

ADS Script for Fortigate Quarantine

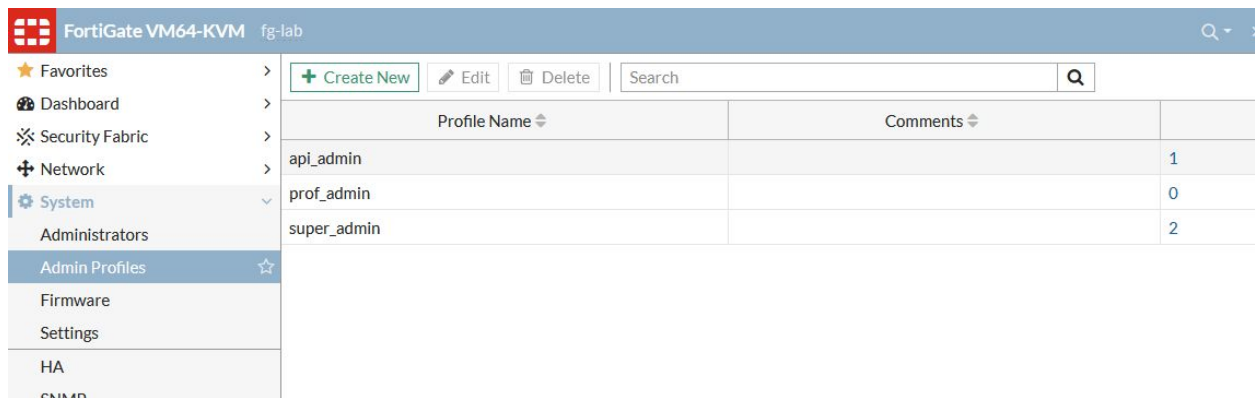
This document describes how to use the mitigation script for blocking suspicious stations automatically on Fortigate firewalls. It is using the Fortigate API. Unblocking needs to be performed manually on a Fortigate device once the threat is mitigated.

Configuration

The script contains configuration such as firewall IP address, API key and timeout settings. These parameters can be provided by Flowmon ADS when the script is triggered or hardcoded in the script itself based on the user preference. You can open and adjust the script before uploading to Flowmon ADS by editing values on lines 13, 14 and 17.

```
13 IP='192.168.47.28'  
14 API_KEY='fp8114zdNpjp8Qf8zN4Hdp57dhgjff'  
15 # Default timeout for action is  
16 # value in seconds or never  
17 TIMEOUT='300'  
18
```

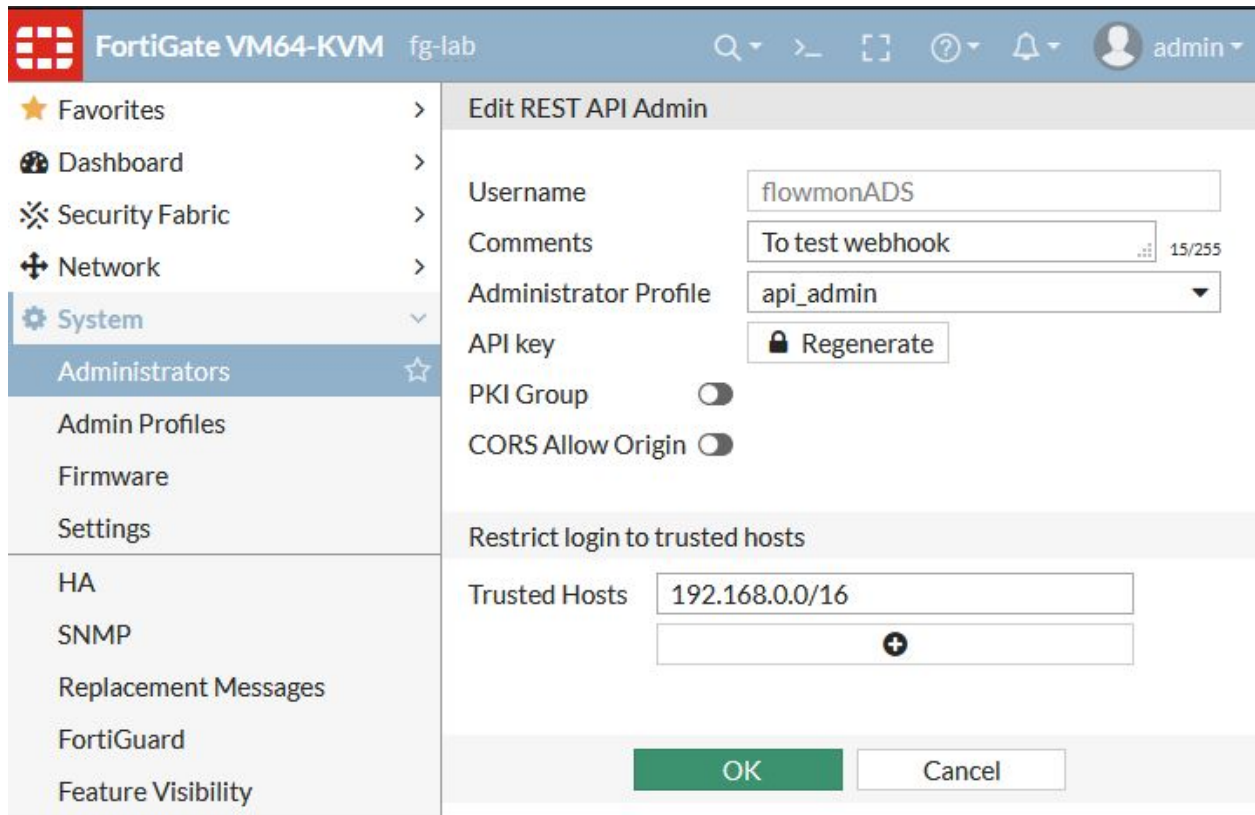
On a Fortigate device you need to add a specific Fortigate user which has access to API. This user will enable Flowmon ADS to access the Fortigate device. To configure such a user you would need first to create a profile at System > Admin Profiles.



The screenshot shows the FortiGate VM64-KVM Admin Profiles page. The left sidebar contains navigation options: Favorites, Dashboard, Security Fabric, Network, System (expanded), Administrators, Admin Profiles (selected), Firmware, Settings, HA, and SNMP. The main content area displays a table of Admin Profiles with columns for Profile Name and Comments. The table contains three entries: api_admin (1 comment), prof_admin (0 comments), and super_admin (2 comments).

Profile Name	Comments
api_admin	1
prof_admin	0
super_admin	2

Then in System > Administrator create a New REST API Admin, you can limit networks/IP addresses which have access to API just to Flowmon appliance IP/network.



The screenshot shows the FortiGate VM64-KVM web interface. The top navigation bar includes the FortiGate logo, the device name 'FortiGate VM64-KVM', the lab name 'fg-lab', and user information 'admin'. A left sidebar contains a menu with items like Favorites, Dashboard, Security Fabric, Network, System, Administrators, Admin Profiles, Firmware, Settings, HA, SNMP, Replacement Messages, FortiGuard, and Feature Visibility. The main content area is titled 'Edit REST API Admin' and contains the following fields and controls:

- Username:** flowmonADS
- Comments:** To test webhook (15/255 characters)
- Administrator Profile:** api_admin
- API key:** A 'Regenerate' button with a lock icon.
- PKI Group:** A toggle switch, currently turned off.
- CORS Allow Origin:** A toggle switch, currently turned off.
- Restrict login to trusted hosts:** A section with a 'Trusted Hosts' field containing '192.168.0.0/16' and a '+' button to add more hosts.

At the bottom of the configuration area are 'OK' and 'Cancel' buttons.

This step will generate for you an API key you need to include in script or ADS configuration. Or you would need to regenerate it later. User name you can use any string to understand that it was this key triggering API key.


Now you are ready to add new action in Flowmon ADS (details are available in Flowmon ADS User Guide). Upload the script in Settings > System settings > Custom scripts. If you have hard coded parameters in the script you do not need to provide any additional parameters. Otherwise configure add username (user), password (pass), firewall IP address (ip) and timeout settings (timeout) parameters to script configuration.

Edit custom script ✕


Name

Run type ▾

Limit (per priority and data feed)

File 

Parameters

Name	Value
 No data	

Now you can set up blocking via Fortigate as custom action in Settings > Processing > Custom scripts for desired perspective and priority of events.

Edit custom script action ✕

Name

Script

Parameters

Name	Value
<div style="border: 1px solid #ccc; padding: 5px;">i No data</div>	

Perspective

Active

Do not send empty reports

Skip identical events

Minimal priority to be reported

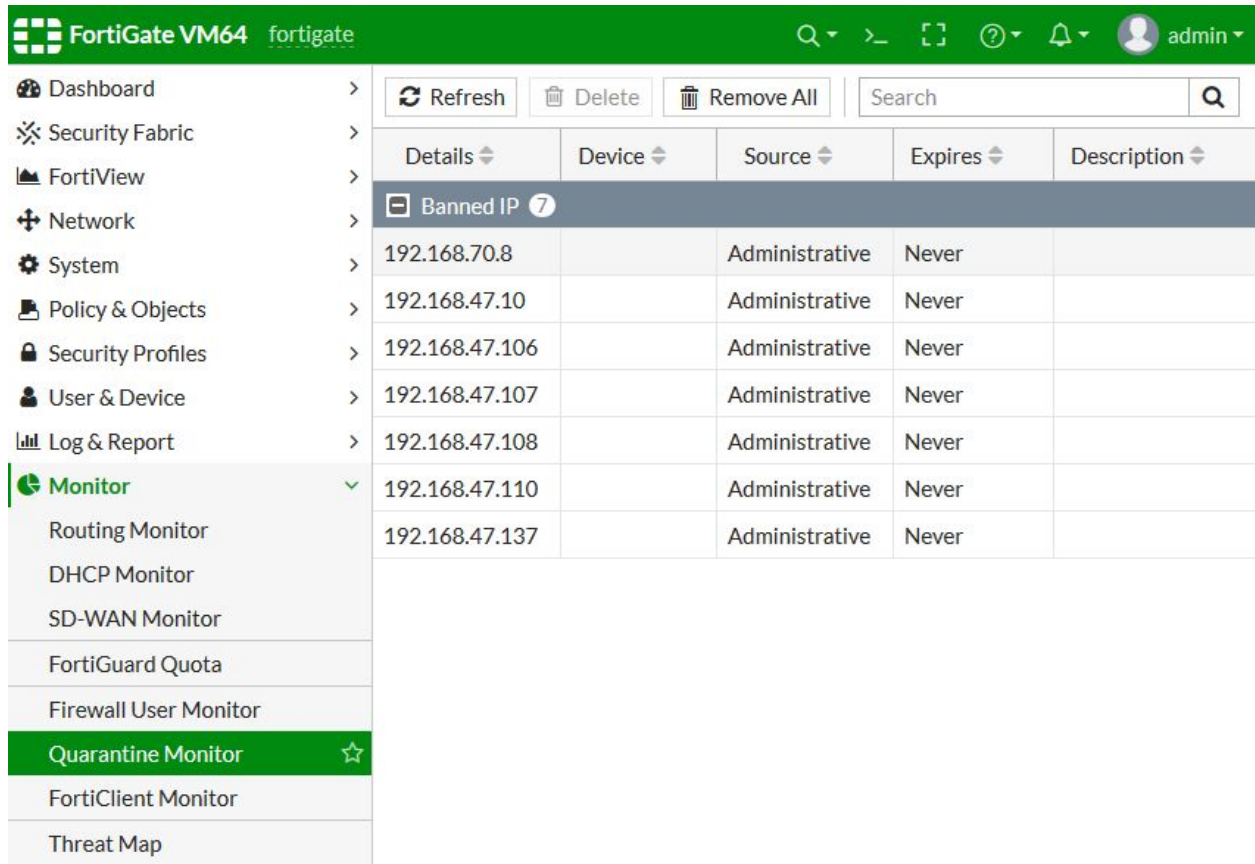
Limit (per priority and data feed)

Owner

SAVE **+ SAVE AS NEW** **CLOSE**

Operation

In Fortigate GUI you can see blocked IPs in Monitor > Quarantine Monitor.



The screenshot shows the FortiGate VM64 GUI interface. The left sidebar contains a navigation menu with 'Monitor' selected and 'Quarantine Monitor' highlighted. The main content area displays a table of blocked IP addresses under the heading 'Banned IP 7'.

Details	Device	Source	Expires	Description
Banned IP 7				
192.168.70.8		Administrative	Never	
192.168.47.10		Administrative	Never	
192.168.47.106		Administrative	Never	
192.168.47.107		Administrative	Never	
192.168.47.108		Administrative	Never	
192.168.47.110		Administrative	Never	
192.168.47.137		Administrative	Never	

Or use a command in CLI.

```
diagnose user quarantine list
```

You would need to delete quarantined IPs manually when a particular threat is mitigated and blocking is no longer needed.