Netsurion | EventTracker®

Integration Guide- Cisco Expressway

EventTracker v9.x and above

Publication Date: April 21, 2020

Abstract

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

Scope

The configurations detailed in this guide are consistent with EventTracker version v9.x or above and **Cisco Expressway.**

Audience

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

Table of Contents

1. Overview

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

EventTracker helps to monitor events from **Cisco Expressway**. It's dashboard, alerts and reports will help you to detect security related attack and authentication failures detected in Cisco Expressway.

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

Through alerts, knowledge base solutions, and reports, EventTracker helps you correct problems long before a disastrous failure occurs.

2. Prerequisites

- **EventTracker v9.x** or **above** should be installed.
- **Cisco Expressway** should be configured.
- **Local Admin permission** for the workstation.

3. Integration of Cisco Expressway with EventTracker

3.1 Enabling Syslog

1. Go to Maintenance > Logging and enter the IP addresses or Fully Qualified Domain Names (FQDNs) of the EventTracker Manager to which this system will send log messages.
2. Click on the **Options** for each server.
3. Specify the Transport protocol and Port you wish to use. If you choose to use TLS, you will see the option to enable Certificate Revocation List (CRL) checking for the syslog server.
4. In the Message Format field, select the writing format for remote syslog messages. The default is Legacy BSD.
5. Use the Filter by Severity option to select how much detail to send. The Expressway sends messages of the selected severity and more severe messages.
6. Use the Filter by Keywords option if you only want to send messages with certain keywords.
7. Click Save.

   Note:
   - The Filter by Keywords option is applied to messages already filtered by severity.
   - You can use up to five keywords, which includes groups of words (for example 'login successful'), separated by commas.
   - You can use a maximum of 256 characters in the keyword search.

- We recommend that you search for the most relevant keywords first to avoid any impact on system performance. This ensures the system pushes the relevant log messages to the syslog server at the earliest opportunity.

4. 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 Expressway.

4.1 Category

- **Cisco Expressway: Security Alert -** This category provides information related to any security related attack detected in Cisco Expressway.
- **Cisco Expressway: Authentication Failure –** This category provides information related to authentication failure detected in Cisco Expressway.
- **Cisco Expressway: Authentication Success –** This category provides information related to successful authentication in Cisco Expressway.
- **Cisco Expressway: Call Activities –** This category provides information related to call activity detected in Cisco Expressway.
- **Cisco Expressway: Configuration Changes –** This category provides information related to configuration changes activities.

4.2 Alert

- **Cisco Expressway: Authentication Failure -** This alert is generated when any authentication failure is detected in Cisco Expressway.
- **Cisco Expressway: Security Alert –** This alert is generated when any related attack is detected in Cisco Expressway

4.3 Report

- **Cisco Expressway: Authentication Failure -** This report gives information regarding all the authentication failures detected in Cisco Expressway. Reports contains IP address, logon type, username and other useful information for further analysis.

LogTime	EventId	Computer	EventSource	EventDescription	Details	Event	Source Ip	Username
04/16/2020 03:28:49 PM	128	172.xx.xx.xx-SYSLOG	SYSLOG local0	Apr 16 15:28:49 172.xx.xx.xx Mar 25 08:42:20 expe2 2020-03-25T08:42:20.516-05:00 expe2 UTCTime="2020-03-25 13:42:43,214" Event="Admin Session CBA	authentication Failure	Admin Session CBA Authorization Failure	127.xx.xx.xx	test1
04/16/2020 03:28:49 PM	128	172.xx.xx.xx-SYSLOG	SYSLOG local0	Apr 16 15:28:49 172.xx.xx.xx Mar 25 08:42:20 expe2 2020-03-25T08:42:20.516-05:00 expe2 UTCTime="2020-03-25 13:42:43,214" Event="Admin Session Login	authentication Failure	Admin Session Login Failure	10.xx.xx.xx	test2
04/16/2020 03:28:49 PM	128	172.xx.xx.xx-SYSLOG	SYSLOG local0	Apr 16 15:28:49 172.xx.xx.xx Mar 25 08:42:20 expe2 2020-03-25T08:42:20.516-05:00 expe2 UTCTime="2020-03-25 13:42:43,214"	authentication Failure	Authorization Failure	10.xx.xx.xx	test3

Figure 1

- **Cisco Expressway: Security Alert** – This report gives information about all the security related attack detected in Cisco Expressway. Report contains event type, event detail and other useful information about the security alert.

- **Cisco Expressway: Call Activity** - This report gives the information about all call activities detected in cisco Expressway such as Call connected, rejected, disconnected, rerouted, etc. Reports contains IP address, event type, call-ID, service, is call authenticated and other useful information.

LogTime	EventId	Computer	EventSource	EventDescription	Authentication	Call Serial Number	Event	Log Priority	Protocol	Service	Source Ip	Source Port
04/17/2020 12:30:41 PM	128	172.xx.xx.xx-SYSLOG	SYSLOG local0	Apr 17 12:30:41 172.xx.xx.xx Mar 25 08:45:02 expe2 2020-03-25T08:45:02.216-05:00 expe2 tvcs:		075408d3-0827-493d-958f-b592def3acc0	Call Disconnected	1	TLS	SIP	192.xx.xx.xx	63032
04/17/2020 12:30:41 PM	128	172.xx.xx.xx-SYSLOG	SYSLOG local0	Apr 17 12:30:41 172.27.100.13 Mar 25 08:45:02 expc2 2020-03-25T08:45:02.236-05:00 expc2 tvcs:		ca593f38-d7ee-4798-9c23-8a085fe7c712	Call Disconnected	1	TLS	SIP	66.xx.xx.xx	7001
04/17/2020 12:30:41 PM	128	172.xx.xx.xx-SYSLOG	SYSLOG local0	Apr 17 12:30:41 172.27.100.13 Mar 25 08:45:02 expc2 2020-03-25T08:45:02.257-05:00 expc2 tvcs:		74a95e20-6a72-473f-93ea-82e3dcd7014e	Call Disconnected	1	TLS	SIP	10.xx.xx.xx	5073

Figure 2

- **Cisco Expressway: Configuration Changes** - This report gives the information about all the Configuration changes performed. Reports contains Event details, Node and PID of the event and other useful information.

LogTime	EventId	Computer	EventSource	EventDescription	Details	Node	PID
04/17/2020 12:30:30 PM	128	172.xx.xx.xx-SYSLOG	SYSLOG local0	Apr 17 12:30:30 172.27.100.13 Mar 25 08:54:00 expc2 2020-03-25T08:54:00.786-05:00 expc2 UTCTime="2020-03-25 13:54:00,786"	xconfiguration edgeConfigProvisioningCredentialC	clusterdb@127.xx.xx.xx	<0.473.0>
04/17/2020 12:30:30 PM	128	172.xx.xx.xx-SYSLOG	SYSLOG local0	Apr 17 12:30:30 172.27.100.13 Mar 25 08:54:00 expc2 2020-03-25T08:54:00.789-05:00 expc2 UTCTime="2020-03-25 13:54:00,789"	xconfiguration edgeConfigProvisioningTokenConfi	clusterdb@127.xx.xx.xx	<0.329.0>
04/17/2020 12:30:37 PM	128	172.xx.xx.xx-SYSLOG	SYSLOG local0	Apr 17 12:30:37 172.27.100.13 Mar 25 08:49:03 expc2 2020-03-25T08:49:03.147-05:00 expc2 UTCTime="2020-03-25 13:49:03,146"	xconfiguration edgeConfigProvisioningCredentialC	clusterdb@127.xx.xx.xx	<0.473.0>

Figure 3

- **Cisco Expressway: Authentication Success** - This report gives information about all the successful authentication detected in Cisco Expressway. Report contains IP address, username, event type, and other useful information.

LogTime	EventId	Computer	EventSource	Username	Log Priority	Event	Details	Source IP	EventDescription
04/15/2020 04:43:25 PM	128	172.xx.xx.xx-SYSLOG	SYSLOG local0	njoynt	INFO		Authenticated user successfully	192.xx.xx.xx	Apr 15 16:43:25 172.27.100.13 Mar 25 08:54:00 e 2020-03-25T08:54:00.783-05:00 expc2
04/15/2020 05:36:34 PM	128	172.xx.xx.xx-SYSLOG	SYSLOG local0	njoynt	INFO		Authenticated user successfully	192.xx.xx.xx	Apr 15 17:36:34 172.27.100.13 Mar 25 08:54:00 e 2020-03-25T08:54:00.783-05:00 expc2
04/15/2020 05:36:52 PM	128	172.xx.xx.xx-SYSLOG	SYSLOG local0	jablack	INFO		Authenticated user successfully	70.xx.xx.xx	Apr 15 17:36:52 172.27.100.13 Mar 25 08:42:43 e 2020-03-25T08:42:43.206-05:00 expc2 edgeconfigprovisioning: Level="INFO"

Figure 4

Logs Considered

category	+ - Call Attempted
event_category	+ - 0
event_computer	+ - 172.27.100.13-syslog
event_datetime	+ - 4/17/2020 1:09:34 PM
event_datetime_utc	+ - 1587109174
event_description	Apr 17 13:09:34 172.27.100.13 Mar 25 08:42:12 expc2 2020-03-25T08:42:12.686-05:00 ex 001" Src-alias-type="SIP" Src-alias="sip:11101@192.168.222.2" Dst-alias-type="SIP" Dst e-4798-9c23-8a085fe7c712" Tag="d2b5d64c-7ed6-4c1d-9468-3e413cbfb82a" Protocol=
event_group_name	+ - Default
event_id	+ - 128
event_log_type	+ - Application
event_source	+ - SYSLOG local0
event_type	+ - Error
event_user_domain	+ - N/A
event_user_name	+ - N/A
group_name	+ - SIP
log_action	+ - YES
log_priority	+ - 1
log_source	+ - Cisco Expressway
log_type	+ - tvcs
protocol_type	+ - TLS
source_type	+ - Cisco Expressway
src_ip_address	+ - 66.6.124.199
src_ip_address_geoip.city_name	+ - Buckner
src_ip_address_geoip.continent_name	+ - North America
src_ip_address_geoip.country_iso_code	+ - US
src_ip_address_geoip.region_name	+ - Missouri
src_ip_address_geoip.location.lat	+ - 39.117
src_ip_address_geoip.location.lon	+ - -94.2118
src_port_no	+ - 7001

Figure 5

4.4 Dashboards

- **Cisco Expressway: Authentication Failure**

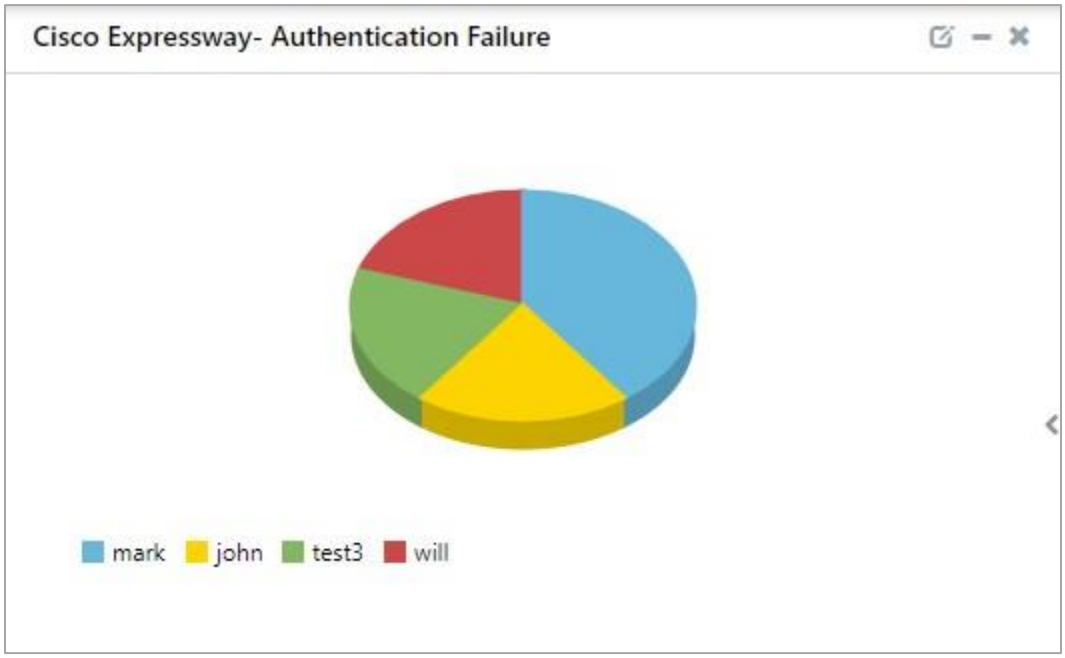

Figure 6

- **Cisco Expressway: Authentication Success**

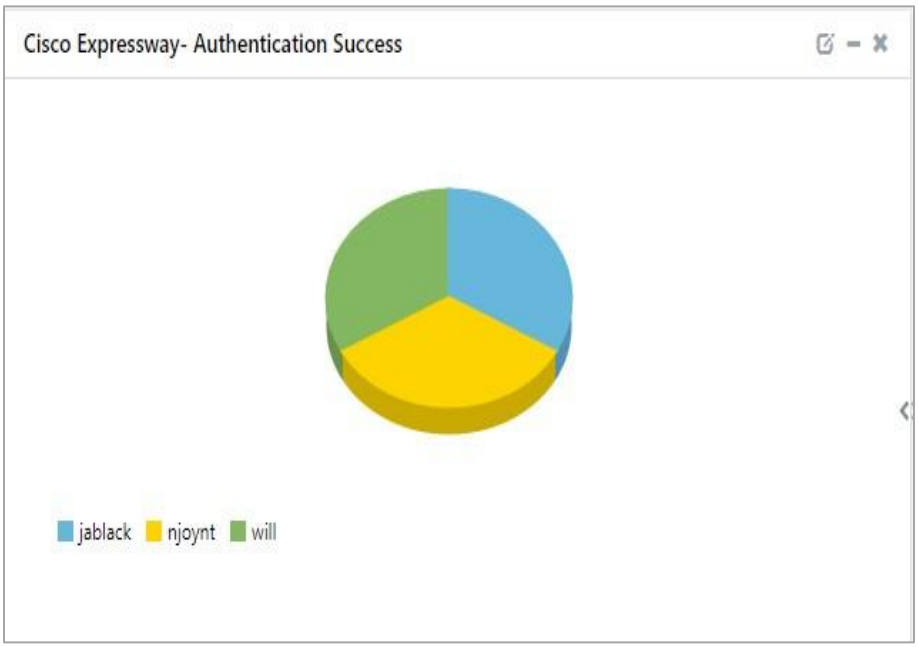

Figure 7

- **Cisco Expressway: Call Activity**

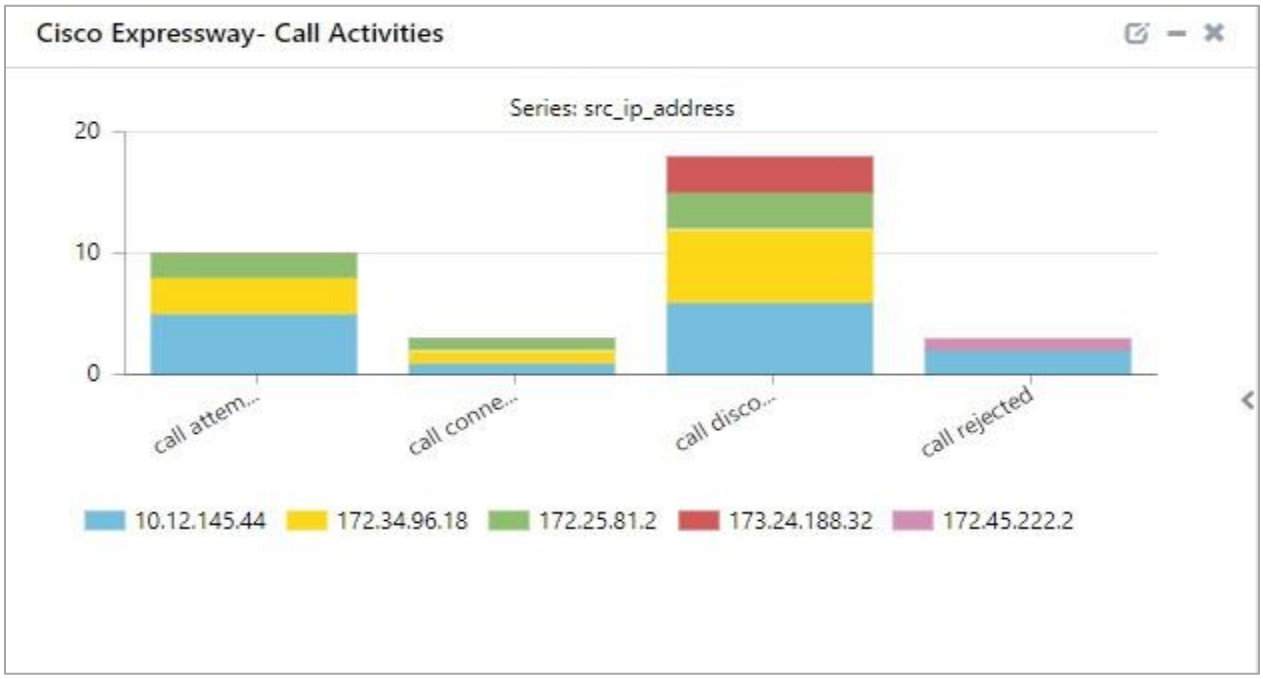

Figure 8

- **Cisco Expressway: User Location**

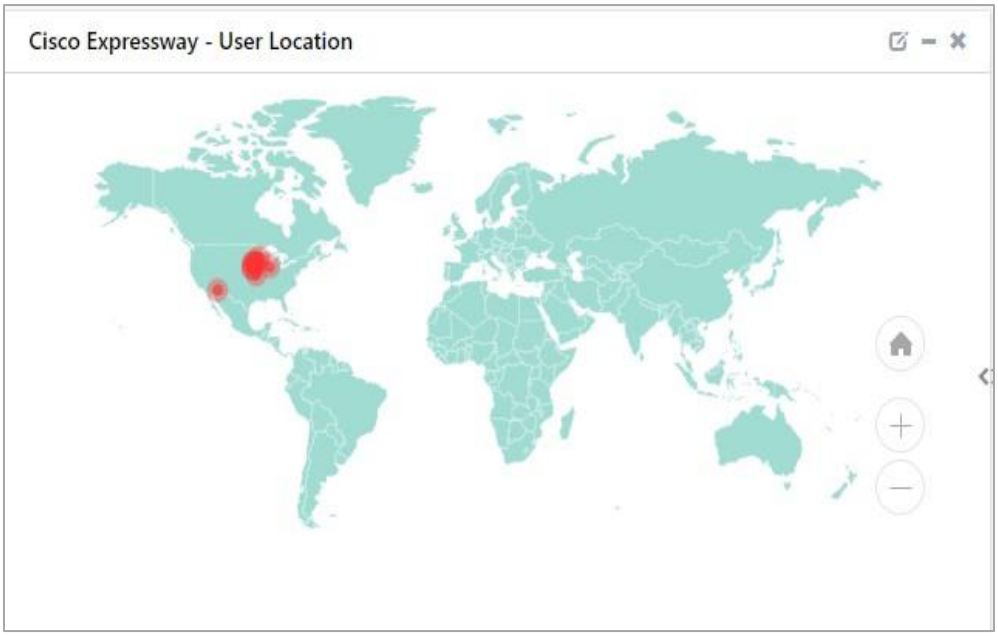

Figure 9

- **Cisco Expressway: License Manager Activity**

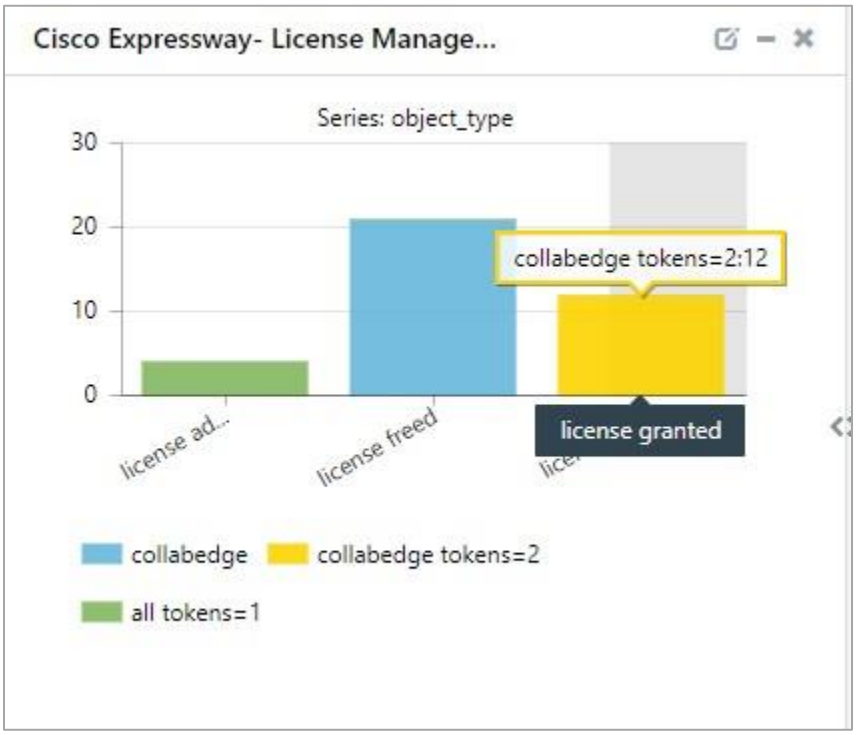

Figure 10

- **Cisco Expressway: Session detail**

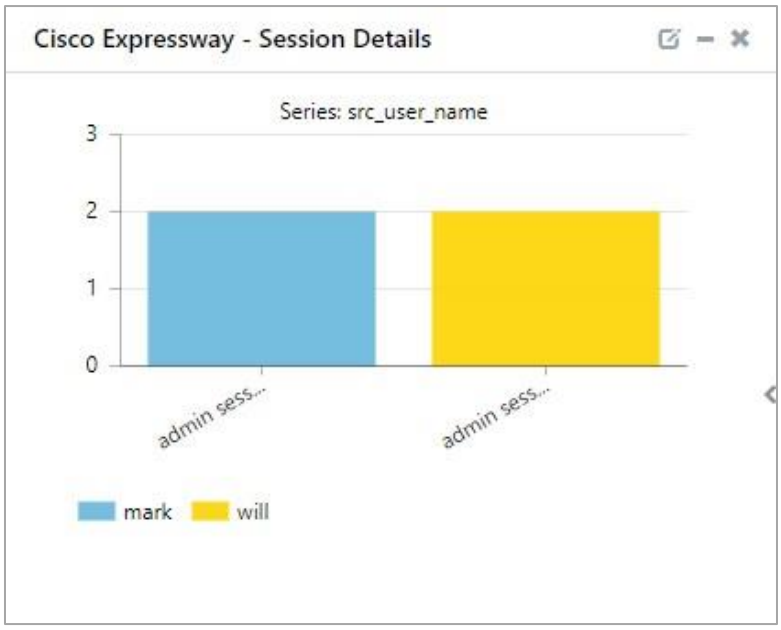

Figure 11

- **Cisco Expressway: B2B User Activity**

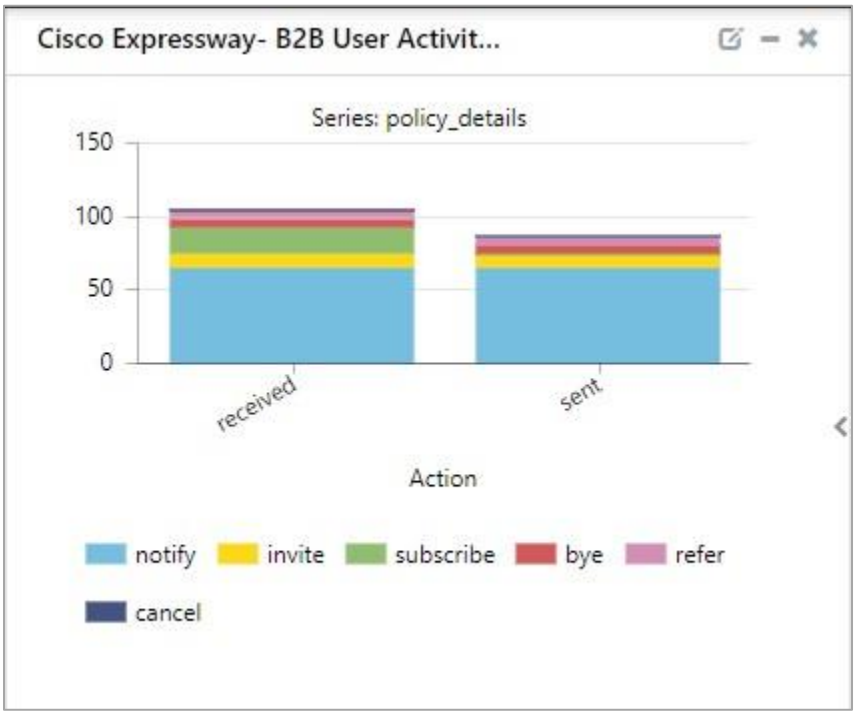

Figure 12

5. Importing Cisco Expressway knowledge pack into EventTracker

NOTE: Import knowledge pack items in the following sequence:

- Category
- Alert
- Knowledge Object
- Report
- Dashboard

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

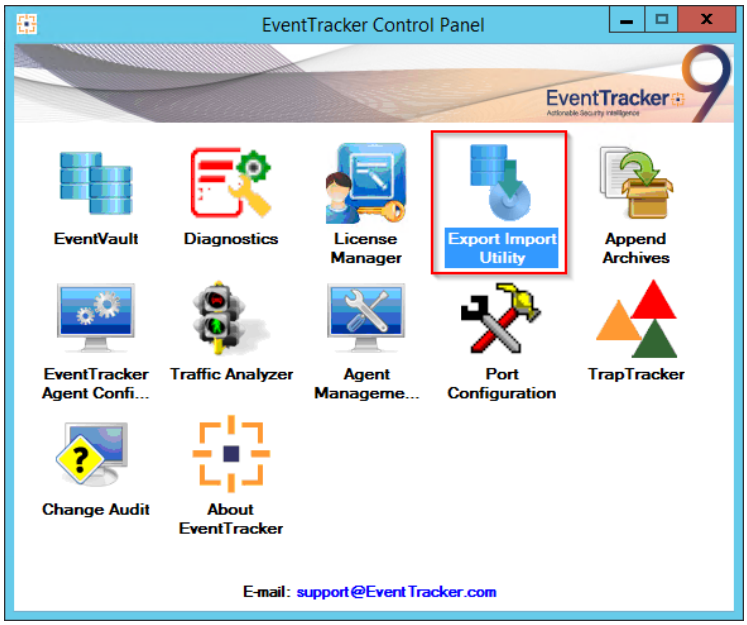

Figure 13

3. Click the **Import** tab.

5.1 Category

1. Click **Category** option, and then click **Browse** ... .

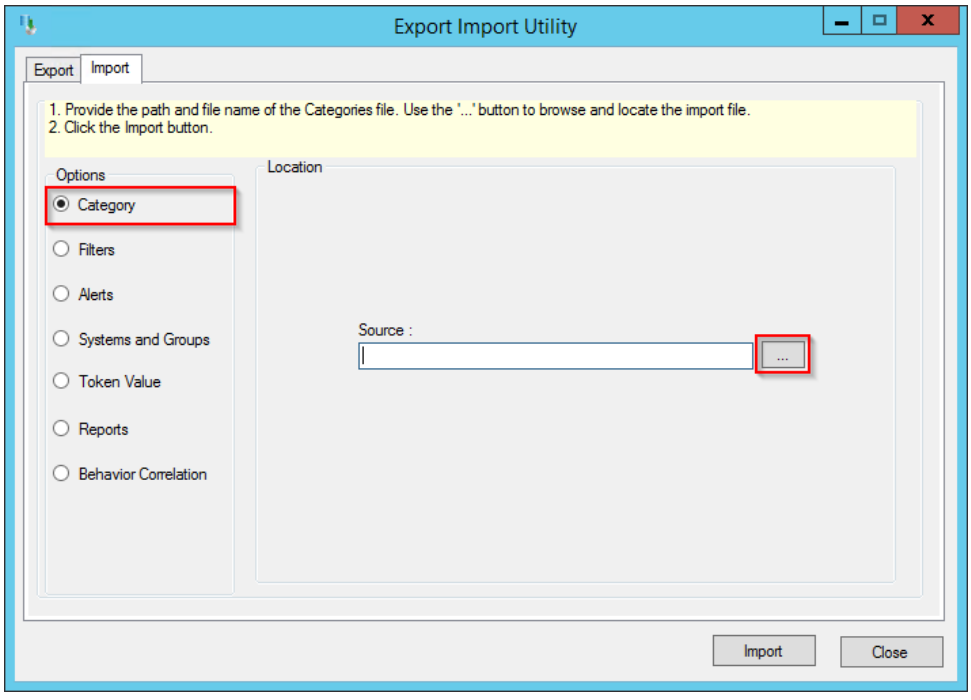

Figure 14

2. Locate **Category_Cisco Expressway.iscat** file, and then click **Open**.

3. To import categories, click **Import**.

   EventTracker displays success message.

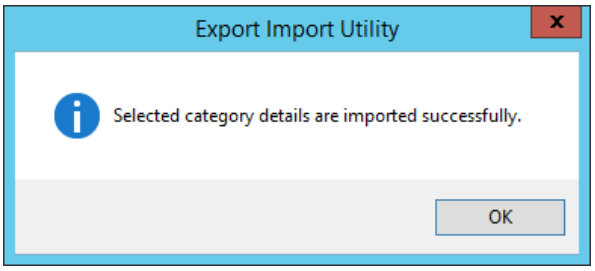

Figure 15

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

5.2 Alert

1. Click **Alert** option, and then click **Browse** ... .

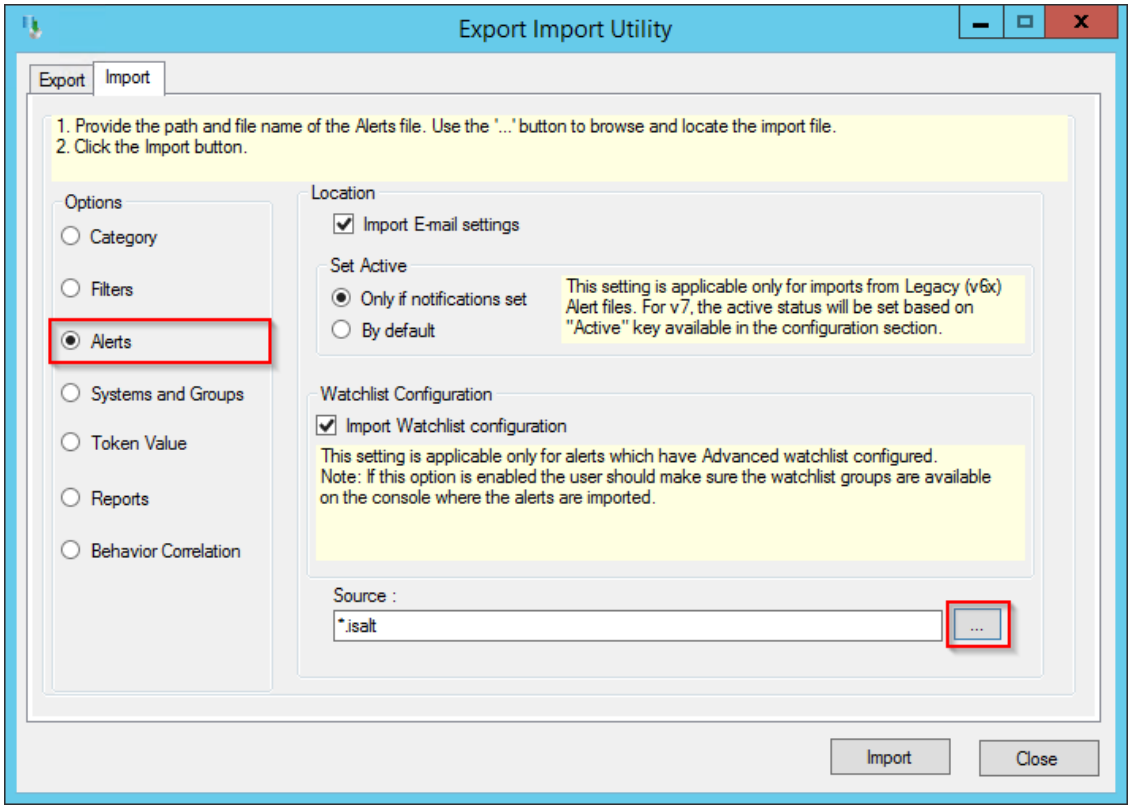

Figure 16

2. Locate **Alert_Cisco Expressway.isalt** file, and then click **Open**.

3. To import alerts, click **Import**.
   EventTracker displays success message.

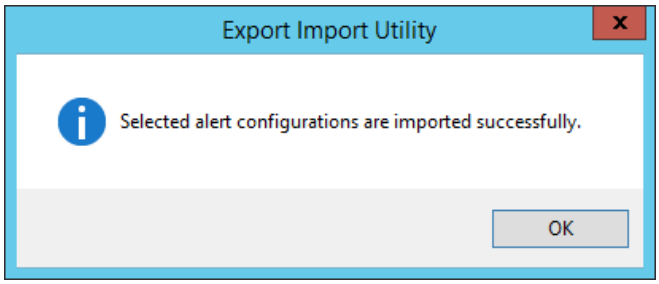

Figure 17

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

5.3 Knowledge Object

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

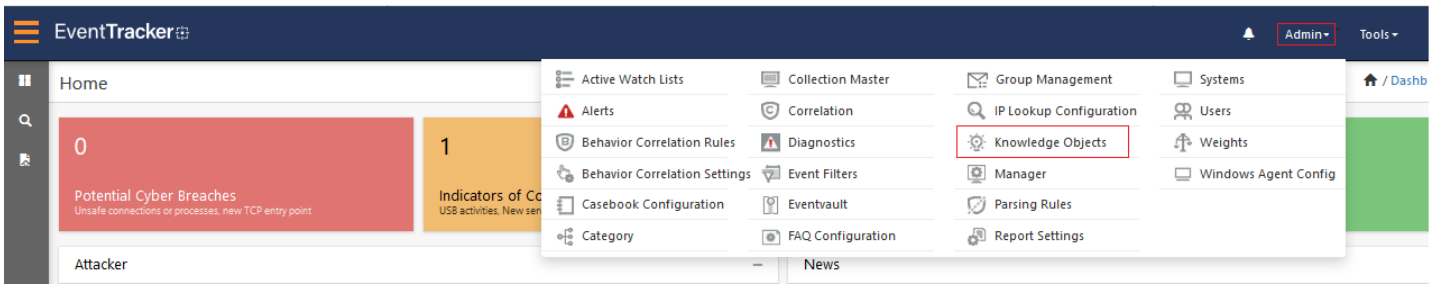

Figure 18

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

Figure 19

3. Click **Browse**.

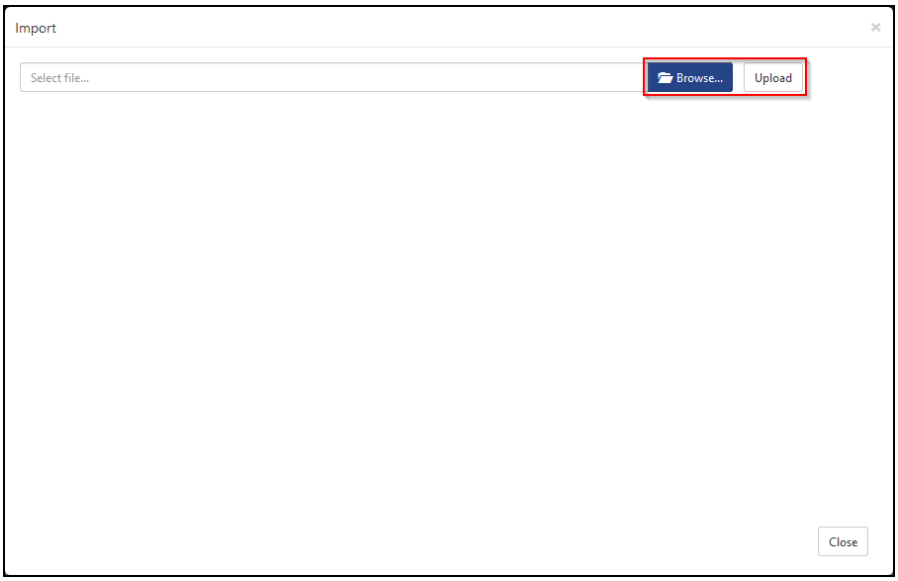

Figure 20

4. Locate the file named **KO_Cisco Expressway.etko**.
5. Now select the check box and then click on **Import** option.

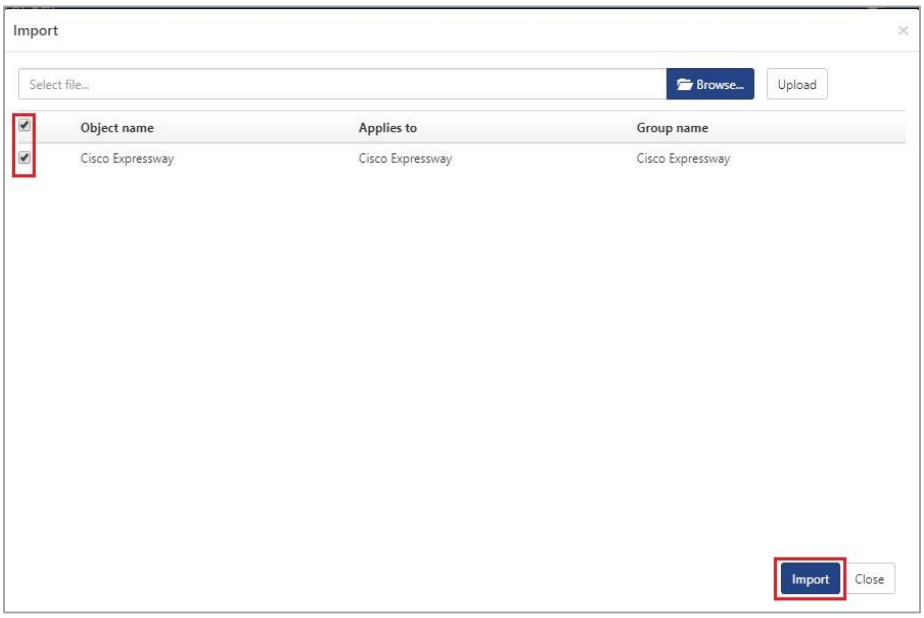

Figure 21

6. Knowledge objects are now imported successfully.

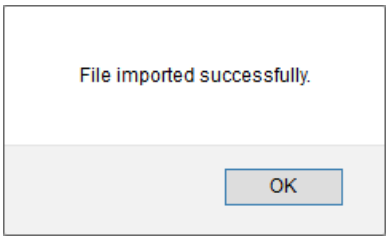

Figure 22

5.4 Report

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

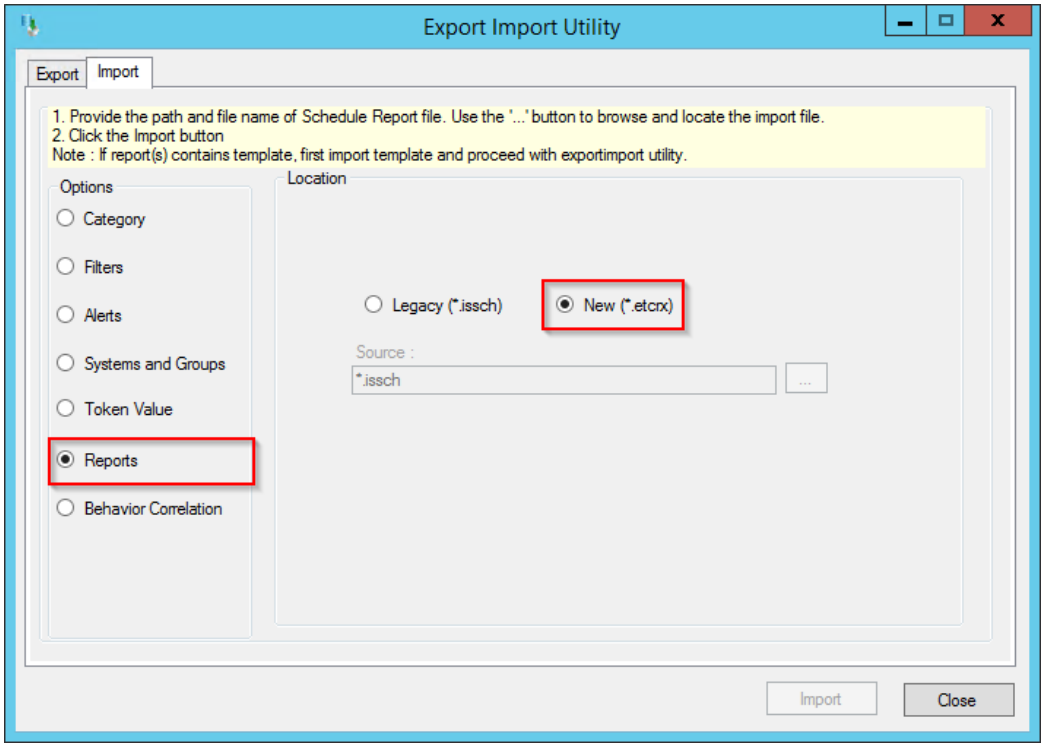

Figure 23

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

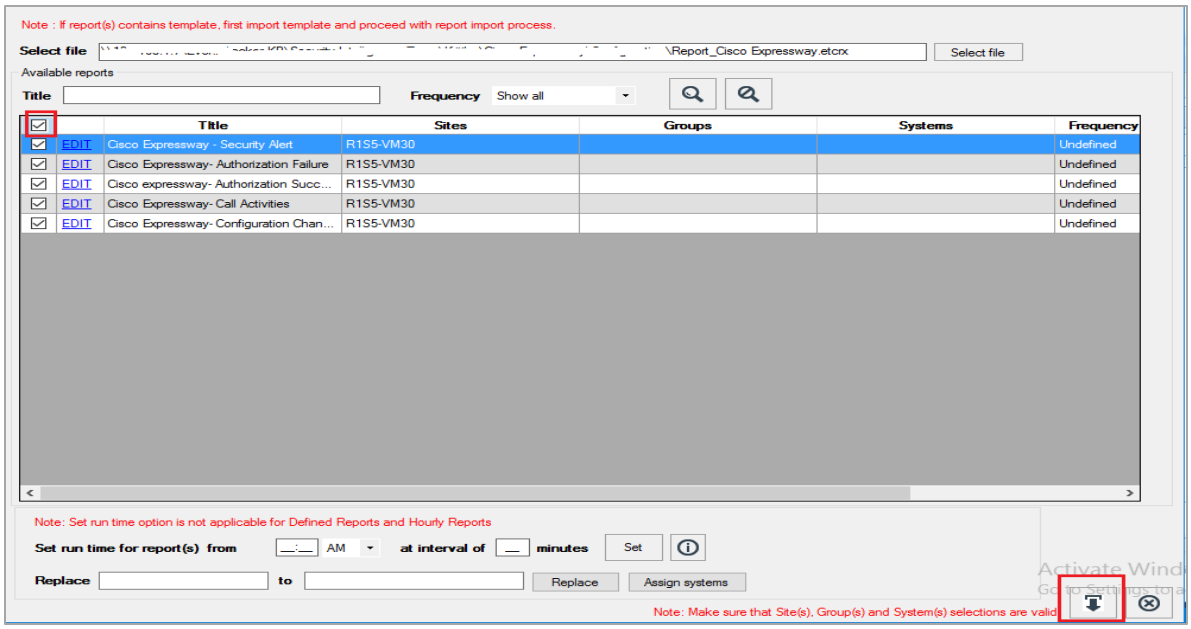

Figure 24

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

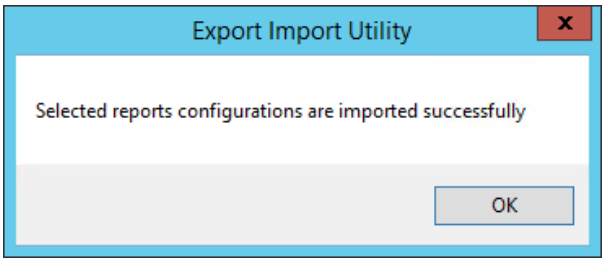

Figure 25

5.5 Dashboards

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

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

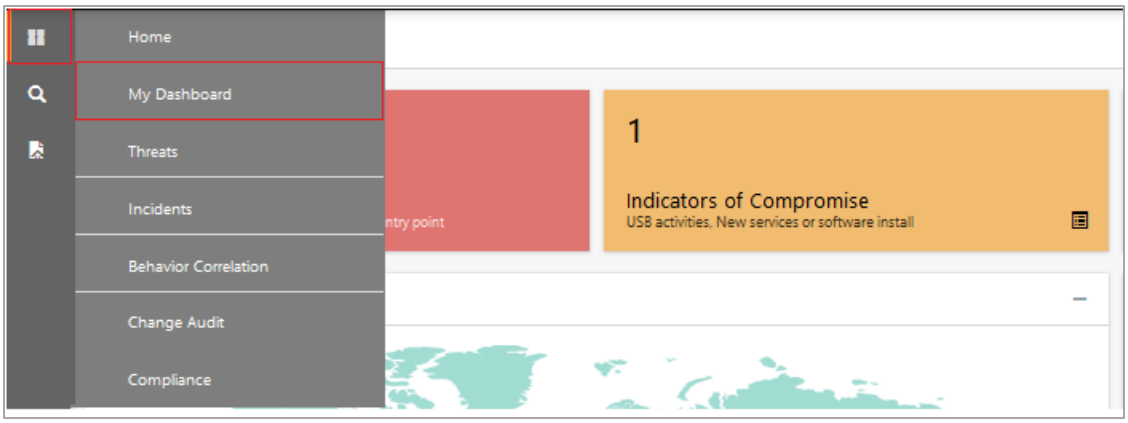

Figure 26

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

Figure 27

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

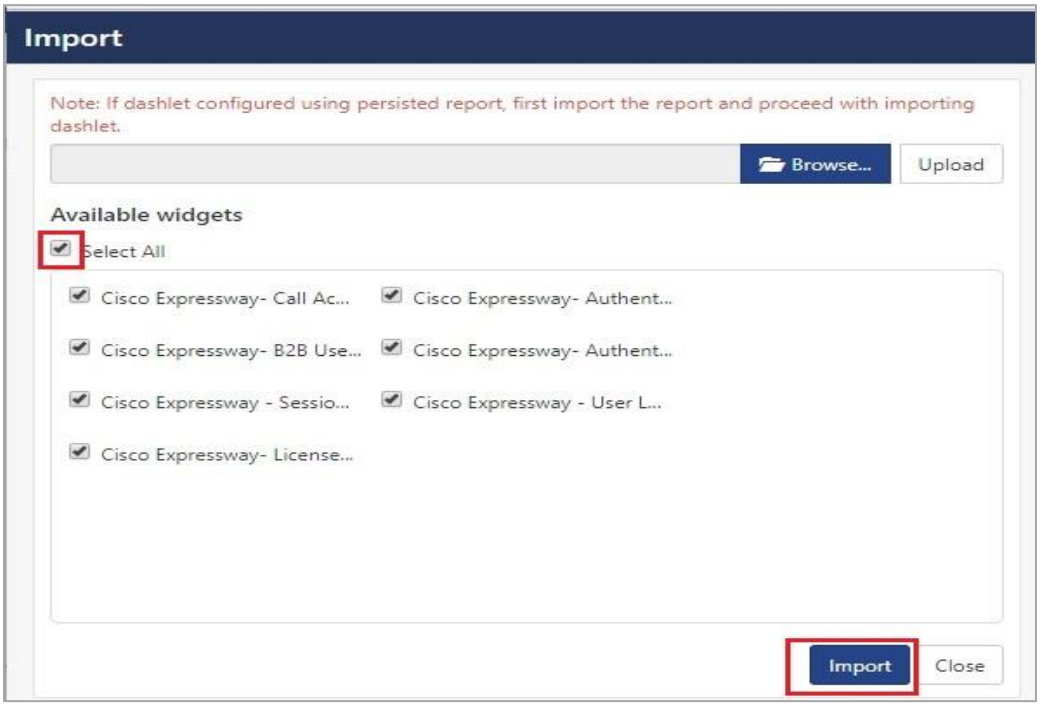

Figure 28

6. Import is now completed successfully.

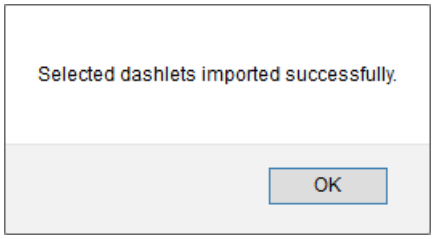

Figure 29

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

Figure 30

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

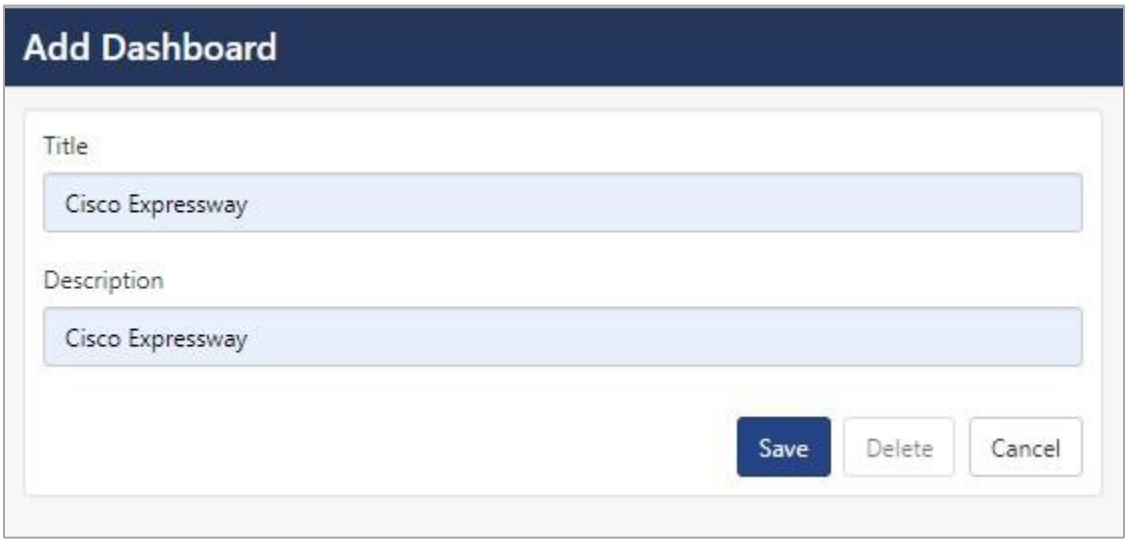

Figure 31

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

Figure 32

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

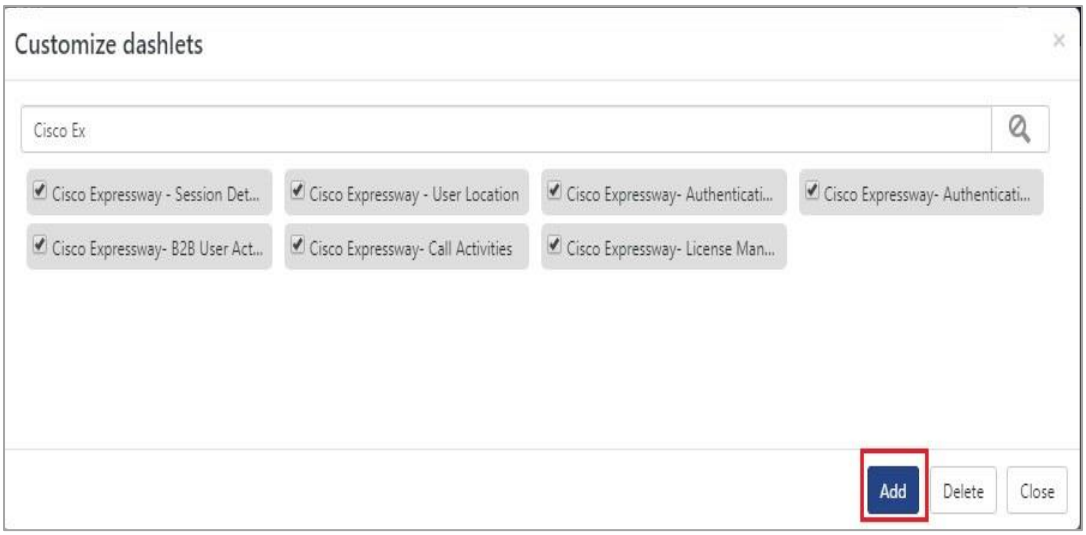

Figure 33

6. Verifying Cisco Expressway knowledge pack in EventTracker

6.1 Category

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

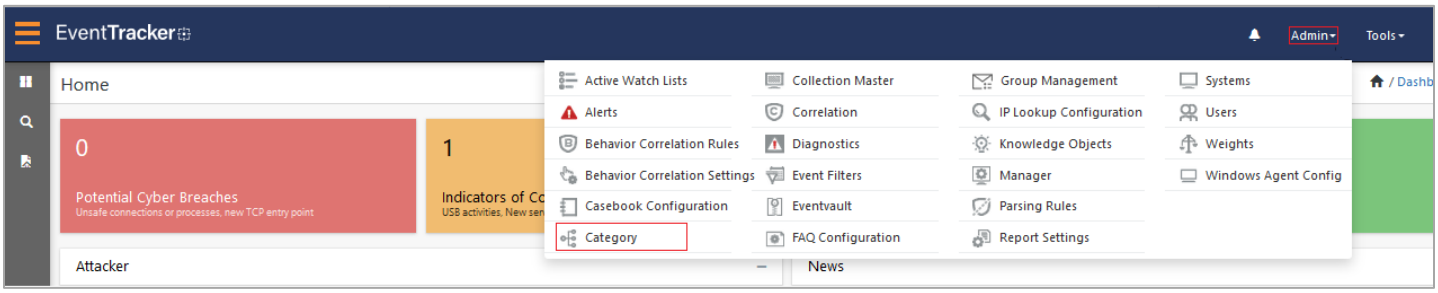

Figure 34

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

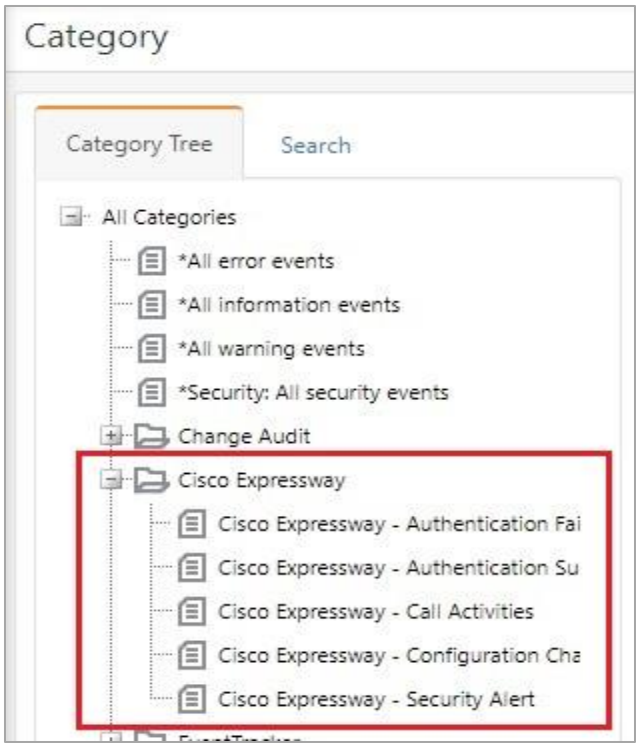

Figure 35

6.2 Alert

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

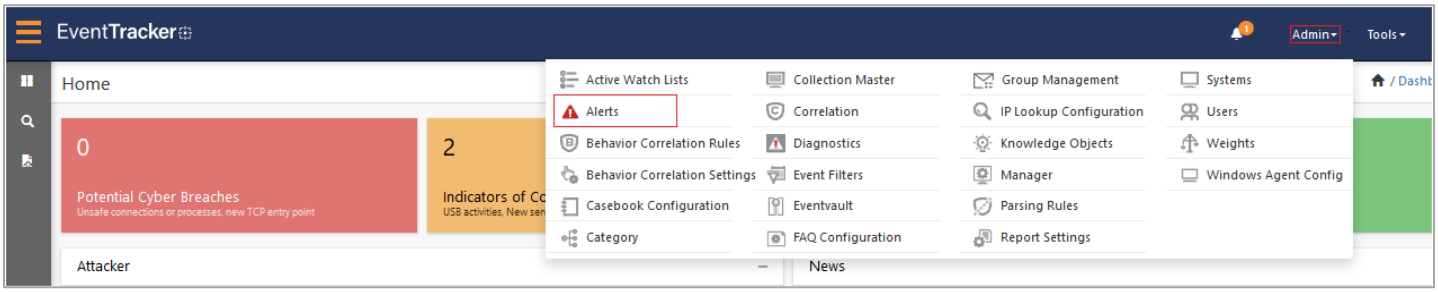

Figure 36

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

Figure 37

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

   EventTracker displays message box.

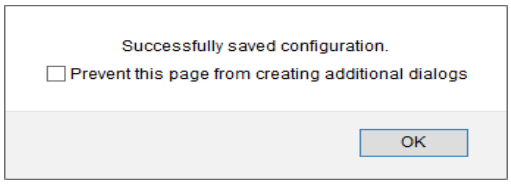

Figure 38

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

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

6.3 Knowledge Object

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

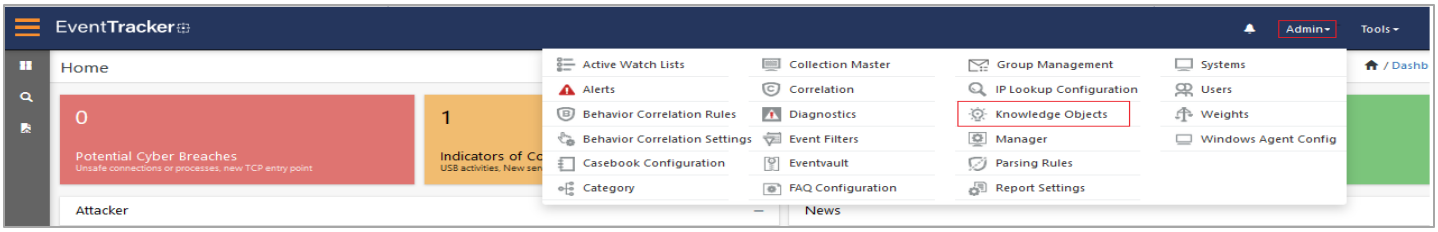

Figure 39

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

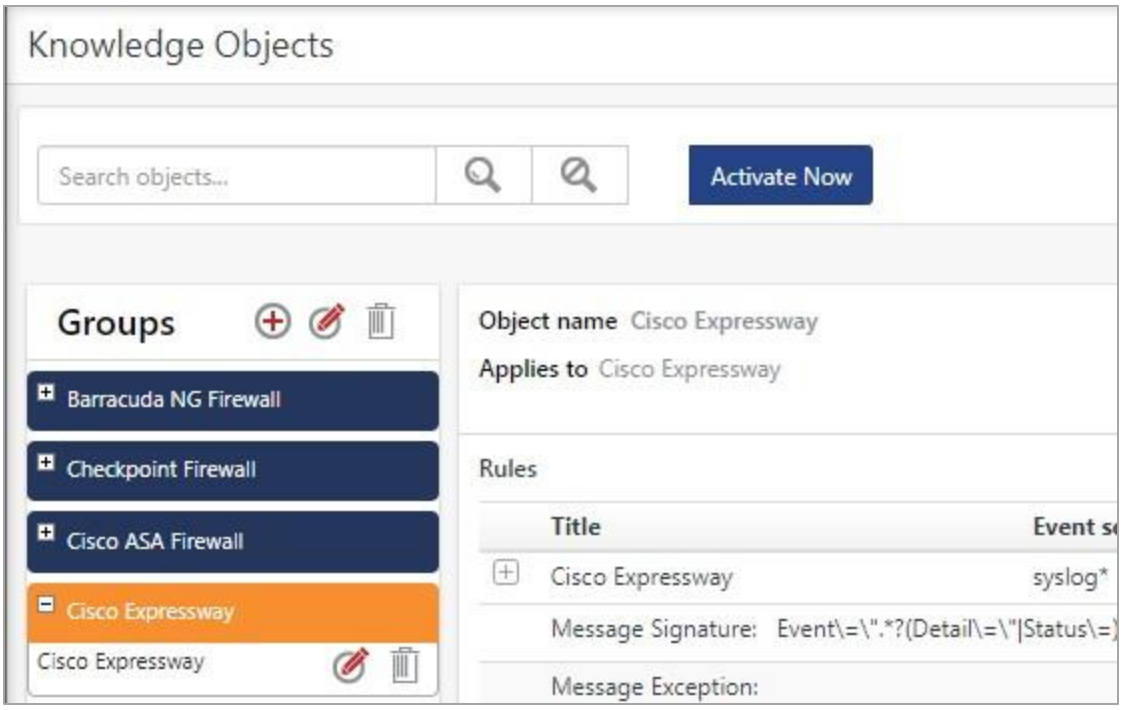

Figure 40

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

6.4 Report

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

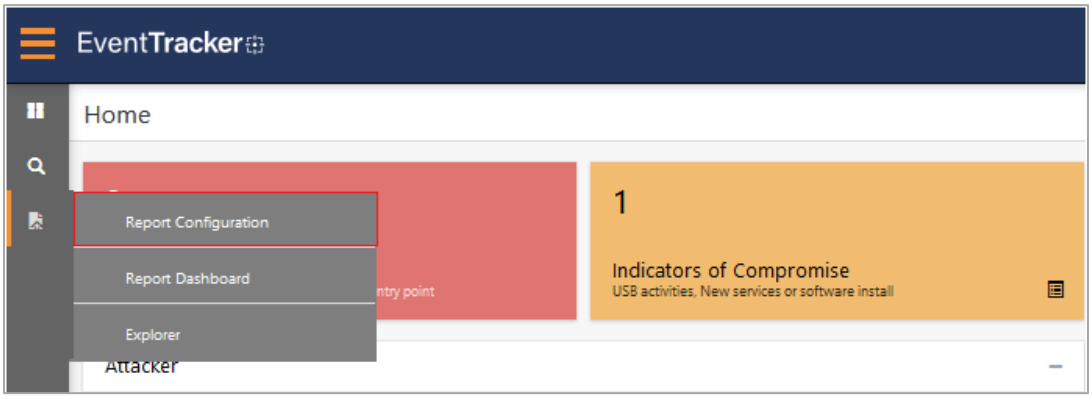

Figure 41

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

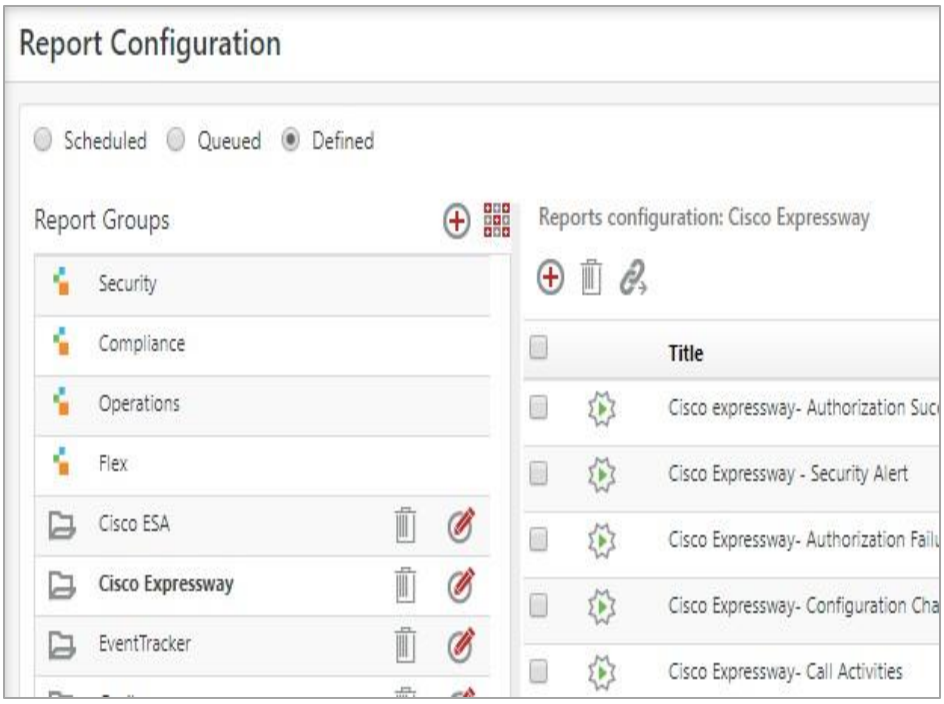

Figure 42

6.5 Dashboards

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

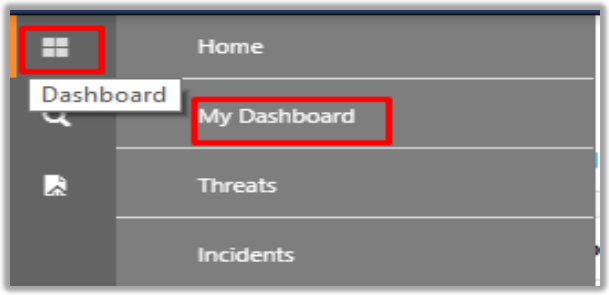

Figure 43

2. In the "**Cisco Expressway**" dashboard you should be now able to see something like this.

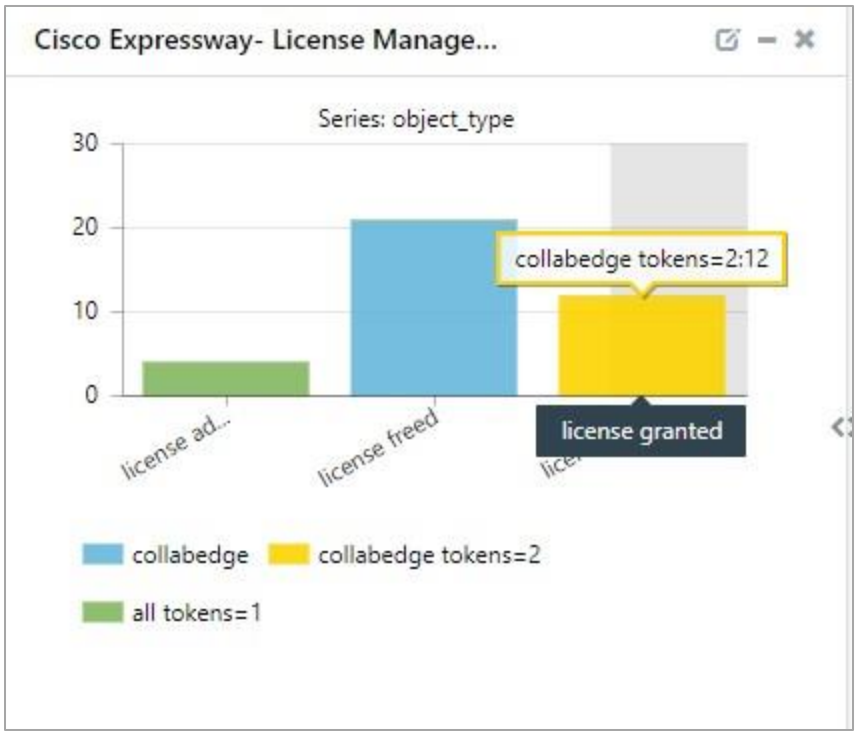
Cisco Expressway- License Manage...
Series: object_type
30
20
10
0
collabedge tokens=2:12
license granted
license ad...
license freed
collabedge
collabedge tokens=2
all tokens=1

Figure 44