observe IT
a proofpoint company

McAfee Integration Guide

Table of Contents

observe IT
a proofpoint company

Overview

This document describes the ObserveIT integration with McAfee Enterprise Security Management (ESM),

McAfee ESM is a security information and event management (SIEM) solution used to prioritize, investigate, and respond to threats.

This integration provides security analysts and security investigation teams with powerful user-activity metadata and smart user behavior alerts.

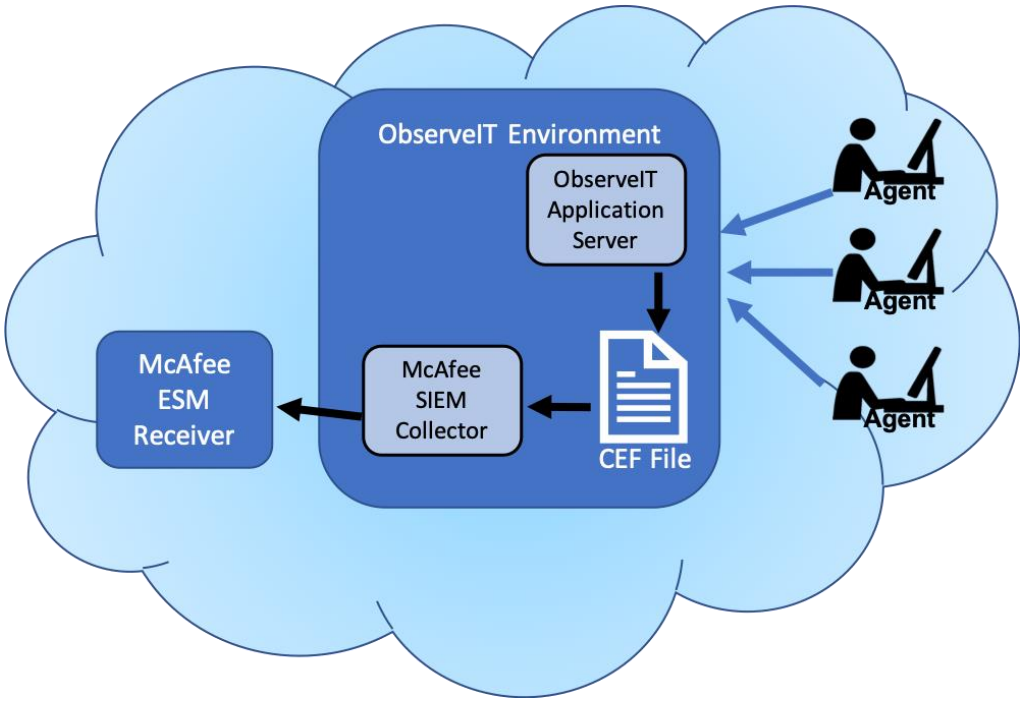
Prerequisites

The ObserveIT integration is generally available in ESM. If you don't see the ObserveIT data source available, you will need to update your rule signatures.

- ObserveIT (Minimum supported version: 7.4)
- McAfee ESM (Minimum supported version: 11)
- McAfee SIEM Collector installed alongside ObserveIT Application Server

Deployment Architecture

This diagram shows how ObserveIT and McAfee ESM integrate.

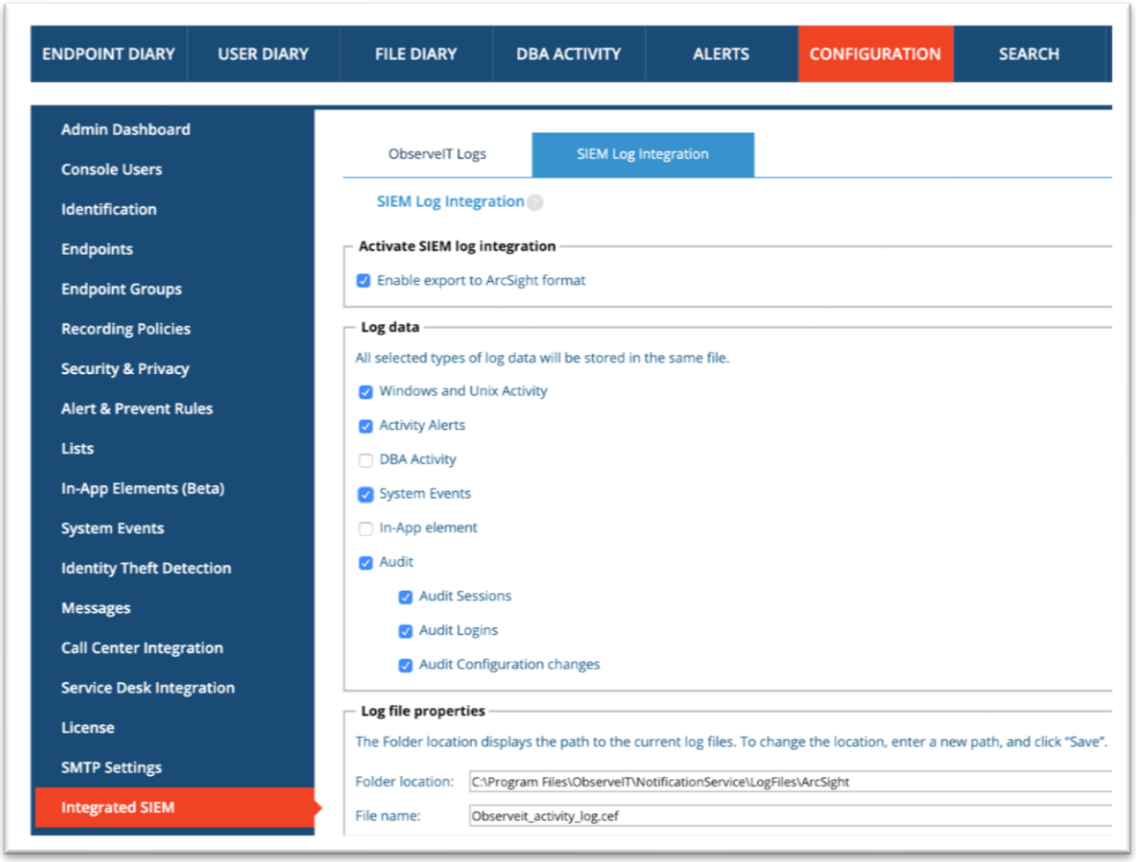


1. Software agents capture user activity data and send it to the ObserveIT Application server.
2. ObserveIT Application server sends the user activity logs in an ArcSight Common Event Format (CEF) file to McAfee SEIM Collector.
3. McAfee SIEM Collector forwards the events from the ObserveIT SIEM logs into McAfee ESM.

ObserveIT Configuration

To configure ObserveIT configuration for integration with McAfee:

- Enable the integrated SIEM logs by selecting the logs you want McAfee to ingest. Windows and Unix Activity, Activity Alerts, System Events and Audit logs are supported.

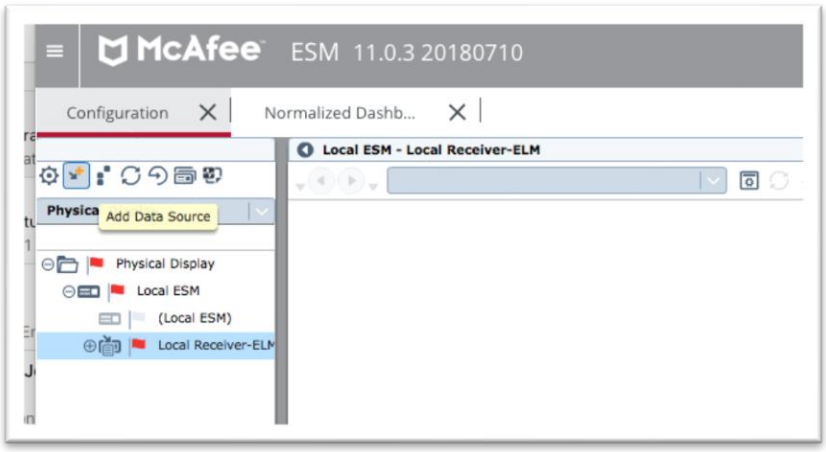


- Enabling the file clean-up process to run every hour. This prevents the log file from becoming too large by deleting the older events and leaving the newer ones.

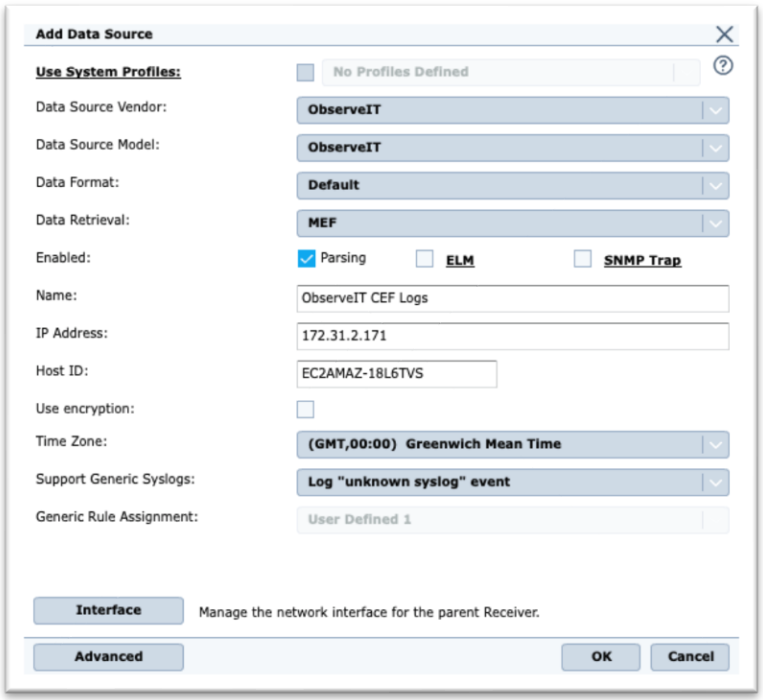
McAfee ESM Configuration

To configure McAfee ESM:

- Make sure you have a Local Receiver configured in McAfee ESM to receive the events being sent by the SIEM collector.



- Add an ObserveIT Data Source, configured as shown below. Specify the IP Address or Host ID with the location of the ObserveIT application server where the SIEM Log Collector runs.



Note: If ObserveIT Data Source type is not available, make sure you have updated your ESM to include the latest rule signature updates.

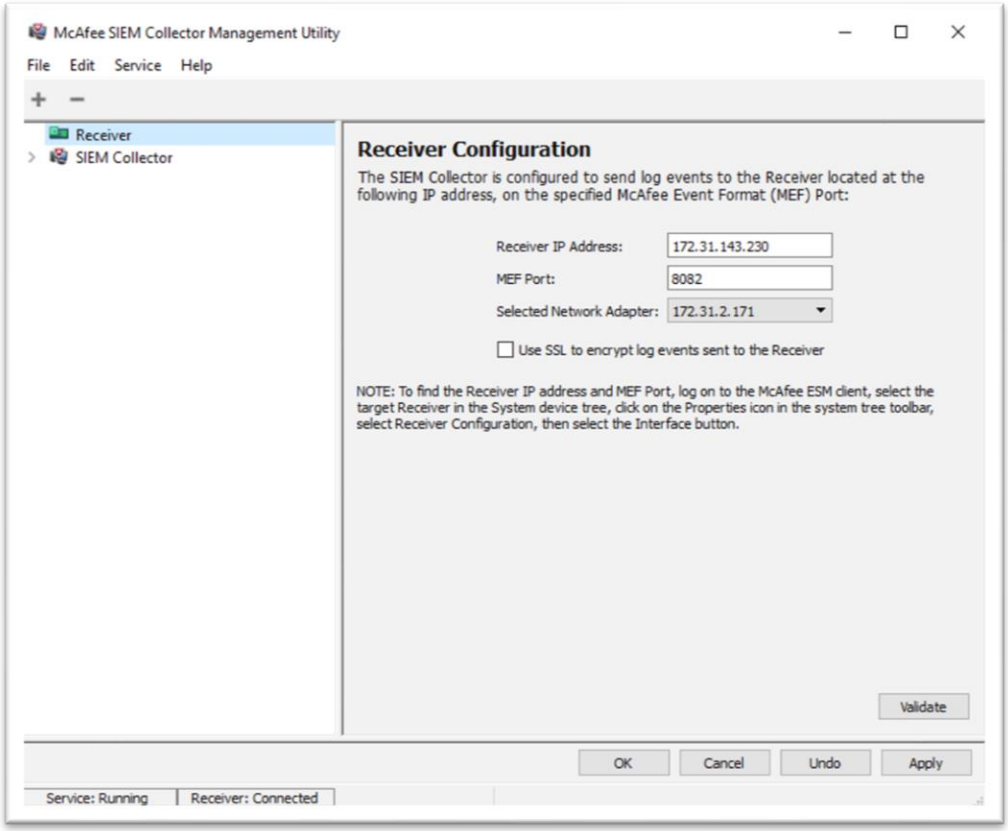
- Roll out the policy to all devices when the Data Source is created and you are prompted.

McAfee SIEM Collector Configuration

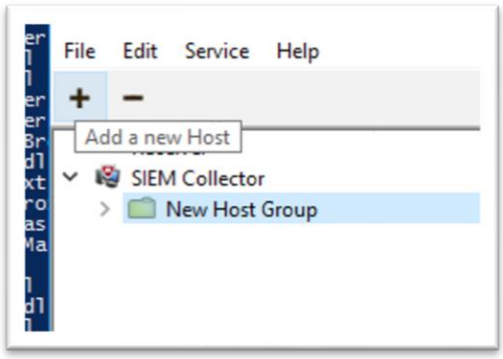
The McAfee SIEM Collector is used to forward the events from the ObserveIT SIEM logs into McAfee ESM.

- To configure McAfee SIEM Collector:
- Install the McAfee SIEM Collector Management Utility on your ObserveIT application server(s).
- Configure the collector to communicate with the ESM Receiver. Enter the receiver's IP address and port (default is 8082).

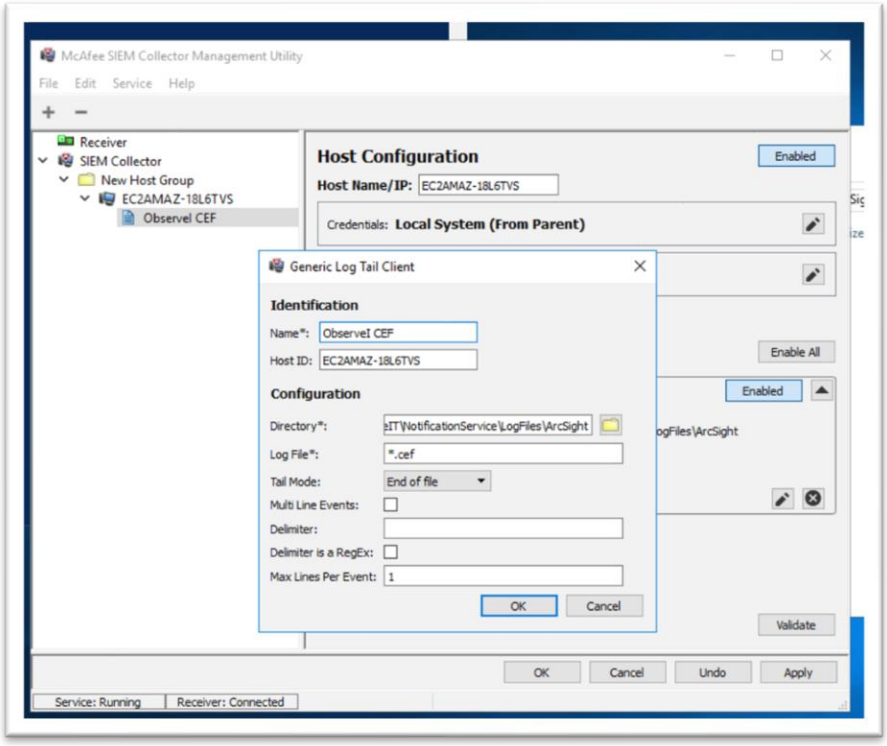
Note: **Receiver: Connecte**d in the bottom- left indicates a successful connection.



- Create a new host group and enable it.
- Add a new host to the host group.

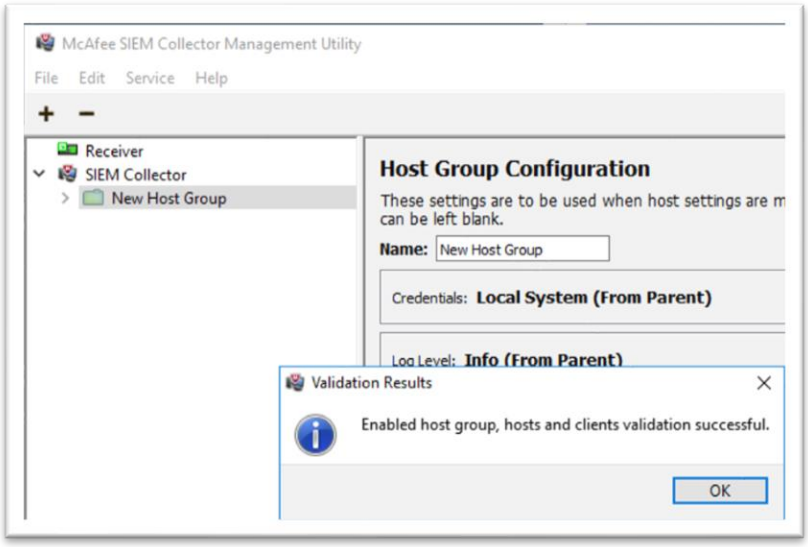


- Configure the new host to read the ObserveIT SIEM log file.
- Enter the **Host Name** of the ObserveIT Application server. Under Clients, select **Generic log tail** from the drop down and click **Add Client**
    - The **Host ID** must match the **Host Name** you entered previously on the **Host Configuration**.
    - The Directory must match what you have configured in the Integrated SIEM log screen in ObserveIT.
    - Use *.cef as the log file name and select **End of file** for tail mode. Other items can be left as default.



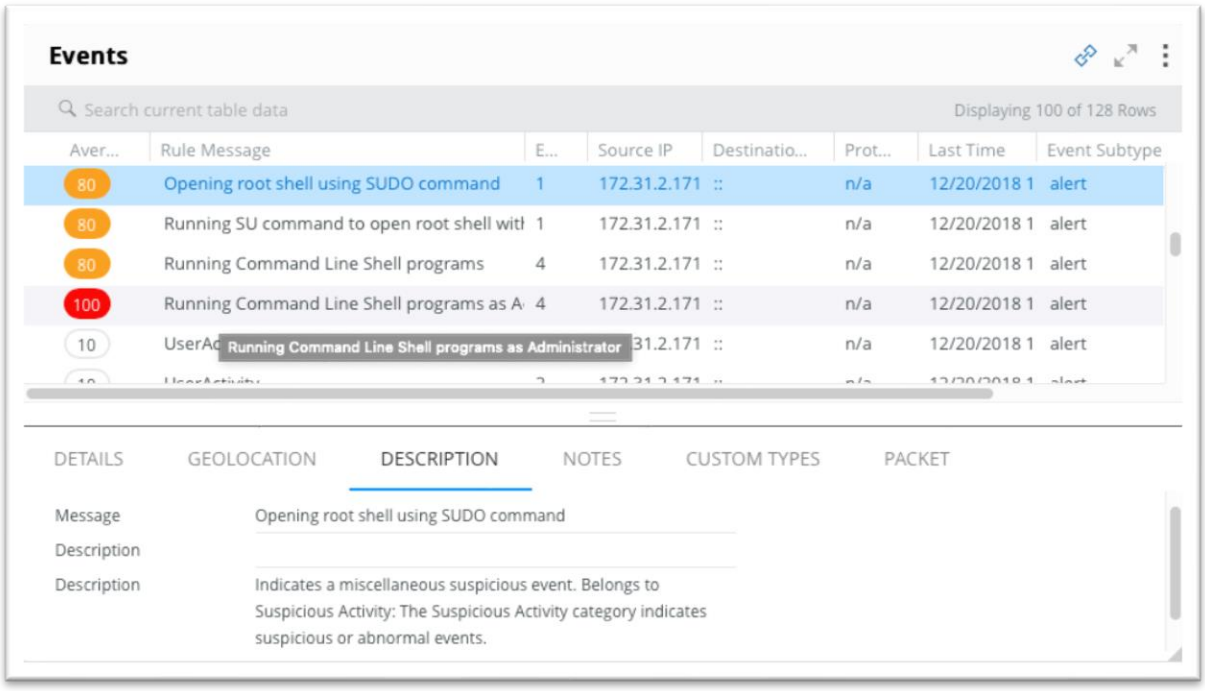
- Set both the Client and the Host to **Enabled**.

- Click on **SIEM Collector** on the left and click the **Validate** button to ensure successful configuration.



Viewing Events

When is configured properly, you will see events flowing into ESM, as shown in the example.

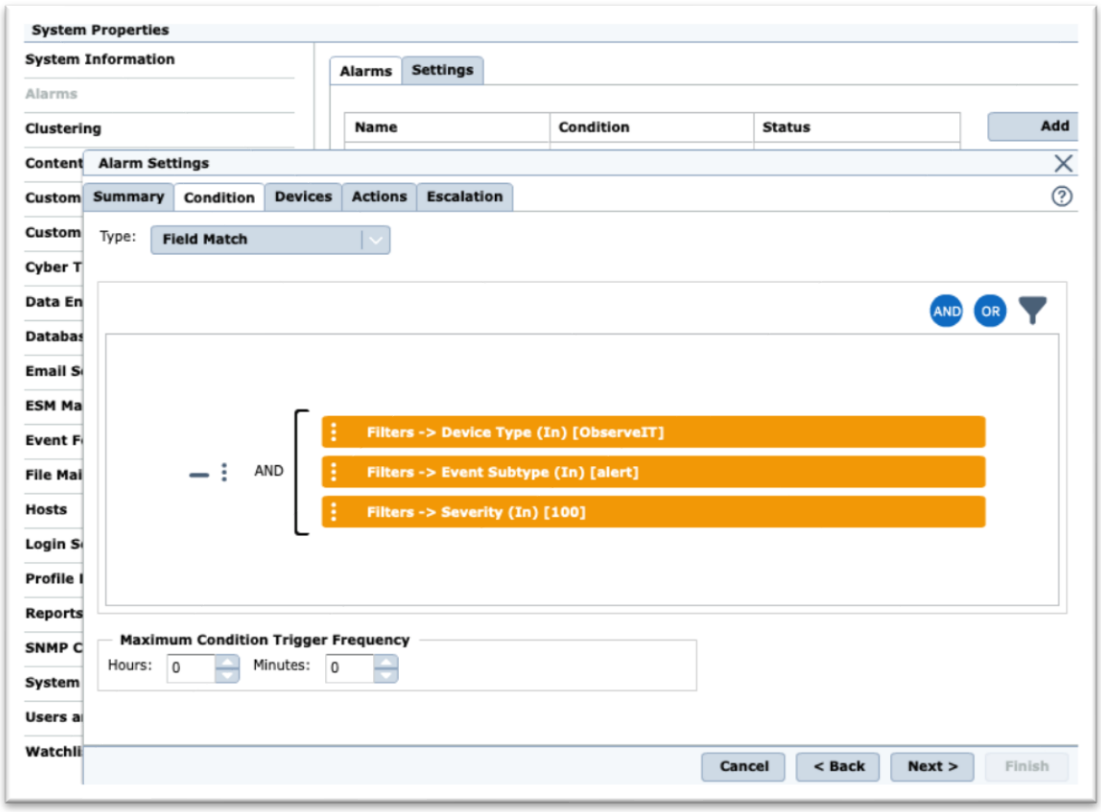


Creating Alarms

You can configure alarms in ESM for certain ObserveIT alerts.

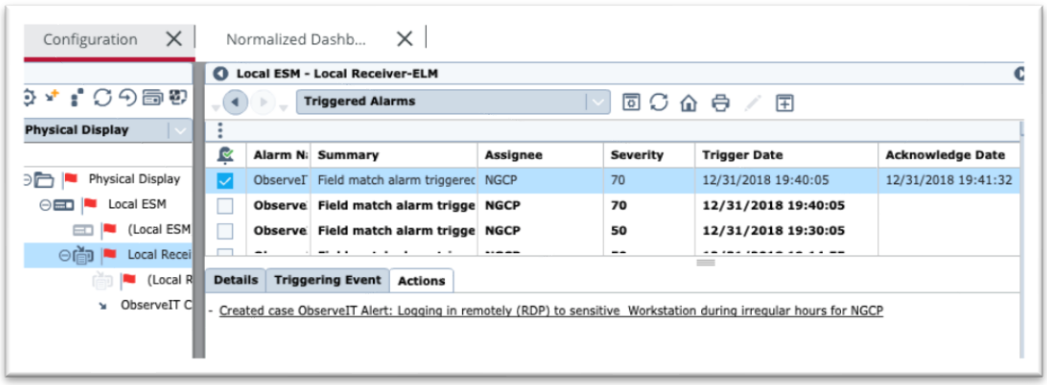
To configure an alarm:

- In the configuration menu in ESM, select Local ESM and open the properties menu.
- Configure an alarm to fire for the ObserveIT device based on field match.



ALARM EXAMPLES

You can automatically create a case for each alert with High or Critical severity level.



If you have the Advanced Correlation Engine Appliance, you can create a rule to group ObserveIT alerts by user. This will then allow you to correlate multiple alerts for the same user into a single alarm.

Support

- For help configuring McAfee ESM or the McAfee SIEM Collector: Consult McAfee Support.
- For help using or configuring the ObserveIT platform: Contact the ObserveIT support organization. https://www.observeit.com/support/

You can also send an email to integrations@observeit.com with questions about this and other ObserveIT integrations.

Not a customer yet? Start your Free Trial of ObserveIT today!

Free Trial

Start your free trial with ObserveIT today. Detect and prevent insider threats in minutes. Reduce your risk, speed up investigations, and streamline compliance.

Release notes

Version	Date	Notes
1.0.0	2018-12-18	• New: ○ Load ObserveIT logs into McAfee ESM • Fixed: N/A • Improved: N/A