FortiGate Integration

FortiEDR 6.2.0

July 4, 2024
FortiEDR 6.2.0 FortiGate Integration
63-620-1022596-20240704

TABLE OF CONTENTS

Change log

Date	Change Description
2024-04-26	Initial document release.
2024-04-29	Updated Configuring FortiGate on page 7.
2024-06-12	Updated the following topics: • Configuring FortiEDR on page 10 • Prerequisites on page 6

Overview

With the integration of FortiEDR and FortiGate, access to malicious destination addresses detected by FortiEDR are automatically denied on the FortiGate through FortiEDR's automatic incident response actions upon security event triggering. FortiEDR also prevents all other devices behind the FortiGate from communicating with the malicious destination, including unmanaged devices and headless devices that do not have FortiEDR installed.

For more information about FortiGate, see the *FortiGate Administration Guide* in the Fortinet Document Library.

Prerequisites

Before you start configuring the integration with FortiGate, verify the following:

- Your FortiEDR deployment includes a Jumpbox that has connectivity to FortiGate.
  - Refer to Installing the FortiEDR Core for details about how to install a FortiEDR Core and configure it as a Jumpbox.
  - Refer to Cores for more information about configuring a Jumpbox.
- The FortiEDR Central Manager has connectivity to the Fortinet Cloud Services (FCS). To verify this, make sure that FCS is in running state (Green) in the *System Components* chart in the Dashboard of the FortiEDR management console.

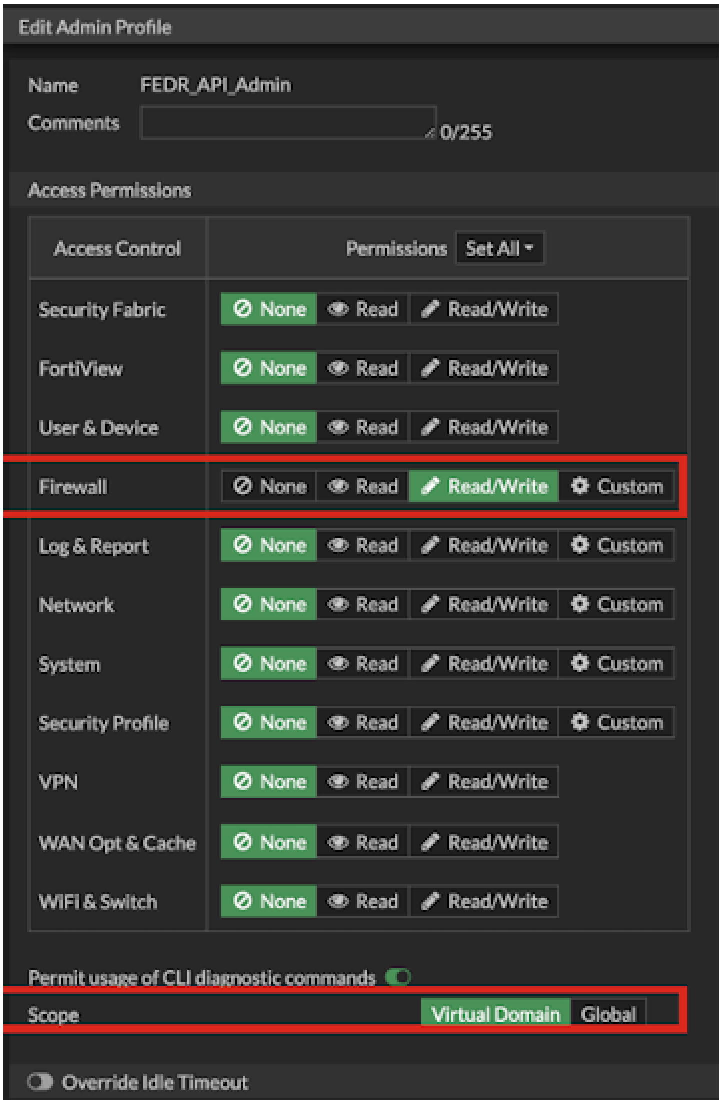
Configuring FortiGate

To integrate FortiEDR with FortiGate, you must first create an admin profile and a REST API admin in FortiGate with sufficient privileges for the integration. You must also set up an address group and a firewall policy on FortiGate.

Fortinet recommends that you create a dedicated admin profile, API admin, address group, and firewall policy for the FortiEDR integration.

To create an admin profile in FortiGate:

1. Go to *System* > *Admin Profiles* and click *Create New*.
2. Configure the admin profile:



Edit Admin Profile

Name: FEDR_API_Admin

Comments: 0/255

Access Permissions

Access Control	Permissions (Set All)
Security Fabric	[✓ None] Read Read/Write
FortiView	[✓ None] Read Read/Write
User & Device	[✓ None] Read Read/Write
Firewall	None Read [✓ Read/Write] Custom
Log & Report	[✓ None] Read Read/Write Custom
Network	[✓ None] Read Read/Write Custom
System	[✓ None] Read Read/Write Custom
Security Profile	[✓ None] Read Read/Write Custom
VPN	[✓ None] Read Read/Write
WAN Opt & Cache	[✓ None] Read Read/Write
WiFi & Switch	[✓ None] Read Read/Write

Permit usage of CLI diagnostic commands ●

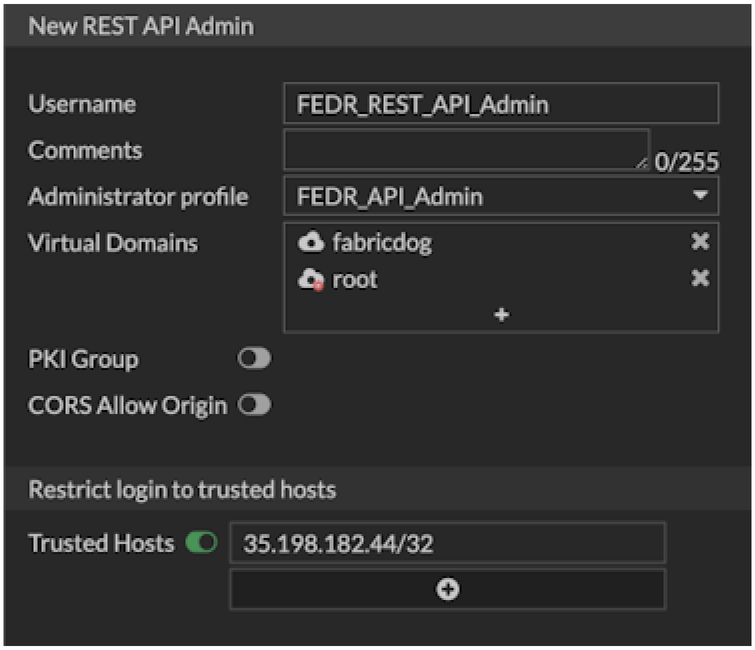
Scope: [✓ Virtual Domain] Global

○ Override Idle Timeout

- a. In the *Name* field, enter the admin profile name.
- b. In the *Access Permissions* section, select *Read/Write* for the *Firewall* row and leave all other fields as *None* as additional privileges are unnecessary for the integration.
- c. Configure other options as needed. See Administrator profiles for more information.
- d. Click *Save*.

To create an associated REST API admin in FortiGate:

1. Go to *System* > *Administrators* and click *Create New* > *REST API Admin*.
2. Configure the administrator:



New REST API Admin

Username: FEDR_REST_API_Admin

Comments: 0/255

Administrator profile: FEDR_API_Admin

Virtual Domains: fabricdog, root

PKI Group

CORS Allow Origin

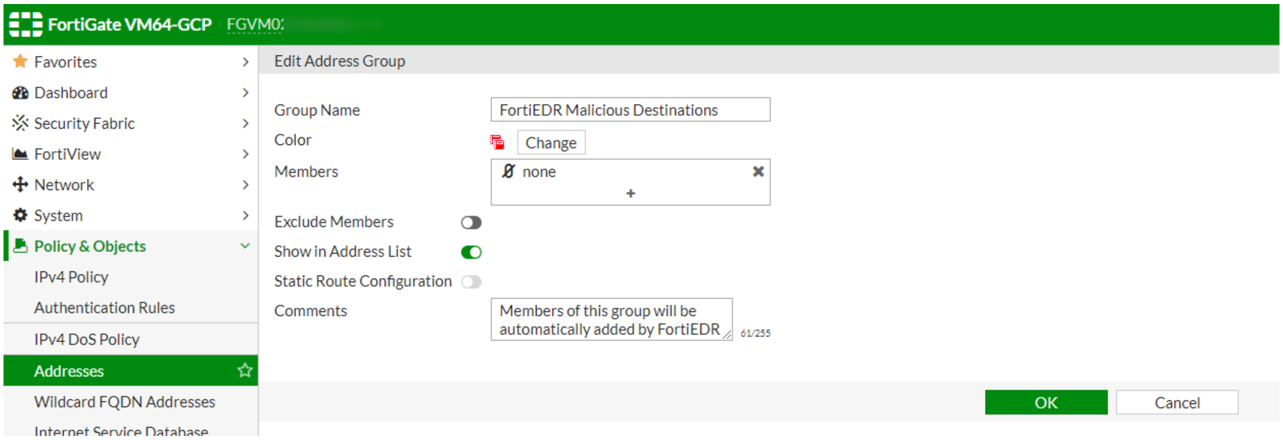
Restrict login to trusted hosts

Trusted Hosts: 35.198.182.44/32

- a. Specify a username.
- b. Select the admin profile that you created earlier.
- c. If using VDOMs, ensure the relevant Virtual Domains are selected.
- d. In *Trusted Hosts*, enter the IP address of the FortiEDR JumpBox.
- e. Configure other options as needed. See REST API administrator for more information.
- f. Click *OK*.
  An API token is generated. Make note of the token, as it is only shown once and you will need to provide it when Configuring FortiEDR on page 10.

To set up an address group and policy on FortiGate:

1. Go to *Policy & Objects* > *Addresses*.
2. Create a new address group to be populated by FortiEDR. The new address group now appears in the FortiGate Addresses table.

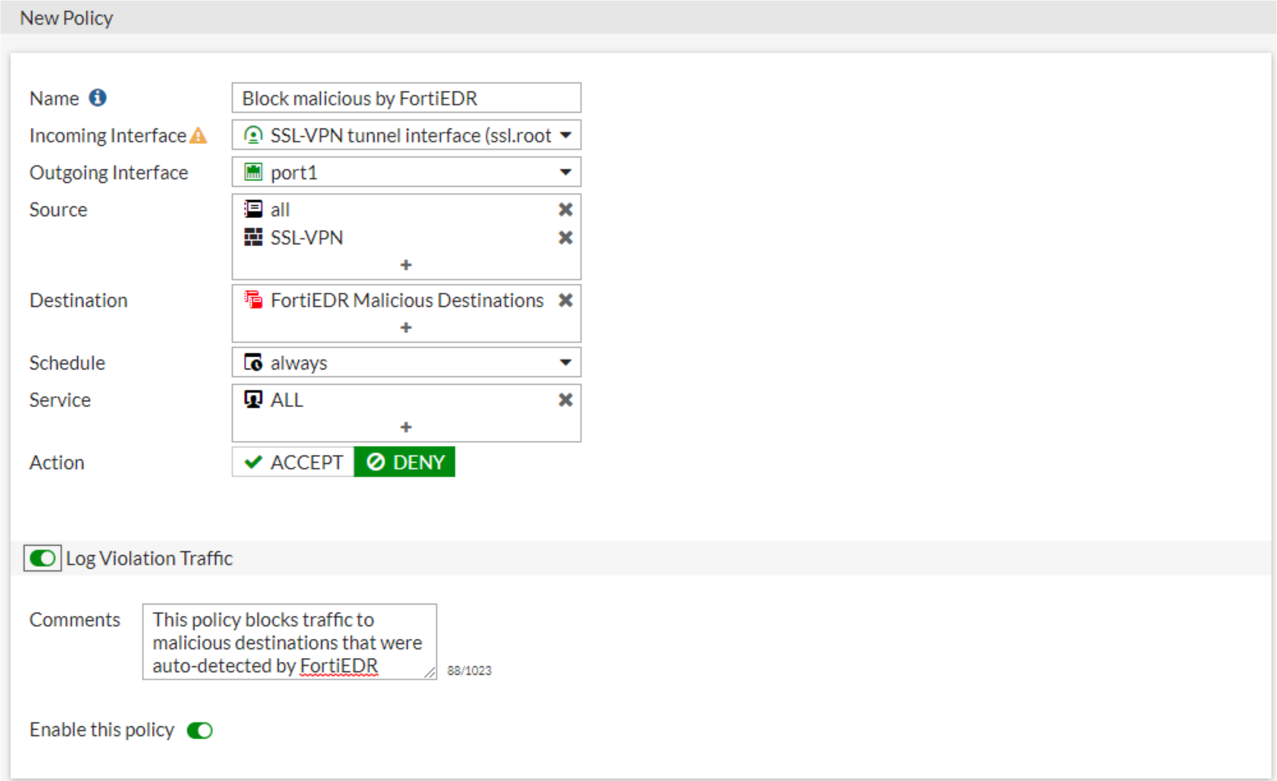


Edit Address Group

Group Name	FortiEDR Malicious Destinations
Color	Change
Members	none
Exclude Members	○
Show in Address List	●
Static Route Configuration	○
Comments	Members of this group will be automatically added by FortiEDR 61/255

3. Go to *Policy & Objects* > *IPv4 Policy*.

4. Create a new policy to deny traffic to any address in the address group that was created as part of step 2. The new policy now appears in the FortiGate Policies table.



New Policy

Name	Block malicious by FortiEDR
Incoming Interface	SSL-VPN tunnel interface (ssl.root
Outgoing Interface	port1
Source	all SSL-VPN
Destination	FortiEDR Malicious Destinations
Schedule	always
Service	ALL
Action	ACCEPT [✓ DENY]

● Log Violation Traffic

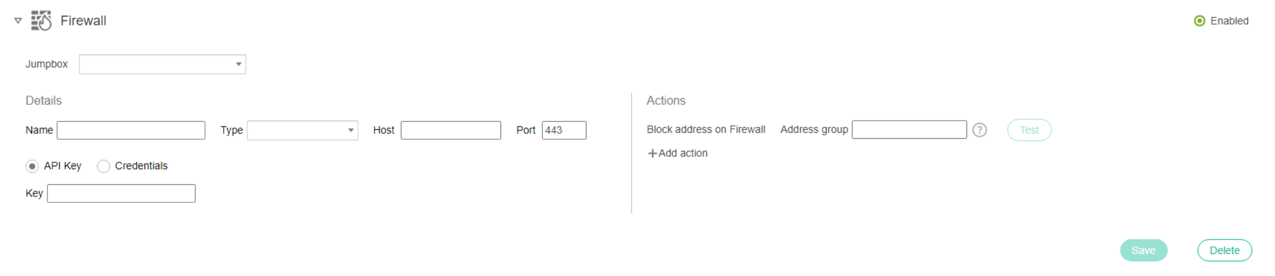
Comments	This policy blocks traffic to malicious destinations that were auto-detected by FortiEDR 88/1023
Enable this policy	●

Configuring FortiEDR

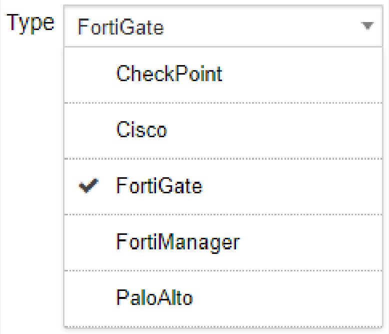
To integrate FortiEDR with FortiGate, you must configure a firewall connector for FortiGate and playbook policies with *Block address on Firewall* action enabled in FortiEDR. Access to malicious destination addresses detected by FortiEDR will then be automatically denied on the firewall through FortiEDR's automatic incident response actions upon security event triggering.

To set up a firewall connector with FortiEDR:

1. Click the *Add Connector* button and select *Firewall* in the *Connectors* dropdown list. The following displays:



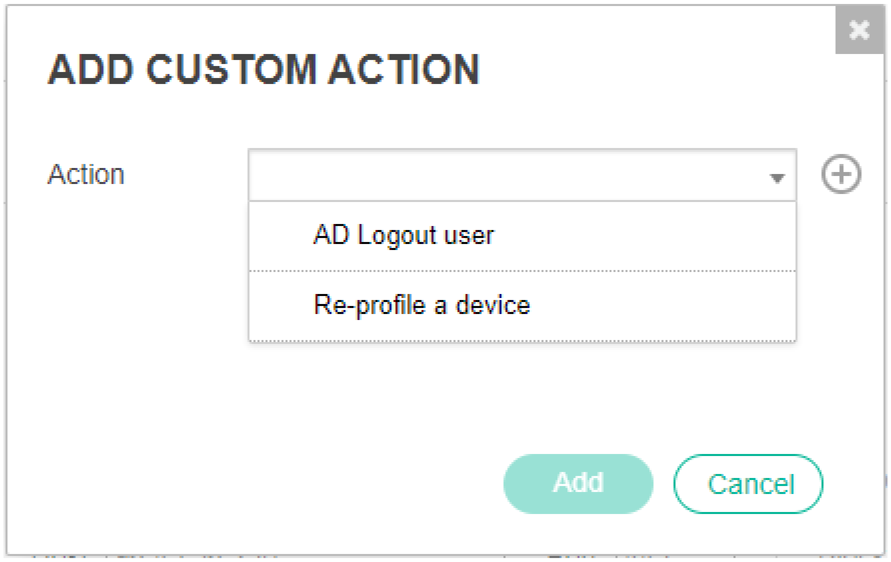
2. Fill in the following fields:

Field	Definition
Jumpbox	Select the FortiEDR Jumpbox to communicate with FortiGate.
Name	Specify a name of your choice to be used to identify the integration with FortiGate.
Type	Select *FortiGate* in the dropdown list.  Type FortiGate CheckPoint Cisco ✓ FortiGate FortiManager PaloAlto
Host	Specify the IP or DNS address of FortiGate.
Port	Specify the port that is used for API communication with FortiGate.
API Key / Credentials	Select *API Key* and specify the API token of the FortiGate, which is generated when you are Configuring FortiGate on page 7.

3. In the *Actions* area on the right, define an action to be taken by this connector.
You have the option to either use an action provided out-of-the-box with FortiEDR (*Block address on Firewall*) or to create and use your own custom actions by clicking *Add action*.

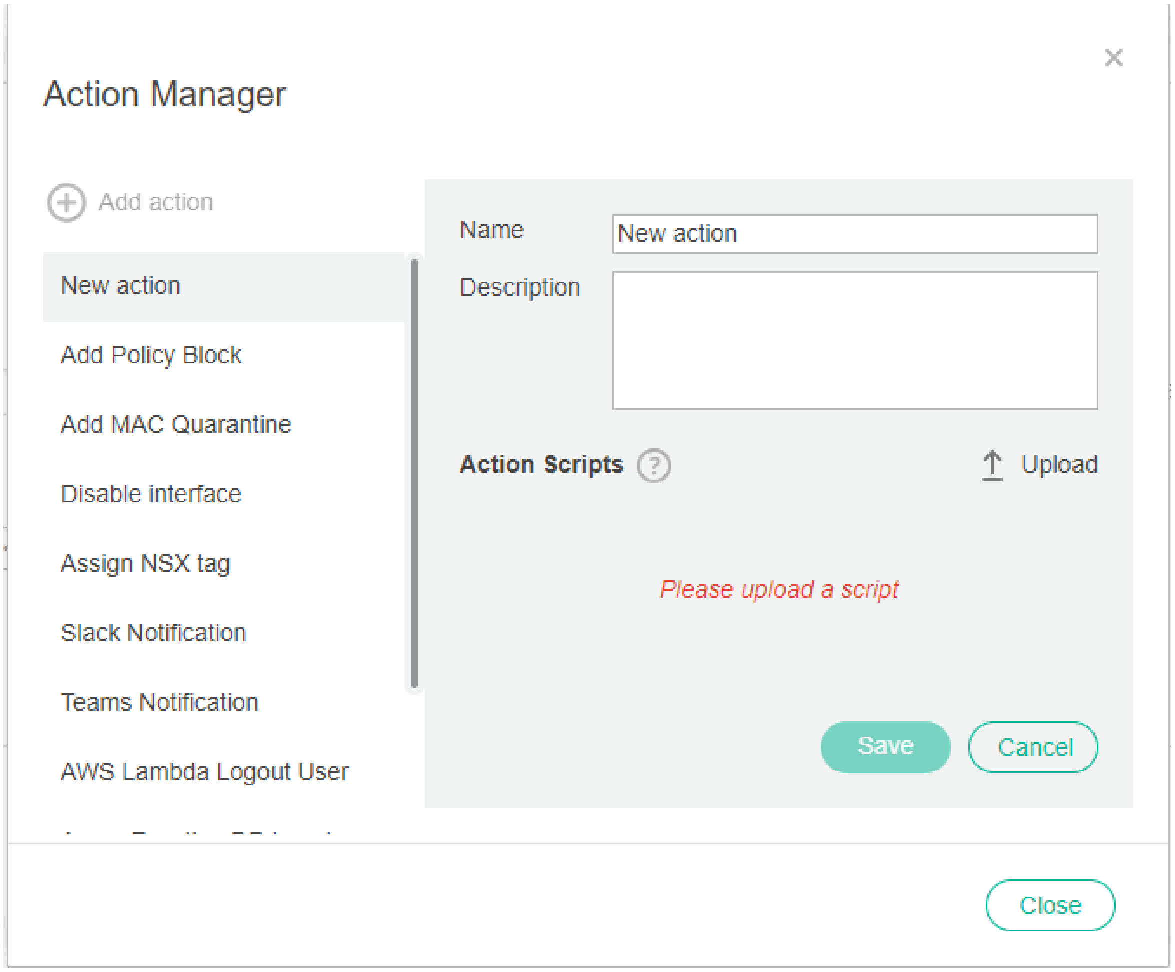
a. To block an address on the FortiGate, in the *Address Group* field, specify the name of the address group you defined when Configuring FortiGate on page 7. You can optionally specify the name of the VDOM domain in the *VDOM* field. FortiEDR uses the default root VDOM if the *VDOM* field is empty.
- OR -

b. To trigger a custom action on the Firewall, click the *Add Action* button to display the following popup window:



- In the *Action* dropdown menu, select one of the previously defined custom integration actions (which were defined in FortiEDR as described in Custom integration).
  – OR –

- Click the *Create New Action* ⊕ button in this popup window to define a new action on the FortiGate to be triggered according to the definitions in the Playbook, as described below. The following displays:



Action Manager

Name: New action

Description:

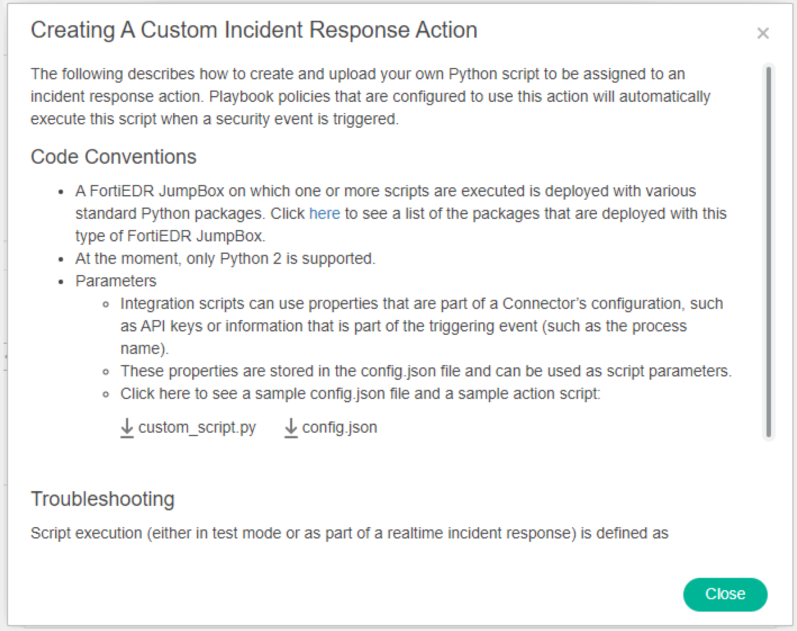
Action Scripts ?

Please upload a script

Fill out the fields of this window as follows in order to define a new action to be triggered in response to an incident.

In order to trigger this action, a Playbook policy must be defined that triggers this action to execute the script when a security event is triggered. The definition of this new action here automatically adds this action as an option in a Playbook policy. This action however, is not selected by default in the Playbook policy. Therefore, you must go to the Playbook policy and select it in order for it to be triggered when a security event is triggered.

Field	Definition
Name	Enter any name for this action.
Description	Enter a description of this action.

Field	Definition
Upload	Upload a Python script that calls an API in the third-party system in order to perform the relevant action. Python 2.7 or later is supported. This Python script must be created according to the coding conventions that can be displayed by clicking the icon ? next to the *Action Scripts* field. The following displays providing an explanation of these coding conventions and provides various links that you can click to see more detail and or/to download sample files. 

Creating A Custom Incident Response Action

×

The following describes how to create and upload your own Python script to be assigned to an incident response action. Playbook policies that are configured to use this action will automatically execute this script when a security event is triggered.

Code Conventions

- A FortiEDR JumpBox on which one or more scripts are executed is deployed with various standard Python packages. Click here to see a list of the packages that are deployed with this type of FortiEDR JumpBox.
- At the moment, only Python 2 is supported.
- Parameters
  - Integration scripts can use properties that are part of a Connector's configuration, such as API keys or information that is part of the triggering event (such as the process name).
  - These properties are stored in the config.json file and can be used as script parameters.
  - Click here to see a sample config.json file and a sample action script:

    ↓ custom_script.py ↓ config.json

Troubleshooting

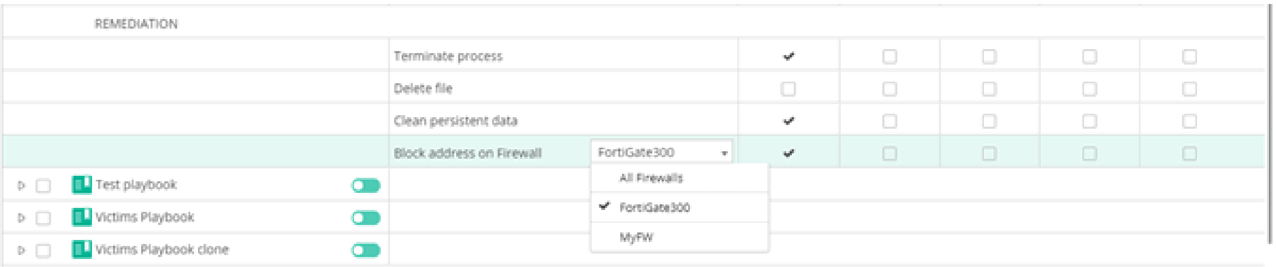
Script execution (either in test mode or as part of a realtime incident response) is defined as

Close

4. Click *Save*. The new action is then listed in the *Actions* area.
5. You can click the *Test* button to test the connectivity. If the test fails, verify the API key you entered in step 3 or the trusted host setting when Configuring FortiGate on page 7.

To configure an automated incident response that uses the firewall connector to block malicious destinations upon security event triggering:

1. Navigate to the *SECURITY SETTINGS* > *Playbooks* page.
2. Open the Playbook policy that is applied on devices for which you want the block IP incident response to apply and place a checkmark in the relevant *Classification* column next to the *Block address on Firewall* row that is under the *REMEDIATION* section. In the dropdown menu next to the action, you can specify which firewalls to use to perform the block or select all of them, as shown below:



REMEDIATION							
	Terminate process		✓	□	□	□	□
	Delete file		□	□	□	□	□
	Clean persistent data		✓	□	□	□	□
	Block address on Firewall	FortiGate300 ▾	✓	□	□	□	□

▷ □ Test playbook

▷ □ Victims Playbook

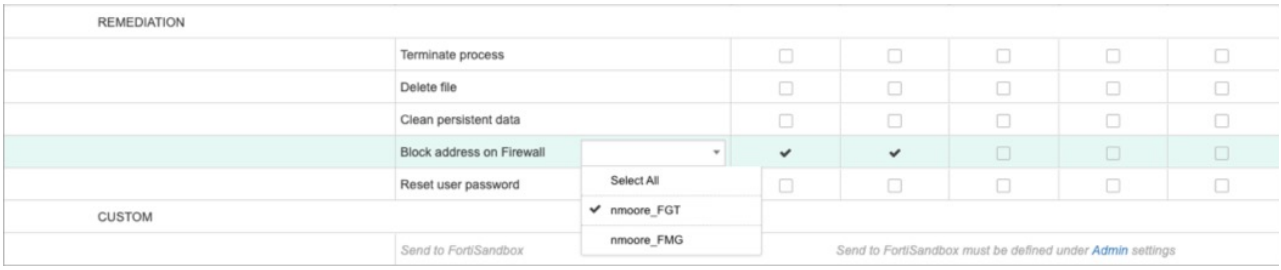
▷ □ Victims Playbook clone

All Firewalls
✓ FortiGate300
MyFW

FortiEDR is now configured to add malicious IP addresses to the blocking policy on the firewall upon triggering of a security event. You can check that malicious IP addresses are added to the address group that was configured in FortiGate following FortiEDR security events.

To configure an automated incident response that uses a firewall connector to perform a custom action upon the triggering of a security event:

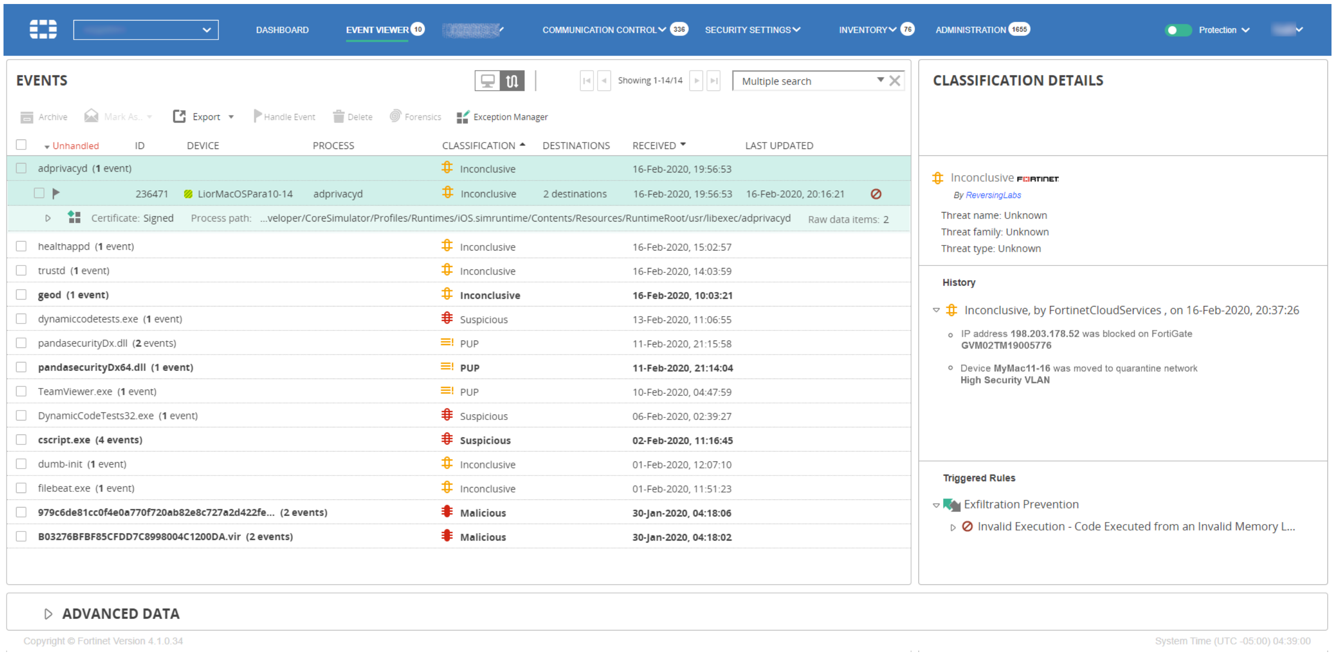
1. Navigate to the *SECURITY SETTINGS* > *Playbooks* page.
2. Open the Playbook policy that is applied on devices for which you want the custom action (defined above) to apply.
3. In the *CUSTOM* section, place a checkmark in the relevant *Classification* columns next to the row of the relevant custom action.
4. In the dropdown menu next to the relevant custom action, select the relevant firewall connector with which to perform the action, as shown below:



REMEDIATION							
	Terminate process		□	□	□	□	□
	Delete file		□	□	□	□	□
	Clean persistent data		□	□	□	□	□
	Block address on Firewall	▾	✓	✓	□	□	□
	Reset user password	Select All ✓ nmoore_FGT nmoore_FMG	□	□	□	□	□
CUSTOM							
	Send to FortiSandbox		*Send to FortiSandbox must be defined under Admin settings*				

FortiEDR is now configured to trigger this action in the third-party system upon the triggering of a security event.

Automatic incident response actions are listed in the *CLASSIFICATION DETAILS* area of the *Events* page of the FortiEDR Console, as shown below:



EVENTS

□ Unhandled	ID	DEVICE	PROCESS	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED
□ adprivacyd (1 event)				Inconclusive		16-Feb-2020, 19:56:53	
□	236471	LiorMacOSPara10-14	adprivacyd	Inconclusive	2 destinations	16-Feb-2020, 19:56:53	16-Feb-2020, 20:16:21
Certificate: Signed	Process path: ...veloper/CoreSimulator/Profiles/Runtimes/iOS.simruntime/Contents/Resources/RuntimeRoot/usr/libexec/adprivacyd						Raw data items: 2
□ healthappd (1 event)				Inconclusive		16-Feb-2020, 15:02:57	
□ trustd (1 event)				Inconclusive		16-Feb-2020, 14:03:59	
□ **geod (1 event)**				**Inconclusive**		**16-Feb-2020, 10:03:21**	
□ dynamiccodetests.exe (1 event)				Suspicious		13-Feb-2020, 11:06:55	
□ pandasecurityDx.dll (2 events)				PUP		11-Feb-2020, 21:15:58	
□ **pandasecurityDx64.dll (1 event)**				**PUP**		**11-Feb-2020, 21:14:04**	
□ TeamViewer.exe (1 event)				PUP		10-Feb-2020, 04:47:59	
□ DynamicCodeTests32.exe (1 event)				Suspicious		06-Feb-2020, 02:39:27	
□ **cscript.exe (4 events)**				**Suspicious**		**02-Feb-2020, 11:16:45**	
□ dumb-init (1 event)				Inconclusive		01-Feb-2020, 12:07:10	
□ filebeat.exe (1 event)				Inconclusive		01-Feb-2020, 11:51:23	
□ **979c6de81cc0f4e0a770f720ab82e8c727a2d422fe... (2 events)**				**Malicious**		**30-Jan-2020, 04:18:06**	
□ **B03276BFBF85CFDD7C8998004C1200DA.vir (2 events)**				**Malicious**		**30-Jan-2020, 04:18:02**	

CLASSIFICATION DETAILS

Inconclusive FORTINET
By ReversingLabs

Threat name: Unknown
Threat family: Unknown
Threat type: Unknown

History

Inconclusive, by FortinetCloudServices , on 16-Feb-2020, 20:37:26

- IP address **198.203.178.52** was blocked on FortiGate **GVM02TM19005776**
- Device **MyMac11-16** was moved to quarantine network **High Security VLAN**

Triggered Rules

Exfiltration Prevention
Invalid Execution - Code Executed from an Invalid Memory L...

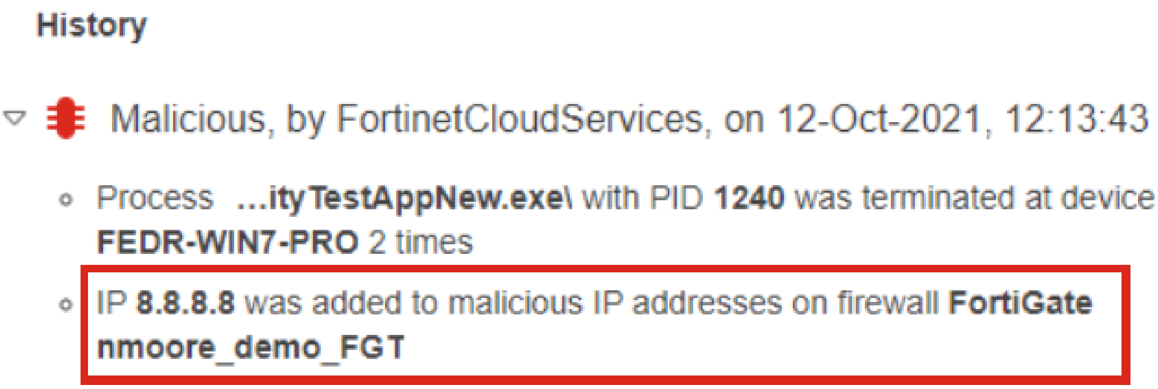
ADVANCED DATA

Copyright © Fortinet Version 4.1.0.34

System Time (UTC -05:00) 04:39:00

Verifying the integration

If the integration is successful, in FortiEDR, the *Block address on Firewall* playbook action will be triggered based on the classification trigger defined within the playbook. In the *Event Viewer*, you should first see an event classified by *FortinetCloudServices*, similar to the following:

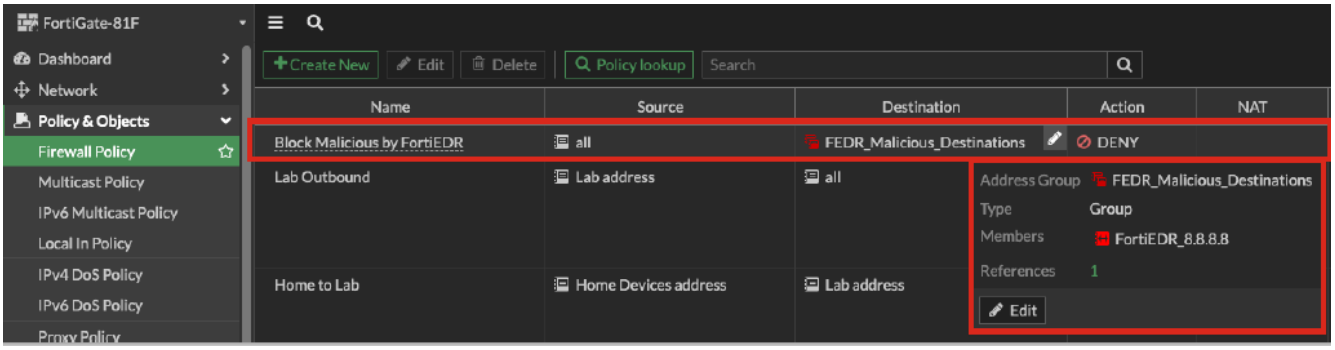


History

Malicious, by FortinetCloudServices, on 12-Oct-2021, 12:13:43

- Process **...ityTestAppNew.exe** with PID **1240** was terminated at device **FEDR-WIN7-PRO** 2 times
- IP **8.8.8.8** was added to malicious IP addresses on firewall **FortiGate nmoore_demo_FGT**

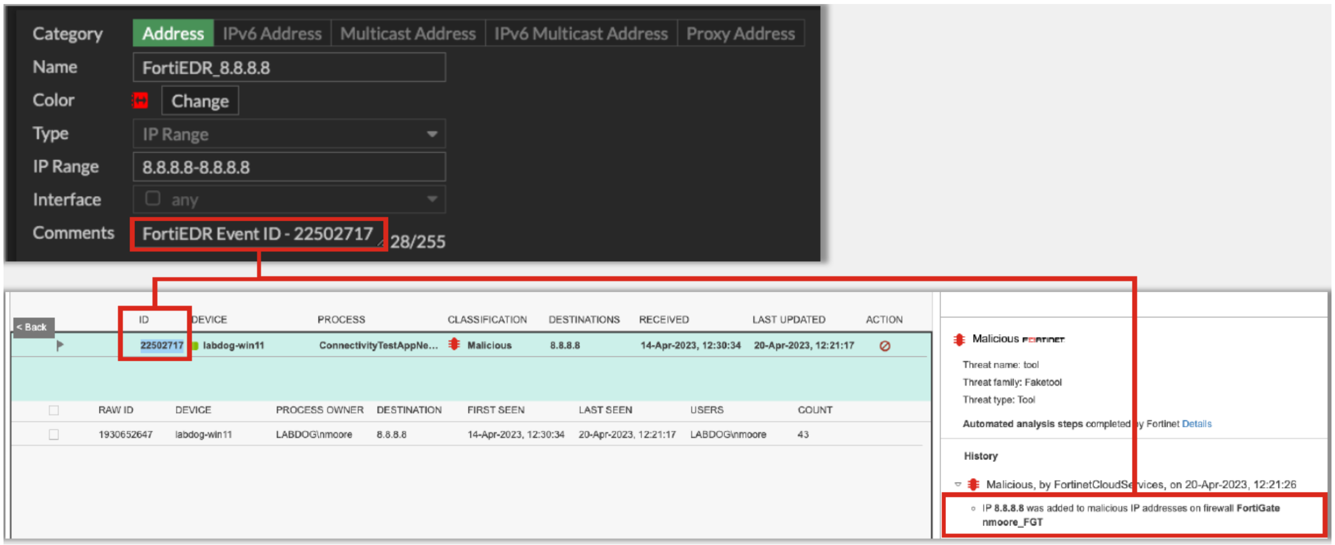
Once the playbook is triggered in FortiEDR, the IP address, if has not been detected and populated before, will be added to the address group for dynamic blocking through the firewall policy. See example below.



Name	Source	Destination	Action	NAT
Block Malicious by FortiEDR	all	FEDR_Malicious_Destinations	DENY	
Lab Outbound	Lab address	all		
Home to Lab	Home Devices address	Lab address		

Address Group: FEDR_Malicious_Destinations
Type: Group
Members: FortiEDR_8.8.8.8
References: 1
Edit

The *Comments* field of the address shows the FortiEDR event ID, which is automatically populated by the FortiEDR playbook API.



Category: Address | IPv6 Address | Multicast Address | IPv6 Multicast Address | Proxy Address

Name: FortiEDR_8.8.8.8

Color: Change

Type: IP Range

IP Range: 8.8.8.8-8.8.8.8

Interface: □ any

Comments: FortiEDR Event ID - 22502717 28/255

< Back

	ID	DEVICE	PROCESS	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED	ACTION
⚑	22502717	labdog-win11	ConnectivityTestAppNe...	Malicious	8.8.8.8	14-Apr-2023, 12:30:34	20-Apr-2023, 12:21:17	⊘

□	RAW ID	DEVICE	PROCESS OWNER	DESTINATION	FIRST SEEN	LAST SEEN	USERS	COUNT
□	1930652647	labdog-win11	LABDOG\nmoore	8.8.8.8	14-Apr-2023, 12:30:34	20-Apr-2023, 12:21:17	LABDOG\nmoore	43

Malicious FORTINET

Threat name: tool

Threat family: Faketool

Threat type: Tool

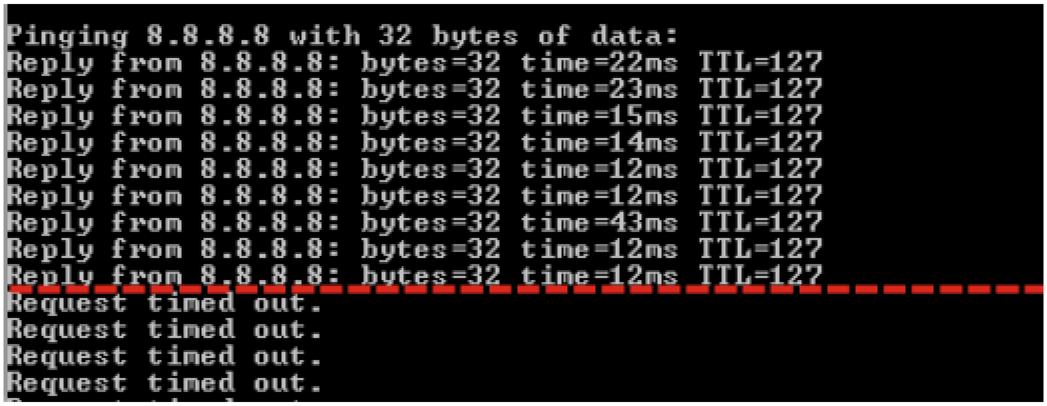
Automated analysis steps completed by Fortinet Details

History

Malicious, by FortinetCloudServices, on 20-Apr-2023, 12:21:26

- IP **8.8.8.8** was added to malicious IP addresses on firewall **FortiGate nmoore_FGT**

After the address is added to the address group, any device matching the firewall policy will be unable to reach the malicious destination IP.



```
Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=22ms TTL=127
Reply from 8.8.8.8: bytes=32 time=23ms TTL=127
Reply from 8.8.8.8: bytes=32 time=15ms TTL=127
Reply from 8.8.8.8: bytes=32 time=14ms TTL=127
Reply from 8.8.8.8: bytes=32 time=12ms TTL=127
Reply from 8.8.8.8: bytes=32 time=12ms TTL=127
Reply from 8.8.8.8: bytes=32 time=43ms TTL=127
Reply from 8.8.8.8: bytes=32 time=12ms TTL=127
Reply from 8.8.8.8: bytes=32 time=12ms TTL=127
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

FORTINET®

www.fortinet.com