

LogRhythm Integration Guide

Contents

Integration Overview	1
Prerequisites	1
ObserveIT Configuration	2
LogRhythm Configuration	.3
Web UI Configuration	4
Creating Alarms	6
Support	7



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.



ObservelT 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**.

ENDPOINT DIARY	USER DIARY	FILE DIARY	DBA ACTIVITY	ALERTS	CONFIGURATION	SEARCH					
Admin Dashboard		ObservelT Log	SIEM Log L	atogration							
Console Users		ObserveIT Logs SIEM Log Integration									
Identification		SIEM Log Integration									
Endpoints		Activate SIEM log i	ntegration								
Endpoint Groups		Enable export to ArcSight format									
Recording Policies		Log data									
Security & Privacy		All selected types of log data will be stored in the same file.									
Alert & Prevent Ru	lles	Vindows and Unix Activity									
Lists		Activity Alerts									
In-App Elements (I	Beta)	DBA Activity									
System Events	/										
Identity Thaft Date	oction	Audit									
identity men bet		Audit Sessions									
Messages		✓ Audit Logins									
Call Center Integra	ation	✓ Audit Configuration changes									
Service Desk Integ	ration	Log file properties									
License		The Folder location	displays the path to the cu	ırrent log files. To char	nge the location, enter a ne	w path, and click "Save".					
SMTP Settings		Folder location: C:	\Program Files\ObserveIT\N	otificationService\LogFile	es\ArcSight						
Integrated SIEM		File name: O	bserveit_activity_log.cef		~						
DAD COMPANY											

- 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.





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).

	•••				LogRhythm Console	e - [Deploym	ent Manager]					_ 0 ×
Image: Second Secon	🗊 File 🛛 Edit	View My Log	Rhythm Tools	Window Help								_ 8 ×
Entities Particut Manager Data Processors Al Engine Network Monitors Log Source Log Processing Policies Allam Rules People Drag a column heeder here to group by that column. Action Status Host Operating System Host IP Address Resolved Known Host Agent Name Agent GUID Image: Status Host Operating System Host IP Address Resolved Known Host Agent Name Agent GUID Image: Status Host Operating System Host IP Address Resolved Known Host Agent Name Agent GUID Image: Status Host Operating System Host IP Address Resolved Known Host Agent Name Agent GUID Image: Status Host Name — Image: Column Name	G G 🙆	2. Personal	Dashboard 🔍 li	nvestigate 📓 Tail 👋 Report	Center 📑 List Manager 🏂 Deploy	ment Monitor	🇊 Deployment N	lanager				
New System Montor Agents Drag a column header here to group by that column. Action Status Host Operating System Host IP Address Resolved Known Host Agent Name Agent QUID Image: Character System Host Name Image: Character System Image: Character System Clear Filter by Enter the System MontorName Type Image: Character System Clear Drag a column header here to group by that column. Action SystemMontorName Type Image: Character System Clear Drag a column header here to group by that column. Action SystemMontorName Type Clear Clear Image: Character System Mod Coll Image: Character System Clear Clear Clear Clear Image: Character System MontorName Type Change Log Source Identification Search Scope SystegEnabled NetWorkEnabled RecordStatus Destu/pdate License Unicense Image: Check All New Check All Optical Character Status System MontorName Term of the System Activate Resolves Activate Resolves Activate Resolves Activate Resolves	Entities Pla	atform Manager	Data Processors	Al Engine Network Monitors Syste	em Monitors Log Sources Log Processing	Policies Alarm I	Rules People					
Drag a column header here to group by that column. Adden Status Host Operating System Host IP Address Resolved Known Host Agent Name Agent CUID Image: Column header here to group by that column.<	New System N	Monitor Agents										<u>e</u>
Action Status Host Operating System Host IP Address Resolved Known Host Agent Name Agent GUID Image: Control of the System Mail	Drag a colu	umn header her	e to group by that	column.								
Image: Control System Mole Control System Monitor Name. Image: Control System Monitor Name. Image: Control System Monitor Name. Filter by Enter the System Monitor Name. Image: Control System Monitor Name. Image: Control System Monitor Name. Primary Side With-CODENHUG Mater Area Resource SystemMonitor Name. Image: Control System Monitor Name. Image: Control System Monitor Name. Image: Control System Monitor Name. Image: Control System Monitor Name. Image: Control System Monitor Name. Image: Control System Monitor Name. Image: Control System Monitor Name. Image: Control System Monitor Name. Image: Control System Monitor Name. Image: Control System Monitor Name. Image: Control System Monitor Name. Image: Control System Monitor Name. Image: Control System Monitor Name. Image: Control System Monitor Name. Image: Control System Monitor Name. Image: Control System Monitor Name. Image: Control System Monitor Name. Image: Control System Monitor Name. Image: Control System Monitor Name. Image: Control System Monitor Name. Image: Control System Monitor Name. Image: Control System Monitor Name. Image: Control System Monitor Name. Image: Control System Monitor Name. Image: Control System Monitor Name. Image: Control System Monitor Name. Image: Control System Monitor Name.	Action		Status	Host Operating System	m Host IP Address		Resolved Known Ho	ost	Agent Name	Ager Versi	nt on	Agent GUID
Filter by Enter the System Mo Description Host Name - Note of the system Mo Description Note of the system Mo Description Clear Drag a column header here to group by that column. Action Host Entity HostName SystemMonton/Name Type - OS Type - Include Retired SystemMonton/Name Type Image Loss Access acces												
Action Host Entity Host Entity Host Name SystemMonitorName Typ Change Log Source Identification Search Scope SystogEnabled NetrowEnabled RecordStatus DateUpdated LicenseType LestHeertbeet Image Log Source Identification Search Scope Image Log Source Identification Search Scope SystogEnabled NetrowEnabled RecordStatus DateUpdated LicenseType LestHeertbeet Image Log Source Identification Search Scope New Unicense Image Log Source Image Log So	Filter by	Enter the S	rstem Mo Descrip	column.	Host IP address Entity		OS Type		Include Retired		Search	Clear
Image: Log Solide Identification Search Scope Image: Log Solide Identification Search Scope Image: Log Solide Identification Search Scope Image: Log Solide Identification Search Scope Image: Log Solide Identification Search Scope Image: Log Solide Identification Search Scope Image: Log Solide Identification Search Scope Image: Log Solide Identification Search Scope Image: Log Solide Identification Search Scope Image: Log Solide Identification Search Scope Image: Log Solide Identification Search Scope Image: Log Solide Identification Search Scope Image: Log Solide Identification Search Scope Image: Log Solide Identification Search Scope Image: Log Solide Identification Search Scope Image: Log Solide Identification Search Scope Activate Image: Log Solide Identification Search Scope Image: Log Solide Identification Search Scope Activate Image: Log Solide Identification Search Scope Image: Log Solide Identification Search Scope Activate Image: Log Solide Identification Search Scope Image: Log Solide Identification Search Scope Service Start Service Start Service Start Service Start Service Start	Action	Host Entity	HostName	SystemMonitorName Type	Change Log Course Identification	Caarab Caapa	SyslogEnabled	NetflowEnabled	RecordStatus	Datel Indated	LicenseType	LastHeartheat
Primary Site WIN-COBINIZING Mask-Anchandragers Mask New Unlicense Unlicense Oheck All Activate Oheck All Displayed Activate Uncheck All Apply Configuration Policy Uncheck All Displayed Update Software Initiate SmartResponse Initiate SmartResponse Actions Service Start Service Start Service Restart Disassociate Add Flat File Log Source Stowing 1 of 1 Export Grid To File Service Requests Export Grid To File					change Log Source Identification	search scope				=		= [
New Unlicense Check All Activate Check All Retire Uncheck All Apply Configuration Policy Uncheck All Update Software Clear Filters Initiate SmartResponse Clear Filters Initiate SmartResponse Actions Service Start Export Grid To File Service Restart Disassociate Add Flat File Log Source Service Requests Export Grid To File	•	Primary Site	WIN-QQ8HIV	3 MINLOORUIVORSEI MIN	License				Active	1/4/2019 9:33	System Monito	or 1/4/2019 10:16: 1
Check All Activate Check All Displayed Retire Uncheck All Displayed Apply Configuration Policy Uncheck All Displayed Update Software Clear Filters Initiate SmartResponse Actions Service Start Export Grid To File Service Restart Disassociate Add Filat File Log Source Showing 1 of 1 Properties Service Requests Export Grid To File				New	Unlicense							
Check All Displayed Uncheck All Uncheck All Displayed Actions Service Start Uncheck All Displayed Add Windows Event Log Source Comparison of the Displayed Export Log Configuration File Export Log Configu				Check All	Activate							
Incheck All Apply Configuration Policy Uncheck All Displayed Update Software Clear Filters Initiate SmartResponse Actions Service Restart Export Grid To File Service Stop Disassociate Add Filat File Log Source Service Restart Export Grid To File Service Restart Export Grid To File Disassociate Add Filat File Log Source Service Restart Export Log Configuration File Service Restart Export Call Configuration File				Check All Displayed	Retire							
Uncheck All Displayed Update Software Clear Filters Initiate SmartResponse Actions Service Start View Service Restart Export Grid To File Service Stop Disassociate Add Filt File Log Source Showing 1 of 1 Export Local Configuration File Service Requests Export Local Configuration File				Uncheck All	Apply Configuration Policy							
Clear Filters Initiate SmartResponse Actions Service Start View Service Restart Export Grid File Service Storp Disassociate Add Filat File Log Source Showing 1 of 1 Properties Service Requests Export Grid Configuration File				Uncheck All Displayed	Update Software							
Actions Service Start View Service Restart Export Grid To File Service Stop Disassociate Add Windows Event Log Source Showing 1 of 1 Properties Service Requests Export Grid To File Edit Departies Export Crig Unit Configuration File				Clear Filters	Initiate SmartResponse							
View Service Restart Export Grid To File Service Stop Disassociate Add Windows Event Log Source Showing 1 of 1 Properties Service Requests Export Grid To File				Actions +	Service Start							
Export Grid To File Service Stop Disassociate Add Windows Event Log Source Showing 1 of 1 Properties Add File Log Source Service Requests Export Carl Configuration File Export Carl Configuration File				View +	Service Restart							
Disassociate Add Windows Event Log Source Showing 1 of 1 Properties Add Flat File Log Source Service Requests Export Local Configuration File				Export Grid To File	Service Stop							
C Properties Add Flat File Log Source Showing 1 of 1 Export Local Configuration File Service Requests Export Local Configuration File				Disassociate	Add Windows Event Log Source							
Showing 1 of 1 Service Requests Export Local Configuration File Export Local Configuration Fil	<			Properties	Add Flat File Log Source							>
Edit Departie	Showing 1 of Service Room	f1 lasts		Topentes	Export Local Configuration File							
Search For Alarm Value In the past	Search For	Alarm - Va	lue	In the past	Edit Properties		• Go					

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

•	LogRhyt	hm Console - [Deployment Manager]			
File Edit View MyLogRhythm Tools Window Help	,				
😉 🕼 🧧 🔔 Personal Dashboard 🔍 Investigate 🍙		Log Source Type Selector	_ 🗆 X		
Entities Platform Manager Data Processors Al Engine Net	File Edit				
New System Monitor Agents	Record Type Filter	Taxt Filter			
Drag a column header here to group by that column.	A - All tems -	obs			
Action Status H	a Custom			ame Agent	Age
	д, System	Text Search Type		version	
		Keyword Regex	Clear Apply		
		Log Source Type			
	-	Flat File - Observei T Enterprise			
Filter by Enter the System Mo Description	4			stred	Search
Drag a column header here to group by that column.					
Action Host Entity HostName SystemM				us DateUpdated Li	icenseType
					1
Primary Site WIN-QQ8HIV03 WIN-QQ8	F			1/4/2019 9:33 S	ystem Monitor
	·				
< 111	Show Retired		OK Cancel		
Showing 1 of 1					
Service Requests					

- 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*>

				LogRhythm Console - [Deployment Manager]	ť
😘 File Edit	t View My Logi	Rhythm Tools \	Window He	p	
00	2 Personal D)ashboard 🔍 Ir	nvestigate	🛿 Tail 🧶 Report Center 🛛 🔳 List Manager 🏂 Deployment Monitor 🎲 Deployment Manager	
Entities PI	atform Manager [Data Processors	Al Engine N	tunde Manitore System Monitore Las Causes Las Desensing Delinion Aleren Dulas Desels	
New System	Monitor Agents			Log Source Settings	
Drag a col	umn header here	to group by that	column.	Basic Configuration Additional Settings Flat File Settings Additional Info	
Action	s	tatus		File Path	Agent Agent GUI
				Date Parsing Format	
				ObserveIT CEF Format (<mm>\s<d>\s<yy>\s<h>:<m>:<s>)</s></m></h></yy></d></mm>	
				Multiline Log Message Settings	
Filter by	Enter the Sys	stem Mo Descrip	otion	Log Message Start Regex	rd Search Cl
0					
Drag a col	umn neader nere	to group by that	column.	Log Message Delimiter Regex	
Action	Host Entity	HostName	System		DateUpdated LicenseType LastHe
	Rrimany Site			Log Message End Regex	= = = 1/4/2019.9:33 System Monitor 1/4/20
	Filling Site	print dedonine	io Mile d		THEOTOGOG. OVACITINOTICE THEO
				- Directory Collection	
				Is Directory Collection	
				Inclusione Exclusion	
				Compression Type	
				Tone	
				·	
				OK Cancel Apply	
					

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

1	Filter by Enter the Log Source Description			Host Name							Search	Clear	
D	ag a col	umn header here t	o group by that column										
	Action	Log Entity	Log Host	Log Source Type	Log Source Name	Collection Host	Last Log Message	MPE Processing Mode	MPE Policy	LogMart	IsChildSource	Archive	Dr
				•			-						
ъ		Primary Site	OIT APP	Flat File - ObservelT	WIN-QQ8HIV03SEL	Entity: Primary Site,	1/4/2019 9:46:50.013 AM	Event Forwarding	LogRhythm Default			v	

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

A	ction	Log	Entity / Log Host	Log Source Type /	Log Source Name	Collection Host	Last Log Message	MPE Processing Mode	MPE Policy	LogMart	IsChildSource	Archive	Drop
8							=					•	
÷,	✓	Primer	Site OIT APP	Flat File - Observel T	WIN-QQ8HIV03SEL	Entity: Primary Site,	1/4/2019 9:46:50.013 AM	Event Forwarding	LogRhythm Default	Yes			
E		Prin	Check All	Flat File - LogRhyth	LogrhythmDXMonitor	Entity: Primary Site,	1/4/2019 9:57:36.270 AM	Disabled	LogRhythm Default	Yes		✓	
		Prin	Check All Displayed	LogRhythm Data Los	WinDataDefender	Entity: Primary Site,		Disabled	LogRhythm Default	Yes		✓	
		Prin	Unchask All	LogRhythm File Moni.	WinFileMon	Entity: Primary Site,	1/4/2019 9:35:10.463 AM	Disabled	LogRhythm Default	Yes		✓	
		Prin	Uncheck All	LogRhythm Network	NetworkConnection	Entity: Primary Site,		Disabled	LogRhythm Default	Yes		✓	
		Prin	Uncheck All Displayed	LogRhythm Process	ProcessMonitor	Entity: Primary Site,		Disabled	LogRhythm Default	Yes		✓	
		Prin	Clear Filters	LogRhythm Registry	RegistryMonitor	Entity: Primary Site,		Disabled	LogRhythm Default	Yes		✓	
		Prin	cicul miters	T 11 C ()	Monitor	Entity: Primary Site,		Disabled	LogRhythm Default	Yes		✓	
			Actions •	I all Log Source(s)									
			Export Grid To File	Change Log Sour	се Туре								
			Add Log Sources from File	Create Virtual Log	Sources								
			Properties	Update Catch All	Sources								

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







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**.



• In the Log Source Criteria, filter by the ObserveIT Log Source.



• Group by User and Object.



÷	Al Engine Rule Block Wizard - Log Observed	
Group By Fields		
Group lone with identical value	as in the following fields. Long without a value for a selected Group By field will be excluded	
* indicates fields not written to	the AlE Event - AlE Drilldown will work, but the field is not available for Smart Response or Event queries.	
Action	Location (Impacted) Hegion (Impacted)	
Application	Location (Origin)	
City (Impacted)	Log Source - Response Code	
City (Origin)	Log Source Entry Result	
Classification -	Log Source Host - Sender	
Command	Log Source Root Entry Sender Identity	
Country (Impacted)	MAC Address (mpacied) Sensi Number	
Country (impacted)	MAC Address (Origin) Session	
Country (Origin)	MALE Rule Rame (master) Session Type	
Direction	NAT IP Address (inipoted) Sevence	
Domain Impacted	NAT IF Address (Origin) Gladus	
Domain Impacted	NAT TOPIOP Part (impacted subject	
Entity (impacted) *	Network (Impacted) TCP/IDP Port (Origin)	
Entity (Origin) *	Network (Origin) Threat D	
Group	M Object	
Hash	Object Name IIII IIII	
Host (Impacted)	Object Turne Ulear (Imparted)	
Host (Origin)	Paret Process ID User (Impacted) Identity	
HostName (Impacted)	Parent Process Name V Liser (Orion)	
HostName (Origin)	Parent Process Path User (Origin) Identity	
Interface (Impacted)	Policy User Agent	
Interface (Origin)	Process ID Vendor Info	
IP Address (Impacted)	Process Name Vendor Message ID	
IP Address (Origin)	Protocol Version	
Known Application	Reason Zone (Impacted) *	
Known Host (Impacted)	Recipient Zone (Origin) *	
Known Host (Origin)	Recipient Identity	
Drimony Criteria Instude Eiltern E	Sustude Filters Day and Time Oritagia Las Course Oritagia D. D. ALE Summary Fields Information	
Finnary Cinteria Include Filters D	Exclude Filters Day and Filter Ciliteria Lug Source Ciliteria Group By All' Summary Fields Information	
<back next=""></back>	ОК	Cancel

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 <u>integrations@observeit.com</u> with questions about this and other ObserveIT integrations.