Netsurion®
Powering Secure and Agile Networks

Integration Guide

Integrating Cisco Catalyst with EventTracker

EventTracker v9.2 and above

Publication Date:

April 12, 2021

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

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 EventTracker 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	joy	10.34.201.101	MGMT	6
04/01/2021 11:43:39 AM	CISCO CATALYST-SYSLOG	joy	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	Type	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: 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.

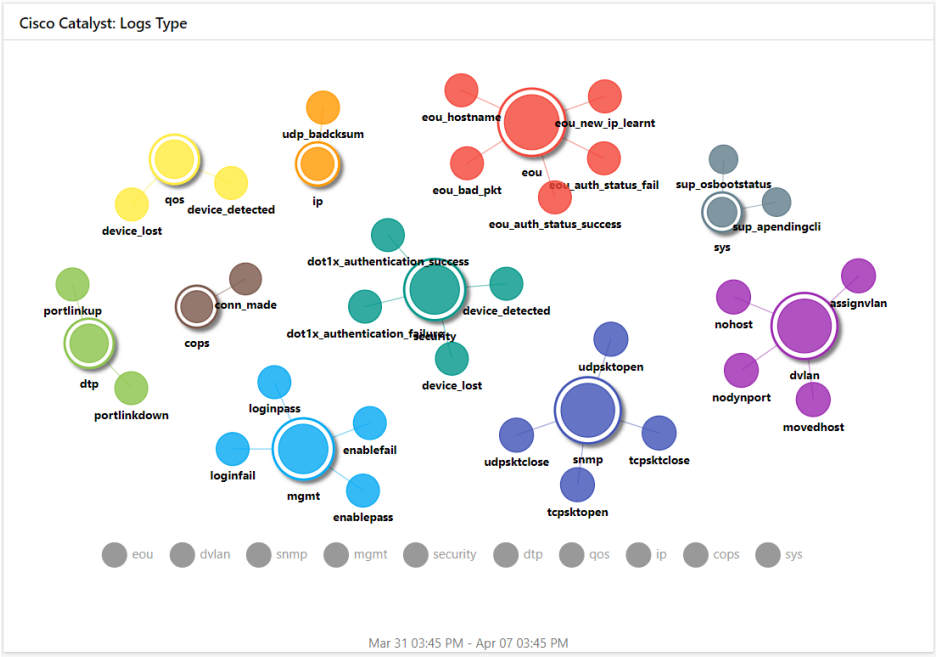
LogTime	Computer	User Name	IP address	Type	priority
03/31/2021 04:35:18 PM	CISCO CATALYST-SYSLOG	jake	10.34.200.100	MGMT	6
04/01/2021 11:43:39 AM	CISCO CATALYST-SYSLOG	jake	10.34.200.100	MGMT	6

- **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.

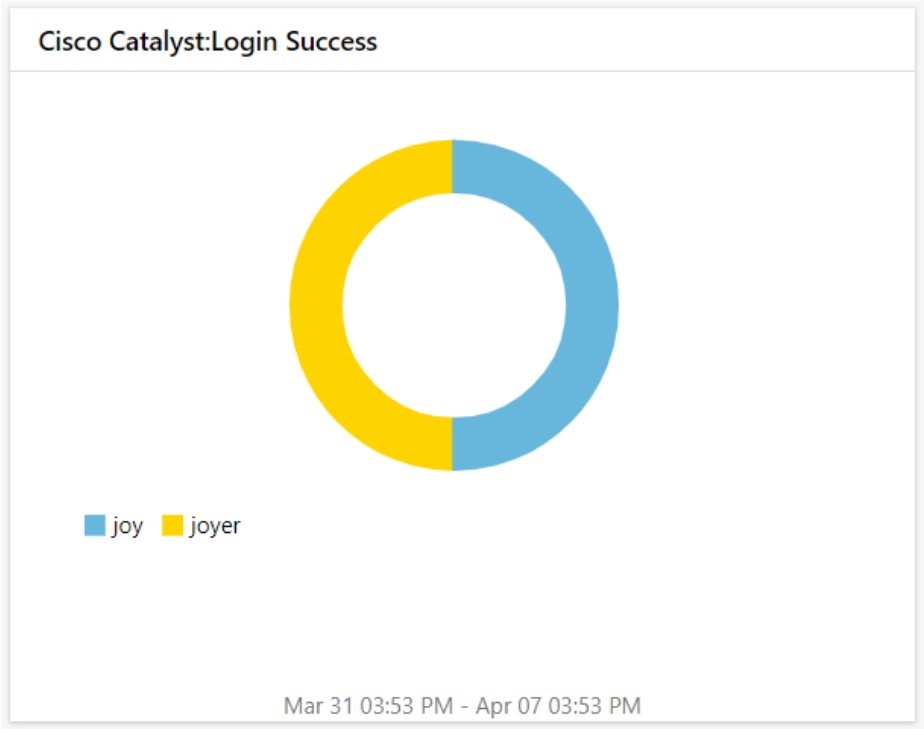
LogTime	Computer	Module/Port	Log Subtype	Message	Log Type	Log priority
04/01/2021 11:43:39 AM	CISCO CATALYST-SYSLOG	C9300-30T/15	DEVICE_DETECTED	ciscoipphone detected on port C9300-30T/15, Auxiliary Vlan enabled	SECURITY	5
04/01/2021 11:43:39 AM	CISCO CATALYST-SYSLOG	C9300-30T/15	DEVICE_LOST	ciscoipphone 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

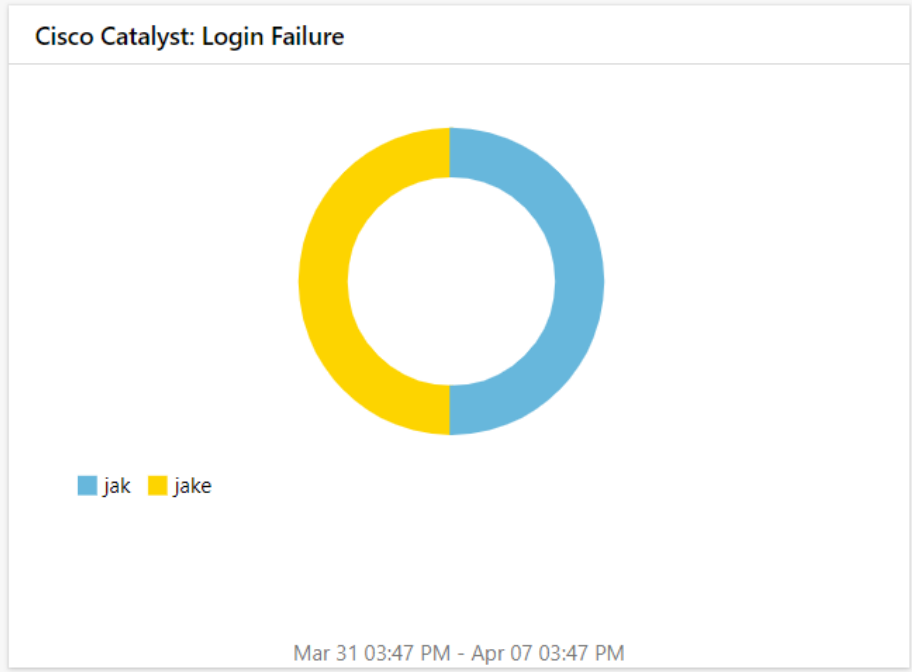
- **Cisco Catalyst: Logs Type**



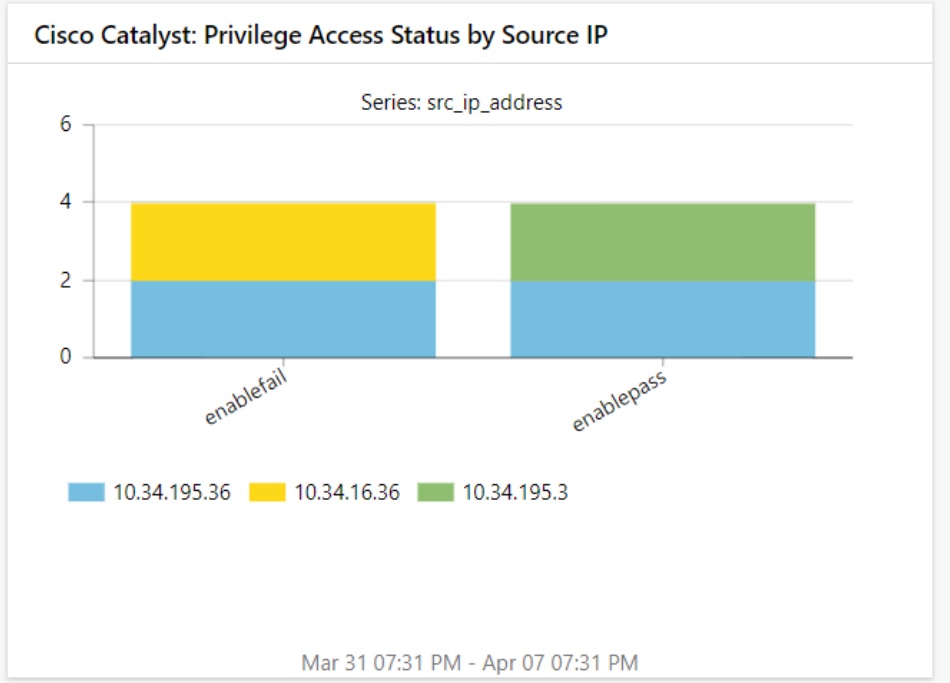
- **Cisco Catalyst: Login Success**



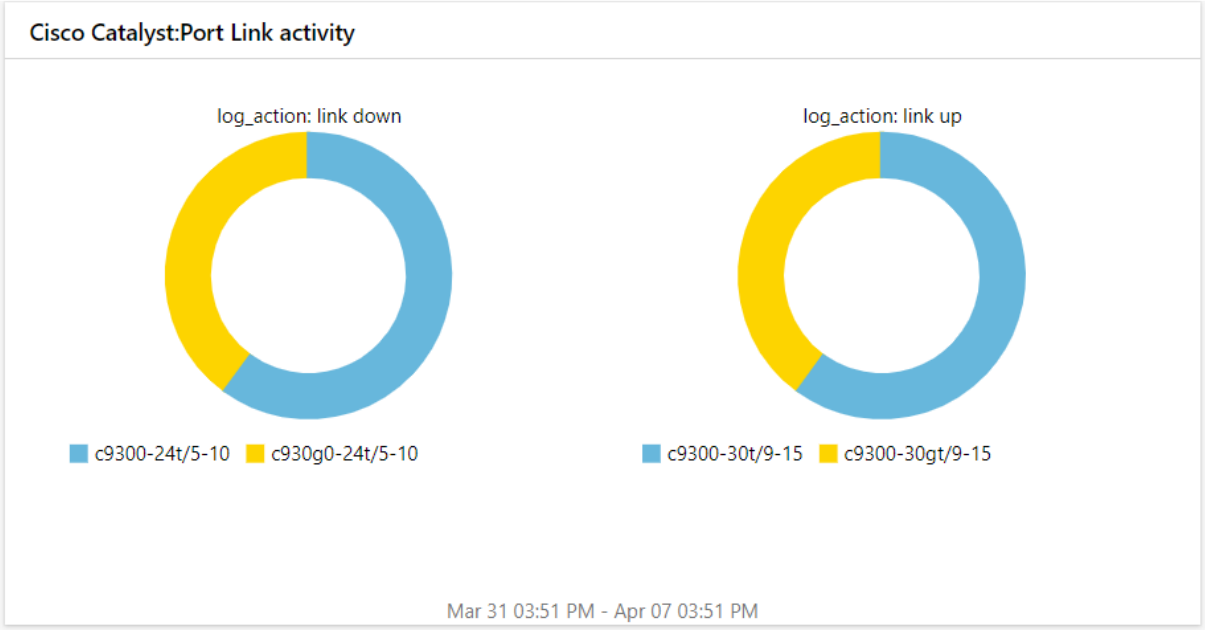
- **Cisco Catalyst: Login Failure**



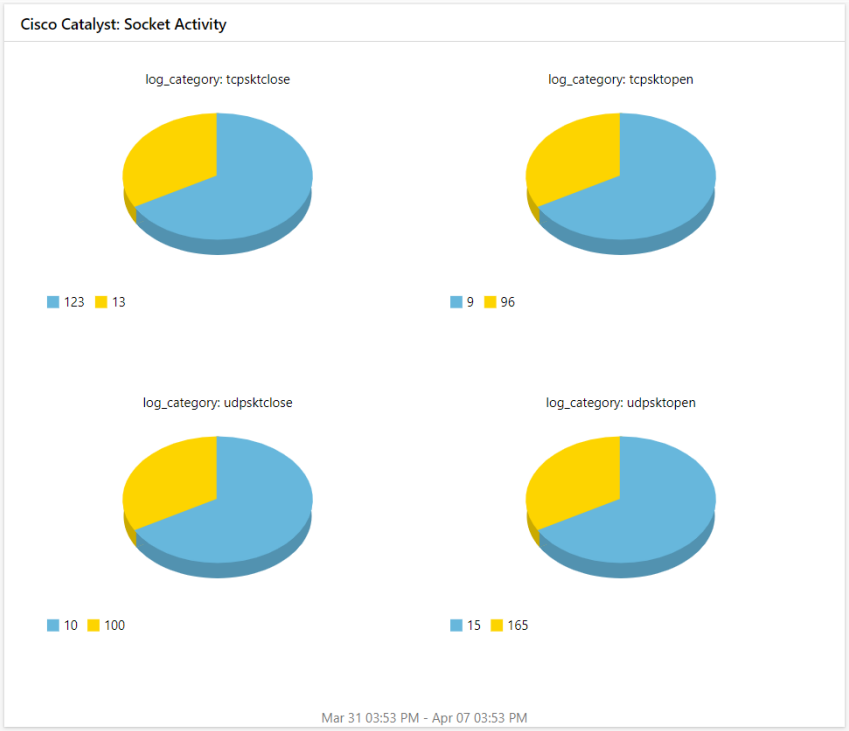
- **Cisco Catalyst: Privilege Access Status by Source IP**



- **Cisco Catalyst: Port Link Activity**



- **Cisco Catalyst: Socket Activity**

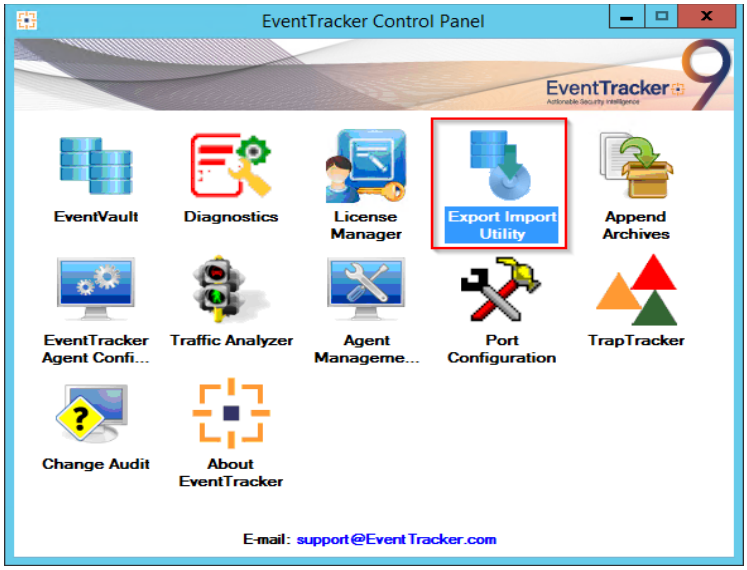


4. Importing Cisco Catalyst knowledge pack into EventTracker

NOTE: Import knowledge pack items in the following sequence:

- Category
- Alert
- Knowledge Object
- Token Template
- Report
- Dashboard

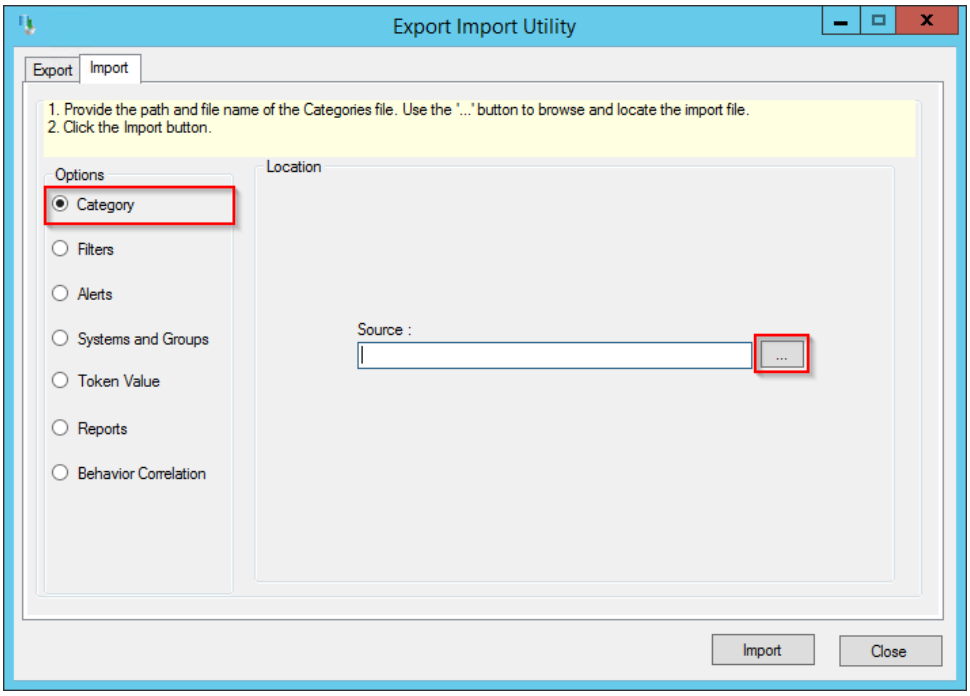
1. Launch **EventTracker Control Panel**.
2. Double click **Export Import Utility**.



3. Click the **Import** tab.

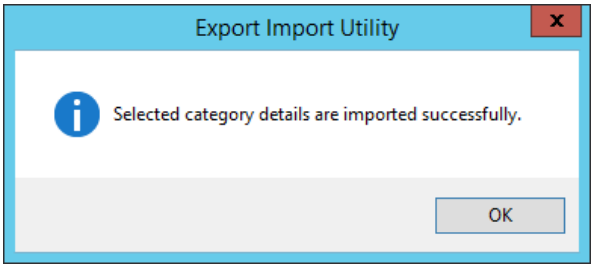
4.1 Category

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



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

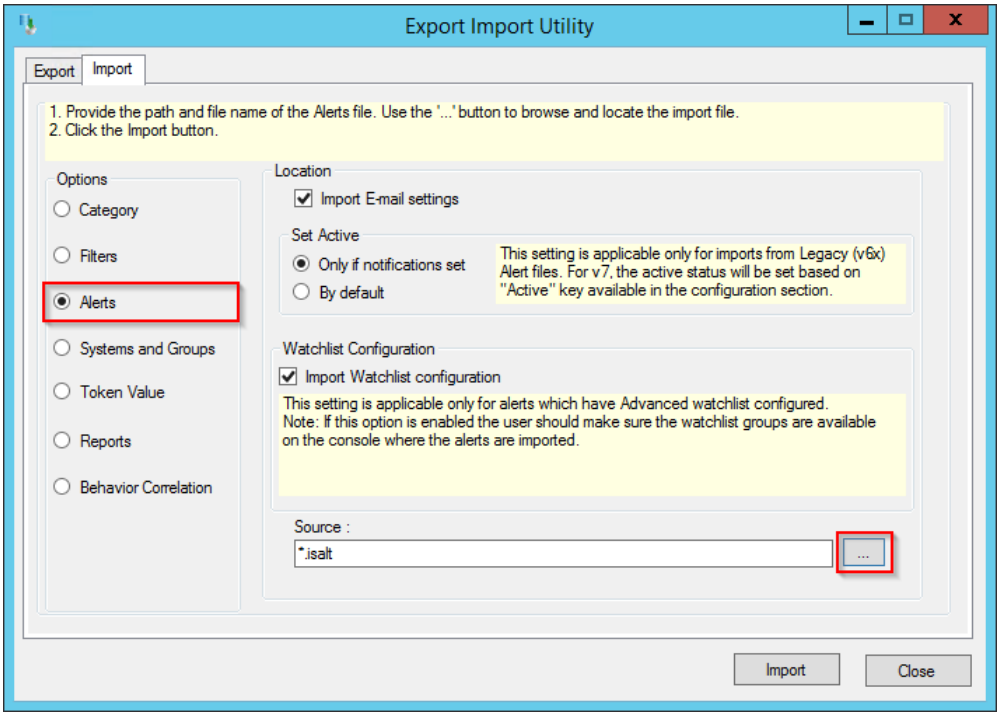
EventTracker displays success message.



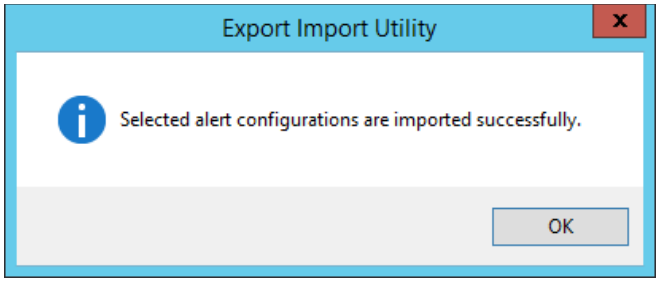
4. Click **OK,** and then click the **Close** button.

4.2 Alert

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



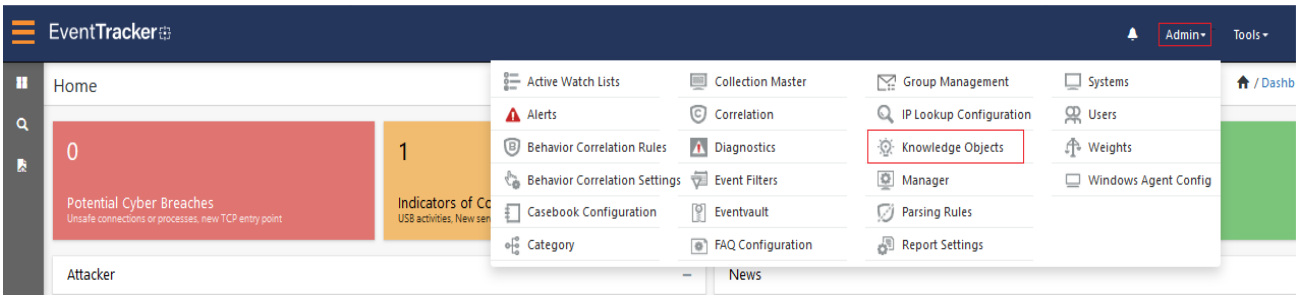
2. Locate **Alert_Cisco Catalyst.isalt** file, and then click the **Open** button.
3. To import alerts, click the **Import** button.
   EventTracker displays success message.



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

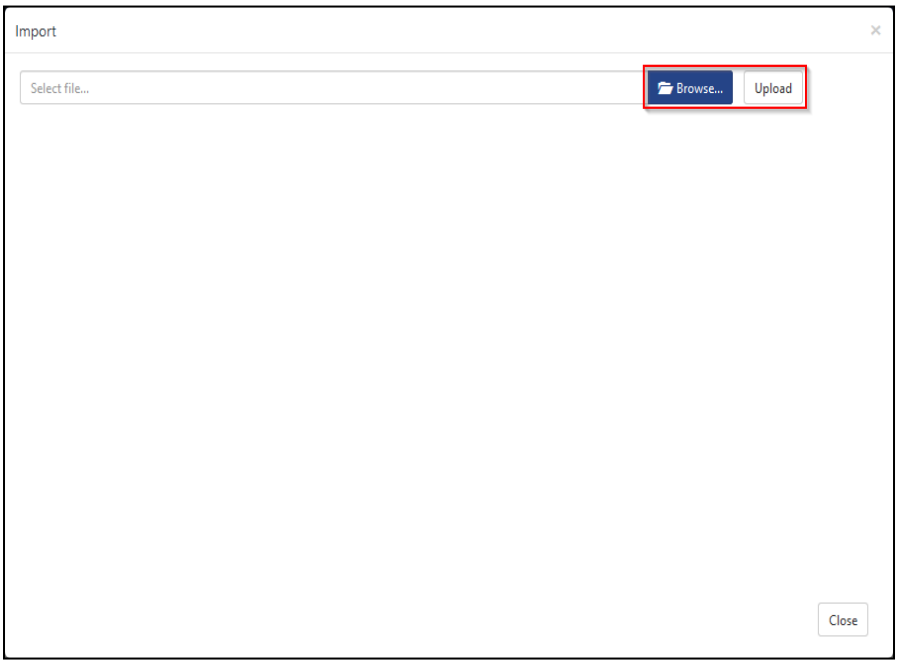
4.3 Knowledge Object

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

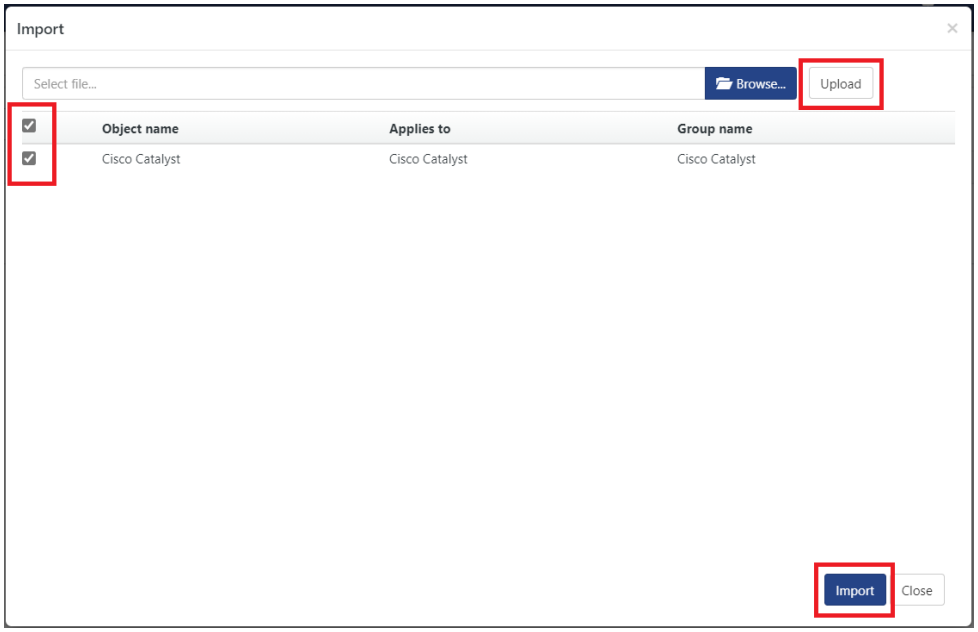


2. Click on **Import** button as highlighted in the below image:

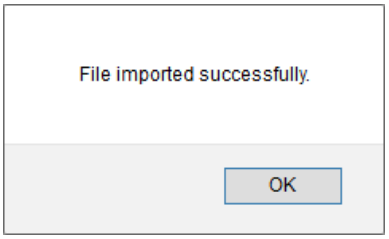
3. Click **Browse**.



4. Locate the file named **KO_Cisco Catalyst.etko**.
5. Select the check box and then click on **Import** option.



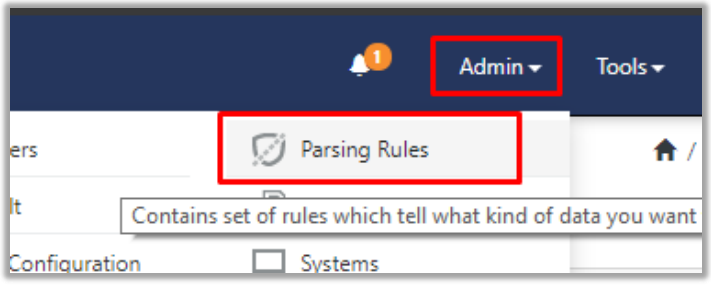
6. Knowledge objects are now imported successfully.



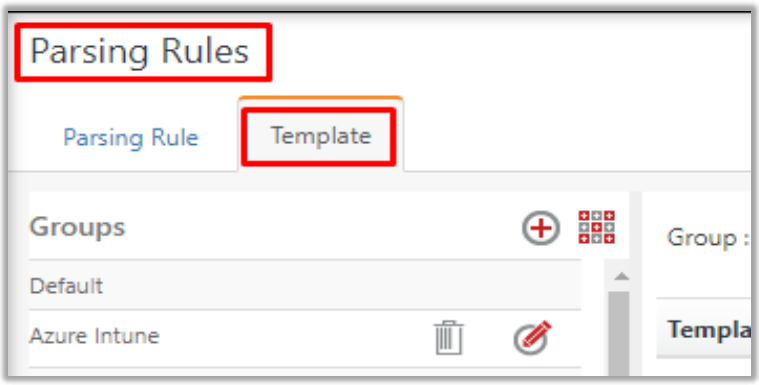
4.4 Token Template

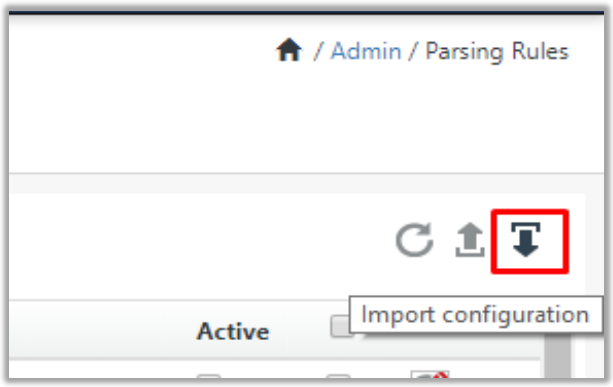
For importing **Token Template**, navigate to **EventTracker manager** web interface.

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

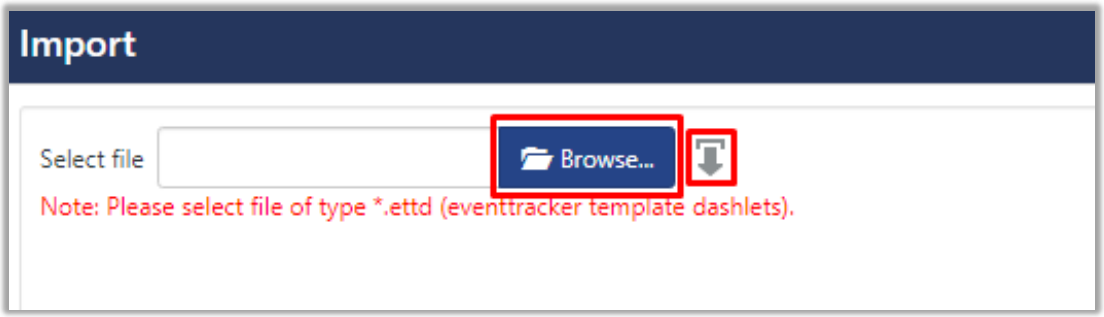


2. Click the **Template** tab and then click the **Import Configuration** button.



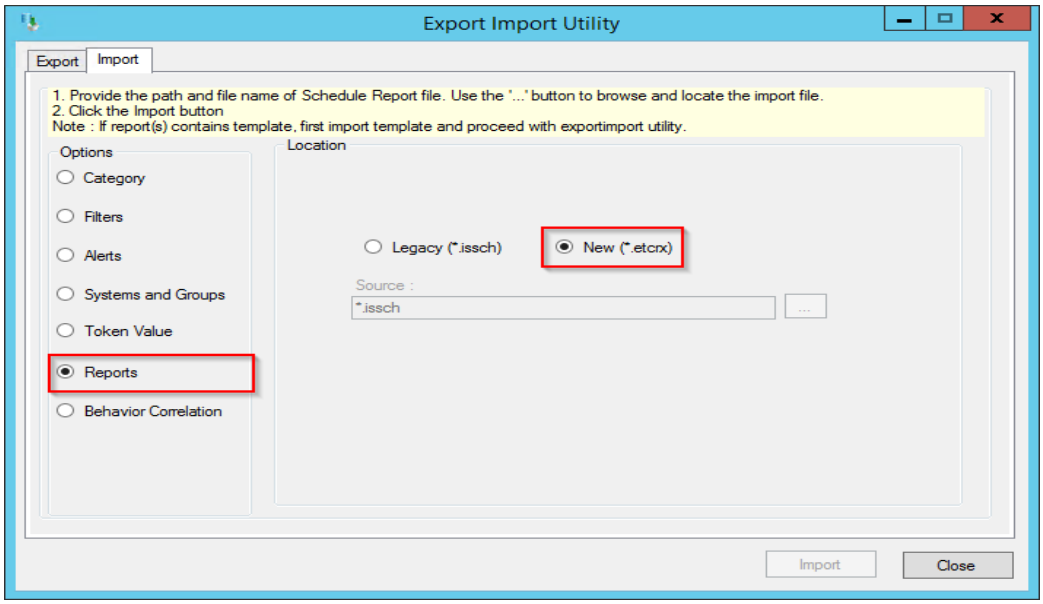


3. Click **Browse** and navigate to the knowledge packs folder (type **%et_install_path%\Knowledge Packs** in navigation bar) where "**.ettd", e.g., "Token Template_Cisco Catalyst.ettd** file is located. Wait for few seconds, as templates will be loaded. Once you see the templates, click desired template,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

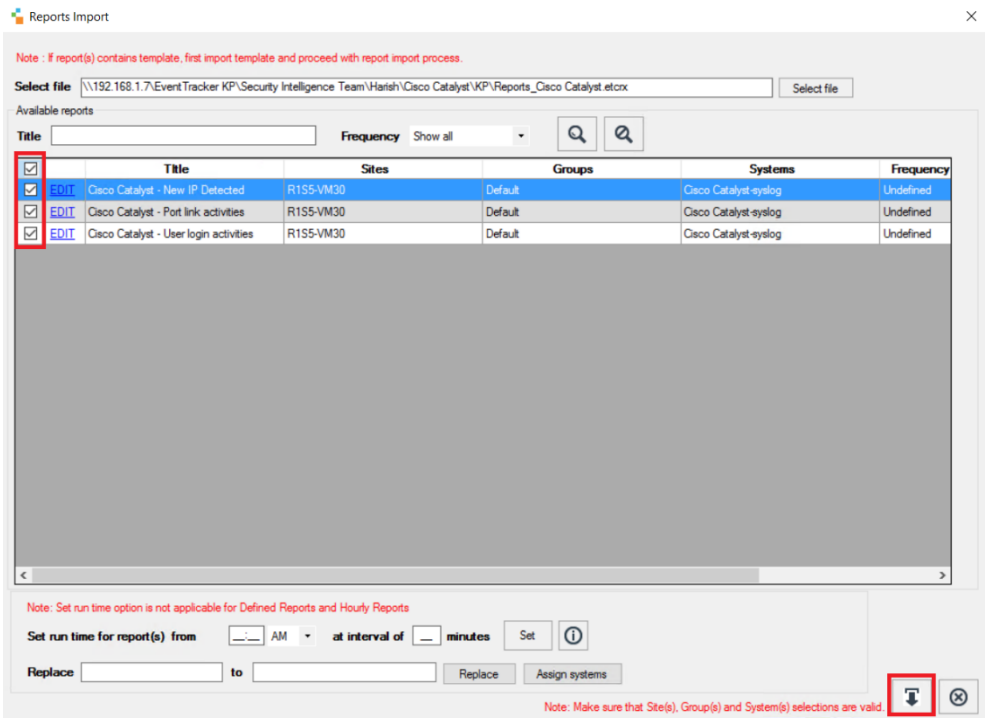


4.5 Report

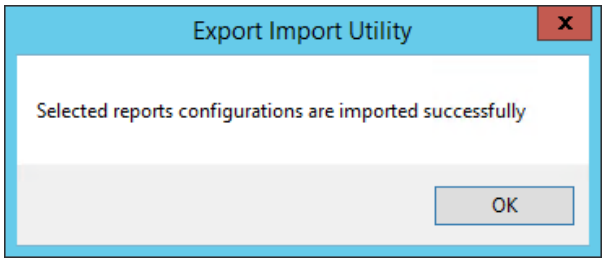
1. Click **Reports** option, and select **New (*.etcrx)** option.



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



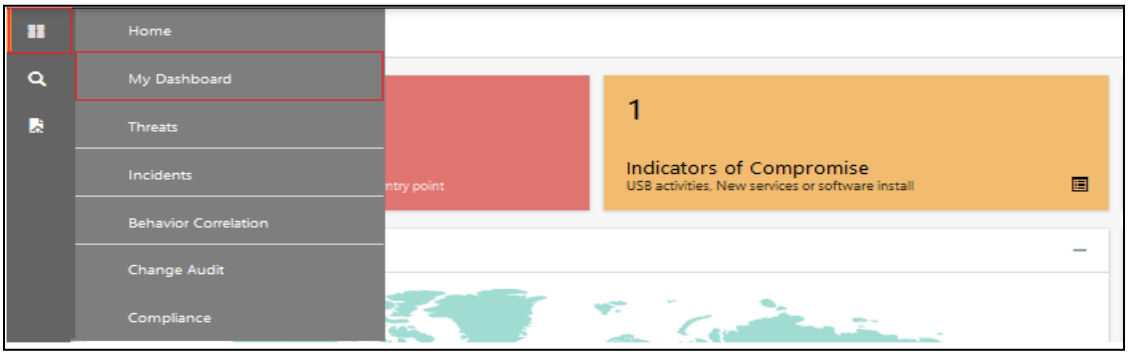
3. Click the **Import** button to import the report. EventTracker displays success message.



4.6 Dashboards

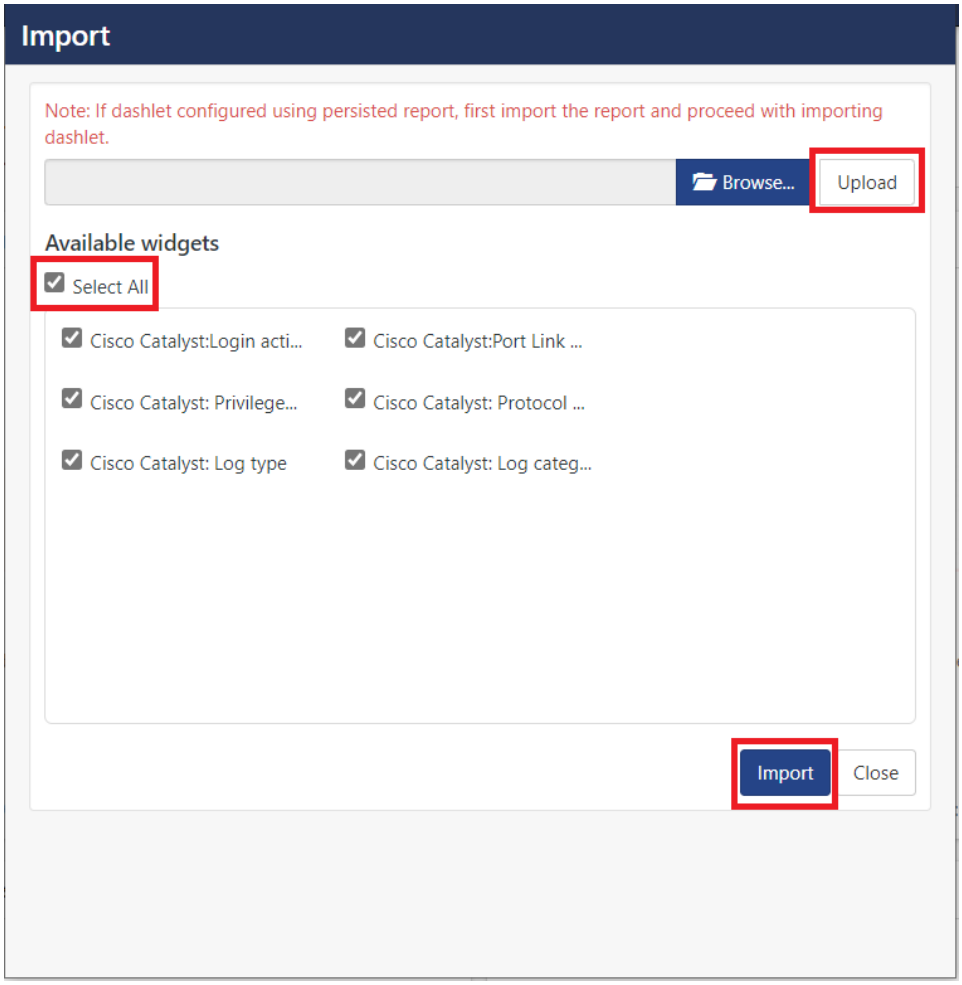
NOTE: Below steps given are specific to EventTracker 9 and later.

1. Open **EventTracker** in browser and logon.

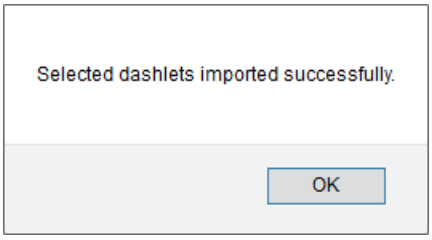


2. Navigate to **My Dashboard** option as shown above.
3. Click on the **Import** button as show below:

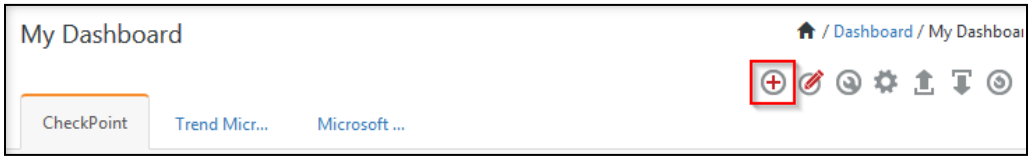
4. Import dashboard file **Dashboard_Cisco Catalyst.etwd** and select **Select All** checkbox.
5. Click on **Import** as shown below:



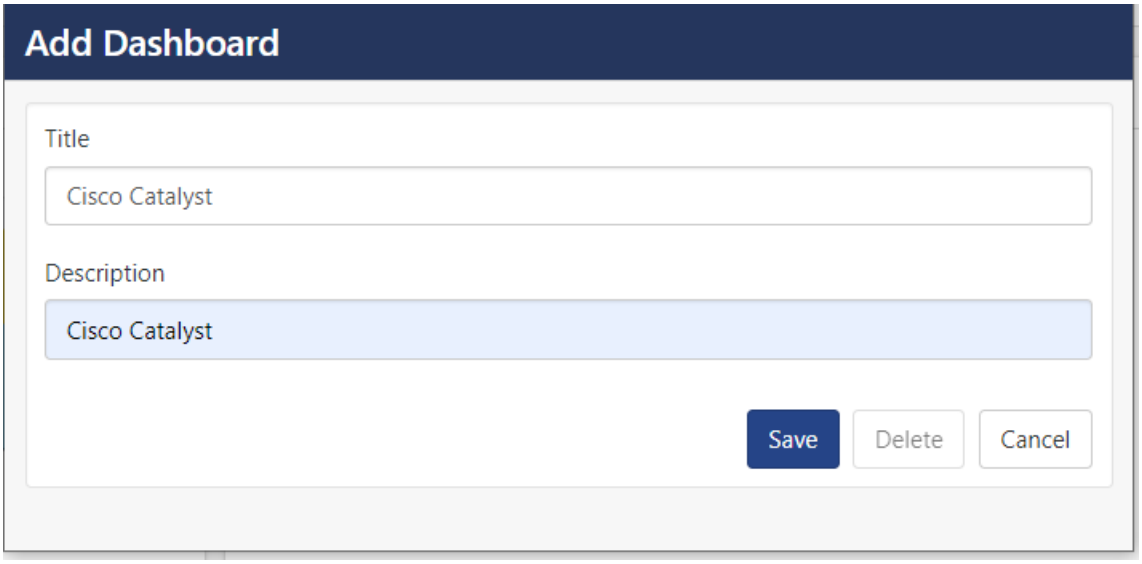
6. Import is now completed successfully.



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

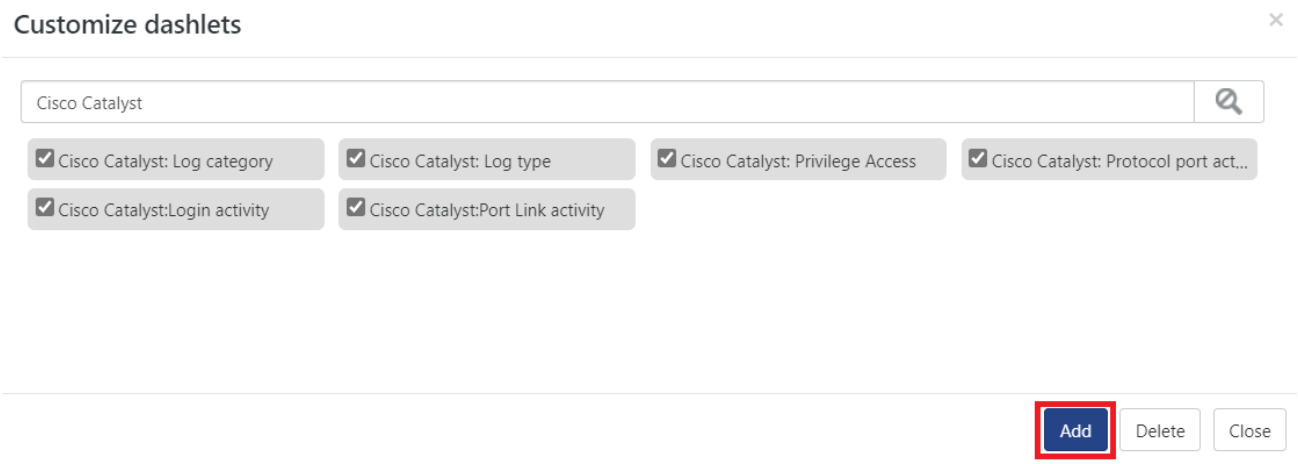


8. Choose appropriate name for **Title** and **Description**. Click **Save**.



9. In **My Dashboard** page select to add dashlets.

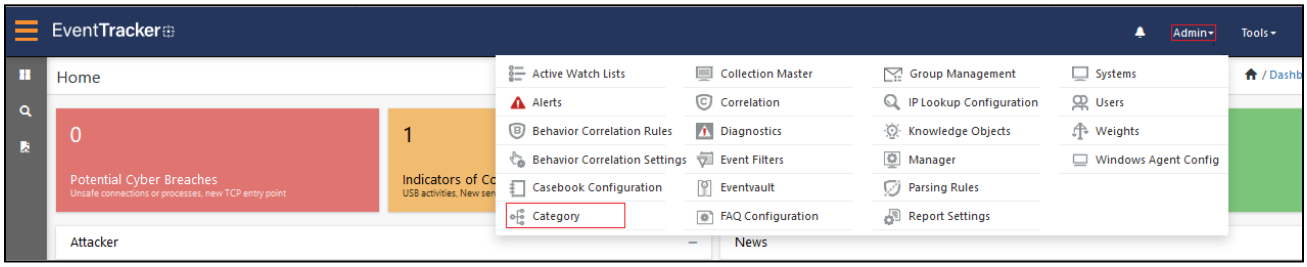
10. Select imported dashlets and click **Add**.



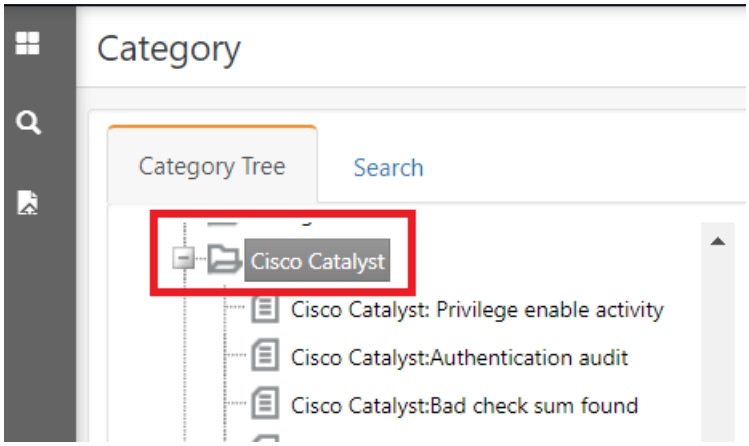
5. Verifying Cisco Catalyst knowledge pack in EventTracker

5.1 Category

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

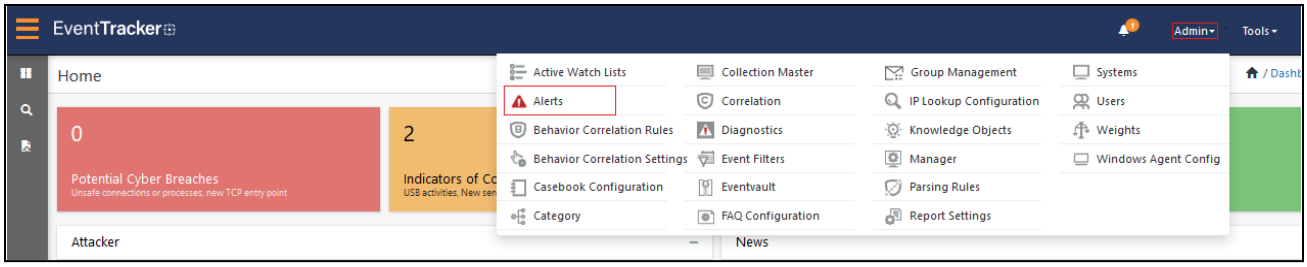


3. In **Category Tree** to view imported category, scroll down and expand **Cisco Catalyst** group folder to view the imported category.

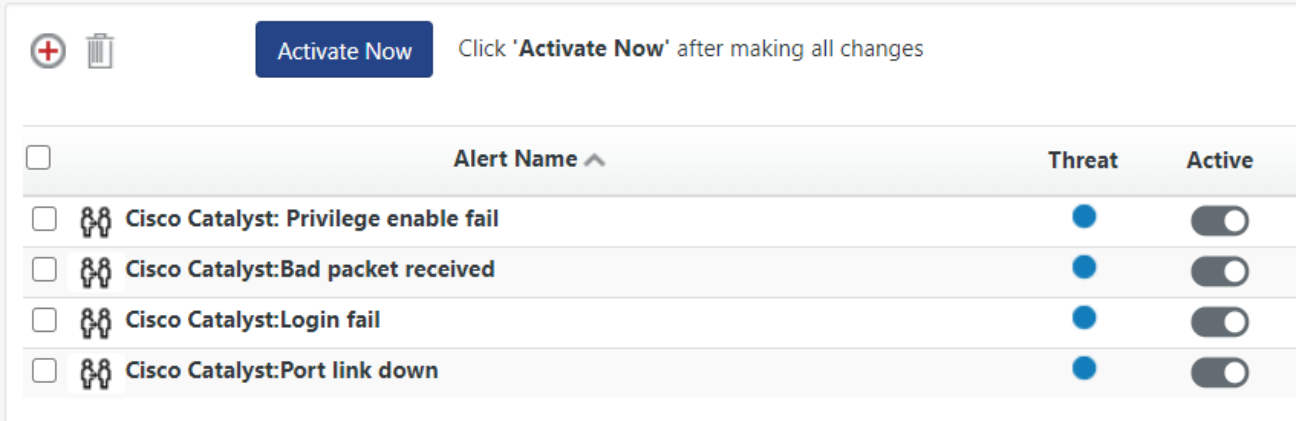


5.2 Alert

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

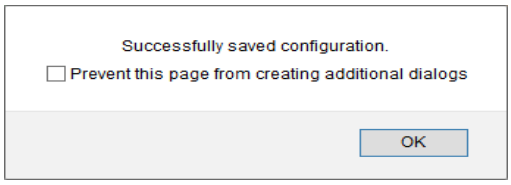


3. In the **Search** box, type '**isco Catalyst**, and then click the **Go** button.
   Alert Management page will display the imported alert.



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

   EventTracker displays message box.

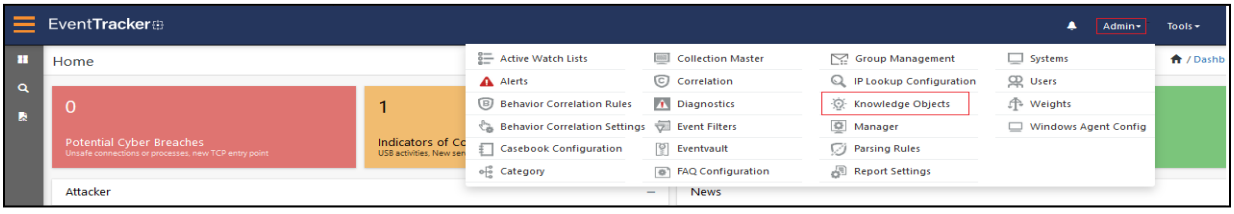


5. Click **OK**, and then click the **Activate Now** button.

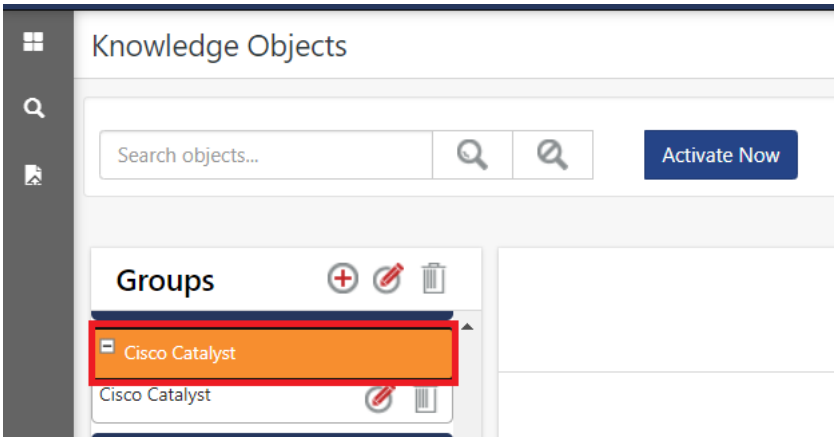
NOTE: Specify appropriate **system** in **alert configuration** for better performance.

5.3 Knowledge Object

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



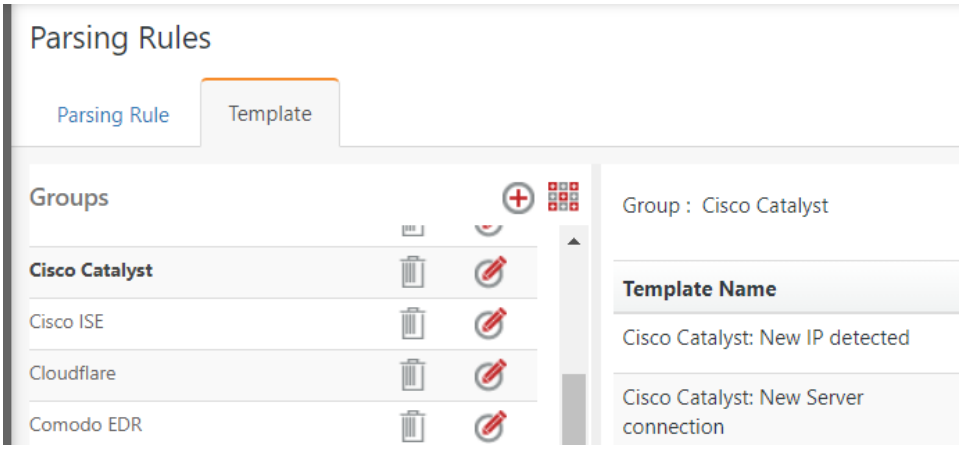
2. In the Knowledge Object tree, expand **Cisco Catalyst** group folder to view the imported knowledge object.



3. Click **Activate Now** to apply imported knowledge objects.

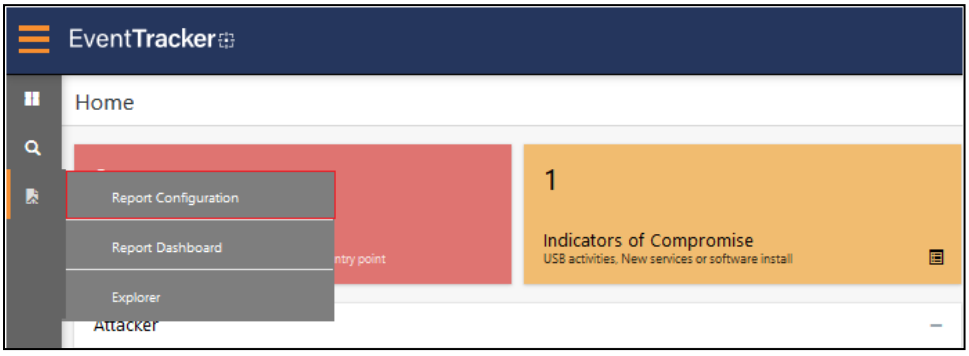
5.4 Token Value

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.

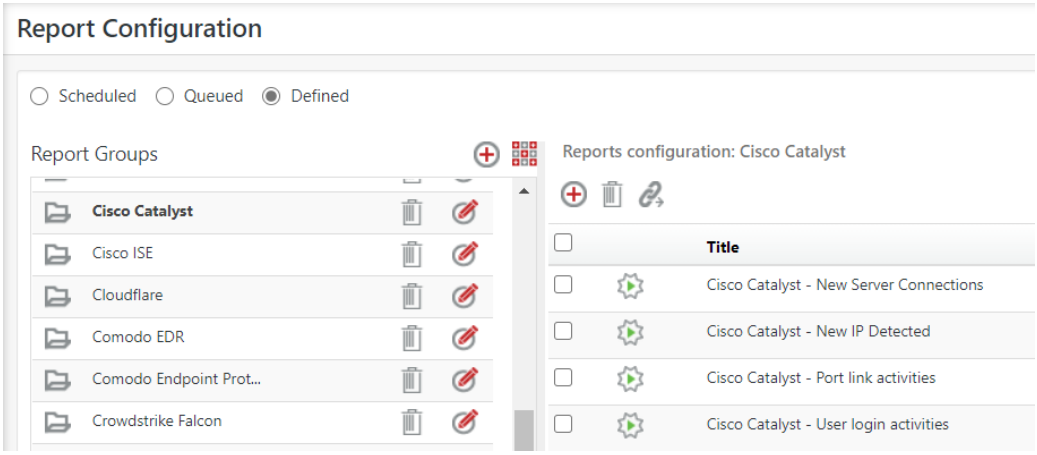


5.5 Report

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

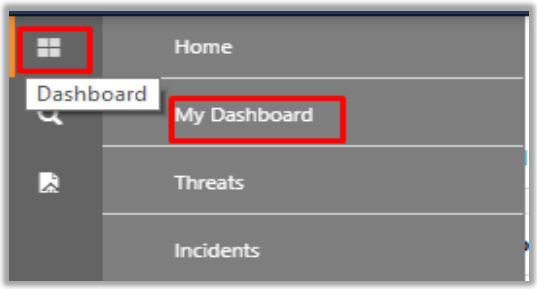


2. In **Reports Configuration** pane, select **Defined** option.
3. Click on the **Cisco Catalyst** group folder to view the imported reports.

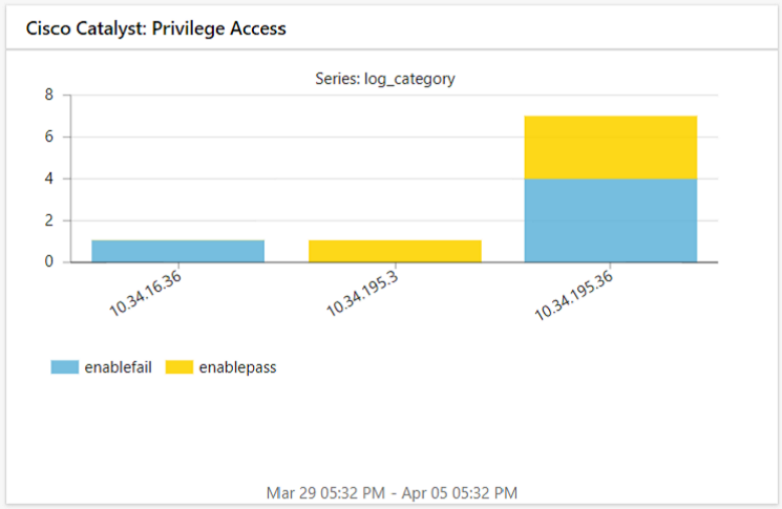


5.6 Dashboards

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 EventTracker 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 BranchSDO delivers purpose-built technology with optional levels of managed services to multi-location 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 netsurion.com or follow us on Twitter or LinkedIn. Netsurion is #19 among MSSP Alert's 2020 Top 250 MSSPs.

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