

Integrating Juniper NetScreen (ScreenOS)

Abstract

This guide provides instructions to configure **Juniper NetScreen (ScreenOS)** to send the syslog events to EventTracker.

Scope

The configurations detailed in this guide are consistent with **EventTracker** version 7.X and later, and **Juniper NetScreen (ScreenOS) 5.2.0** and later.

Audience

Administrators who are assigned the task to monitor and manage Juniper NetScreen events 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
- Overview..... 3
- Prerequisites..... 3
- Configuration..... 3
 - Configure Syslog logging..... 3
- EventTracker Knowledge Pack 4
 - Categories..... 4
 - Alerts 5
 - Reports 5
- Import Juniper NetScreen knowledge pack into EventTracker..... 7
 - Import Category 7
 - Import Alerts 8
 - Import Flex Reports..... 9
 - Import Template..... 10
- Verify Juniper NetScreen knowledge pack in EventTracker..... 13
 - Verify Juniper NetScreen Categories..... 13
 - Verify Juniper NetScreen Alerts 13
 - Verify Juniper NetScreen Reports 15
 - Verifying Template 16
 - Sample Reports 17

Overview

The Juniper Networks NetScreen Series Security Systems are ideally suited for large enterprise network backbones, including departmental or campus segmentation, Enterprise data centers for securing high-density server environments and carrier-based managed services or core infrastructure.

Prerequisites

- EventTracker 7.x and later should be installed.
- Juniper ScreenOS 5.2.x and later should be installed on Juniper NetScreen.
- Administrative access on the EventTracker Enterprise and Juniper NetScreen.
- An exception should be added into Windows Firewall on EventTracker machine for syslog port 514.
- Port 514 should be opened on Juniper NetScreen (ScreenOS).

Configuration

To monitor Juniper NetScreen in EventTracker, configure Juniper NetScreen to send all events as Syslog to the EventTracker system.

Configure Syslog logging

1. Login into **WebUI** of Juniper NetScreen.
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 Juniper NetScreen events are enabled and Juniper NetScreen events are received in EventTracker, the Categories, Alerts and Flex based Reports can be configured in EventTracker.

The following Knowledge Packs are available in EventTracker to support Juniper NetScreen monitoring.

Categories

- **NetScreen: Account management** - This category based report provides information related to account management.
- **NetScreen: Administration** - This category based report provides information related to administration.
- **NetScreen: All events** - This category based report provides information related to all events of NetScreen.
- **NetScreen: Antivirus** - This category based report provides information related to antivirus.
- **NetScreen: Firewall policy** - This category based report provides information related to firewall policy.
- **NetScreen: Firewall traffic allowed** - This category based report provides information related to firewall traffic allowed.
- **NetScreen: Firewall traffic denied** - This category based report provides information related to firewall traffic denied.
- **NetScreen: Intrusion detection** - This category based report provides information related to Intrusion detection.
- **NetScreen: Network services** - This category based report provides information related to network services.
- **NetScreen: Security device events** - This category based report provides information related to security device events.
- **NetScreen: System authentication** - This category based report provides information related to system authentication.
- **NetScreen: System services** - This category based report provides information related to system services.
- **NetScreen: URL allowed** - This category based report provides information related to URL allowed.
- **NetScreen: URL blocked** - This category based report provides information related to URL blocked.
- **NetScreen: User authentication** - This category based report provides information related to user authentication.

- **NetScreen: Virtual router** - This category based report provides information related to virtual router.
- **NetScreen: Virtual systems** - This category based report provides information related to virtual systems.
- **NetScreen: VPN** - This category based report provides information related to VPN.
- **NetScreen: Web filtering** - This category based report provides information related to Web filtering.

Alerts

- **NetScreen: Authentication failure** - This alert is generated when system or user related authentication fails.
- **NetScreen: IDS intrusion detection** - This alert is generated when attacks are detected through NetScreen.
- **NetScreen: Security device error** - This alert is generated when response to problems or processes that occur at the hardware or Screen OS level.
- **NetScreen: Spam found** - This alert is generated when spam found.
- **NetScreen: System configuration erased** - This alert is generated when system configuration gets erased.
- **NetScreen: USB storage device attached/detached** - This alert is generated when USB storage device is attached/detached.
- **Juniper NetScreen-IP address conflict** - This alert is generated when IP address conflict occurs.
- **Juniper NetScreen-VPN service down** - This alert is generated when VPN service is down.

Reports

- **Juniper NetScreen: User Logon Success Report:** This report provides information related to user logon success for different logon types like SSH, Console, Telnet etc.
- **Juniper NetScreen: User Logoff Report:** This report provides information related to user logoff from different terminals.
- **Juniper NetScreen: User Authentication Success Report:** This report provides information related to authentication success done for different users from different source addresses.
- **Juniper NetScreen: User Authentication Failed Report:** This report provides information related to authentication failure for different users with what reasons.
- **Juniper NetScreen: Intrusion Detection Report:** This report provides information related with source IP and ports, destination IP and ports (victim details) and intrusion occurs in NetScreen firewall.
- **Juniper NetScreen: Account Management Report:** This report provides information related with creation, deletion and modification of user, group and account of NetScreen and by whom it is done.

- **Juniper NetScreen: System Authentication Report:** This report provides information related with MAC address of systems authenticated with NetScreen firewall.
- **Juniper NetScreen: URL Allowed or Blocked Report:** This report provides information related with URL blocked and allowed with source IP of system trying to access it.
- **Juniper NetScreen: Firewall Policy Change Report:** This report provides information related with changes in firewall policy component and by whom it is done.
- **Juniper NetScreen: USB Storage Device Attached and Detached Report:** This report provides information related with attached and detached of USB devices with NetScreen.
- **Juniper NetScreen: Web Filtering Report:** This report provides information about the changes in category and profiles of web filtering in NetScreen and by whom.
- **Juniper NetScreen: Traffic allowed and blocked report:** This report provides information related with what kind of traffic are allowed and blocked in NetScreen firewall.
- **Juniper NetScreen: Administration:** This report provides information related with the configuration changes happen and by whom it is done in NetScreen firewall.
- **Juniper NetScreen-DHCP server operations** - This report provides information related to DHCP server operations which include IP address, MAC address, status and reason from fields.
- **Juniper NetScreen-VPN service status** - This report provides information related to VPN service status which includes VPN name, source address and status from fields.

Import Juniper NetScreen 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/Template as given below.

Import Category

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

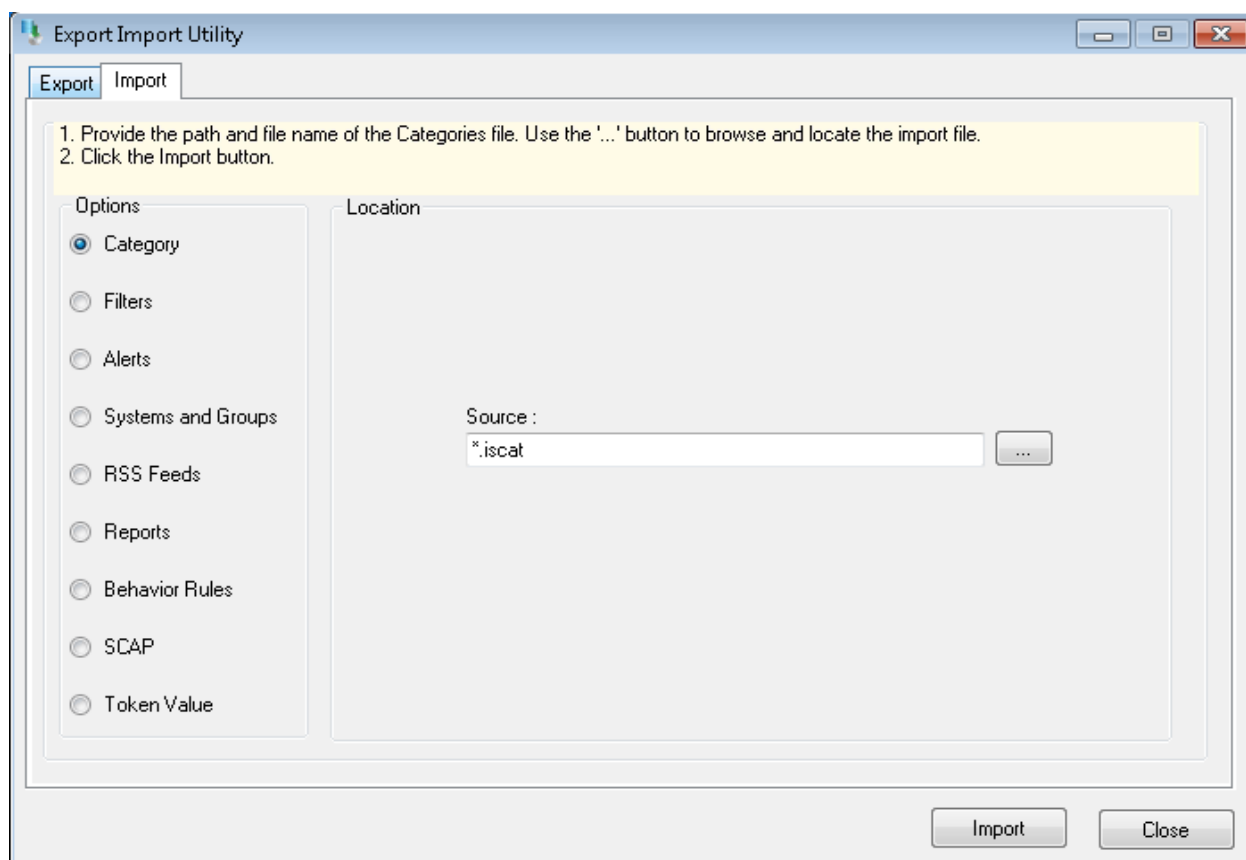


Figure 1

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

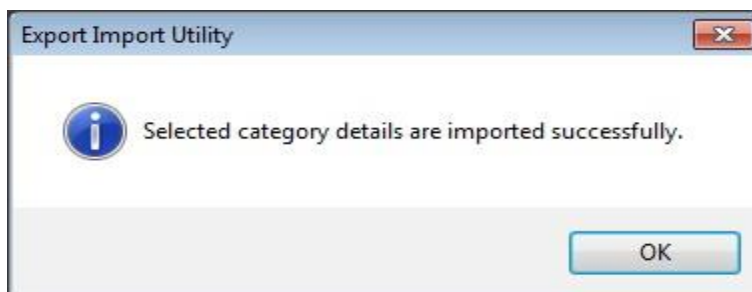



Figure 2

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

Import Alerts

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

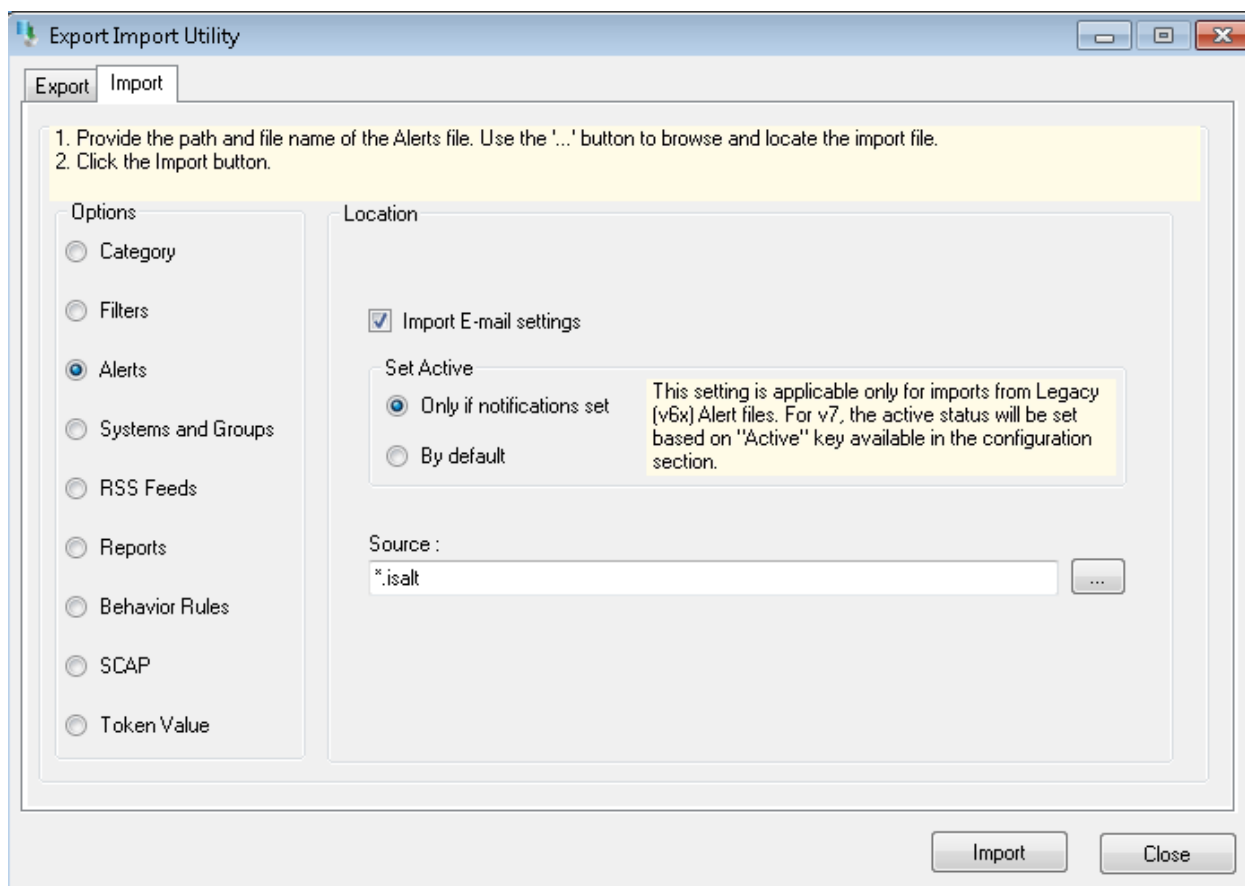


Figure 3

2. Locate **All Juniper NetScreen group of Alerts.isalt** file, and then click the **Open** button.
3. To import alerts, click the **Import** button.

EventTracker displays success message.

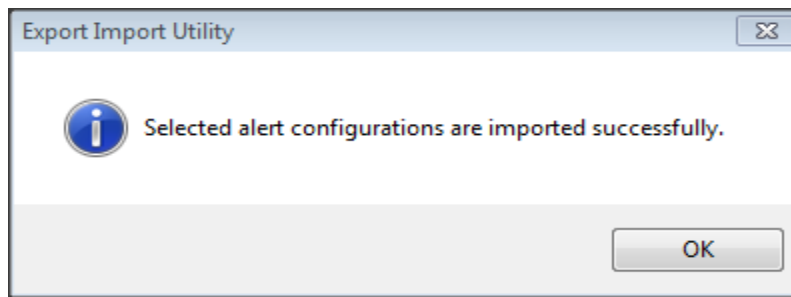



Figure 4

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

Import Flex Reports

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

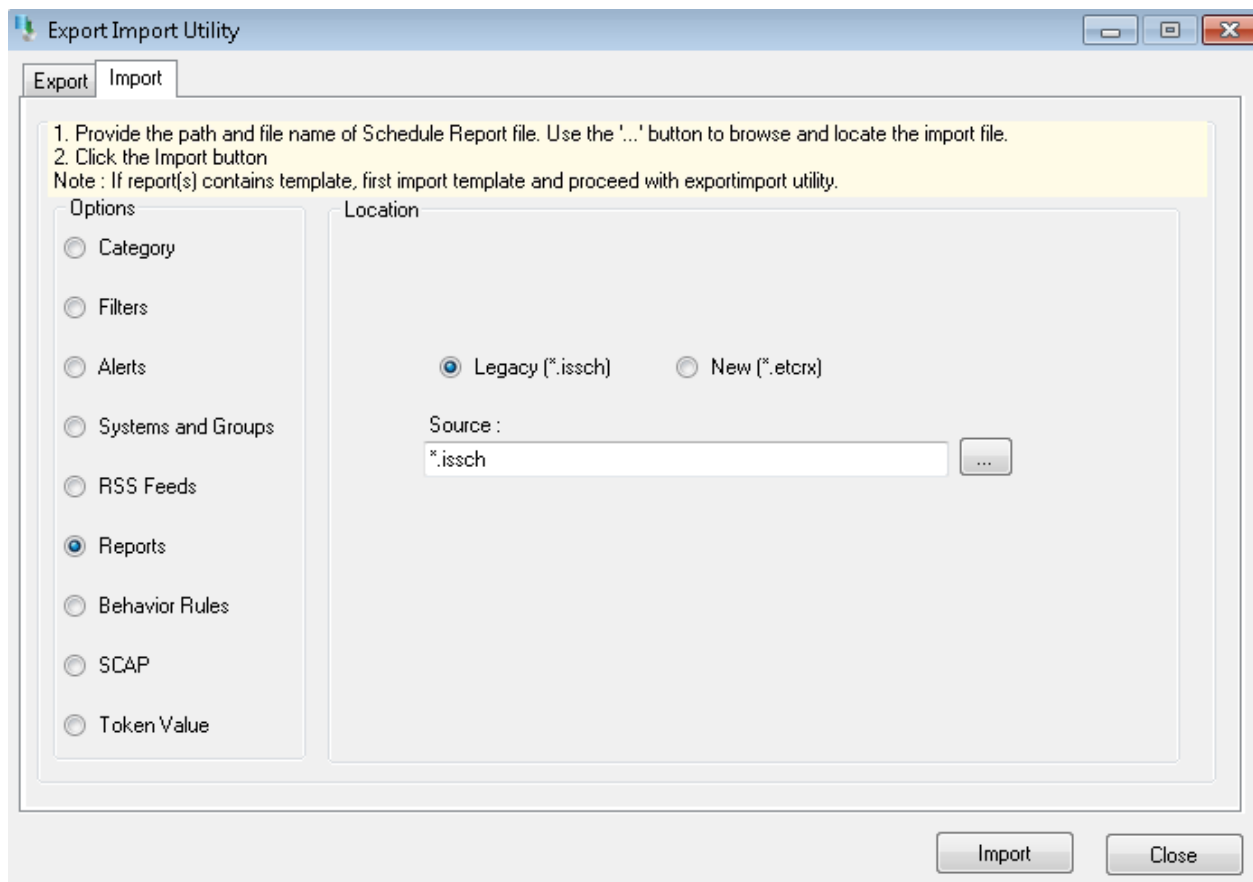


Figure 6

2. Locate **All Juniper NetScreen group of Report .issch** file, and then click the **Open** button.
3. To import flex report, click the **Import** button.
EventTracker displays success message

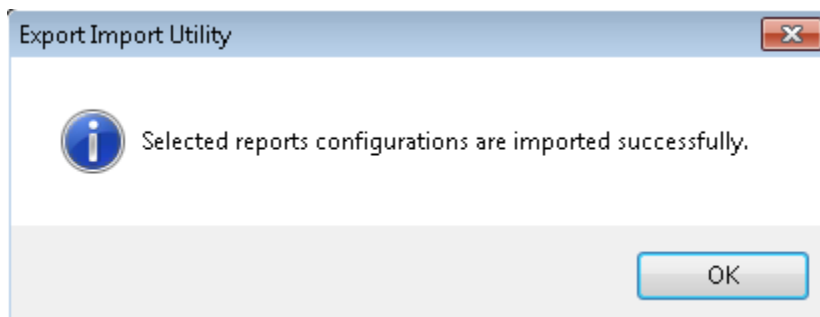


Figure 7

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

Import Template

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu and then click the **Parsing rule**.
3. Click the **Template** tab.
4. Click the **Import** button and it will open a new window.
(**Note:** Make sure pop-up is enabled for EventTracker)

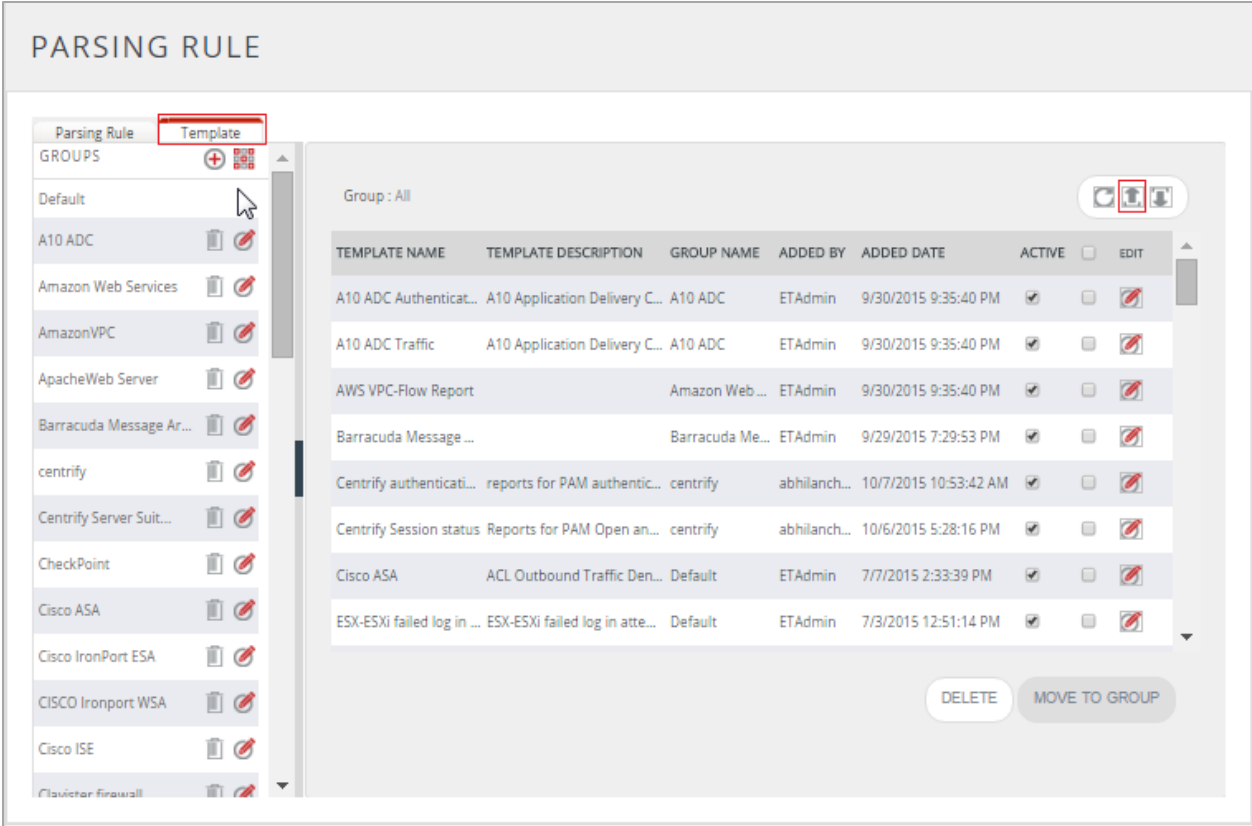


Figure 8

5. Locate and select the .ETTD file and then click the **Open** button.

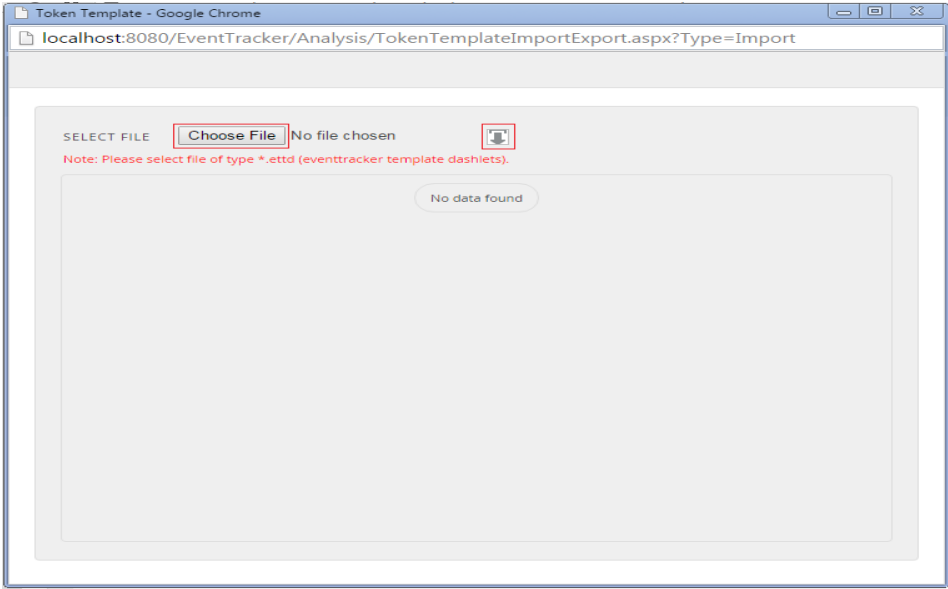


Figure 9

6. Select the template that you want to upload.

7. Click on the **Import configuration**  button.

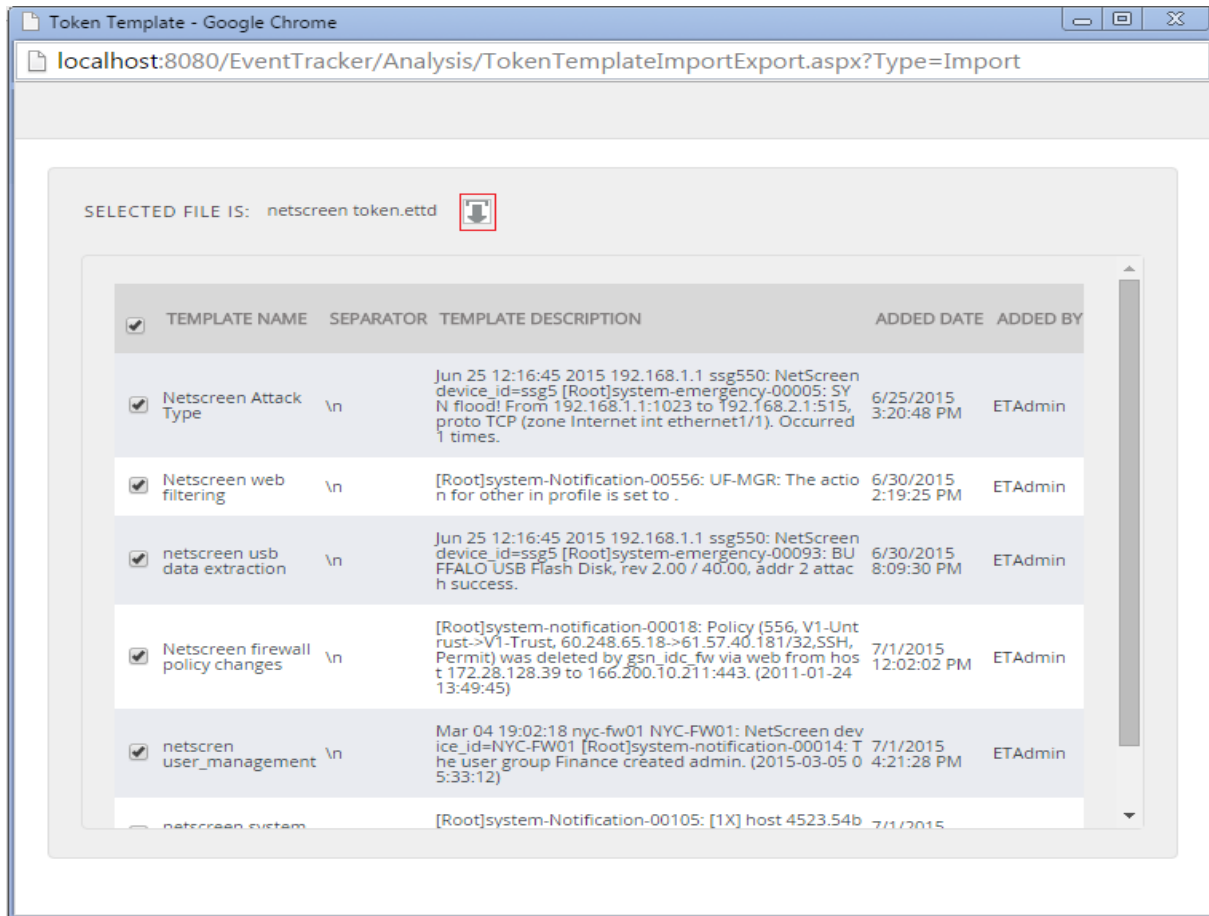


Figure 10

EventTracker displays success message.

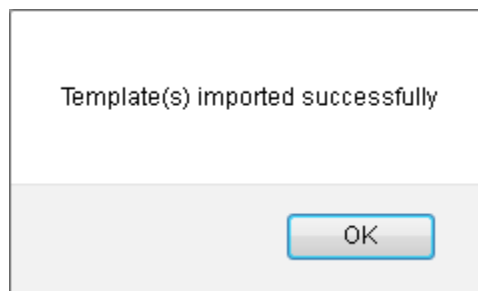


Figure 11

8. Click **OK** and it will automatically close the window.

Verify Juniper NetScreen knowledge pack in EventTracker

Verify Juniper NetScreen 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 **Juniper NetScreen** group folder to view the imported categories.

The screenshot displays the 'CATEGORY MANAGEMENT' interface. On the left, a 'Category Tree' is expanded to show the 'Netscreen' group, which contains various sub-categories such as 'Netscreen: Account management', 'Netscreen: Administration', 'Netscreen: All events', 'Netscreen: Antivirus', 'Netscreen: Firewall policy', 'Netscreen: Firewall traffic allowed', 'Netscreen: Firewall traffic denied', 'Netscreen: Intrusion detection', 'Netscreen: Network services', 'Netscreen: Security device events', 'Netscreen: System authentication', 'Netscreen: System services', 'Netscreen: URL allowed', 'Netscreen: URL blocked', 'Netscreen: User authentication', 'Netscreen: Virtual router', 'Netscreen: Virtual systems', 'Netscreen: VPN', and 'Netscreen: Web filtering'. On the right, a table titled 'Last 10 modified categories' provides details for the most recent updates.

NAME	MODIFIED DATE	MODIFIED BY
Netscreen: All events	7/15/2015 4:50:52 PM	gurmukhnishan
Netscreen: VPN	7/15/2015 4:50:34 PM	gurmukhnishan
Netscreen: Security device events	7/15/2015 4:49:57 PM	gurmukhnishan
Netscreen: URL allowed	7/15/2015 4:49:35 PM	gurmukhnishan
Netscreen: Web filtering	7/15/2015 4:49:13 PM	gurmukhnishan
Netscreen: Intrusion detection	7/15/2015 4:48:42 PM	gurmukhnishan
Netscreen: Firewall traffic denied	7/15/2015 4:48:12 PM	gurmukhnishan
Netscreen: Firewall traffic allowed	7/15/2015 4:47:53 PM	gurmukhnishan
Netscreen: Firewall policy	7/15/2015 4:47:36 PM	gurmukhnishan
Netscreen: Account management	7/15/2015 4:47:14 PM	gurmukhnishan

Figure 12

Verify Juniper NetScreen Alerts

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

ALERT MANAGEMENT netscreen

Click 'Activate Now' after making all changes 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"/>	Netscreen: Authentication failure	<input type="checkbox"/> 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"/>	Netscreen-25.Scr...
<input type="checkbox"/>	Netscreen: IDS intrusion detection	<input type="checkbox"/> 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"/>	Netscreen-25.Scr...
<input type="checkbox"/>	Netscreen: Security device error	<input type="checkbox"/> Critical	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Netscreen-25.Scr...
<input type="checkbox"/>	Netscreen: Spam found	<input type="checkbox"/> 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"/>	Netscreen-25.Scr...
<input type="checkbox"/>	Netscreen: System configuration era...	<input type="checkbox"/> Critical	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Netscreen-25.Scr...
<input type="checkbox"/>	Netscreen: USB storage device attach...	<input type="checkbox"/> 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"/>	Netscreen-25.Scr...

Figure 13

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

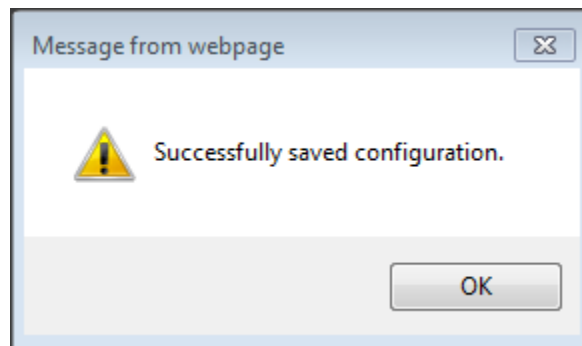


Figure 14

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

NOTE: You can select alert notifications 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 Juniper NetScreen Reports

1. Logon to **EventTracker Enterprise**.
2. Click the **Report Option** and select **Defined**.
3. In Report Group Tree, to view imported reports, scroll down and expand Juniper NetScreen report group folder for the imported reports.

The screenshot displays the 'REPORTS CONFIGURATION' interface. At the top, there are radio buttons for 'Scheduled', 'Queued', and 'Defined', with 'Defined' selected. A search bar is located to the right. On the left, a 'REPORT GROUPS' tree lists various system categories, with 'Juniper Netscreen' highlighted. The main area, titled 'REPORTS CONFIGURATION >> JUNIPER NETSCREEN', contains a table of reports. A red box highlights this table, which includes columns for report name, start time, end time, and action icons (info, refresh, delete, add).

Report Name	Start Time	End Time	Actions
Juniper NetScreen-Account management	7/9/2015 10:10:31 AM	7/9/2015 10:10:31 AM	Info, Refresh, Delete, Add
Juniper NetScreen-Administration	7/2/2015 2:26:49 PM	7/2/2015 2:26:49 PM	Info, Refresh, Delete, Add
Juniper NetScreen-Intrusion detection system	7/1/2015 7:20:09 PM	7/2/2015 3:26:40 PM	Info, Refresh, Delete, Add
Juniper NetScreen-System authentication	7/1/2015 5:56:45 PM	7/9/2015 12:08:33 PM	Info, Refresh, Delete, Add
Juniper NetScreen- Firewall policy change	7/1/2015 5:03:34 PM	7/1/2015 8:07:07 PM	Info, Refresh, Delete, Add
Juniper NetScreen-USB storage device attached or detached	6/30/2015 8:03:02 PM	7/1/2015 8:09:45 PM	Info, Refresh, Delete, Add
Juniper NetScreen-URL allowed or blocked	6/30/2015 6:51:04 PM	7/3/2015 4:23:57 PM	Info, Refresh, Delete, Add

Figure 15

Verifying Template

1. Logon to **EventTracker Enterprise** and go to **Parsing rule**.
2. Click on **Template** tab.
3. Check the template you have uploaded.

The screenshot shows the 'PARSING RULE' configuration page in EventTracker Enterprise. The 'Template' tab is selected, and the 'Juniper Netscreen' template is highlighted in the left sidebar. The main area displays a table of templates for the 'Juniper Netscreen' group.

TEMPLATE NAME	TEMPLATE DESCRIPTION	ADDED BY	ADDED DATE	ACTIVE		EDIT
Juniper NetScreen- Fire...		ETAdmin	9/29/2015 8:19:51 PM	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Juniper NetScreen-Acc...		ETAdmin	9/29/2015 8:19:51 PM	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Juniper Netscreen-Ad...		ETAdmin	9/29/2015 8:19:51 PM	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Juniper Netscreen-Logi...		ETAdmin	9/29/2015 8:19:51 PM	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Juniper NetScreen-Syst...		ETAdmin	9/29/2015 8:19:51 PM	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Juniper NetScreen-USB...		ETAdmin	9/29/2015 8:19:51 PM	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Juniper NetScreen-We...		ETAdmin	9/29/2015 8:19:51 PM	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

Buttons at the bottom right: DELETE, MOVE TO GROUP

Figure 16

Sample Reports

1. Juniper NetScreen: Account Management Report

Juniper NetScreen: Account Management Report				
User Selection :				
From Date:6/30/2015 4:23:25 PM				
To Date: 7/1/2015 4:23:25 PM				
Limit Time Range: None				
Refine: None				
Filter: None				
Categories Selected: Netscreen: Account management				
Computers Selected: NETSCREEN				
Description: None				
Detail:				
LogTime	Computer	User or Group	Changes	By Whom
07/01/2015 04:21:37 PM	NETSCREEN	user john	enabled	admin
07/01/2015 04:21:37 PM	NETSCREEN	user john	enabled	admin
07/01/2015 04:21:37 PM	NETSCREEN	group Marketing	modified	admin
07/01/2015 04:21:37 PM	NETSCREEN	group HR	deleted	admin
07/01/2015 04:21:37 PM	NETSCREEN	group Finance	created	admin
07/01/2015 04:21:37 PM	NETSCREEN	user john	enabled	admin

Figure 17

2. Juniper NetScreen: Intrusion Detection Report

Juniper NetScreen: Intrusion Detection Report

User Selection :
From Date: 6/30/2015 7:20:14 PM
To Date: 7/1/2015 7:20:14 PM
Limit Time Range: None
Refine: None
Filter: None
Categories Selected: Netscreen: Intrusion detection
Computers Selected: NETSCREEN
Description: None

Detail:

LogTime	Computer	Source IP and Port	Destination IP and Port	Attack Type
07/01/2015 07:12:23 PM	NETSCREEN	192.168.1.1	192.168.2.1	ActiveX control blocked
07/01/2015 07:12:23 PM	NETSCREEN	192.168.1.1	224.0.0.22	IP spoofing
07/01/2015 07:12:23 PM	NETSCREEN	192.168.1.1:35634	192.168.2.1:1514	UDP flood
07/01/2015 07:12:23 PM	NETSCREEN	192.168.1.1	192.168.2.1	Java applet blocked
07/01/2015 07:12:23 PM	NETSCREEN	192.168.1.1	192.168.2.1	Java applet blocked

Figure 18