INTEGRATION GUIDE

F5 BIG-IP AFM and FireMon integration guide

Use FireMon to manage all firewall policies in a central location

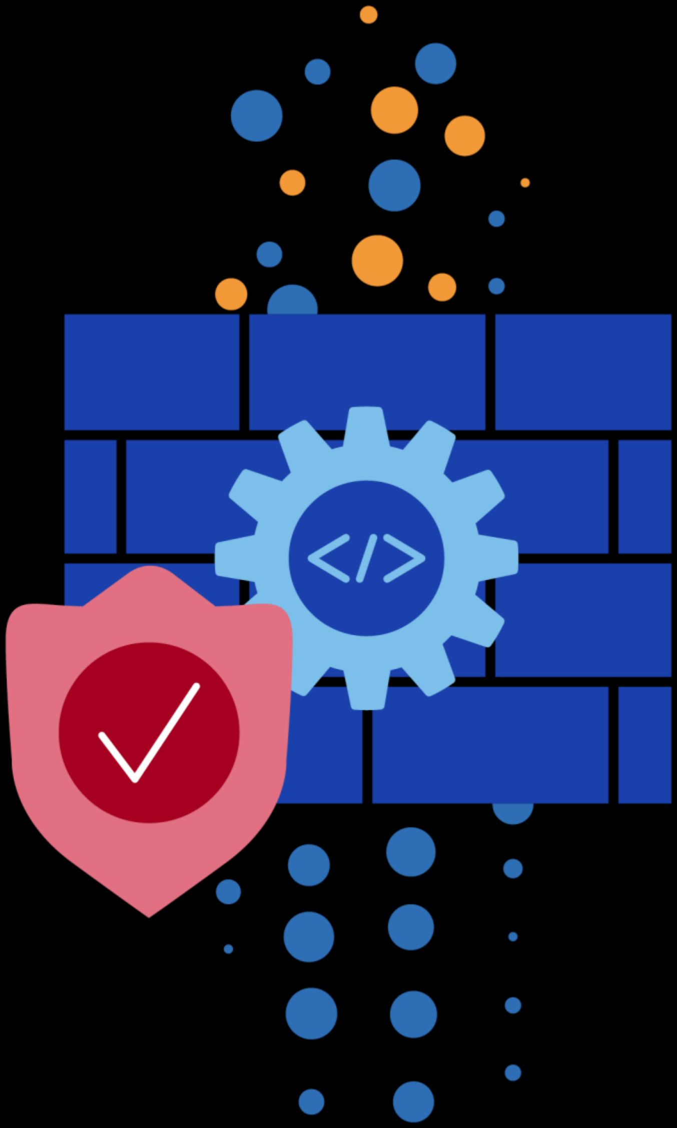


Table of Contents

Introduction

FireMon's Policy Manager is the industry's most trusted firewall policy automation platform enabling organizations to stay compliant, reduce risk, and accelerate secure access changes across all environments, from legacy data centers to multi-cloud deployments. Eliminate policy-related risk, accurately and quickly change rules, and meet internal and external compliance requirements.

F5 BIG-IP Advanced Firewall Manager (AFM) is a high-performance, full-proxy network security solution designed to protect networks and data centers against incoming threats that enter the network on the most widely deployed protocols. This product's unique application-centric design enables greater effectiveness in guarding against targeted network infrastructure-level attacks. Additionally, with BIG-IP AFM, organizations receive protection from more than 100 attack signatures—more hardware-based signatures than any other leading firewall vendor—along with unsurpassed programmability, interoperability, and visibility into threat conditions.

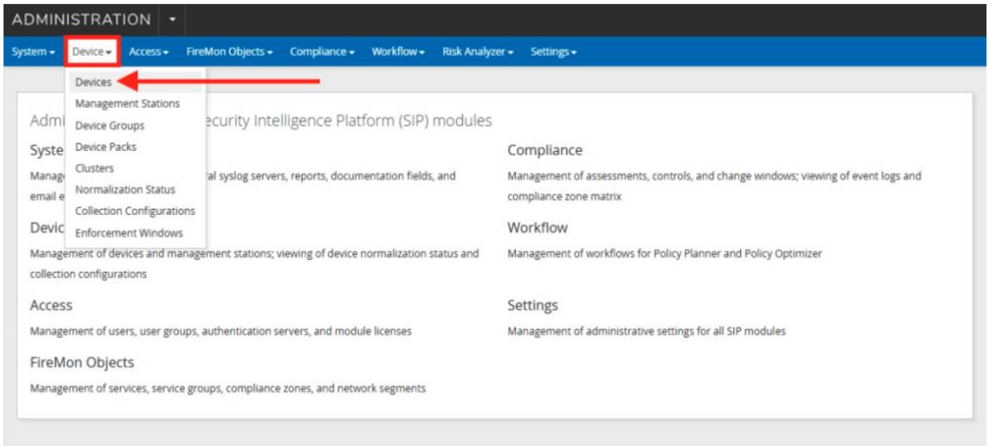
Deployment prerequisites

This guide was tested with the following software versions:

- F5 BIG-IP versions 15.1, 16.1, 17.5
- FireMon version FMOS 2025.2.1

FireMon configuration

From the FireMon Administrative view select Device > Devices



Admi ecurity Intelligence Platform (SIP) modules

Syste

Manag al syslog servers, reports, documentation fields, and email e

Devic

Management of devices and management stations; viewing of device normalization status and collection configurations

Access

Management of users, user groups, authentication servers, and module licenses

FireMon Objects

Management of services, service groups, compliance zones, and network segments

Compliance

Management of assessments, controls, and change windows; viewing of event logs and compliance zone matrix

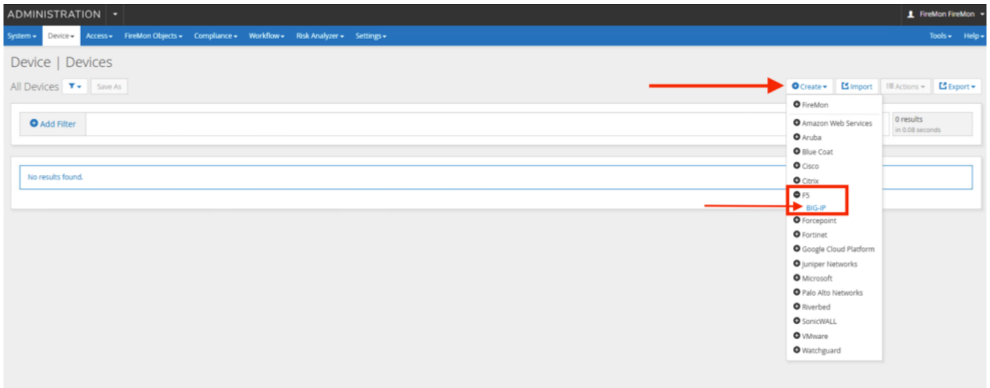
Workflow

Management of workflows for Policy Planner and Policy Optimizer

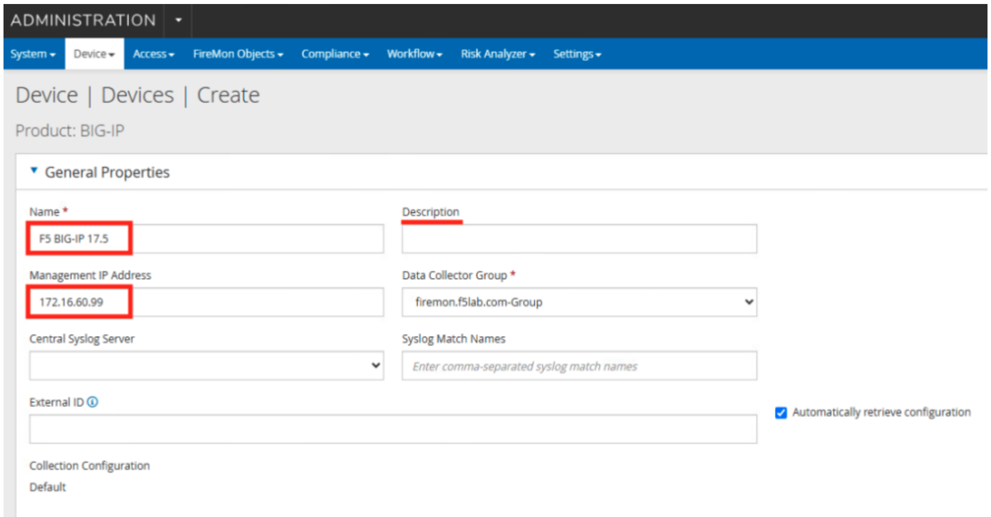
Settings

Management of administrative settings for all SIP modules

On the right click Create. Select F5 then BIG-IP.



Give it a Name and optionally a Description. Enter the Management IP Address.



Device | Devices | Create

Product: BIG-IP

General Properties

Name *: F5 BIG-IP 17.5

Description:

Management IP Address: 172.16.60.99

Data Collector Group *: firemon.f5lab.com-Group

Central Syslog Server:

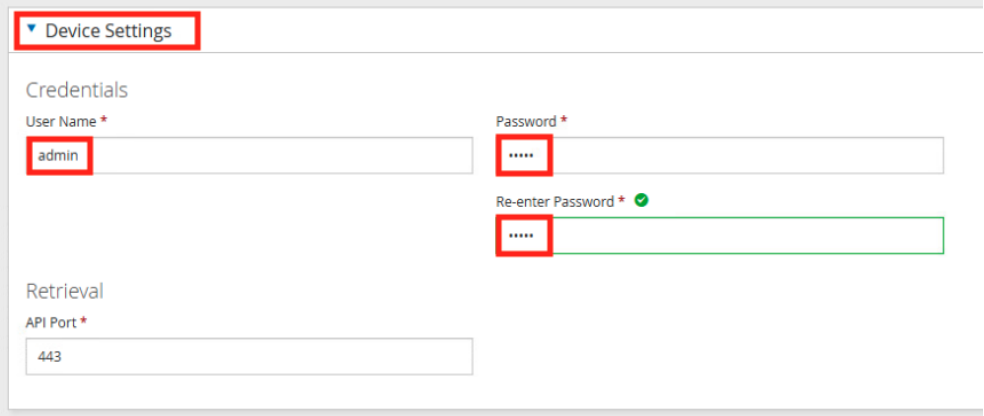
Syslog Match Names: *Enter comma-separated syslog match names*

External ID:

☑ Automatically retrieve configuration

Collection Configuration: Default

Under Device Settings enter a Username and Password that can be used to login to the BIG-IP.



Device Settings

Credentials

User Name *: admin

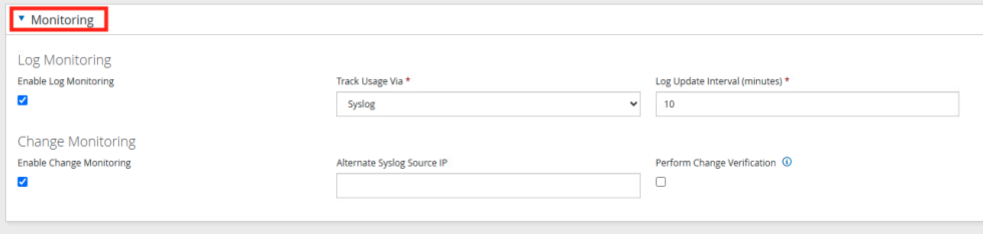
Password *: •••••

Re-enter Password *: •••••

Retrieval

API Port *: 443

Expand Monitoring to review the configuration. Make changes if needed.



Monitoring

Log Monitoring

Enable Log Monitoring: ☑

Track Usage Via *: Syslog

Log Update Interval (minutes) *: 10

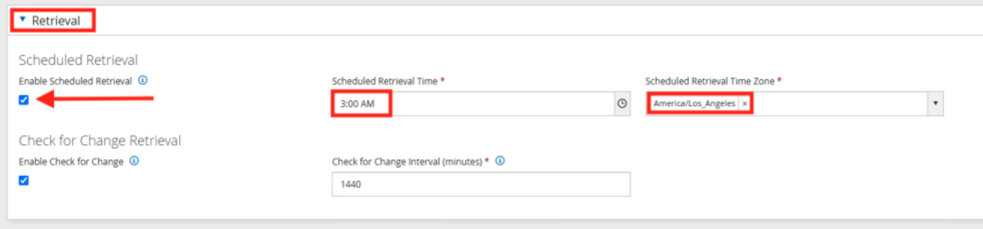
Change Monitoring

Enable Change Monitoring: ☑

Alternate Syslog Source IP:

Perform Change Verification: □

Expand Retrieval to review the configuration. As a best practice you should schedule automatic retrieval.



Scheduled Retrieval

Enable Scheduled Retrieval ⓘ ☑

Scheduled Retrieval Time * 3:00 AM

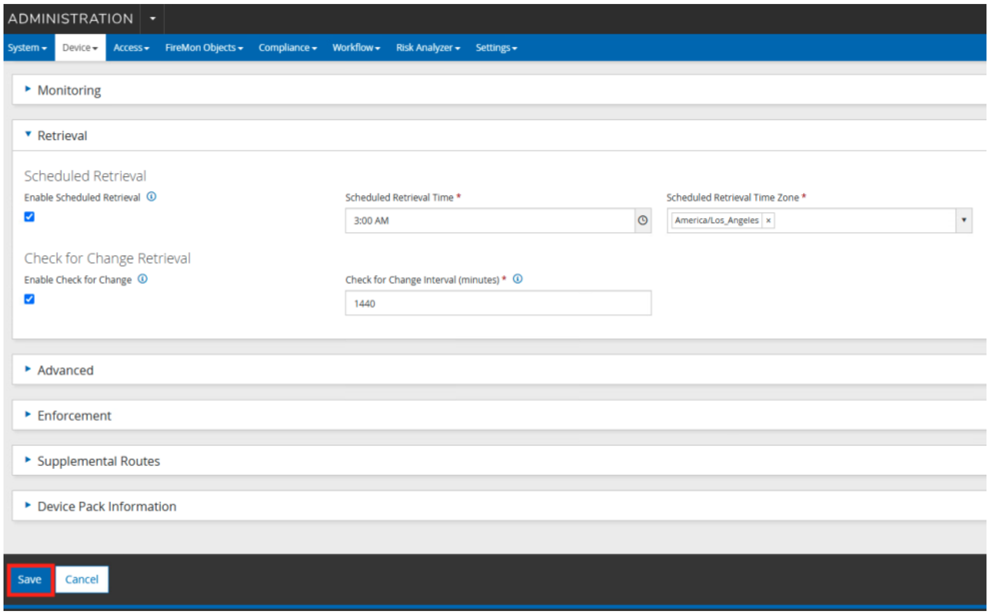
Scheduled Retrieval Time Zone * America/Los_Angeles ×

Check for Change Retrieval

Enable Check for Change ⓘ ☑

Check for Change Interval (minutes) * ⓘ 1440

Click Save when done



Scheduled Retrieval

Enable Scheduled Retrieval ⓘ ☑

Scheduled Retrieval Time * 3:00 AM

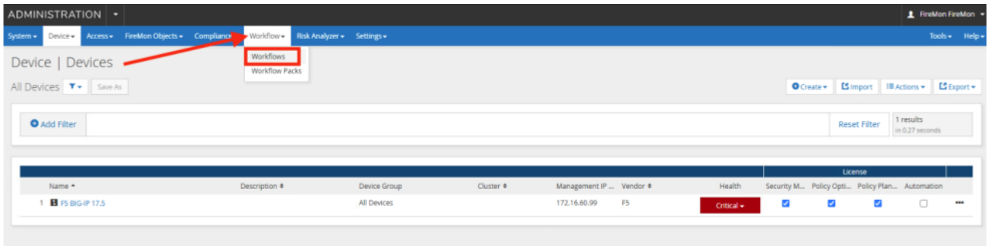
Scheduled Retrieval Time Zone * America/Los_Angeles ×

Check for Change Retrieval

Enable Check for Change ⓘ ☑

Check for Change Interval (minutes) * ⓘ 1440

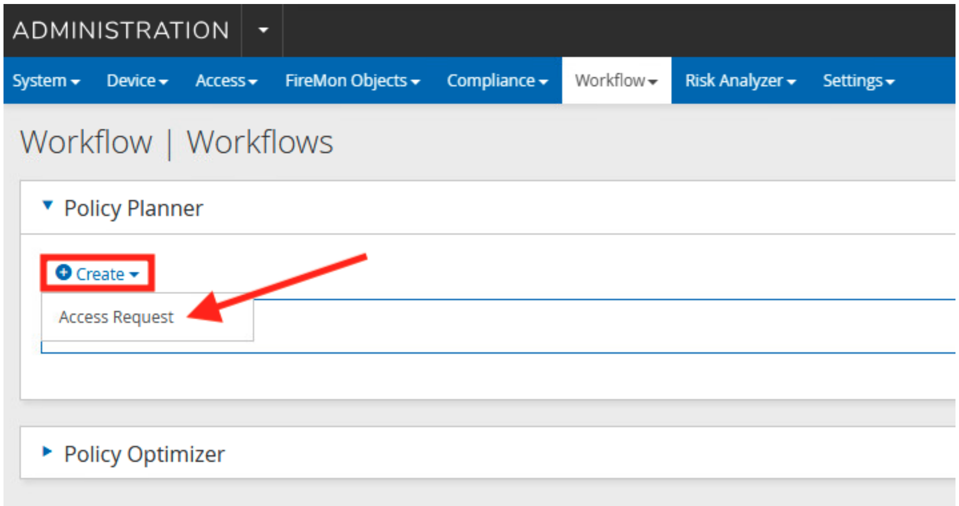
Then go to Workflow > Workflows.



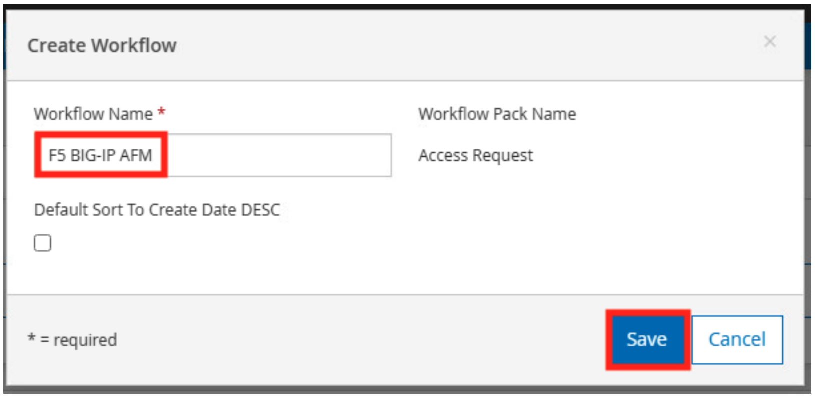
1 results
in 0.27 seconds

	Name	Description	Device Group	Cluster	Management IP ...	Vendor	Health	License Security M...	Policy Opti...	Policy Plan...	Automation	
1	F5 BIG-IP 17.5		All Devices		172.16.60.99	F5	Critical	☑	☑	☑	☐	•••

Under Policy Planner click Create > Access Request.



Give it a name and click Save.



Workflow Name *

F5 BIG-IP AFM

Workflow Pack Name

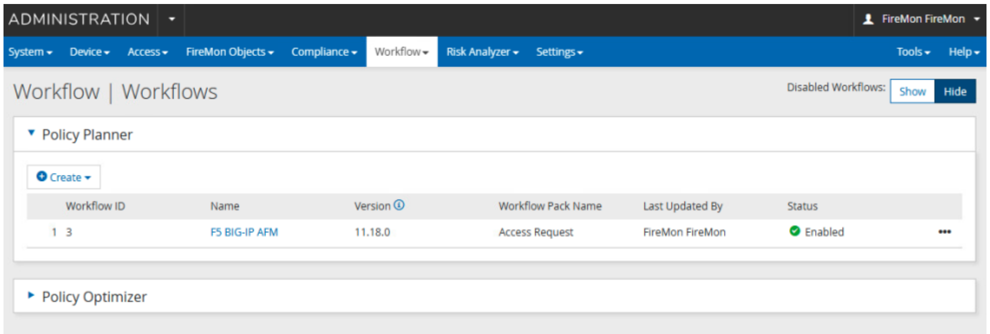
Access Request

Default Sort To Create Date DESC

□

* = required

The Workflow screen should look like the image below.

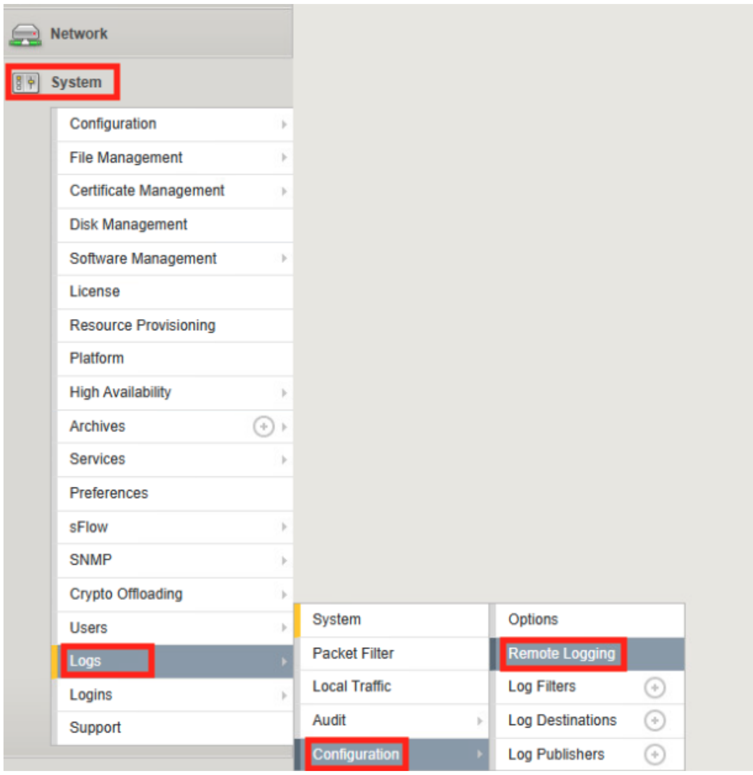


	Workflow ID	Name	Version	Workflow Pack Name	Last Updated By	Status
1	3	F5 BIG-IP AFM	11.18.0	Access Request	FireMon FireMon	✓ Enabled

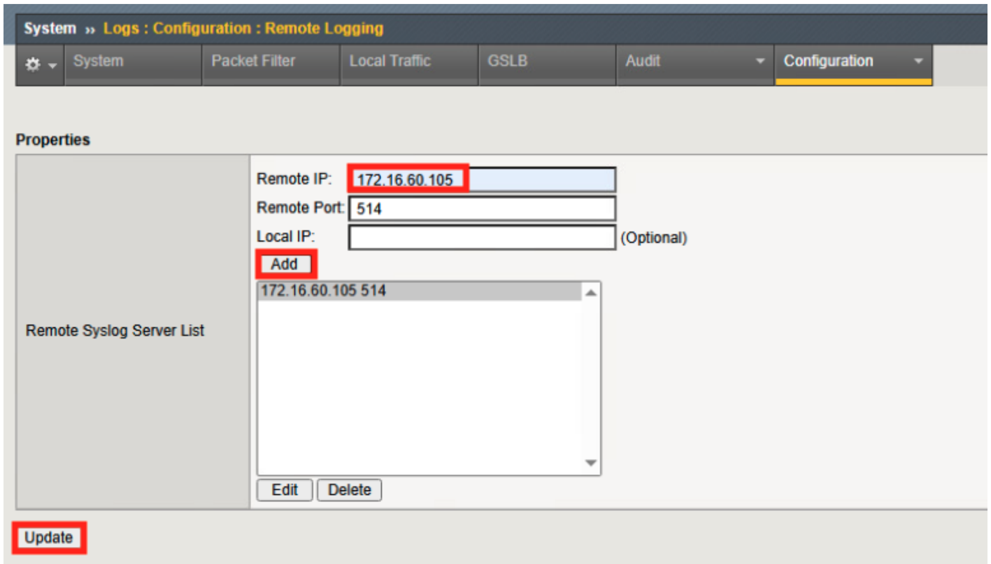
Do the same for the Policy Optimizer configuration.

F5 BIG-IP AFM configuration

In the BIG-IP UI navigate to System > Logs > Configuration > Remote Logging.



Enter the IP address of the FireMon then click Add. Click Update when done.



Properties

Remote Syslog Server List

Remote IP: 172.16.60.105

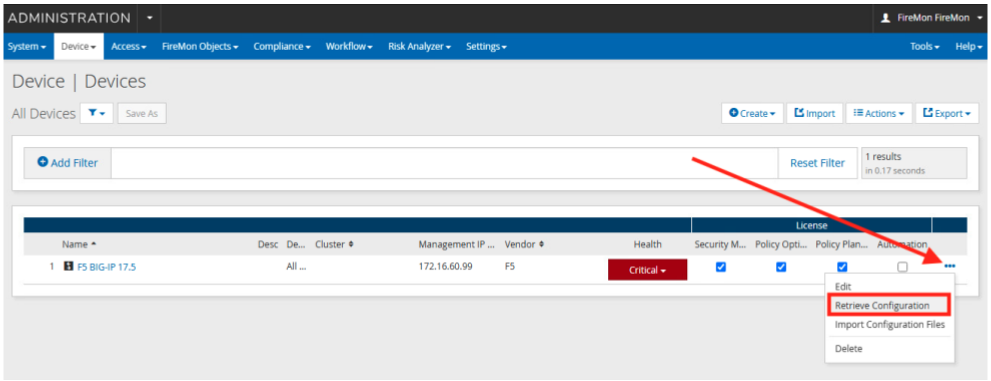
Remote Port: 514

Local IP: (Optional)

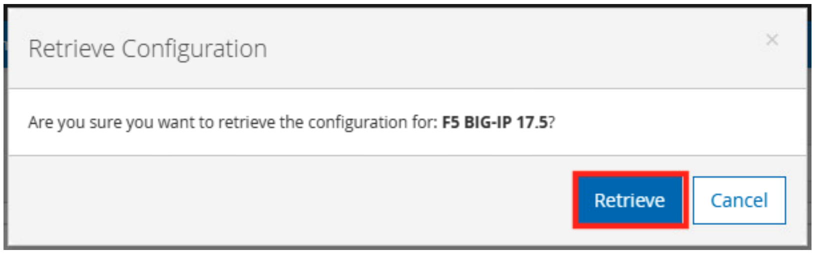
172.16.60.105 514

FireMon administration

Click the 3 dots on the far right and select Retrieve Configuration.



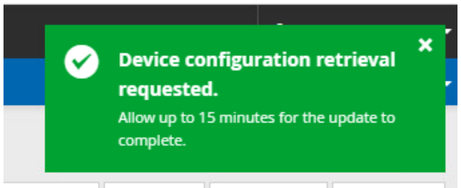
Click Retrieve



Retrieve Configuration

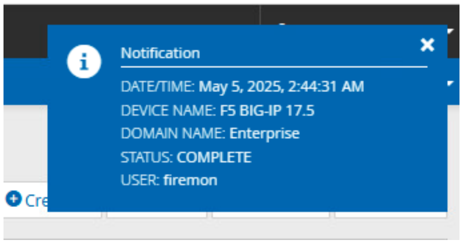
Are you sure you want to retrieve the configuration for: **F5 BIG-IP 17.5**?

You should see the following messages.



Device configuration retrieval requested.

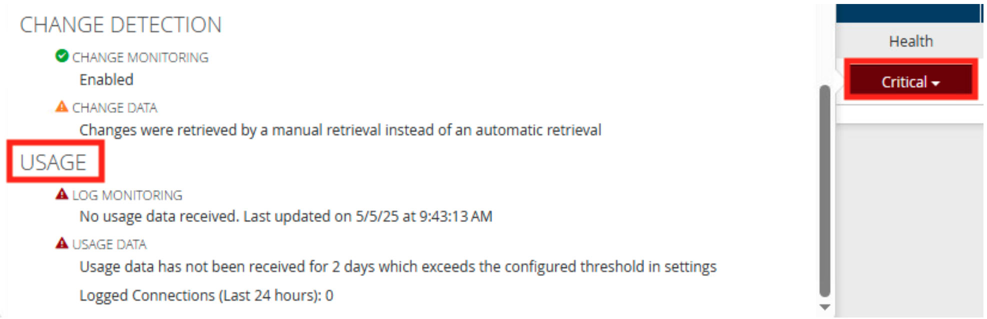
Allow up to 15 minutes for the update to complete.



Notification

DATE/TIME: May 5, 2025, 2:44:31 AM
DEVICE NAME: F5 BIG-IP 17.5
DOMAIN NAME: Enterprise
STATUS: COMPLETE
USER: firemon

Note the Health Status might be Critical



CHANGE DETECTION

CHANGE MONITORING
Enabled

CHANGE DATA
Changes were retrieved by a manual retrieval instead of an automatic retrieval

USAGE

LOG MONITORING
No usage data received. Last updated on 5/5/25 at 9:43:13 AM

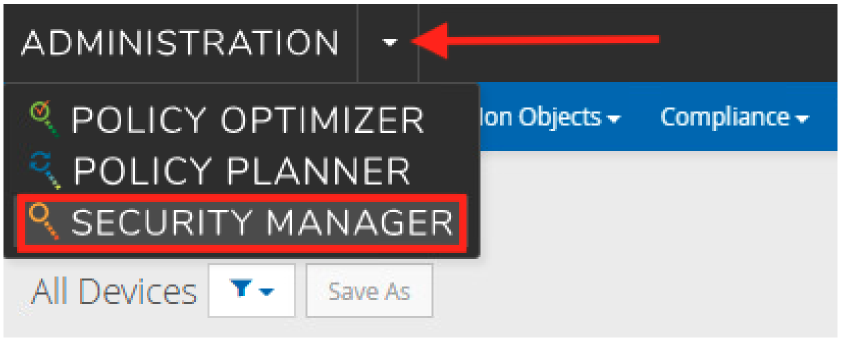
USAGE DATA
Usage data has not been received for 2 days which exceeds the configured threshold in settings

Logged Connections (Last 24 hours): 0

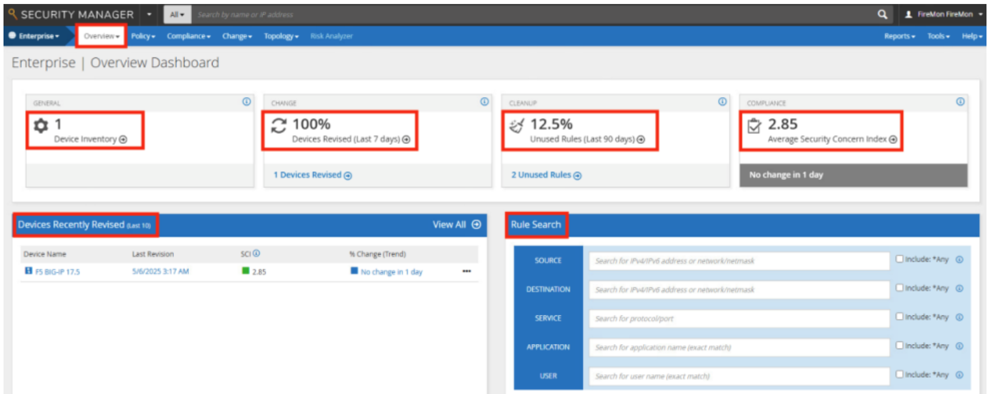
This is because no Usage Data has been received. The Health should go to Normal once Usage Data is received.

FireMon security manager

Access the FireMon Security Manager from the menu on the top left.



The main Dashboard gives an overview of your Device Inventory. It also has an intuitive Rule Search widget so you can easily find the rules you're looking for.



Enterprise | Overview Dashboard

GENERAL: 1 Device Inventory

CHANGE: 100% Devices Revised (Last 7 days) — 1 Devices Revised

CLEANUP: 12.5% Unused Rules (Last 90 days) — 2 Unused Rules

COMPLIANCE: 2.85 Average Security Concern Index — No change in 1 day

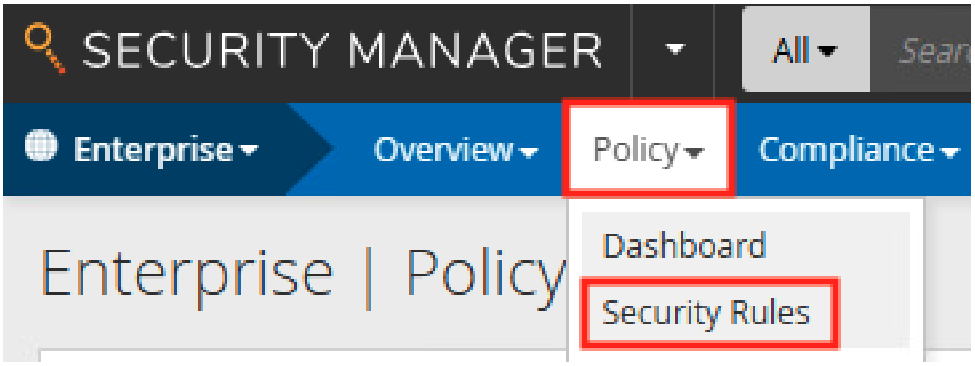
Devices Recently Revised (Last 10) View All

Device Name	Last Revision	SCI	% Change (Trend)
F5 BIG-IP 17.5	5/6/2025 3:17 AM	🟩 2.85	🟦 No change in 1 day

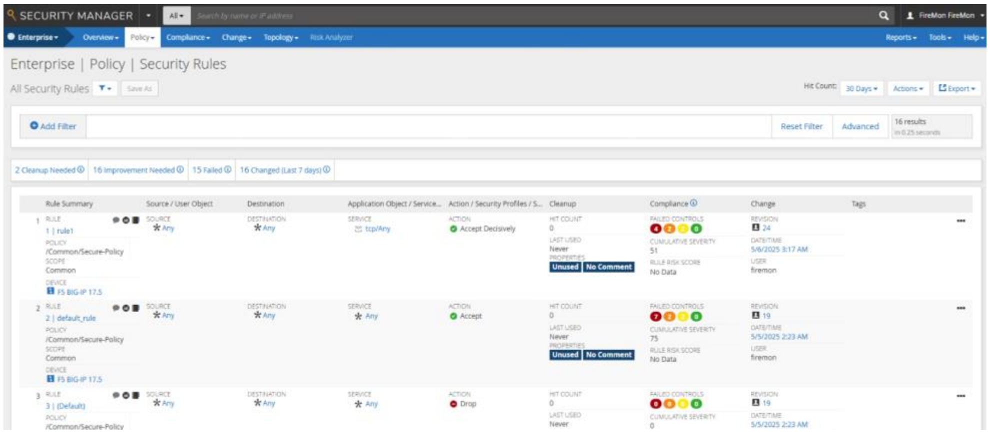
Rule Search

SOURCE	Search for IPv4/IPv6 address or network/netmask	□ Include: *Any
DESTINATION	Search for IPv4/IPv6 address or network/netmask	□ Include: *Any
SERVICE	Search for protocol/port	□ Include: *Any
APPLICATION	Search for application name (exact match)	□ Include: *Any
USER	Search for user name (exact match)	□ Include: *Any

Select Policy then Security Rules.



This gives you a detailed view of your F5 AFM Policy.



Enterprise | Policy | Security Rules

All Security Rules

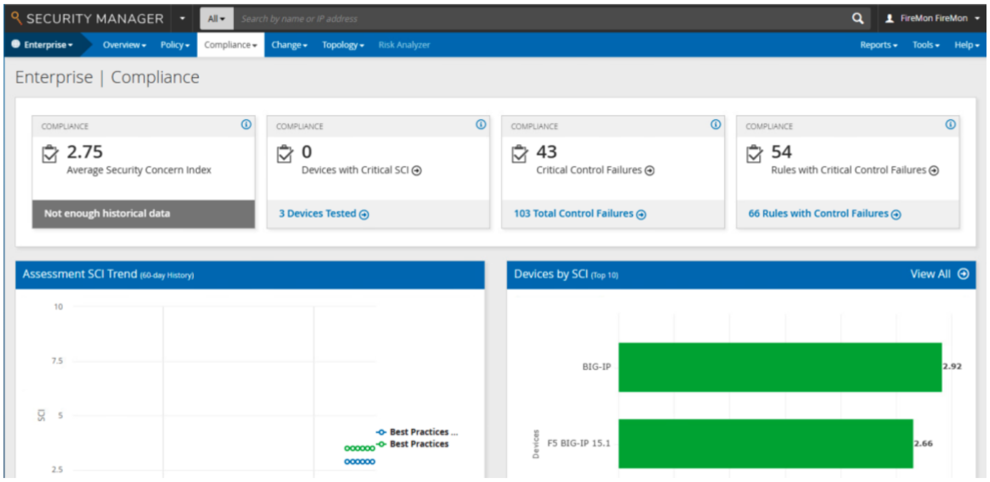
Hit Count: 30 Days

16 results in 0.25 seconds

2 Cleanup Needed | 16 Improvement Needed | 15 Failed | 16 Changed (Last 7 days)

	Rule Summary	Source / User Object	Destination	Application Object / Service...	Action / Security Profiles / S...	Cleanup	Compliance	Change	Tags
1	RULE 1 | rule1 POLICY /Common/Secure-Policy SCOPE Common DEVICE F5 BIG-IP 17.5	SOURCE Any	DESTINATION Any	SERVICE tcp/Any	ACTION Accept Decisively	HIT COUNT 0 LAST USED Never PROPERTIES Unused No Comment	FAILED CONTROLS 4 2 [illegible] 0 CUMULATIVE SEVERITY 51 RULE RISK SCORE No Data	REVISION 24 DATE/TIME 5/6/2025 3:17 AM USER firemon	
2	RULE 2 | default_rule POLICY /Common/Secure-Policy SCOPE Common DEVICE F5 BIG-IP 17.5	SOURCE Any	DESTINATION Any	SERVICE Any	ACTION Accept	HIT COUNT 0 LAST USED Never PROPERTIES Unused No Comment	FAILED CONTROLS 7 2 [illegible] 0 CUMULATIVE SEVERITY 75 RULE RISK SCORE No Data	REVISION 19 DATE/TIME 5/5/2025 2:23 AM USER firemon	
3	RULE 3 | (Default) POLICY /Common/Secure-Policy	SOURCE Any	DESTINATION Any	SERVICE Any	ACTION Drop	HIT COUNT 0 LAST USED Never	FAILED CONTROLS 0 0 0 0 CUMULATIVE SEVERITY 0	REVISION 19 DATE/TIME 5/5/2025 2:23 AM	

The Compliance Dashboard is useful for getting a quick snapshot of your overall Compliance



Enterprise | Compliance

COMPLIANCE
2.75
Average Security Concern Index
Not enough historical data

COMPLIANCE
0
Devices with Critical SCI
3 Devices Tested

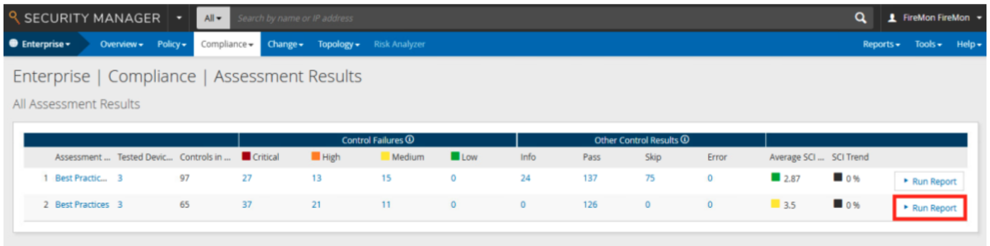
COMPLIANCE
43
Critical Control Failures
103 Total Control Failures

COMPLIANCE
54
Rules with Critical Control Failures
66 Rules with Control Failures

Assessment SCI Trend (60-day History)

Devices by SCI (Top 10)

Assessment Results will show any previous results. Click Run Report to run the Assessment again.

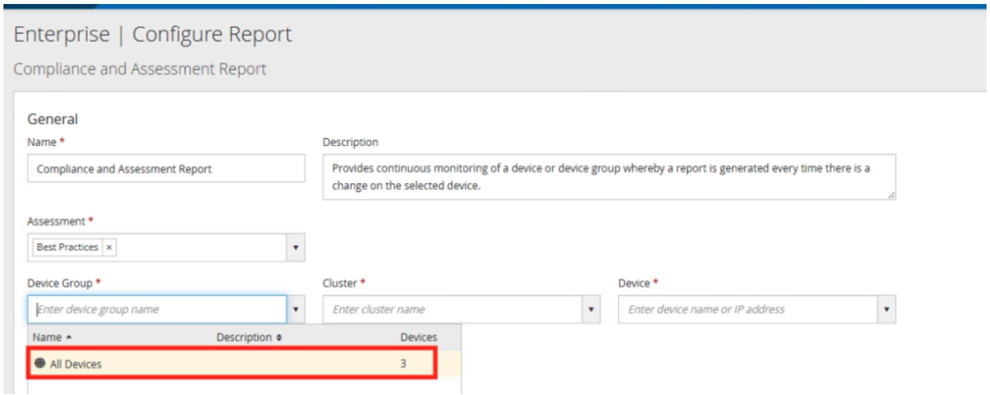


Enterprise | Compliance | Assessment Results

All Assessment Results

				Control Failures				Other Control Results						
	Assessment ...	Tested Devic...	Controls in ...	🟥 Critical	🟧 High	🟨 Medium	🟩 Low	Info	Pass	Skip	Error	Average SCI ...	SCI Trend	
1	Best Practic...	3	97	27	13	15	0	24	137	75	0	🟩 2.87	⬛ 0 %	▸ Run Report
2	Best Practices	3	65	37	21	11	0	0	126	0	0	🟨 3.5	⬛ 0 %	▸ Run Report

Select the Devices you want to run the assessment against.



Enterprise | Configure Report

Compliance and Assessment Report

General

Name *: Compliance and Assessment Report

Description: Provides continuous monitoring of a device or device group whereby a report is generated every time there is a change on the selected device.

Assessment *: Best Practices ×

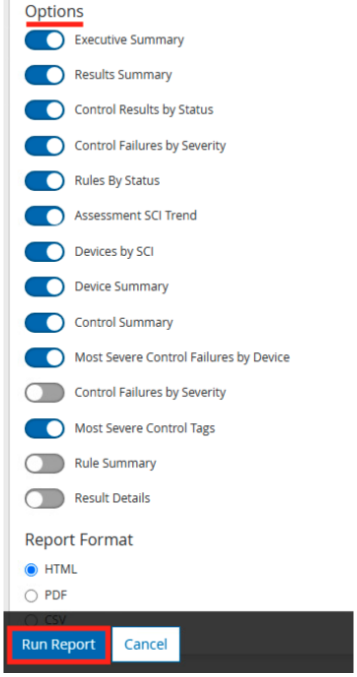
Device Group *: Enter device group name

Cluster *: Enter cluster name

Device *: Enter device name or IP address

Name ▲	Description ⬍	Devices
● All Devices		3

Enable any additional Options then click Run Report.



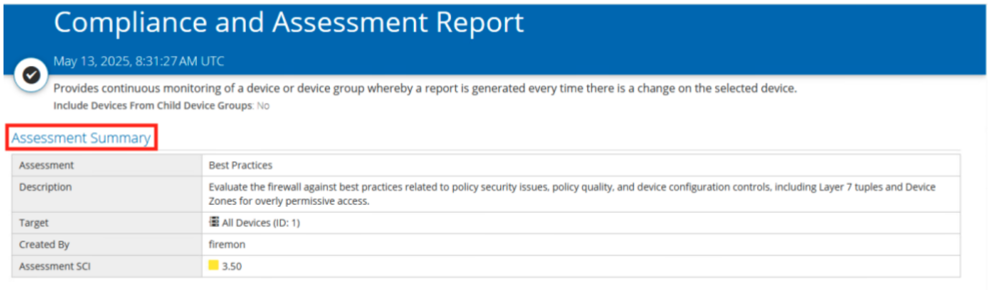
Options

- ☑ Executive Summary
- ☑ Results Summary
- ☑ Control Results by Status
- ☑ Control Failures by Severity
- ☑ Rules By Status
- ☑ Assessment SCI Trend
- ☑ Devices by SCI
- ☑ Device Summary
- ☑ Control Summary
- ☑ Most Severe Control Failures by Device
- ☐ Control Failures by Severity
- ☑ Most Severe Control Tags
- ☐ Rule Summary
- ☐ Result Details

Report Format

- ● HTML
- ○ PDF
- ○ CSV

The Assessment Summary



Compliance and Assessment Report

May 13, 2025, 8:31:27 AM UTC

Provides continuous monitoring of a device or device group whereby a report is generated every time there is a change on the selected device.

Include Devices From Child Device Groups: No

Assessment Summary

Assessment	Best Practices
Description	Evaluate the firewall against best practices related to policy security issues, policy quality, and device configuration controls, including Layer 7 tuples and Device Zones for overly permissive access.
Target	All Devices (ID: 1)
Created By	firemon
Assessment SCI	🟨 3.50

The Executive Summary

Conclusion

FireMon helps keep F5 firewalls running smoothly with a complete configuration management solution, including full support for the BIG-IP AFM 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. F5 AFM devices can be monitored directly or indirectly if another event collection system is in place.

Related Content

F5 Blog: Boost Efficiency and Security with F5 BIG-IP Advanced Firewall Manager

F5 Webpage: BIG-IP Advanced Firewall Manager