

A decorative pattern of overlapping, multi-lined hexagons in a light blue color, set against a dark blue background, located at the top of the page.

FortiNAC - FortiDeceptor Integration Guide

Version 7.2 F



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<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>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com

December 7, 2023

FortiNAC 7.2 F FortiDeceptor Integration Guide

49-922-769106-20211216

TABLE OF CONTENTS

Overview	4
What it Does	4
Requirements	4
Step 1: Generate the Authorization Token in FortiNAC	5
Step 2: Configure the GEN-WEBHOOK in FortiDeceptor	6
Validate	8

Overview

This document provides guidance on integrating FortiDeceptor with FortiNAC.

What it Does

FortiDeceptor is based on deception technology that complements an organization's existing breach protection strategy designed to deceive, expose, and eliminate attacks originating from either external or internal sources before any real damage occurs.

FortiNAC is the Fortinet network access control solution. It enhances the overall Fortinet Security Fabric with visibility, control, and automated response for everything that connects to the network. FortiNAC provides protection against IoT threats, extends control to third-party devices, and orchestrates automatic responses to a wide range of networking events.

FortiDeceptor from V.3.2 provides the capability to integrate with third-party security tools using the GEN WEBHOOK as part of the "integrated devices" feature for alert mitigation.

The integration between FortiDeceptor and FortiNAC allows us to automatically isolate any infected device from the network based on FortiDeceptor alert detection.

One of the compelling use cases for this integration is Ransomware mitigation using SMB Deception Token by luring the ransomware to encrypt fake files and raise alerts. Fortideceptor will use FortiNAC to isolated the infected endpoint from the network automatically and save the network damage.

Requirements

FortiNAC

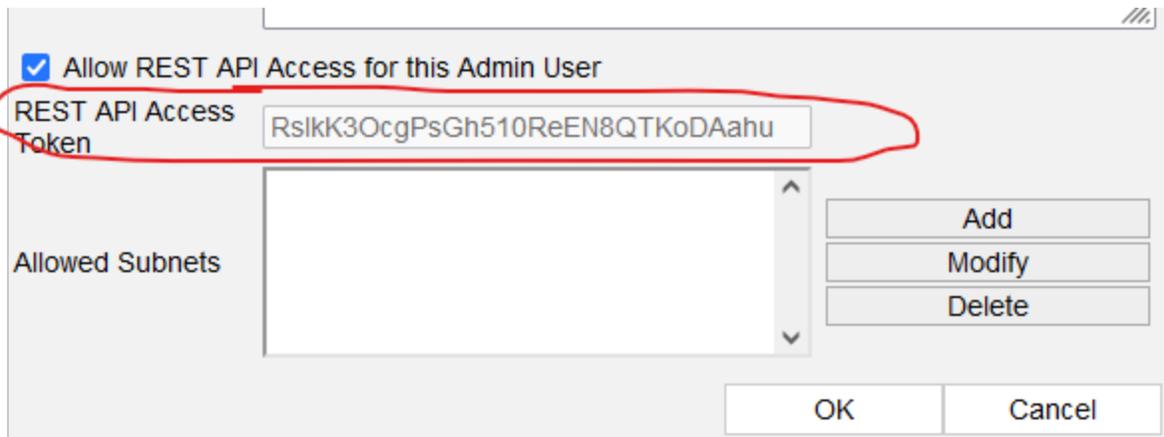
Minimum software version: 8.8 and greater

FortiDeceptor

Supported firmware version: v3.2 and greater

Step 1: Generate the Authorization Token in FortiNAC

1. Log in to the FortiNAC Administration UI.
2. Navigate to **Users & Hosts > Hosts**.
3. Create a new Admin User with REST API access and copy the Authorization token. For instructions see [Add an Administrator](#) in the Administration Guide.



The screenshot shows a configuration window for an Admin User. At the top, there is a checkbox labeled "Allow REST API Access for this Admin User" which is checked. Below this, the "REST API Access Token" field is highlighted with a red circle and contains the value "RslkK3OcgPsGh510ReEN8QTKoDAahu". To the left of the token field is the label "REST API Access Token". Below the token field is a list box labeled "Allowed Subnets" which is currently empty. To the right of the list box are three buttons: "Add", "Modify", and "Delete". At the bottom of the window are "OK" and "Cancel" buttons.

Step 2: Configure the GEN-WEBHOOK in FortiDeceptor

1. Access the FortiDeceptor Admin console. (https://IP_ADDRESS)
2. Click on **Fabric-> Integration Devices** to configure the gen-webhook.
3. Click on “+integrate with new device”.
4. Configure the WEBHOOK parameters for FortiNAC using the table below.

Block Action

Expiry	3600
Http Method	POST
URL	'https://IP_ADDRESS:8443/api/v2/host/enable-by-ip
Authorization	<Insert the Authorization token here>
HTTP Header	blockheader :: Empty
HTTP Data	ip :: Hacker-IP

Unblock Action

Expiry	3600
Http Method	POST
URL	'https://IP_ADDRESS:8443/api/v2/host/disable-by-ip
Authorization	<Insert the Authorization token here>
HTTP Header	blockheader :: Empty
HTTP Data	ip :: Hacker-IP

Step 2: Configure the GEN-WEBHOOK in FortiDeceptor

Integrate With New Device
✕

Block Action:

Expiry: seconds

Http Method:

URL:

Authorization:

HTTP Header: : ▼ 🗑️ +

HTTP Data: : ▼ 🗑️ +

Unblock Action:

Http Method:

URL:

Authorization:

HTTP Header: : ▼ 🗑️ +

HTTP Data: : ▼ 🗑️ +

+ Integrate With New Device						
Action	Enabled	Status	Name	Integrate Method	Severity	Detail
Edit Delete	✖	🕒 Unchecked	fgtblocker	FGT-REST-API	Critical	IP: 172.16.69.70; Username: admin; Password: *****; Port: 443; Expiry: 360; Vdom: root;
Edit Delete	✖	🕒 Unchecked	fgtwebhook	FGT-WEBHOOK	Low	<p>Block URL: https://172.16.69.66/api/v2/monitor/system/automation-stitch/webhook/crystal_ipblocker; Expiry: 61; Authorization: zsdph8QheShN0kczQw5Hq94dtkHG;</p> <p>Unblock URL: https://172.16.69.66/api/v2/monitor/system/automation-stitch/webhook/crystal_ipunblocker; Authorization: zsdph8QheShN0kczQw5Hq94dtkHG;</p>
Edit Delete	✖	🕒 Unchecked	pan	PAN-XMLAPI	Low	Device IP: 2.2.2.2; Port: 443; Username: wwwwww; Password: *****; Expiry: 7200;
Edit Delete	✔	🟢 Ready	fortinac	GEN-WEBHOOK	Low	<p>Block URL: https://172.16.69.51:8443/api/v2/host/enable-by-ip; HttpMethod: POST; Expiry: 3600; Authorization: 1YNLHddjCmAG9ryBn5Jpppl8rOKFQw; Header: [blockheader: Empty,]; Data: [ip: Hacker-IP,].</p> <p>Unblock URL: https://172.16.69.51:8443/api/v2/host/disable-by-ip; HttpMethod: POST; Authorization: 1YNLHddjCmAG9ryBn5Jpppl8rOKFQw; Header: [whunblockheader: Empty,]; Data: [ip: Hacker-IP,].</p>

Validate

FDC <-> FNAC - Attack Simulation

Use two network desktops: One for accessing the Fortideceptor & FortiNAC and the second for the attack simulation.

1. Access the FortiDeceptor Admin console. (https://IP_ADDRESS)
2. Click **Deception > Decoy & Lure Status** and identify a Decoy IP you are willing to attack (example: choose a windows decoy with SMB enabled).
3. Log in the FortiNAC Administration UI.
4. Navigate to **Users & Hosts > Hosts**.
5. Search for the “attacker endpoint” IP address and confirm it is connected to a port or SSID that is under enforcement.
6. Log into the “attacker endpoint” machine and access the windows Decoy IP network share to generate an alert.

The “attacker endpoint” will get isolated from the network automatically by the FortiNAC.

In the FortiDeceptor Admin console, verify that Fortideceptor raised an alert under incident analysis. Navigate to Fabric > quarantine status to confirm that FortiDeceptor sent a quarantine command to FortiNAC.



Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, 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 General Counsel, 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. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. 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.