DEPLOYMENT GUIDE

Fortinet FortiGate and FireMon

Fortinet FortiGate and FireMon

Overview 3

Deployment Prerequisites 3

FireMon Configuration 4

Fortinet Configuration 7

Summary 12

Overview

The FireMon Security Manager Core Platform provides detailed, customizable IT risk analytics that allows network and security management to respond quickly to changing business demands and ensure protection, with real-time assessment of policy enforcement spanning from the specific rules and configurations of every individual device to the combined effectiveness of all defenses.

Fortinet (NASDAQ: FTNT) secures the largest enterprise, service provider, and government organizations around the world. Fortinet empowers its customers with intelligent, seamless protection across the expanding attack surface and the power to take on ever-increasing performance requirements of the borderless network—today and into the future. Only the Fortinet Security Fabric architecture can deliver security features without compromise to address the most critical security challenges, whether in networked, application, cloud, or mobile environments. Fortinet ranks No. 1 in the most security appliances shipped worldwide and more than 400,000 customers trust Fortinet to protect their businesses. Learn more at https://www.fortinet.com, the Fortinet Blog, or FortiGuard Labs.

Deployment Prerequisites

1. Fortinet FortiGate version 4.x or newer
2. FireMon FMOS version 8.15.x or newer

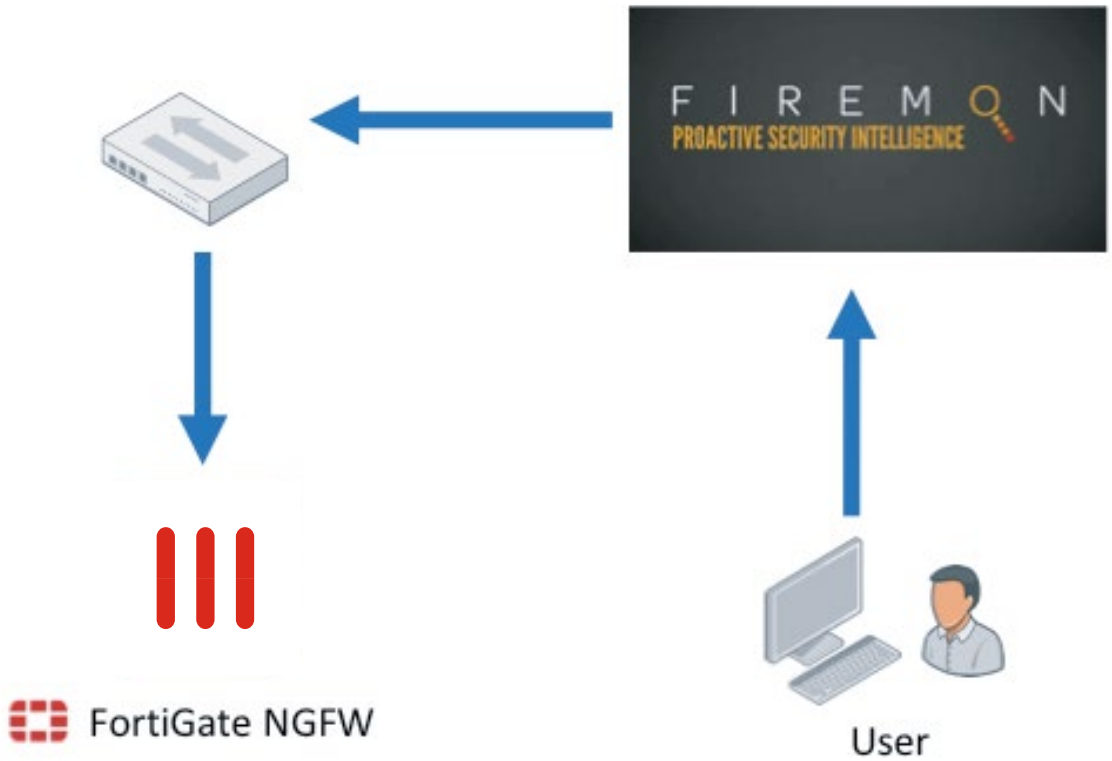
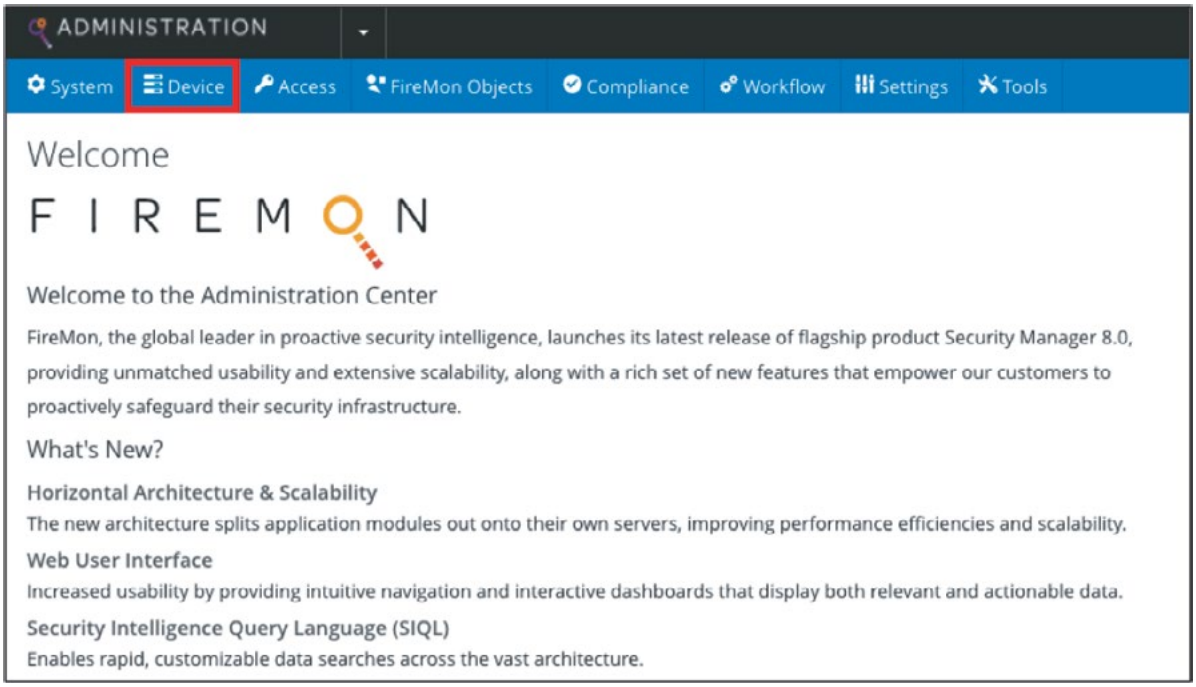


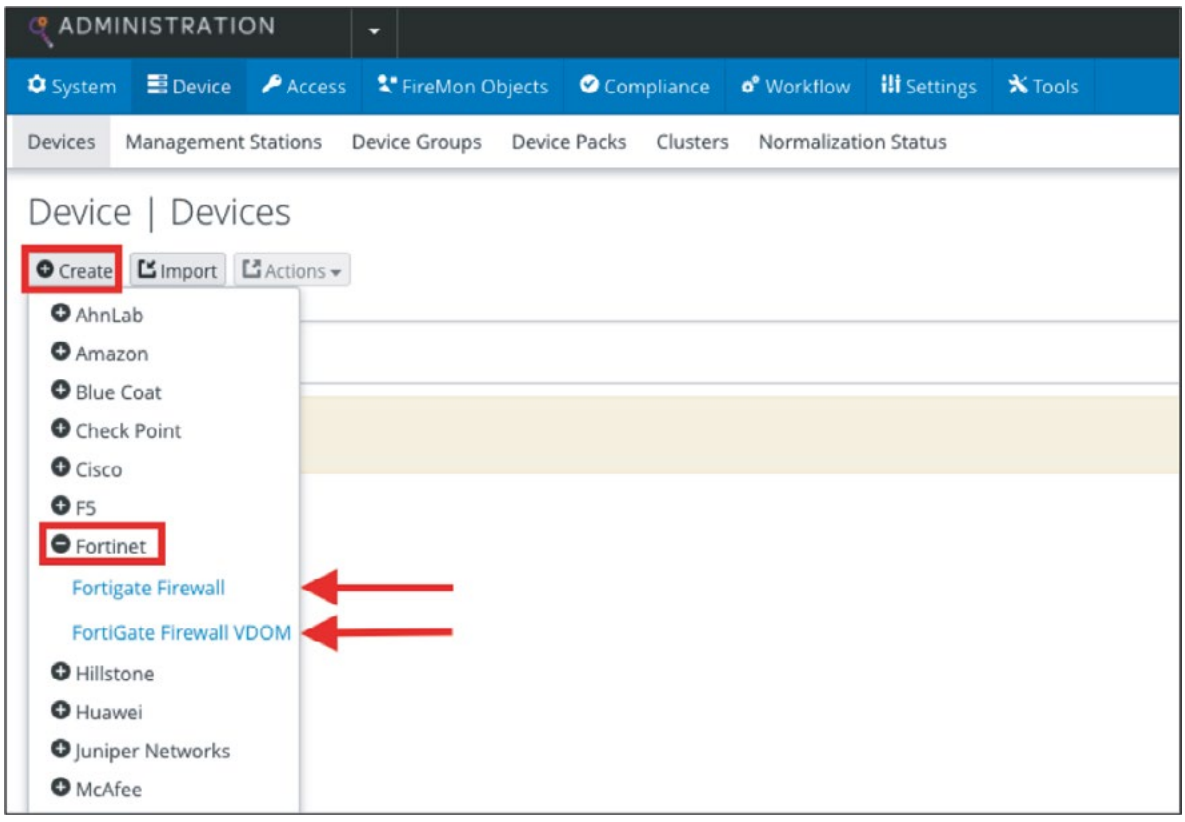
Figure 1: Architecture overview.

FireMon Configuration

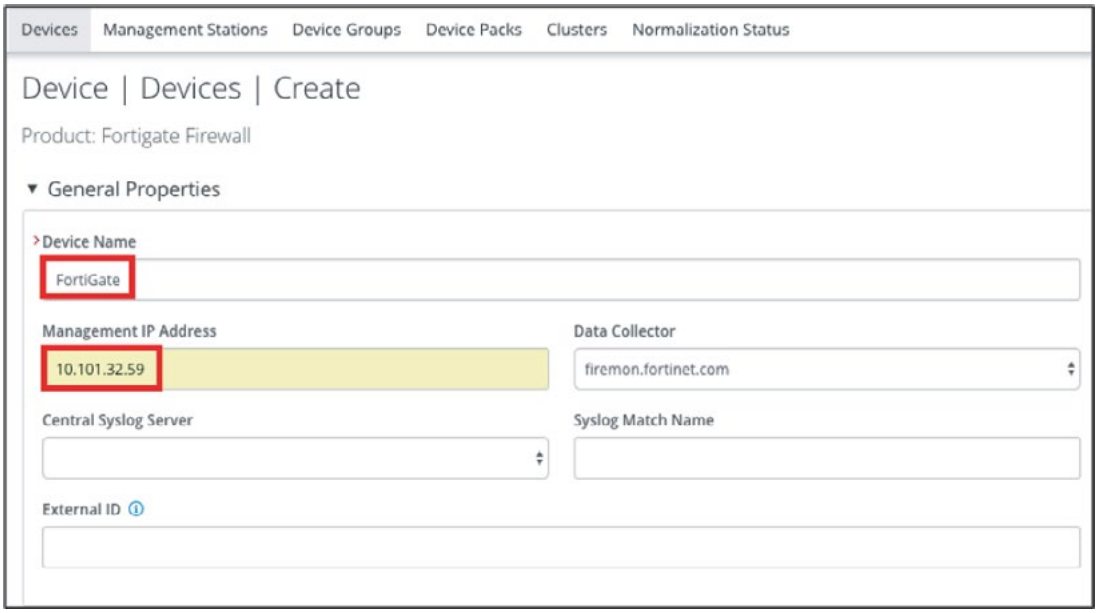
1. From the Administration screen, click Device.



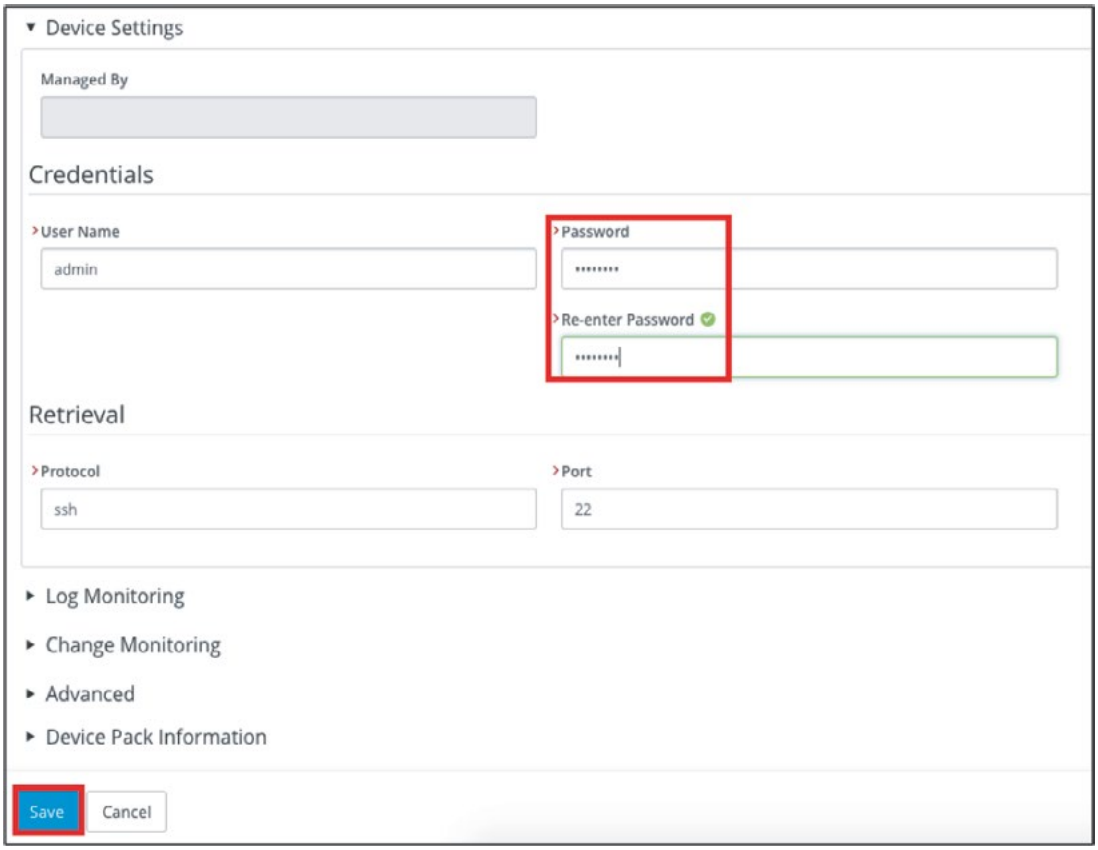
2. From the Devices screen, click Create > Fortinet.
3. Choose FortiGate Firewall or FortiGate Firewall VDOM if your deployment has VDOMs.
4. For VDOMs, be sure to input the correct VDOM name in the device property section.



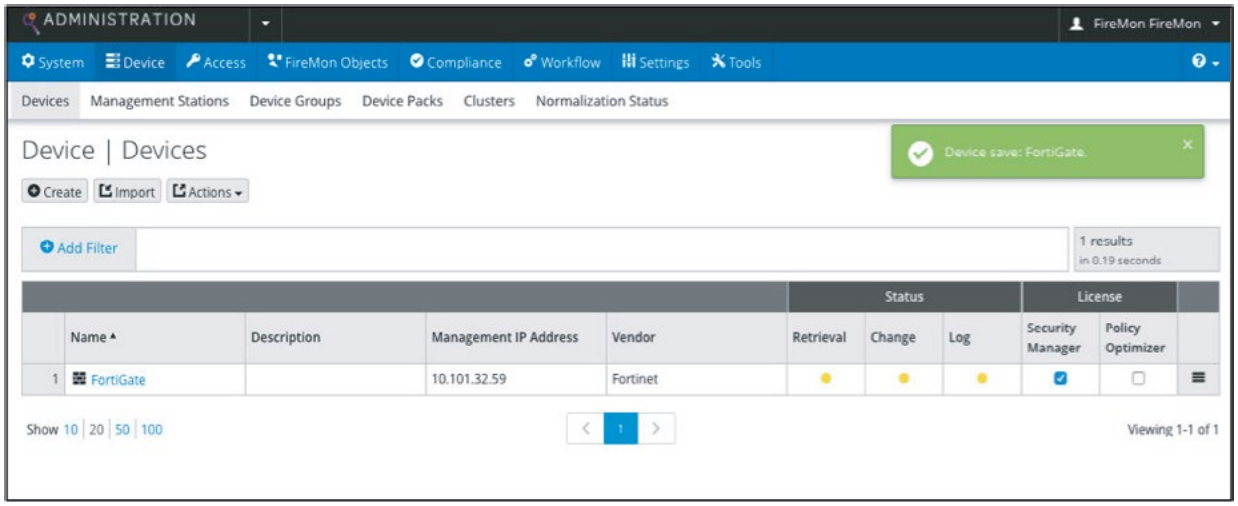
5. Under General Properties, give the device a name and enter the IP Address.



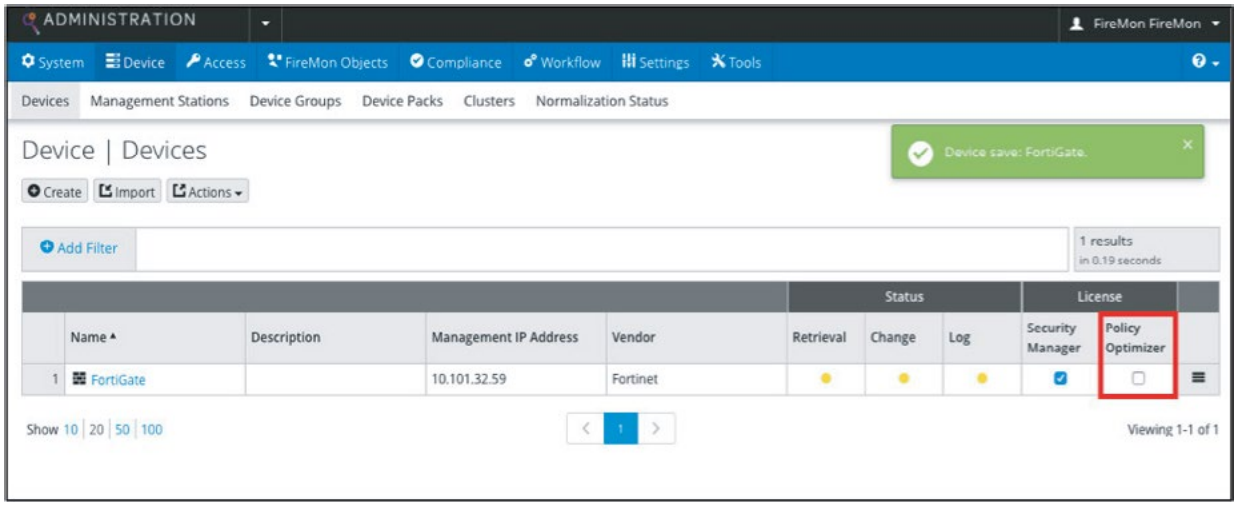
6. Under Device Settings, enter the password for the Admin user then re-enter the password.
7. Click Save when done.
8. Please note: The Admin user will need to be configured with the super_admin profile on the FortiGate.



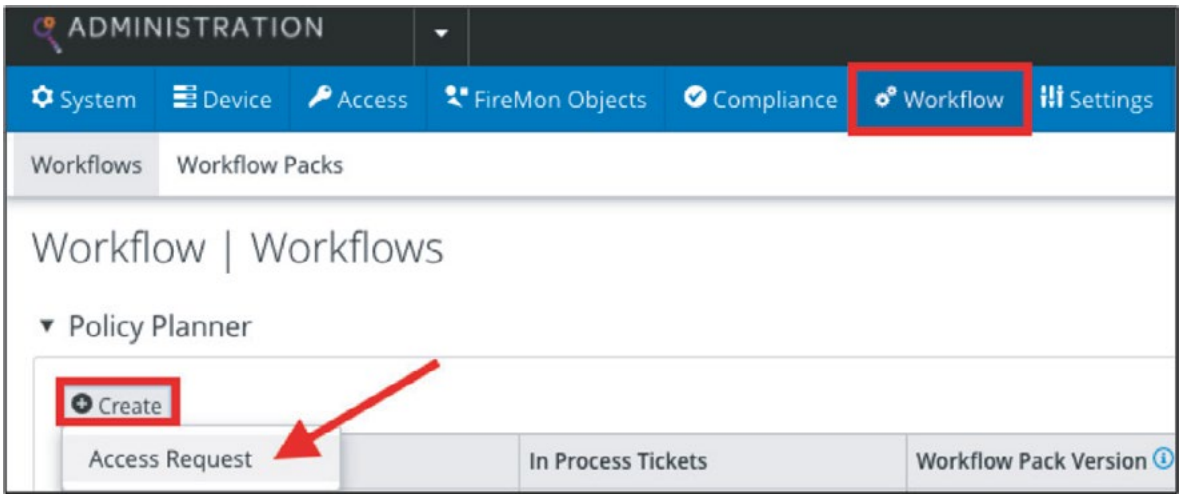
The next screen should look like this.



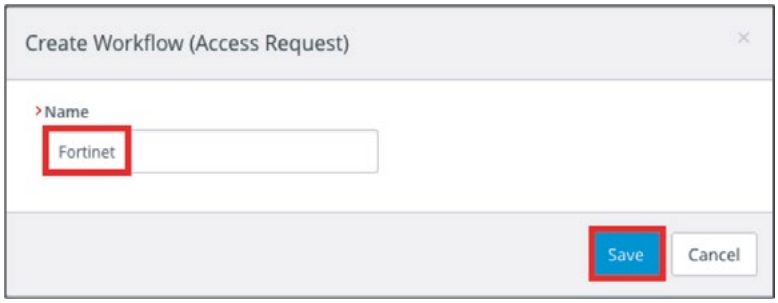
If you plan on using Policy Optimizer, make sure to check the box to enable the License.



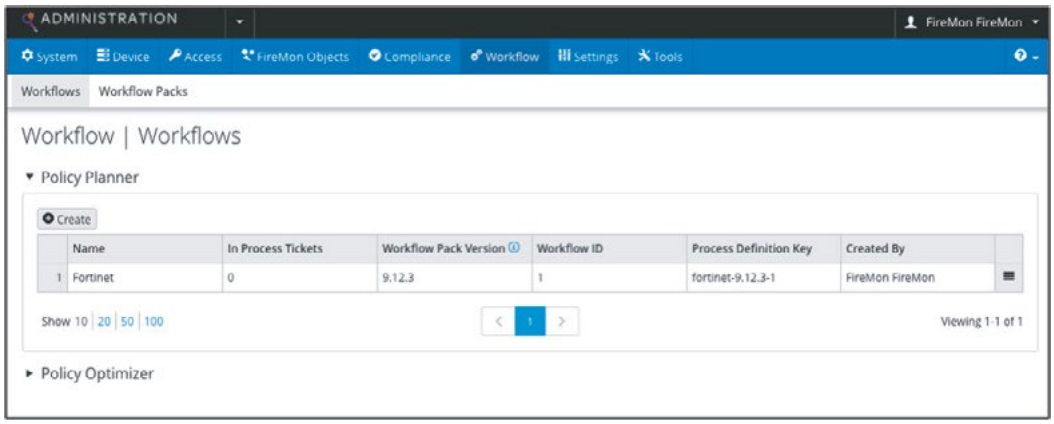
9. Then go to Workflow.
10. Under Policy Planner, click Create > Access Request.



11. Give it a Name, then click Save.

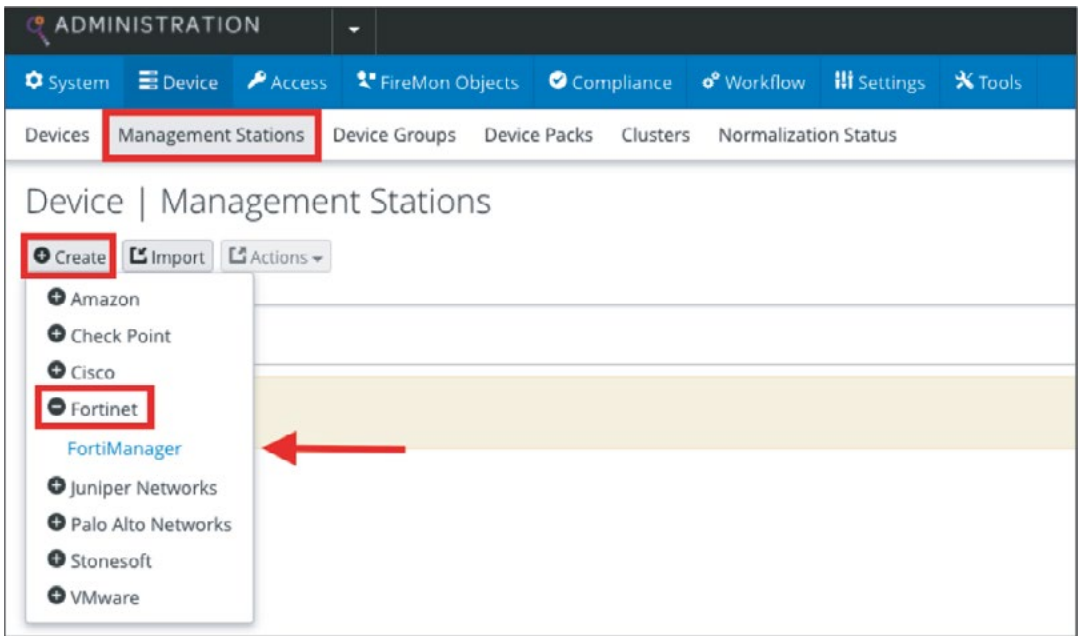


The Workflow screen shout now look like the image below.



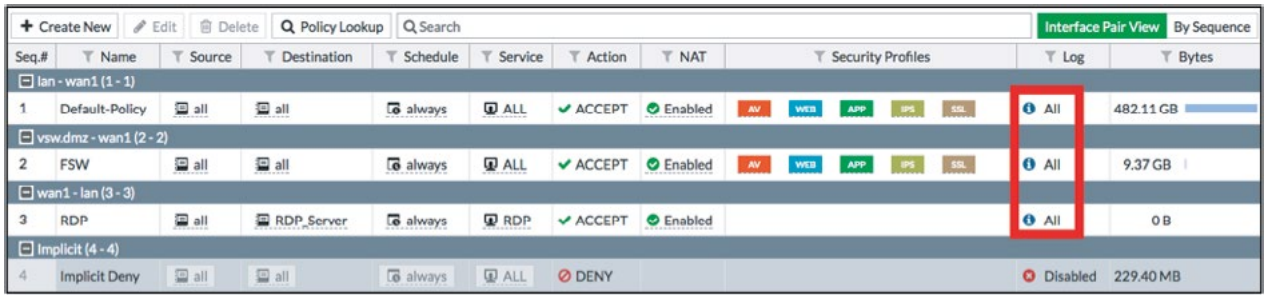
12. Do the same for the Policy Optimizer configuration.

Note: If adding FortiGate firewalls via FortiManager, do this from Devices > Management Stations. The Admin user will need access to all VDOMs enabled.

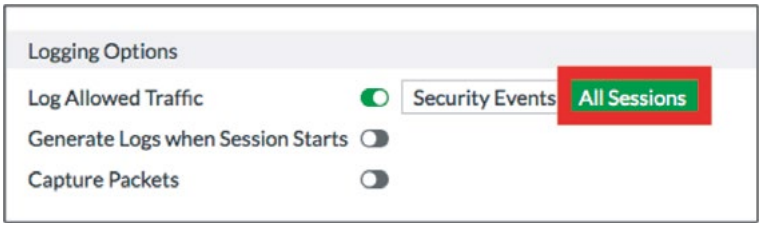


Fortinet Configuration

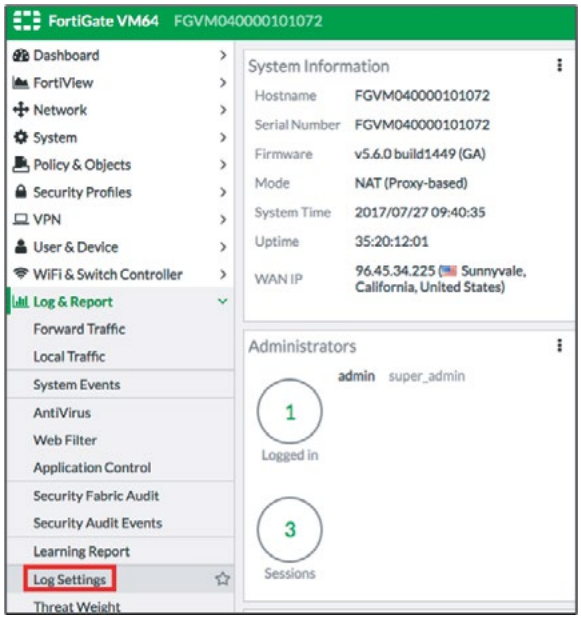
1. Ensure all Firewall rules are set to Log All Sessions.



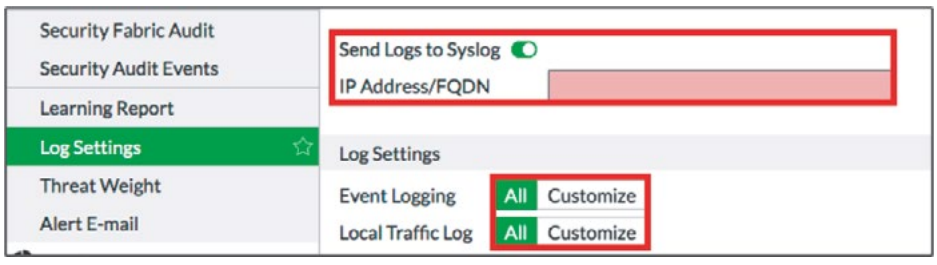
If not, enable this for each rule under Logging Options.



2. Configure FortiGate to send Syslog to the FireMon IP address.
3. Under Log & Report, click Log Settings.



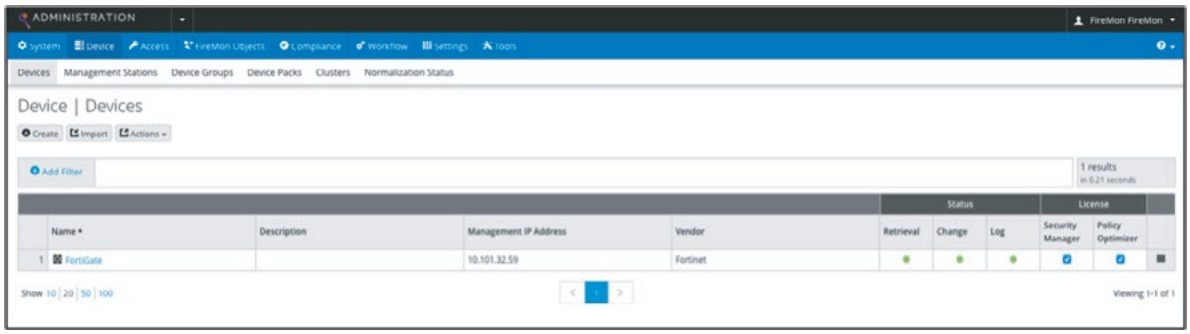
4. Enable Send Logs to Syslog.
5. Enter the IP Address or FQDN of the FireMon server.
6. Select the desired Log Settings.
7. Click Save.



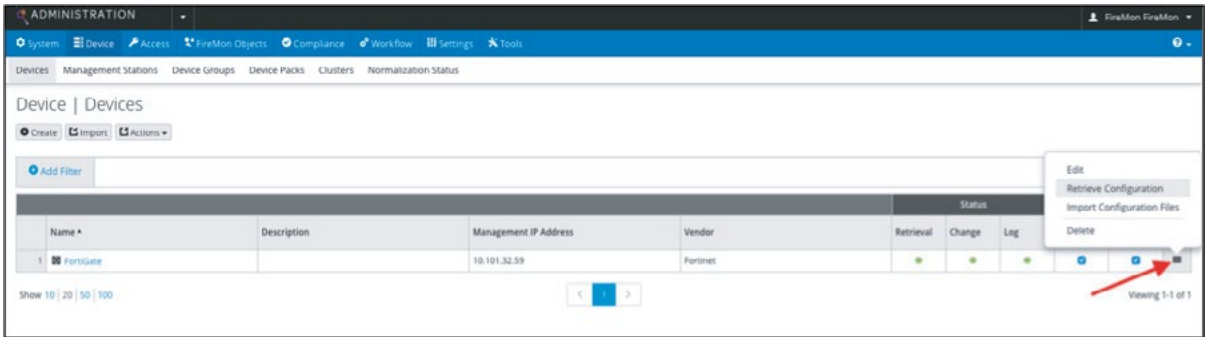
Note: If the primary Syslog is already configured, you can use the CLI to configure additional Syslog servers.

```
FortiGate-ESX2 # config log syslogd2 setting
FortiGate-ESX2 (setting) # set status enable
FortiGate-ESX2 (setting) # set server 1.2.3.4
FortiGate-ESX2 (setting) # end
FortiGate-ESX2 #
```

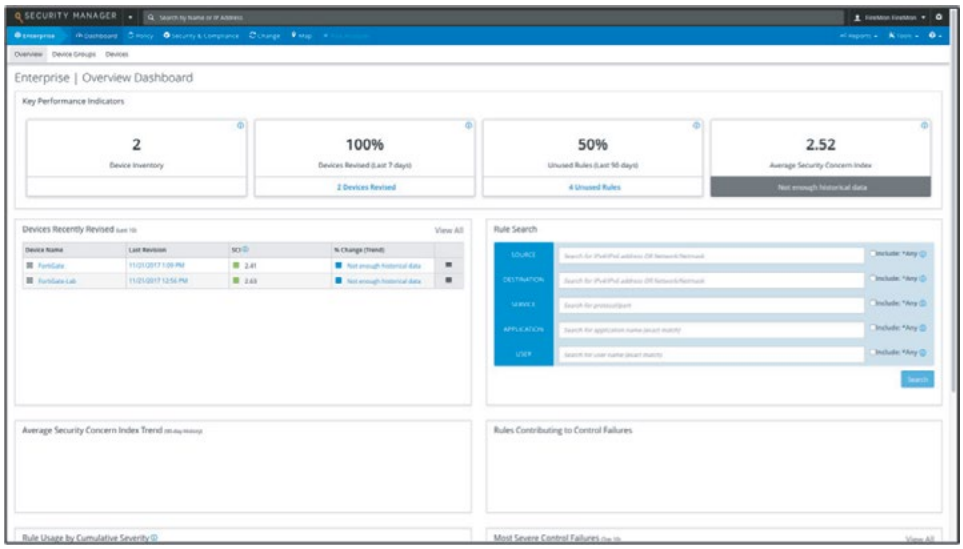
8. The configuration is now complete. Go back to the Devices screen in the FireMon interface. It should look like the image below once logs are received and the configuration has been retrieved.

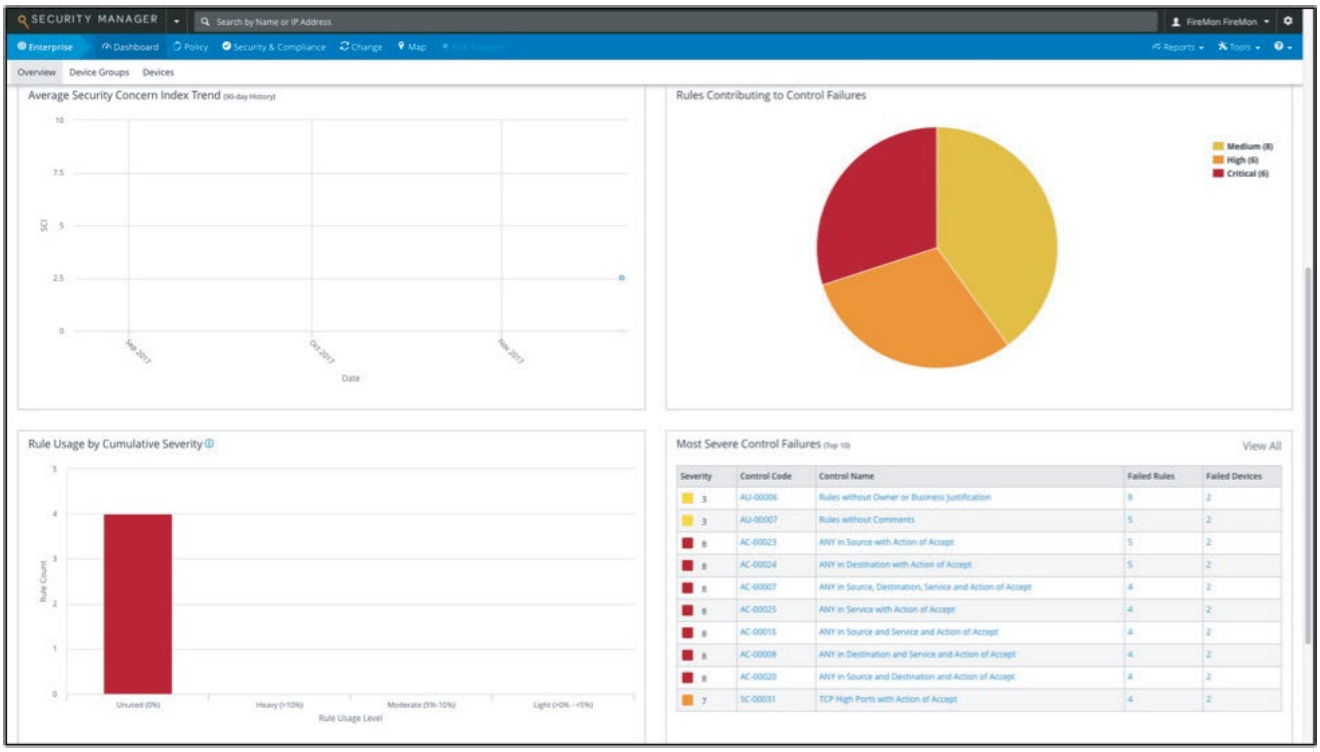


9. You can initiate a manual retrieval of the configuration by clicking the box on the far right.

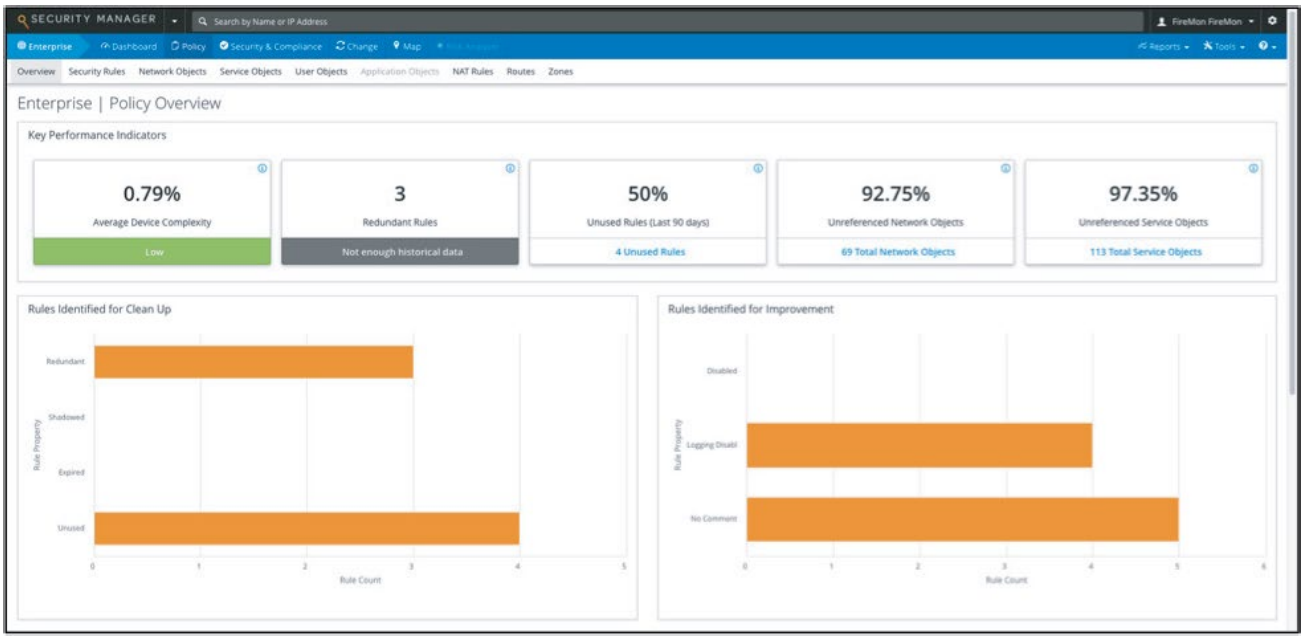


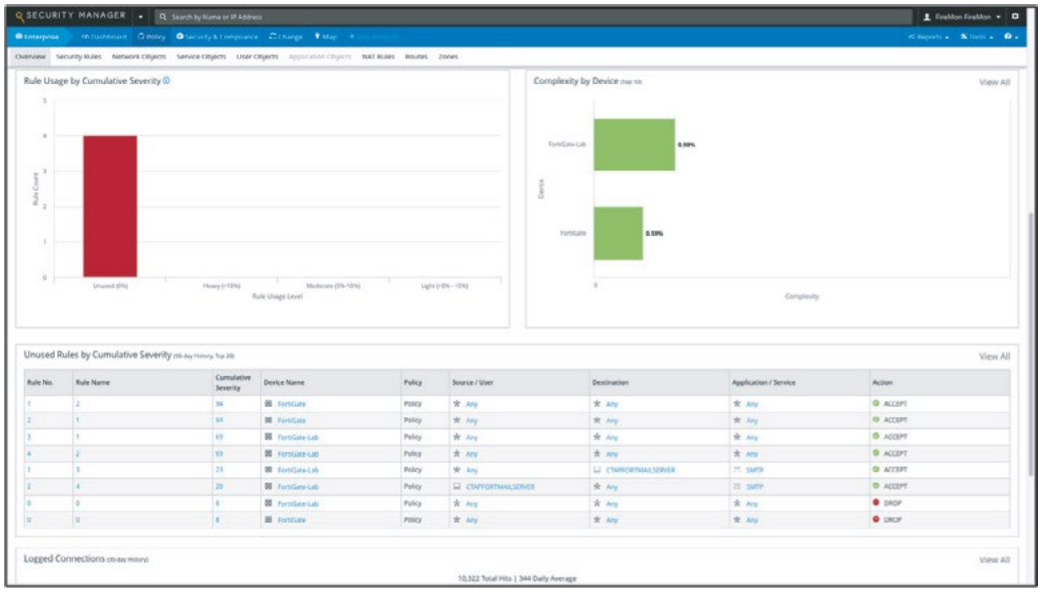
Security Manager Dashboard Views.



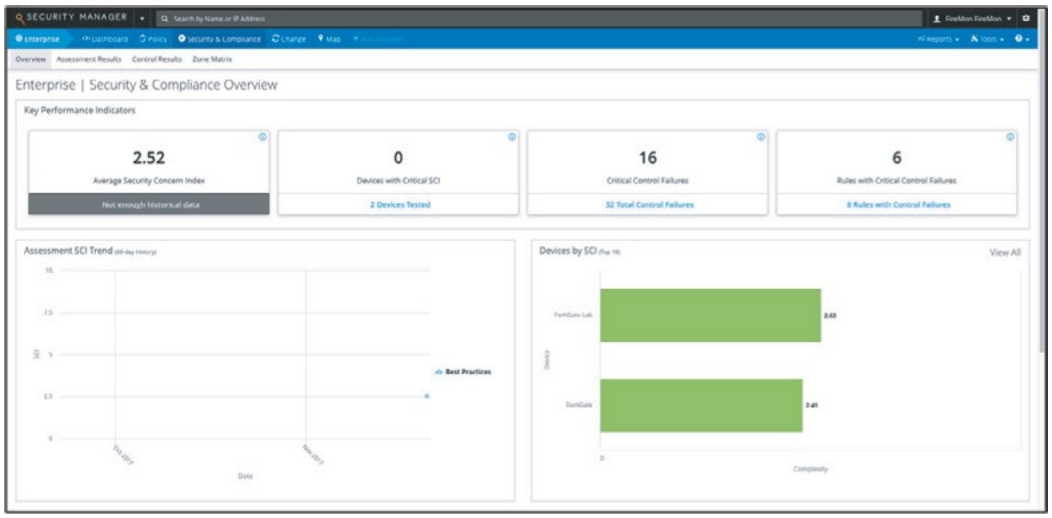


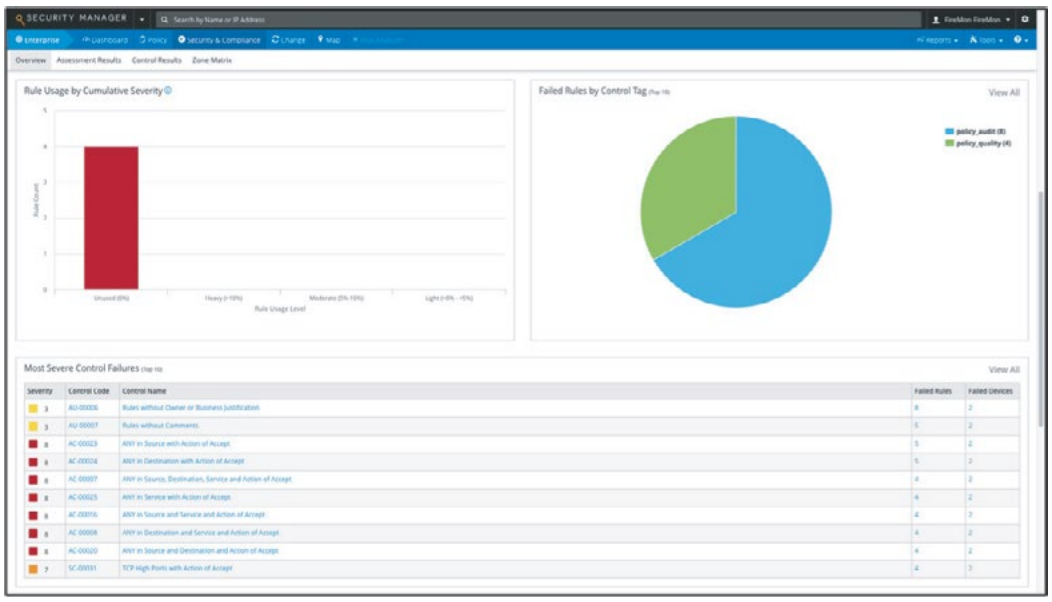
Security Manager Policy Views



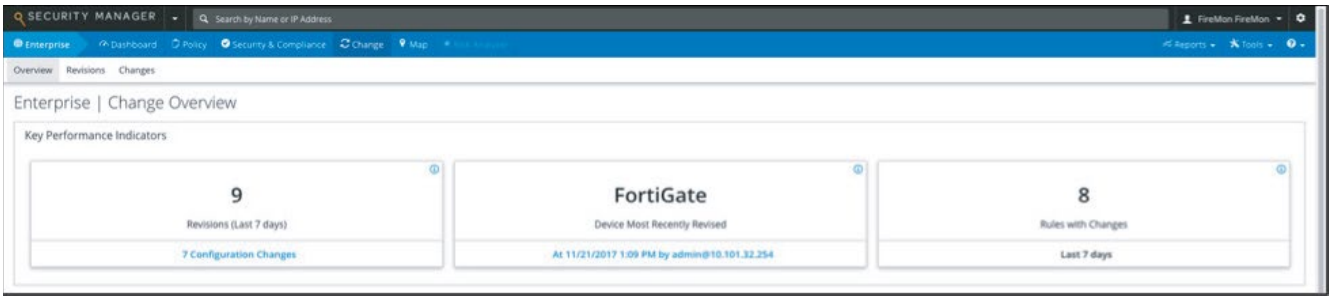


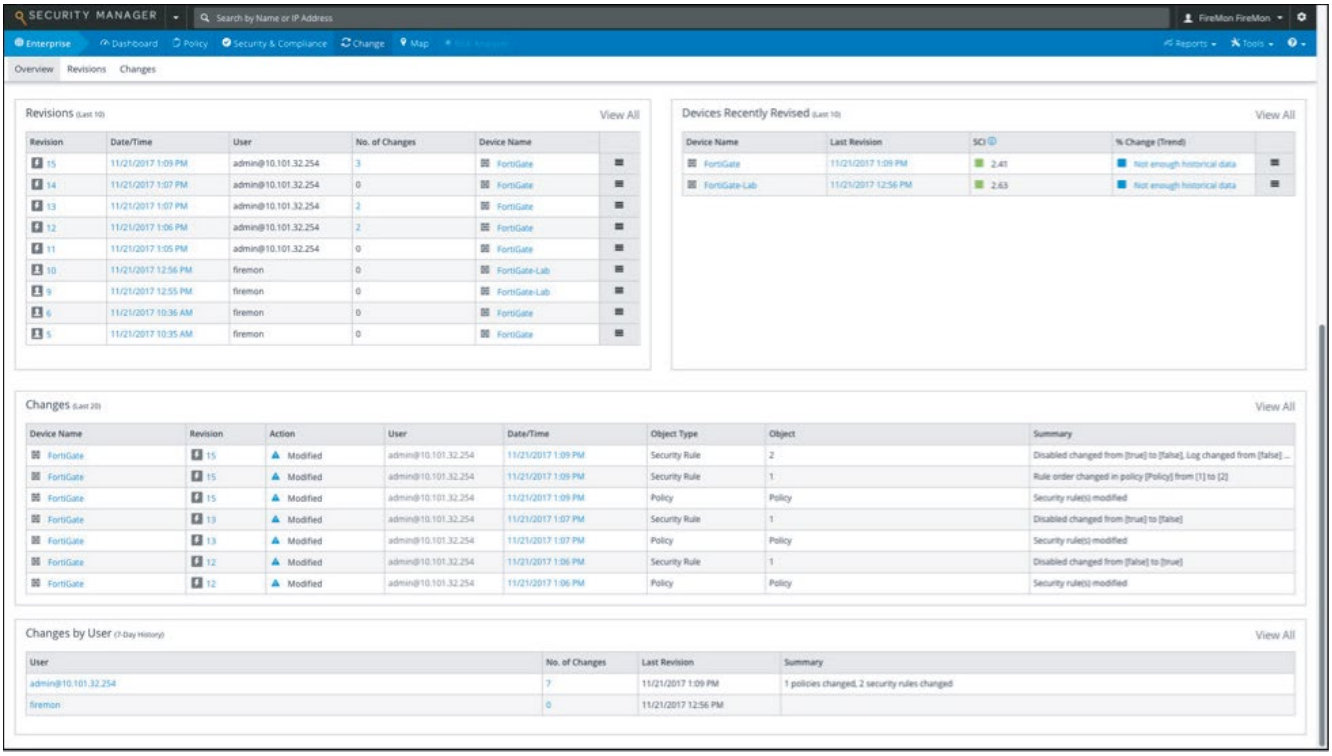
Security Manager Security & Compliance Views





Security Manager Security & Change Views





Summary

FireMon helps keep Fortinet firewalls running smoothly with a complete configuration management solution, including full support for the FortiGate line of network security platforms and appliances. FireMon monitors each appliance, capturing event and traffic logs in real time. All change events trigger a full configuration capture including detailed change history and a full audit trail of operations. Fortinet devices can be monitored directly or indirectly if another event collection system is in place.

Solution Guide: https://www.fortinet.com/content/dam/fortinet/assets/alliances/firemon-integration-brief-for-fortinet.pdf
FortiGate 5.6 Handbook: https://docs.fortinet.com/uploaded/files/3999/fortios-handbook-56.pdf

FORTINET

www.fortinet.com

October 7, 2021 3:55 PM
Macintosh HD:Users:austin:Dropbox (Red Rider):Clients:Fortinet:Solution Brief Updates:Working Group 5:DG-Fortinet-and-Firemon-102021:DG-Fortinet-and-Firemon-102021
91828-A-0-EN