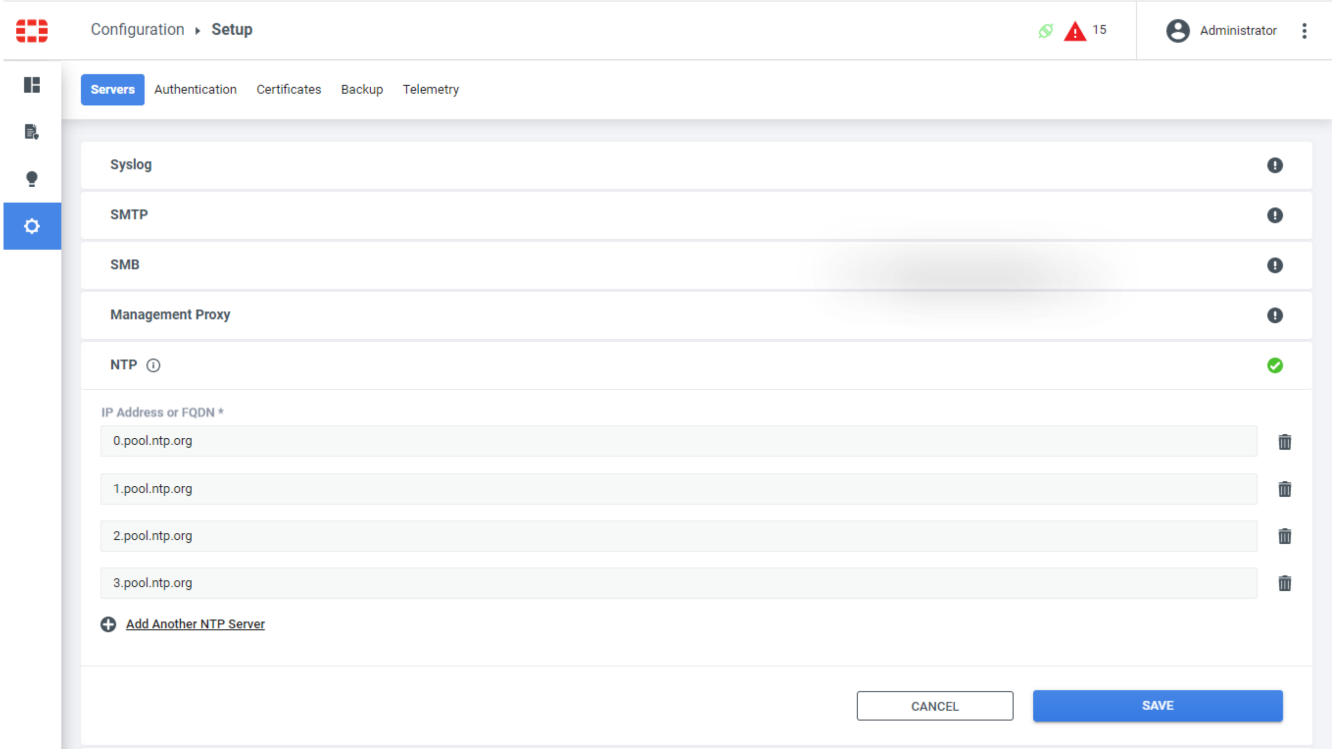
1. Enter the name of the proxy server.
2. Enter the IP address or fully qualified domain name of the proxy server.
3. Enter the port number that the proxy server will use.
4. If you want to use authentication, select *Basic Auth* or *NTLM*.
5. If you selected *Basic Auth*, enter the user name and password to access the proxy server.

6. If you selected *NTLM*, enter the user name and password to access the proxy server, the name of the NTLM domain, and the name of the proxy workstation.
7. Enter a URL to test the connection to the proxy server with.
8. Click *IMPORT CERTIFICATE* and select the certificate to use.
9. Click *TEST CONNECTION* to use the proxy server with the test URL.
10. Click *SAVE* to save the configuration.

NTP

FortiPolicy infrastructure workloads, segments, microsegments, management console, and so on are all required to be synchronized and therefore need access to an NTP server. FortiPolicy networked components must also be synchronized with customer workloads and with computers in and outside the firewall. For most uses, one or two backup NTP servers are enough. If a networked computer cannot access one NTP server for any reason, it will try to connect to the next one in the configuration set.

Go to the *NTP* section of the *Configuration* > *Setup* > *Servers* page to configure the NTP servers.



IP Address or FQDN *
0.pool.ntp.org
1.pool.ntp.org
2.pool.ntp.org
3.pool.ntp.org

1. Enter the IP address or fully qualified domain name (FQDN) of the primary NTP server.
2. Enter up to three backup IP addresses or FQDNs.
3. If you want to add another NTP server, click *Add Another NTP Server*.
4. Click *SAVE* to save the configuration.

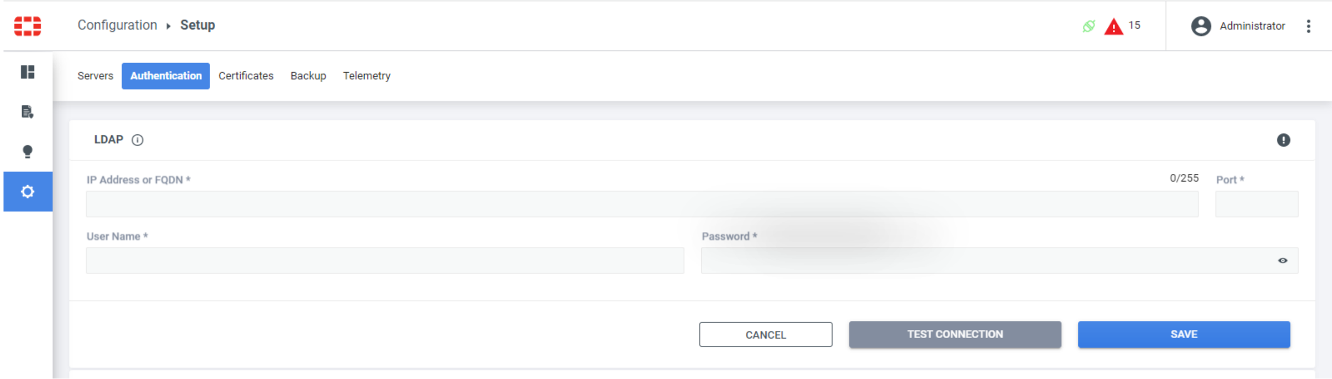
Authentication

Go to *Configuration* > *Setup* > *Authentication* to configure the following:

- LDAP authentication on page 119
- RADIUS authentication on page 119
- SSH public keys on page 121

LDAP authentication

Go to the *LDAP* section of the *Configuration* > *Setup* > *Authentication* page to configure an LDAP server.



To configure an LDAP server:

1. Enter an IP address or fully qualified domain name for the LDAP server.
2. Enter the port number that the LDAP server will use.
3. Enter a user name and password to access the LDAP server.
4. Click *TEST CONNECTION* to verify that the LDAP server can be accessed.

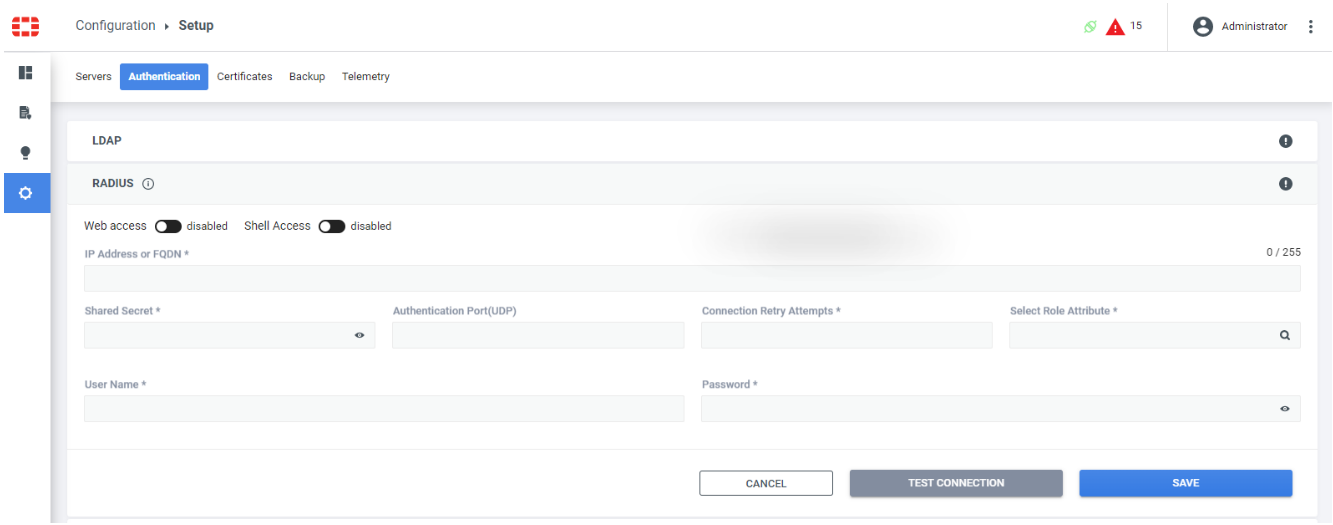
   Be sure to test the connection *before* saving the configuration.
5. Click *SAVE* to save the configuration.

   After configuring the LDAP server, go to *Configuration* > *Users* > *Users* to add a user, the user’s FortiPolicy user role, and the user’s user domain name for each user to be authenticated by LDAP.

RADIUS authentication

To integrate FortiPolicy with your RADIUS server, you need to configure your RADIUS users with the supported FortiPolicy roles: GlobalAdministrator, PolicyProvisioner, and Auditor.

You need to configure the user role for RADIUS two-factor authentication.



To configure a RADIUS server:

1. Enable or disable web access.
2. Enable or disable shell access
3. Enter the IP address or fully qualified domain name for the RADIUS server.
4. Enter the shared secret for the RADIUS server.
5. Enter the authentication port (UDP) number.
6. Enter the number of times that FortiPolicy will retry connecting to the RADIUS server.
7. Select the RADIUS role attribute that will provide the FortiPolicy role in the authentication response from the RADIUS server
8. Enter the user name and password to access the RADIUS server.
9. Click *TEST CONNECTION* to verify that FortiPolicy can access the RADIUS server.
10. Click *SAVE*.

    Unlike LDAP, you do not need to create an entry in the FortiPolicy repository for RADIUS authentication and authorization.

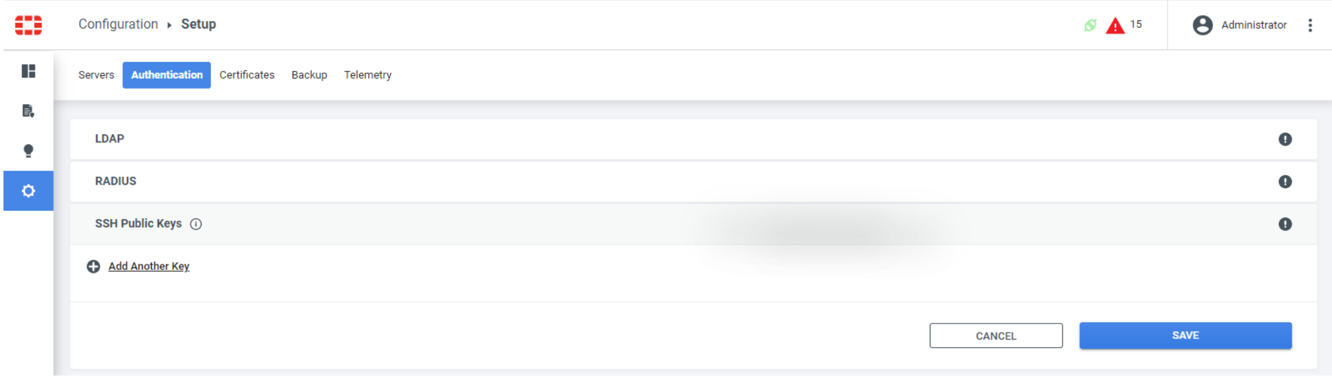
Authentication and authorization for RADIUS users uses both a password and a QR code (time-based one-time password). By default, a new token is generated every 30 seconds. To compensate for a potential time-skew between the client and the server, FortiPolicy allows an extra token before and after the current time. This allows for a time-skew of up to 30 seconds between authentication server and client. If you experience problems with poor time synchronization, you can increase the window from its default size of three permitted codes (one previous code, the current code, the next code) to 17 permitted codes (the 8 previous codes, the current code, and the 8 next codes). This will allow a time-skew of up to 4 minutes between client and server if necessary.

You might need to install Google Authenticator and then scan the QR code per user to obtain the one-time password. Google Authenticator implements a one-time password for various platforms. It can be used in conjunction with FreeRADIUS to provide two-factor authentication using a library called Pluggable Authentication Module (PAM) for Linux user-password authentication. For more information on PAM, refer to http://www.linux-pam.org.

SSH public keys

You can import SSH keys to access the FortiPolicy console using the CLI. Multiple keys can be added for different users.

The keys are imported for users who want to SSH into FortiPolicy. The FortiPolicy console supplies the password for access to the virtual machine. Using a single common password to log in is not adequately secure. To best protect the FortiPolicy console, FortiPolicy uses both the SSH key and one-time password (OTP) for two-factor authentication, which is time-based (using short-lived OTPs that change every 30 seconds).



An SSH key must have a user name assigned at all times. ECDSA key types are not supported.

To import SSH keys:

1. Click *Add Another Key*.
   Enter the public key.
2. If you want to add more public keys for multiple users, click *Add Another Key*.
3. Click *SAVE* to save the public keys.

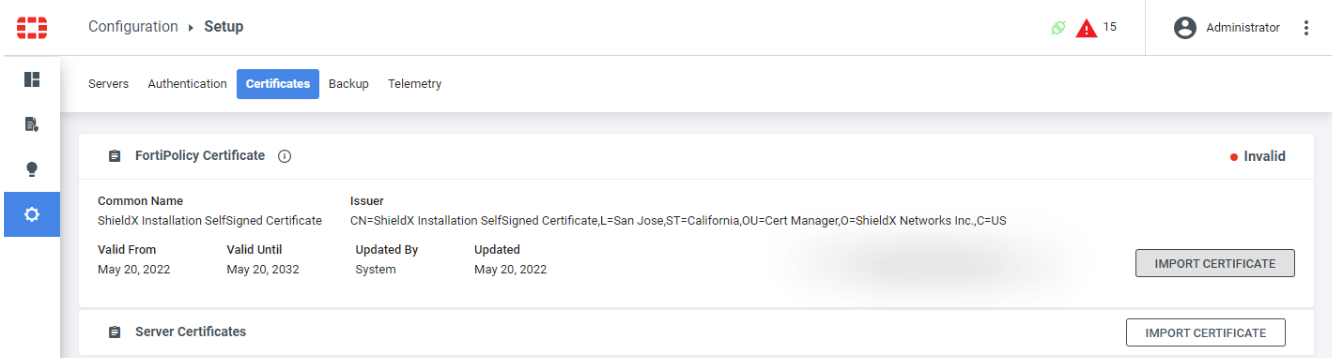
Click the trash can icon at the end of a row to delete the SSH key configuration.

Certificates

Use the *Certificates* page for the following:

- FortiPolicy certificate on page 122
- Server certificates on page 122

FortiPolicy certificate



FortiPolicy Certificate ● Invalid

Common Name: ShieldX Installation SelfSigned Certificate

Issuer: CN=ShieldX Installation SelfSigned Certificate,L=San Jose,ST=California,OU=Cert Manager,O=ShieldX Networks Inc.,C=US

Valid From: May 20, 2022

Valid Until: May 20, 2032

Updated By: System

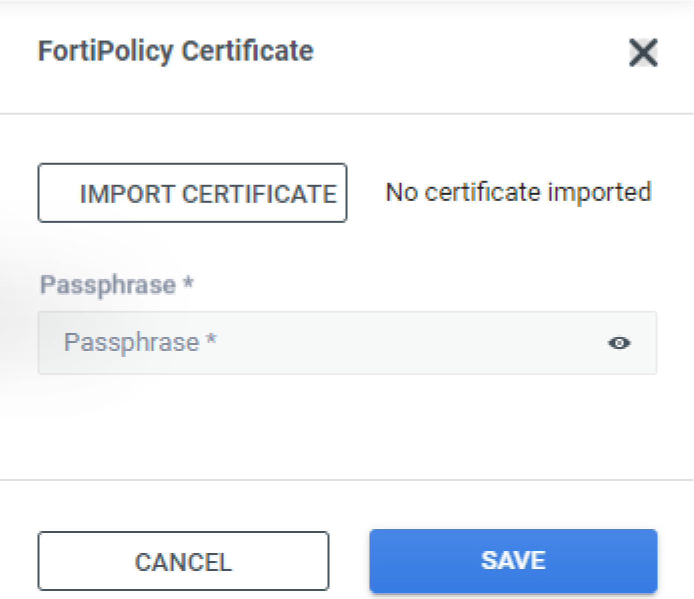
Updated: May 20, 2022

Server Certificates

The FortiPolicy default certificate is self-signed. To avoid being flagged by the browser, you can import your own Certificate Authority (CA) signed certificate.

To import a new FortiPolicy certificate:

1. Go to the *FortiPolicy Certificate* section of the *Configuration* > *Setup* > *Certificates* page.
2. Click *IMPORT CERTIFICATE*.

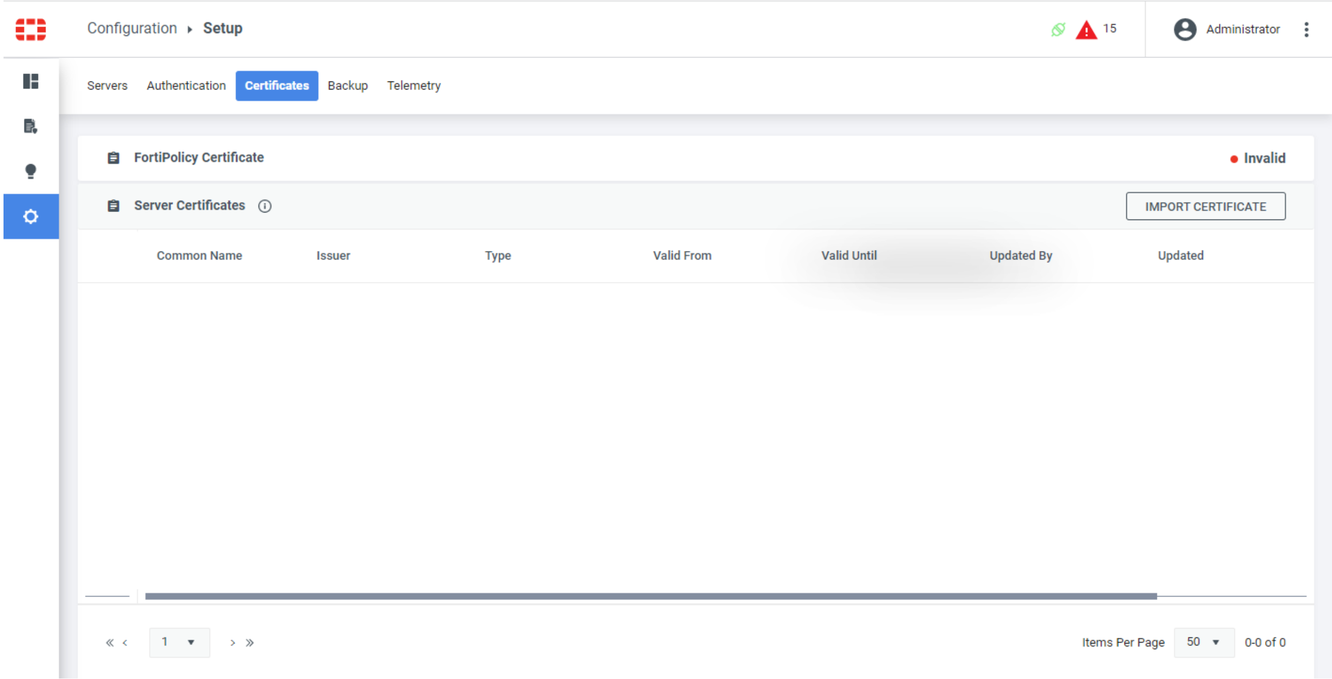


No certificate imported

3. In the *FortiPolicy Certificate* panel, click *IMPORT CERTIFICATE* and select the certificate to import.
4. Enter the passphrase.
5. Click *SAVE*.

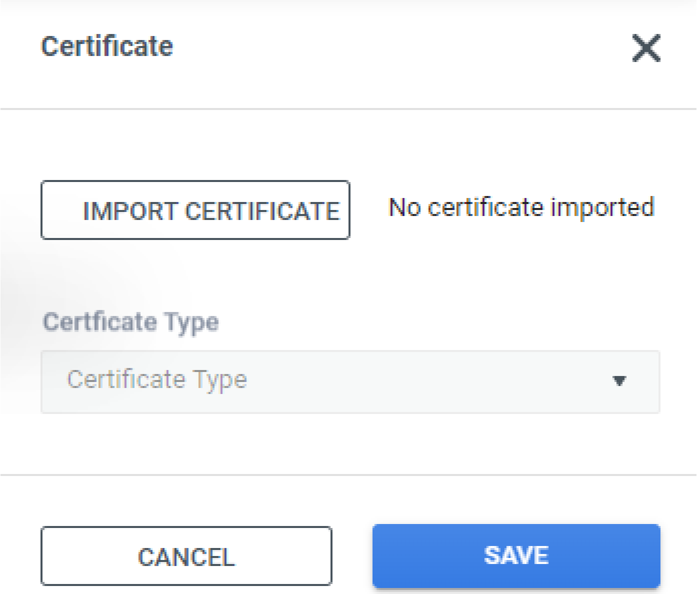
Server certificates

Use the following procedure to import a server certificate.



To import a server certificate:

1. Go to the *Server Certificates* section of the *Configuration* > *Setup* > *Certificates* page.
2. Click *IMPORT CERTIFICATE*.



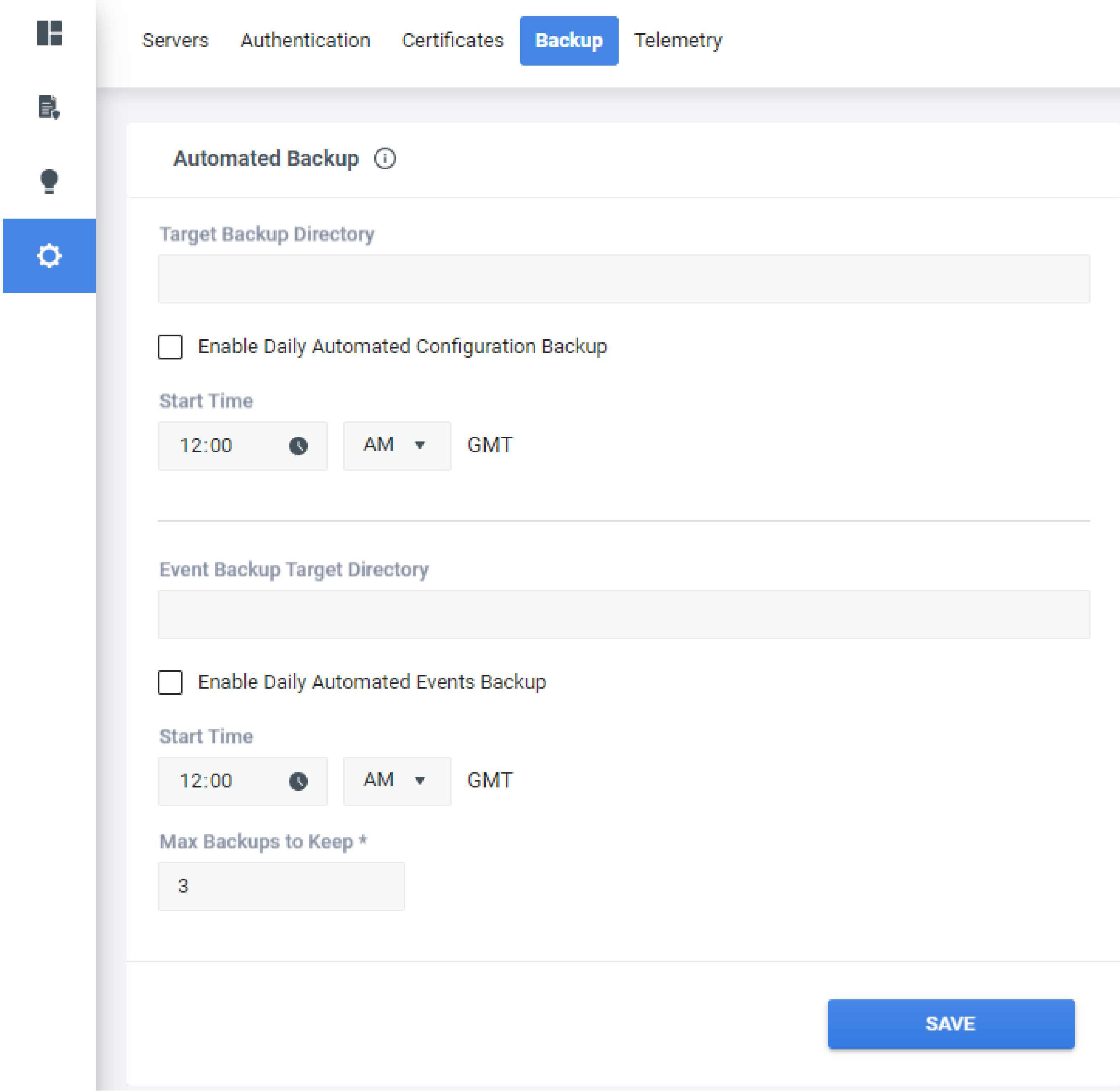
3. In the *Server Certificate* panel, click *IMPORT CERTIFICATE* and select the certificate to import.
4. Select the certificate type: *WEB PROXY*.
5. Click *SAVE*.

Backup

Go to *Configuration* > *Setup* > *Backup* to do the following:

- Automated backup on page 124
- Configuration backup on demand on page 126
- Restore configuration data on page 126

Automated backup



Automated Backup ⓘ

Target Backup Directory

□ Enable Daily Automated Configuration Backup

Start Time

12:00 AM GMT

Event Backup Target Directory

□ Enable Daily Automated Events Backup

Start Time

12:00 AM GMT

Max Backups to Keep *

3

Before setting up backups, configure an SMB server. See SMB on page 116

.

There are two types of backups:

- Configuration backup

  This is a full snapshot of the entire analytics store for compliance and disaster recovery purposes. This backup can run on a specified daily schedule.

  This backup will retain data for each event type on a monthly index basis. At the end of the calendar month, a new index is created, and the old index is retained on the disk subject to availability of disk space. When disk space runs out (the high water is 50% free disk), the oldest index is deleted and then the second oldest, and so on, until the disk free space falls below the low water mark of 40%. The daily archival contains the full data set and supersedes the previous day’s archive. Fortinet recommends keeping backups spanning multiple days to guard against data corruption seeping in for any index on a particular day. In that case, a clean older backup is available to which you can fall back.
- Events backup

  This archive contains only log and threat data, which are used by FortiPolicy to improve the product. This backup can run on a specified daily schedule.

Both archive types are deleted from a local disk as soon as they are copied to their ultimate location to free up disk space.

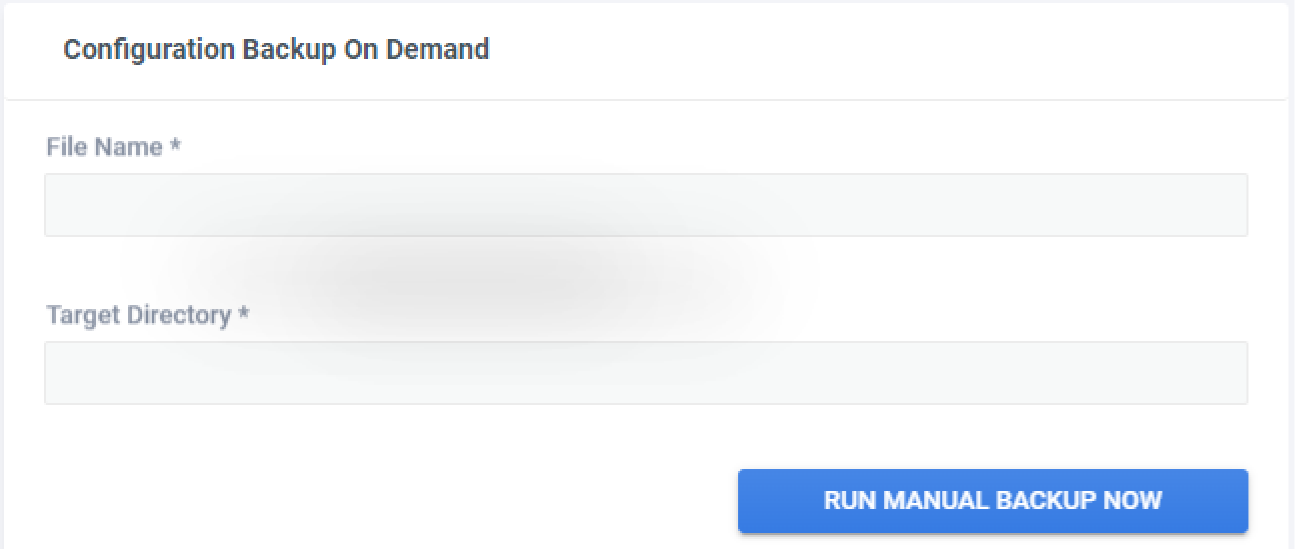
To schedule an automated configuration backup:

1. Enter the target backup directory on your SMB server.
2. Select the *Enable Daily Automated Configuration Backup* checkbox.
3. Set the time to perform the daily backup.
4. Click *SAVE*.

To schedule an automated events backup:

1. Enter the events backup target directory on your SMB server.
2. Select the *Enable Daily Automated Events Backup* checkbox.
3. Set the time to perform the daily backup.
4. Click *SAVE*.

Configuration backup on demand



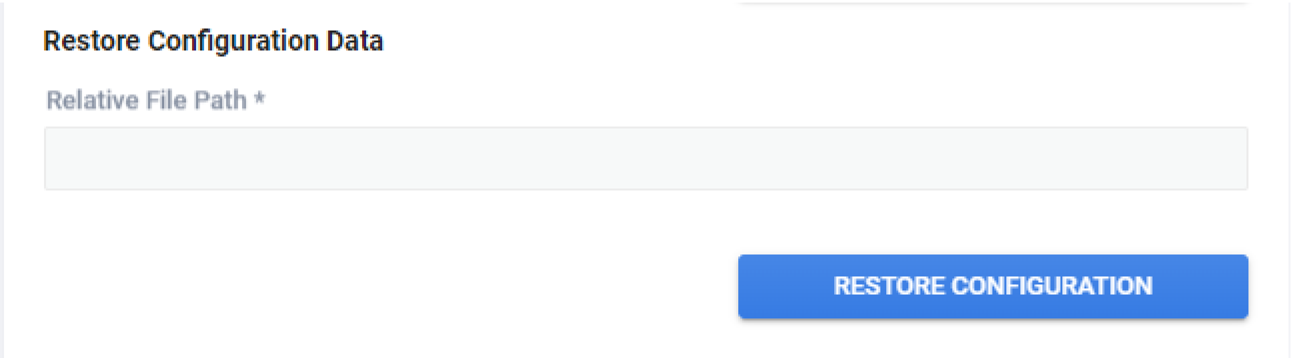
To run a manual backup:

1. Enter the file name for the backup.
2. Enter the name of the target directory on your SMB server.
3. Click *RUN MANUAL BACKUP NOW*.

Restore configuration data

Use the *Configuration* > *Setup* > *Backup* page to restore a configuration backup or an events backup.

When the configuration is restored, there is a fault on Infrastructure authentication. This is due to an essential security protection that prevents an unauthorized entity from gaining access to the backup. To continue with the restore, re-input the password on the IC vCenter credentials , perform a re-discovery, and then redeploy the data plane.



To restore your configuration data:

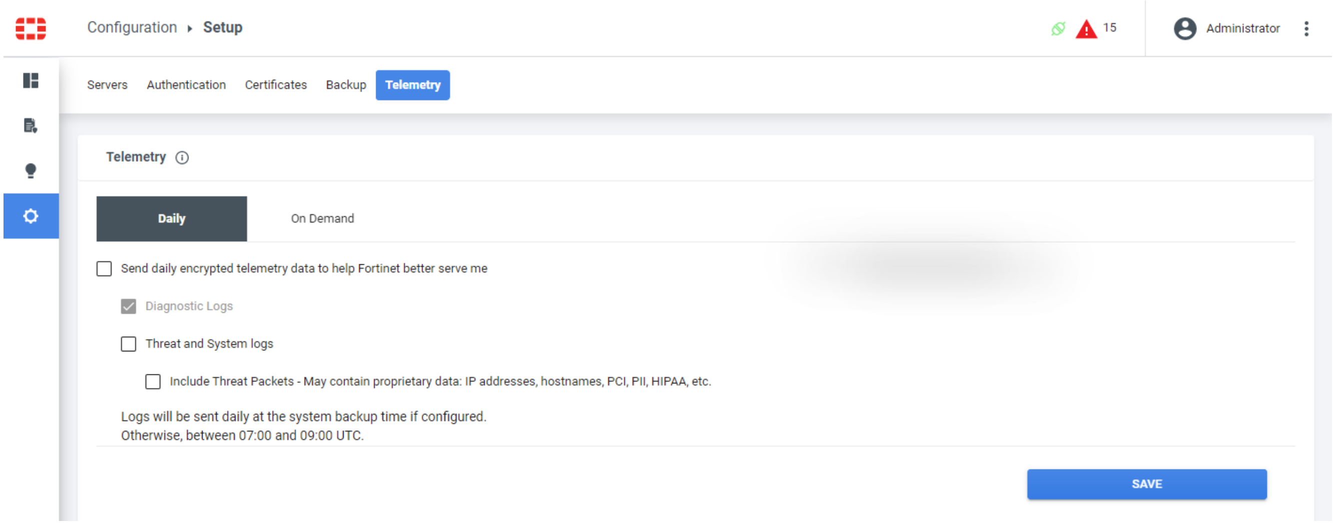
1. Enter the Relative file path to restore. This is the target backup directory and the file name separated by slashes (but do not include the SMB share name).

   For example:

   ```
   Backup/Apr20_m5891_Backup39175.bakup
   ```
2. Click *RESTORE CONFIGURATION*.

Telemetry

Use the *Configuration* > *Setup* > *Telemetry* page to upload daily or on demand logs.



□ Send daily encrypted telemetry data to help Fortinet better serve me

☑ Diagnostic Logs

□ Threat and System logs

□ Include Threat Packets - May contain proprietary data: IP addresses, hostnames, PCI, PII, HIPAA, etc.

Logs will be sent daily at the system backup time if configured.
Otherwise, between 07:00 and 09:00 UTC.

To send diagnostics data to Fortinet daily:

1. Click *Daily*.
2. Enable the *Send daily encrypted telemetry data to help Fortinet better serve me* checkbox.
3. Click *SAVE*.

Logs are sent daily at the system backup time if configured; otherwise, the logs are sent between 07:00 and 09:00 UTC.

To upload on-demand logs:

1. Click *On Demand*.
2. Click *SEND NOW*.

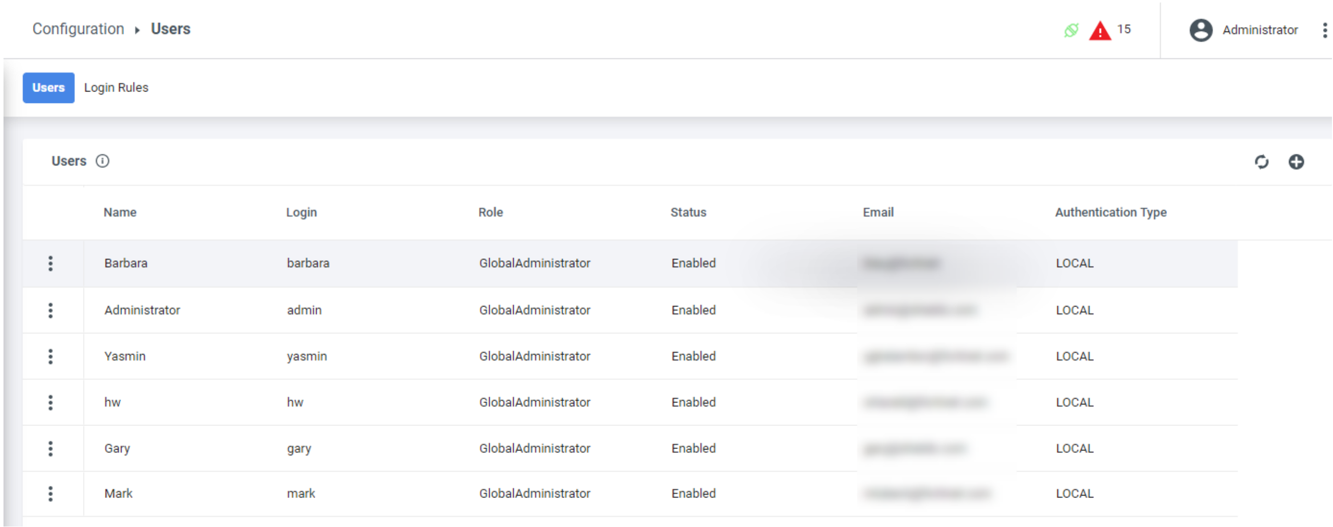
Users

Go to *Configuration* > *Users* to view, add, or edit FortiPolicy user profiles or to assign user login rules for inactivity, lockout, idle session timeout, local password expiration, and local password criteria.

The *Configuration* > *Users* page has two tabs:

- Users on page 127
- Login rules on page 131

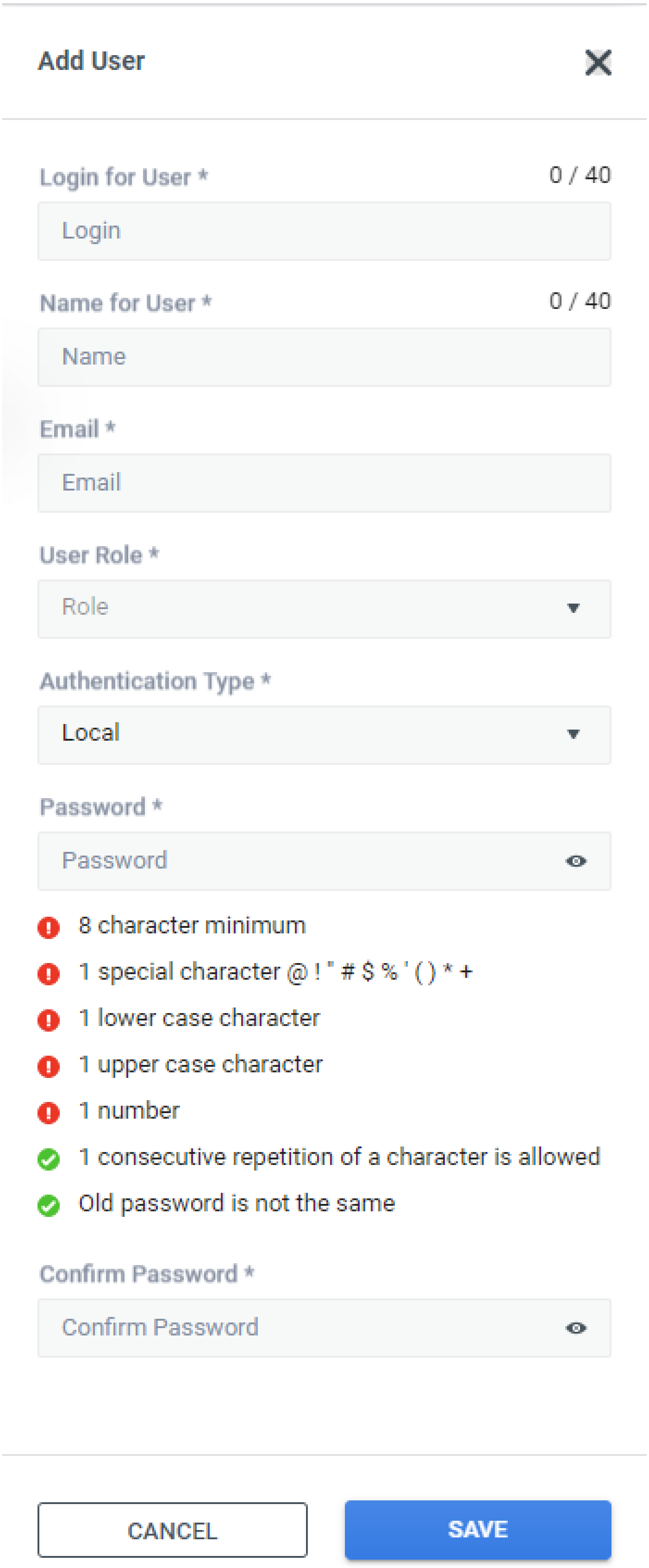
Users



	Name	Login	Role	Status	Email	Authentication Type
⋮	Barbara	barbara	GlobalAdministrator	Enabled	[redacted]	LOCAL
⋮	Administrator	admin	GlobalAdministrator	Enabled	[redacted]	LOCAL
⋮	Yasmin	yasmin	GlobalAdministrator	Enabled	[redacted]	LOCAL
⋮	hw	hw	GlobalAdministrator	Enabled	[redacted]	LOCAL
⋮	Gary	gary	GlobalAdministrator	Enabled	[redacted]	LOCAL
⋮	Mark	mark	GlobalAdministrator	Enabled	[redacted]	LOCAL

To create a new user profile:

1. Go to*Configuration* > *Users* > *Users*.
2. Click the + icon in the upper right corner.



Add User

Login for User * 0 / 40

Login

Name for User * 0 / 40

Name

Email *

Email

User Role *

Role ▾

Authentication Type *

Local ▾

Password *

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
- ✓ Old password is not the same

Confirm Password *

Confirm Password

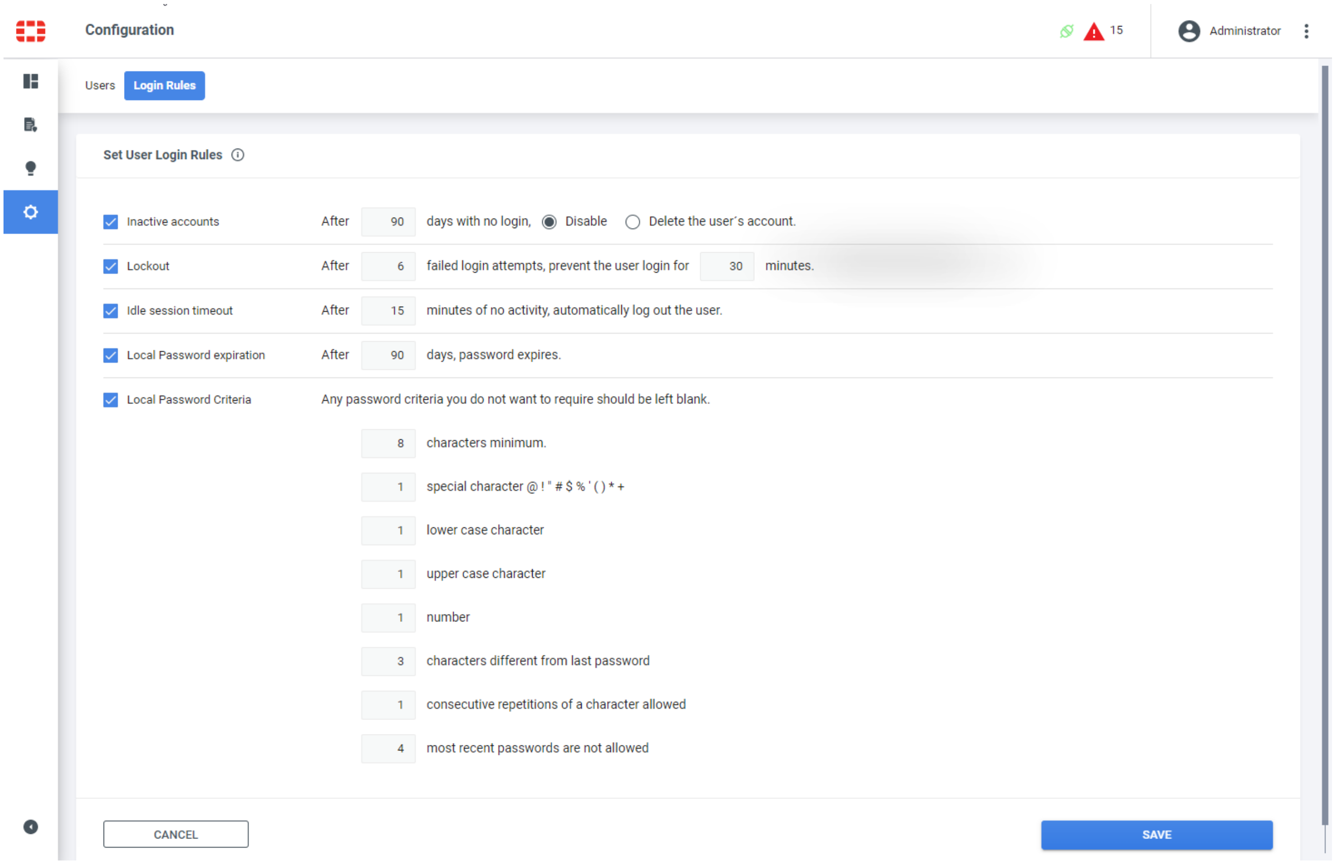
3. Enter the login name for the users.
4. Enter the full name of the user.
5. Enter the email address for the user.
6. Select the user role: *GlobalAdministrator*, *PolicyProvisioner*, or *Auditor*.

Role	Description
GlobalAdministrator	Global—Full access to all permissions; can assign or remove GlobalAdministrators.
PolicyProvisioner	Responsible for overall security of the system; configures and manages security policies, infrastructure and security-related dashboards, and alerts.
Auditor	A subset of the PolicyProvisioner role; has view-only access to security policies, reports, dashboards, and role-based access control (RBAC).

7. Select the authentication type, either *Local* or *LDAP*.
8. If you selected *Local*, enter the password and then confirm it.
9. If you selected *LDAP*, enter the user DN.
   Go to *Configuration* > *Setup* > *Authentication* > *LDAP* to configure communication with the LDAP server.
10. Click *SAVE*.

To edit a user profile, click the vertical ellipsis at the start of the user profile row in the table and select *Edit* or *Delete*.

Login rules



Set User Login Rules

☑ Inactive accounts After 90 days with no login, ● Disable ○ Delete the user's account.

☑ Lockout After 6 failed login attempts, prevent the user login for 30 minutes.

☑ Idle session timeout After 15 minutes of no activity, automatically log out the user.

☑ Local Password expiration After 90 days, password expires.

☑ Local Password Criteria Any password criteria you do not want to require should be left blank.

8 characters minimum.

1 special character @ ! " # $ % ' ( ) * +

1 lower case character

1 upper case character

1 number

3 characters different from last password

1 consecutive repetitions of a character allowed

4 most recent passwords are not allowed

FortiPolicy provides PCI support for local users. PCI hygiene options are available for login password changes and lockouts. Passwords include expiry configuration, as well as inactivity, idle session timing, and local password handling.

To configure FortiPolicy local user login settings:

1. Go to *Configuration* > *Users* > *Login Rules*.
2. Check a rule checkbox to apply it to all local users (select as many checkbox options as needed) and then enter the rule criteria (default settings are displayed for reference).

Login Rule	Description
Inactive accounts	Choose an inactivity criteria. After X days with no login, either disable or delete the user's account. The default is 90 days of inactivity to disable the user's account. **NOTE:** The specified number of consecutive days of inactivity results in the disabling or automatic removal of the user's account, based on your selected choice. Audit logs include user ID, type of event, time stamp, success or failure indication, origination of event, and identity or name of the system component /resource accessed.

Login Rule	Description
Lockout	Enter the number of login attempts you'll allow before locking out the user for a set number of minutes. The defaults are 6 failed logins and 30 minutes of lockout.
Idle session timeout	Enter the number of minutes of inactivity you will allow before logging out the user session. The default is 15 minutes.
Local password expiration	Enter the number of days after which user passwords will expire. The default is 90 days.
Local password criteria	Set variables for password configuration. Leave the setting blank if you do not want to include it. A minimum of 8 characters are required • At least 1 special character is required: !"#$%&'( )*+ • At least 1 lower case character is required • At least 1 upper case character is required • At least 1 number is required • At least 3 characters must be different from last-used password • 1 consecutive repetition of a character is allowed • 4 of the most recent passwords are not allowed

3. Click *SAVE* to save your changes.

Responses

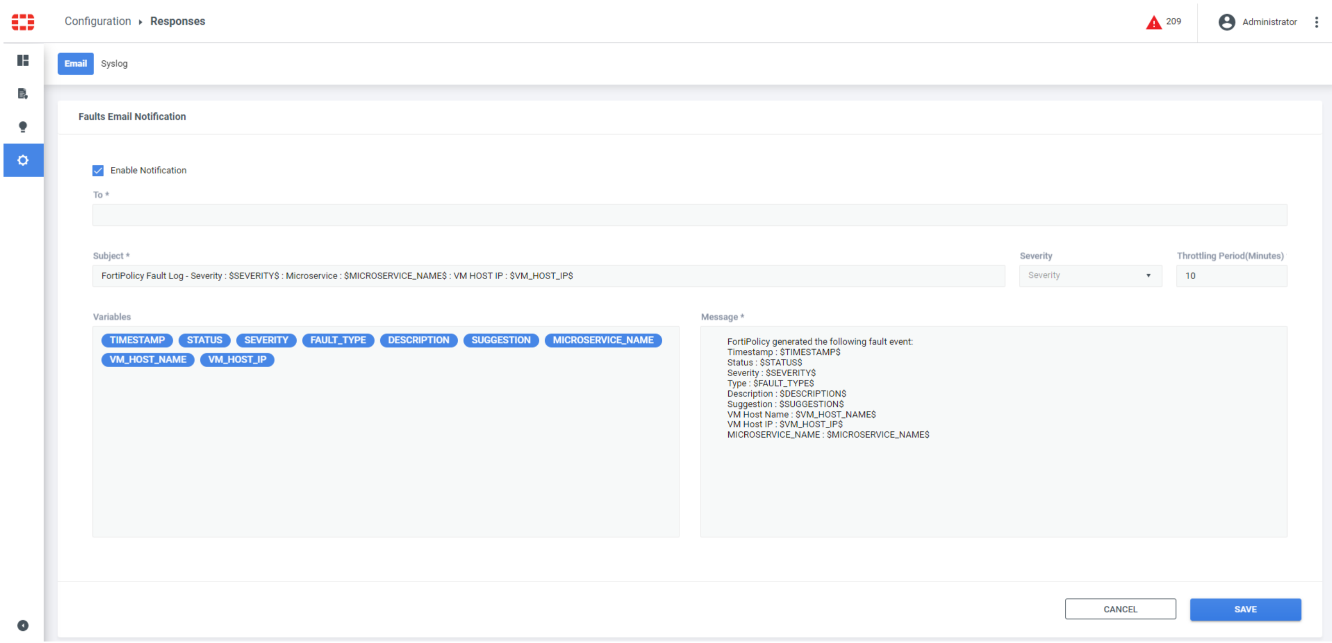
The *Responses* page has two tabs:

- Email on page 132
- Syslog on page 133

Email

FortiPolicy can send email notifications for faults to a list of recipients.

Email notifications for threats have recently become obsolete and are no longer required. This configuration will be removed.



Faults Email Notification

☑ Enable Notification

To *

Subject *
FortiPolicy Fault Log - Severity : $SEVERITY$: Microservice : $MICROSERVICE_NAME$: VM HOST IP : VM_HOST_IP

Severity
Severity ▾

Throttling Period(Minutes)
10

Variables
TIMESTAMP STATUS SEVERITY FAULT_TYPE DESCRIPTION SUGGESTION MICROSERVICE_NAME VM_HOST_NAME VM_HOST_IP

Message *

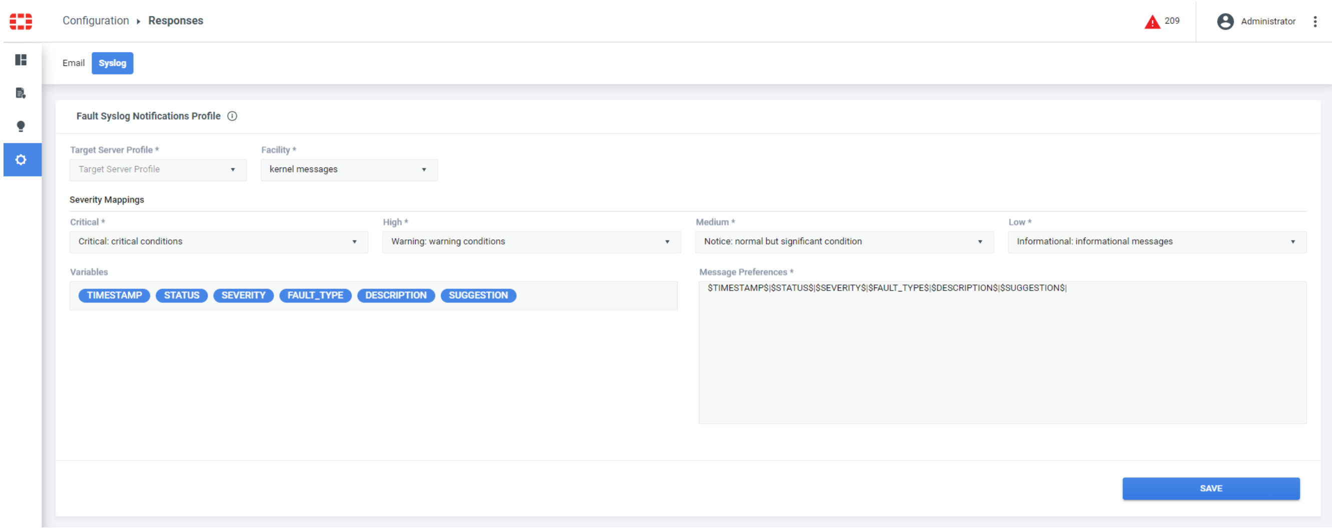
```
FortiPolicy generated the following fault event:
Timestamp : $TIMESTAMP$
Status : $STATUS$
Severity : $SEVERITY$
Type : $FAULT_TYPE$
Description : $DESCRIPTION$
Suggestion : $SUGGESTION$
VM Host Name : $VM_HOST_NAME$
VM Host IP : $VM_HOST_IP$
MICROSERVICE_NAME : $MICROSERVICE_NAME$
```

To configure email notifications for faults:

1. Go to *Configuration >Responses > Email*.
2. Select the *Enable Notification* checkbox.
3. Make any necessary changes in the *Faults Email Notification* form.
4. Click *SAVE*.

Syslog

The ACL and Threat notifications profiles are obsolete. These configurations have recently become obsolete and are no longer required. They will be removed.



Fault Syslog Notifications Profile

Target Server Profile *: Target Server Profile

Facility *: kernel messages

Severity Mappings

Critical *: Critical: critical conditions

High *: Warning: warning conditions

Medium *: Notice: normal but significant condition

Low *: Informational: informational messages

Variables: TIMESTAMP STATUS SEVERITY FAULT_TYPE DESCRIPTION SUGGESTION

Message Preferences *: $TIMESTAMP$|$STATUS$|$SEVERITY$|$FAULT_TYPE$|$DESCRIPTION$|$SUGGESTION$|

To configure Fault Syslog notification profiles:

1. Go to *Configuration* > *Responses* > *Syslog*.
2. Make any necessary changes in the *Fault Syslog Notifications Profile* form.
3. Click *SAVE*.

.

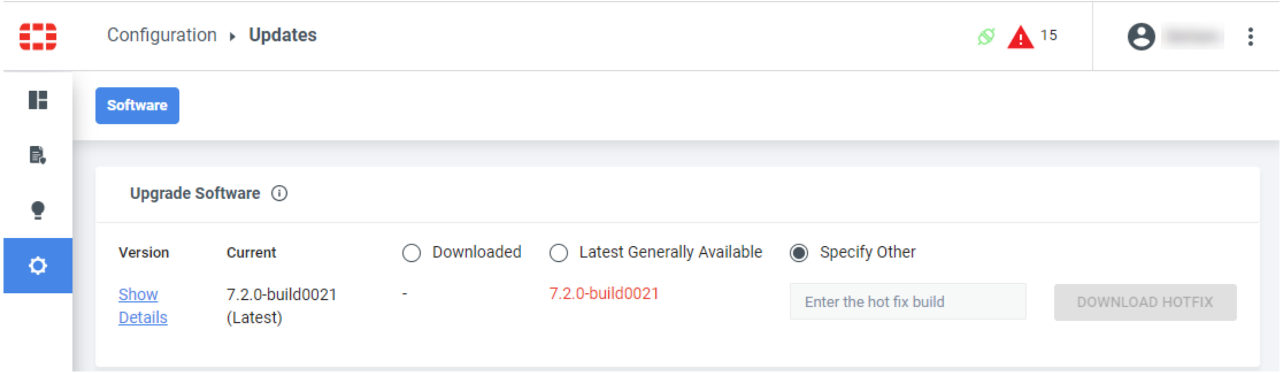
Updates

Go to *Configuration* > *Updates* to upgrade the FortiPolicy software.

If you are using Google Chrome, either clear the Chrome cache or launch a new browser after performing an upgrade.

To upgrade the FortiPolicy software:

1. Go to *Configuration* > *Updates* > *Software*.



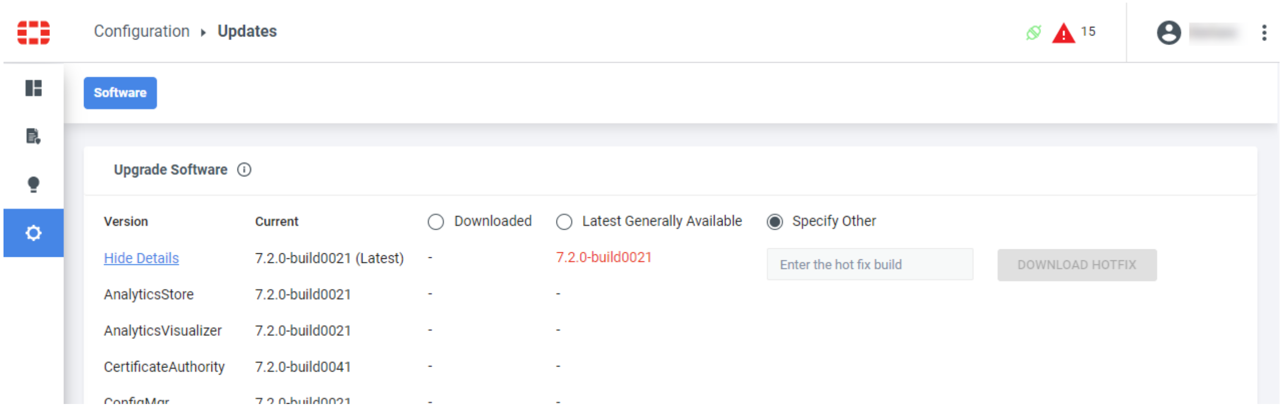
Configuration ▸ **Updates** 15 [redacted]

Software

Upgrade Software ⓘ

Version	Current	○ Downloaded	○ Latest Generally Available	● Specify Other	
Show Details	7.2.0-build0021 (Latest)	-	7.2.0-build0021	Enter the hot fix build	DOWNLOAD HOTFIX

2. Click *Show Details* to review the list of deployed microservices and software versions.



Configuration ▸ **Updates** 15 [redacted]

Software

Upgrade Software ⓘ

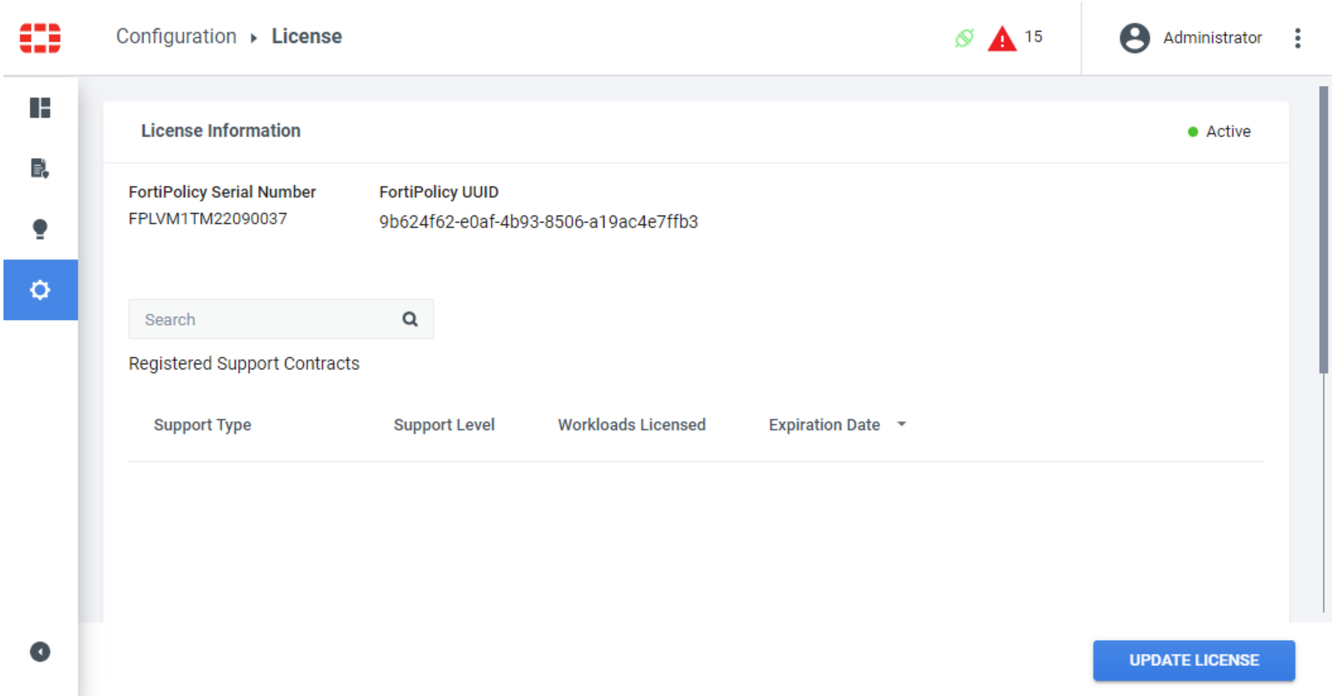
Version	Current	○ Downloaded	○ Latest Generally Available	● Specify Other	
Hide Details	7.2.0-build0021 (Latest)	-	7.2.0-build0021	Enter the hot fix build	DOWNLOAD HOTFIX
AnalyticsStore	7.2.0-build0021	-	-		
AnalyticsVisualizer	7.2.0-build0021	-	-		
CertificateAuthority	7.2.0-build0041	-	-		
ConfigMgr	7.2.0-build0021	-	-		

3. Click *Downloaded* to view only downloaded software and then click *UPGRADE SOFTWARE* to upgrade the software.
4. Click *Latest Generally Available* to view only the latest and generally available software and then click *DOWNLOAD SOFTWARE* to download the software.
5. To deploy a hot fix build, click *Specify Other*, enter the hot fix build number, and then click *DOWNLOAD HOTFIX*.

License

Go to *Configuration* > *License* to view or update your FortiPolicy licenses.

When a license expires, TCP/DPI cannot scale-out to multiple instances, and the system will not execute upgrades.



License Information ● Active

FortiPolicy Serial Number
FPLVM1TM22090037

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

Search

Registered Support Contracts

Support Type	Support Level	Workloads Licensed	Expiration Date

To update your FortiPolicy license:

1. Go to FortiCloud and create a new account or log in with an existing account.
2. In the *Registration Code* field, enter the FortiPolicy UUID.
   The FortiPolicy UUID is located in the *Configuration* > *License* page in FortiPolicy.
3. 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.
4. In FortiPolicy, go to *Configuration* > *License* and click *BROWSE LICENSE FILE*.
5. Select your FortiPolicy license.
6. Click *IMPORT LICENSE*.
7. Click *IMPORT*.
8. Check in the upper right corner that the status of the license is *Active*.
   You will see that the *Registered Support Contracts* table is updated with all the latest contracts that have been assigned to your license.

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

Reports

On the *Configuration* > *Reports* page, you can generate an access control rules report. See Access control rules report on page 137.

Access control rules report

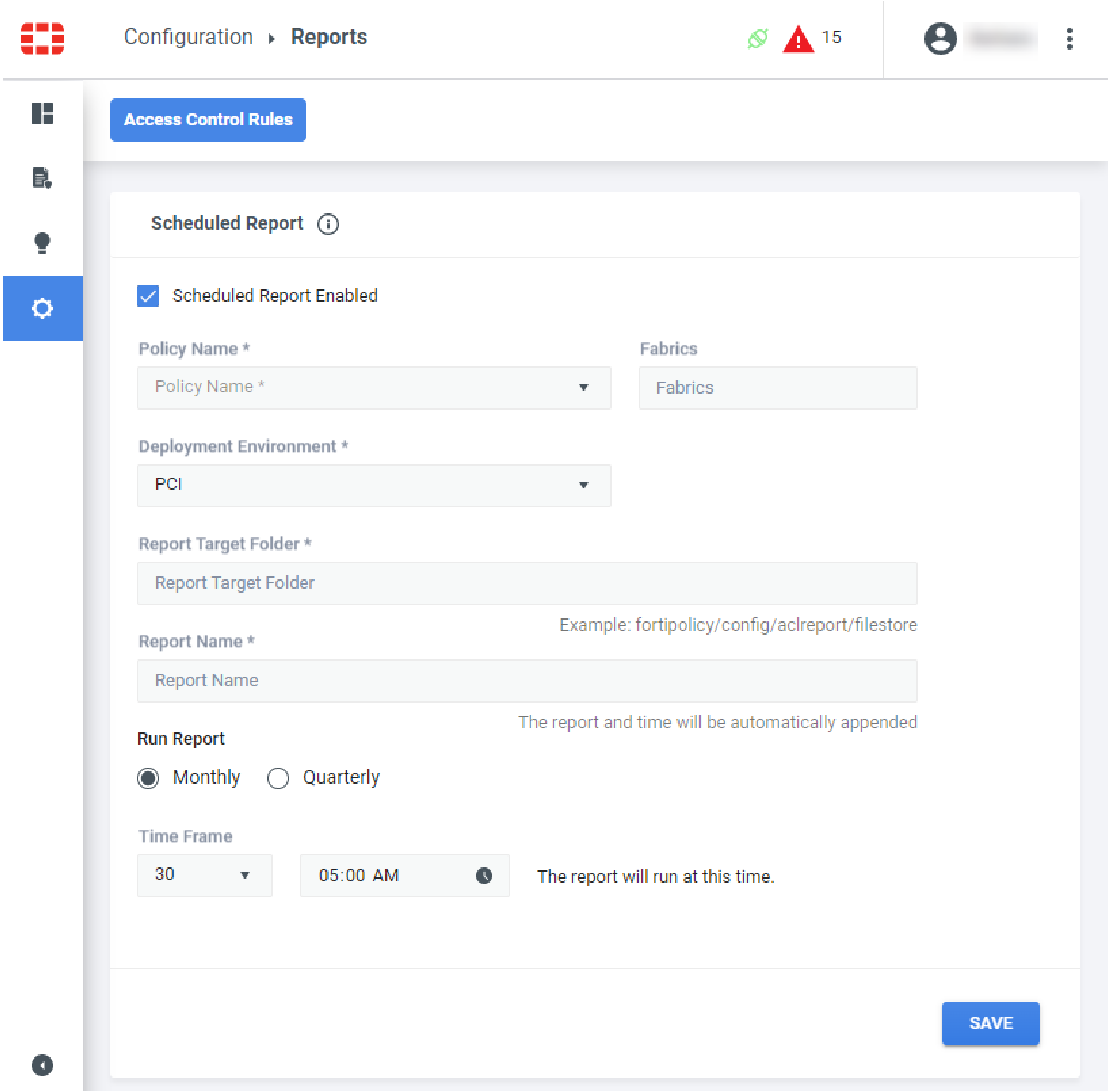
Access control reporting includes options to schedule and generate monthly or quarterly audit reports, including the ability to choose either all deployment environments or a specific deployment environment.

Configure report generation for either default or custom ACLs, as needed.

You will need the path to a location on an SMB share to render the report.

To schedule an access control rules report:

1. Go to *Configuration > Reports > Access Control Rules*.



Scheduled Report ⓘ

☑ Scheduled Report Enabled

Policy Name * : Policy Name *

Fabrics: Fabrics

Deployment Environment * : PCI

Report Target Folder * : Report Target Folder

Example: fortipolicy/config/aclreport/filestore

Report Name * : Report Name

The report and time will be automatically appended

Run Report

● Monthly ○ Quarterly

Time Frame: 30 05:00 AM

The report will run at this time.

2. Select the *Scheduled Report Enabled* checkbox.
3. Select an ACL policy.

   If the selected policy is assigned to the Security Fabric, the fabric name is displayed in the *Fabrics* field.
4. Select a deployment environment or select *All Environments*.
5. Enter a target folder path for the report.
6. Enter a report name.
7. Select whether to run the report on a monthly or quarterly basis.

8. Select when the report will run.
9. Click *SAVE.*

Glossary

A

AAA
Authentication, Authorization, and Accounting

AD
Active Directory

ADOM
Administrative Domain

AES
Advanced Encryption Standard

AMI
Amazon Machine Image

AP
Access Point

API
Application Programming Interface

APN
Access Point Name

APT
Advanced Persistent Threat

ATP
Advanced Threat Protection

AV
Antivirus

AVP
Attribute Value Pairs

AWS
Amazon Web Service

B

BGP
Border Gateway Protocol

C

C&C
Command and Control

CA
Certificate Authority

CASI
Cloud Access Security Inspection

CBC
Cipher Block Chaining

CHAP
Challenge-Handshake Authentication Protocol

CIDR
Classless Inter-Domain Routing

CLI
Command Line Interface

CN
Common Name

CoA
Change of Authorization

CPU
Central Processing Unit

CRL
Certificate Revocation List

CSR
Certificate Signing Request

CSV
Comma Separated Value

CVE
Common Vulnerabilities and Exposures

D

DC
Domain Controller, Direct Current

DES
Data Encryption Standard

DH
Diffie-Hellman

DHCP
Dynamic Host Configuration Protocol

DLL
Dynamic-Link Library

DLP
Data Loss Prevention

DN
Distinguished Name

DNAT
Destination Network Address Translation

DNS
Domain Name System

DSCP
Differentiated Services Code Point

DSRI
Disable Server Response Inspection

DTLS
Datagram Transport Layer Security

E

EA
E-mail Address

EAPOL
Extensible Authentication Protocol over LAN (Local Area Network)

EC
Endpoint Control

EC2
Elastic Compute Cloud

EGP
Exterior Gateway Protocol

EMS
Enterprise Management Server

ESD
Electrostatic Discharge

ESP
Encapsulated Security Payload

F

FAZ
FortiAnalyzer

FCT
FortiClient

FDN
FortiGuard Distribution Network

FDS
FortiGuard Distribution Servers

FG
FortiGate

FGFM
FortiGate-FortiManager

FMG
FortiManager

FQDN
Fully Qualified Domain Name

FSA
FortiSandbox

FSSO
Fortinet Single Sign-On

FTP
File Transfer Protocol

G

GCF
Gatekeeper Confirm

GPRS
General Packet Radio Service

GRE
Generic Routing Encapsulation

GTP
GPRS Tunneling Protocol

GUI
Graphical User Interface

GUID
Globally Unique Identifier

H

HA
High Availability

hcache
Hard Cache

HDD
Hard Disk Drive

HTML
HyperText Markup Language

HTTP
HyperText Transfer Protocol

I

I/O
Input / Output

IBP
Identity-based Policy

ICAP
Internet Content Adaptation Protocol

ICMP
Internet Control Message Protocol

IGP
Interior Gateway Protocol

IKE
Internet Key Exchange

IMAP
Internet Message Access Protocol

IOC
Indicators of Compromise

IP
Internet Protocol

IPS
Intrusion Prevention System

IPsec
Internet Protocol Security

ISDB
Internet Service Database

ISP
Internet Service Provider

IV
Initialization Vector

J

JSON
JavaScript Object Notation

L

L2TP
Layer 2 Tunneling Protocol

LACP
Link Aggregation Control Protocol

LAN
Local Area Network

LDAP
Lightweight Directory Access Protocol

M

MAC
Media Access Control

MD5
Message Digest 5

MGCP
Media Gateway Controller Protocol

MIB
Management Information Base

MMC
Microsoft Management Console

MSCHAP
Microsoft Challenge-Handshake Authentication Protocol

MSS
Maximum Segment Size

N

NAC
Network Access Control or Compliance

NAS
Network Access Server

NAT
Network Address Translation

NAT-PT
Network Address Translation (NAT) Port Translation

NDcPP
Network Device Collaborative Protection Profile

NGFW
Next-Generation Firewall

NNTP
Network News Transfer Protocol

NOC
Network Operations Center

NPU
Network Processing Unit

NTLM
NT LAN Manager

NTP
Network Time Protocol

O

OCSP
Online Certificate Status Protocol

OFTP
Odette File Transfer Protocol

ONC-RPC
Open Network Computing Remote Procedure Call

OSPF
Open Shortest Path First

OTP
One-time Password

OU
Organization Unit

OUI
Organizationally Unique Identifier

OVF
Open Virtualization Format

P

PAP
Password Authentication Protocol

PAT
Port Address Translation

PEM
Power Entry Module

PFS
Perfect Forward Secrecy

PKCS
Public Key Cryptography Standards

PKI
Public Key Infrastructure

PoE
Power over Ethernet

POP3
Post Office Protocol 3

PPP
Point-to-Point Protocol

PPPoE
Point-to-Point Protocol over Ethernet

PPTP
Point-to-Point Tunneling Protocol

PSK
Pre-Shared Key

R

RADIUS
Remote Authentication Dial-In User

RAID
Redundant Array of Independent Disks

RAM
Random Access Memory

RAS
Registration, Admission, and Status

RBAC
Role Based Access Control

RCF
Registration Confirm

RDP
Remote Desktop Protocol

REST
Representational State Transfer

RFC
Remote Function Call

RSH
Remote Shell

RSSO
RADIUS Single Sign-On

RTM
Real-Time Monitor

RTP
Real-Time Protection

RTSP
Real-Time Streaming Protocol

S

SAN
Storage Area Network

SAP
Shelf Alarm Panel

SCEP
Simple Certificate Enrollment Protocol

SCP
Secure Copy

SCVP
Server-based Certificate Validation Protocol

SDK
Software Development Kit

SDN
Software-Defined Networking

SFTP
Secure (or SSH) File Transfer Protocol

SHA1
Secure Hash Algorithm 1

SIP
Session Initiation Protocol

SMTP
Simple Mail Transfer Protocol

SNAT
Secure Network Address Translation

SNI
Server Name Indication

SNMP
Simple Network Management Protocol

SOC
Security Operations Center

SQL
Structured Query Language

SSH
Secure Shell

SSID
Service Set Identifier

SSL
Secure Sockets Layer

SSO
Single Sign-On

T

TACACS+
Terminal Access Controller Access-Control System

Tcl
Tool Command Language

TCP
Transmission Control Protocol

TFTP
Trivial File Transfer Protocol

TLS
Transport Layer Security

TNS
Transparent Network Substrate

TTL
Time-to-live

U

UDP
User Datagram Protocol

UID
Unique Identifier

URI
Uniform Resource Identifier

URL
Uniform Resource Locator

UTM
Unified Threat Management

UUID
Universally Unique Identifier

V

VDOM
Virtual Domain

VHD
Virtual Hard Disk

VIP
Virtual Internet Protocol

VLAN
Virtual Local Area Network

VM
Virtual Machine

VMDK
Virtual Machine Disk

VoIP
Voice over Internet Protocol

VPC
Virtual Private Cloud

VPN
Virtual Private Network

VSA
Vendor Specific Attribute

W

WAF
Web Application Firewall

WAN
Wide Area Network

WCCP
Web Cache Communication Protocol

WIDS
Wireless Intrusion Detection System

WPA
Wi-Fi Protected Access

WPA2
Wi-Fi Protected Access II

WSDL
Web Services Description Language

WTP
Wireless Transaction Protocol

X

XAuth
Extended Authentication

XML
eXtensible Markup Language

XSS
Cross-site Scripting

XVA
XenServer Virtual Appliance

www.fortinet.com