



FortiNAC - FortiSIEM Device Integration

Version 9.2



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 5, 2022

FortiNAC 9.2 FortiSIEM Device Integration

49-922-769106-20211216

TABLE OF CONTENTS

Overview	4
FortiSIEM Integration	5
Configure FortiSIEM	5
Configure FortiNAC	6

Overview

The information in this document provides guidance for configuring the XXXX device to be managed by FortiNAC. This document details the items that must be configured.

Note: As much information as possible about the integration of this device with FortiNAC is provided. However, the hardware vendor may have made modifications to the device's firmware that invalidate portions of this document. If having problems configuring the device, contact the vendor for additional support.

Tip: For hyperlinks referencing other documentation, right-click the link and select **Open in New Tab**.

What it Does

FortiSIEM generates incidents when logs are received that match rules configured in the system. These logs can be from any supported device. When an incident is generated, FortiSIEM can forward the incident details to FortiNAC for enforcement.

FortiNAC parses the incident received from FortiSIEM, and uses the parsed data to generate a security event. These security events can then be used by FortiNAC to trigger an automated or manual action, such as a device quarantine.

In return, FortiNAC can send logs back to FortiSIEM via Syslog. These can be parsed by FortiSIEM and stored along with other events for inclusion in dashboards, reports, analytics and rules.

This flexible integration allows FortiSIEM and FortiNAC to work together to action events from across the network.

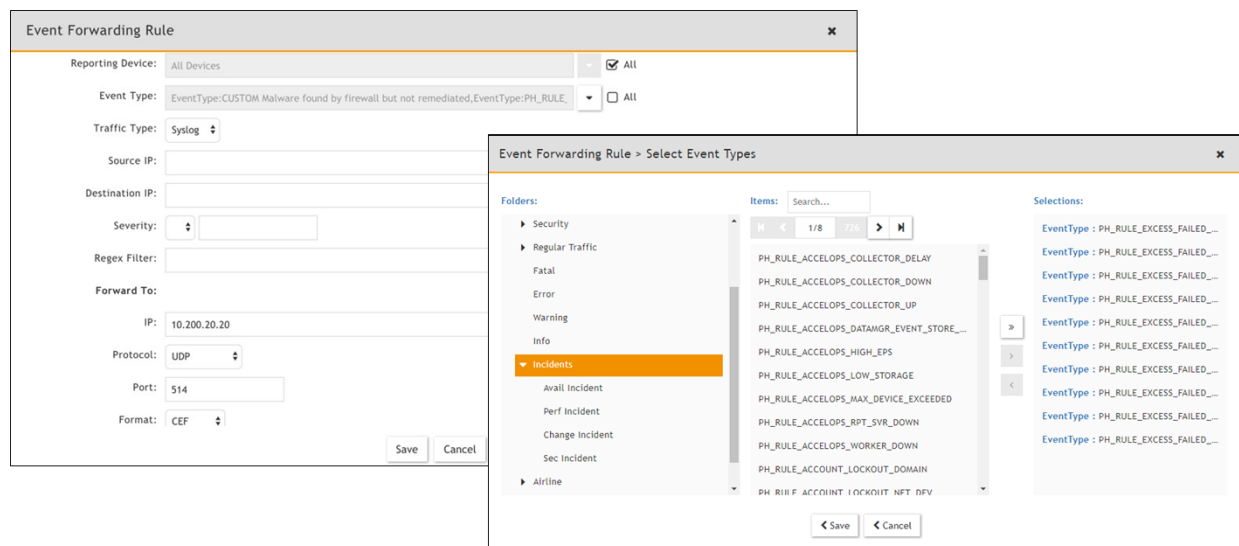
FortiSIEM Integration

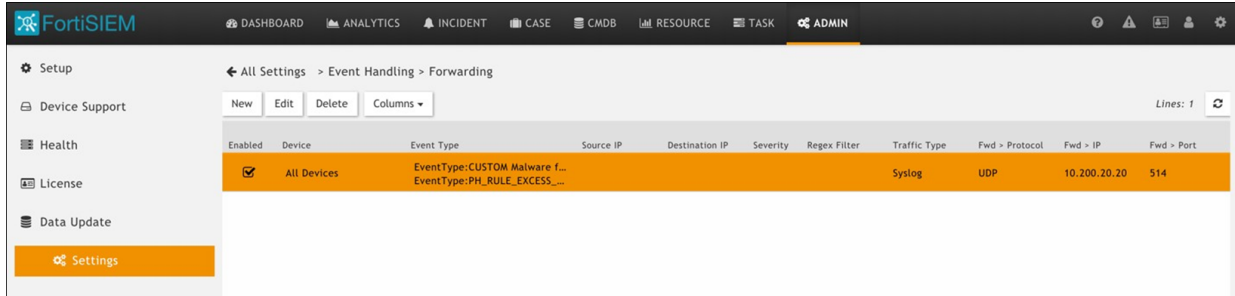
Configure FortiSIEM

Configure FortiSIEM to forward the events generated by security incidents to FortiNAC.

1. Navigate to **Admin > Settings > Event Handling > Forwarding**.
2. Create **New Rule**.
3. Select the Reporting Device or **All Devices**.
4. Select Event Type:
 - a. Navigate to the 'Incidents' event type group.
 - b. Choose the incidents that should be forwarded to FortiNAC from the list.

Note: In FSM 5.2.1 the individual incidents must be selected. Selecting the group does not work.
5. Set **Traffic Type** to Syslog.
6. Under **Forward To**:
 - **IP:** FortiNAC ETH0 IP address
 - **Protocol:** UDP
 - **Port:** 514
 - **Format:** CEF
7. Click **Save**.
8. Ensure the Enabled check box is ticked.





Configure FortiNAC

1. Create new security event parser for FortiSIEM as follows:
 - a. Navigate to **System > Settings > System Communication > Security Event Parsers**.
 - b. Create **New** Parser. For instructions see [Security event parsers](#) in the Administration Guide.
 - Name: FortiSIEM
 - Vendor: Fortinet
 - Format: CEF
 - Data Fields:

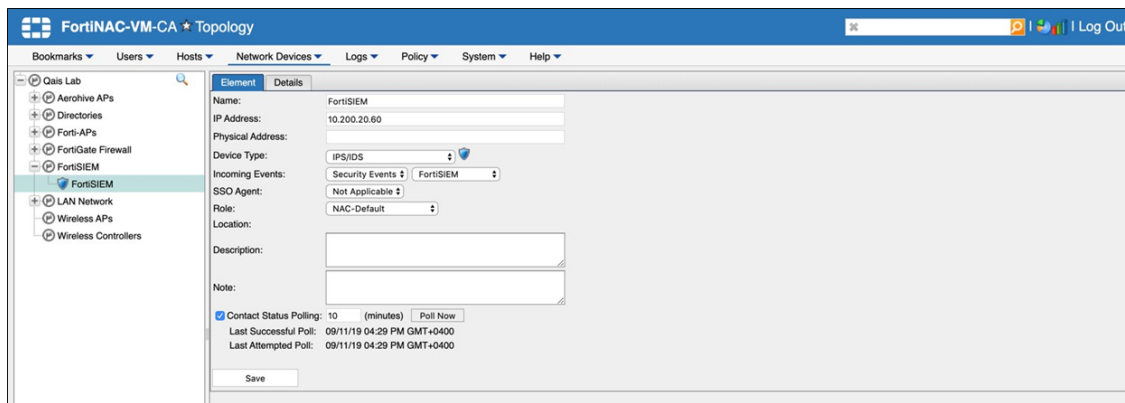
Source IP Column/Tag:	Entire Column/Tag	SRC
Destination IP Column/Tag:	Entire Column/Tag	DST
Type Column/Tag:	Entire Column/Tag	DEVICEPRODUCT
Subtype Column/Tag:	Entire Column/Tag	RULENAME
Threat ID Column/Tag:	Entire Column/Tag	RT
Description Column/Tag:	Entire Column/Tag	INCIDENTDETAIL
Severity Column/Tag:	Entire Column/Tag	SEVERITY

- Severity Mapping:

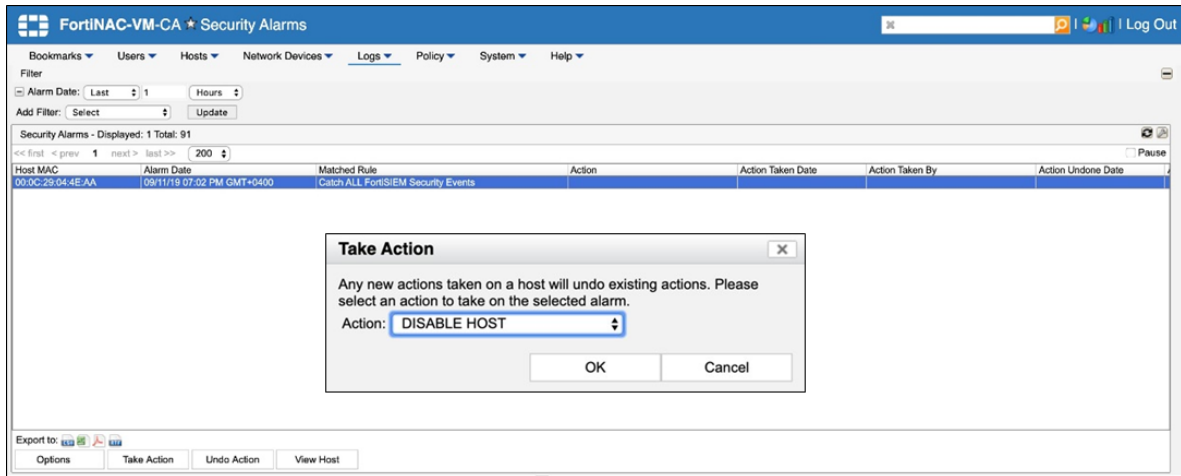
Source Value	Severity Value
1	1
2	2
3	3
4	4
5	5
6	6
7	7

Source Value	Severity Value
8	8
9	9
10	10

2. In order to parse the received Security Events from FortiSIEM, add FortiSIEM as pingable device in Inventory.
 - a. Navigate to **Network > Inventory**.
 - b. Select a **Container** from the left side panel.
 - c. Click **Add Pingable**
 - **Name:** FortiSIEM
 - **IP Address:** FortiSIEM IP Address
 - **Physical Address:** FortiSIEM MAC address
 - **Device Type:** IPS/IDS
 - **Incoming Events:** Security Event >> FortiSIEM
 - **Save**



3. Create new Security Rule to catch all the incoming security events from FortiSIEM.
 - a. Navigate to **Logs > Security Incidents > Rules**.
 - b. Create new Rule. For instructions see [Add or modify a security rule](#) in the Administration Guide.
 - **Enable** the Rule.
 - **Name:** any, example: “Catch ALL FortiSIEM Security Events”.
 - **Trigger:** Create New Trigger:
 - Vendor: Fortinet
 - Type: FortiSIEM
 - **User/Host Profile:** None
 - **Action:** None
4. To view security events, go to **Logs > Security Incidents > Events**. For details see [Security events](#) in the Administration Guide.
5. Create and manage security rules based on triggers that correlate incoming events from FortiSIEM. When a security event is received, the highest ranked security rule with a trigger satisfied and a matching User/Host profile creates a security alarm. The rule may then take an action automatically or manually.





Copyright© 2022 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.