EventTracker

Actionable Security Intelligence

Integrate Cisco ACS

Publication Date: January 5, 2016

Abstract

This guide helps in configuring Cisco ACS and EventTracker to receive Cisco ACS events. You will find the detailed procedure required for monitoring Cisco ACS Appliance.

Scope

The configurations detailed in this guide are consistent with EventTracker version **7.x and later**, and **Cisco ACS 4.0** and later.

Audience

Administrators who wish to forward Cisco ACS logs to EventTracker Manager which monitors events by using EventTracker.

Table of Contents

Overview

Cisco Secure Access Control Server (ACS) is an access policy control platform that helps you comply with growing regulatory and corporate requirements. By integrating with your other access control systems, it helps improve productivity and reduce costs.

This guide provides instructions to configure Cisco Secure ACS to send the syslog to EventTracker.

Prerequisites

- EventTracker should be installed.
- Cisco ACS Appliance should be installed.
- Port 514 must be opened on Cisco ACS.
- Port 514 must not be used by other services of Cisco ACS.
- An exception should be added into Windows Firewall on EventTracker machine for Syslog port 514.

Configure Cisco ACS to forward all logs to EventTracker

Configure Syslog logging

1. Open the **WebUI**.
2. Expand **Configuration** and select **Report Settings**, and then click **Syslog.**
3. Check '**Enable Syslog Messages'** to enable **Syslog**.

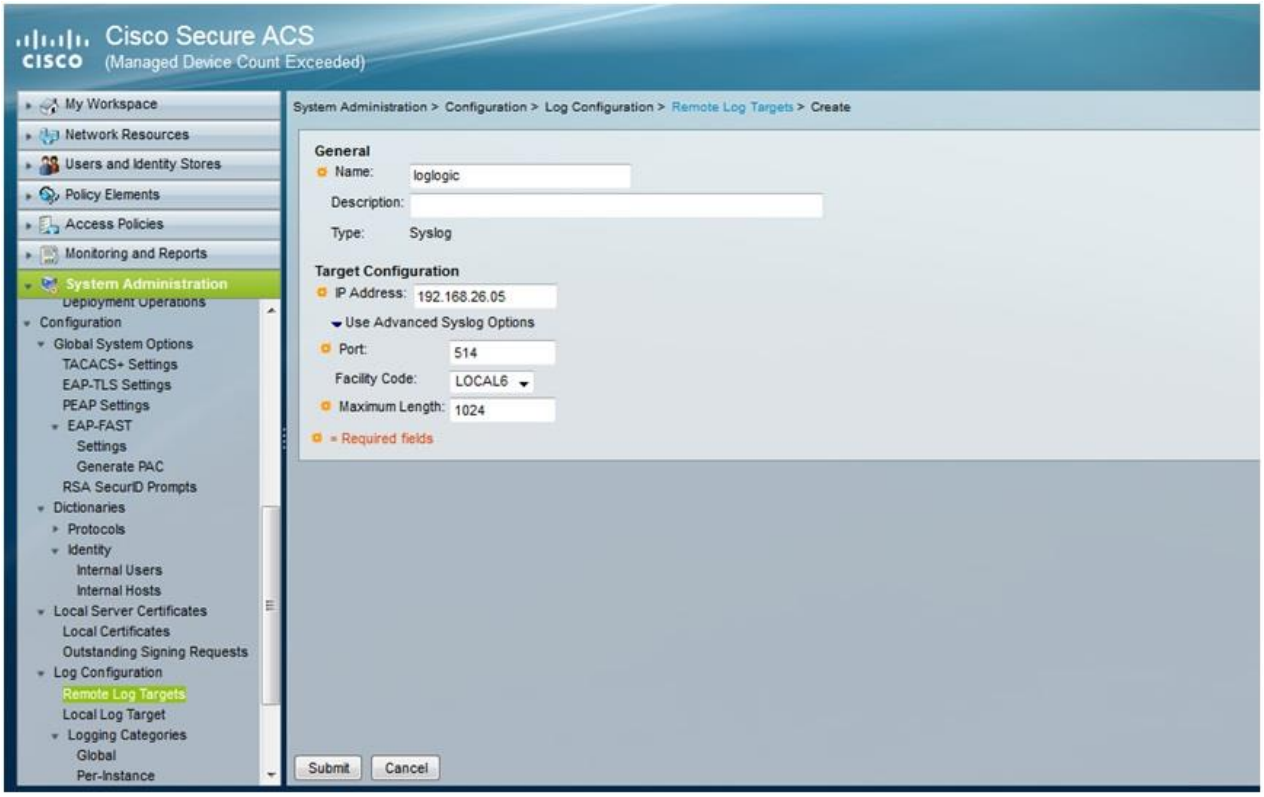

Figure 1

4. In the **Syslog Host Name/Port** field, type the IP address of the EventTracker Manager.
5. Click **Apply**.

EventTracker Knowledge Pack

Once Cisco ACS events are enabled and received in EventTracker then Alerts and Reports can be configured in EventTracker.

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

Categories

- **Cisco ACS-Administrator Logon Activity-** This category based report provides information related to administrator logon activity.
- **Cisco ACS-User Authentication Failure-** This category based report provides information related to user authentication failure.
- **Cisco ACS-User Authentication Success-** This category based report provides information related to user authentication success.
- **Cisco ACS-Administrator Audit Details-** This category based report provides information related to administrator audit details.

- **Cisco ACS-Password Changd-** This category based report provides information related to password changed.
- **Cisco ACS-Configuration Changed** - This category based report provides information related to configuration changed.

Alerts

- **Cisco ACS-Administrator Logon Failed-** This alert is generated when admin fails to login to the system.
- **Cisco ACS-Configuration Changed-** This alert is generated when there is any change in the system configuration.
- **Cisco ACS-Password Changed-** This alert is generated when there is any change in the password.
- **Cisco ACS-User Authentication Failed-** This alert is generated when the user's authentication fails.

Reports

- **Cisco ACS-Administrator Logon Activity:** This report provides information related to administrator logon activity.
- **Cisco ACS-User Authentication Failure:** This report provides information related to user authentication failure.
- **Cisco ACS-User Authentication Success:** This reports provides information related to user authentication success.
- **Cisco ACS-Administrator Audit Details:** This reports provides information related to administrator audit details.
- **Cisco ACS-Password Changed:** This reports provides information related to user password changes in the system.

Import Cisco ACS knowledge pack into EventTracker

1. Launch **EventTracker Control Panel**.
2. Double click **Export Import Utility**, and then click **Import** tab.
   Import **Category/Alert/Flex reports/parsing rule/Knowledge Object** as given below.

Import Category

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

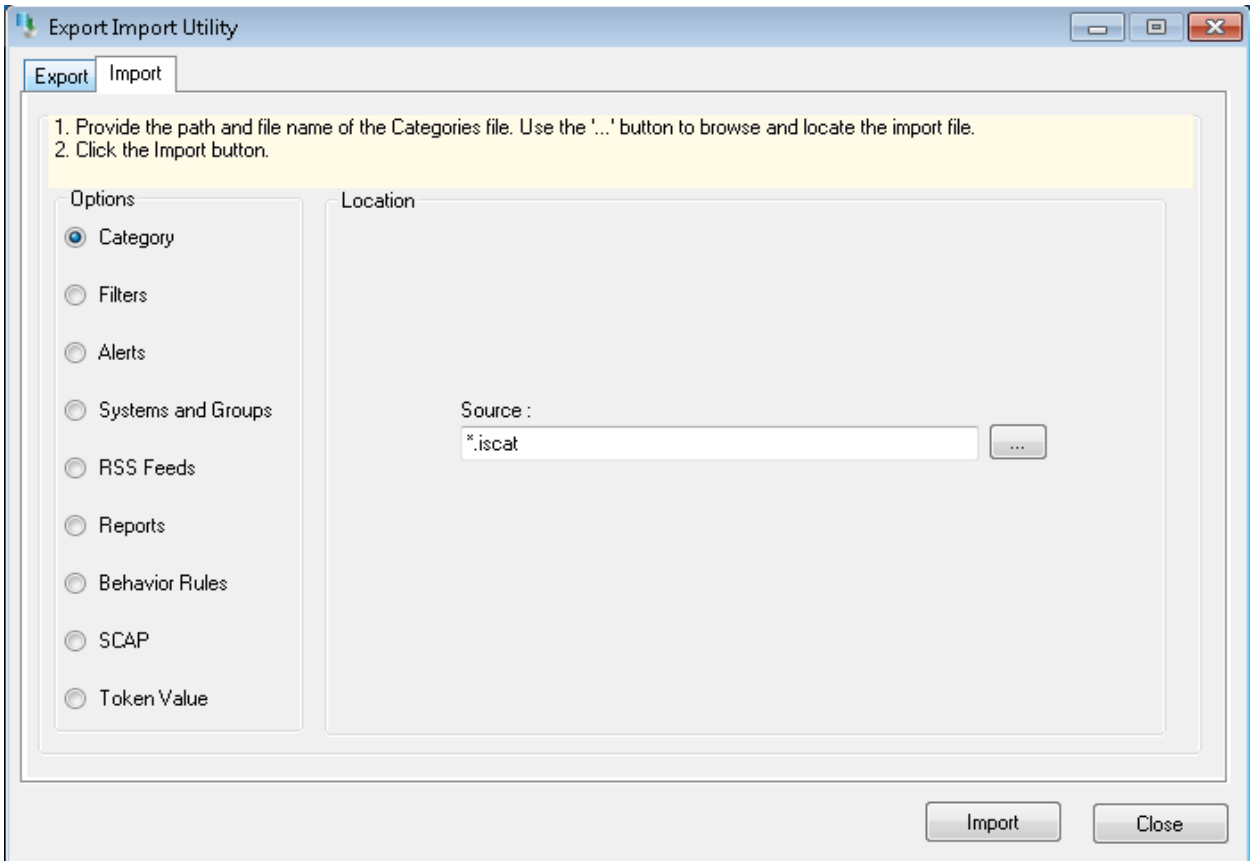

Figure 2

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

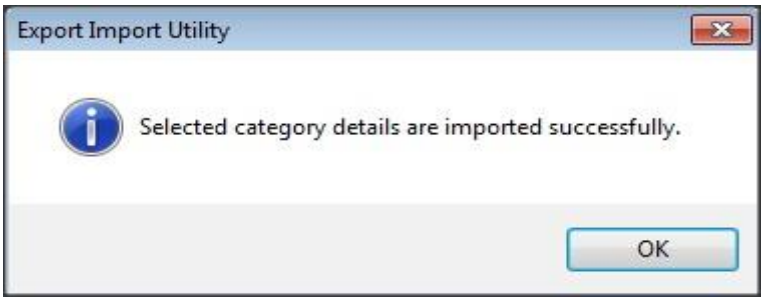

Figure 3

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

Import Alerts

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

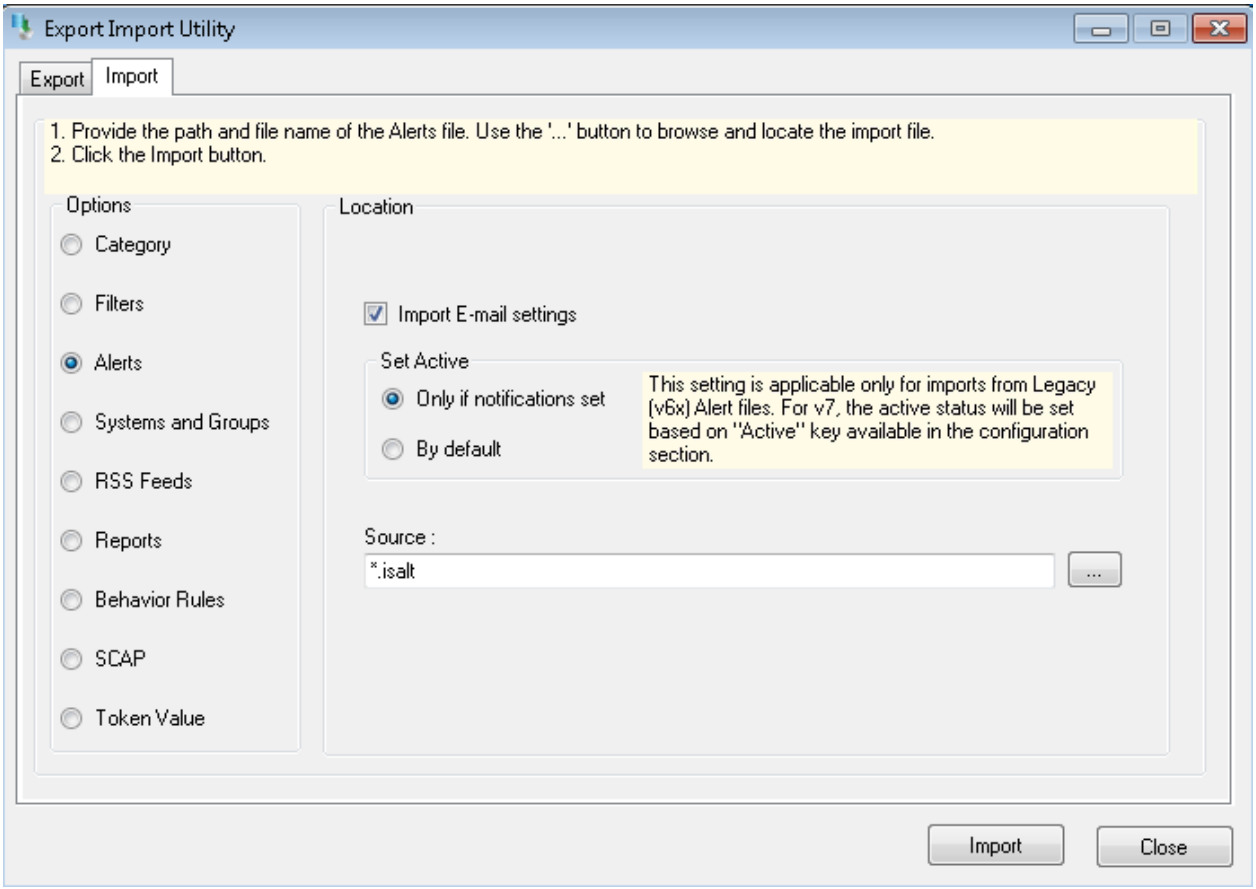

Figure 4

2. Locate **All Cisco ACS group of Alerts.isalt** file, and then click the **Open** button.
3. To import categories, click the **Import** button.

   EventTracker displays success message.

Figure 5

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

Import Flex Alerts

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

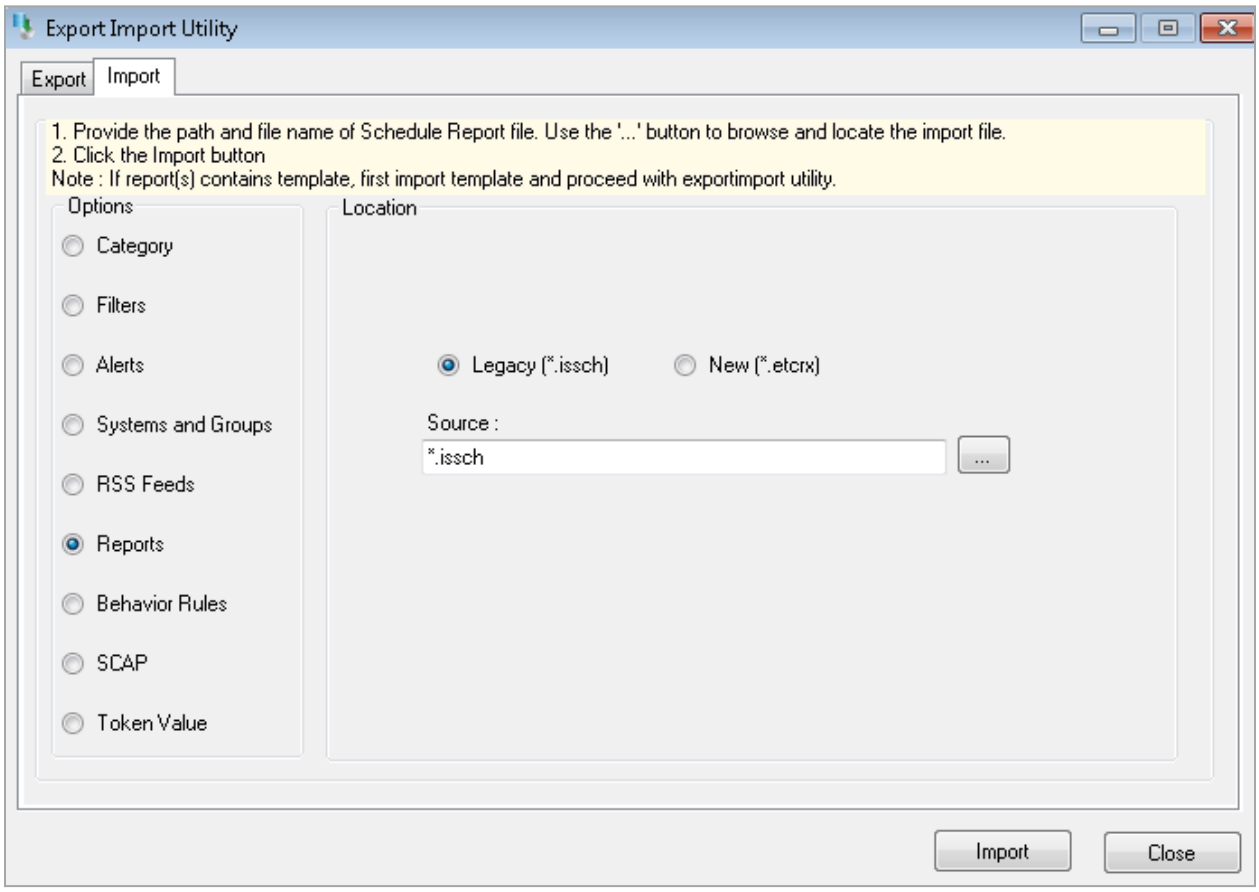

Figure 6

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

Figure 7

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

Import Parsing Rule

1. Click the **Admin** menu, and then click **Parsing rule**.

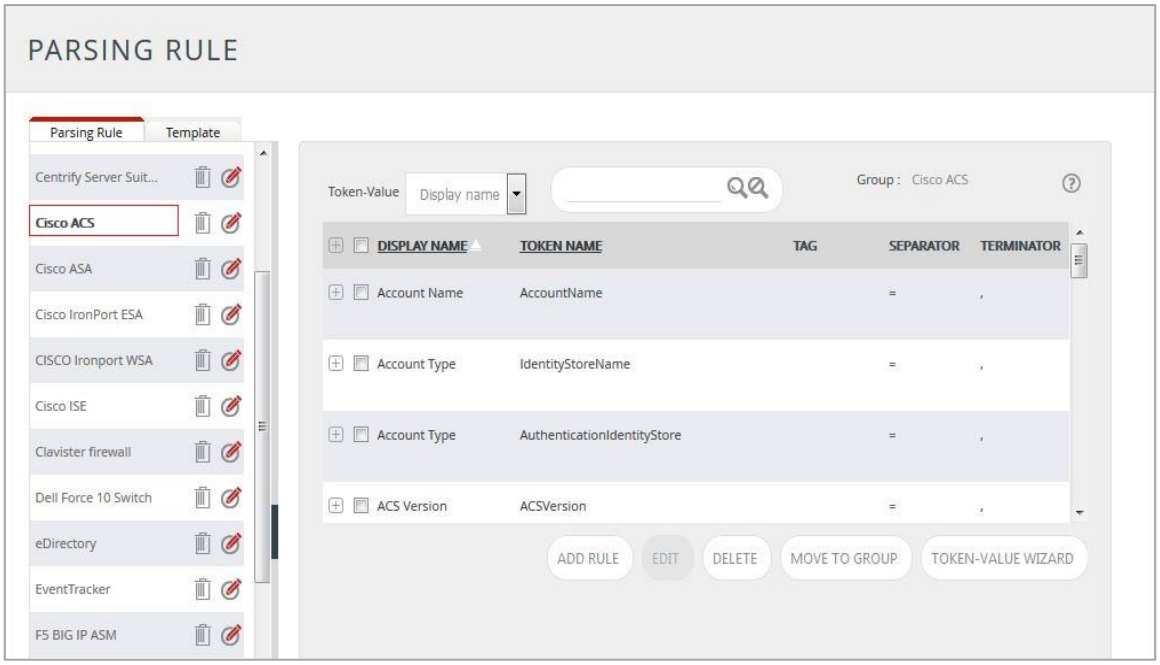

Figure 8

Import knowledge Object

1. Click the **Admin** menu, and then click **Knowledge Objects**.
2. Click on ‘**Import**’ option

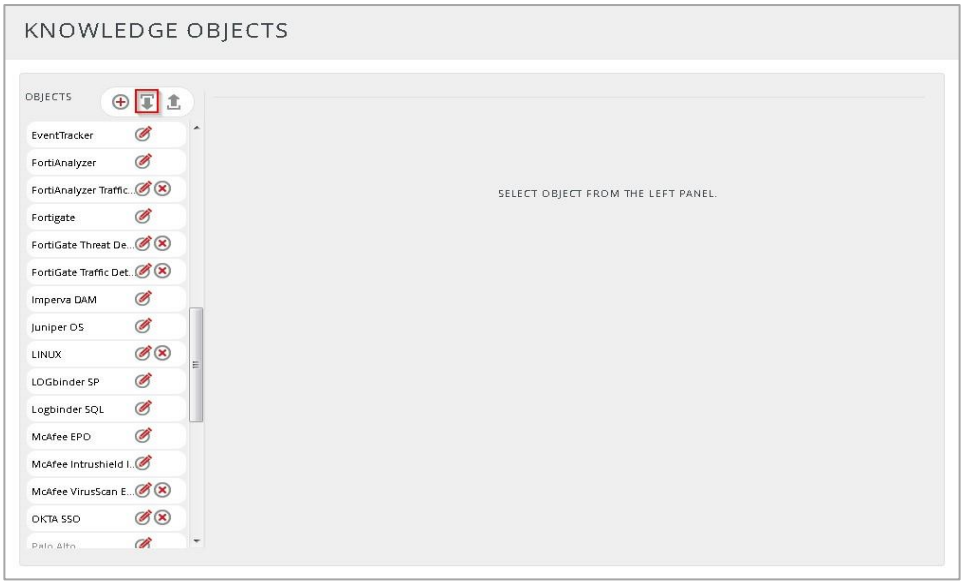

Figure 9

3. In **IMPORT** pane click on **Browse** button.

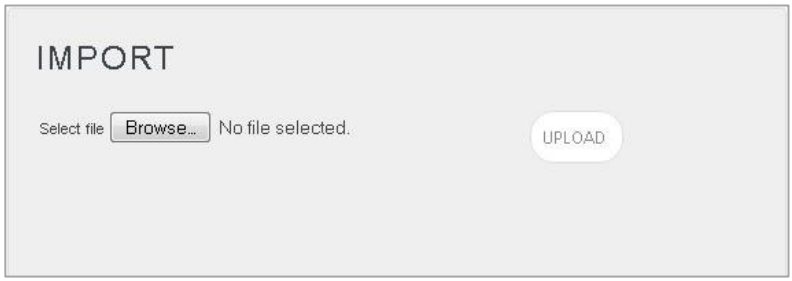

Figure 10

4. Locate **Cisco ACS.etko** file, and then click the **UPLOAD** button.

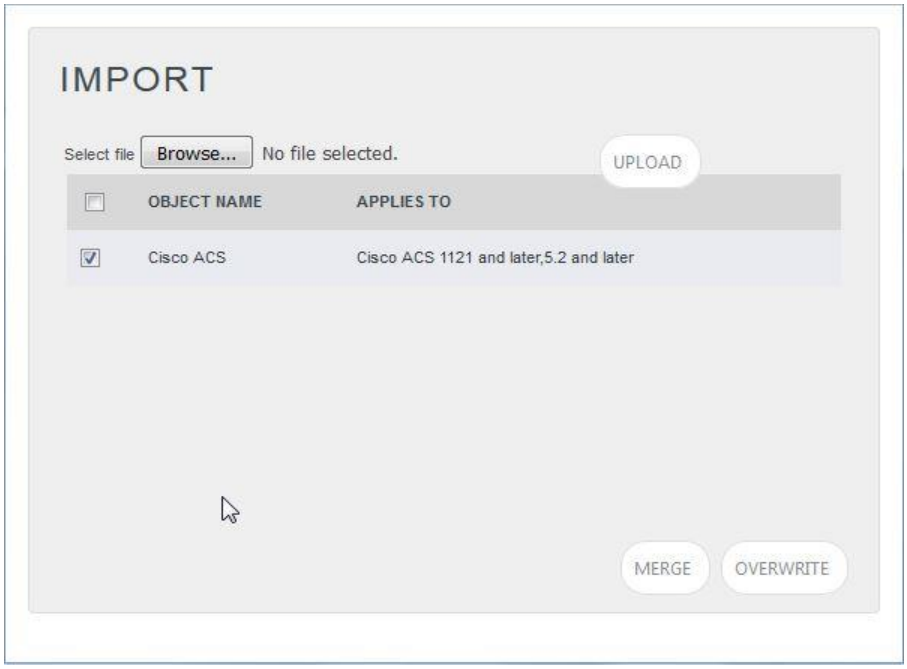

Figure 11

5. Now select the check box and then click on '**MERGE**' option.
   EventTracker displays success message.

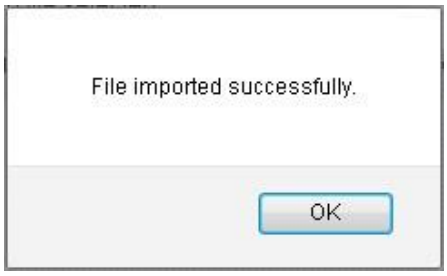

Figure 12

6. Click on **OK** button.

Verify Cisco ACS Knowledge Pack in EventTracker

Verify Cisco ACS Categories

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

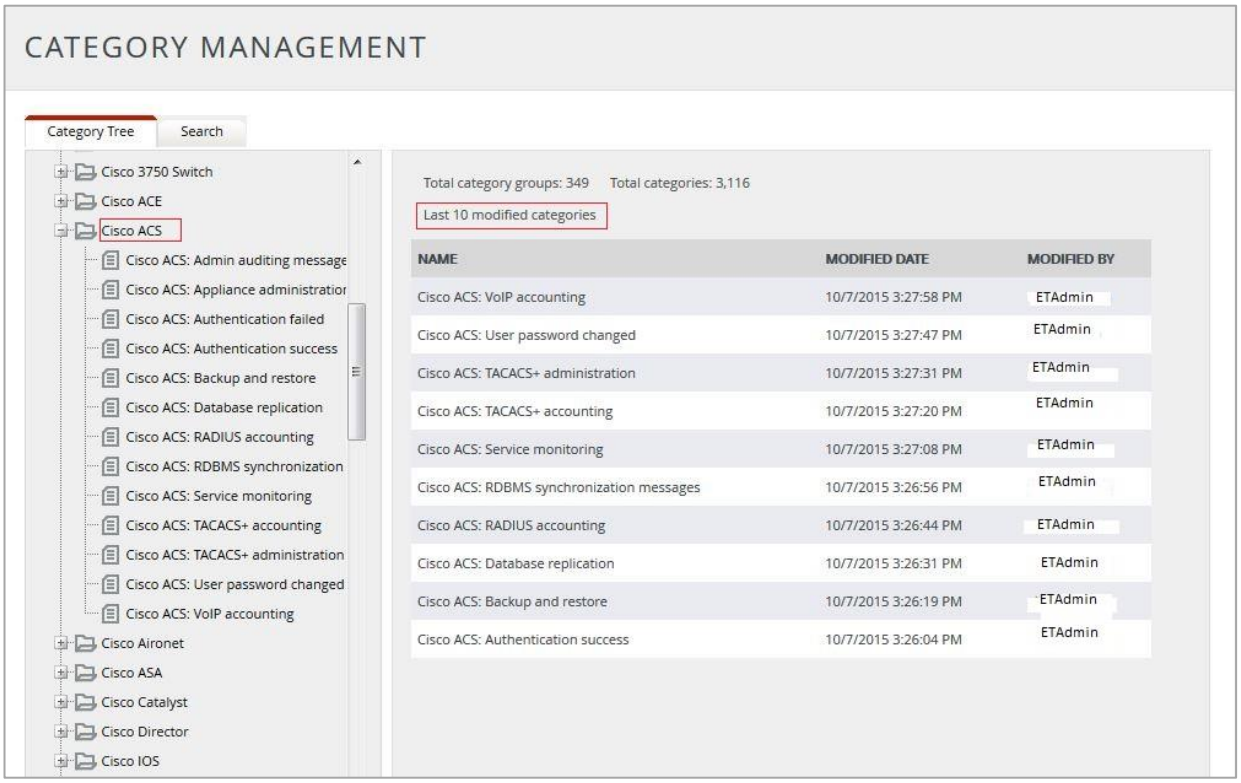

Figure 13

Verify Cisco ACS Alerts

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Alerts**.
3. In **Search** field, type '**Cisco ACS'**, and then click the **Go** button.

   Alert Management page will display all the imported Cisco ACS alerts.

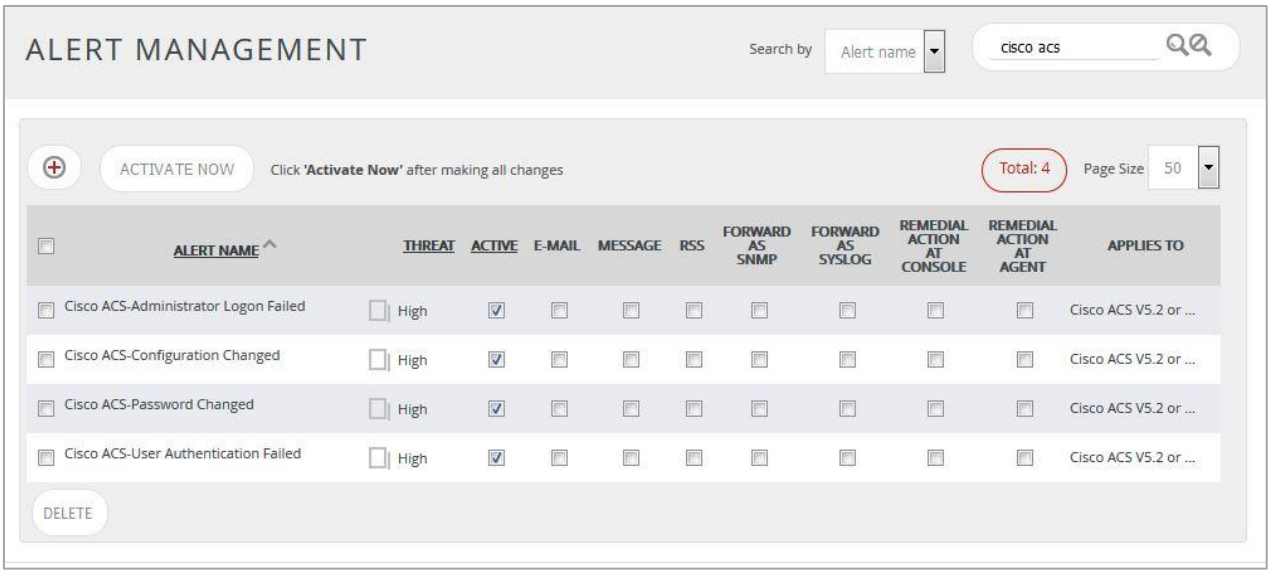

Figure 14

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

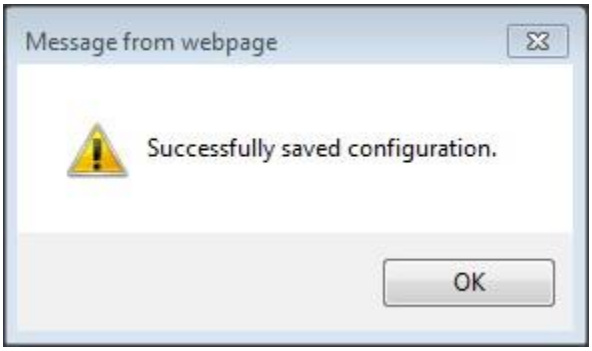

Figure 15

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

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

Verify Cisco ACS 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 Scheduled Reports, scroll down and click **Cisco ACS** group folder.

   Scheduled Reports are displayed in the Reports configuration pane

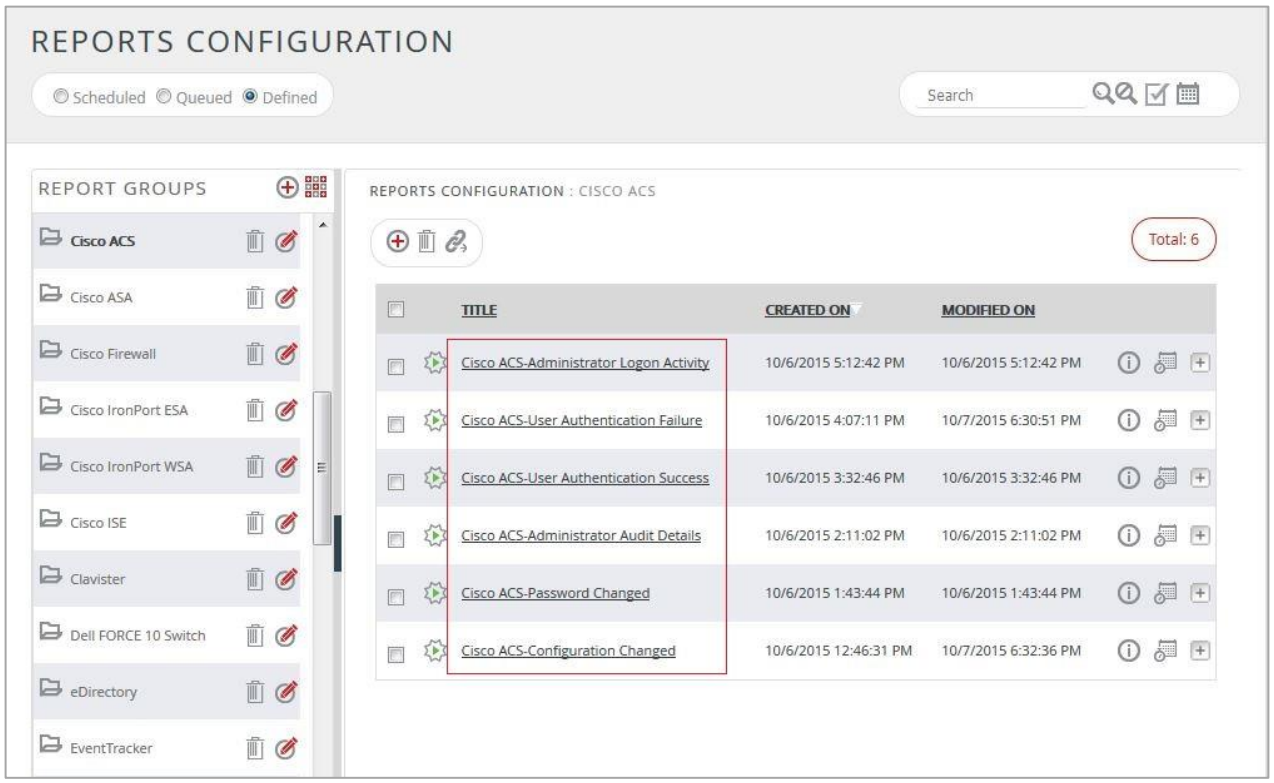

Figure 16

Verify Cisco ACS Parsing Rule

1. Click the **Admin** menu, and then click **Parsing rule**.
2. Scroll and find imported **Parsing rule**.

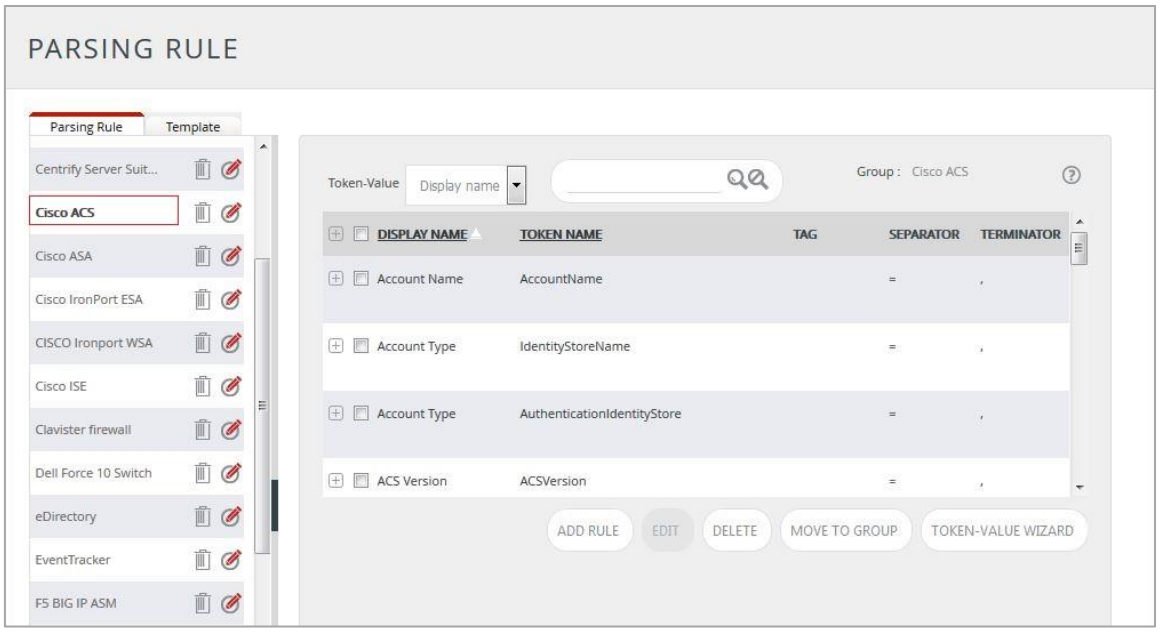

Figure 17

Verify Cisco ACS Knowledge Object

1. Click the **Admin** menu, and then click **Knowledge Objects.**
2. Scroll down and select **Cisco ACS** in **Objects** pane.
   Imported Cisco ACS object details are shown.

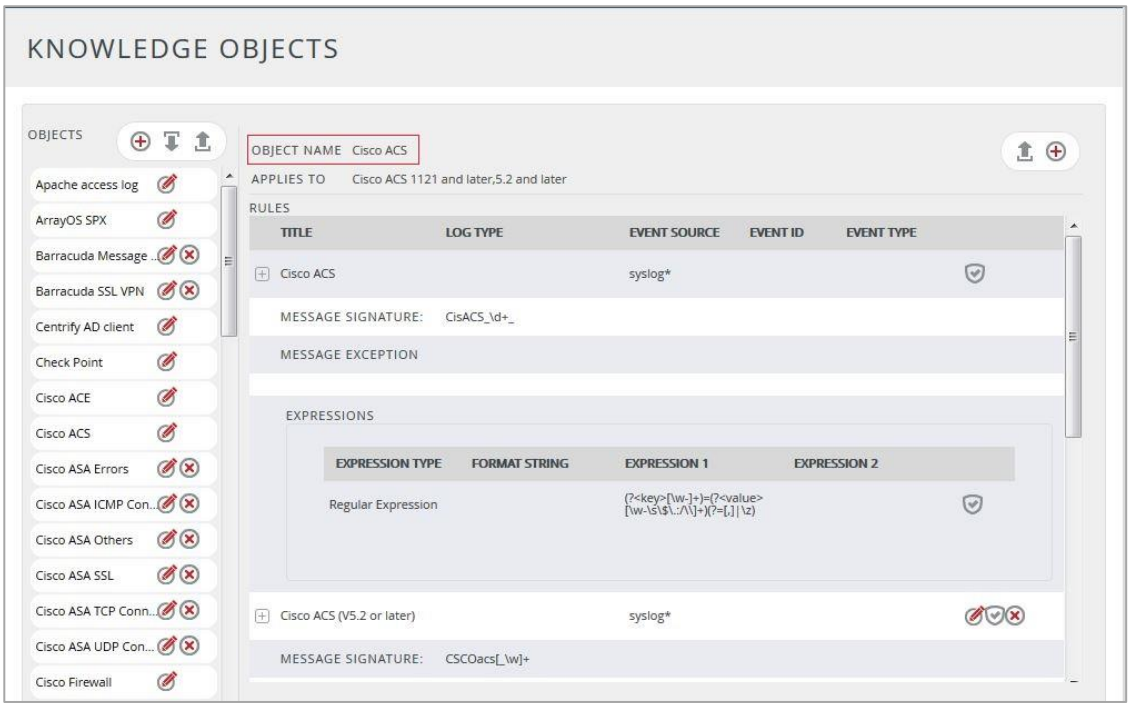

Figure 18

Create Dashboards in EventTracker

Schedule Reports

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

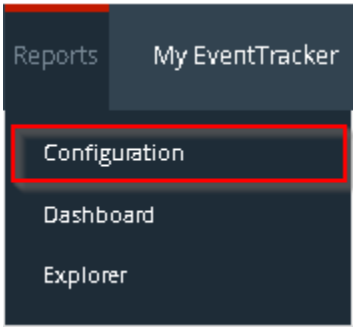

Figure 19

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

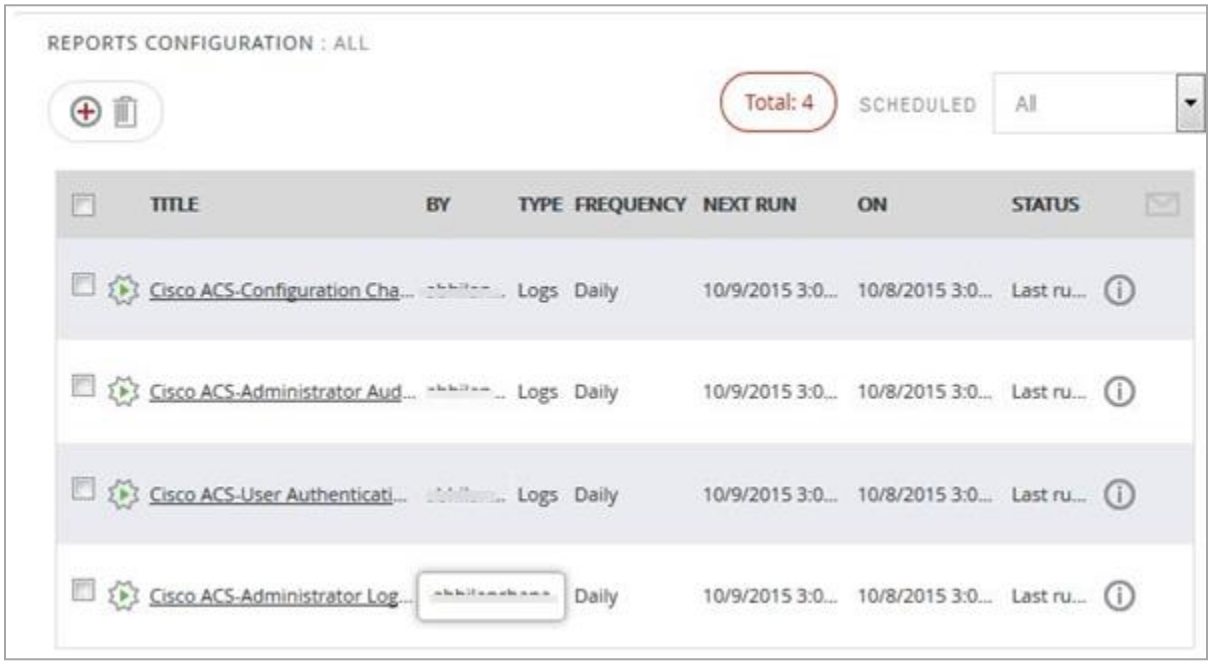

Figure 20

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

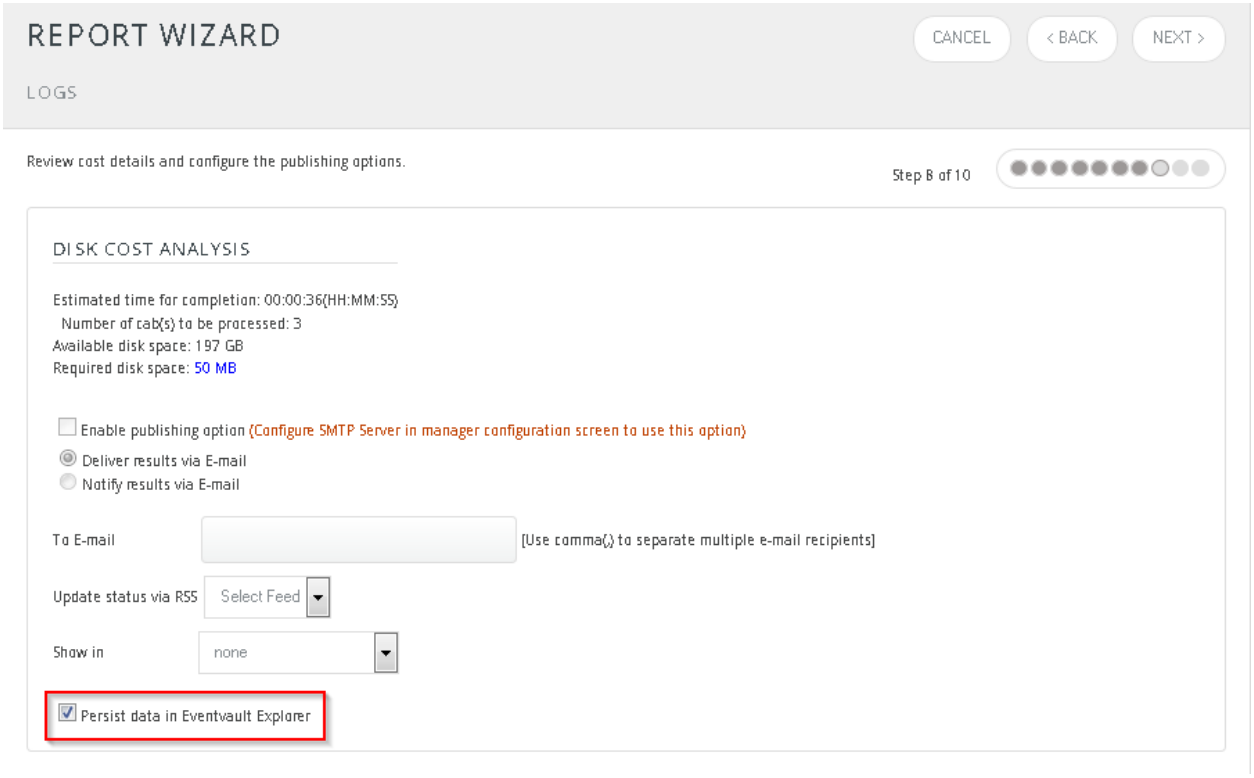

Figure 21

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

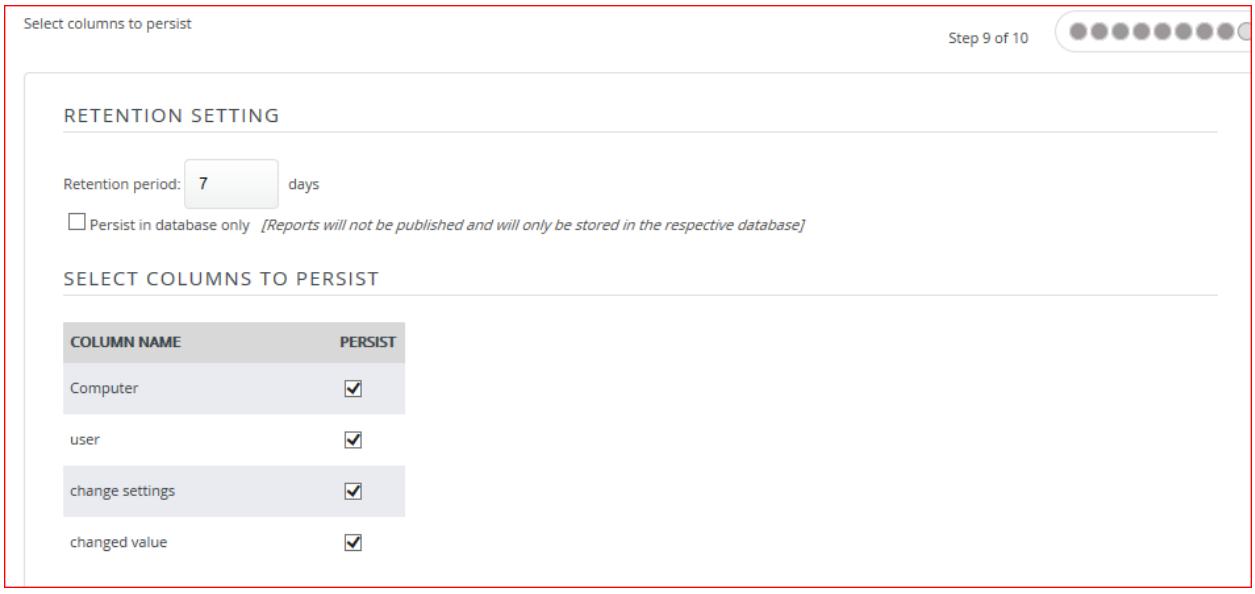

Figure 22

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.

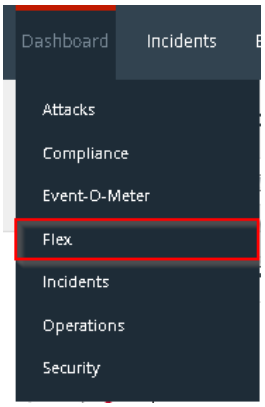

Figure 23

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

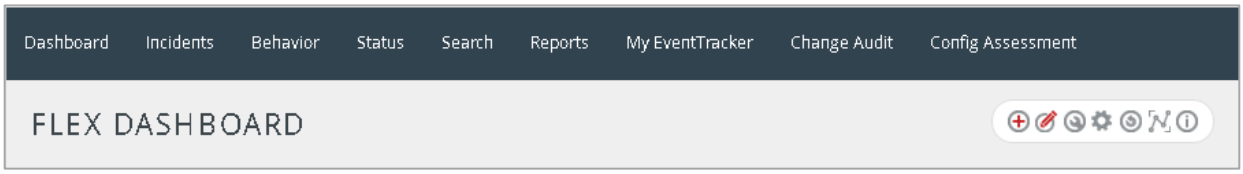

Figure 24

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

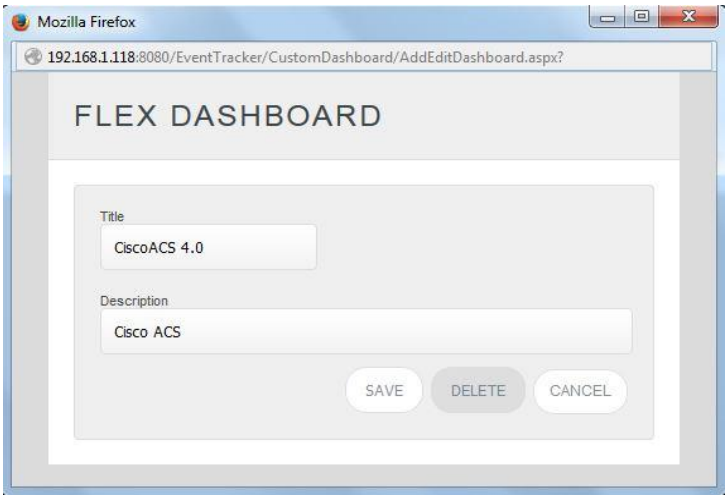

Figure 25

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

   Widget configuration pane is shown.

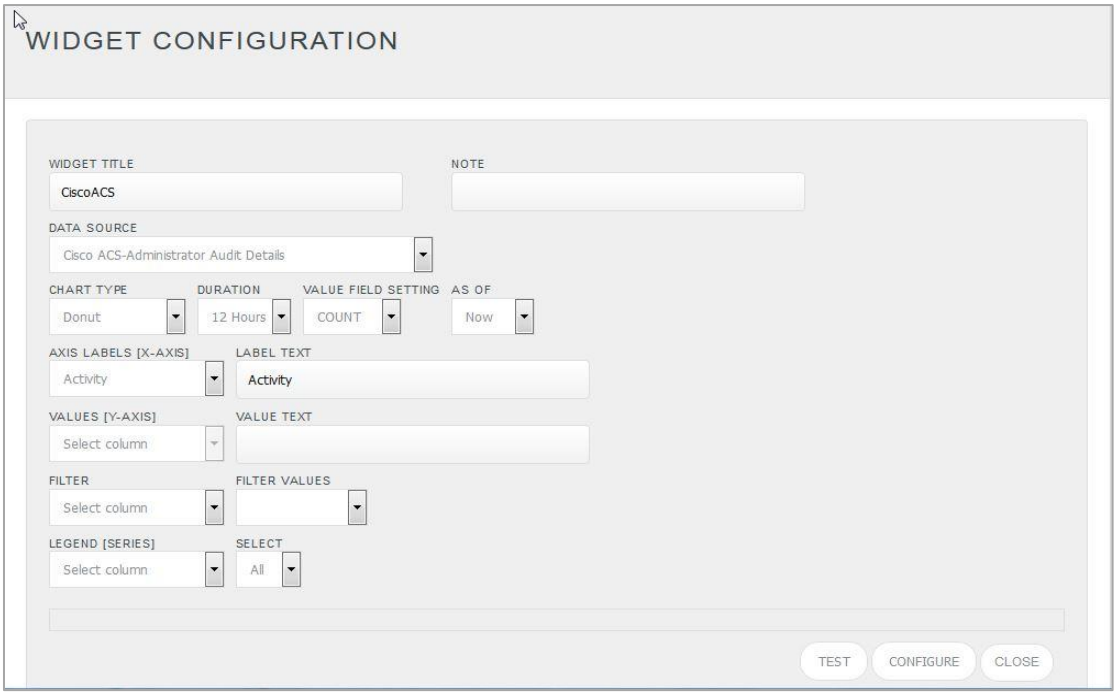

Figure 26

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.

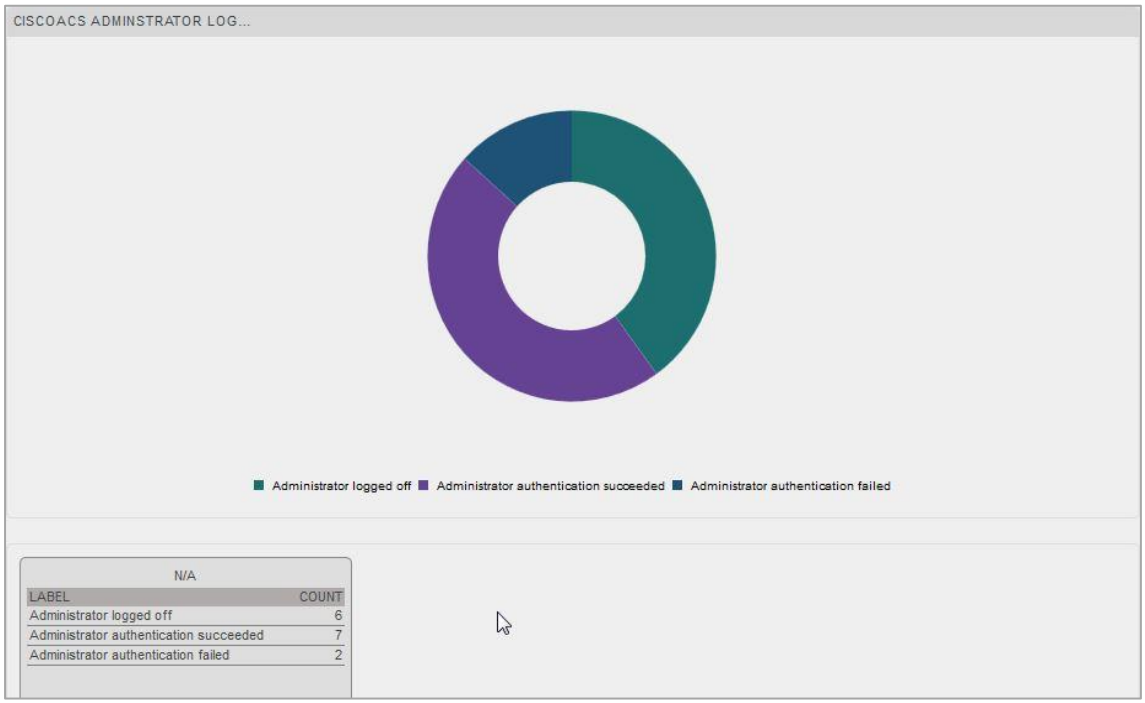

Figure 27

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

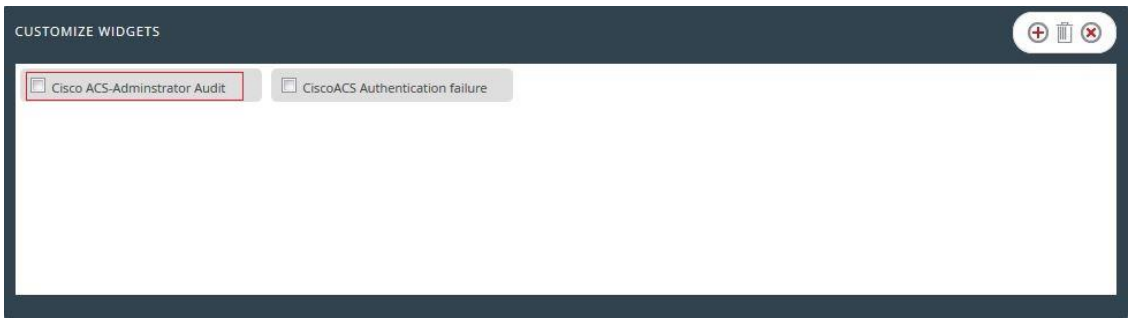

Figure 28

17. Click 'customize' to locate and choose created dashlet
18. Click to add dashlet to earlier created dashboard.

Sample Dashboards

1. Cisco ACS Administrator Logon Activity.

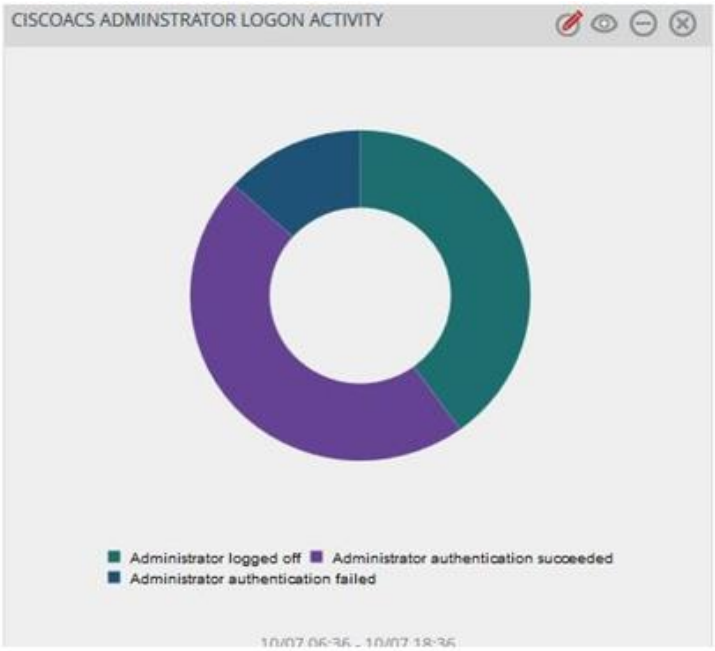

Figure 29

2. Cisco Configuration Changes Activity

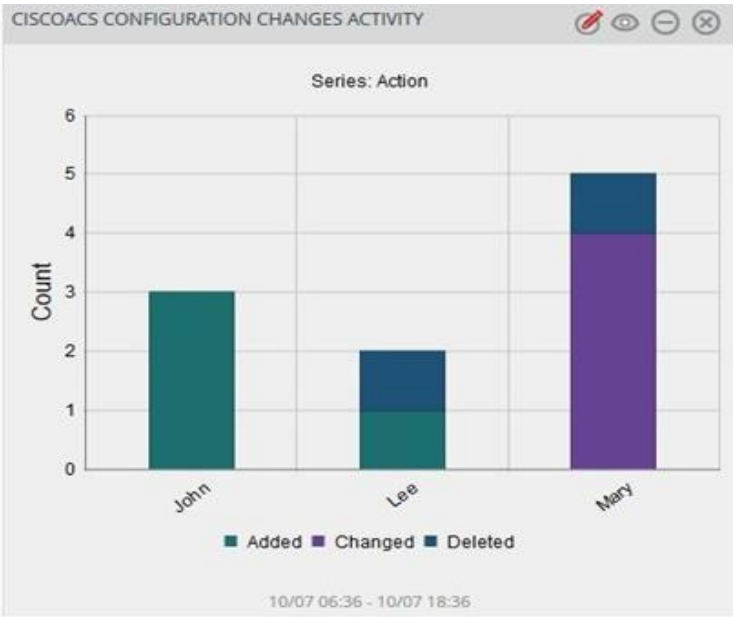

Figure 30

Sample Reports

1. Cisco ACS-User Authentication Failure

Cisco ACS-User Authentication Failure

LogTime	Device Address	Device Port	User Name	Authentication Type	NAS Address	NAS Port	Reason
10/06/2015 04:08:40 PM	10.60.1.212	1076	john	Radius	10.60.1.240	129	RADIUS Request dropped
10/06/2015 04:08:40 PM	10.60.1.240	1076	tsmith	Radius	10.60.1.240	129	RADIUS Request dropped
10/06/2015 04:08:40 PM	10.60.1.212	1077	john	Radius	10.60.1.240	129	Authentication failed
10/06/2015 04:08:40 PM	10.60.1.223	1076	michel	Radius	10.60.1.240	129	RADIUS Request dropped
10/06/2015 04:08:40 PM	10.60.1.240	1077	john	Radius	10.60.1.240	129	Authentication failed
10/06/2015 04:08:40 PM	10.60.1.223	1077	michel	Radius	10.60.1.240	129	Authentication failed
10/06/2015 04:08:40 PM	10.60.1.212	1076	john	Radius	10.60.1.240	129	RADIUS Request dropped
10/06/2015 04:08:40 PM	10.60.1.240	1077	michel	Radius	10.60.1.240	129	Authentication failed
10/06/2015 04:08:40 PM	10.60.1.212	1076	tsmith	Radius	10.60.1.240	129	RADIUS Request dropped
10/06/2015 04:08:40 PM	10.60.1.243	1077	michel	Radius	10.60.1.240	129	Authentication failed
10/06/2015 04:08:40 PM	10.60.1.240	1076	tsmith	Radius	10.60.1.240	129	RADIUS Request dropped

Figure 31

2. Cisco ACS-User Authentication Success

Cisco ACS-User Authentication Success

LogTime	Device Address	User Name	Account Type	Authentication Type	NAS Address	NAS Port	Destination Address	Destination Port
10/07/2015 02:01:16 PM	10.60.1.240	trav	Internal Users	Radius	10.60.1.240	129		
10/07/2015 02:19:36 PM	10.60.1.240	Racidbkupusr	Meggitt-LDAP	Radius	10.212.9.250	2	10.212.9.140	1645
10/07/2015 02:18:35 PM	10.60.1.240	Racidbkupusr	Meggitt-LDAP	Radius	10.212.9.250	1	10.212.9.140	1645
10/07/2015 02:13:16 PM	10.60.1.240	trav	Internal Users	Radius	10.60.1.240	129		
10/07/2015 02:39:56 PM	10.60.1.240	Racidbkupusr	Meggitt-LDAP	Radius	10.212.9.250	1	10.212.9.140	1645
10/07/2015 02:14:56 PM	10.60.1.240	Racidbkupusr	Meggitt-LDAP	Radius	10.212.9.250	2	10.212.9.140	1645
10/07/2015 01:49:36 PM	10.60.1.240	Racidbkupusr	Meggitt-LDAP	Radius	10.212.9.250	1	10.212.9.140	1645
10/07/2015 01:19:36 PM	10.60.1.240	trav	Internal Users	Radius	10.60.1.240	129		
10/07/2015 09:39:56 PM	10.60.1.240	Racidbkupusr	Meggitt-LDAP	Radius	10.212.9.250	2	10.212.9.140	1645
10/07/2015 04:19:26 PM	10.60.1.240	Racidbkupusr	Meggitt-LDAP	Radius	10.212.9.250	1	10.212.9.140	1645
10/07/2015 02:17:33 PM	10.60.1.240	trav	Internal Users	Radius	10.60.1.240	129		
10/07/2015 02:49:36 PM	10.60.1.240	Racidbkupusr	Meggitt-LDAP	Radius	10.212.9.250	2	10.212.9.140	1645
10/07/2015 02:49:56 PM	10.60.1.240	Racidbkupusr	Meggitt-LDAP	Radius	10.212.9.250	1	10.212.9.140	1645
10/07/2015 02:19:36 PM	10.60.1.240	Racidbkupusr	Meggitt-LDAP	Radius	10.212.9.250	2	10.212.9.140	1645
10/07/2015 02:49:26 PM	10.60.1.240	trav	Internal Users	Radius	10.60.1.240	129		
10/07/2015 02:19:16 PM	10.60.1.240	trav	Internal Users	Radius	10.60.1.240	129		
10/07/2015 03:19:36 PM	10.60.1.240	Racidbkupusr	Meggitt-LDAP	Radius	10.212.9.250	2	10.212.9.140	1645
10/07/2015 02:17:33 PM	10.60.1.240	Racidbkupusr	Meggitt-LDAP	Radius	10.212.9.250	1	10.212.9.140	1645
10/07/2015 02:49:36 PM	10.60.1.240	trav	Internal Users	Radius	10.60.1.240	129		
10/07/2015 02:49:56 PM	10.60.1.240	Racidbkupusr	Meggitt-LDAP	Radius	10.212.9.250	1	10.212.9.140	1645
10/07/2015 02:19:36 PM	10.60.1.240	Racidbkupusr	Meggitt-LDAP	Radius	10.212.9.250	2	10.212.9.140	1645
10/07/2015 02:49:26 PM	10.60.1.240	trav	Internal Users	Radius	10.60.1.240	129		

Figure 32