observe IT
a proofpoint® company

LogRhythm Integration Guide

Contents

Version 1.0.0 - January 2019

Integration Overview

The LogRhythm integration with ObserveIT provides security analysts and investigation teams with powerful user activity meta-data and smart user behaviour alerts. By correlating this powerful user context with the other data sources in your SIEM, a complete picture of a user's activities emerges, allowing for creation of smarter alerts and quicker threat elimination.

The LogRhythm System Monitor agent will be used to forward the events from the ObserveIT SIEM logs into LogRhythm.

PREREQUISITES

The ObserveIT integration is generally available in LogRhythm.

Update the LogRhythm Knowledgebase to the latest version to ensure the latest log processing policies are installed.

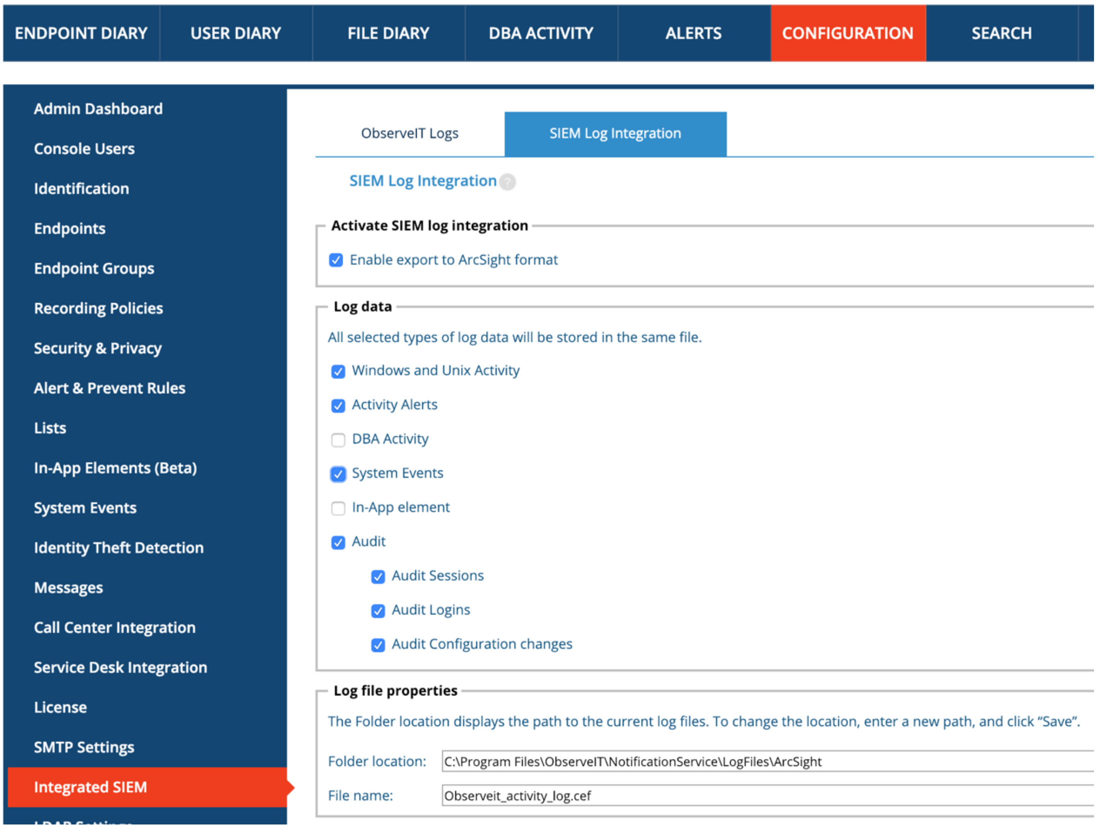
- ObserveIT (Minimum supported version: 7.4)
- LogRhythm (Minimum supported version: 7.x)

LogRhythm System Monitor installed with ObserveIT Application Server or with ObserveIT SIEM logs available remotely.

ObserveIT Configuration

To configure ObserveIT for integration with LogRhythm:

1. From the ObserveIT Web Console, in the **Configuration** tab, select **Integrated SIEM** in the left menu. Select the **SIEM Log Integration tab**.



SIEM Log Integration

Activate SIEM log integration

☑ Enable export to ArcSight format

Log data

All selected types of log data will be stored in the same file.

☑ Windows and Unix Activity
☑ Activity Alerts
☐ DBA Activity
☑ System Events
☐ In-App element
☑ Audit
  ☑ Audit Sessions
  ☑ Audit Logins
  ☑ Audit Configuration changes

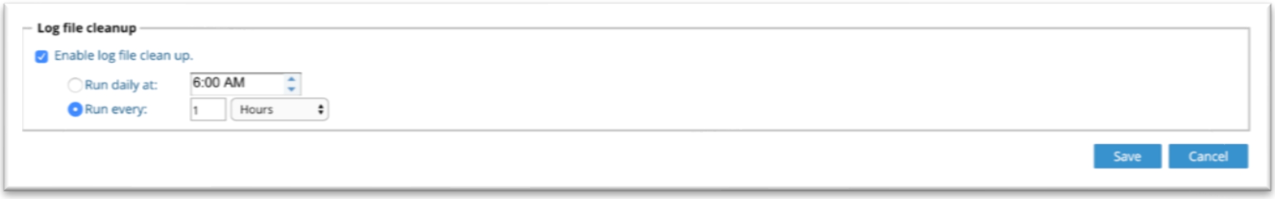
Log file properties

The Folder location displays the path to the current log files. To change the location, enter a new path, and click "Save".

Folder location: C:\Program Files\ObserveIT\NotificationService\LogFiles\ArcSight

File name: Observeit_activity_log.cef

2. Select the logs you want LogRhythm to ingest. The User Activity, Alert, Audit, and Internal Event logs are supported.
3. **Enable export to ArcSight** format must be checked.
4. Enable 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.



Log file cleanup

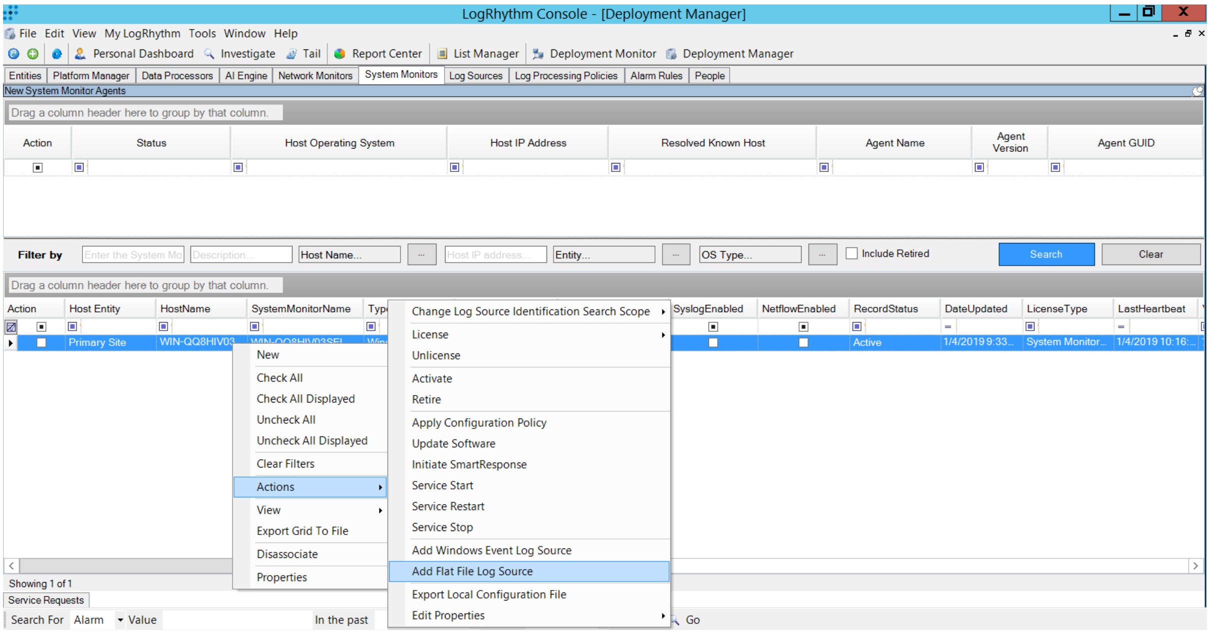
☑ Enable log file clean up.

○ Run daily at: 6:00 AM
● Run every: 1 Hours

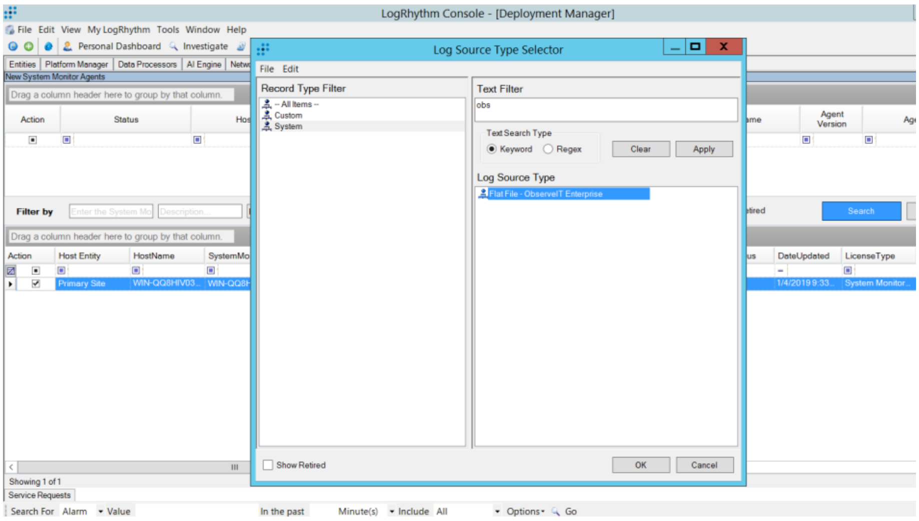
LogRhythm Configuration

As detailed above LogRhythm is configured to read the CEF files generated by the ObserveIT application server.

1. To configure this, navigate to **LR Console** > **Deployment Manager** > **System Monitor**.
2. Check the **System Monitor** agent that is either installed on the ObserveIT or will have access to the CEF files produced.
3. Right-click on the agent and navigate to **Add Flat File Log Source** (see below screenshot).



4. Use the search box to find the ObserveIT Enterprise log source. Highlight this entry and click **OK**.



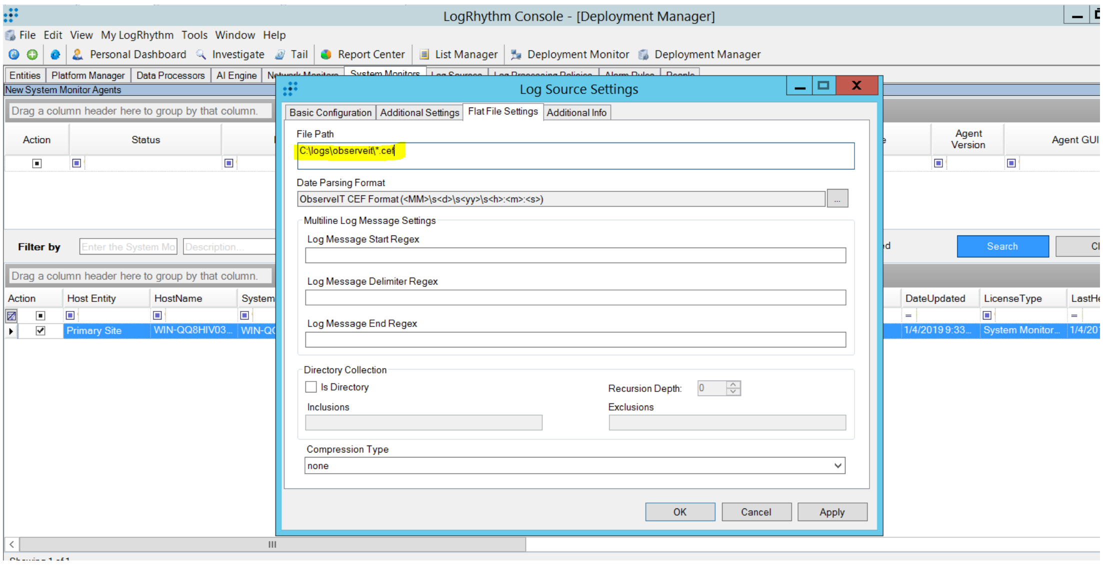
Text Filter: obs

Text Search Type: ● Keyword ○ Regex

Log Source Type: Flat File - ObserveIT Enterprise

5. In the flat file configuration settings, select **Basic Configuration** tab.
6. Change the processing policy to the LogRhythm Default.

7. Click **Flat File Settings** and change the file path to the location of where the .CEF files are being written to, as configured in the ObserveIT Configuration.
8. Click on the ellipses next to the **Date Parsing Format** and add a new entry with the below regex:
   <MM>\s<d>\s<yy>\s<h>:<m>:<s>



File Path: C:\logs\observeit*.cef

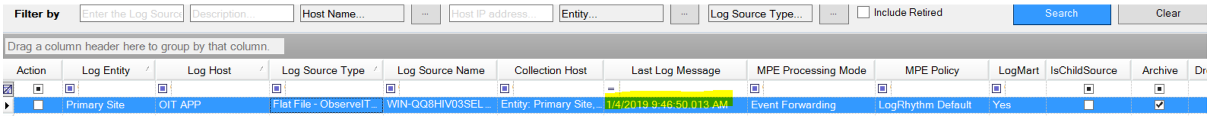
Date Parsing Format: ObserveIT CEF Format (<MM>\s<d>\s<yy>\s<h>:<m>:<s>)

Multiline Log Message Settings
Log Message Start Regex:
Log Message Delimiter Regex:
Log Message End Regex:

Directory Collection
□ Is Directory
Recursion Depth: 0
Inclusions:
Exclusions:

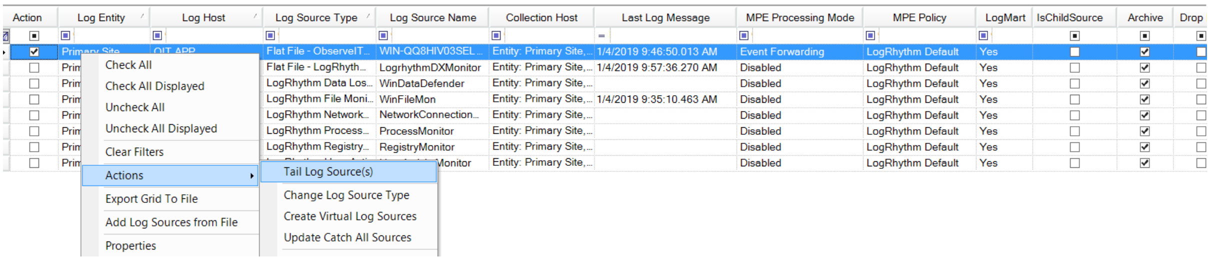
Compression Type: none

9. Wait a few minutes and verify that the last log message is updating (**Deployment Manager** > **Log Sources**).



Action	Log Entity	Log Host	Log Source Type	Log Source Name	Collection Host	Last Log Message	MPE Processing Mode	MPE Policy	LogMart	IsChildSource	Archive
□	Primary Site	OIT APP	Flat File - ObserveIT...	WIN-QQ8HIV03SEL...	Entity: Primary Site,...	1/4/2019 9:46:50.013 AM	Event Forwarding	LogRhythm Default	Yes	□	☑

10. You can also select to **Tail Log Sources** to ensure that new entries are being parsed.

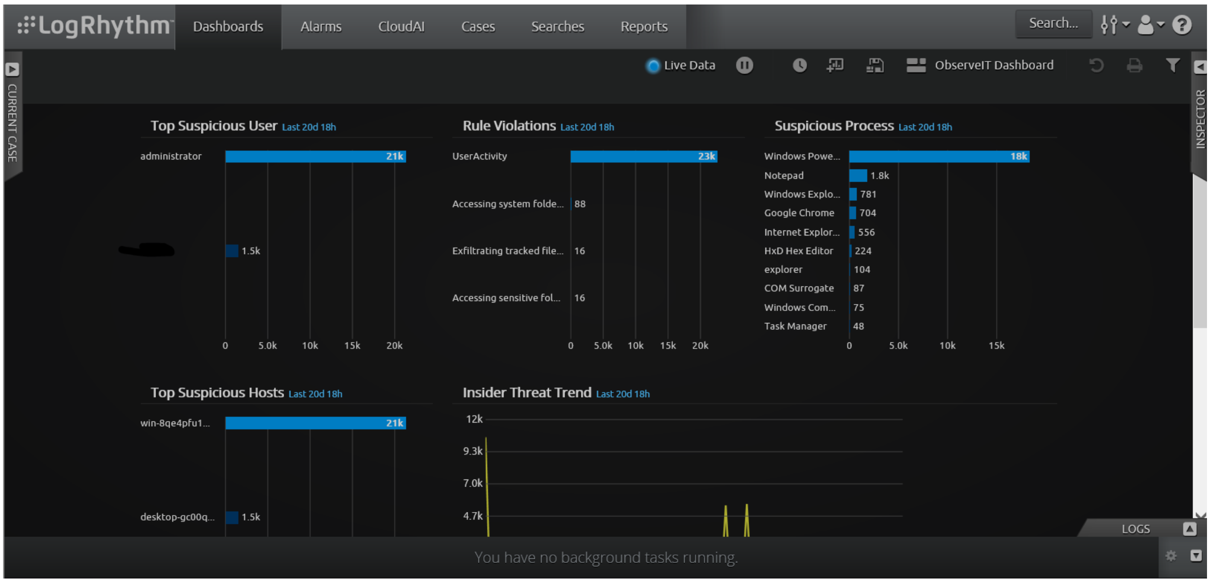


Action	Log Entity	Log Host	Log Source Type	Log Source Name	Collection Host	Last Log Message	MPE Processing Mode	MPE Policy	LogMart	IsChildSource	Archive	Drop
☑	Primary Site	OIT APP	Flat File - ObserveIT...	WIN-QQ8HIV03SEL...	Entity: Primary Site,...	1/4/2019 9:46:50.013 AM	Event Forwarding	LogRhythm Default	Yes	□	☑	□
□	Prim		Flat File - LogRhyth...	LogrhythmDXMonitor	Entity: Primary Site,...	1/4/2019 9:57:36.270 AM	Disabled	LogRhythm Default	Yes	□	☑	□
□	Prim		LogRhythm Data Los...	WinDataDefender	Entity: Primary Site,...		Disabled	LogRhythm Default	Yes	□	☑	□
□	Prim		LogRhythm File Moni...	WinFileMon	Entity: Primary Site,...	1/4/2019 9:35:10.463 AM	Disabled	LogRhythm Default	Yes	□	☑	□
□	Prim		LogRhythm Network...	NetworkConnection...	Entity: Primary Site,...		Disabled	LogRhythm Default	Yes	□	☑	□
□	Prim		LogRhythm Process...	ProcessMonitor	Entity: Primary Site,...		Disabled	LogRhythm Default	Yes	□	☑	□
□	Prim		LogRhythm Registry...	RegistryMonitor	Entity: Primary Site,...		Disabled	LogRhythm Default	Yes	□	☑	□
□	Prim			Monitor	Entity: Primary Site,...		Disabled	LogRhythm Default	Yes	□	☑	□

Web UI Configuration

A basic dashboard has been created to provide visualisation of the ObserveIT data. Download the dashboard file and import to the Web UI.

http://files.observeit.com/docs/ObserveIT_Dashboard.wdlt.zip



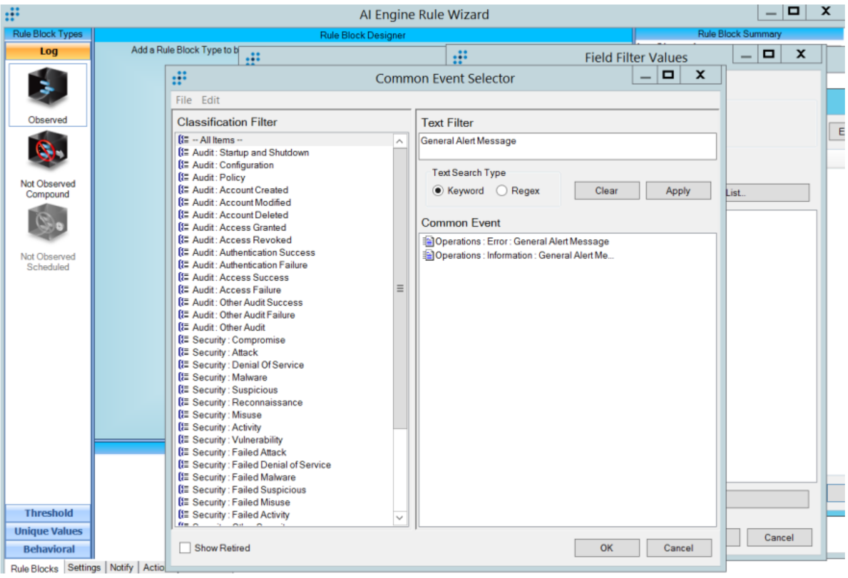
You have no background tasks running.

Creating Alarms

You can configure alarms in LogRhythm for ObserveIT alerts.

To configure an alarm:

- In the **AI Engine** tab, create a new rule, then drag a **Log Observed** Rule Block onto the main working area.
- Set the primary criteria to look for the **Common Event: Error: General Alert Message**.



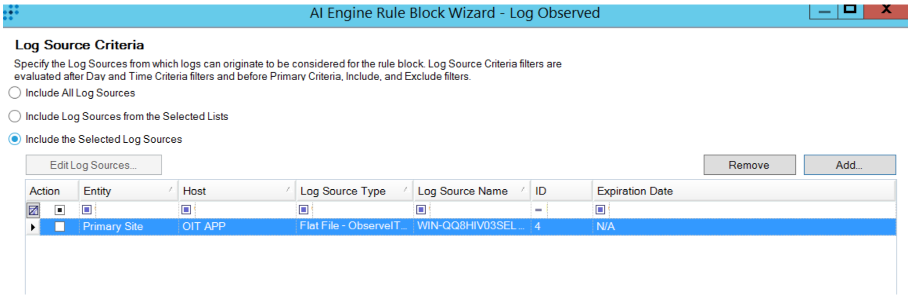
Text Filter: General Alert Message

Text Search Type: ● Keyword ○ Regex

Common Event:
Operations : Error : General Alert Message
Operations : Information : General Alert Me...

□ Show Retired

- In the **Log Source Criteria**, filter by the ObserveIT Log Source.



Log Source Criteria

Specify the Log Sources from which logs can originate to be considered for the rule block. Log Source Criteria filters are evaluated after Day and Time Criteria filters and before Primary Criteria, Include, and Exclude filters.

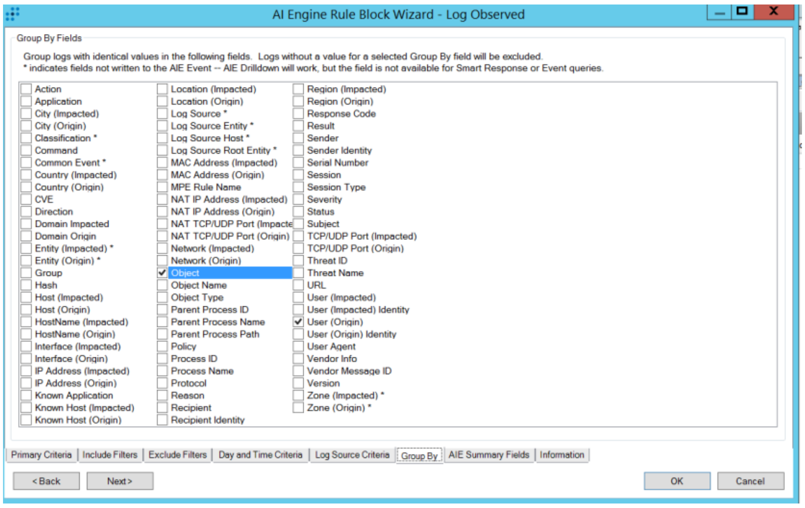
○ Include All Log Sources

○ Include Log Sources from the Selected Lists

● Include the Selected Log Sources

Action	Entity	Host	Log Source Type	Log Source Name	ID	Expiration Date
□	Primary Site	OIT APP	Flat File - ObserveIT...	WIN-QQ8HIV03SEL...	4	N/A

- Group by **User** and **Object**.



Group By Fields

Group logs with identical values in the following fields. Logs without a value for a selected Group By field will be excluded.
* indicates fields not written to the AIE Event -- AIE Drilldown will work, but the field is not available for Smart Response or Event queries.

- □ Action
- □ Application
- □ City (Impacted)
- □ City (Origin)
- □ Classification *
- □ Command
- □ Common Event *
- □ Country (Impacted)
- □ Country (Origin)
- □ CVE
- □ Direction
- □ Domain Impacted
- □ Domain Origin
- □ Entity (Impacted) *
- □ Entity (Origin) *
- □ Group
- □ Hash
- □ Host (Impacted)
- □ Host (Origin)
- □ HostName (Impacted)
- □ HostName (Origin)
- □ Interface (Impacted)
- □ Interface (Origin)
- □ IP Address (Impacted)
- □ IP Address (Origin)
- □ Known Application
- □ Known Host (Impacted)
- □ Known Host (Origin)
- □ Location (Impacted)
- □ Location (Origin)
- □ Log Source *
- □ Log Source Entity *
- □ Log Source Host *
- □ Log Source Root Entity *
- □ MAC Address (Impacted)
- □ MAC Address (Origin)
- □ MPE Rule Name
- □ NAT IP Address (Impacted)
- □ NAT IP Address (Origin)
- □ NAT TCP/UDP Port (Impacte
- □ NAT TCP/UDP Port (Origin)
- □ Network (Impacted)
- □ Network (Origin)
- ☑ Object
- □ Object Name
- □ Object Type
- □ Parent Process ID
- □ Parent Process Name
- □ Parent Process Path
- □ Policy
- □ Process ID
- □ Process Name
- □ Protocol
- □ Reason
- □ Recipient
- □ Recipient Identity
- □ Region (Impacted)
- □ Region (Origin)
- □ Response Code
- □ Result
- □ Sender
- □ Sender Identity
- □ Serial Number
- □ Session
- □ Session Type
- □ Severity
- □ Status
- □ Subject
- □ TCP/UDP Port (Impacted)
- □ TCP/UDP Port (Origin)
- □ Threat ID
- □ Threat Name
- □ URL
- □ User (Impacted)
- □ User (Impacted) Identity
- ☑ User (Origin)
- □ User (Origin) Identity
- □ User Agent
- □ Vendor Info
- □ Vendor Message ID
- □ Version
- □ Zone (Impacted) *
- □ Zone (Origin) *

Support

- For help configuring LogRhythm, consult LogRhythm 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.