EventTracker
Secure. Comply. Succeed.

Integrating Cisco Catalyst

EventTracker v7.x

EventTracker
8815 Centre Park Drive
Columbia MD 21045
www.eventtracker.com

Publication Date: Sep 4, 2014

About this Guide

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

Scope

The configurations detailed in this guide are consistent with **EventTracker Enterprise** version 7.X and later, and Cisco Catalyst 4000 Series Switch and later, CatOS 7.1 and later.

Audience

Cisco Catalyst users, who wish to forward syslog events to EventTracker manager.

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

This document is for informational purposes only. Prism Microsystems 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 Prism, as long as its content is unaltered, nothing is added to the content and credit to Prism is provided.

Prism Microsystems 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 Prism Microsystems, 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.

Contents

Overview

Catalyst is the brand name for a variety of network switches sold by Cisco Systems. While commonly associated with Ethernet switches, a number of different interfaces have been available throughout the history of the brand. The industry-leading Cisco Switch appliances support high-speed connectivity, applications, and communications systems for customers worldwide.

Cisco Catalyst can be configured to send to Event Tracker manager, alerts and reports can be configured into EventTracker.

Pre-requisite

Prior to configuring Cisco Catalyst and the EventTracker Enterprise, ensure that you meet the following prerequisites:

- EventTracker v7.x should be installed.
- Cisco Catalyst should be installed and proper access permissions to make configuration changes.
- Administrative access on the EventTracker Enterprise.

Integration of EventTracker with Cisco Catalyst

To configure Cisco Catalyst to forward the log to EventTracker Enterprise:

1. Log in to your Cisco CatOS user interface.
2. Type the following command to access privileged EXEC mode:

   Enable

3. Configure the system to timestamp messages:

   set logging timestamp enable

4. Type the IP address of EventTracker Enterprise:

   set logging server <IP address>

5. Limit messages that are logged by selecting a severity level:

   set logging server severity <server severity level>

6. Configure the facility level that should be used in the message. The default is **local7**.

   set logging server facility <server facility parameter>

7. Enable the switch to send syslog messages to the EventTracker Enterprise.

   set logging server enable

   Events forwarded to EventTracker by Cisco Catalyst are displayed on the Log Search tab of EventTracker Enterprise.

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 v7 to support Cisco Catalyst monitoring.

Categories

- **Cisco Catalyst: Access control list -** This category based report provides information related to access control list.
- **Cisco Catalyst: Access control list error -** This category based report provides information related to access control list error.
- **Cisco Catalyst: Accounting messages -** This category based report provides information related to accounting messages.
- **Cisco Catalyst: Authentication failed -** This category based report provides information related to authentication failed.
- **Cisco Catalyst: Call home protocol error -** This category based report provides information related to call home protocol error.
- **Cisco Catalyst: Cisco discovery protocol -** This category based report provides information related to cisco discovery protocol.
- **Cisco Catalyst: Common open policy service error -** This category based report provides information related to common open policy service error.
- **Cisco Catalyst: DHCP snooping -** This category based report provides information related to DHCP snooping.
- **Cisco Catalyst: Dual ring protocol -** This category based report provides information related to dual ring protocol.
- **Cisco Catalyst: Dynamic trunking protocol -** This category based report provides information related to dynamic trunking protocol.
- **Cisco Catalyst: Dynamic VLAN -** This category based report provides information related to dynamic VLAN.

- **Cisco Catalyst: Enhanced address recognition logic -** This category based report provides information related to enhanced address recognition logic.

- **Cisco Catalyst: Ethernet connectivity error -** This category based report provides information related to ethernet connectivity error.

- **Cisco Catalyst: Flash file system -** This category based report provides information related to flash file system.

- **Cisco Catalyst: Generic layer protocol -** This category based report provides information related to generic layer protocol.

- **Cisco Catalyst: GVRP -** This category based report provides information related to GVRP.

- **Cisco Catalyst: High availability -** This category based report provides information related to high availability.

- **Cisco Catalyst: Internal software error -** This category based report provides information related to internal software error.

- **Cisco Catalyst: Kernel error -** This category based report provides information related to kernel error.

- **Cisco Catalyst: Loop error -** This category based report provides information related to loop error.

- **Cisco Catalyst: Multicast messages -** This category based report provides information related to multicast messages.

- **Cisco Catalyst: Multilayer switching -** This category based report provides information related multilayer switching.

- **Cisco Catalyst: Networks management-** This category based report provides information related to networks management.

- **Cisco Catalyst: Radius server error -** This category based report provides information related to radius server error.

- **Cisco Catalyst: Resource reservation error -** This category based report provides information related to resource reservation error.

- **Cisco Catalyst: SNMP error -** This category based report provides information related to SNMP error.

- **Cisco Catalyst: Spantree protocol error -** This category based report provides information related to spantree protocol error.

- **Cisco Catalyst: System configuration-** This category based report provides information related to system configuration.
- **Cisco Catalyst: System resources error -** This category based report provides information related to system resources error.
- **Cisco Catalyst: VLAN error -** This category based report provides information related to VLAN error.
- **Cisco Catalyst: VLAN membership policy-** This category based report provides information related to VLAN membership policy.

Alerts

- **Cisco Catalyst: Chassis fan failed -** This alert is generated when chassis fan failed occurs.
- **Cisco Catalyst: Excessive number of links down/up -** This alert is generated when excessive number of links down/up occurs.
- **Cisco Catalyst: Linecard system exception -** This alert is generated when command linecard system exception occurs.
- **Cisco Catalyst: Memory allocation failed -** This alert is generated when memory allocation failed.
- **Cisco Catalyst: Module failed to come online -** This alert is generated when module failed to come online.
- **Cisco Catalyst: Module inserted -** This alert is generated when module inserted.
- **Cisco Catalyst: Module powerup failed -** This alert is generated when module powerup failed.
- **Cisco Catalyst: Module removed -** This alert is generated when module removed.
- **Cisco Catalyst: Module self test failed-** This alert is generated when module self test failed.
- **Cisco Catalyst: Module was reset-** This alert is generated when error module was reset.
- **Cisco Catalyst: Operational port in port channel changed -** This alert is generated when operational port in port channel changed.
- **Cisco Catalyst: Port shutdown due to security violation -** This alert is generated when port shutdown due to security violation occurs.

- **Cisco Catalyst: Port channel interface down -** This alert is generated when port channel interface down occurs.
- **Cisco Catalyst: Power supply failed -** This alert is generated when power supply failed.
- **Cisco Catalyst: Power supply fan failed -** This alert is generated when power supply fan failed.
- **Cisco Catalyst: Runtime diagnostics warning -** This alert is generated when runtime diagnostics warning occurs.
- **Cisco Catalyst: Security violation occurred -** This alert is generated when security violation occurred occurs.
- **Cisco Catalyst: Slot powered off -** This alert is generated when slot powered off event occurs.

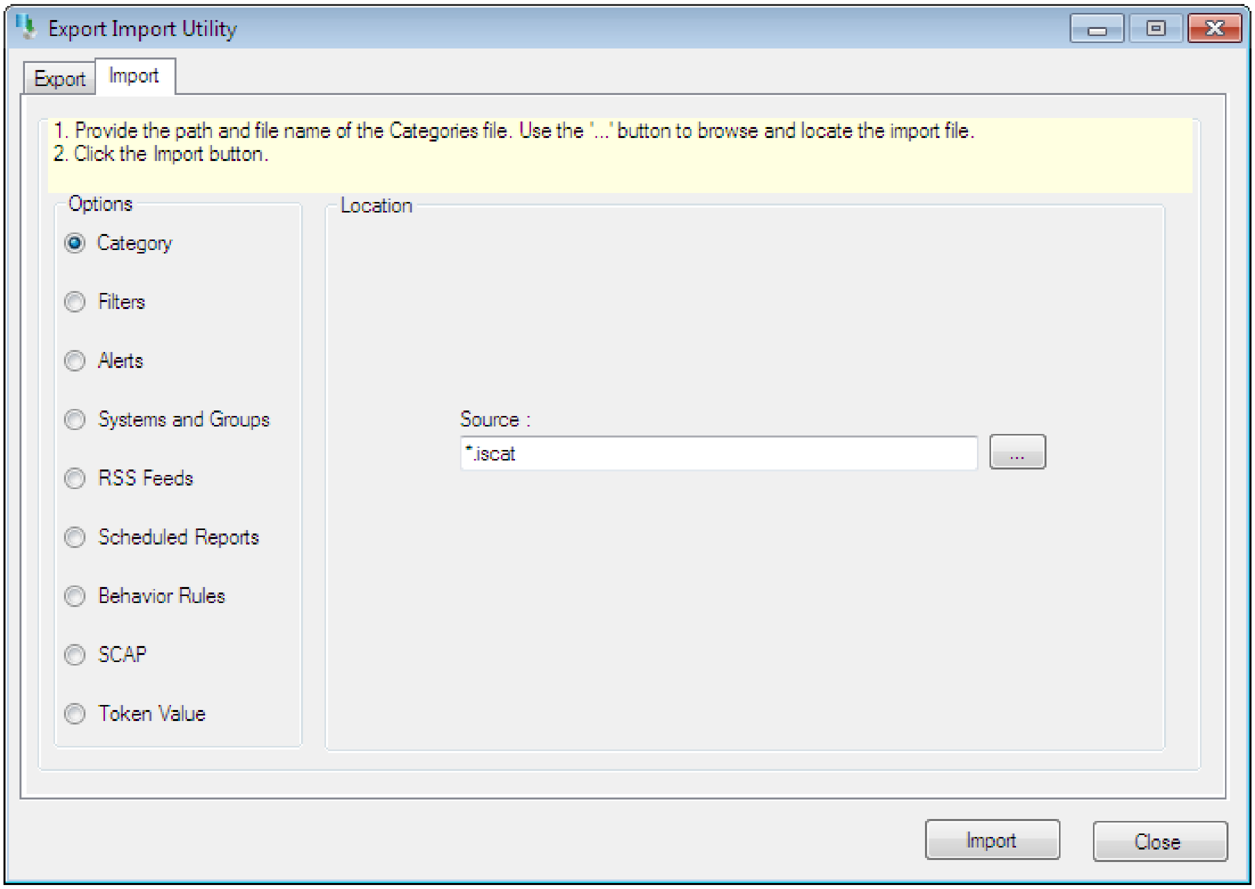
Import Cisco Catalyst Knowledge pack into EventTracker

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

   Import **Category/Alert** as given below.

To import Category

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



1. Provide the path and file name of the Categories file. Use the '...' button to browse and locate the import file.
2. Click the Import button.

● Category
○ Filters
○ Alerts
○ Systems and Groups
○ RSS Feeds
○ Scheduled Reports
○ Behavior Rules
○ SCAP
○ Token Value

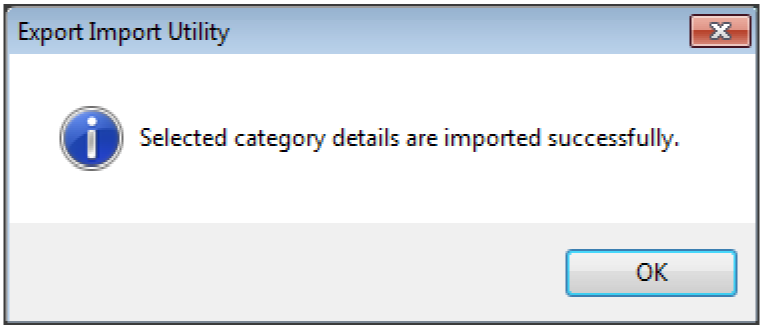
Source : *.iscat

Figure 1

2. Locate the **All Cisco Catalyst group of Categories.iscat** file, and then click the **Open** button.

3. Click the **Import** button to import the categories.

   EventTracker displays success message.



Export Import Utility

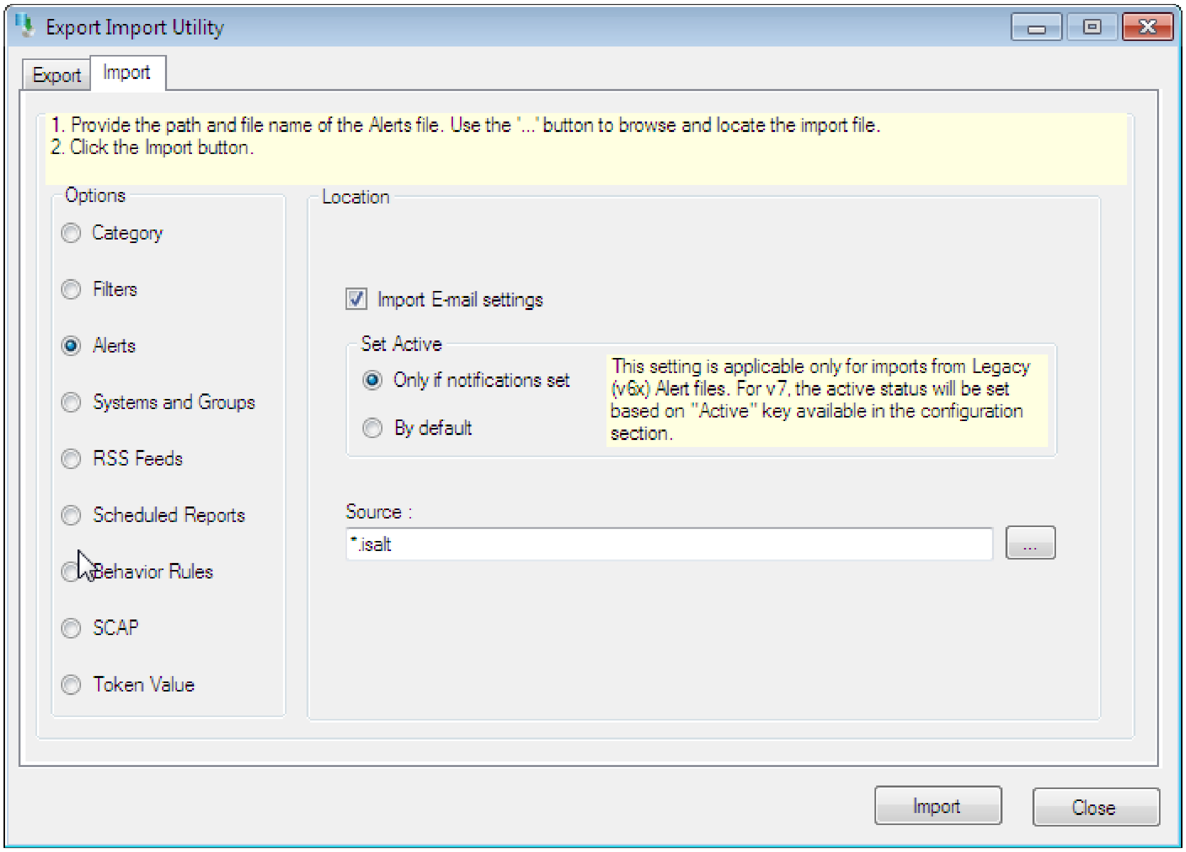
Selected category details are imported successfully.

Figure 2

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

To import Alerts

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



1. Provide the path and file name of the Alerts file. Use the '...' button to browse and locate the import file.
2. Click the Import button.

Options

○ Category
○ Filters
● Alerts
○ Systems and Groups
○ RSS Feeds
○ Scheduled Reports
○ Behavior Rules
○ SCAP
○ Token Value

Location

☑ Import E-mail settings

Set Active

● Only if notifications set
○ By default

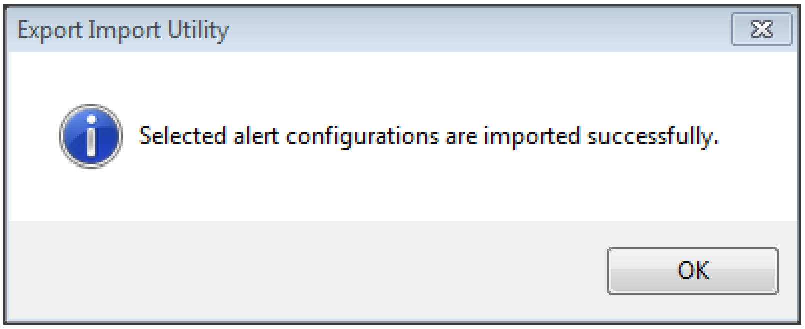
This setting is applicable only for imports from Legacy (v6x) Alert files. For v7, the active status will be set based on "Active" key available in the configuration section.

Source : *.isalt

Figure 3

2. Locate the **All Cisco Catalyst group of Alerts.isalt** file, and then click the **Open** button.
3. Click the **Import** button to import the alerts.

   EventTracker displays success message.



Selected alert configurations are imported successfully.

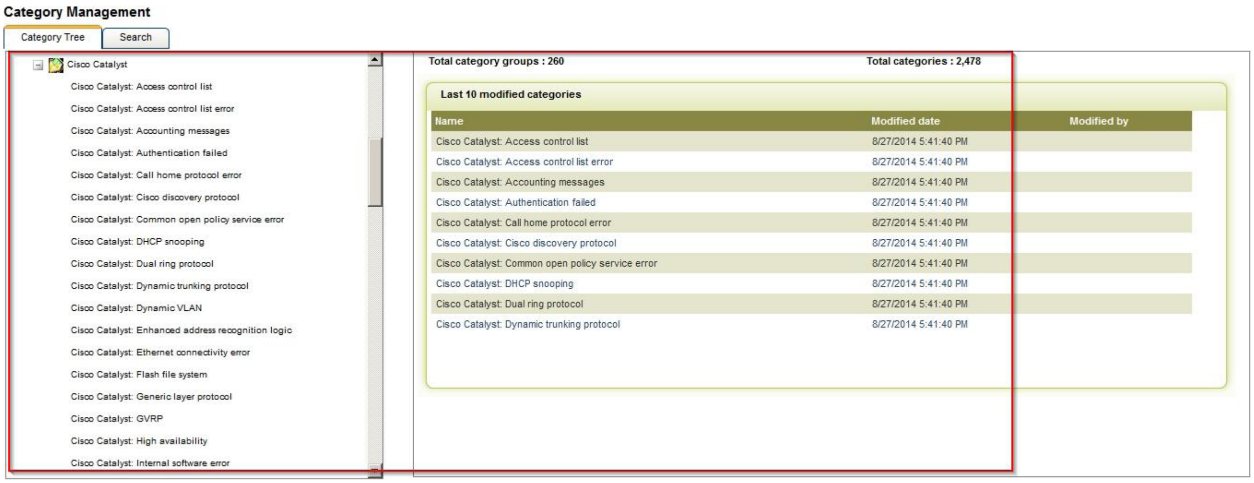
Figure 4

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

Verify Cisco Catalyst knowledge pack in EventTracker

Verify Cisco Catalyst Categories

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



Category Management

Cisco Catalyst
- Cisco Catalyst: Access control list
- Cisco Catalyst: Access control list error
- Cisco Catalyst: Accounting messages
- Cisco Catalyst: Authentication failed
- Cisco Catalyst: Call home protocol error
- Cisco Catalyst: Cisco discovery protocol
- Cisco Catalyst: Common open policy service error
- Cisco Catalyst: DHCP snooping
- Cisco Catalyst: Dual ring protocol
- Cisco Catalyst: Dynamic trunking protocol
- Cisco Catalyst: Dynamic VLAN
- Cisco Catalyst: Enhanced address recognition logic
- Cisco Catalyst: Ethernet connectivity error
- Cisco Catalyst: Flash file system
- Cisco Catalyst: Generic layer protocol
- Cisco Catalyst: GVRP
- Cisco Catalyst: High availability
- Cisco Catalyst: Internal software error

Total category groups : 260

Total categories : 2,478

Last 10 modified categories

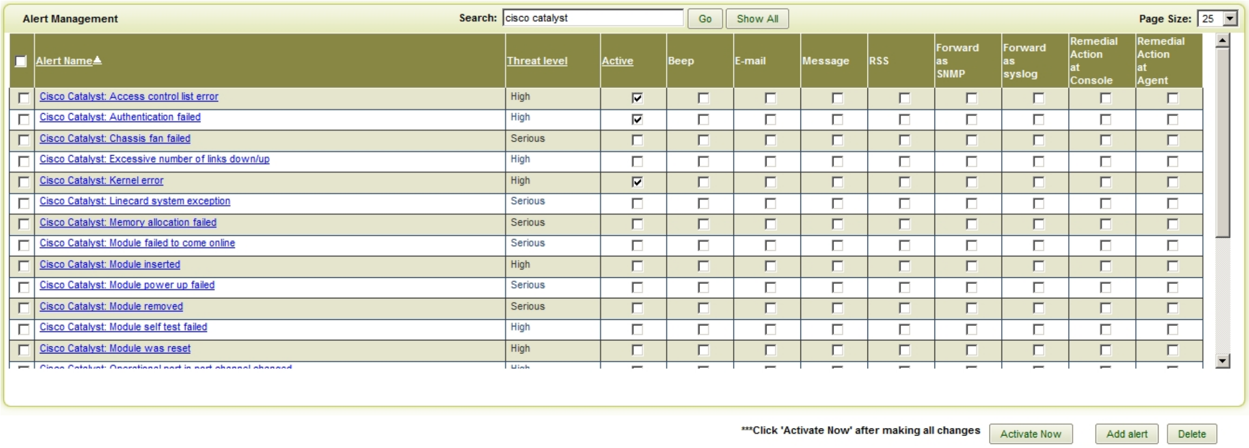
Name	Modified date	Modified by
Cisco Catalyst: Access control list	8/27/2014 5:41:40 PM	
Cisco Catalyst: Access control list error	8/27/2014 5:41:40 PM	
Cisco Catalyst: Accounting messages	8/27/2014 5:41:40 PM	
Cisco Catalyst: Authentication failed	8/27/2014 5:41:40 PM	
Cisco Catalyst: Call home protocol error	8/27/2014 5:41:40 PM	
Cisco Catalyst: Cisco discovery protocol	8/27/2014 5:41:40 PM	
Cisco Catalyst: Common open policy service error	8/27/2014 5:41:40 PM	
Cisco Catalyst: DHCP snooping	8/27/2014 5:41:40 PM	
Cisco Catalyst: Dual ring protocol	8/27/2014 5:41:40 PM	
Cisco Catalyst: Dynamic trunking protocol	8/27/2014 5:41:40 PM	

Figure 5

Verify Cisco Catalyst Alerts

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

   Alert Management page will display all the imported Cisco Catalyst device alerts.



Alert Management   Search: cisco catalyst   Page Size: 25

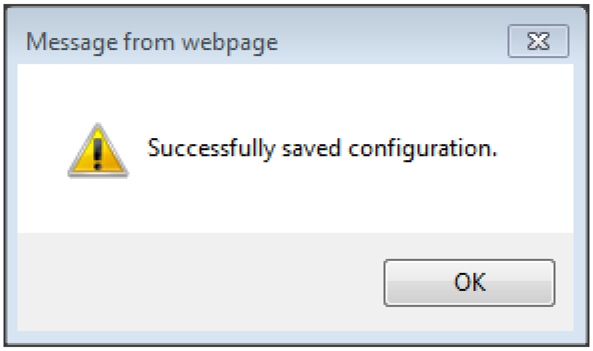
□	Alert Name▲	Threat level	Active	Beep	E-mail	Message	RSS	Forward as SNMP	Forward as syslog	Remedial Action at Console	Remedial Action at Agent
□	Cisco Catalyst: Access control list error	High	☑	□	□	□	□	□	□	□	□
□	Cisco Catalyst: Authentication failed	High	☑	□	□	□	□	□	□	□	□
□	Cisco Catalyst: Chassis fan failed	Serious	□	□	□	□	□	□	□	□	□
□	Cisco Catalyst: Excessive number of links down/up	High	□	□	□	□	□	□	□	□	□
□	Cisco Catalyst: Kernel error	High	☑	□	□	□	□	□	□	□	□
□	Cisco Catalyst: Linecard system exception	Serious	□	□	□	□	□	□	□	□	□
□	Cisco Catalyst: Memory allocation failed	Serious	□	□	□	□	□	□	□	□	□
□	Cisco Catalyst: Module failed to come online	Serious	□	□	□	□	□	□	□	□	□
□	Cisco Catalyst: Module inserted	High	□	□	□	□	□	□	□	□	□
□	Cisco Catalyst: Module power up failed	Serious	□	□	□	□	□	□	□	□	□
□	Cisco Catalyst: Module removed	Serious	□	□	□	□	□	□	□	□	□
□	Cisco Catalyst: Module self test failed	High	□	□	□	□	□	□	□	□	□
□	Cisco Catalyst: Module was reset	High	□	□	□	□	□	□	□	□	□
□	Cisco Catalyst: Operational port in port channel changed	High	□	□	□	□	□	□	□	□	□

***Click 'Activate Now' after making all changes

Figure 6

4. To activate the imported alerts, select the respective checkbox in the **Active** column.

   EventTracker displays message box.



Message from webpage

Successfully saved configuration.

Figure 7

5. Click the **OK** button, 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.