DEPLOYMENT GUIDE

Fortinet and Tufin SecureTrack

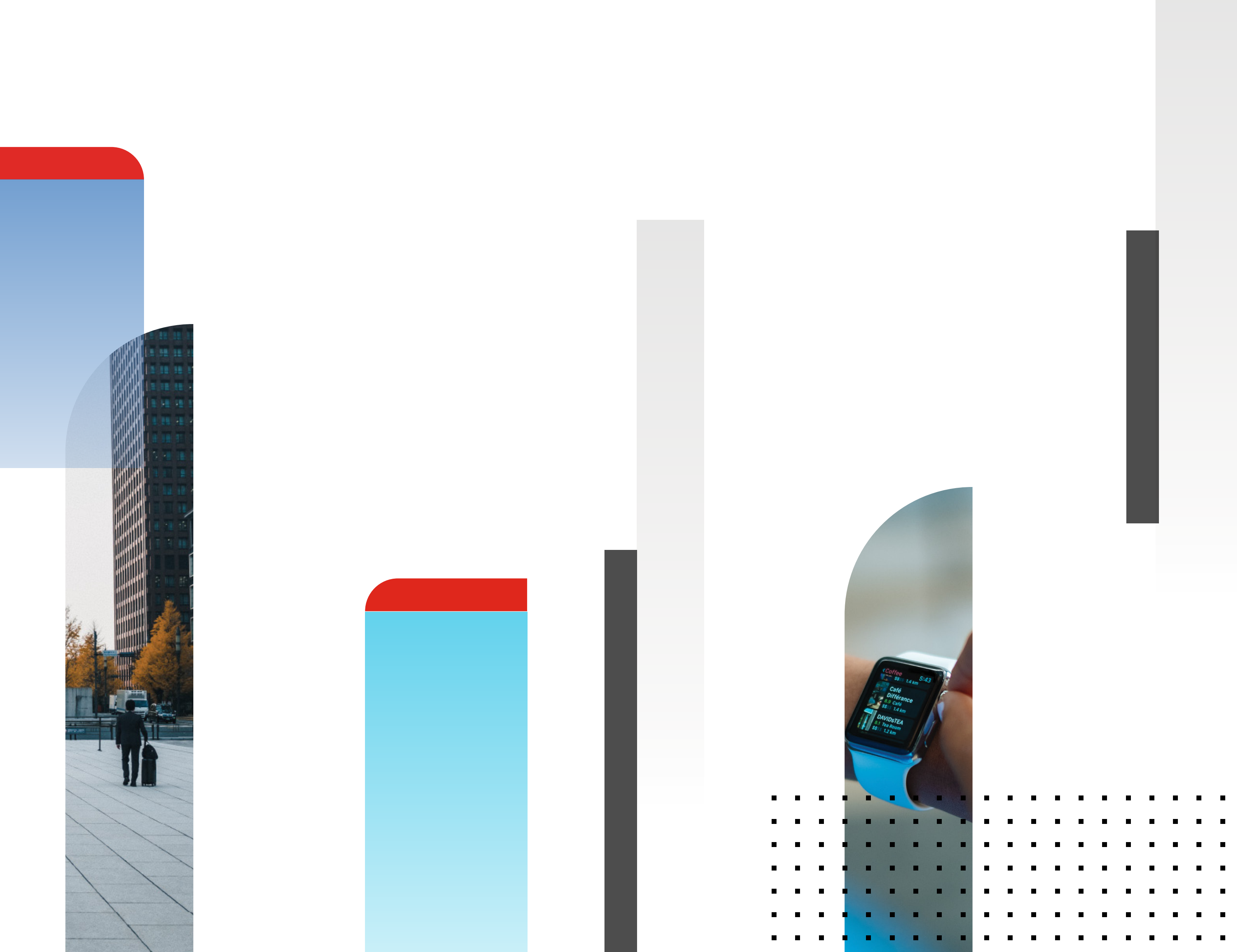


Table of Contents

Overview

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 #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.

About Tufin

Tufin is the leader in Network Security Policy Orchestration for enterprise cybersecurity. More than half of the top 50 companies in the Forbes Global 2000 turn to Tufin to simplify management of some of the largest, most complex networks in the world, consisting of thousands of firewall and network devices and emerging hybrid cloud infrastructures. Enterprises select the company's award-winning Tufin Orchestration Suite™ to increase agility in the face of ever-changing business demands while maintaining a robust security posture. The Suite reduces the attack surface and meets the need for greater visibility into secure and reliable application connectivity. Its network security automation enables enterprises to implement changes in minutes with proactive risk analysis and continuous policy compliance. Tufin serves over 1,900 customers spanning all industries and geographies; its products and technologies are patent-protected in the U.S. and other countries. Find out more at www.tufin.com.

Deployment Prerequisites

1. Fortinet FortiManager version 5.x (tested with versions 5.4.2 and 5.6.0)
2. Tufin Orchestration Suite SecureTrack version 17.1 GA.2 build 93488

FORTINET FABRIC-READY

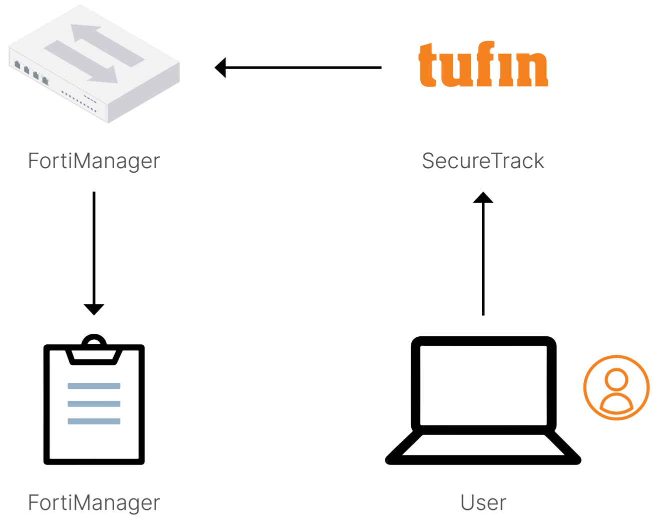
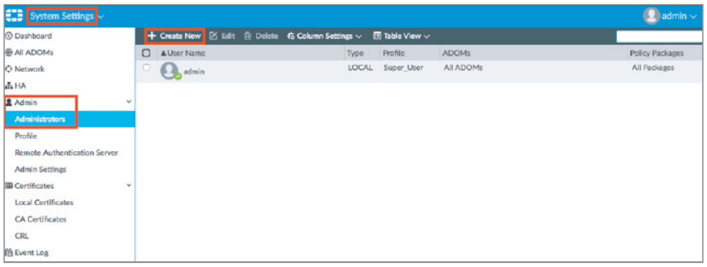


Figure 1: Architecture overview.

FortiManager Configuration

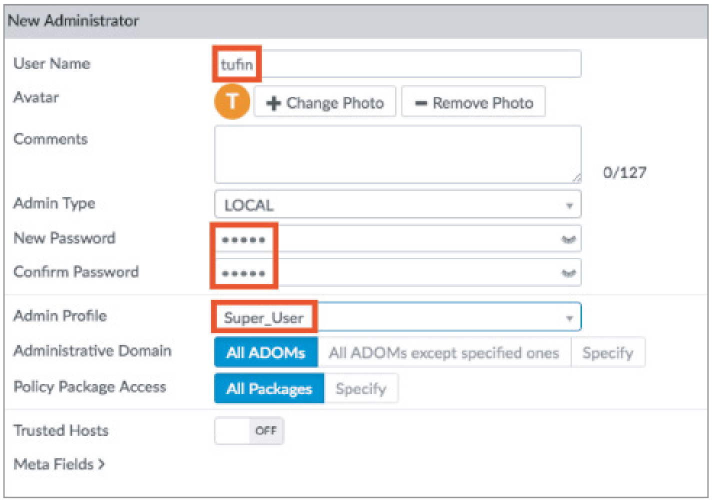
Create and configure an administrator account for tufin to use.

1. Create and configure an administrator account for Tufin to use.
2. From System Settings go to Admin > Administrators > Create New.



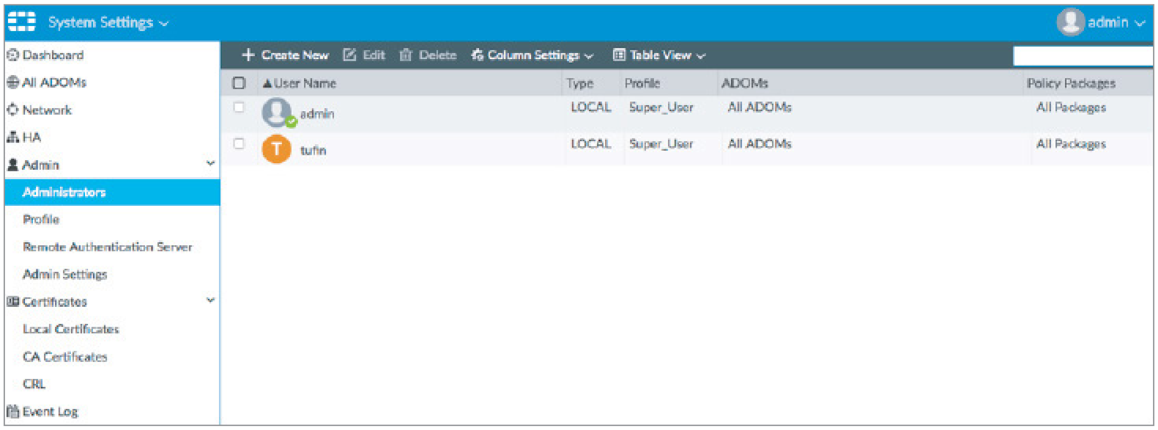
□	User Name	Type	Profile	ADOMs	Policy Packages
□	admin	LOCAL	Super_User	All ADOMs	All Packages

3. Enter a username, new password and confirm the password. Set the Admin Profile to Super_User and click OK at the bottom.



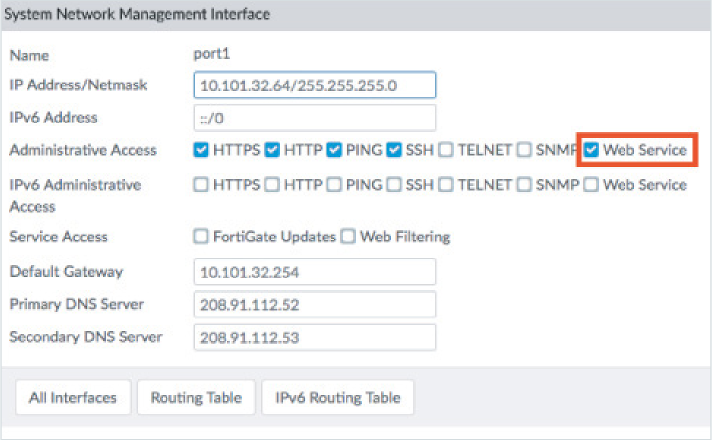
User Name	tufin
Avatar	T
Comments	
Admin Type	LOCAL
New Password	•••••
Confirm Password	•••••
Admin Profile	Super_User
Administrative Domain	All ADOMs / All ADOMs except specified ones / Specify
Policy Package Access	All Packages / Specify
Trusted Hosts	OFF
Meta Fields >	

4. The screen should look like the image below.



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

5. 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

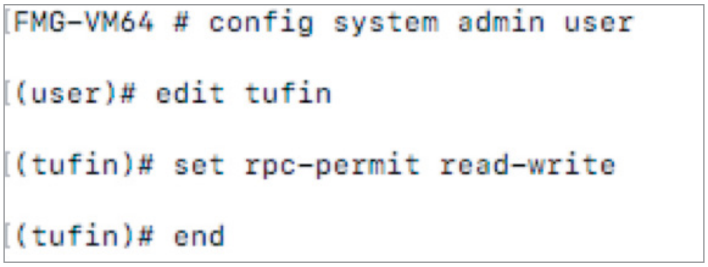
Primary DNS Server: 208.91.112.52

Secondary DNS Server: 208.91.112.53

6. 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).

7. Connect to the FortiManager CLI to change the Tufin administrator account permissions.

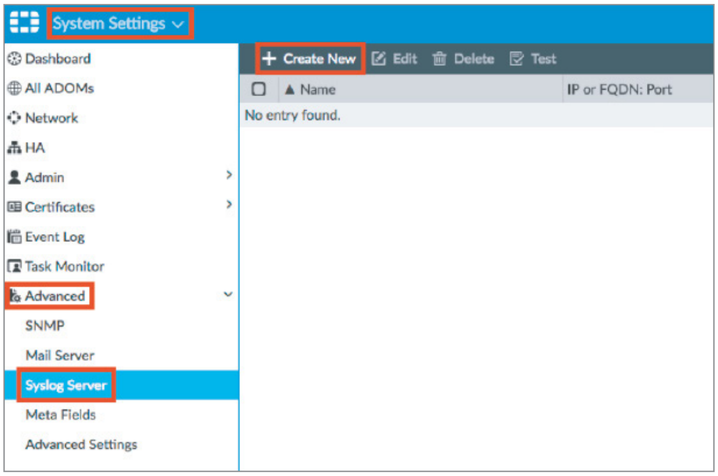
8. Enter the following CLI commands:



```
FMG-VM64 # config system admin user

(user)# edit tufin

(tufin)# set rpc-permit read-write

(tufin)# end
```

9. Configure FortiManager to send Syslog to the Tufin IP address.

10. From System Settings go to Advanced > Syslog Server and click Create New.

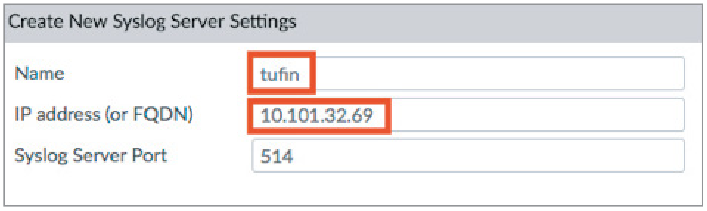


No entry found.

11. Enter a Name.

12. Enter the IP Address or FQDN of the tufin server.

13. Click OK.



Create New Syslog Server Settings

Name: tufin

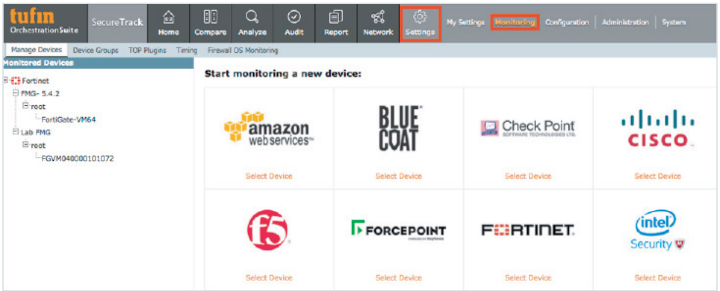
IP address (or FQDN): 10.101.32.69

Syslog Server Port: 514

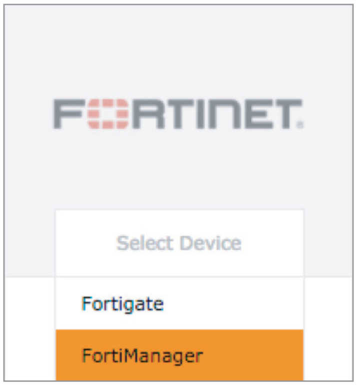
Tufin SecureTrack Configuration

14. Configure tufin SecureTrack to monitor FortiManager.

15. Go to Settings > Monitoring.



16. Click the Fortinet panel > Select Device > FortiManager.



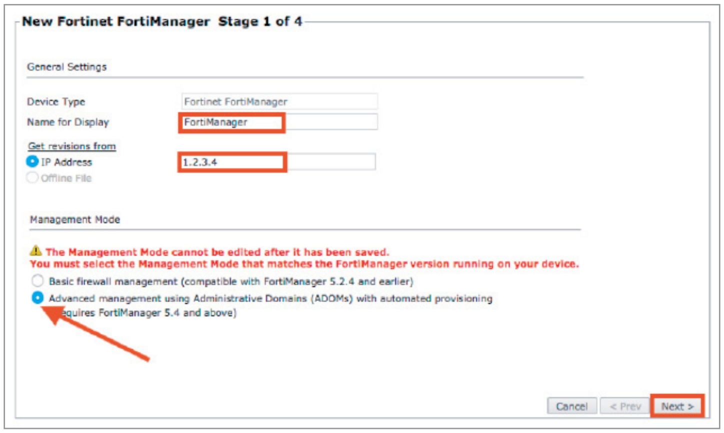
17. Enter a Name for Display.

18. Enter the IP address of the FortiManager.

19. Select Basic firewall management if using FortiManager 5.2 and earlier.

20. Select Advanced management if using FortiManager 5.4 and above.

21. Click Next.



New Fortinet FortiManager Stage 1 of 4

General Settings

Device Type: Fortinet FortiManager

Name for Display: FortiManager

Get revisions from

● IP Address: 1.2.3.4

○ Offline File

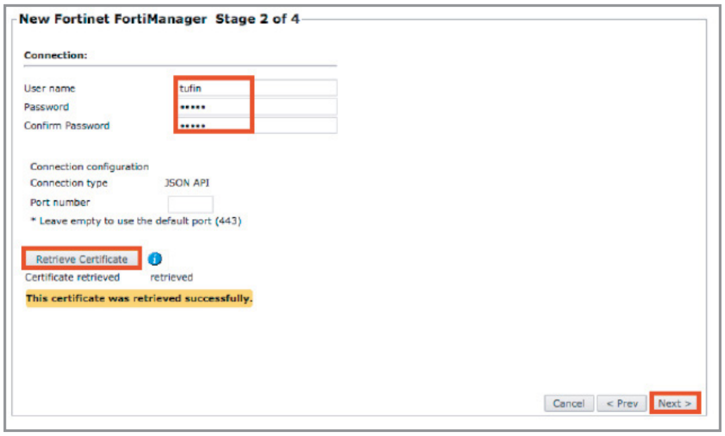
Management Mode

⚠ The Management Mode cannot be edited after it has been saved.
You must select the Management Mode that matches the FortiManager version running on your device.

○ Basic firewall management (compatible with FortiManager 5.2.4 and earlier)

● Advanced management using Administrative Domains (ADOMs) with automated provisioning
equires FortiManager 5.4 and above)

22. Enter the username and password configured previously.
23. Click Retrieve Certificate and wait for confirmation it was retrieved.
24. Click Next.



New Fortinet FortiManager Stage 2 of 4

Connection:

User name: tufin

Password: •••••

Confirm Password: •••••

Connection configuration

Connection type: JSON API

Port number:

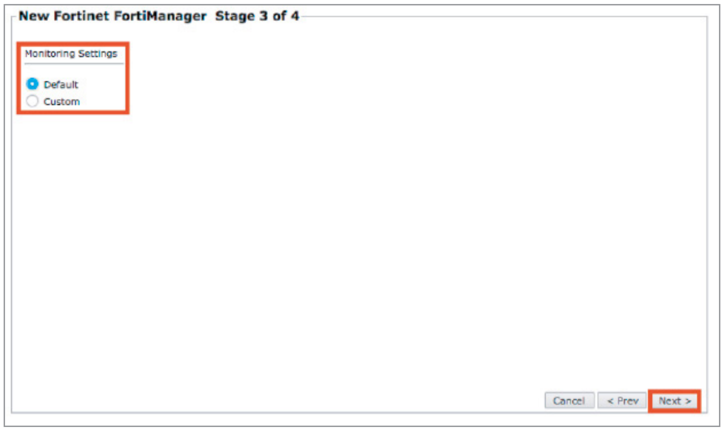
* Leave empty to use the default port (443)

Retrieve Certificate

Certificate retrieved: retrieved

This certificate was retrieved successfully.

25. Select the desired Monitoring Settings, either Default or Custom.
26. Click Next.



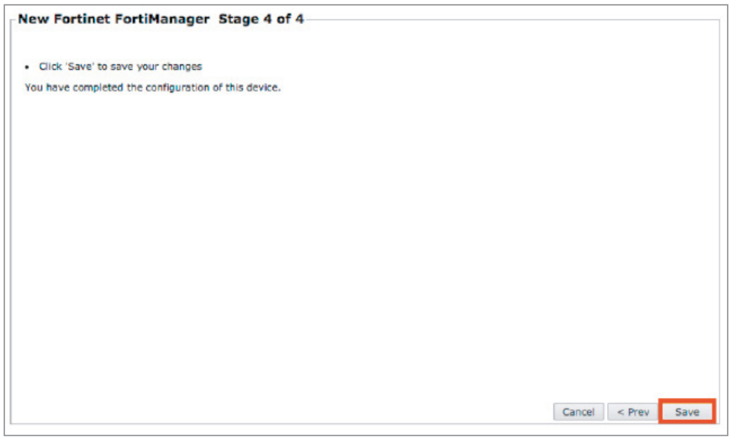
New Fortinet FortiManager Stage 3 of 4

Monitoring Settings

● Default

○ Custom

27. Click Save.

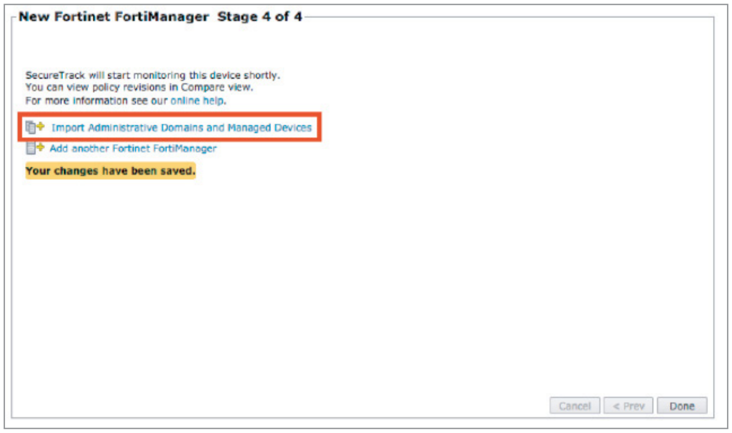


New Fortinet FortiManager Stage 4 of 4

- Click 'Save' to save your changes

You have completed the configuration of this device.

28. Click Import Administrative Domains and Managed Devices.



New Fortinet FortiManager Stage 4 of 4

SecureTrack will start monitoring this device shortly.
You can view policy revisions in Compare view.
For more information see our online help.

Import Administrative Domains and Managed Devices

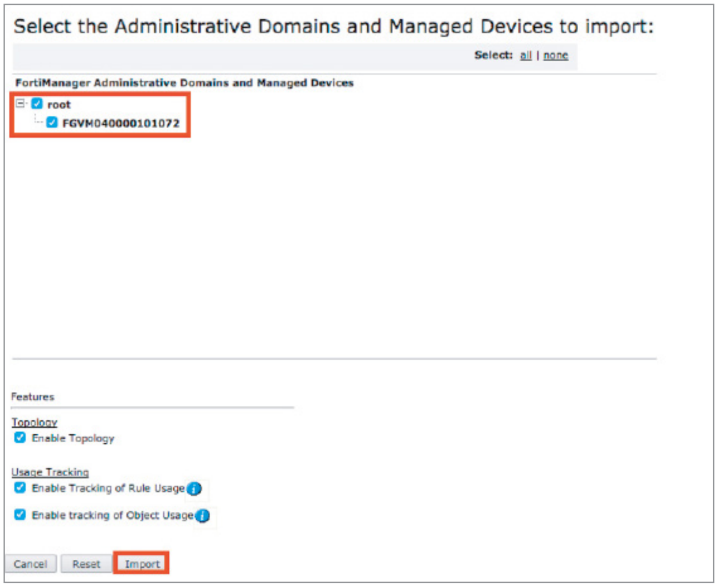
Add another Fortinet FortiManager

Your changes have been saved.

29. Select the Administrative Domains and Managed Devices to import.

30. Select the desired Features.

31. Click Import.



Select the Administrative Domains and Managed Devices to import:

Select: all | none

FortiManager Administrative Domains and Managed Devices

☑ root
☑ FGVM040000101072

Features

Topology

☑ Enable Topology

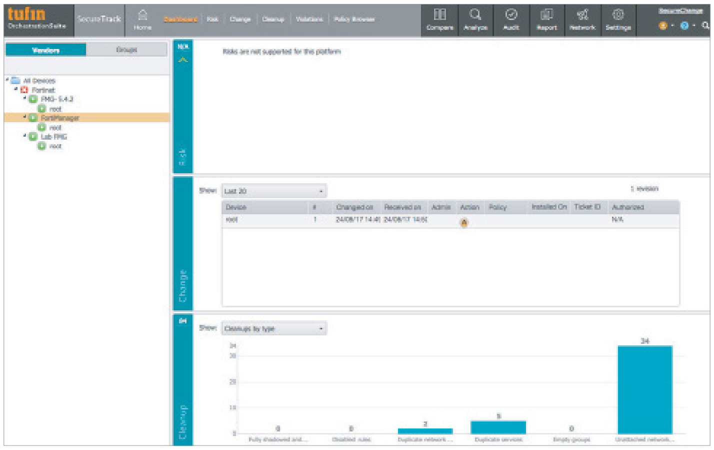
Usage Tracking

☑ Enable Tracking of Rule Usage

☑ Enable tracking of Object Usage

32. The configuration is now complete.

The Home Dashboard should look like this:



Risks are not supported for this platform

Show: Last 20

1 revision

Device	#	Changed on	Received on	Admin	Action	Policy	Installed On	Ticket ID	Authorized
root	1	24/08/17 14:4(	24/08/17 14:5(						N/A

Show: Cleanups by type

Summary

Fortinet and Tufin have developed an integrated offering for comprehensive network security policy orchestration. Together, the Tufin Orchestration Suite with Fortinet FortiGate firewalls and FortiManager network security management products reduce attack surface for mitigation of cyber threats. The joint offering enables IT security teams to manage complex heterogeneous physical networks and cloud platforms through a single pane of glass, providing advanced visibility and risk-free policy modifications. Based on advanced analysis and automation technologies, network security policies are orchestrated across the enterprise networks, leveraging the advanced capabilities and unparalleled security protection of Fortinet FortiGate firewalls.

FortiManager Administration Guide

Technical Note on enabling RPC in FortiManager

Solution Brief

Solution Overview Video

Tufin Knowledge Center

FORTINET

www.fortinet.com

June 7, 2021 10:43 PM
127405-C-0-EN