

Integration Guide

Integrating Cisco Catalyst with EventTracker

EventTracker v9.2 and above

Publication Date:

April 12, 2021

© Copyright Netsurion. All Rights Reserved.



Abstract

This guide helps you in configuring **Cisco Catalyst** with EventTracker to receive **Cisco Catalyst** events. In this guide, you will find the detailed procedures required for monitoring **Cisco Catalyst**.

Scope

The configuration details in this guide are consistent with EventTracker version v9.2x or above and **Cisco Catalyst.**

Audience

Administrators, who are assigned the task to monitor and manage **Cisco Catalyst** events using **EventTracker**.

Table of Contents

1	Overview				
2	Pre	erequisites	4		
	2.1	Integration of Cisco Catalyst with EventTracker	4		
3	Eve	entTracker Knowledge Pack	4		
	3.1	Category	5		
	3.2	Alert	5		
	3.3	Report	5		
	3.4	Dashboards	7		
4	Im	porting Cisco Catalyst knowledge pack into EventTracker	10		
	4.1	Category	10		
	4.2	Alert	11		
	4.3	Knowledge Object	12		
	4.4	Token Template	14		
	4.5	Report	16		
	4.6	Dashboards	17		
5	Ve	rifying Cisco Catalyst knowledge pack in EventTracker	20		
	5.1	Category	20		
	5.2	Alert	20		
	5.3	Knowledge Object	21		
	5.4	Token Value	22		
	5.5	Report	22		
	5.6	Dashboards	23		
	Abou	It Netsurion	24		
	Conta	24			

1. Overview

This guide helps you in configuring **Cisco Catalyst** with EventTracker to receive activity logs via syslog. In this guide, you will find the detailed procedures required for monitoring **Cisco Catalyst**.

EventTracker helps to monitor events from **Cisco Catalyst**. Its dashboard, alerts and reports will help you to detect attacks, suspicious host and accounts.

EventTracker's built-in knowledge pack enables you to gather business intelligence providing increased security, performance, availability, and reliability of your systems.

2. Prerequisites

- EventTracker v9.x or above should be installed.
- Cisco Catalyst should be installed and proper access permissions to make configuration changes.
- Administrative access on the EventTracker.

2.1 Integration of Cisco Catalyst with EventTracker

 $Cisco\ Catalyst\ can\ be\ integrated\ with\ Event Tracker\ via\ syslog\ configuration.$

To configure Cisco Catalyst to forward the log to EventTracker:

- 1. Log in to your Cisco CatOS user interface.
- 2. Type the following command to access privileged EXEC mode: **Enable**
- 3. Configure the system to timestamp messages:

Set logging timestamp enable.

- 4. Type the IP address of EventTracker: Set logging server <IP address>
- 5. Limit messages that are logged by selecting a severity level: Set logging server severity.
- 6. Configure the facility level that should be used in the message. The default is local7. **Set logging server facility.**
- 7. Enable the switch to send syslog messages to the EventTracker.
 - Set logging server enable.

Events forwarded to EventTracker by Cisco Catalyst are displayed on the **Log Search** tab of EventTracker.

3. EventTracker Knowledge Pack

Once logs are received by EventTracker manager, knowledge packs can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker to support Cisco Catalyst.

3.1 Category

- **Cisco Catalyst: Privilege Enable Fail-** This category provides information related to all privilege enable failure detected in Cisco Catalyst.
- **Cisco Catalyst: Privilege Enable Success-** This category provides information related to all privilege enable success detected in Cisco Catalyst.
- **Cisco Catalyst: Bad check sum found-** This category provides information related to all bad check sum found in Cisco Catalyst.
- **Cisco Catalyst: Device audit-** This category provides information related to all the device found lost detected in Cisco Catalyst.
- **Cisco Catalyst: New IP found-** This category provides information related to all the new IP found in Cisco Catalyst.
- **Cisco Catalyst: Login fail-** This category provides information related to all the login failure detected in Cisco Catalyst.
- **Cisco Catalyst: Login Success-** This category provides information related to all the login success detected in Cisco Catalyst.
- **Cisco Catalyst: Port link down-** This category provides information related to all the port link down detected in Cisco Catalyst.
- **Cisco Catalyst: Port link up-** This category provides information related to all the port link up detected in Cisco Catalyst.
- **Cisco Catalyst: Socket Activity-** This category provides information related to all the port open/close of UDP/TCP detected in Cisco Catalyst.

3.2 Alert

- **Cisco Catalyst: Bad packet received:** This alert is generated when malformed packet is received in Cisco Catalyst.
- **Cisco Catalyst: Login fail:** This alert is generated when user fails to login is detected in Cisco Catalyst.
- **Cisco Catalyst: Port link down:** This alert is generated when a broken link for the port is detected in Cisco Catalyst.
- **Cisco Catalyst: Privilege enable fail:** This alert is generated when privilege enable failure is detected in Cisco Catalyst.

3.3 Report

• **Cisco Catalyst: User Login Success:** This report gives information about all the login successful detected in Cisco Catalyst. Report contains IP address, username, and other useful information.

LogTime	Computer	User Name	IP Address	Log Type	Log Priority
03/31/2021 04:35:18 PM	CISCO CATALYST-SYSLOG	јоу	10.34.201.101	MGMT	6
04/01/2021 11:43:39 AM	CISCO CATALYST-SYSLOG	јоу	10.34.201.101	MGMT	6
04/02/2021 10:23:05 AM	CISCO CATALYST-SYSLOG	joyer	10.34.201.10	MGMT	6

• **Cisco Catalyst: User login Failure:** This report gives information about all the login failure detected in Cisco Catalyst. Report contains IP address, username, and other useful information.

LogTime	Computer	User Name	IP address	Туре	priority	1
03/31/2021 04:35:18 PM	CISCO CATALYST-SYSLOG	jake	10.34.200.100	MGMT	6	1
04/01/2021 11:43:39 AM	CISCO CATALYST-SYSLOG	jake	10.34.200.100	MGMT	6	4

• **Cisco Catalyst: Interface Management:** This report gives information about all the broken/active link on the port activities in Cisco Catalyst. Report contains module, port and other useful information.

LogTime	Computer	Device name	Log Subtype	Log Type	Log priority
04/01/2021 11:43:39 AM	CISCO CATALYST-SYSLOG	C9300-24T/5-10	PORTLINKDOWN	DTP	7
04/01/2021 11:43:39 AM	CISCO CATALYST-SYSLOG	C9300-30T/9-15	PORTLINKUP	DTP	7
04/02/2021 10:23:05 AM	CISCO CATALYST-SYSLOG	C930g0-24T/5-10	PORTLINKDOWN	DTP	7
04/02/2021 10:23:05 AM	CISCO CATALYST-SYSLOG	C9300-30gT/9-15	PORTLINKUP	DTP	7
					_

• **Cisco Catalyst: New IP Detected:** This report gives information about all the new IP address learned on a port detected in Cisco Catalyst. Report contains IP address, username, successful login or login failure, and other useful information.

LogTime	Computer	User Name	IP address	Туре	priority
03/31/2021 04:35:18 PM	CISCO CATALYST-SYSLOG	jake	10.34.200.100	MGMT	6
04/01/2021 11:43:39 AM	CISCO CATALYST-SYSLOG	jake	10.34.200.100	MGMT	6

• **Cisco Catalyst: Device Connection Activity:** This report gives information about all the device connection detected/lost in Cisco Catalyst. Report contains module, port and other useful information.

LogTime	Computer	Module/Port	Log Subtype	Message	Log Type	Log priority
04/01/2021 11:43:39 AM	CISCO CATALYST-SYSLOG	C9300-30T/15	DEVICE_DETECTED	ciscoipphone detected on port C9300- 30T/15, Auxiliary Vlan enabled	SECURITY	5
04/01/2021 11:43:39 AM	CISCO CATALYST-SYSLOG	C9300-30T/15	DEVICE_LOST	ciscoipphone not detected on port C9300-30T/15, Auxiliary Vlan disabled	SECURITY	5
04/02/2021 10:23:05 AM	CISCO CATALYST-SYSLOG	C930h0-30T/15	DEVICE_DETECTED	ciscoipphone detected on port C930h0-30T/15, Auxiliary Vlan enabled	SECURITY	5



3.4 Dashboards

• Cisco Catalyst: Logs Type



• Cisco Catalyst: Login Success





• Cisco Catalyst: Login Failure



• Cisco Catalyst: Privilege Access Status by Source IP





• Cisco Catalyst: Port Link Activity





• Cisco Catalyst: Socket Activity



4. Importing Cisco Catalyst knowledge pack into EventTracker

NOTE: Import knowledge pack items in the following sequence:

- Category
- Alert
- Knowledge Object
- Token Template
- Report
- Dashboard
- 1. Launch EventTracker Control Panel.
- 2. Double click Export Import Utility.



3. Click the **Import** tab.

4.1 Category

1. Click **Category** option, and then click the browse button.

- Ъ	Export Import Utility	-		x
Export Import 1. Provide the path and file nam 2. Click the Import button. Options • Category • Filters • Alerts • Systems and Groups • Token Value • Reports • Behavior Correlation	Export Import Utility e of the Categories file. Use the '' button to browse and locate the import file. Location Source :	-		×
	Import		Close	e

- 2. Locate Category_Cisco Catalyst.iscat file, and then click the Open button.
- 3. To import categories, click the **Import** button.

EventTracker displays success message.



4. Click **OK**, and then click the **Close** button.

4.2 Alert

1. Click **Alert** option, and then click the **browse** button.

3	Export li	mport Utility		×	
Export Import					
1. Provide the path and file na 2. Click the Import button.	ame of the Alerts file. Use the '' but	ton to browse and locate the import file.			
Ontions	Location				
 Category 	Import E-mail settings				
	Set Active				
 Filters 	 Only if notifications set 	Alert files. For v7, the active status will be set based on	V6X) 1		
 Alerts 	 By default 	"Active" key available in the configuration section.			
 Systems and Groups 	Watchlist Configuration				
	Import Watchlist configurat	ion			
	This setting is applicable only for alerts which have Advanced watchlist configured.				
○ Reports	on the console where the aler	ts are imported.	DIC		
Behavior Correlation					
	Source :				
	*.isalt				
			_		
				_	
		Import	Clos	e	

- 2. Locate Alert_Cisco Catalyst.isalt file, and then click the Open button.
- 3. To import alerts, click the **Import** button. EventTracker displays success message.



4. Click the **OK** button, and then click the **Close** button.

4.3 Knowledge Object

1. Click **Knowledge objects** under **Admin** option in the EventTracker manager page.

≡	EventTracker					.↓ Admin•	Tools +
	Home		Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dashb
٩		_	Alerts	Correlation	🔍 IP Lookup Configuration	QQ Users	_
	0	1	Behavior Correlation Rules	Diagnostics	·@. Knowledge Objects	r Weights	
k			🇞 Behavior Correlation Settings	Event Filters	Manager	Windows Agent Config	
	Potential Cyber Breaches Unsafe connections or processes, new TCP entry point	Indicators of Cc USB activities, New sen	Casebook Configuration	P Eventvault	Parsing Rules		
				FAQ Configuration	Report Settings		
	Attacker		- News				

2. Click on **Import** ^T button as highlighted in the below image:

	Knowledge Objects				
Q R	Search objects	Q	Q Activate Now	Objects 🕀 📳 🏦 🌣	
	Groups	🕀 🧭 🗓		Î	
	• Cylance				
	EventTracker				

3. Click Browse.

Import		×
Select file	🚰 Browse Upload]
		Close

- 4. Locate the file named **KO_Cisco Catalyst.etko**.
- 5. Select the check box and then click on \mathbb{T} Import option.



Impor	t			×
Sele	ct file		🗁 Browse Upload	
	Object name	Applies to	Group name	
	Cisco Catalyst	Cisco Catalyst	Cisco Catalyst	
			Import Close	

6. Knowledge objects are now imported successfully.

File imported successfully.	
ОК	

4.4 Token Template

For importing **Token Template**, navigate to **EventTracker manager** web interface.

1. Click **Parsing Rules** under the **Admin** option in the EventTracker manager web interface:

	•	Admin	-	Tools -
ers	😥 Parsing Rules			† /
lt Contains	set of rules which tell v	vhat kind	l of dat	a you want
Configuration	Systems			



2. Click the **Template** tab and then click the **Import Configuration** button.

Parsing Rule	5			
Parsing Rule	Template			
Groups			(+)	Group :
Default				
Azure Intune		Ī	1	Templa

A	/ Admin / Parsing Rules
	C 1
Active	Import configuration

 Click Browse and navigate to the knowledge packs folder (type %et_install_path%\Knowledge Packs in navigation bar) where ".ettd", e.g., "Token Template_Cisco Catalyst.ettd file is located. Wait for few seconds, as templates will be loaded. Once you see the templates, click desired template, and click Import button:

Import	
Select file Note: Please select file	of type *.ettd (eventtracker template dashlets).



4.5 Report

1. Click **Reports** option, and select **New (*.etcrx)** option.

Export Import 1. Provide the path and file r 2. Click the Import button	name of Schedule Report file. Use the '' button to browse and locate the import file.
Options Options Category Filters Alerts Systems and Groups Token Value Reports Behavior Correlation	Location Uccation Legacy (*.issch) Source : *.issch
	Import

2. Locate the file named **Reports_Cisco Catalyst.etcrx** and select all the check box.

: If rep	ort(s) contains template, first import template	and proceed with report import process.			
ect file	\\192.168.1.7\EventTracker KP\Securi	y Intelligence Team\Harish\Cisco Catalyst	\KP\Reports_Cisco Catalyst.etcrx	Select file	
lable rep	ports				
, 🗌		Frequency Show all	- Q Q		
1	Title	Sites	Groups	Systems	Frequenc
EDIT	Cisco Catalyst - New IP Detected	R1S5-VM30	Default	Cisco Catalyst-syslog	Undefined
EDIT	Cisco Catalyst - Port link activities	R1S5-VM30	Default	Cisco Catalyst-syslog	Undefined
EDIT	Cisco Catalyst - User login activities	R1S5-VM30	Default	Cisco Catalyst-syslog	Undefined
					,
ter Cet		Reports and March Reports			3
xte: Set ≭ run 1	run time option is not applicable for Define time for report(s) from	Reports and Hourly Reports	des Set		
te: Set splace	run time option is not applicable for Define time for report(s) from to	Pepots and Hourly Repots	des Set ① place Asign systems		



3. Click the Import I button to import the report. EventTracker displays success message.



4.6 Dashboards

NOTE: Below steps given are specific to EventTracker 9 and later.

1. Open EventTracker in browser and logon.

	Home			
٩	My Dashboard			
	Threats		1	
	Incidents	ntry point	Indicators of Compromise USB activities, New services or software install	
	Behavior Correlation			
	Change Audit	l		-
	Compliance		Carlos and	

- 2. Navigate to **My Dashboard** option as shown above.
- 3. Click on the **Import** show below:

Event Tracker ⊕	ņ	Admin -	Tools •	💽 ETAdmin 🔹
My Dashboard		f	/ Dashboard	d / My Dashboard
		(+)	g @ 🌣	1 3 0

- 4. Import dashboard file Dashboard_Cisco Catalyst.etwd and select Select All checkbox.
- 5. Click on **Import** as shown below:

mport		
Note: If dashlet configured using dashlet.	persisted report, first import the report	and proceed with importing
		🖆 Browse Upload
Available widgets Select All		
Cisco Catalyst:Login acti	Cisco Catalyst:Port Link	
Cisco Catalyst: Privilege	Cisco Catalyst: Protocol	
Cisco Catalyst: Log type	Cisco Catalyst: Log categ	
		Import Close

6. Import is now completed successfully.



7. In **My Dashboard** page select ⊕ to add dashboard.

My Dashboard			👚 / Dashboard / My Dashboar
CheckPoint	Trend Micr	Microsoft	+ × • • • • • • • • • • • • • • • • • •



8. Choose appropriate name for **Title** and **Description**. Click **Save**.

Add Dashboard
Title
Cisco Catalyst
Description
Cisco Catalyst
Save Delete Cancel

9. In **My Dashboard** page select ^(a) to add dashlets.

My Dashboard		👚 / Dashboard / My Dashboa
CheckPoint Trend	licr Microsoft	⊕ ⊘ 🖓 ‡ ∓ ⊚

10. Select imported dashlets and click Add.

Customize dashlets

Cisco Catalyst				Q
Cisco Catalyst: Log category	Cisco Catalyst: Log type	Cisco Catalyst: Privilege Access	Cisco Catalyst: Protocol por	t act
Cisco Catalyst:Login activity	Cisco Catalyst:Port Link activity			

Add	Delete	Close

 \times



5. Verifying Cisco Catalyst knowledge pack in EventTracker

5.1 Category

- 1. Logon to **EventTracker**.
- 2. Click Admin dropdown, and then click Category.

≡	Event Tracker ⊕					🐥 🛛 Admin 🗸	Tools -
	Home		Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dashb
a			Alerts	Correlation	🔍 IP Lookup Configuration	🛱 Users	
	0	1	Behavior Correlation Rules	A Diagnostics	·⊙ Knowledge Objects	1 Weights	
~			🗞 Behavior Correlation Settings	🐨 Event Filters	Manager	Windows Agent Config	
	Potential Cyber Breaches Unsafe connections or processes, new TCP entry point	Indicators of Cc USB activities, New sen	Casebook Configuration	C Eventvault	🧭 Parsing Rules		
			olooo Category	FAQ Configuration	Report Settings		
	Attacker			 News 			

3. In **Category Tree** to view imported category, scroll down and expand **Cisco Catalyst** group folder to view the imported category.



5.2 Alert

- 1. Logon to EventTracker.
- 2. Click the Admin menu, and then click Alerts.

	Event Tracker ⊕					🔎 Admin-	Tools -
	Home		Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dashi
a		_	Alerts	Correlation	🔍 IP Lookup Configuration	🛱 Users	
	0	2	Behavior Correlation Rules	Diagnostics	· Knowledge Objects	The Weights	
~			🍪 Behavior Correlation Settings	Event Filters	Manager	Windows Agent Config	
	Potential Cyber Breaches Unsafe connections or processes, new TCP entry point	Indicators of Co USB activities, New sen	Casebook Configuration	Eventvault	😥 Parsing Rules		
		_	₀ Category	FAQ Configuration	Report Settings		
	Attacker			- News			



3. In the **Search** box, type **'isco Catalyst**, and then click the **Go** button. Alert Management page will display the imported alert.

🕂 🗓	Activate Now Click 'Activate Now' after making all changes		
	Alert Name 🔨	Threat	Active
64	Cisco Catalyst: Privilege enable fail	٠	
🗆 දීදී	Cisco Catalyst:Bad packet received	٠	
🗆 දීදී	Cisco Catalyst:Login fail	٠	
🗆 දීදී	Cisco Catalyst:Port link down	٠	

4. To activate the imported alert, toggle the **Active** switch.

EventTracker displays message box.

Successfully saved configur	ation. ditional dialogs
	OK

5. Click **OK**, and then click the **Activate Now** button.

NOTE: Specify appropriate **system** in **alert configuration** for better performance.

5.3 Knowledge Object

1. In the EventTracker web interface, click the Admin dropdown, and then select Knowledge Objects.

≡	Event Tracker ⊕					Admin-	To ols -
	Home		Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dashb
٩			Alerts	C Correlation	Q IP Lookup Configuration	였 Users	
	0	1	Behavior Correlation Rules	A Diagnostics	·@· Knowledge Objects	The Weights	
~			🗞 Behavior Correlation Settings	😨 Event Filters	Manager	Windows Agent Config	
	Potential Cyber Breaches Unsafe connections or processes, new TCP entry point	USB activities, New sen	Casebook Configuration	Eventvault	🧭 Parsing Rules		
			olo Category	FAQ Configuration	Report Settings		
	Attacker			- News			

2. In the Knowledge Object tree, expand **Cisco Catalyst** group folder to view the imported knowledge object.



	Knowledge Objects	
Q R	Search objects Q Q Activate Now	
	Groups 🕒 🧭 🗓	
	Cisco Catalyst	

3. Click Activate Now to apply imported knowledge objects.

5.4 Token Value

- 1. In the **EventTracker** web interface, click the **Admin** dropdown, and then click **Template**.
- 2. In the **Template** tab, click on the **Zix Email Threat Protection** group folder to view the imported Token Values.

Parsing Rule	S			
Parsing Rule	Template			
Groups		[III.]	÷	Group : Cisco Catalyst
Cisco Catalyst			1	Template Name
Cisco ISE			0	Cisco Catalyst: New IP detected
Cloudflare			1	Cisco Catalyst: New Server
Comodo EDR		Ī	1	connection

5.5 Report

1. In the **EventTracker** web interface, click the **Reports** menu, and then select **Report Configuration**.

	Event Tracker ⊕			
	Home			
Q				
R	Report Configuration		1	
	Report Dashboard	ntry point	Indicators of Compromise USB activities, New services or software install	
	Explorer			
	Attacker	1		-



- 2. In Reports Configuration pane, select Defined option.
- 3. Click on the **Cisco Catalyst** group folder to view the imported reports.

Report Configuration							
O Sch	neduled 🔵 Queued 💿 Defined						
Repor	t Groups		÷		Repo	orts configu	ration: Cisco Catalyst
	Cisco Catalyst	Ē.	Ø	•	÷	Ū <i>0</i> ,	
	Cisco ISE	Ŵ	1				Title
	Cloudflare	Ē	1			€\$3	Cisco Catalyst - New Server Connections
	Comodo EDR	Ē	1			2.23	Cisco Catalyst - New IP Detected
	Comodo Endpoint Prot	Ē	1			2	Cisco Catalyst - Port link activities
	Crowdstrike Falcon		Ø	II.		2	Cisco Catalyst - User login activities

5.6 Dashboards

1. In the EventTracker web interface, Click Home and select My Dashboard.



2. In the Cisco Catalyst dashboard you see the following screen.





About Netsurion

Flexibility and security within the IT environment are two of the most important factors driving business today. Netsurion's cybersecurity platforms enable companies to deliver on both. Netsurion's approach of combining purpose-built technology and an ISO-certified security operations center gives customers the ultimate flexibility to adapt and grow, all while maintaining a secure environment.

Netsurion's <u>EventTracker</u> cyber threat protection platform provides SIEM, endpoint protection, vulnerability scanning, intrusion detection and more; all delivered as a managed or co-managed service. Netsurion's <u>BranchSDO</u> delivers purpose-built technology with optional levels of managed services to multilocation businesses that optimize network security, agility, resilience, and compliance for branch locations. Whether you need technology with a guiding hand or a complete outsourcing solution, Netsurion has the model to help drive your business forward. To learn more visit <u>netsurion.com</u> or follow us on <u>Twitter</u> or <u>LinkedIn</u>. Netsurion is #19 among <u>MSSP Alert's 2020 Top 250 MSSPs</u>.

Contact Us

Corporate Headquarters

Netsurion Trade Centre South 100 W. Cypress Creek Rd Suite 530 Fort Lauderdale, FL 33309

Contact Numbers

EventTracker Enterprise SOC: 877-333-1433 (Option 2) EventTracker Enterprise for MSP's SOC: 877-333-1433 (Option 3) EventTracker Essentials SOC: 877-333-1433 (Option 4) EventTracker Software Support: 877-333-1433 (Option 5) https://www.netsurion.com/eventtracker-support