DEPLOYMENT GUIDE

Fortinet and AlgoSec Security Management Suite

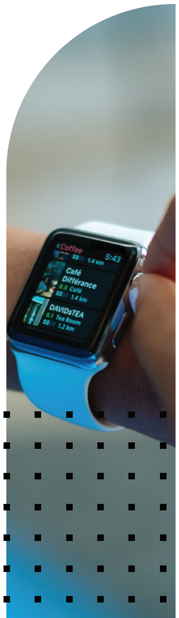


Table of Contents

Overview

Fortinet (NASDAQ: FTNT) is a global provider of highperformance network security and specialized security solutions that provide our customers with the power to protect and control their IT infrastructure. Our purpose-built, integrated security technologies, combined with our FortiGuard security intelligence services, provide the high performance and complete content protection our customers need to stay abreast of a constantly evolving threat landscape.

The Fortinet Security Fabric brings together all components in your network. It is Broad, Powerful and Automated. In addition to Fortinet products, the Security Fabric also integrates with 3rd Party partners to extend the power of the Security Fabric to other parts of an organization. For more information regarding our Security Fabric Partners, please refer to our Technology Alliances here: https://www.fortinet.com/partners/partnerships/alliancepartners.html

The leading provider of business-driven security management solutions, AlgoSec helps the world's largest organizations align security with their business processes. With the AlgoSec Security Management Suite, users can discover, map and migrate business application connectivity, proactively analyze risk from the business perspective, tie cyber-attacks to business processes and intelligently automate network security changes with zero touch – across their cloud, SDN and on-premise networks. Over 1,500 enterprises, including 20 of the Fortune 50, utilize AlgoSec's solutions to make their organizations more agile, more secure and more compliant – all the time. Since its inception, AlgoSec has offered the industry's only money-back guarantee.

Deployment Prerequisites

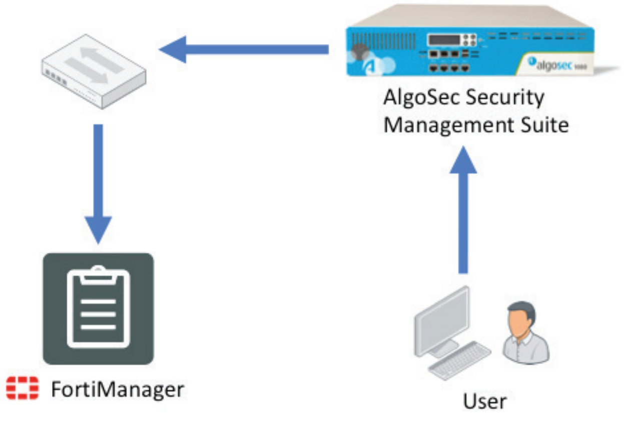
- Fortinet FortiManager version 5.4.3 or newer
- AlgoSec Security Management Suite (AlgoSec), including AlgoSec Firewall Analyzer, FireFlow and BusinessFlow version 6.11, already configured

Note: AlgoSec also supports Fortinet FortiGate but it is not covered in this guide. For details on how to configure AlgoSec and FortiGate refer to the AlgoSec Firewall Analyzer Administration Guide.

Today's business environment is characterized by continual changes, and business needs rapidly evolve across various organizational functions of companies. In this dynamic and rapidly changing business environment, IT often struggles to gain adequate visibility and control, to ensure security policies and regulatory guidelines are complied with. Effective security policy management that accommodates the dynamic nature of today's organizations is a key challenge for many IT departments.

Fortinet and AlgoSec have partnered to deliver an industry-leading security solution to address these needs. Bringing together AlgoSec's business-driven security policy automation with Fortinet's industry-leading FortiGate® network security firewall platform enables customers to benefit from AlgoSec's comprehensive security policy management capabilities, while simultaneously leveraging the best-validated security protection in the industry provided by Fortinet.

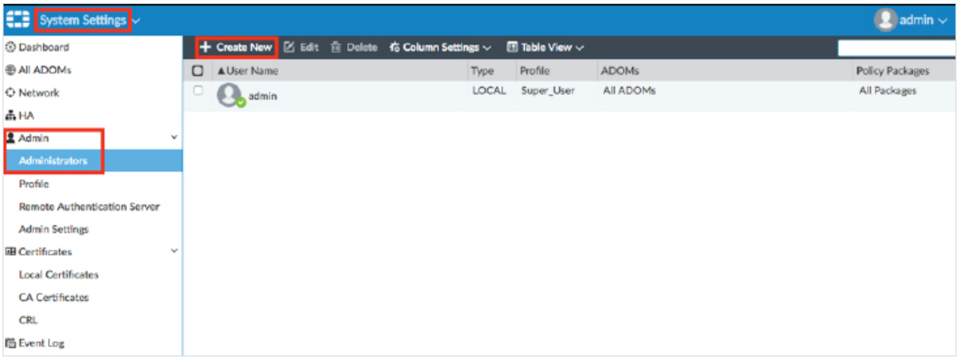
Architecture Overview



FortiManager Configuration

Create and configure an administrator account for AlgoSec.

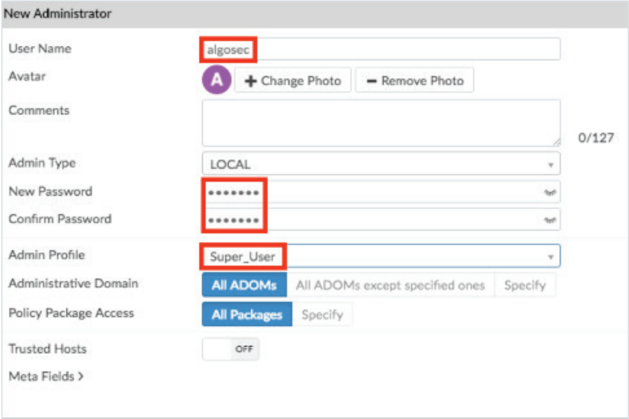
From System Settings go to Admin > Administrators > Create New.



□	User Name	Type	Profile	ADOMs	Policy Packages
□	admin	LOCAL	Super_User	All ADOMs	All Packages

Enter a User Name, New Password and Confirm the Password.

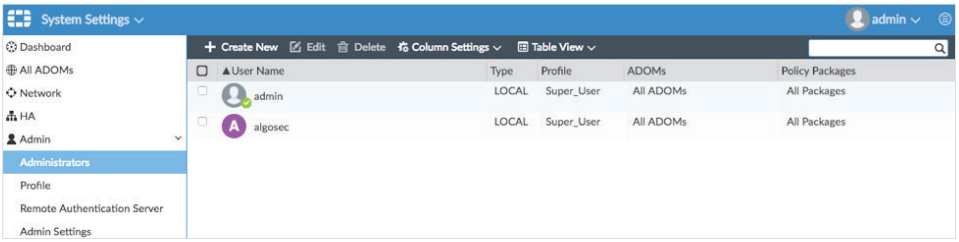
Set the Admin Profile to Super_User and click OK at the bottom.



New Administrator

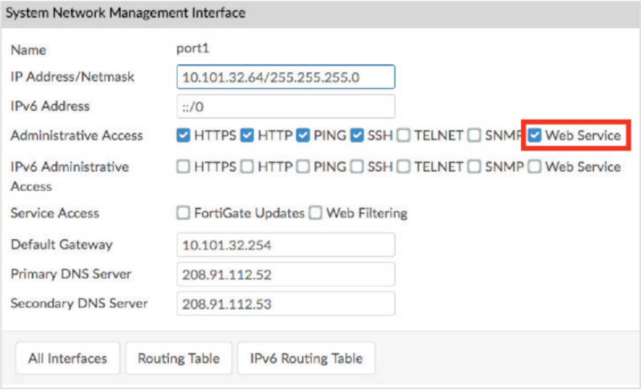
User Name	algosec
Avatar	A
Comments	0/127
Admin Type	LOCAL
New Password	•••••••
Confirm Password	•••••••
Admin Profile	Super_User
Administrative Domain	All ADOMs
Policy Package Access	All Packages
Trusted Hosts	OFF

The screen should look like the image below.



□	User Name	Type	Profile	ADOMs	Policy Packages
□	admin	LOCAL	Super_User	All ADOMs	All Packages
□	algosec	LOCAL	Super_User	All ADOMs	All Packages

Enable the Web Service from the Network settings.



System Network Management Interface

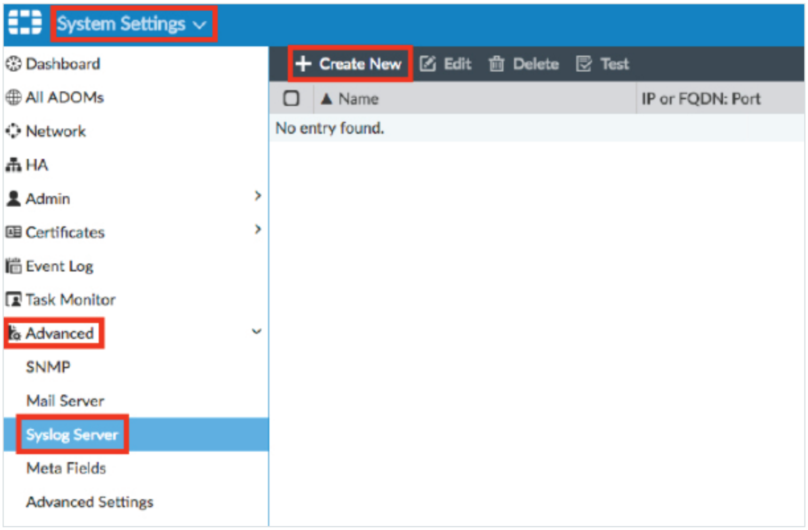
Name	port1
IP Address/Netmask	10.101.32.64/255.255.255.0
IPv6 Address	::/0
Administrative Access	☑ HTTPS ☑ HTTP ☑ PING ☑ SSH □ TELNET □ SNMP ☑ Web Service
IPv6 Administrative Access	□ HTTPS □ HTTP □ PING □ SSH □ TELNET □ SNMP □ Web Service
Service Access	□ FortiGate Updates □ Web Filtering
Default Gateway	10.101.32.254
Primary DNS Server	208.91.112.52
Secondary DNS Server	208.91.112.53

Remote Procedure Call (RPC) needs to be set to read-write when using FortiManager version 5.2.3 and above (see link to the Technical Note at the end for more details).

Connect to the FortiManager CLI to change the AlgoSec administrator account permissions.
Enter the following CLI commands:

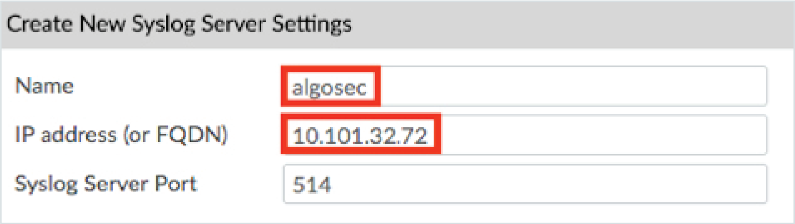
```
FMG-VM64 # config system admin user

(user)# edit algosec

(algosec)# set rpc-permit read-write

(algosec)# end
```

Configure FortiManager to send Syslog to the AlgoSec IP address.
From System Settings go to Advanced > Syslog Server and click Create New.



No entry found.

Enter a Name.
Enter the IP Address or FQDN of the AlgoSec server.
Click OK.



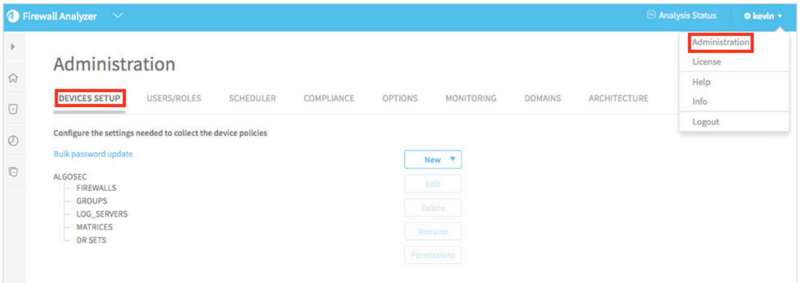
Create New Syslog Server Settings

Name	algosec
IP address (or FQDN)	10.101.32.72
Syslog Server Port	514

AlgoSec Security Management Suite Configuration

Configure AlgoSec to monitor FortiManager.

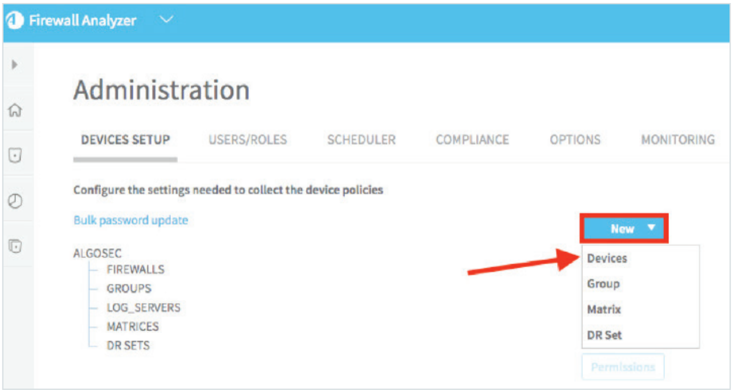
Go to Administration > Devices Setup.



Administration

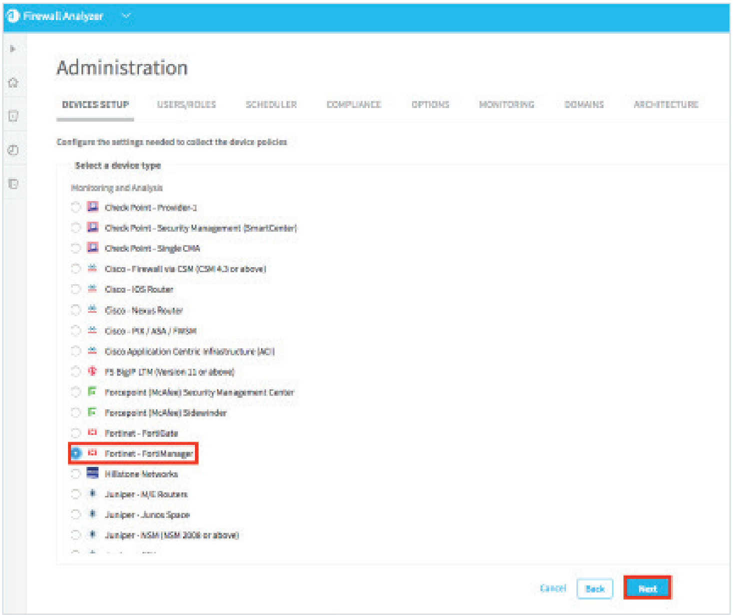
Configure the settings needed to collect the device policies

Click New and select Devices.



Configure the settings needed to collect the device policies

For Device Type select Fortinet FortiManager and click Next.



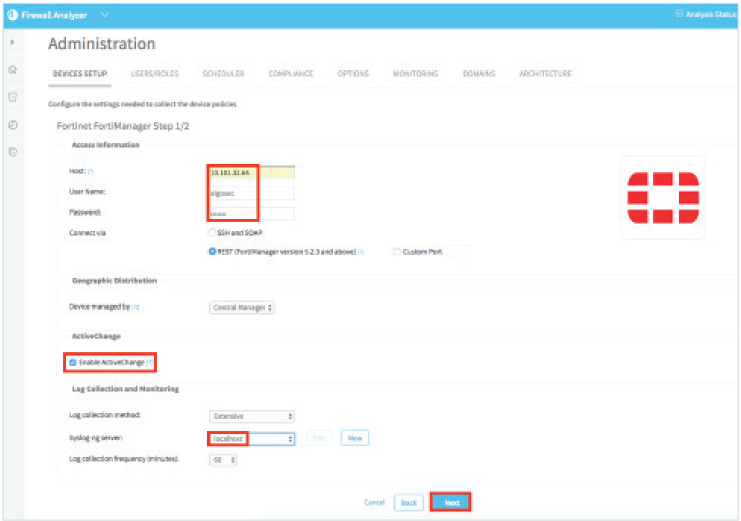
Configure the settings needed to collect the device policies

Select a device type

Monitoring and Analysis

- ○ Check Point - Provider-1
- ○ Check Point - Security Management (SmartCenter)
- ○ Check Point - Single CMA
- ○ Cisco - Firewall via CSM (CSM 4.3 or above)
- ○ Cisco - IOS Router
- ○ Cisco - Nexus Router
- ○ Cisco - PIX / ASA / FWSM
- ○ Cisco Application Centric Infrastructure (ACI)
- ○ F5 BigIP LTM (Version 11 or above)
- ○ Forcepoint (McAfee) Security Management Center
- ○ Forcepoint (McAfee) Sidewinder
- ○ Fortinet - FortiGate
- ● Fortinet - FortiManager
- ○ Hillstone Networks
- ○ Juniper - M/E Routers
- ○ Juniper - Junos Space
- ○ Juniper - NSM (NSM 2008 or above)

For Access Information enter the FortiManager IP address, User Name and Password.
Enable Active Change.
Set the Syslog-ng server to Localhost and click Next.



Configure the settings needed to collect the device policies

Fortinet FortiManager Step 1/2

Access Information

Host: 10.101.32.66

User Name: algosec

Password: •••••

Connect via: ○ SSH and SOAP ● REST (FortiManager version 5.2.3 and above) ○ Custom Port

Geographic Distribution

Device managed by: Central Manager

ActiveChange

☑ Enable ActiveChange

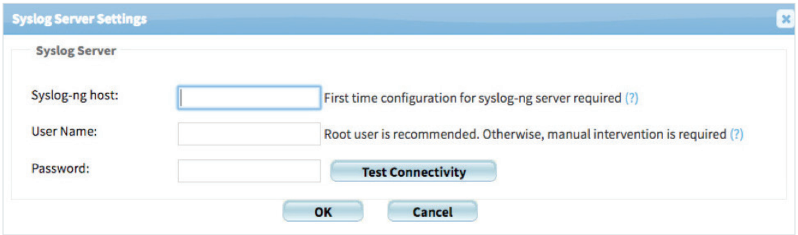
Log Collection and Monitoring

Log collection method: Extensive

Syslog-ng server: localhost

Log collection frequency (minutes): 60

Note: if you wish to use your own Syslog server click New and configure the following.



Syslog Server Settings

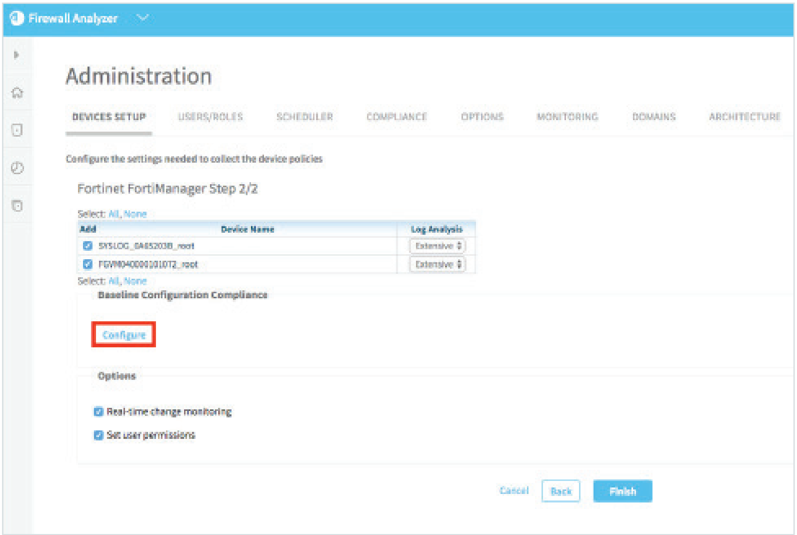
Syslog Server

Syslog-ng host: First time configuration for syslog-ng server required (?)

User Name: Root user is recommended. Otherwise, manual intervention is required (?)

Password:

Under Baseline Configuration Compliance click Configure.



Administration

Configure the settings needed to collect the device policies

Fortinet FortiManager Step 2/2

Select: All, None

Add	Device Name	Log Analysis
☑	SYSLOG_0A65203B_root	Extensive
☑	FGVM040000101072_root	Extensive

Select: All, None

Baseline Configuration Compliance

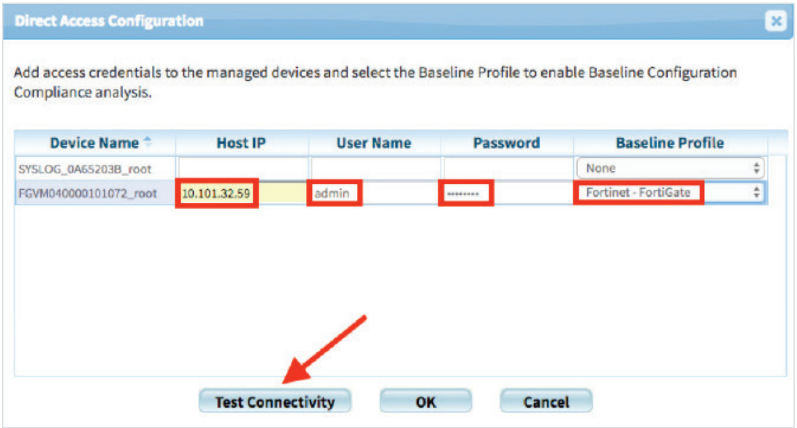
Configure

Options

☑ Real-time change monitoring

☑ Set user permissions

Enter the Host IP, User Name and Password. For Baseline Profile select Fortinet – FortiGate.
Click Test Connectivity.

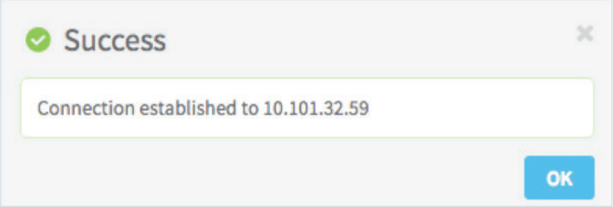


Direct Access Configuration

Add access credentials to the managed devices and select the Baseline Profile to enable Baseline Configuration Compliance analysis.

Device Name	Host IP	User Name	Password	Baseline Profile
SYSLOG_0A65203B_root				None
FGVM040000101072_root	10.101.32.59	admin	••••••••	Fortinet - FortiGate

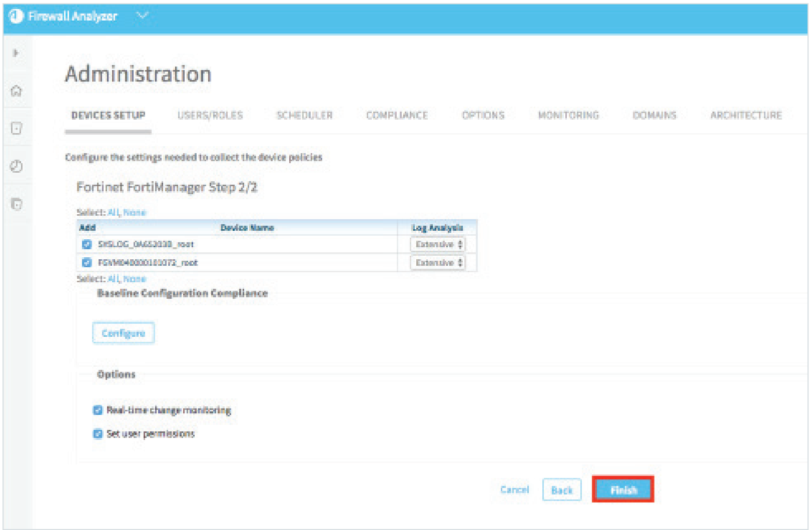
Enter the Host IP, User Name and Password. For Baseline Profile select Fortinet – FortiGate.
Click Test Connectivity.



Success

Connection established to 10.101.32.59

Click OK and OK.
Your screen should look similar to the following.
Click Finish.



Configure the settings needed to collect the device policies

Fortinet FortiManager Step 2/2

Select: All, None

Add	Device Name	Log Analysis
☑	SYSLOG_0A65203B_root	Extensive
☑	FGVM040000101072_root	Extensive

Select: All, None

Baseline Configuration Compliance

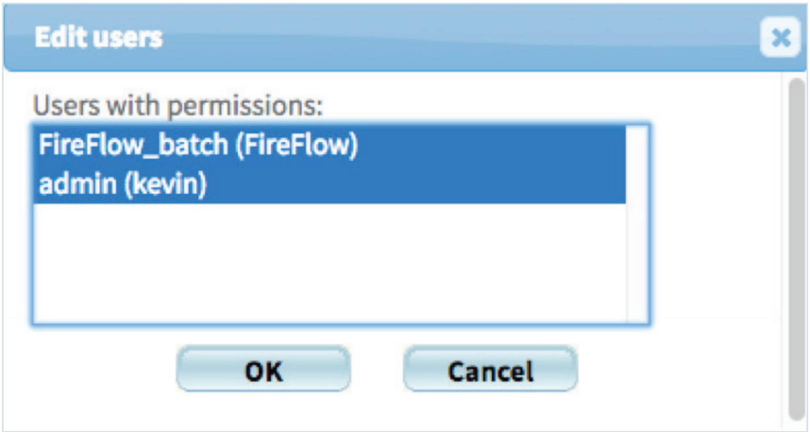
Options

☑ Real-time change monitoring

☑ Set user permissions

Note: if you selected Set user permissions then the Edit Users dialog box appears.

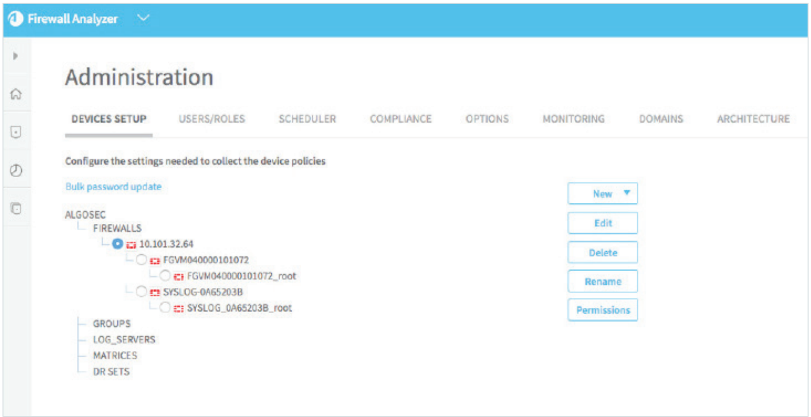
Set which users will have access to the reports produced by the device (see below).



Users with permissions:

FireFlow_batch (FireFlow)
admin (kevin)

When configuration is completed you will see the following screen.

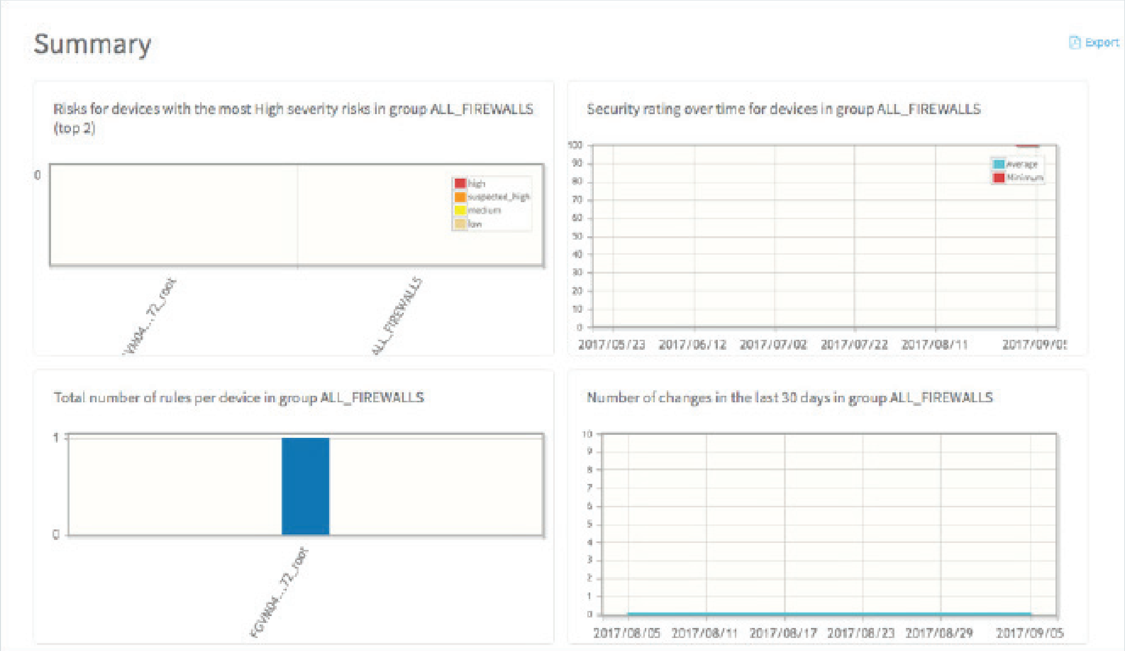


Configure the settings needed to collect the device policies

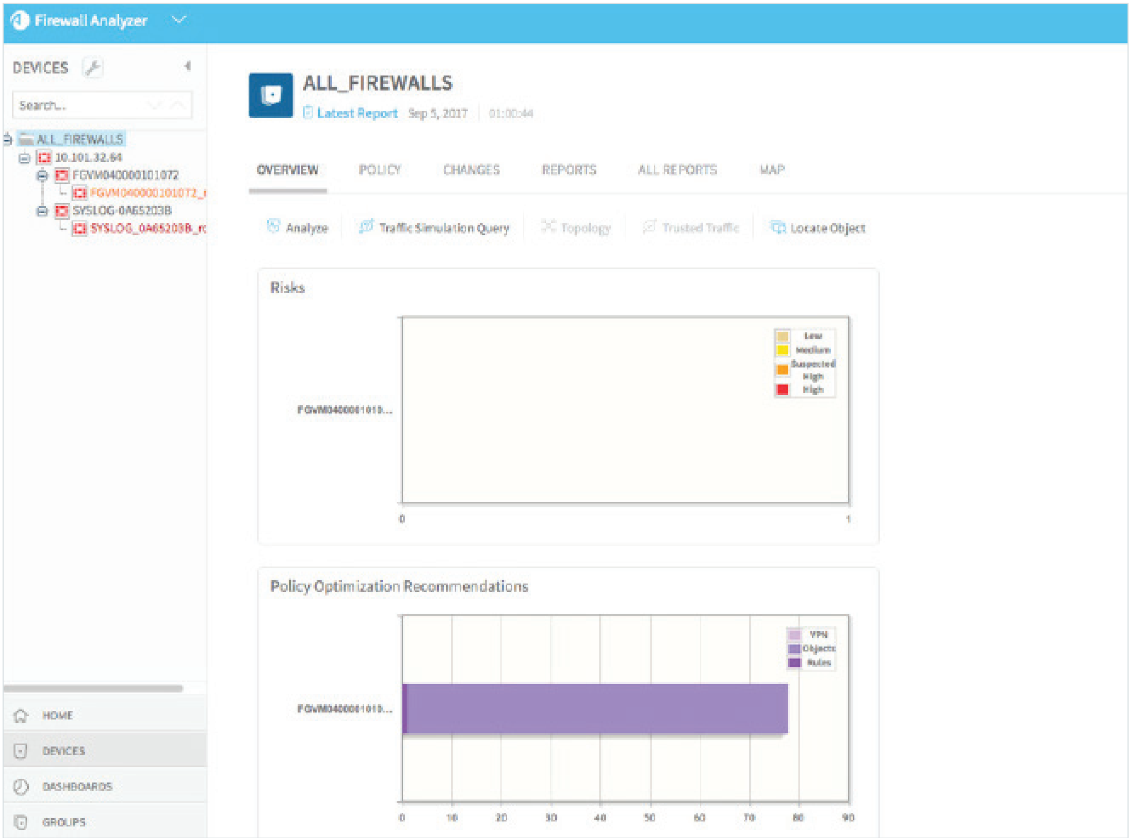
```
ALGOSEC
  FIREWALLS
    ● 10.101.32.64
      ○ FGVM040000101072
        ○ FGVM040000101072_root
      ○ SYSLOG-0A65203B
        ○ SYSLOG_0A65203B_root
  GROUPS
  LOG_SERVERS
  MATRICES
  DR SETS
```

Switch to the Devices page, and select ALL_FIREWALLS in the firewall tree on the left.

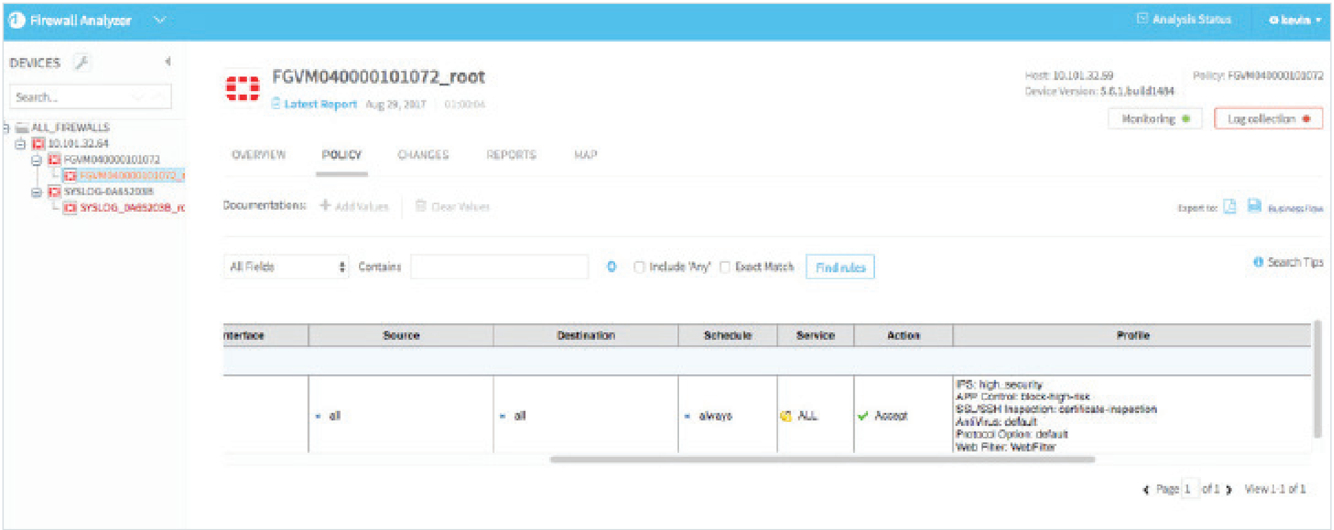
Then click 'Analyze' on the right pane to run a full risk, compliance and cleanup analysis on all the newly added Fortinet firewalls.


Summary
Export
Risks for devices with the most High severity risks in group ALL_FIREWALLS (top 2)
0
high
suspected_high
medium
low
VM04...72_root
ALL_FIREWALLS
Security rating over time for devices in group ALL_FIREWALLS
100
90
80
70
60
50
40
30
20
10
0
Average
Minimum
2017/05/23
2017/06/12
2017/07/02
2017/07/22
2017/08/11
2017/09/0!
Total number of rules per device in group ALL_FIREWALLS
1
0
FGVM04...72_root
Number of changes in the last 30 days in group ALL_FIREWALLS
10
9
8
7
6
5
4
3
2
1
0
2017/08/05
2017/08/11
2017/08/17
2017/08/23
2017/08/29
2017/09/05

All Devices screen.



Devices Policy screen.



FGVM040000101072_root

Latest Report Aug 29, 2017 01:00:04

Host: 10.101.32.59
Device Version: 5.6.1,build1484

Policy: FGVM040000101072

□ Include 'Any' □ Exact Match

nterface	Source	Destination	Schedule	Service	Action	Profile
	all	all	always	ALL	✓ Accept	IPS: high_security APP Control: block-high-risk SSL/SSH Inspection: certificate-inspection AntiVirus: default Protocol Option: default Web Filter: WebFilter

Page 1 of 1 View 1-1 of 1

Conclusion

You are now ready to use the AlgoSec Security Management Solution with your Fortinet Firewalls. Refer to AlgoSec Firewall Analyzer, FireFlow and BusinessFlow user guides for more information on the various capabilities you can use.

FortiManager Administration Guide:
http://docs.fortinet.com/uploaded/files/3872/FortiManager-5.6.0-Administration-Guide.pdf

Technical Note on enabling RPC in FortiManager:
http://kb.fortinet.com/kb/documentLink.do?externalID=FD40394

Solution Brief:
https://www.fortinet.com/content/dam/fortinet/assets/alliances/Fortinet-AlgoSec-Solution-Brief.pdf

For Manual Data Collection methods refer to the AlgoSec Firewall Analyzer Administration Guide.

June 25, 2021 9:43 PM

139156-C-0-EN