

Integrate Cisco ACS

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.

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
Prerequisites.....	3
Configure Cisco ACS to forward all logs to EventTracker	3
Configure Syslog logging.....	3
EventTracker Knowledge Pack	4
Categories.....	4
Alerts	5
Reports	5
Import Cisco ACS knowledge pack into EventTracker.....	5
Import Category	6
Import Alerts	7
Import Flex Alerts	8
Import Parsing Rule	9
Import knowledge Object.....	9
Verify Cisco ACS Knowledge Pack in EventTracker	11
Verify Cisco ACS Categories.....	11
Verify Cisco ACS Alerts	11
Verify Cisco ACS Flex Reports	13
Verify Cisco ACS Parsing Rule	13
Verify Cisco ACS Knowledge Object	14
Create Dashboards in EventTracker	15
Schedule Reports.....	15
Create Dashlets	17
Sample Dashboards.....	20
Sample Reports	21

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**.

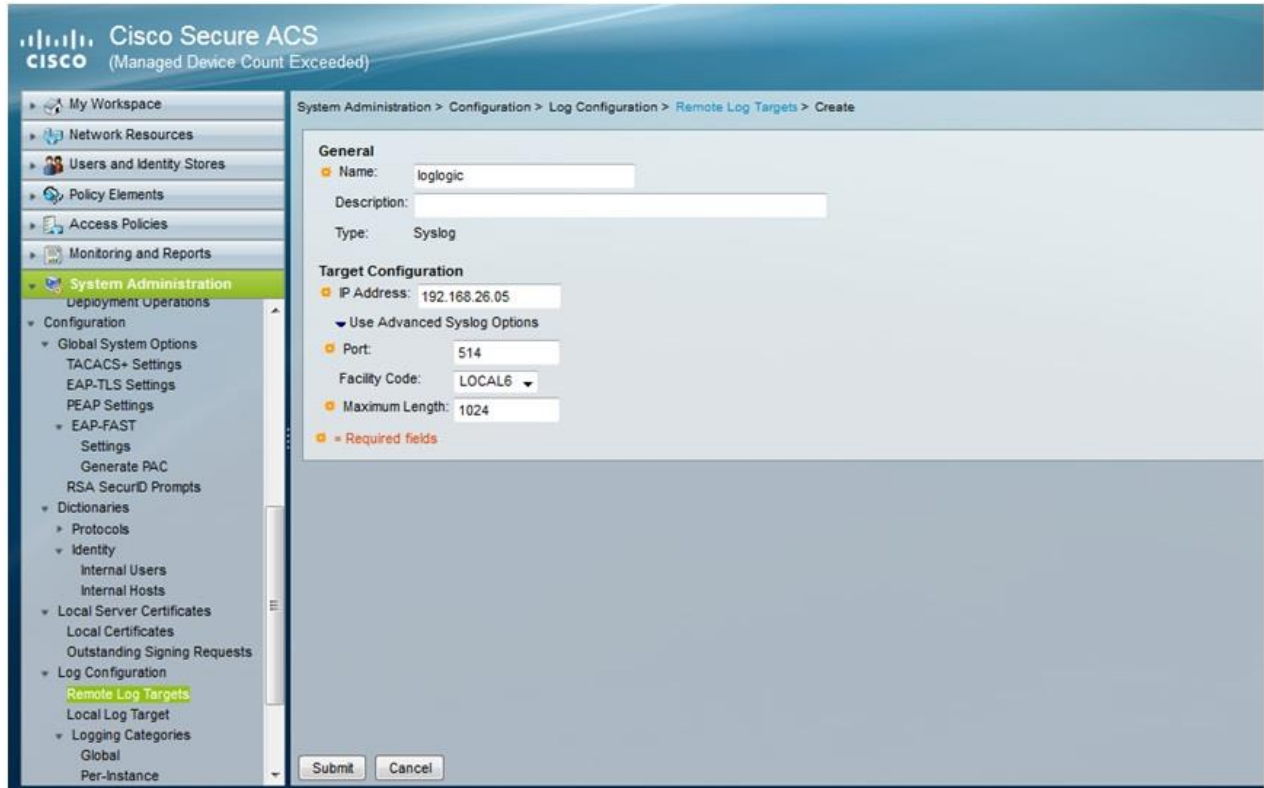


Figure 1

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.

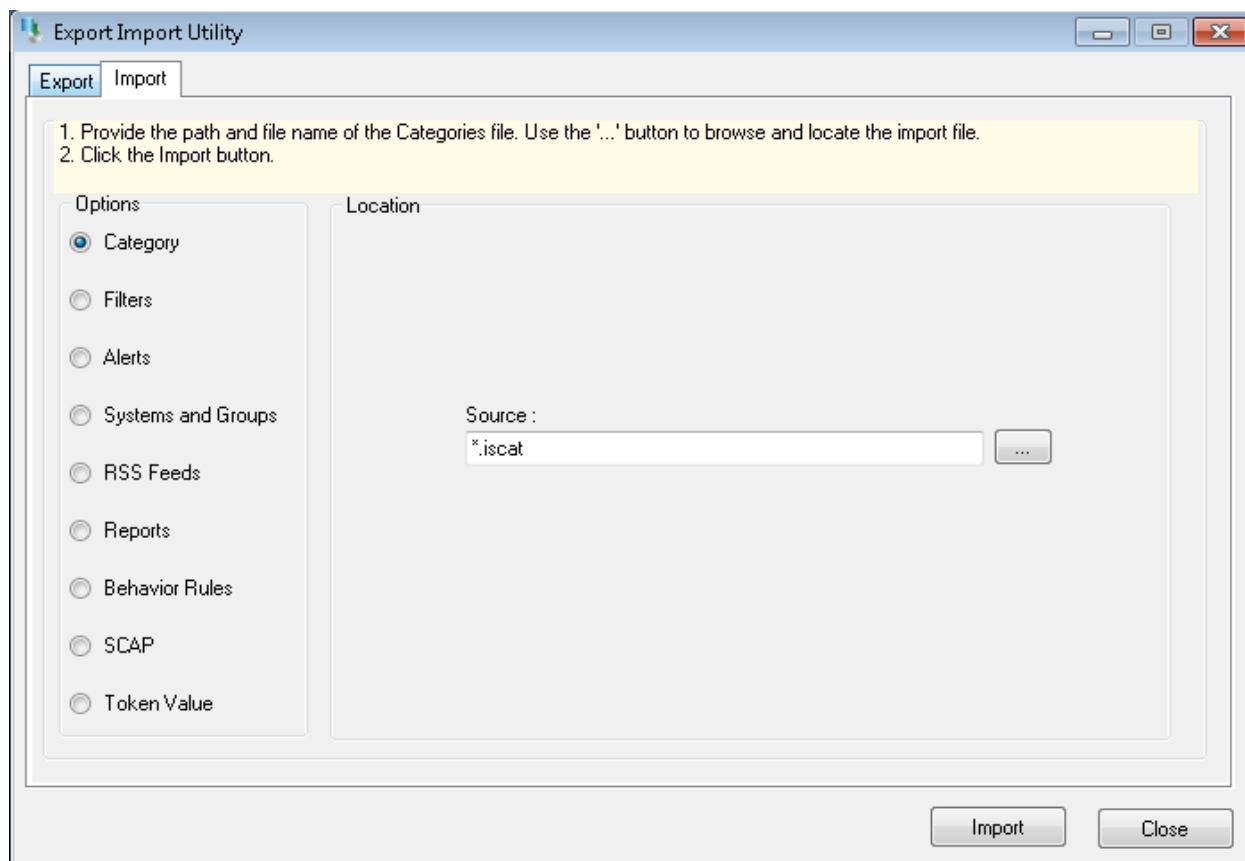


Figure 2

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.

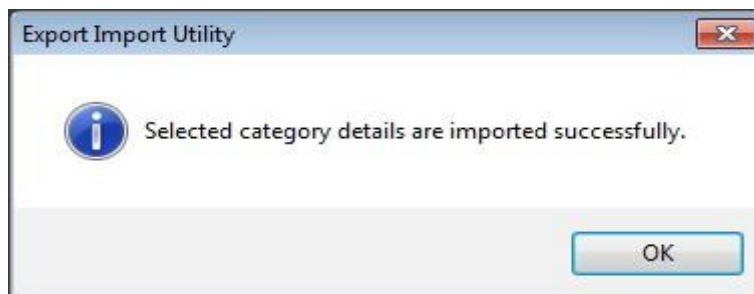


Figure 3

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

Import Alerts

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

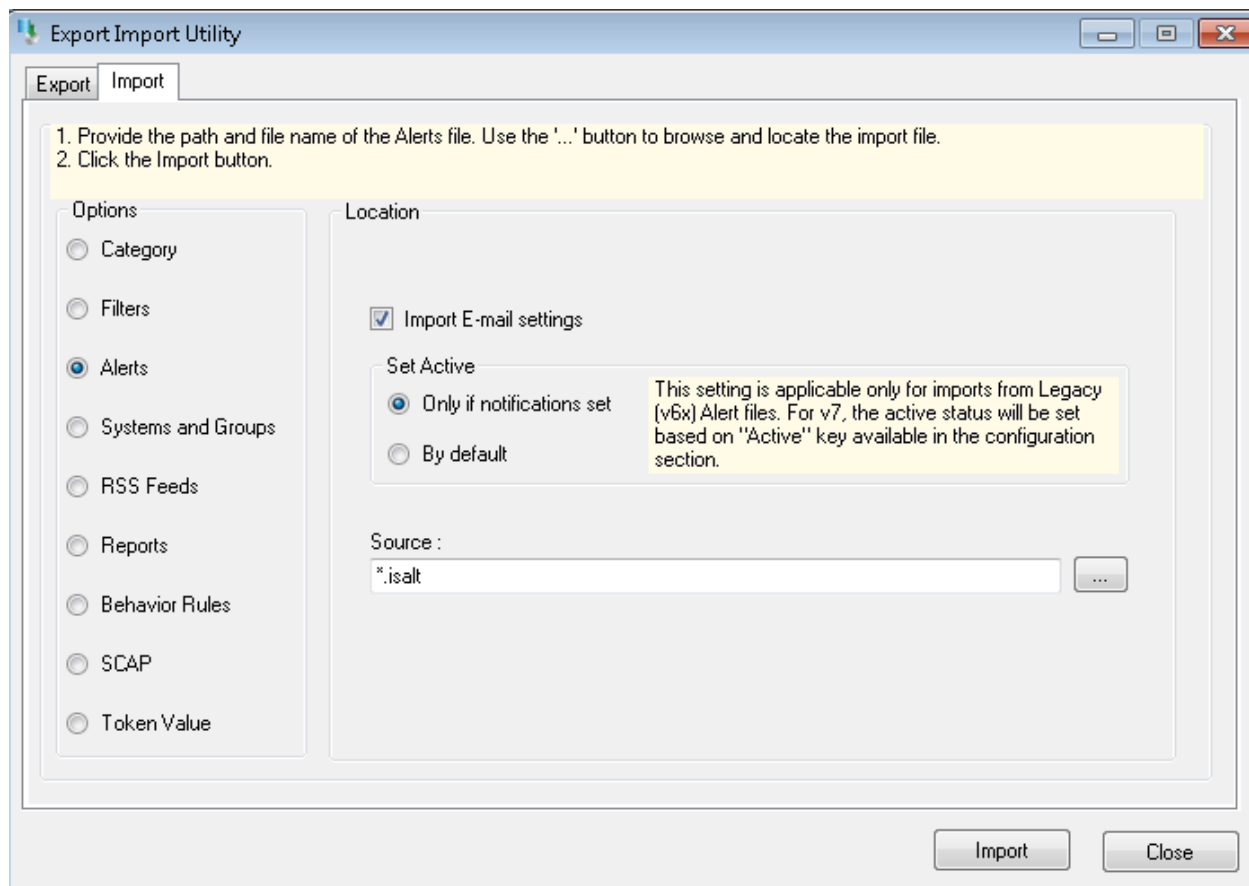


Figure 4

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.

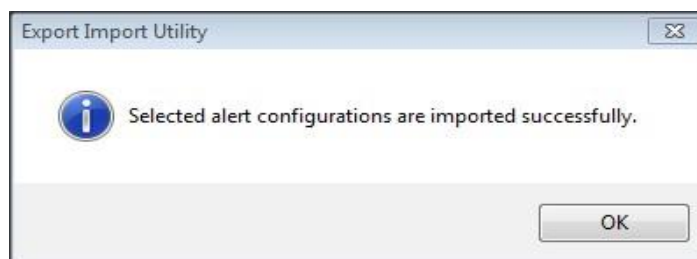



Figure 5

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.

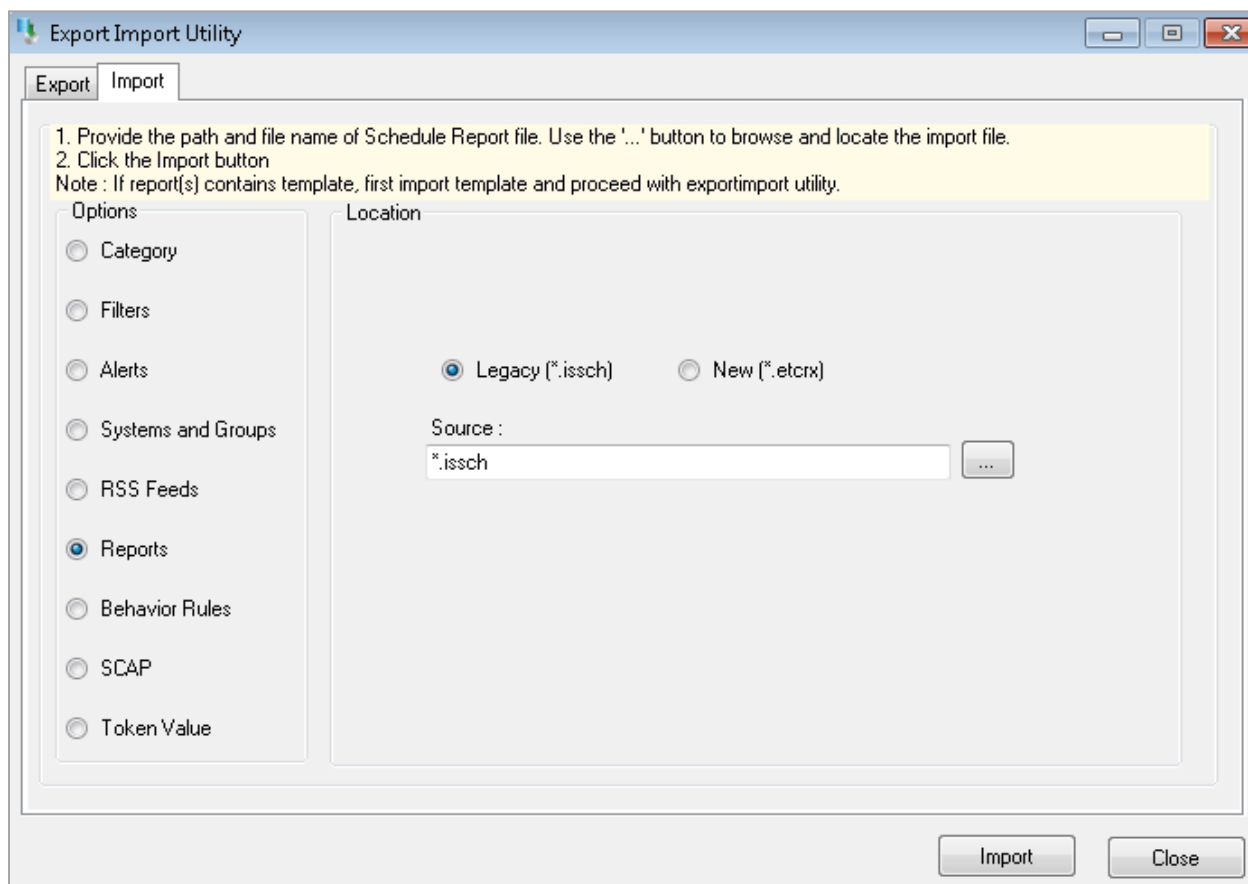


Figure 6

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

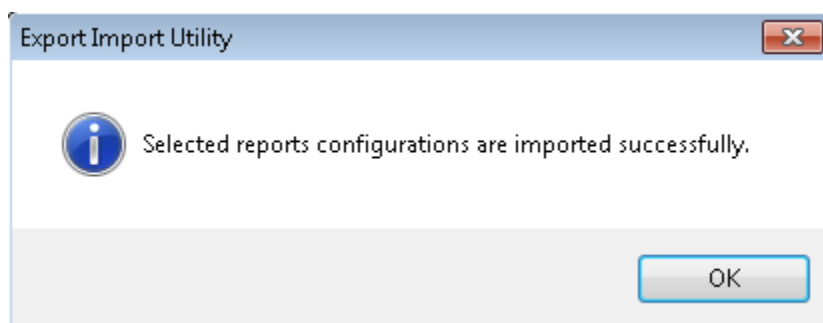


Figure 7

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

Import Parsing Rule

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

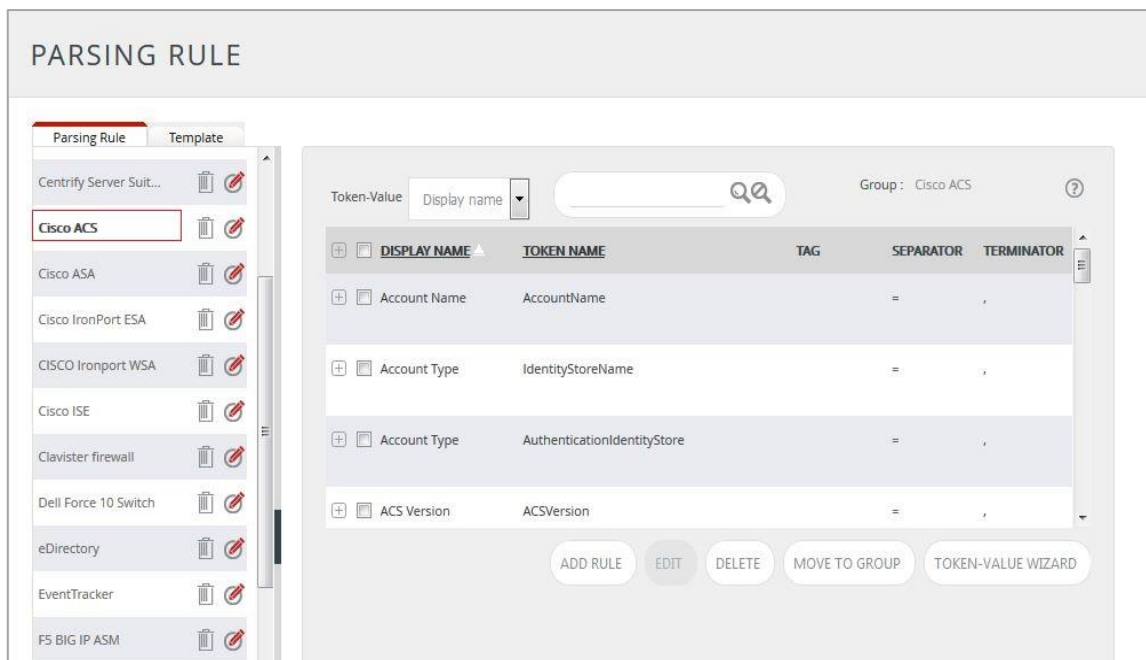


Figure 8

Import knowledge Object

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

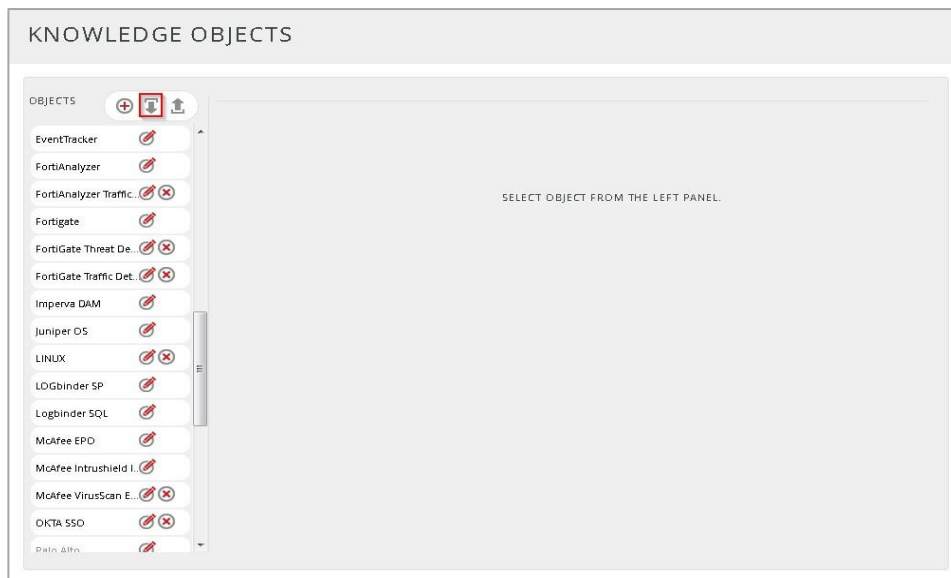


Figure 9

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

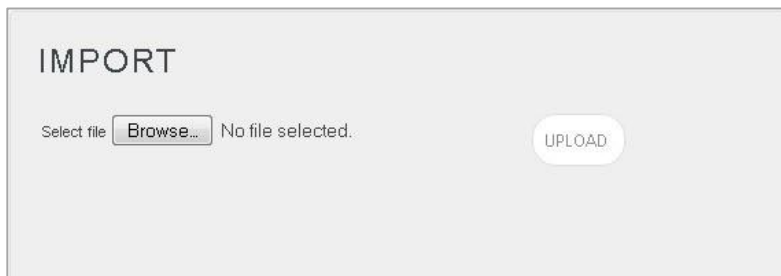


Figure 10

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

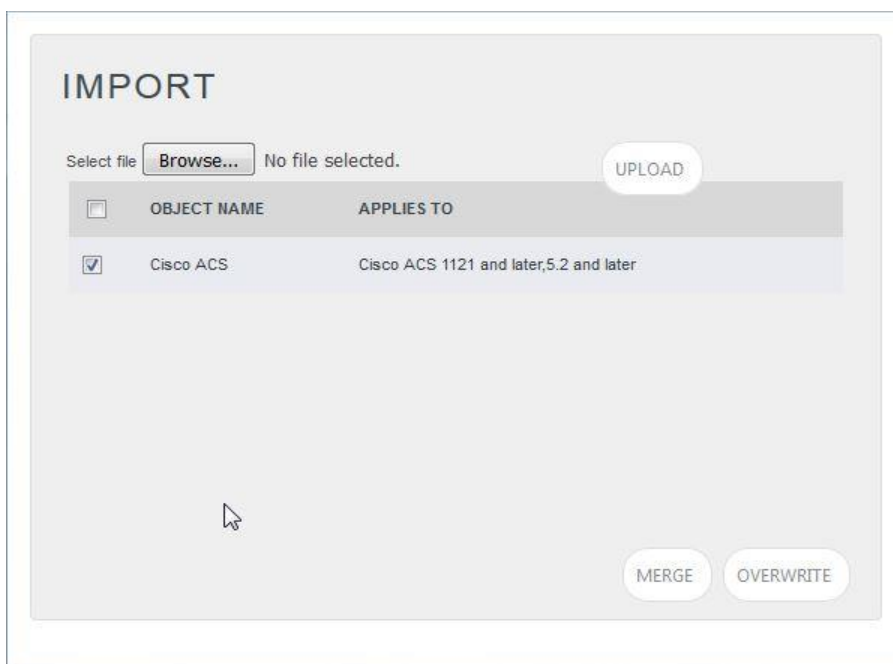


Figure 11

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

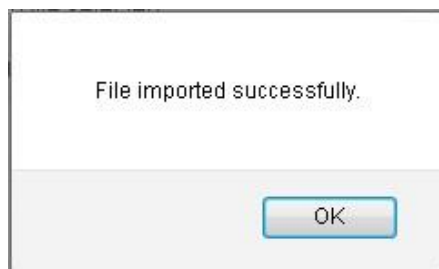


Figure 12

- 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.

The screenshot displays the 'CATEGORY MANAGEMENT' interface. On the left, a 'Category Tree' shows a hierarchy of folders including Cisco 3750 Switch, Cisco ACE, Cisco ACS (highlighted with a red box), Cisco Aironet, Cisco ASA, Cisco Catalyst, Cisco Director, and Cisco IOS. Under the Cisco ACS folder, several sub-categories are listed, such as 'Cisco ACS: Admin auditing message', 'Cisco ACS: Appliance administrator', 'Cisco ACS: Authentication failed', 'Cisco ACS: Authentication success', 'Cisco ACS: Backup and restore', 'Cisco ACS: Database replication', 'Cisco ACS: RADIUS accounting', 'Cisco ACS: RDBMS synchronization', 'Cisco ACS: Service monitoring', 'Cisco ACS: TACACS+ accounting', 'Cisco ACS: TACACS+ administration', 'Cisco ACS: User password changed', and 'Cisco ACS: VoIP accounting'. On the right, a table titled 'Last 10 modified categories' shows the following data:

NAME	MODIFIED DATE	MODIFIED BY
Cisco ACS: VoIP accounting	10/7/2015 3:27:58 PM	ETAdmin
Cisco ACS: User password changed	10/7/2015 3:27:47 PM	ETAdmin
Cisco ACS: TACACS+ administration	10/7/2015 3:27:31 PM	ETAdmin
Cisco ACS: TACACS+ accounting	10/7/2015 3:27:20 PM	ETAdmin
Cisco ACS: Service monitoring	10/7/2015 3:27:08 PM	ETAdmin
Cisco ACS: RDBMS synchronization messages	10/7/2015 3:26:56 PM	ETAdmin
Cisco ACS: RADIUS accounting	10/7/2015 3:26:44 PM	ETAdmin
Cisco ACS: Database replication	10/7/2015 3:26:31 PM	ETAdmin
Cisco ACS: Backup and restore	10/7/2015 3:26:19 PM	ETAdmin
Cisco ACS: Authentication success	10/7/2015 3:26:04 PM	ETAdmin

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.

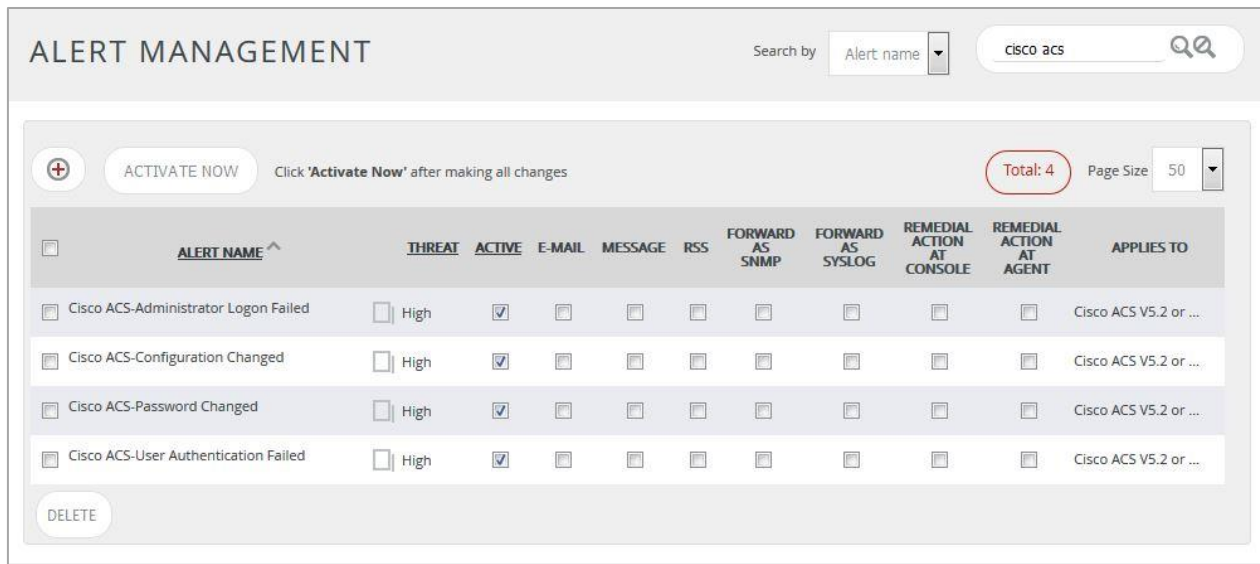


Figure 14

- 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: 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

REPORTS CONFIGURATION

Scheduled Queued Defined

Search

REPORT GROUPS

- Cisco ACS
- Cisco ASA
- Cisco Firewall
- Cisco IronPort ESA
- Cisco IronPort WSA
- Cisco ISE
- Clavister
- Dell FORCE 10 Switch
- eDirectory
- EventTracker

REPORTS CONFIGURATION : CISCO ACS Total: 6

TITLE	CREATED ON	MODIFIED ON	
Cisco ACS-Administrator Logon Activity	10/6/2015 5:12:42 PM	10/6/2015 5:12:42 PM	<input type="button" value="i"/> <input type="button" value="📄"/> <input type="button" value="⊕"/>
Cisco ACS-User Authentication Failure	10/6/2015 4:07:11 PM	10/7/2015 6:30:51 PM	<input type="button" value="i"/> <input type="button" value="📄"/> <input type="button" value="⊕"/>
Cisco ACS-User Authentication Success	10/6/2015 3:32:46 PM	10/6/2015 3:32:46 PM	<input type="button" value="i"/> <input type="button" value="📄"/> <input type="button" value="⊕"/>
Cisco ACS-Administrator Audit Details	10/6/2015 2:11:02 PM	10/6/2015 2:11:02 PM	<input type="button" value="i"/> <input type="button" value="📄"/> <input type="button" value="⊕"/>
Cisco ACS-Password Changed	10/6/2015 1:43:44 PM	10/6/2015 1:43:44 PM	<input type="button" value="i"/> <input type="button" value="📄"/> <input type="button" value="⊕"/>
Cisco ACS-Configuration Changed	10/6/2015 12:46:31 PM	10/7/2015 6:32:36 PM	<input type="button" value="i"/> <input type="button" value="📄"/> <input type="button" value="⊕"/>

Figure 16

Verify Cisco ACS Parsing Rule

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

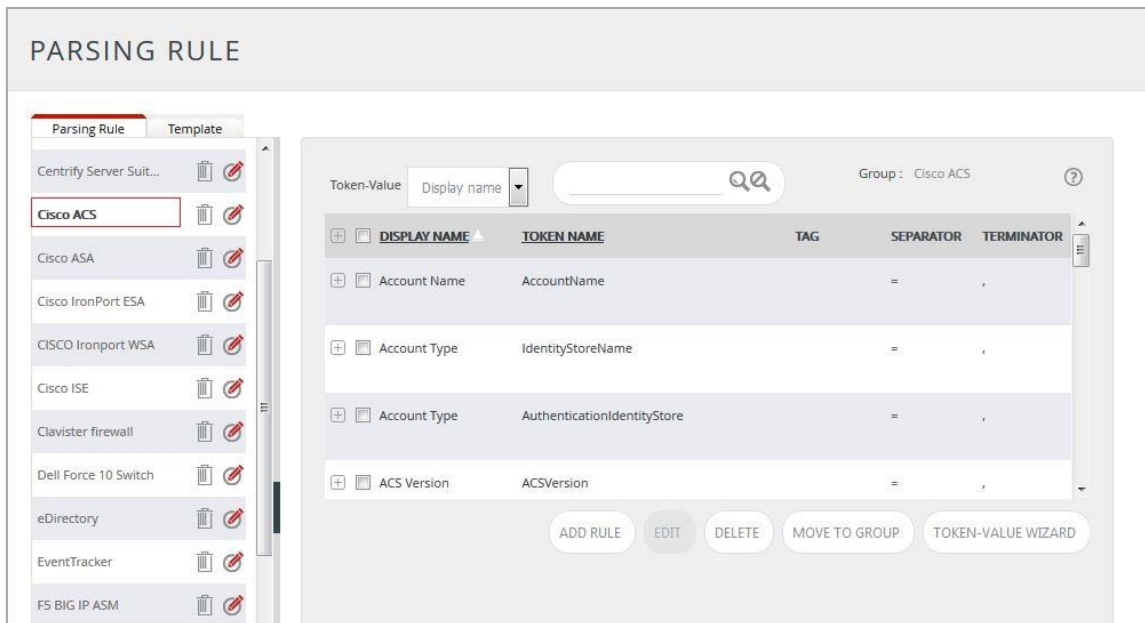


Figure 17

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.

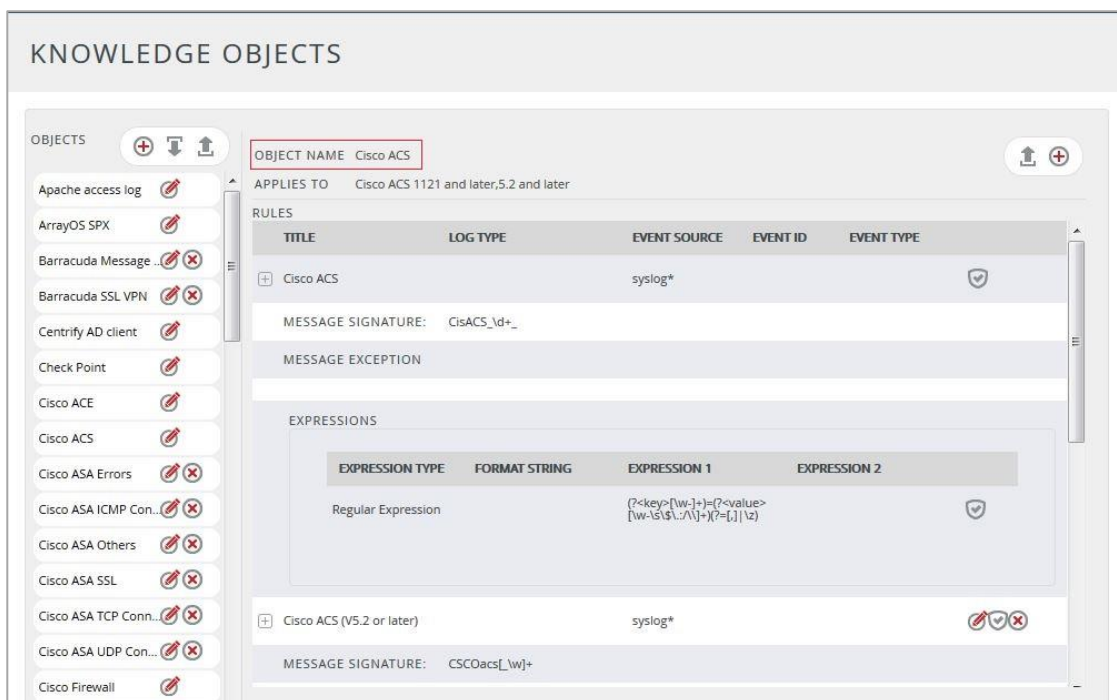


Figure 18

Create Dashboards in EventTracker

Schedule Reports

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

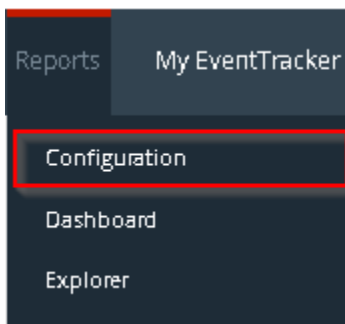


Figure 19


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

REPORTS CONFIGURATION : ALL

Total: 4 SCHEDULED All

<input type="checkbox"/>	TITLE	BY	TYPE	FREQUENCY	NEXT RUN	ON	STATUS	<input type="checkbox"/>
<input type="checkbox"/>	Cisco ACS-Configuration Cha...	...	Logs	Daily	10/9/2015 3:0...	10/8/2015 3:0...	Last ru...	<input type="checkbox"/>
<input type="checkbox"/>	Cisco ACS-Administrator Aud...	...	Logs	Daily	10/9/2015 3:0...	10/8/2015 3:0...	Last ru...	<input type="checkbox"/>
<input type="checkbox"/>	Cisco ACS-User Authenticati...	...	Logs	Daily	10/9/2015 3:0...	10/8/2015 3:0...	Last ru...	<input type="checkbox"/>
<input type="checkbox"/>	Cisco ACS-Administrator Log...	...		Daily	10/9/2015 3:0...	10/8/2015 3:0...	Last ru...	<input type="checkbox"/>

Figure 20

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

REPORT WIZARD

LOGS

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

DISK COST ANALYSIS

Estimated time for completion: 00:00:36(HH:MM:SS)
 Number of tab(s) to be processed: 3
 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 21

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

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
Computer	<input checked="" type="checkbox"/>
user	<input checked="" type="checkbox"/>
change settings	<input checked="" type="checkbox"/>
changed value	<input checked="" type="checkbox"/>

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.

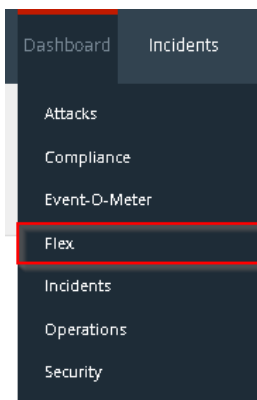


Figure 23

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

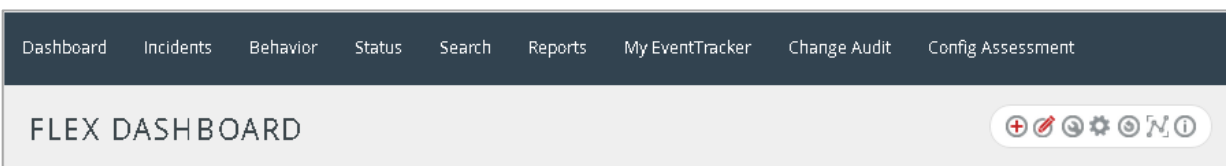



Figure 24

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

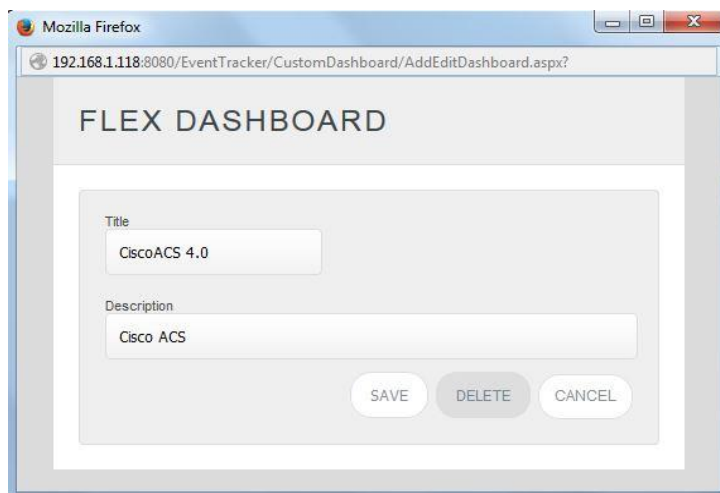



Figure 25

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

Widget configuration pane is shown.

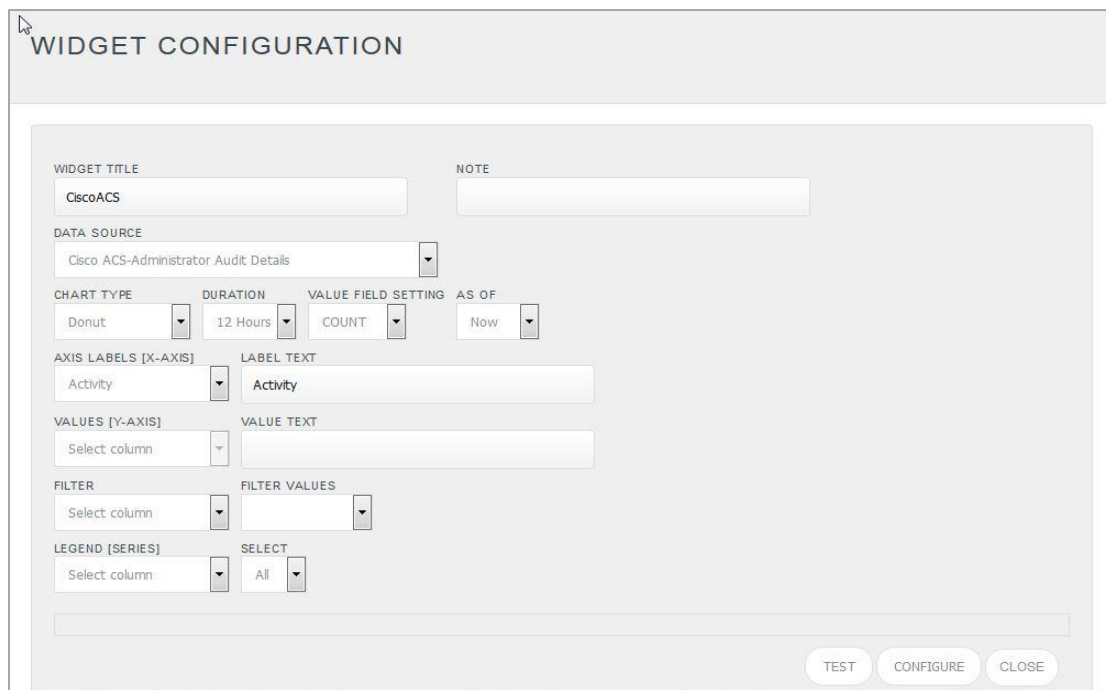


Figure 26

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.

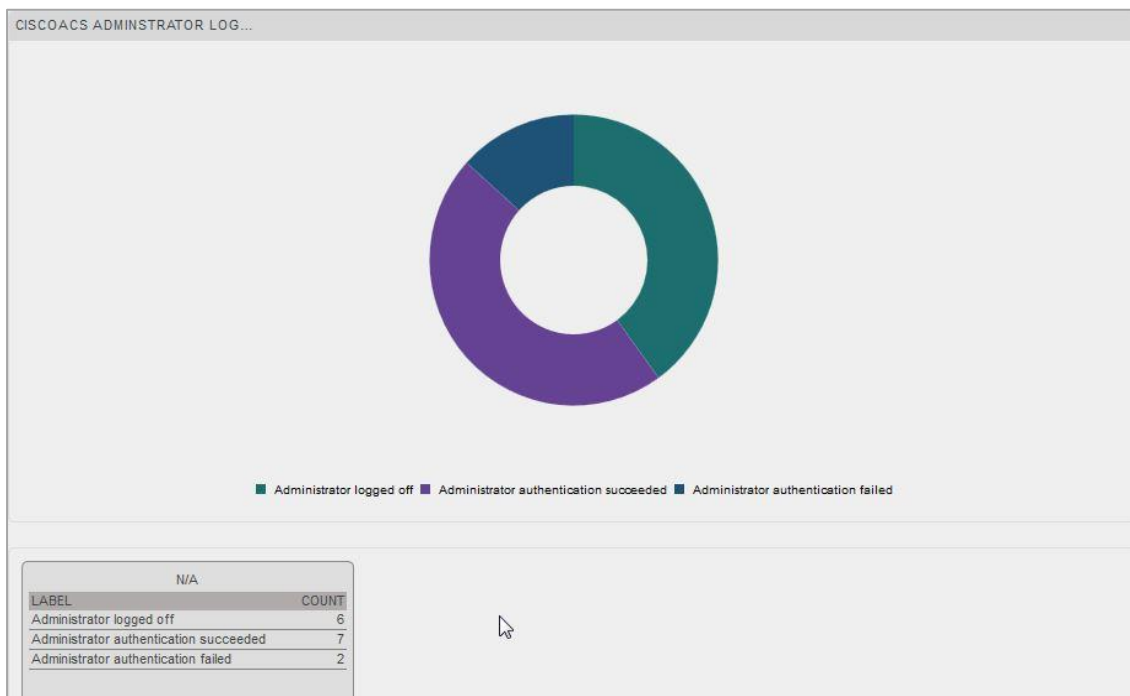


Figure 27

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

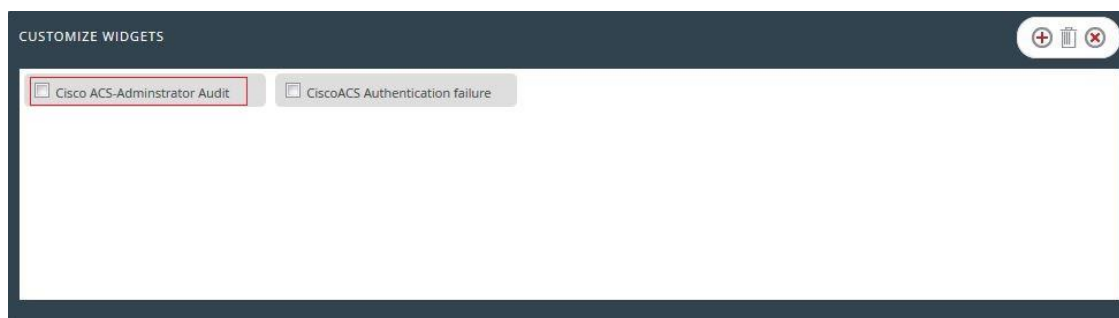




Figure 28

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.

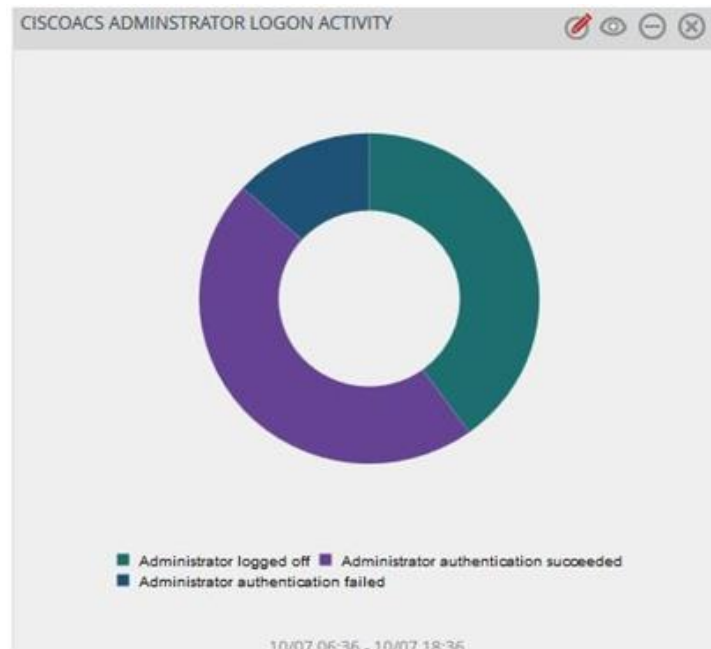


Figure 29

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	Authenticati on 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	Authenticati on 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	Authenticati on failed
10/06/2015 04:08:40 PM	10.60.1.223	1077	michel	Radius	10.60.1.240	129	Authenticati on 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	Authenticati on 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	Authenticati on 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 02:19:36 PM	10.60.1.240	trav	Internal Users	Radius	10.60.1.240	129		

Figure 32