

# Integrate Cisco Switch

## Abstract

This guide provides instructions to configure Cisco Switch to send the syslog events to EventTracker.

## Scope

The configurations detailed in this guide are consistent with **EventTracker** version 7.x and later, and **Cisco Switch 12.x and 15.x**.

## Audience

Administrators, who are responsible for monitoring Cisco Switch devices using EventTracker Manager.

*The information contained in this document represents the current view of EventTracker. on the issues discussed as of the date of publication. Because EventTracker must respond to changing market conditions, it should not be interpreted to be a commitment on the part of EventTracker, and EventTracker cannot guarantee the accuracy of any information presented after the date of publication.*

*This document is for informational purposes only. EventTracker MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.*

*Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from EventTracker, if its content is unaltered, nothing is added to the content and credit to EventTracker is provided.*

*EventTracker may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from EventTracker, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.*

*The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.*

*© 2017 EventTracker Security LLC. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.*

# Table of Contents

Abstract .....	1
Scope .....	1
Audience .....	1
Overview.....	3
Pre requisites.....	3
Configure Cisco Switch to send syslog to EventTracker .....	3
EventTracker Knowledge Pack (KP).....	4
Categories.....	4
Alerts .....	5
Reports .....	5
Import Cisco Switch Knowledge Pack into EventTracker .....	9
Categories.....	10
Alerts .....	11
Templates .....	12
Flex Reports.....	13
Verify Cisco Switch knowledge pack in EventTracker .....	15
Categories.....	15
Alerts .....	15
Template.....	17
Flex Reports.....	17
Create Dashboards in EventTracker .....	18
Schedule Reports.....	18
Create Dashlets .....	21
Sample Dashboards.....	25

## Overview

Switches are used to connect multiple devices together on the same network. In a properly designed network, LAN switches are responsible for directing and controlling the data the flow at the access layer to networked resources.

EventTracker compiles and inspects critical events to provide an administrator insight on user behavior, traffic anomalies, link flaps etc.

**NOTE: Applicable to the following series of switch 2600,2800,1900,2900,3900,4500,6500 with IOS 12.x and 15.x**

## Pre requisites

- EventTracker v7.x or later should be installed.
- Cisco Switch devices with software release version IOS 12.4 or higher.

## Configure Cisco Switch to send syslog to EventTracker

To enable and configure Cisco Switch for Syslog,

1. Enter global configuration mode and type the command **Router# configure terminal**

2. To specify **syslog server**, type the command -

**Router(config)#logging host**

It specifies the EventTracker Manager by IP address or host name.

3. To specify **Severity level**, type the command -

**Router(config)# logging trap level**

- Informational: 6

4. To specify **facility level**, type the command **Router(config)# logging facility facility-level**.

The default is local7. Possible values are local0, local1, local2, local3, local4, local5, local6 and local7.

# EventTracker Knowledge Pack (KP)

Once logs are received in to EventTracker; Alerts and Reports can be configured into EventTracker. The following Knowledge Packs are available in EventTracker to support Cisco Switch monitoring.

## Categories

- **Cisco Switch: Access control list** - This category provides information related to access control list.
- **Cisco Switch: Access information element** - This category provides information related to access information element.
- **Cisco Switch: Accounting services** - This category provides information related to accounting services.
- **Cisco Switch: Adapter messages** - This category provides information related to adapter messages.
- **Cisco Switch: Adjacency subsystem** - This category provides information related to adjacency subsystem.
- **Cisco Switch: Administration** - This category provides information related to administration.
- **Cisco Switch: Advance integration module** - This category provides information related to advance integration module.
- **Cisco Switch: Advanced interface module** - This category provides information related to advanced interface module.
- **Cisco Switch: Airline protocol support** - This category provides information related to airline protocol support.
- **Cisco Switch: Alarm interface controller mgmt** - This category provides information related to alarm interface controller management.
- **Cisco Switch: Align messages** - This category provides information related to align messages.
- **Cisco Switch: Archive configuration** - This category provides information related to archive configuration.
- **Cisco Switch: Asynchronous security protocol** - This category provides information related to asynchronous security protocol.
- **Cisco Switch: ATM interface processor** - This category provides information related to ATM interface processor.
- **Cisco Switch: ATM line card** - This category provides information related to ATM line card.
- **Cisco Switch: Attachment circuit** - This category provides information related to attachment circuit.
- **Cisco Switch: Authentication failure** - This category provides information related to authentication failure.
- **Cisco Switch: Authentication proxy** - This category provides information related to authentication proxy.
- **Cisco Switch: Automatic protection switching** - This category provides information related to automatic protection switching.
- **Cisco Switch: Cache messages** - This category provides information related to cache messages.
- **Cisco Switch: Chassis alarm** - This category provides information related to chassis alarm.

- **Cisco Switch: Ethernet devices** - This category provides information related to Ethernet devices.
- **Cisco Switch: Hardware device error** - This category provides information related to hardware device error.
- **Cisco Switch: HTTP subsystem** - This category provides information related to HTTP subsystem.
- **Cisco Switch: Intrusion detection** - This category provides information related to intrusion detection.
- **Cisco Switch: Networks** - This category provides information related to networks.

## Alerts

- **Cisco Switch: Interface down or detached** - This alert is generated when interface down or detached event occurs.
- **Cisco Switch: Internal software error** - This alert is generated when internal software error occurs.
- **Cisco Switch: Line protocol down** - This alert is generated when line protocol is down.
- **Cisco Switch: Runaway processes** - This alert is generated when runaway processes occur.

## Reports

- **Cisco Switch -Configuration changed**

This report provides information related to configuration changes which include Device Address, User Name, and Command Issued fields.

```
%FR_VCB-5-UPDOWN: FR VC-Bundle NYKLAXLINK changed state to InActive
```

LogTime	Computer	Message	Facility Code
12/08/2016 05:05:27 PM	CISCO-IOS9	Controller server, changed state to Active due to unknown	CONTROLLER-5-DOWNDETAIL
12/08/2016 05:05:27 PM	CISCO-IOS9	Dot1x unable to start.	DOT1X-4-PROC_START_ERR

- **Cisco Switch -Access denied**

This report provides information related to connection denial events occurring on router or switch which includes Source address, Source Port, Destination Address, Destination port and Packets Transferred fields.

```
Nov 7 12:20:08.139 EST: %SW_DAI-4-ACL_DENY: 1 Invalid ARPs (Res) on Gi1/3, vlan 1502.([001d.e513.8ef1/10.1.1.65/001d.e513.8ef1/10.1.1.65/12:20:07 EST Fri Nov 7 2008])
```

LogTime	Computer	Source Address	Source Port	Destination Address	Destination Port	Protocol Type	Interface	VLAN Number	Packets Transferred	Reason
12/01/2016 04:39:01 PM	CISCO-IOS	192.168.10.112	4206	65.55.127.194	80					Access denied URL http://www.websense.com
12/01/2016 04:39:01 PM	CISCO-IOS	170.1.1.2		170.1.1.1			Gi3/31	100	9	Invalid ARPs (Req)
12/01/2016 04:39:01 PM	CISCO-IOS	192.168.10.112	4206	65.55.127.194	80					Access denied URL http://www.websense.com
12/01/2016 04:39:01 PM	CISCO-IOS	192.168.0.5		192.168.0.1			Fa0/5	100	1	Invalid ARPs (Req)
12/01/2016 04:39:01 PM	CISCO-IOS	192.168.1.3	1024	192.168.2.1	22	tcp			1	list ACL-IPv4-E0/0-IN
12/01/2016 04:39:01 PM	CISCO-IOS	192.168.1.3	1024	192.168.2.1	22	tcp			1	list ACL-IPv4-E0/0-IN

- **Cisco Switch -Port status change**

This report provides information related to port status changed from UP to DOWN or vice versa which includes Device Address, Interface Name and Port Status fields.

**00:00:20: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to up**

LogTime	Computer	Facility Code	Message
01/03/2017 12:07:06 PM	CISCO-IOS1	PM-4-ERR_DISABLE	psecure-violation error detected on Fa4/4, putting Fa4/4 in err-disable state
01/03/2017 12:07:06 PM	CISCO-IOS1	PM-4-ERR_DISABLE	psecure-violation error detected on Fa4/4, putting Fa4/4 in err-disable state

- **Cisco Switch -User logon success**

This report provides information related to user logon success which includes User Name, Source Address and Source Port fields.

**Oct 16 09:32:37.657: %SEC\_LOGIN-5-LOGIN\_SUCCESS: Login Success [user: neteng] [Source: 0.0.0.0] [localport: 0] at 09:32:37 UTC Fri Oct 16 2009**

LogTime	User Name	Source IP Address	Local Port
12/01/2016 05:14:43 PM	David	10.10.2.32	22

- **Cisco Switch -User logon failure**

This report provides information related to user logon failure which includes User Name, Source Address, Source Port and Reason fields.

**Feb 9 2015 18:34:38.236 MSK: %SEC\_LOGIN-4-LOGIN\_FAILED: Login failed [user: rrr] [Source: 10.0.10.169] [localport: 23] [Reason: Login Authentication Failed] at 18:34:38 MSK Mon Feb 9 2015**

LogTime	User Name	Source IP Address	Local Port	Reason
12/01/2016 05:14:43 PM	David	10.10.2.32	22	Invalid login

- **Cisco Switch -Authentication failure**

This report provides information related to authentication failure that is whenever the user tries to login into one of the Cisco Switch.

**Sep 15 13:09:47.308: %GLBP-4-BADAUTH: Bad authentication received from 149.212.19.162, group**

LogTime	Computer	Facility Code	Client	Message
01/03/2017 04:09:22 PM	CISCO-IOS8	GLBP-4-UNAVAILABLE	192.23.43.23	Bad authentication received from 192.23.43.23, group 2
01/03/2017 04:09:22 PM	CISCO-IOS8	CRYPTO-6-UNAVAILABLE		Authentication method 192.23.12.2 failed with host accel

- **Cisco Switch -Administrative account activity**

This report provides information related to account activities that is done by the administrator.

**%AAA-5-USER\_LOCKED: User michel locked out on authentication failure**

LogTime	Computer	User Name	Reason	Admin Name
11/25/2016 07:12:17 PM	CISCO	Smith	locked out on authentication failure	
11/25/2016 07:12:17 PM	CISCO	Smith	failed attempts reset	Charles
11/25/2016 07:12:18 PM	CISCO	Smith	unlocked	Charles

- **Cisco Switch -VTP management**

This report provides information related to activities that occur and are related to VTP.

**%%VTP-2-MODE\_OFF\_PVLAN\_EXIST Format: VTP Mode changed to off as Private VLAN configuration exists**

LogTime	Computer	Facility Code	Message
01/03/2017 04:40:38 PM	CISCO-IOS2	VTP-4- BAD_STARTUP_VLAN_CONFIG_FILE Format	Failed to configure VLAN from startup-config. Fallback to use VLAN configuration file from non-volatile
01/03/2017 04:40:38 PM	CISCO-IOS2	SW_VLAN-3- VTP_PROTOCOL_ERROR	VTP protocol internal error: Version 1 device detected on Fa0/23



- **Cisco Switch-VLAN management**

This report provides information related to activities that occurs which are related to VLAN.

***%VLAN\_MGR-6-VLAN\_OPER\_STATUS\_CHG: VLAN 135367, status changed to Active***

LogTime	Computer	Facility Code	VLAN Name	Message
01/03/2017 04:24:29 PM	CISCO-IOS	CDP-4-NATIVE_VLAN_MISMATCH		Native VLAN mismatch discovered on GigabitEthernet0/1 (1), with Cisco500 FastEthernet0/3(99).VTP
01/03/2017 04:24:20 PM	CISCO-IOS	VLAN_MGR-6-VLAN_OPER_STATUS_CHG	135367	VLAN 135367, status changed to Active
01/03/2017 04:24:29 PM	CISCO-IOS	VLAN_MGR-6-VLAN_CREATED Format	accel	VLAN accel

- **Cisco Switch-Port security**

This report provides information related to port security violation.

***%PORT\_SECURITY-2-PSECURE\_VIOLATION: Security violation occurred, caused by MAC address 0023.339c.e1cf on port FastEthernet4/4***

LogTime	Computer	Facility Code	Message
01/03/2017 12:07:06 PM	CISCO-IOS1	PM-4-ERR_DISABLE	psecure-violation error detected on Fa4/4, putting Fa4/4 in err-disable state
01/03/2017 12:07:06 PM	CISCO-IOS1	PM-4-ERR_DISABLE	psecure-violation error detected on Fa4/4, putting Fa4/4 in err-disable state
01/03/2017 12:07:06 PM	CISCO-IOS1	PORT_SECURITY-2-PSECURE_VIOLATION	Security violation occurred, caused by MAC address 0023.339c.e1cf on port FastEthernet4/4.
01/03/2017 12:07:06 PM	CISCO-IOS1	PM-4-ERR_RECOVER	Attempting to recover from psecure-violation err-disable state on Fa4/4

# Import Cisco Switch Knowledge Pack into EventTracker

1. Launch **EventTracker Control Panel**.
2. Double click **Export Import Utility**, and then click the **Import** tab.

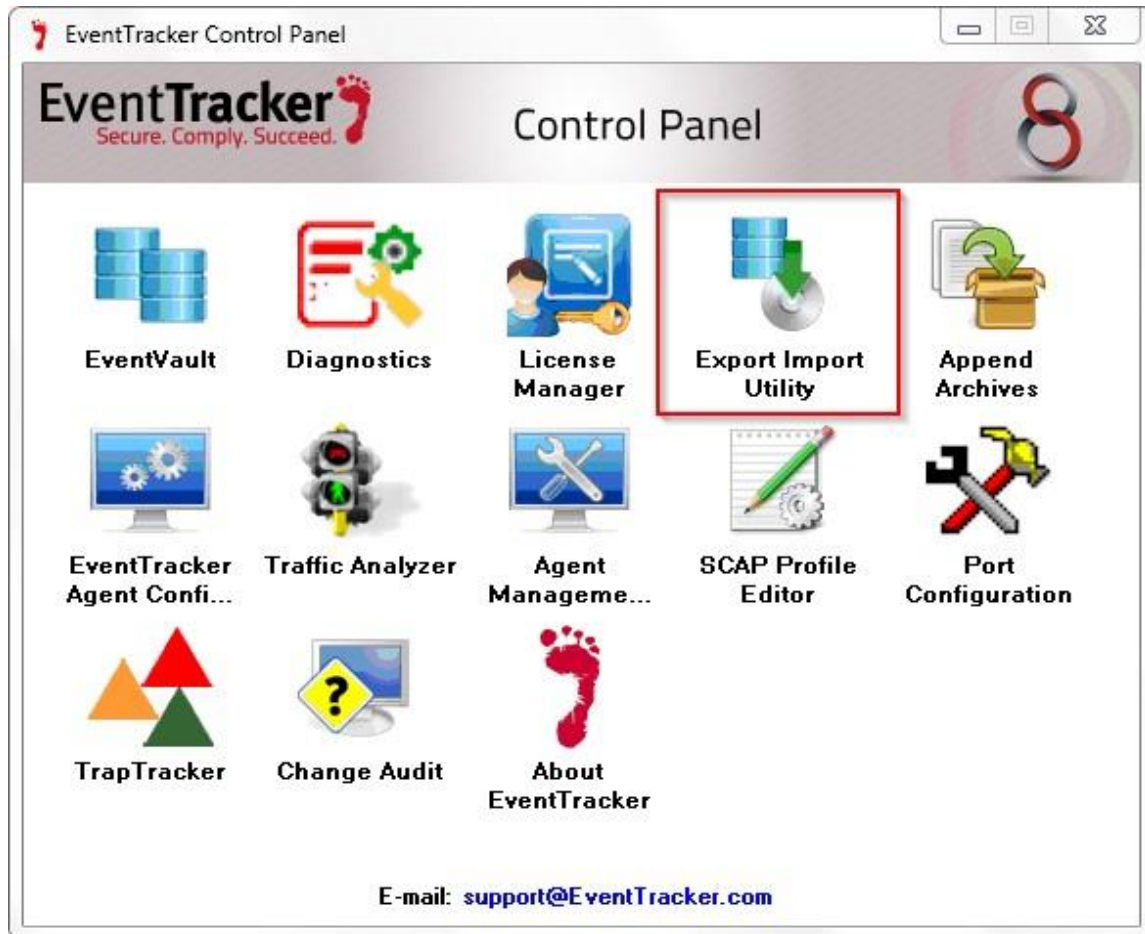


Figure 1

Import in the same order as mentioned:

**Templates**

**Categories**

**Alerts**

**Reports** as given below:

## Categories

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

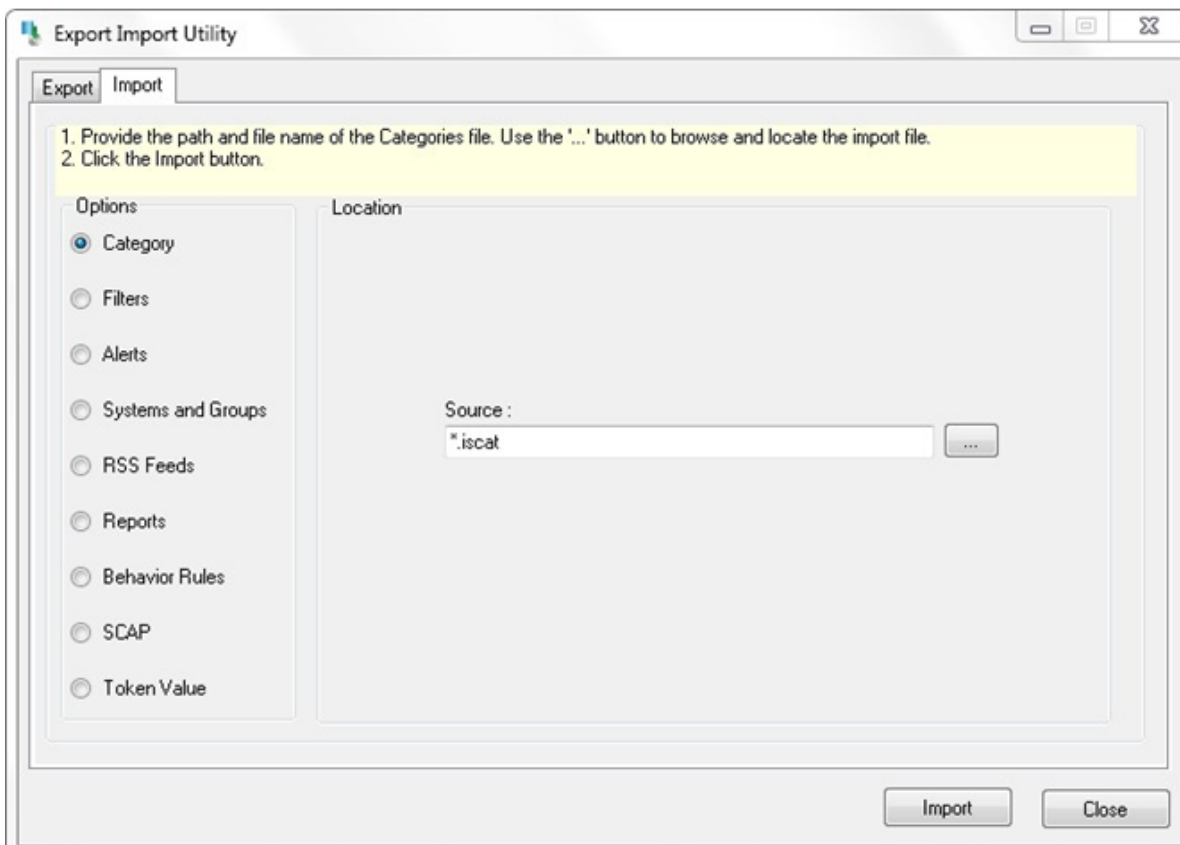


Figure 2

2. Locate **All Cisco Switch group of Categories.iscat** file, and then click the **Open** button.
3. To import the categories, click the **Import** button.  
EventTracker displays success message.

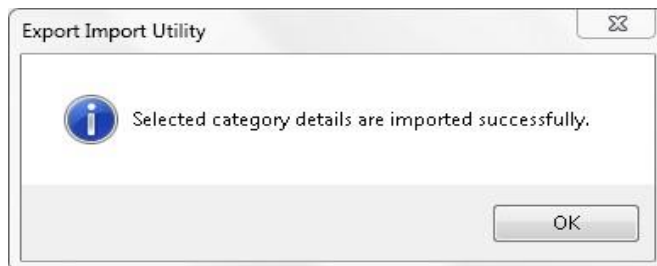


Figure 3

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

## Alerts

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

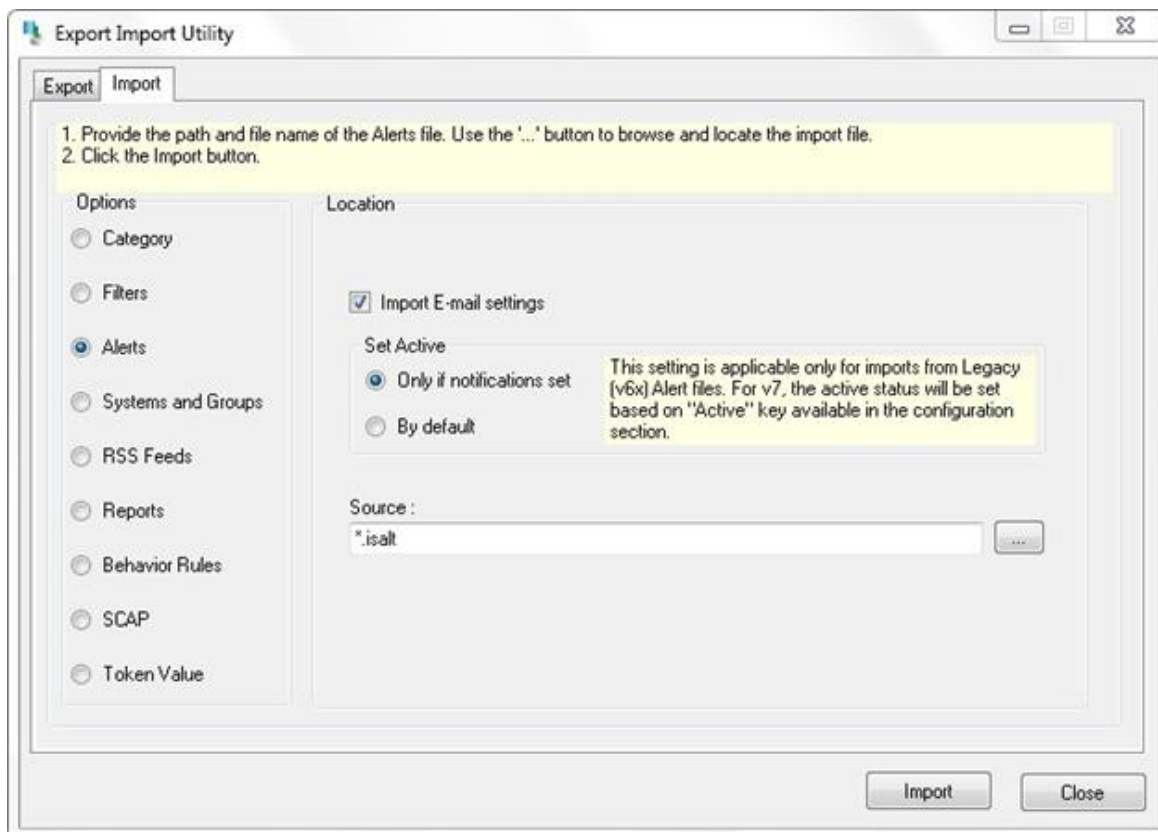


Figure 4

2. Locate **All Cisco Switch group of Alerts.isalt** file, and then click the **Open** button.
3. To import alerts, click the **Import** button.  
EventTracker displays success message.




Figure 5

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

**NOTE:** You can select alert notification such as Beep, Email, and Message etc. Select the respective checkbox in the Alert management page, and then click the **Activate Now** button.

## Templates

1. Click the **Admin** menu, and then click **Parsing rule**.
2. Select **Template** tab, and then click on  **'Import'** option.

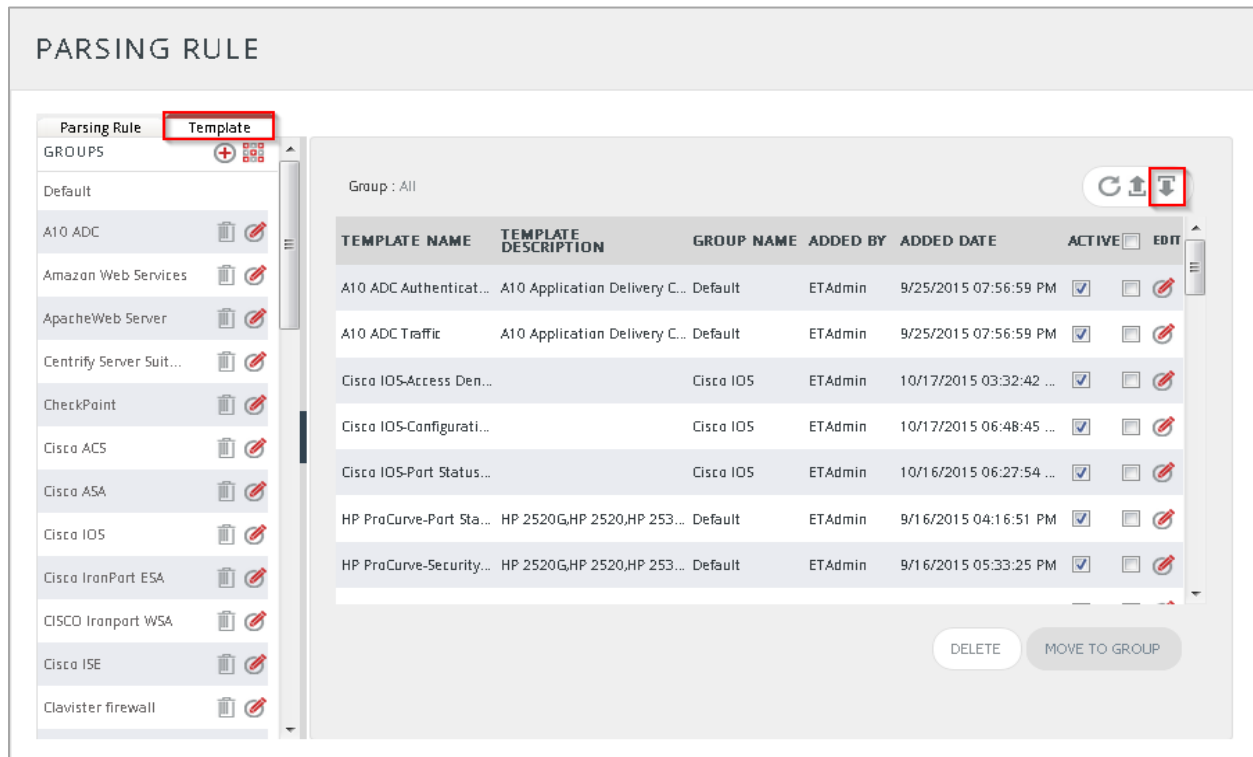


Figure 6

3. Click on **Browse** button.

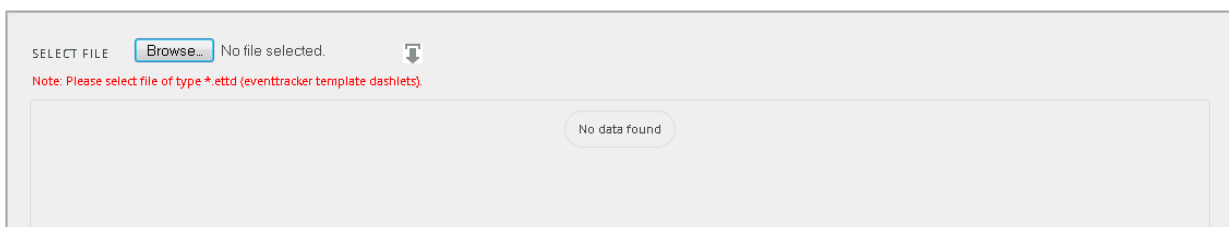



Figure 7

4. Locate **All Cisco Switch** group of **Template.ettd** file, and then click the **Open** button

SELECTED FILE IS: All Cisco Switch group of Template.issch

TEMPLATE NAME	SEPARATOR	TEMPLATE DESCRIPTION	ADDED DATE	ADDED BY	GROUP NAME
<input type="checkbox"/> Citrix AAA session login/logout	t	Jan 13 23:22:25 10.217.28.160 01/13/2015:23:22:25 GMT 0-PPE:0 -AAATM LOG OUT 3312 0 : Context_57007c73094b76545378f62e042a095@10.252.112.245 - SessionId: 58-User_57007c73094b76545378f62e042a095 - Client_ip 10.252.112.245 - Nat_ip "Mapped Ip" - Vserver 10.217.28.163:443 - Start_time "01/13/2015:23:22:17 GMT" - End_time "01/13/2015:23:22:25 GMT" - Duration 00:00:08 - Http_resources_accessed 0 - Total_TCP_connections 0 - Total_policies_allowed 0 - Total_policies_denied 0 - Total_bytes_send 0 - Total_bytes_recv 0 - Total_compressedbytes_send 0 - Total_compressedbytes_recv 0 - Compression_ratio_send 0.00% - Compression_ratio_recv 0.00% - LogoutMethod "FreeViaDHCP" - Group(s) "N/A"	11/9/2016 5:17:42 PM	ETAdmin	Citrix NetScaler
<input type="checkbox"/> Citrix ACL logging	t	Jun 8 16:03:12 10.12.33.16 06/08/2009:16:03:12 GMT ns - ACL_ACL_PKT_LOG 6 7868 : Source 10.12.33.12:5353 -> Destination 224.0.0.251:5353 - Protocol UDP - TimeStamp 871184790(ms) - Hitcount 0 - Hit Rule Deny 12 - Data 0 0 0 0 1 1 5/8/2016 5:02:59 PM 0 0 0 0 0 7 5f 64 6f 6d 61 69 6e 4 5f 75 64 70 5 6c 6f 63 61 6c 0 0 21 0 1 90 7a f aa 41 43 41 41 41 0 0 20 0 1 98 5a 4a 83 74 69 6f 6e 3a 20 43 6c 6f 73	11/9/2016 5:02:59 PM	ETAdmin	Citrix NetScaler
		May 29 01:26:31 10.217.31.98 05/29/2015:01:26:31 GMT ns 0-PPE:0 : default: A PPFW APPFW SAFECOMMERCE 2181 0 : 10.217.253.62 1098-PPE0 4er1Vkaht0			

Figure 9

- Now select the check box and then click on  'Import' option. EventTracker displays success message.

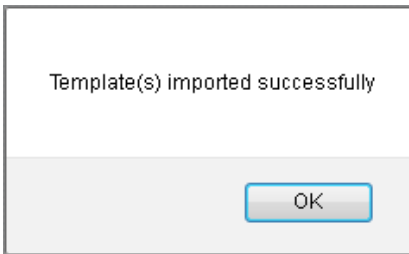



Figure 10

- Click on **OK** button.

## Flex Reports

- Click **Reports** option, and then click the 'browse'  button.
- Locate **All Cisco Switch group reports.issch** file, and then click the **Open** button.

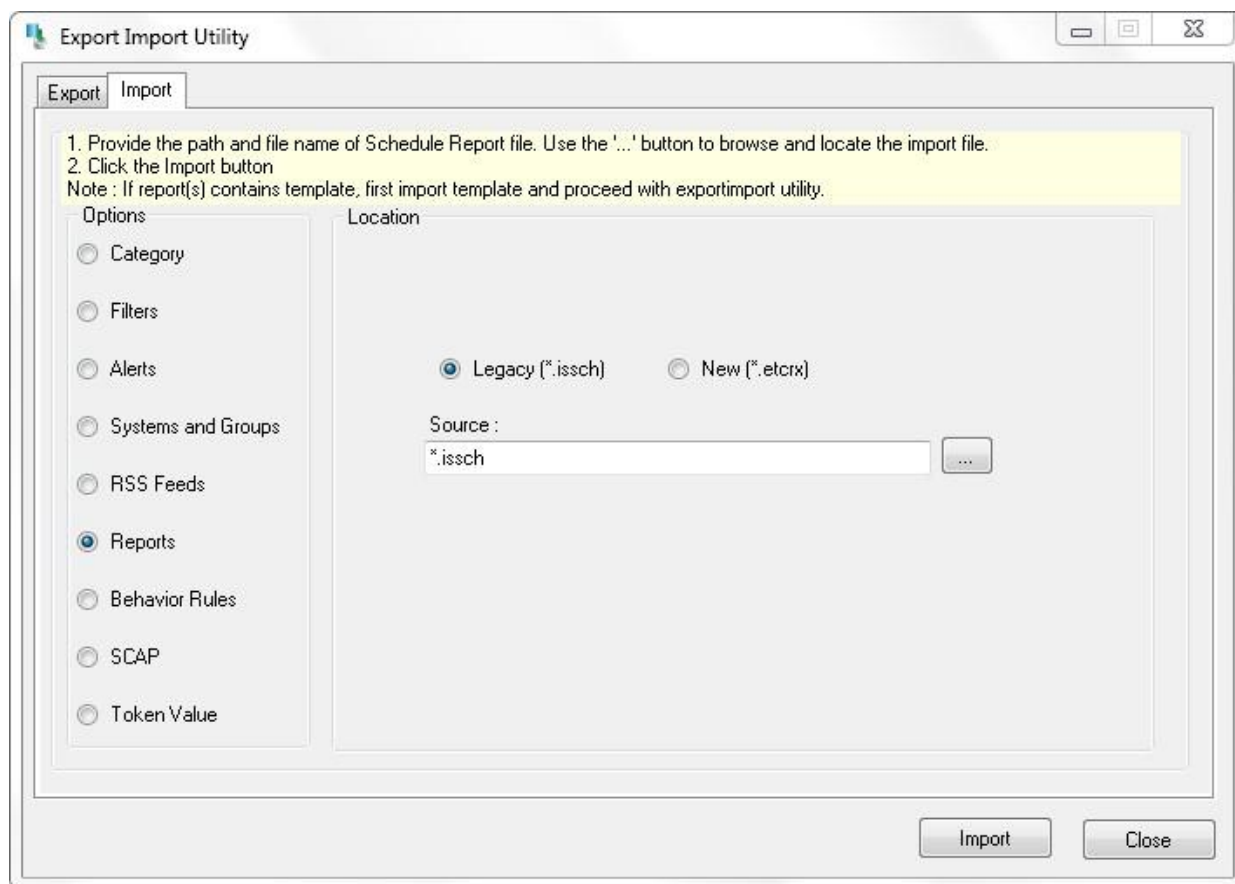


Figure 11

3. To import scheduled reports, click the **Import** button.

EventTracker displays success message.



Figure 12

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

# Verify Cisco Switch knowledge pack in EventTracker

## Categories

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Categories**.
3. In the **Category Tree**, expand **Cisco Switch** group folder to view imported categories.

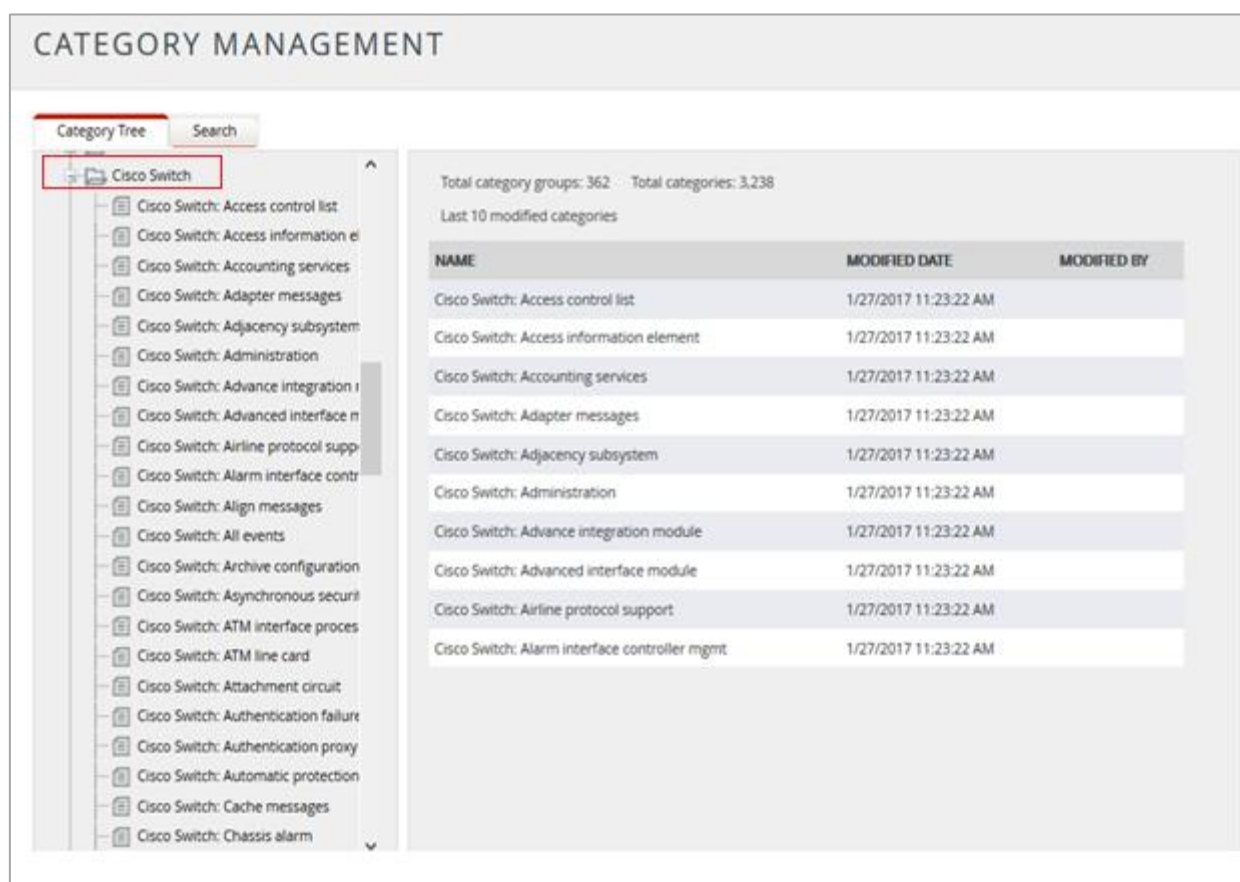


Figure 13

## Alerts

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Alerts**.
3. In **Search** field, type '**Cisco Switch**', and then click the **Go** button.  
Alert Management page will display all the imported Cisco Switch alerts.



**ALERT MANAGEMENT** Search by Alert name

ACTIVATE NOW Click 'Activate Now' after making all changes Total: 16 Page Size: 25

<input type="checkbox"/>	ALERT NAME ^	THREAT	ACTIVE	E-MAIL	MESSAGE	RSS	FORWARD AS SNMP	FORWARD AS SYSLOG	REMEDIAL ACTION AT CONSOLE	REMEDIAL ACTION AT AGENT	APPLIES TO
<input type="checkbox"/>	Cisco Switch: Border Gateway Protoc...	High	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Cisco Router 290...
<input type="checkbox"/>	Cisco Switch: Ethernet controller erro...	High	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Cisco IOS Release ...
<input type="checkbox"/>	Cisco Switch: Express Setup Failed	Medium	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Cisco IOS Release ...
<input type="checkbox"/>	Cisco Switch: GBIC security error	Medium	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Cisco IOS Release ...
<input type="checkbox"/>	Cisco Switch: Hardware error	Serious	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Cisco IOS Release ...
<input type="checkbox"/>	Cisco Switch: Hot Standby Router Pro...	High	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Cisco Router 290...
<input type="checkbox"/>	Cisco Switch: Interface down or detac...	High	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Cisco Router 290...
<input type="checkbox"/>	Cisco Switch: Internal software error	High	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Cisco Router 290...
<input type="checkbox"/>	Cisco Switch: IP-EIGRP neighbour is u...	High	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Cisco Router 290...
<input type="checkbox"/>	Cisco Switch: Line protocol down	High	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Cisco Router 290...
<input type="checkbox"/>	Cisco Switch: Port manager error	High	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Cisco IOS Release ...
<input type="checkbox"/>	Cisco Switch: Runaway processes	Medium	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Cisco Router 290...

Figure 14

- To activate the imported alerts, select the respective checkbox in the **Active** column. EventTracker displays message box.

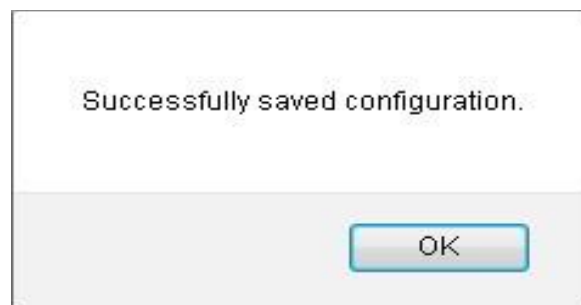


Figure 15

- Click **OK**, and then click the **Activate now** button.

**NOTE:** Please specify appropriate **systems** in **Alert configuration** for better performance.

## Template

1. Logon to EventTracker Enterprise web interface.
2. Click the **Admin** menu, and then click **Parsing Rules** and click **Template**.

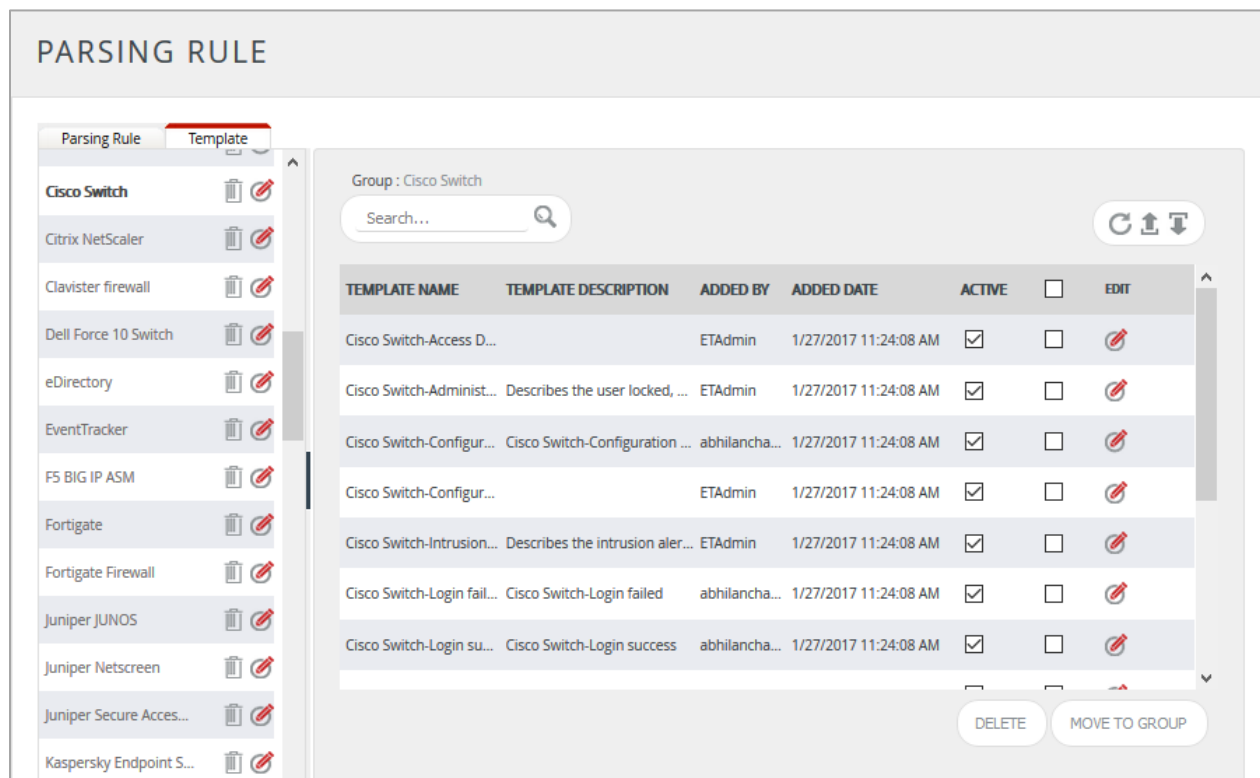


Figure 16

## Flex Reports

1. Logon to **EventTracker Enterprise**.
2. Click the **Reports** menu, and then **Configuration**.
3. Select **Defined** in report type.
4. In **Report Groups Tree** to view imported flex reports, scroll down and click **Cisco Switch** group folder. Imported reports are displayed in the Reports Configuration pane.

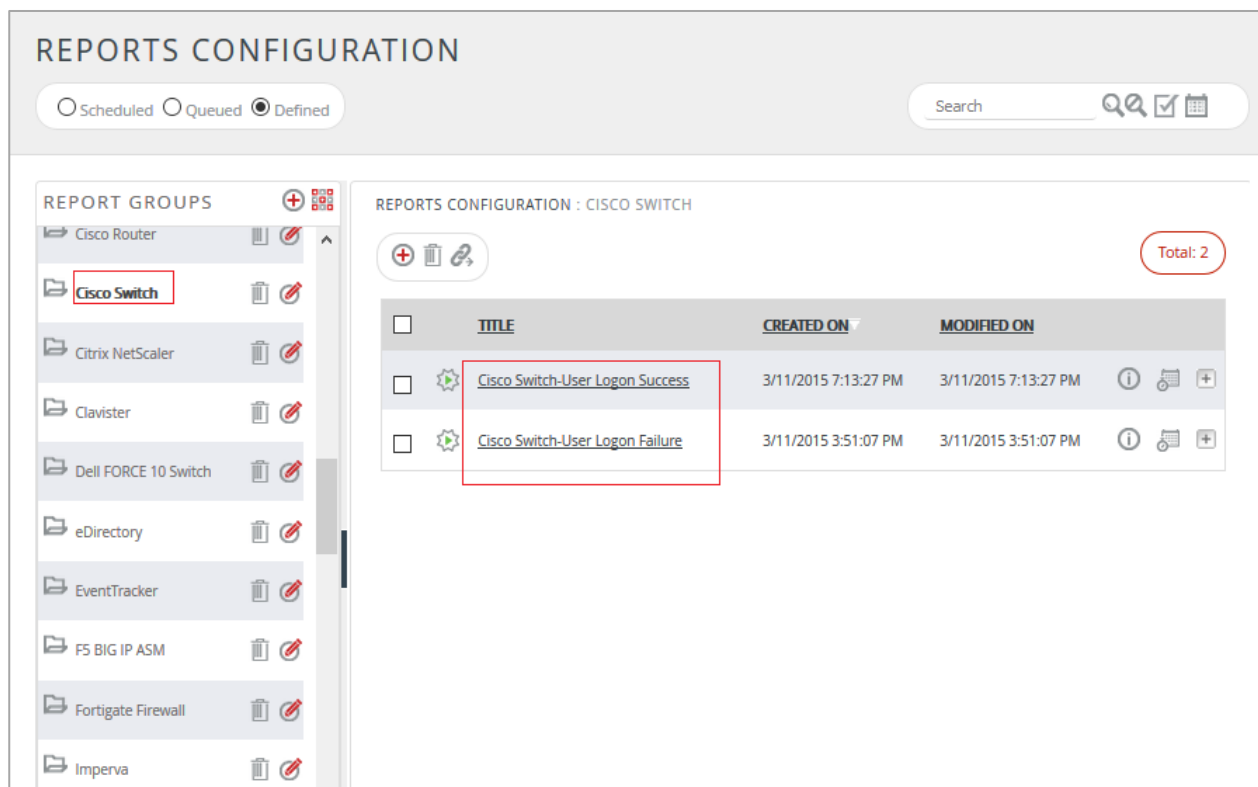


Figure 17

**NOTE:** Please specify appropriate **systems** in **report wizard** for better performance.

## Create Dashboards in EventTracker

### Schedule Reports

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

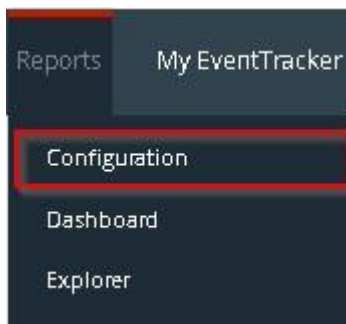


Figure 18

2. Navigate to **Reports>Configuration**.

REPORTS CONFIGURATION

Scheduled  Queued  Defined Search

REPORT GROUPS

- Cisco Router
- Cisco Switch**
- Citrix NetScaler
- Clavister
- Dell FORCE 10 Switch
- eDirectory
- EventTracker
- FS BIG IP ASM
- Fortigate Firewall
- Imperva

REPORTS CONFIGURATION : CISCO SWITCH

Total: 2

<input type="checkbox"/>	TITLE	CREATED ON	MODIFIED ON			
<input type="checkbox"/>	<u>Cisco Switch-User Logon Success</u>	3/11/2015 7:13:27 PM	3/11/2015 7:13:27 PM			
<input type="checkbox"/>	<u>Cisco Switch-User Logon Failure</u>	3/11/2015 3:51:07 PM	3/11/2015 3:51:07 PM			

Figure 19

3. Select **Cisco Switch** in report groups. Check **Defined** dialog box.
4. Click on 'schedule' to plan a report for later execution.

## REPORT WIZARD

TITLE: CISCO SWITCH-USER LOGON FAILURE

LOGS

CANCEL < BACK NEXT >

Review cost details and configure the publishing options. Step 8 of 10

### DISK COST ANALYSIS

Estimated time for completion: 00:00:42(HH:MM:SS)  
Number of cab(s) to be processed: 6  
Available disk space: 218 GB  
Required disk space: 50 MB

Enable publishing option (Configure SMTP Server in manager configuration screen to use this option)  
 Deliver results via E-mail  
 Notify results via E-mail

To E-mail  [Use comma(,) to separate multiple e-mail recipients]

Update status via RSS

Show in

Persist data in Eventvault Explorer

Figure 20

5. Choose appropriate time for report execution and in **Step 8** check **Persist data in EventVault explorer** box.

## REPORT WIZARD

TITLE: CISCO SWITCH-USER LOGON FAILURE  
DATA PERSIST DETAIL

CANCEL < BACK NEXT >

---

Select columns to persist

Step 9 of 10 ●●●●●●●●●●

### RETENTION SETTING

Retention period:  days ⓘ

Persist in database only *[Reports will not be published and will only be stored in the respective database]*

### SELECT COLUMNS TO PERSIST

COLUMN NAME	PERSIST
User Name	<input checked="" type="checkbox"/>
Source IP Address	<input checked="" type="checkbox"/>
Local Port	<input checked="" type="checkbox"/>
Reason	<input checked="" type="checkbox"/>

Figure 21

6. Check column names to persist using **PERSIST** checkboxes beside them. Choose suitable **Retention period**.
7. Proceed to next step and click **Schedule** button.
8. Wait for scheduled time or generate report manually.

## Create Dashlets

1. **EventTracker 8** is required to configure flex dashboard.
2. Open **EventTracker** in browser and logon.



Figure 22

3. Navigate to **Dashboard>Flex**.  
Flex Dashboard pane is shown.

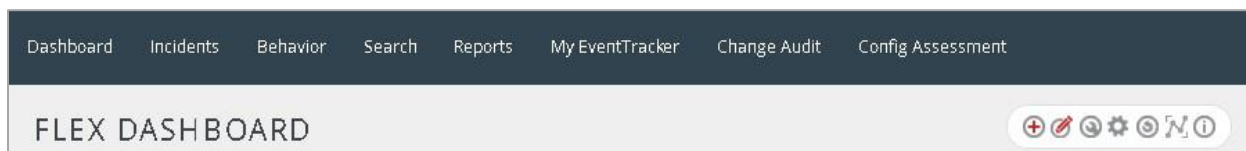




Figure 23

4. Click  to add a new dashboard.  
Flex Dashboard configuration pane is shown.

 The Flex Dashboard configuration pane is shown. It has a title bar 'FLEX DASHBOARD'. Below it is a form with two input fields: 'Title' and 'Description'. Both fields contain the text 'Cisco Switch'. At the bottom of the form are three buttons: 'SAVE', 'DELETE', and 'CANCEL'.

Figure 24

4. Fill fitting title and description and click **Save** button.
5. Click  to configure a new flex dashlet.

Widget configuration pane is shown.

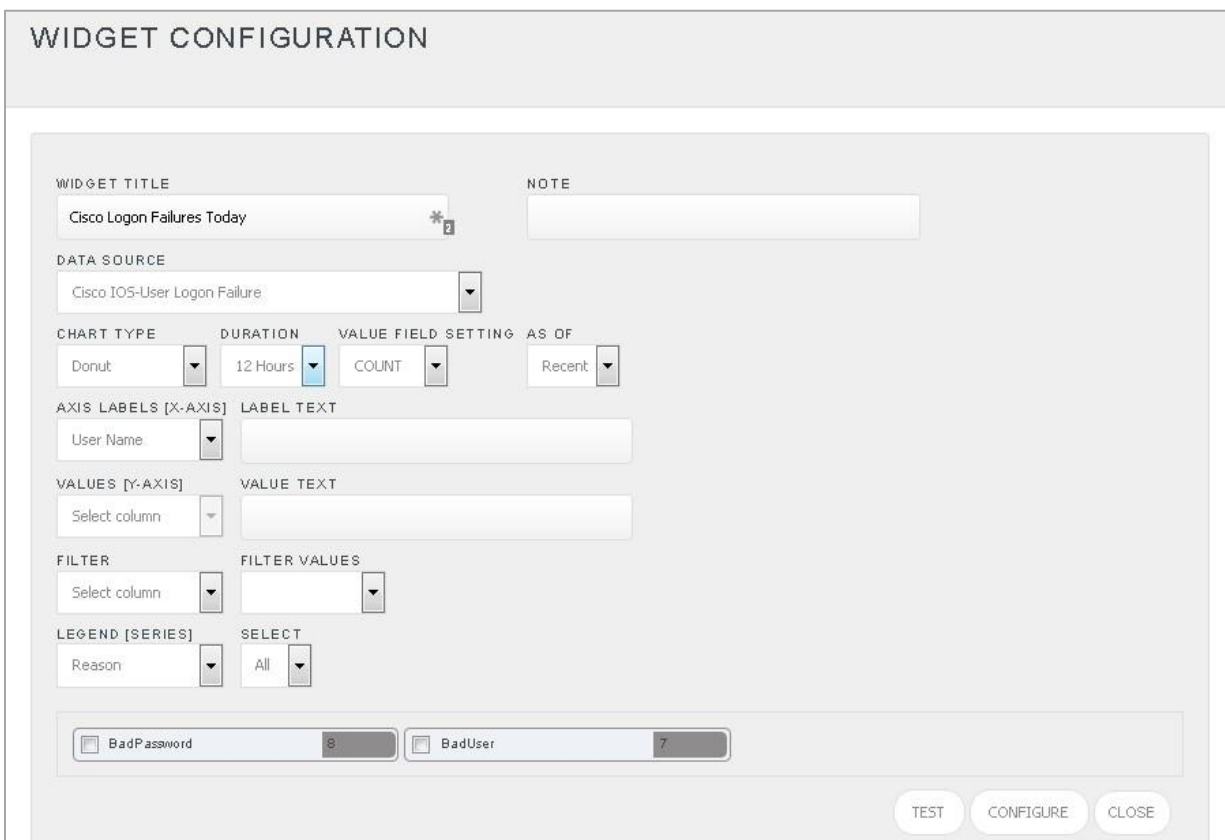


Figure 25

6. Locate earlier scheduled report in **Data Source** dropdown.
7. Select **Chart Type** from dropdown.
8. Select extent of data to be displayed in **Duration** dropdown.
9. Select computation type in **Value Field Setting** dropdown.
10. Select evaluation duration in **As Of** dropdown.
11. Select comparable values in **X Axis** with suitable label.
12. Select numeric values in **Y Axis** with suitable label.
13. Select comparable sequence in **Legend**.
14. Click **Test** button to evaluate.  
Evaluated chart is shown.



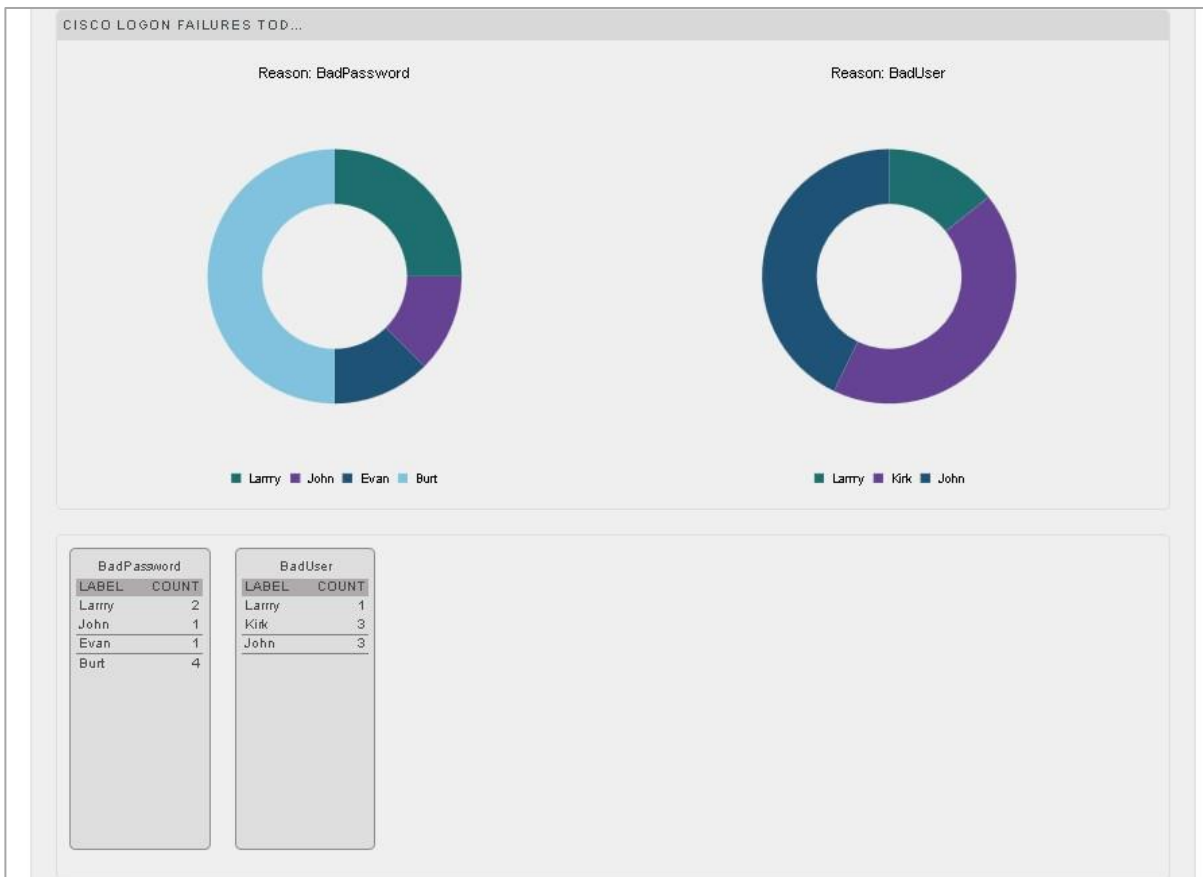


Figure 26

15. If satisfied, click **Configure** button.

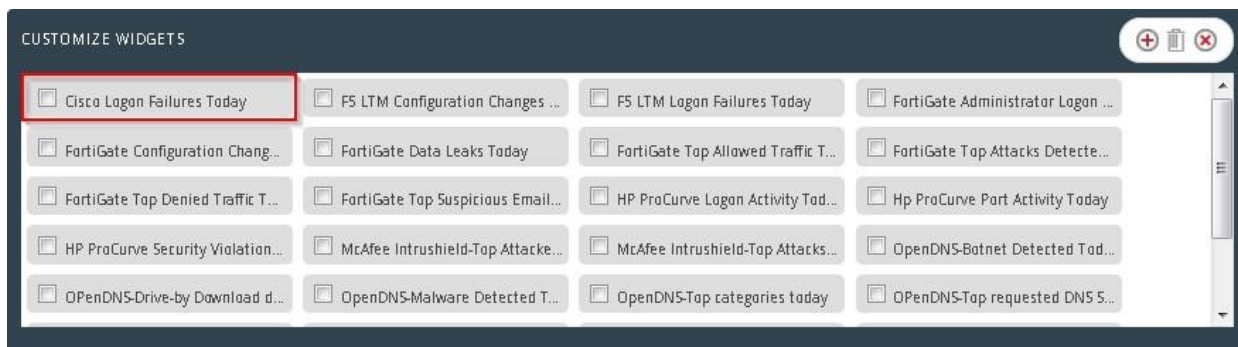



Figure 27

16. Click 'customize'  to locate and choose created dashlet.

17. Click  to add dashlet to earlier created dashboard.

# Sample Dashboards

## 1. Cisco Logon Failures Today



Figure 28