

Integrate Cisco IOS

Abstract

This guide provides instructions to configure Cisco IOS 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 IOS 12.4 and later**.

Audience

Administrators, who are responsible for monitoring Cisco's IOS 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
Overview.....	3
Prerequisites.....	3
Configure Cisco IOS to send syslog to EventTracker	3
EventTracker Knowledge Pack (KP)	4
Categories.....	4
Alerts	5
Reports	5
Import Cisco IOS Knowledge Pack into EventTracker	6
Import Categories.....	7
Import Alerts	8
Import Parsing Rules	9
Import Flex Reports.....	10
Verify Cisco IOS knowledge pack in EventTracker	11
Verify Categories	11
Verify Alerts	11
Verify Parsing Rules	13
Verify Flex Reports	13
Create Dashboards in EventTracker	14
Schedule Reports.....	14
Create Dashlets	18
Sample Dashboards	21
Sample Reports	22

Overview

Cisco IOS (Internetwork Operating System) is firmware for Cisco Routers and Switches (earlier switches ran CatOS). IOS is a package of Routing, Switching, Internetworking and Telecommunication functions integrated into a multitasking operating system.

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

Prerequisites

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

Configure Cisco IOS to send syslog to EventTracker

To enable and configure Cisco Routers 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

The possible values for severity level are as follows:

- Emergency: 0
- Alert: 1
- Critical: 2
- Error: 3
- Warning: 4
- Notice: 5
- Informational: 6
- Debug: 7

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 IOS monitoring.

Categories

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

- **Cisco IOS: Cache messages** - This category provides information related to cache messages.
- **Cisco IOS: Chassis alarm** - This category provides information related to chassis alarm.
- **Cisco IOS: Ethernet devices** - This category provides information related to Ethernet devices.
- **Cisco IOS: Hardware device error** - This category provides information related to hardware device error.
- **Cisco IOS: HTTP subsystem** - This category provides information related to HTTP subsystem.
- **Cisco IOS: Intrusion detection** - This category provides information related to intrusion detection.
- **Cisco IOS: Networks** - This category provides information related to networks

Alerts

- **Cisco IOS: Border Gateway Protocol (BGP) neighbors up or down** - This alert is generated when Border Gateway Protocol (BGP) neighbors up or down event occurs.
- **Cisco IOS: Hot Standby Router Protocol (HSRP) state** - This alert is generated when Hot Standby Router Protocol (HSRP) state change occurs.
- **Cisco IOS: Interface down or detached** - This alert is generated when interface down or detached event occurs.
- **Cisco IOS: Internal software error** - This alert is generated when internal software error occurs.
- **Cisco IOS: IP-EIGRP neighbor is up or down** - This alert is generated when IP-EIGRP neighbor is up or down.
- **Cisco IOS: Line protocol down** - This alert is generated when line protocol is down.
- **Cisco IOS: Runaway processes** - This alert is generated when runaway processes occur.

Reports

- **Cisco IOS-Configuration changed**
This report provides information related to configuration changes which include Device Address, User Name, and Command Issued fields.
- **Cisco IOS-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.
- **Cisco IOS-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.
- **Cisco IOS-User logon success**
This report provides information related to user logon success which includes User Name, Source Address and Source Port fields.
- **Cisco IOS-User logon failure**

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

Import Cisco IOS Knowledge Pack into EventTracker

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

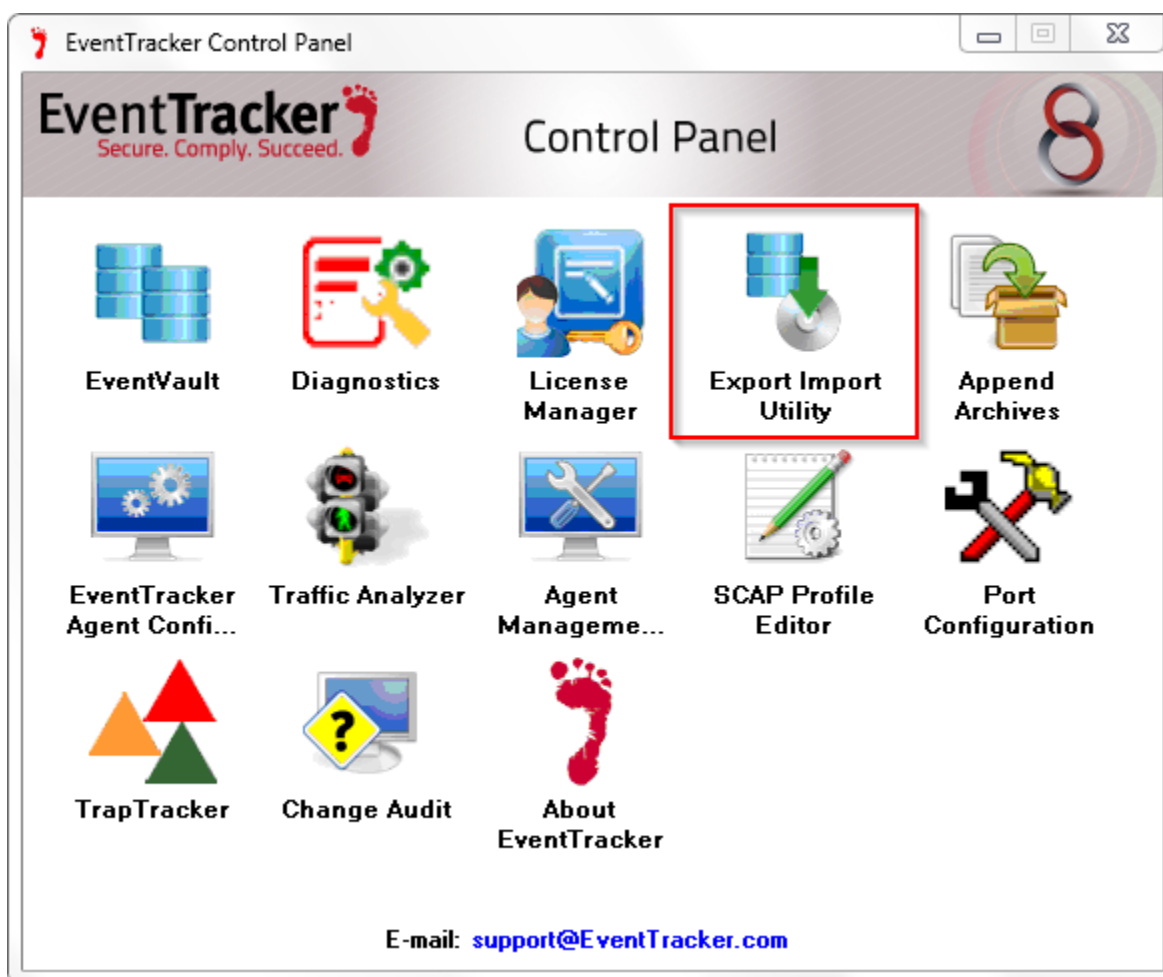


Figure 1

Import **Categories, Alerts, and Reports** as given below.

Import Categories

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

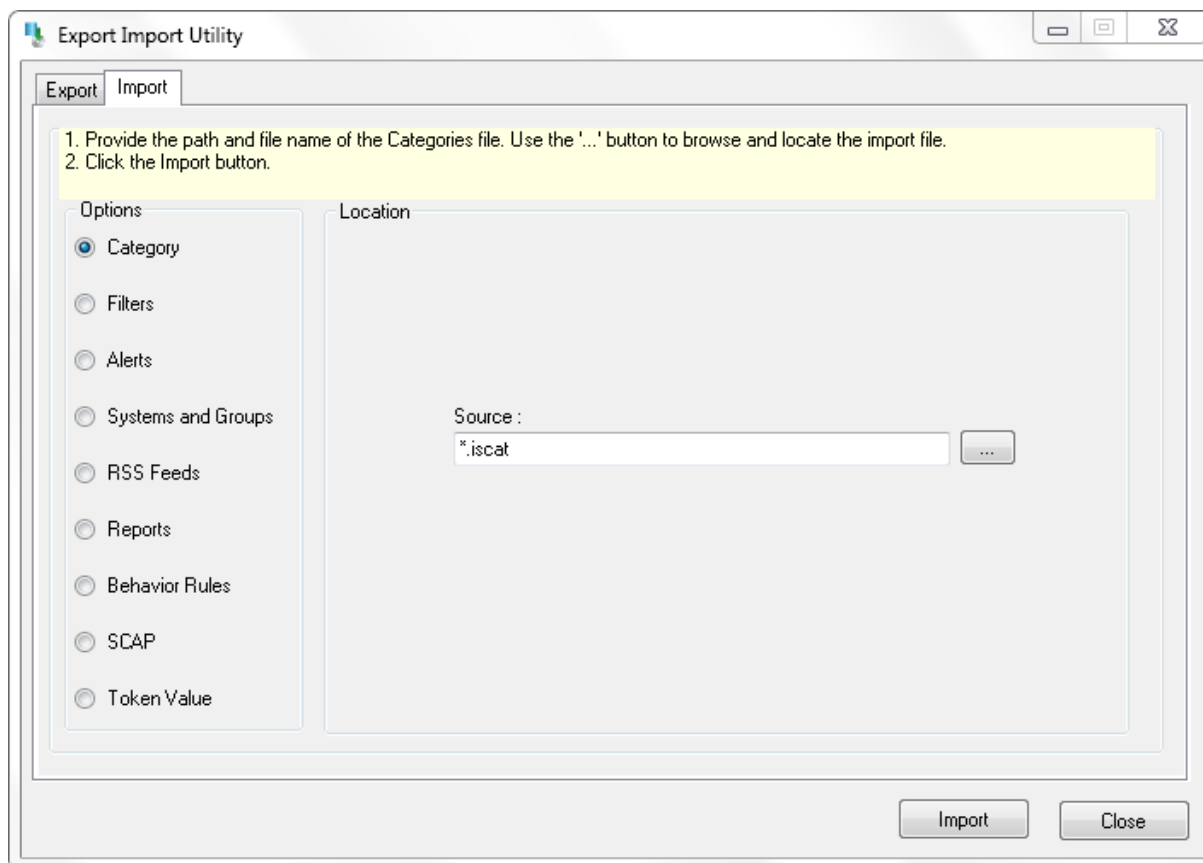


Figure 2

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

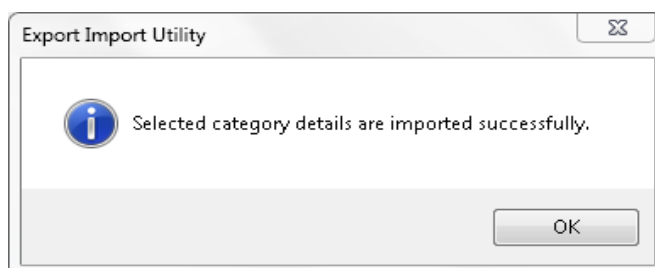


Figure 3

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

Import Alerts

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

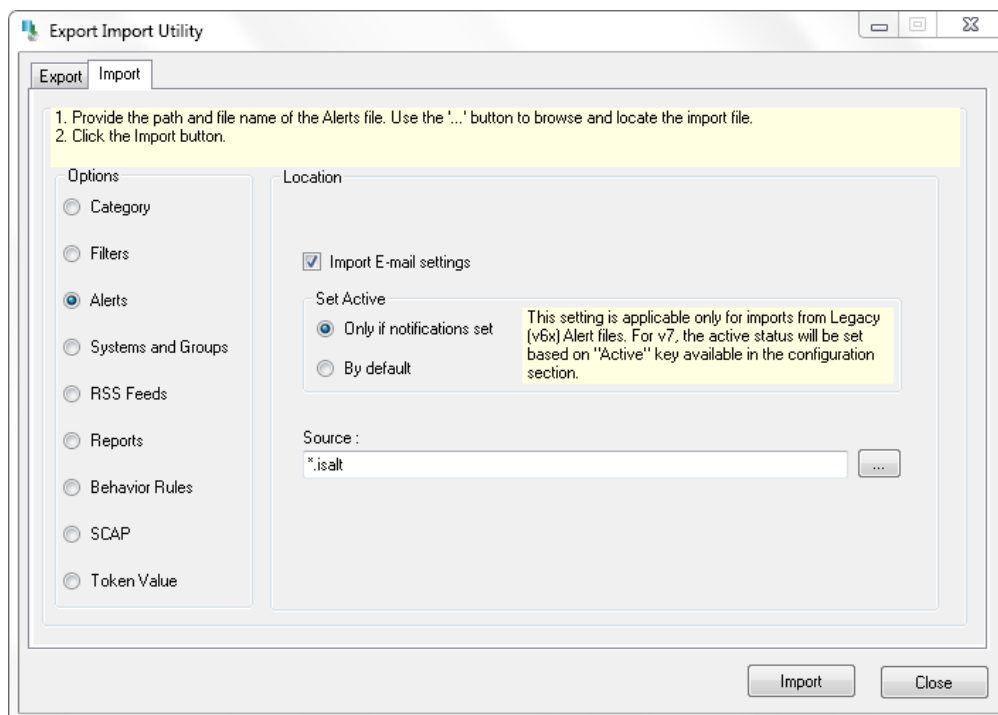


Figure 4

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

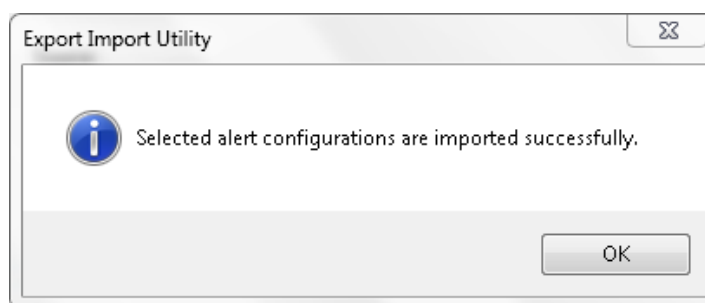



Figure 5

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.

Import Parsing Rules

1. Click **Token Value** option, and then click the browse  button.
2. Locate **All Cisco IOS group of Tokens.istoken** file, and then click the **Open** button.

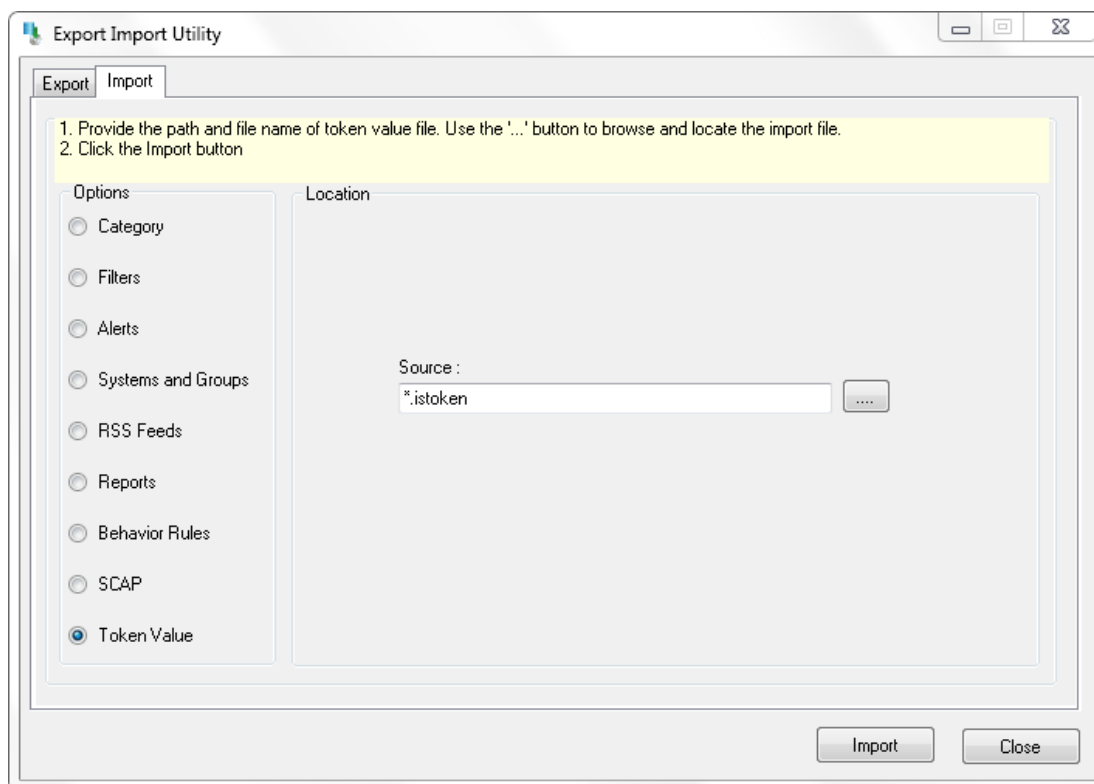


Figure 6

3. To import token value, click the **Import** button.
EventTracker displays success message.

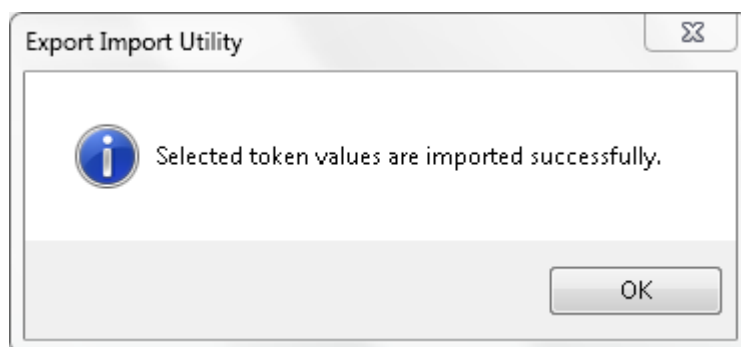



Figure 7

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

Import Flex Reports

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

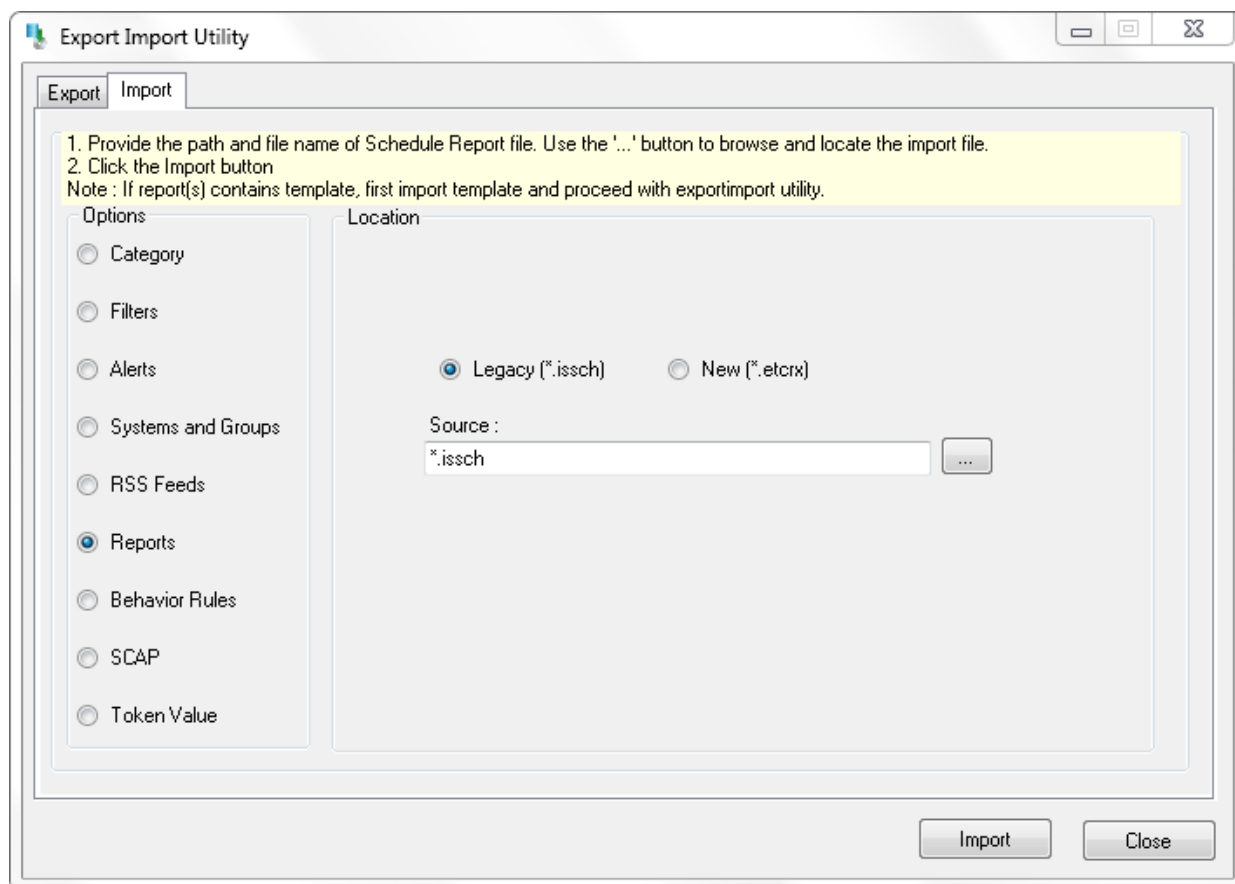


Figure 8

3. To import scheduled reports, click the **Import** button.
EventTracker displays success message.

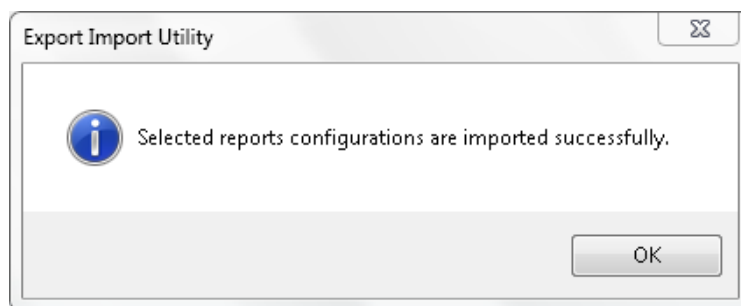


Figure 9

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

Verify Cisco IOS knowledge pack in EventTracker

Verify Categories

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

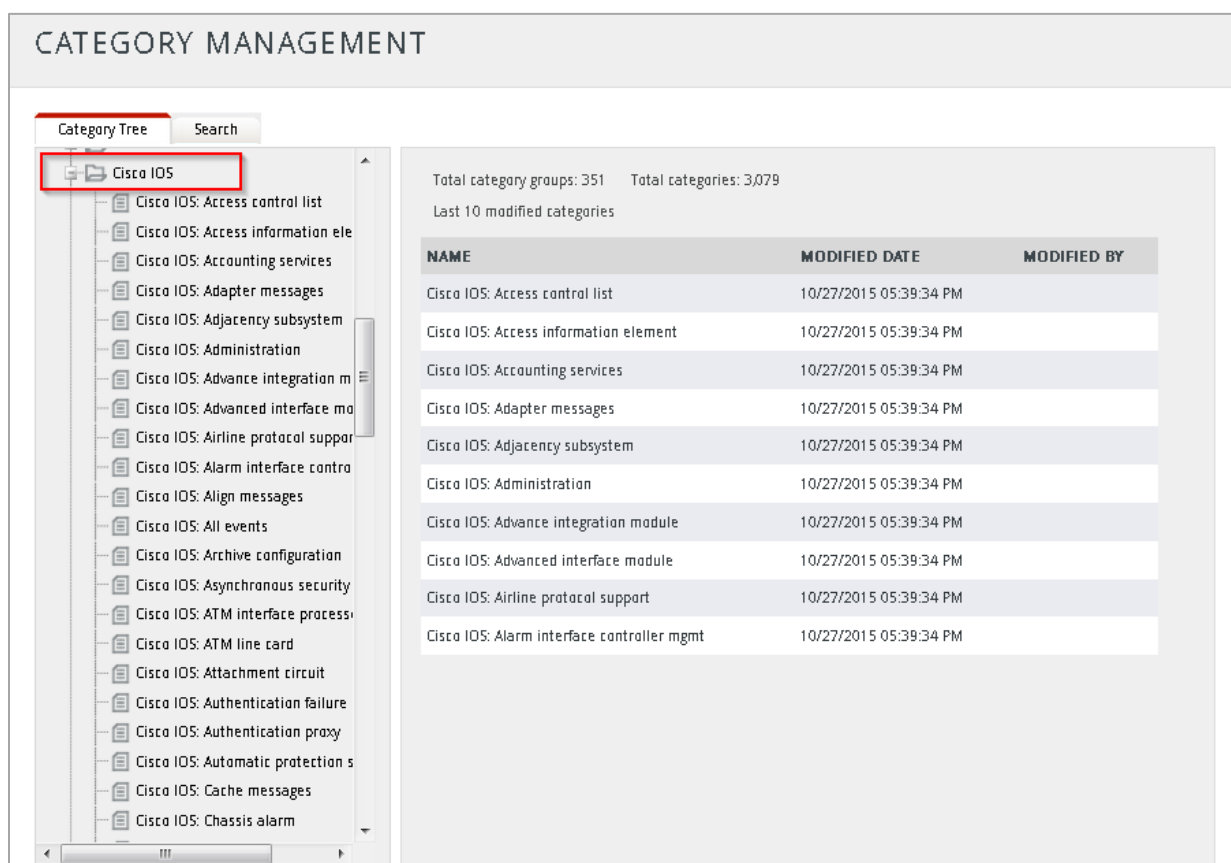


Figure 10

Verify Alerts

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

ALERT MANAGEMENT

Search by: Alert name Cisco IOS

Click 'Activate Now' after making all changes Total: 7 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 IOS: Border Gateway Protocol...	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 IOS: Hot Standby Router Prot...	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 IOS: Interface down or detach...	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 IOS: 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 IOS: IP-EIGRP neighbour is up ...	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 IOS: 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 IOS: 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 11

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

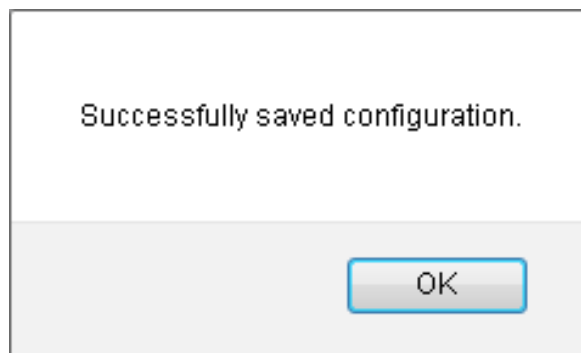


Figure 12

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

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

Verify Parsing Rules

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Parsing Rules**.
3. In **Token Value Group Tree** to view imported token values, scroll down and click **Cisco IOS** group folder. Token values are displayed in the token value pane.

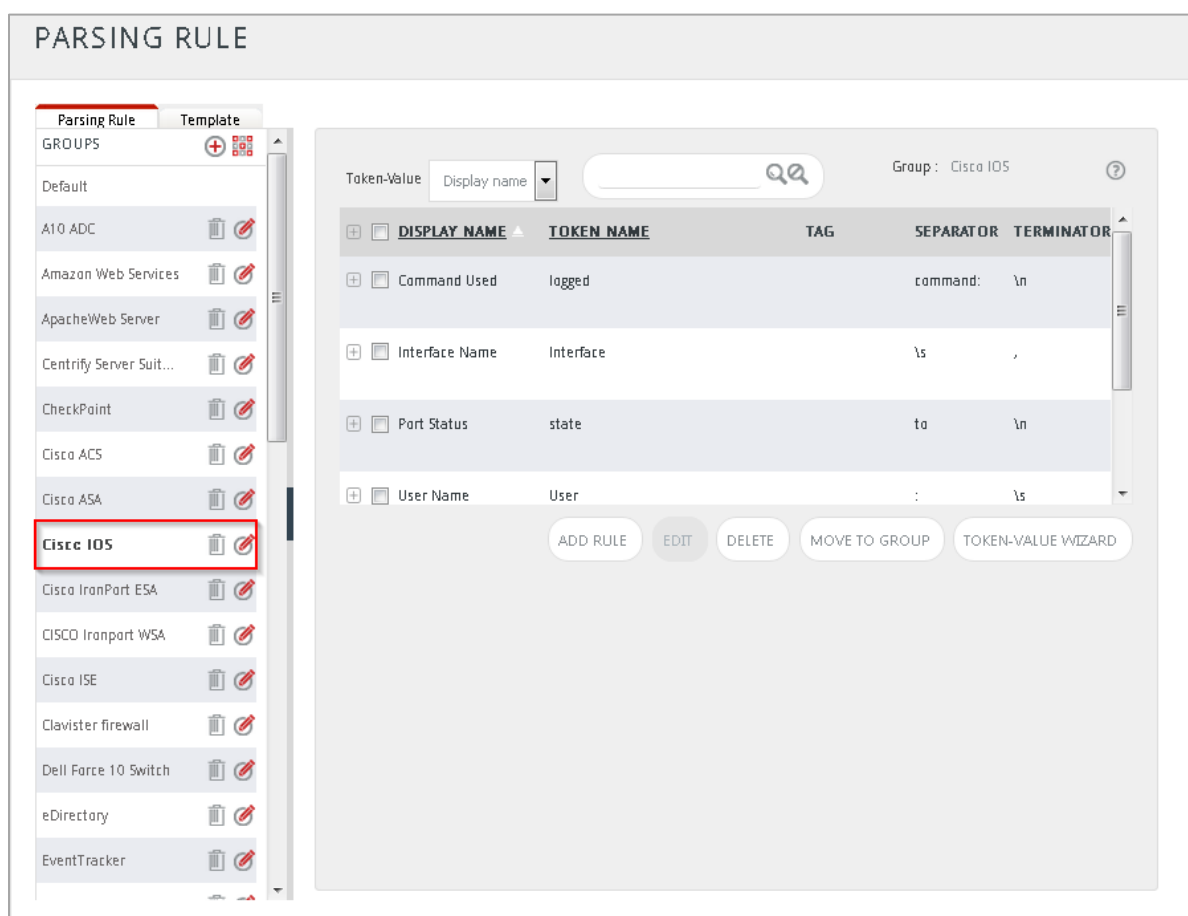


Figure 13

Verify 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 IOS** group folder. Imported reports are displayed in the Reports Configuration pane.

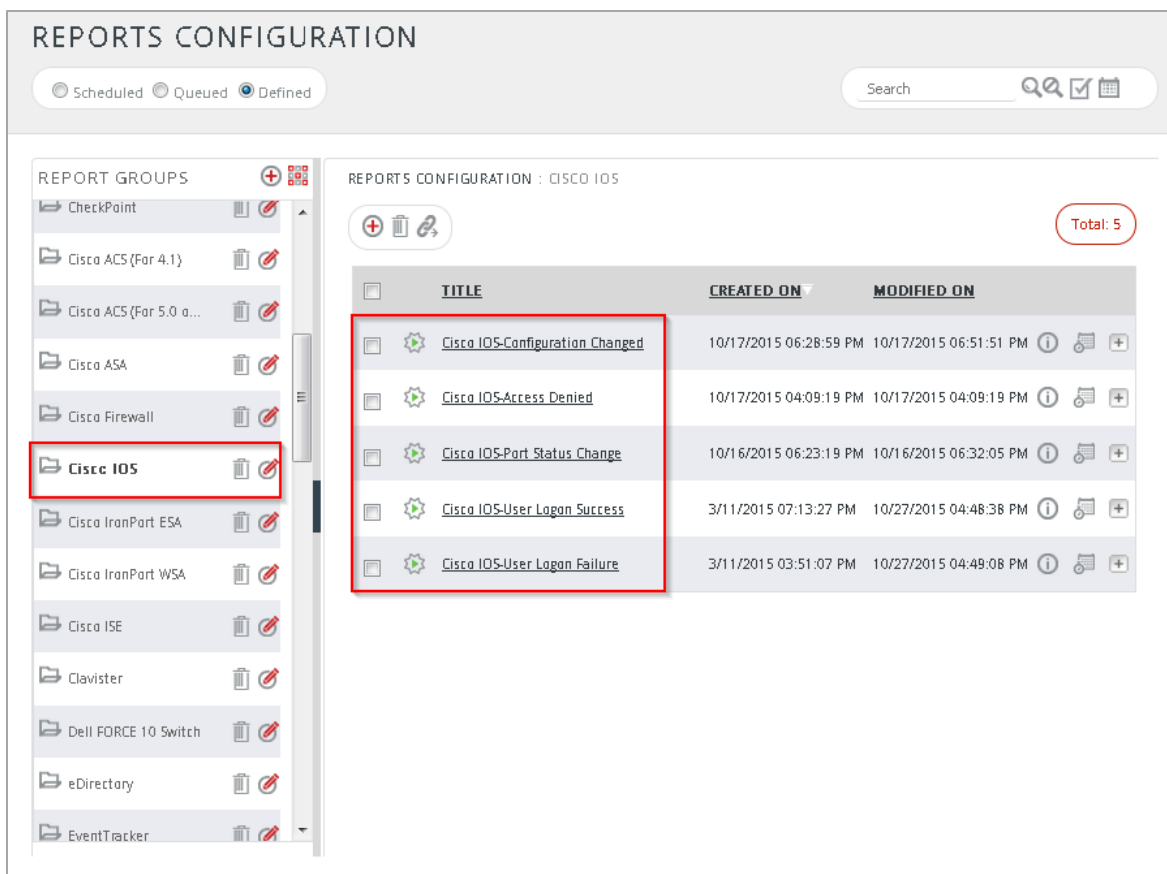


Figure 14

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

Create Dashboards in EventTracker

Schedule Reports

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

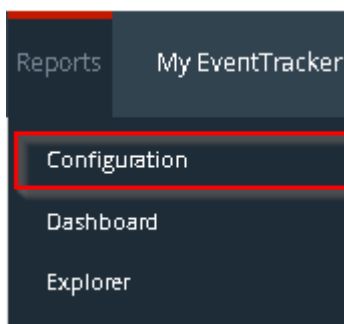


Figure 15

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

The screenshot shows the 'REPORTS CONFIGURATION' page in EventTracker. At the top, there are tabs for 'Scheduled', 'Queued', and 'Defined', with 'Defined' being the active tab. A search bar is located on the right. On the left, under 'REPORT GROUPS', a list of device types is shown, with 'Cisco IOS' highlighted by a red rectangle. The main area, titled 'REPORTS CONFIGURATION : CISCO IOS', displays a table of configured reports. A red circle in the top right corner of this section indicates 'Total: 5' reports.

	TITLE	CREATED ON	MODIFIED ON	
<input type="checkbox"/>	Cisco IOS-Configuration Changed	10/17/2015 06:28:59 PM	10/17/2015 06:51:51 PM	
<input type="checkbox"/>	Cisco IOS-Access Denied	10/17/2015 04:09:19 PM	10/17/2015 04:09:19 PM	
<input type="checkbox"/>	Cisco IOS-Port Status Change	10/16/2015 06:23:19 PM	10/16/2015 06:32:05 PM	
<input type="checkbox"/>	Cisco IOS-User Login Success	3/11/2015 07:13:27 PM	10/27/2015 04:48:38 PM	
<input type="checkbox"/>	Cisco IOS-User Login Failure	3/11/2015 03:51:07 PM	10/27/2015 04:49:08 PM	

Figure 16

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

REPORT WIZARD

TITLE: CISCO IOS-USER LOGIN FAILURE
LOGS

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

DISK COST ANALYSIS

Estimated time for completion: 00:00:38(HH:MM:SS)
Number of tab(s) to be processed: 4
Available disk space: 197 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 17

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

REPORT WIZARD

TITLE: CISCO IOS-USER LOGON FAILURE
DATA PERSIST DETAIL

CANCEL < BACK NEXT >

Select columns to persist Step 9 of 10

RETENTION SETTING

Retention period: 7 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 18

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 login.

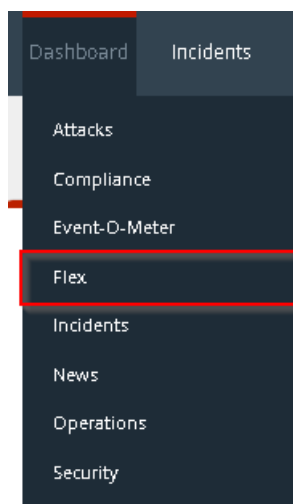


Figure 19

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

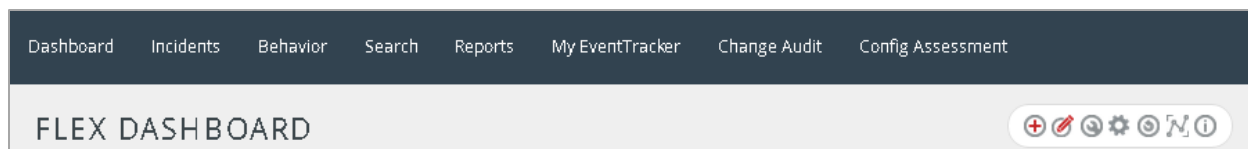




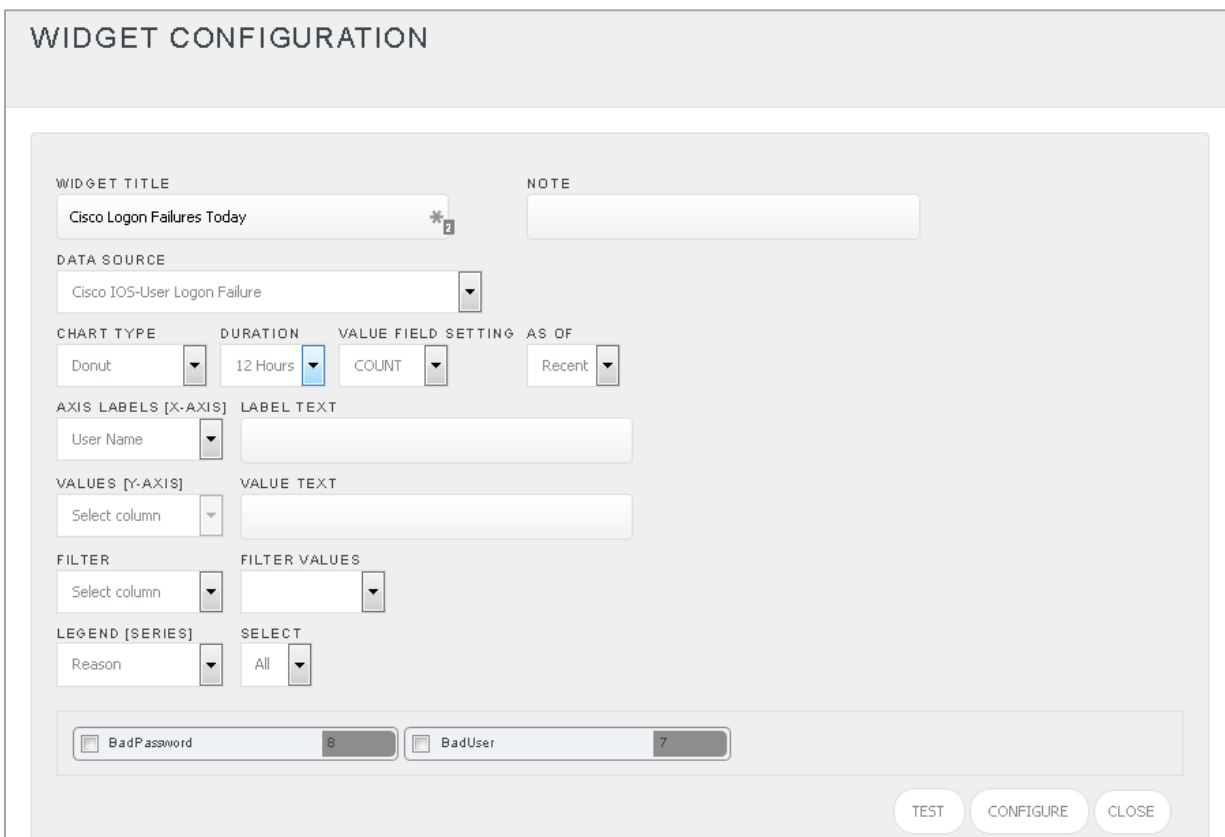
Figure 20

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


A screenshot of the Flex Dashboard configuration pane. It has a title 'FLEX DASHBOARD' at the top. Below it is a form with two input fields: 'Title' with the value 'Cisco IOS' and 'Description' with the value 'Cisco IOS 12.4 and later'. At the bottom of the form are three buttons: 'SAVE', 'DELETE', and 'CANCEL'.

Figure 21

5. Fill fitting title and description and click **Save** button.
6. Click  to configure a new flex dashlet.
Widget configuration pane is shown.



WIDGET CONFIGURATION

WIDGET TITLE
Cisco Logon Failures Today 

NOTE

DATA SOURCE
Cisco IOS-User Logon Failure

CHART TYPE Donut **DURATION** 12 Hours **VALUE FIELD SETTING** COUNT **AS OF** Recent

AXIS LABELS [X-AXIS] User Name **LABEL TEXT**

VALUES [Y-AXIS] Select column **VALUE TEXT**

FILTER Select column **FILTER VALUES**

LEGEND [SERIES] Reason **SELECT** All

☐ BadPassword 8 ☐ BadUser 7

TEST CONFIGURE CLOSE

Figure 22

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

Evaluated chart is shown.

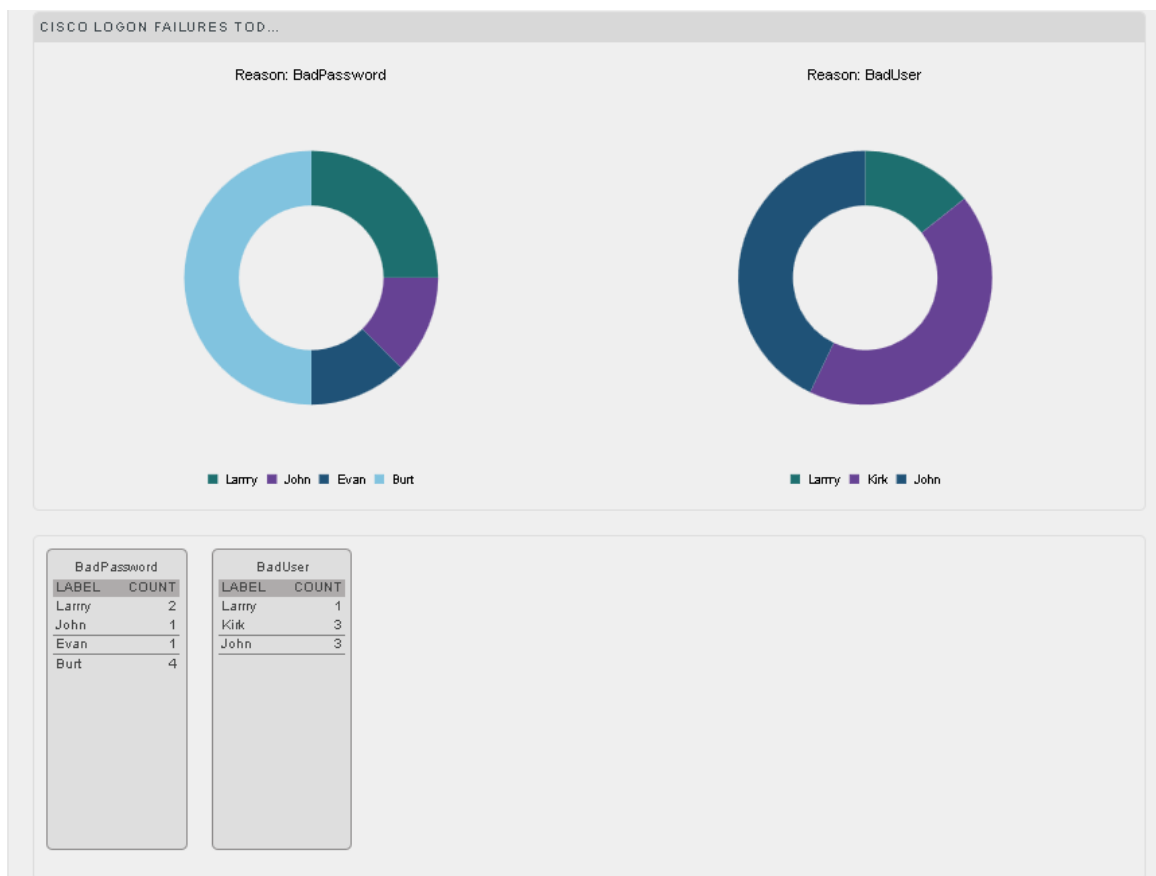


Figure 23

16. If satisfied, Click **Configure** button.

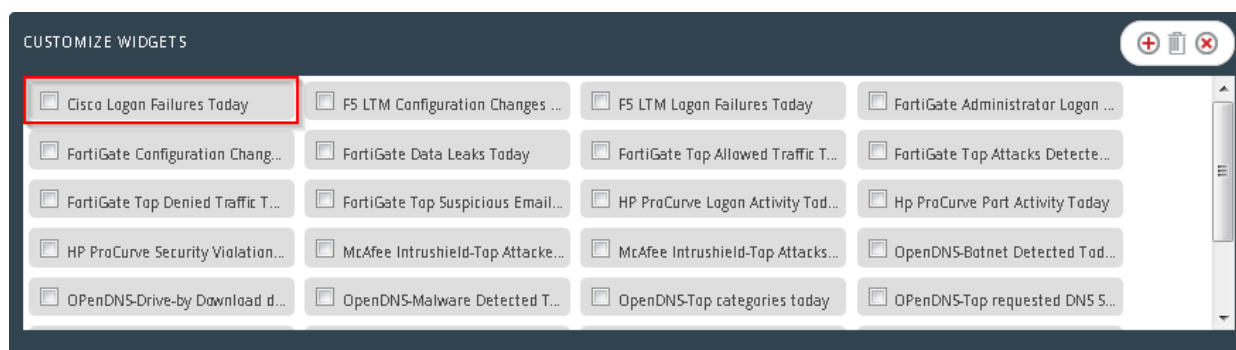




Figure 24

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

18. Click  to add dashlet to earlier created dashboard.

Sample Dashboards

1. Cisco Denied Traffic Today

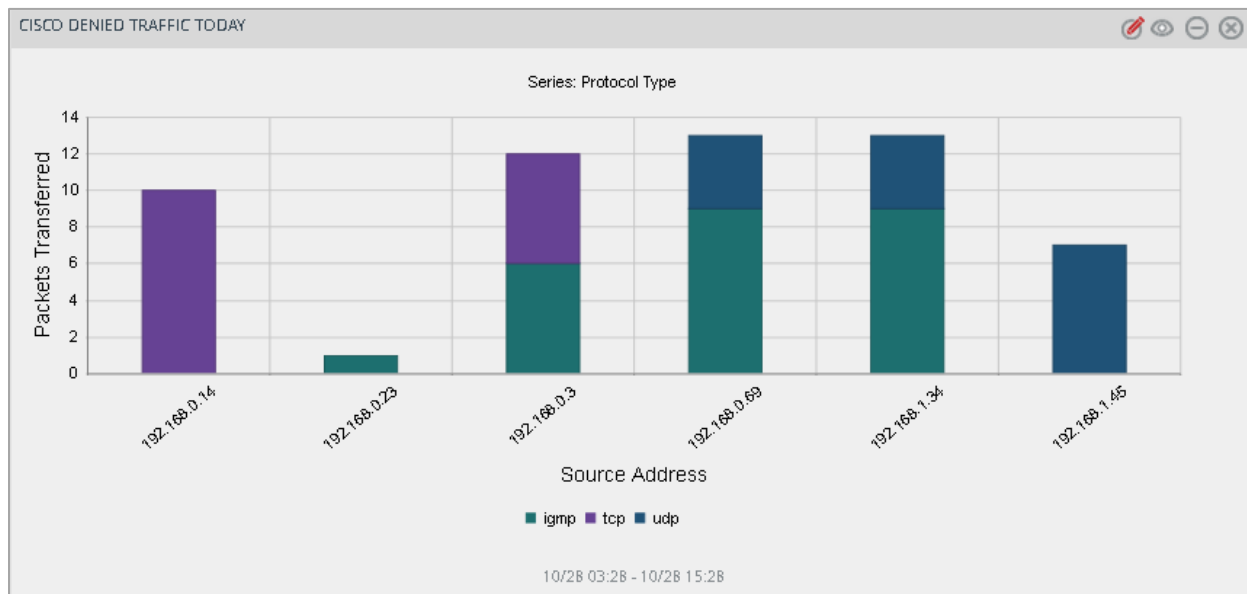


Figure 25

2. Cisco Logon Failures Today

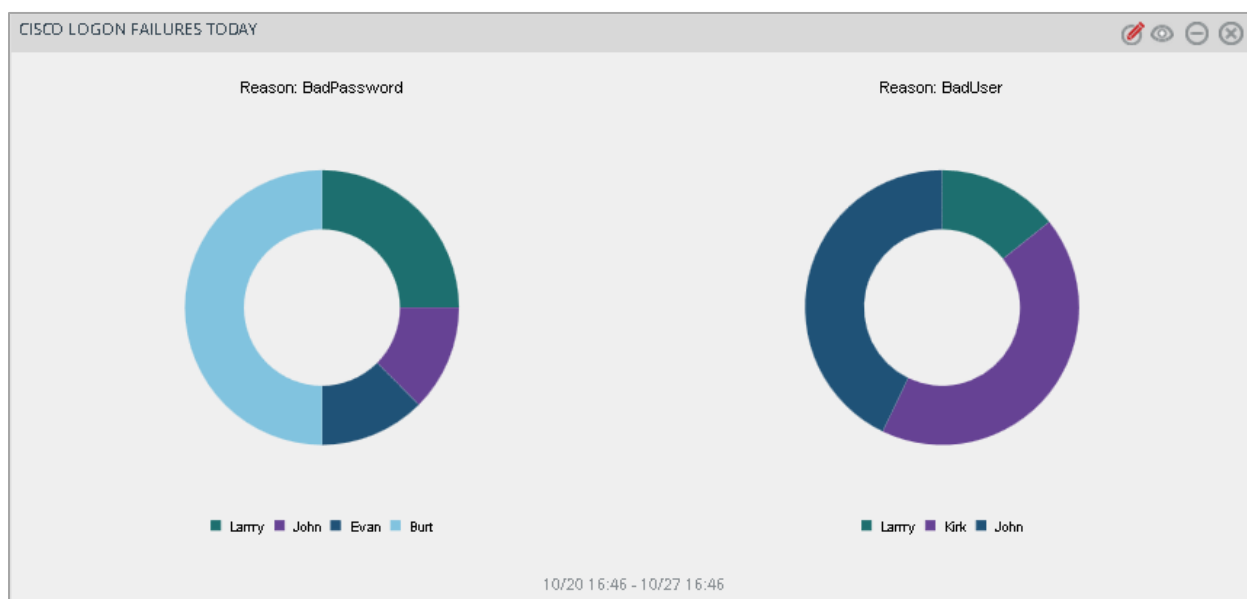


Figure 26

Sample Reports

1. Cisco IOS – Access denied

Event Time	Source Address	Source Port	Destination Address	Destination Port	Protocol Type	Packets Transferred
5/19/2015 16:39	130.237.188.216	6667	66.201.46.53	49789	tcp	
5/19/2015 19:14	192.168.0.36		192.168.0.1		ICMP	
5/19/2015 21:49	192.168.0.25	42829	192.168.0.36	80	tcp	
5/20/2015 00:23	10.1.0.1	2000	10.1.0.189	21348	udp	
5/20/2015 02:58	192.168.0.69	34559	192.168.0.10	80		
5/20/2015 05:33	192.168.0.69	34559	192.168.0.10	80		
5/20/2015 08:08	192.168.0.23		192.168.0.98	128	icmp	1
5/20/2015 10:43	192.168.0.78		192.168.0.154	80		1
5/20/2015 13:18	192.168.0.35	45629	192.168.0.35	22	tcp	1
5/20/2015 15:52	192.168.0.23		192.168.0.98	1	igmp	1
5/20/2015 18:27	192.168.0.27		192.168.0.215			
5/20/2015 21:02	192.168.0.2		192.168.0.216			
5/20/2015 23:37	192.168.0.3		192.168.0.217			
5/21/2015 02:12	192.168.0.10		192.168.0.1			
5/21/2015 04:47	192.168.0.10		192.168.0.1			
5/21/2015 07:21	192.168.0.10		192.168.0.1			
5/21/2015 09:56	192.168.30.20		192.1.1.1	0	icmp	1
5/21/2015 12:31	192.168.0.14		192.168.0.15	50		15

Figure 27

2. Cisco IOS – User login failure

LogTime	User Name	Source IP Address	Local Port	Reason
10/27/2015 04:49:11 PM	Kirk	10.0.10.169	22	BadUser
10/27/2015 09:44:17 PM	Kirk	10.0.10.169	22	BadUser
10/28/2015 02:39:23 AM	Scott	10.0.10.17	22	
10/28/2015 07:34:29 AM	Burt	10.0.10.172	80	BadPassword
10/28/2015 12:29:35 PM	Adam	10.0.10.170	23	BadUser
10/28/2015 05:24:41 PM	John	10.0.10.173	22	
10/28/2015 10:19:47 PM	Burt	10.0.10.172	80	BadPassword
10/29/2015 03:14:53 AM	Evan	10.0.10.17	25	BadPassword
10/29/2015 08:09:59 AM	Adam	10.0.10.170	23	BadUser
10/29/2015 01:05:05 PM	Kirk	10.0.10.169	22	BadUser
10/29/2015 06:00:11 PM	Scott	10.0.10.173	22	
10/29/2015 10:55:17 PM	Evan	10.0.10.17	25	BadPassword
10/30/2015 03:50:23 AM	John	10.0.10.173	22	
10/30/2015 08:45:29 AM	John	10.0.10.171	25	BadPassword
10/30/2015 01:40:35 PM	Burt	10.0.10.172	80	BadPassword
10/30/2015 06:35:41 PM	Adam	10.0.10.17	23	BadUser
10/30/2015 11:30:47 PM	Kirk	10.0.10.169	22	BadUser
10/31/2015 04:25:53 AM	Kirk	10.0.10.169	22	BadUser

Figure 28