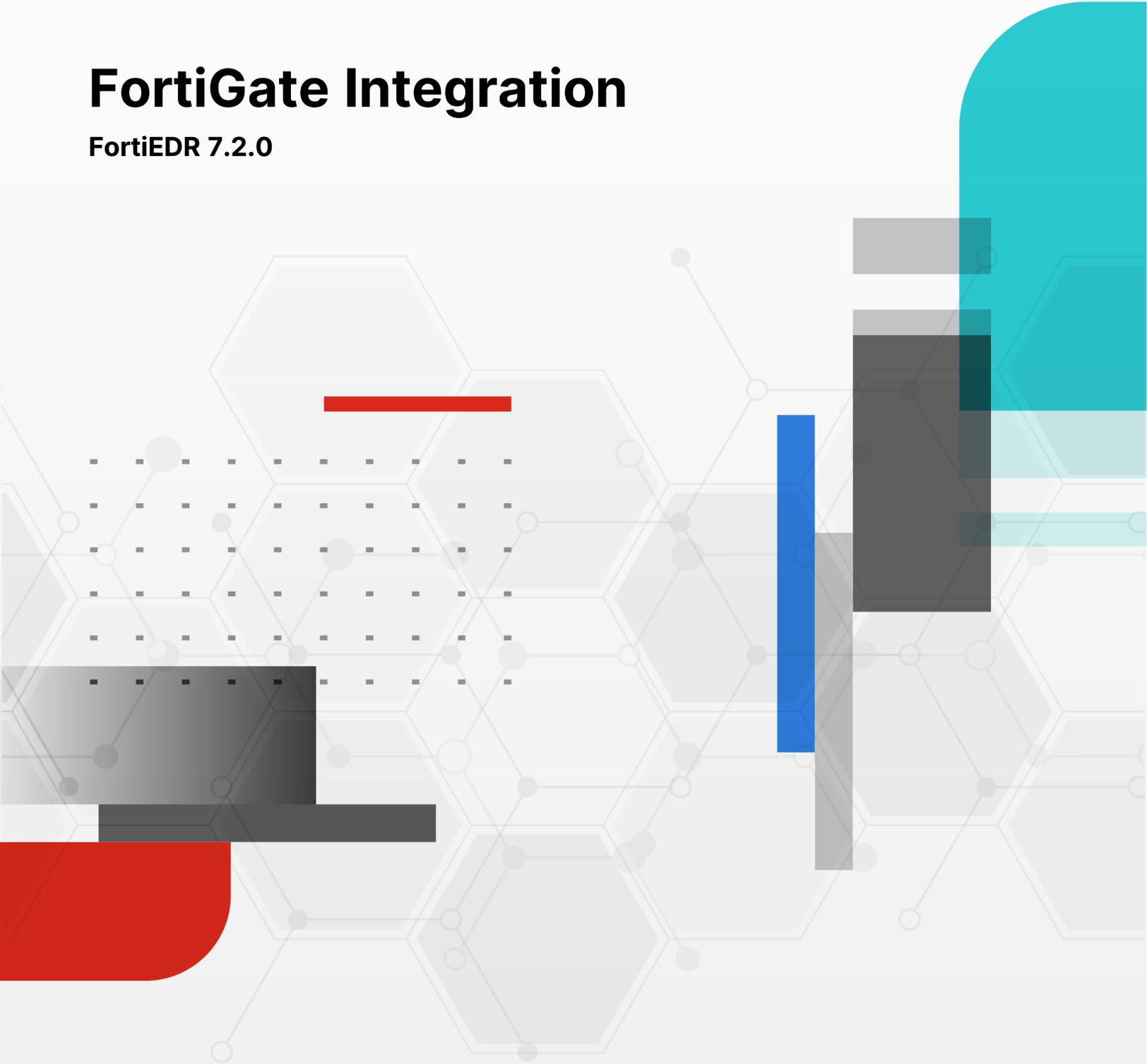


FortiGate Integration

FortiEDR 7.2.0



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO LIBRARY

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/training-certification>

FORTINET TRAINING INSTITUTE

<https://training.fortinet.com>

FORTIGUARD LABS

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



October 10, 2025

FortiEDR 7.2.0 FortiGate Integration

63-720-1214304-20251010

TABLE OF CONTENTS

Change log	4
Overview	5
Prerequisites	6
Configuring FortiGate	7
Configuring FortiEDR	11
Verifying the integration	16

Change log

Date	Change Description
2025-10-10	Initial document release.

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	<input checked="" type="radio"/> None <input type="radio"/> Read <input type="radio"/> Read/Write	
FortiView	<input checked="" type="radio"/> None <input type="radio"/> Read <input type="radio"/> Read/Write	
User & Device	<input checked="" type="radio"/> None <input type="radio"/> Read <input type="radio"/> Read/Write	
Firewall	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read/Write <input type="radio"/> Custom	
Log & Report	<input checked="" type="radio"/> None <input type="radio"/> Read <input type="radio"/> Read/Write <input type="radio"/> Custom	
Network	<input checked="" type="radio"/> None <input type="radio"/> Read <input type="radio"/> Read/Write <input type="radio"/> Custom	
System	<input checked="" type="radio"/> None <input type="radio"/> Read <input type="radio"/> Read/Write <input type="radio"/> Custom	
Security Profile	<input checked="" type="radio"/> None <input type="radio"/> Read <input type="radio"/> Read/Write <input type="radio"/> Custom	
VPN	<input checked="" type="radio"/> None <input type="radio"/> Read <input type="radio"/> Read/Write	
WAN Opt & Cache	<input checked="" type="radio"/> None <input type="radio"/> Read <input type="radio"/> Read/Write	
WiFi & Switch	<input checked="" type="radio"/> None <input type="radio"/> Read <input type="radio"/> Read/Write	

Permit usage of CLI diagnostic commands:

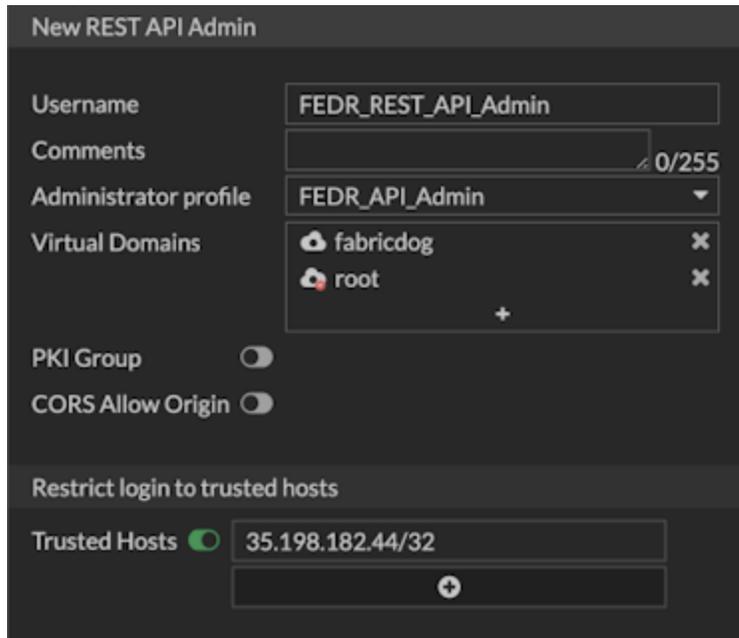
Scope: Virtual Domain Global

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:



The screenshot shows the 'New REST API Admin' configuration interface. The fields are as follows:

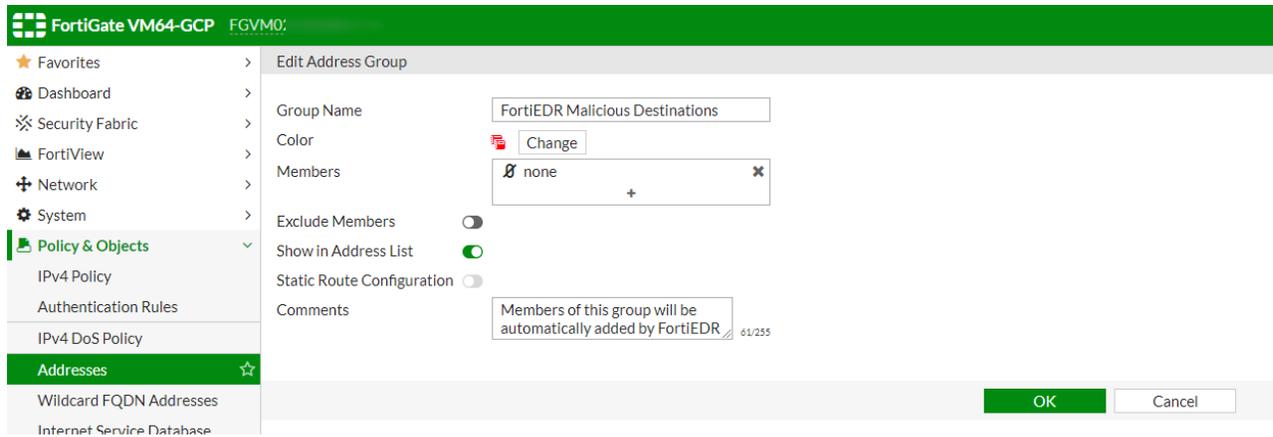
- Username:** FEDR_REST_API_Admin
- Comments:** 0/255
- Administrator profile:** FEDR_API_Admin
- Virtual Domains:** fabricdog, root
- PKI Group:** Disabled
- CORS Allow Origin:** Disabled
- Restrict login to trusted hosts:** Enabled
- Trusted Hosts:** 35.198.182.44/32

- 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*.

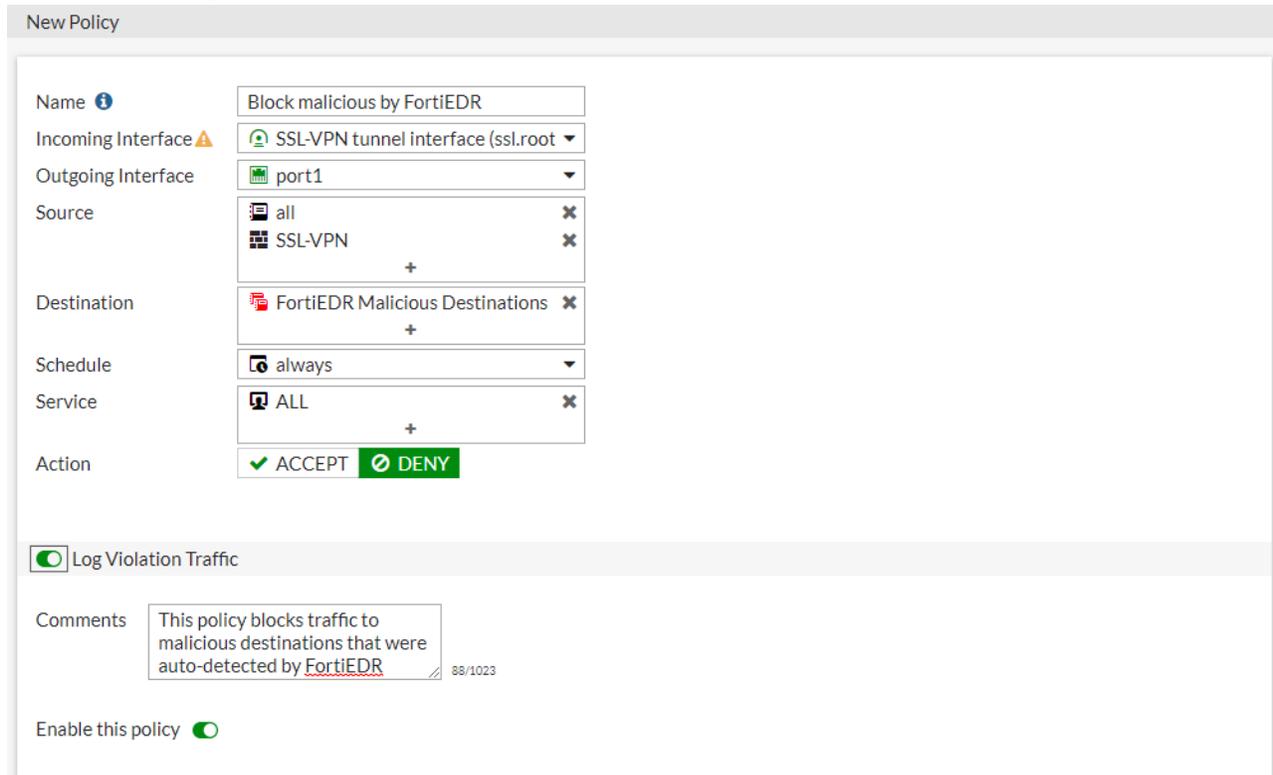
An API token is generated. Make note of the token, as it is only shown once and you will need to provide it when [Configuring FortiEDR on page 11](#).

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.



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.

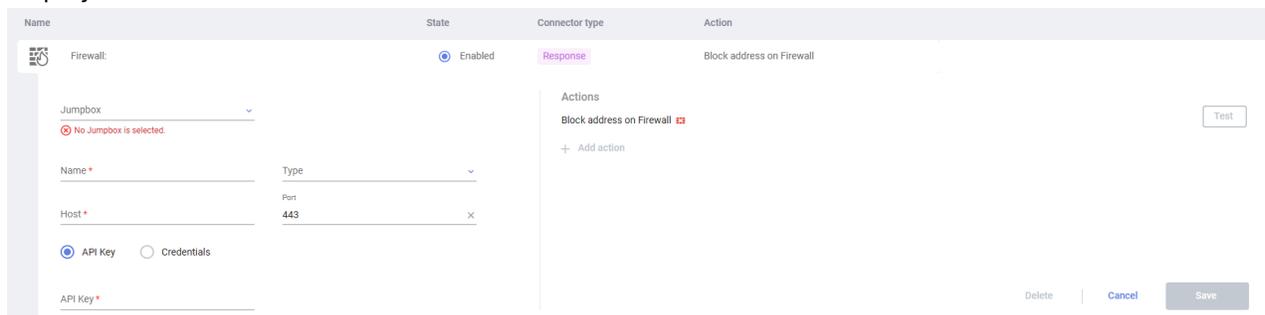


Configuring FortiEDR

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:

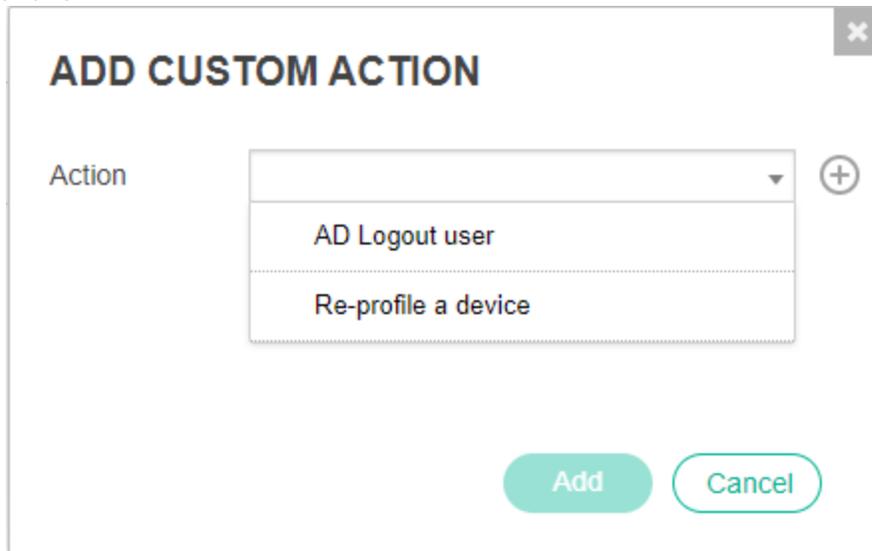


2. Fill in the following fields:

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 <i>FortiGate</i> in the dropdown list. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> <p>Type FortiGate ▾</p> <p>CheckPoint</p> <p>Cisco</p> <p>✓ FortiGate</p> <p>FortiManager</p> <p>PaloAlto</p> </div>
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 <i>API Key</i> 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:

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	<p>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 <i>Action Scripts</i> 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.</p> <div data-bbox="651 562 1435 1178" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p>Creating A Custom Incident Response Action ×</p> <p>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.</p> <p>Code Conventions</p> <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> ◦ 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. <p style="text-align: center;"> ↓ custom_script.py ↓ config.json </p> <p>Troubleshooting</p> <p>Script execution (either in test mode or as part of a realtime incident response) is defined as</p> <p style="text-align: right;">Close</p> </div>

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	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Delete file	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Clean persistent data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Block address on Firewall	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Test playbook	<input checked="" type="checkbox"/>				
<input type="checkbox"/>	Victims Playbook	<input checked="" type="checkbox"/>				
<input type="checkbox"/>	Victims Playbook clone	<input checked="" type="checkbox"/>				

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	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Delete file	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Clean persistent data	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Block address on Firewall	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Reset user password	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

CUSTOM	
Send to FortiSandbox	<input type="checkbox"/> Select All <input checked="" type="checkbox"/> nmoore_FGT <input type="checkbox"/> nmoore_FMG

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 *Incidents* page of the FortiEDR Console.

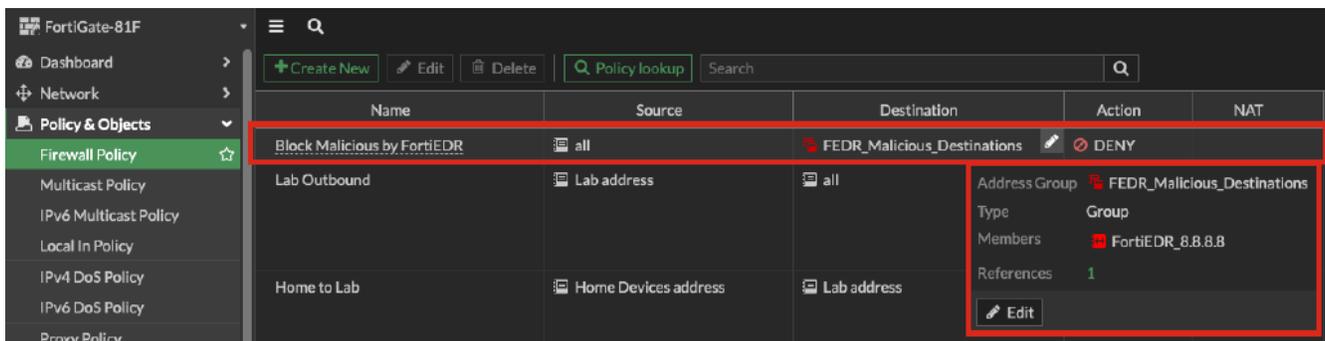
Verifying the integration

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 *Incidents* page, 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.



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

Verifying the integration

The screenshot shows the FortiGate configuration interface for an address group named 'FortiEDR_8.8.8.8'. The configuration includes the name, color, type (IP Range), IP Range (8.8.8.8-8.8.8.8), and interface (any). The comments field contains 'FortiEDR Event ID - 22502717'. Below the configuration, the event log shows a 'Malicious' event for the process 'ConnectivityTestAppNe...' on device 'labdog-win11' at destination '8.8.8.8'. The event details show the threat name 'tool', threat family 'Faketool', and threat type 'Tool'. The history shows that the IP '8.8.8.8' was added to the malicious IP addresses on the firewall 'FortiGate' on 20-Apr-2023, 12:21:26.

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\nmooore	8.8.8.8	14-Apr-2023, 12:30:34	20-Apr-2023, 12:21:17	LABDOG\nmooore	43

Malicious runner
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 nmooore_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  
Request timed out.  
Request timed out.  
Request timed out.  
Request timed out.
```



www.fortinet.com

Copyright© 2025 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.