

Integrate Juniper SBR

EventTracker v7.x

Publication Date: Aug 11, 2014

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

Abstract

Steel-Belted Radius Server Enterprise Edition centrally manages and secures network access, enforcing uniform access rights over virtually any combination of network environments. This radius server provides reliable uptime, flexibility, and powerful user management make it extremely dependable and adaptive.

EventTracker provides instant security alerts and a real-time dashboard for viewing every incident in the infrastructure, with an optional automatic remediation function that can be set to perform any action required. Once syslog is been configured to send logs to Event Tracker Manager, alerts, dashboard and reports can be configured in EventTracker.

Scope

The configurations detailed are consistent with EventTracker Enterprise version 7.X and later, and Juniper SBR 6.1 and later.

Audience

Juniper SBR users, who wish to forward syslog events to EventTracker Manager and monitor events using Event Tracker Enterprise.

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. © 2014 Prism Microsystems Corporation. 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
Juniper SBR	3
Prerequisites.....	3
Configure Juniper SBR to send syslog to EventTracker	3
Procedure 1	4
Procedure 2.....	4
Import Juniper SBR knowledge pack in EventTracker.....	6
Import Category.....	6
Import Alerts.....	7
Verify Juniper SBR knowledge pack in EventTracker	8
Verify categories.....	8
Verify alerts.....	8
EventTracker Knowledge Pack.....	10
Categories	10
Alerts	11

Juniper SBR

SBR Appliance is a stand-alone RADIUS server combining the power and flexibility of SBR Enterprise Series servers with the convenience of a dedicated device that integrates easily into any network closet.

Prerequisites

- EventTracker v7.x and later should be installed
- Juniper SBR 6.1 and later should be installed.

Configure Juniper SBR to send syslog to EventTracker

Syslog is a standard for forwarding log messages in an IP network. Syslog captures log information provided by network devices. Compatible applications (such as rsyslog) can be used to forward these system log messages to a remote server or database.

Parameter	Function
Enable	<p>Enables authentication request information to be written to the system log file.</p> <p>If set to 1, this setting enables writing of authentication requests to the system log file. If set to 0, this setting disables writing of authentication requests to the system log file.</p> <p>The default value is 0.</p> <p>Note: This setting is independent of the Enable setting in the [Configure] section of the authentication log.</p>
Facility	<p>This parameter sets the system log facility.</p> <p>The default value is Daemon, but could be set to Local[X], where X = 0–7.</p>

Parameter	Function
Severity	This parameter sets the severity of the system log message. The value could be Info or Notice. The default value is Info.

Procedure 1

To write all authlog messages to `/var/adm/messages` using the LOCAL3 facility and LOG_INFO severity:

1. Configure the **authlog.ini** file as:

```
[Syslog]
```

```
Enable = 1
```

```
Facility = local3
```

```
Severity = Info
```

2. Add the following statement in the `/etc/syslog.conf` file:

```
*.err;kern.debug;daemon.notice;mail.crit;local3.info /var/adm/messages
```

3. Run the following command:

```
kill -HUP `pgrep syslogd`
```

4. Restart the **sbrd** process.

```
./sbrd restart
```

5. Authlog messages are written to the system log (`/var/adm/messages`).

Procedure 2

To write all authlog messages to a remote server (Linux configuration example):

1. Configure the **authlog.ini** file in the local server as:

[Syslog]

Enable = 1

Facility = daemon

Severity = Info

2. Restart the **sbrd** process.

./sbrd restart

3. Update the **/etc/rsyslog.conf** file in the local server as:

***.* @@192.168.1.1:514**

NOTE: Here, **192.168.1.1:514** is a remote SBR server.

4. Restart the rsyslog service.

Service rsyslog restart

5. Update the **/etc/rsyslog.conf** file in the remote server as:

Provides TCP system log reception

\$ModLoad imtcp.so

\$InputTCPServerRun 514

***.info;mail.none;authpriv.none;cron.none /var/log/messages**

6. Restart the **rsyslog** service.

Service rsyslog restart

7. Authlog messages are written to the remote server's system log (**/var/log/messages**).

Import Juniper SBR knowledge pack in EventTracker

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

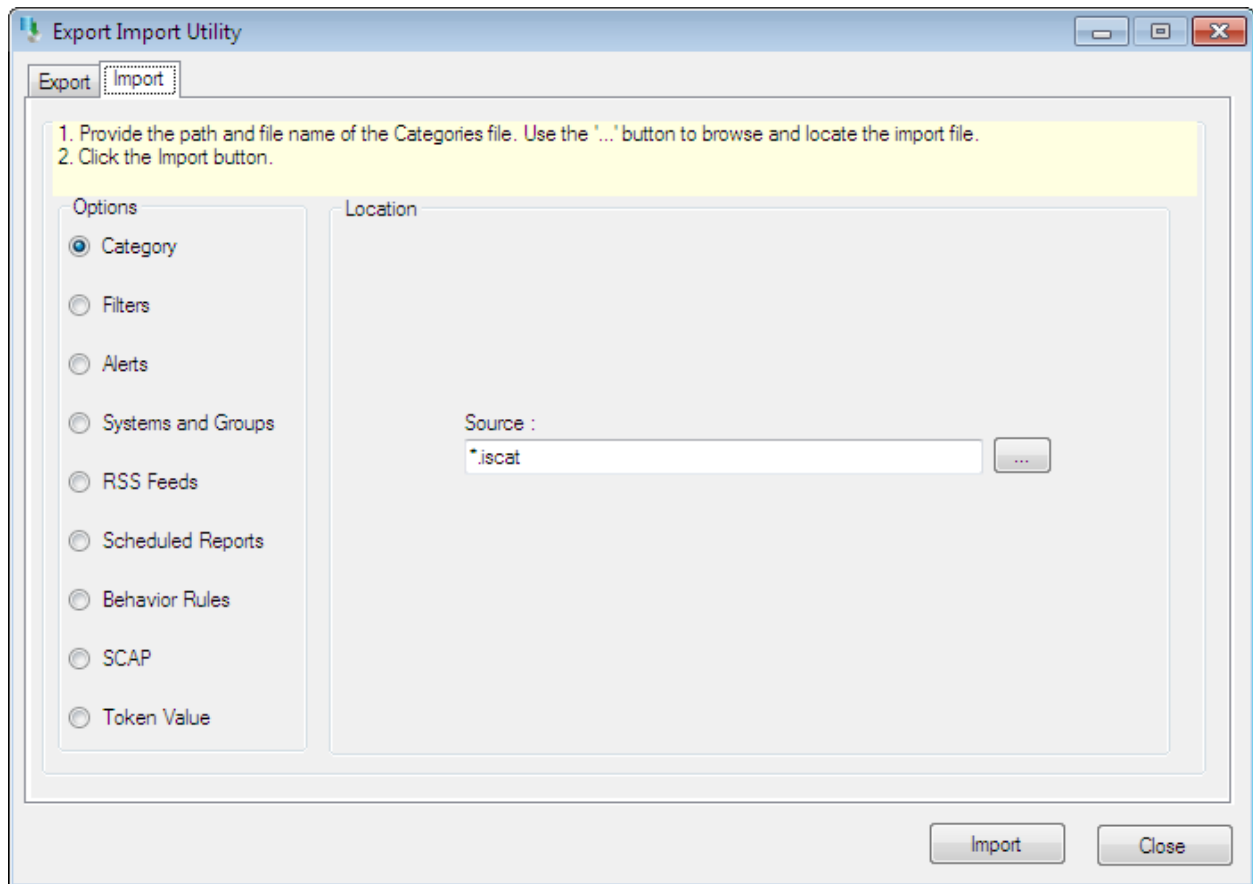



Figure 1

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

Import Category

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

2. Locate **Juniper SBR.iscat** file, and then click the **Open** button.
3. To import categories, click the **Import** button.

EventTracker displays success message.

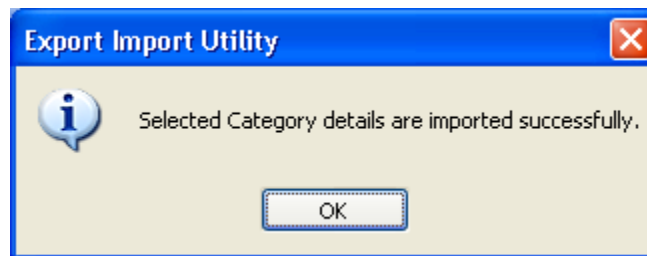



Figure 2

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

Import Alerts

1. Click **Alert** option, and then click the **browse**  button.
2. Locate **Juniper SBR.isalt** file, and then click the **Open** button.
3. To import alerts, click the **Import** button.

EventTracker displays success message.

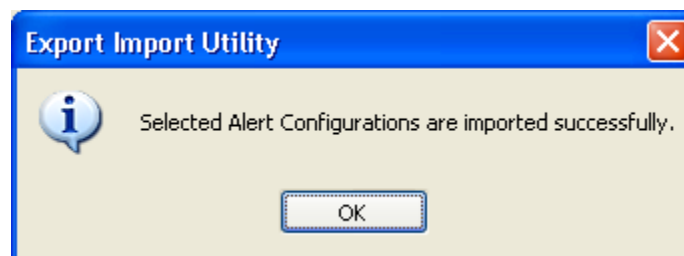


Figure 3

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

Verify Juniper SBR knowledge pack in EventTracker

Verify categories

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Categories**.
3. To view the imported categories, in the **Category Tree**, expand **Juniper SBR** group folder.

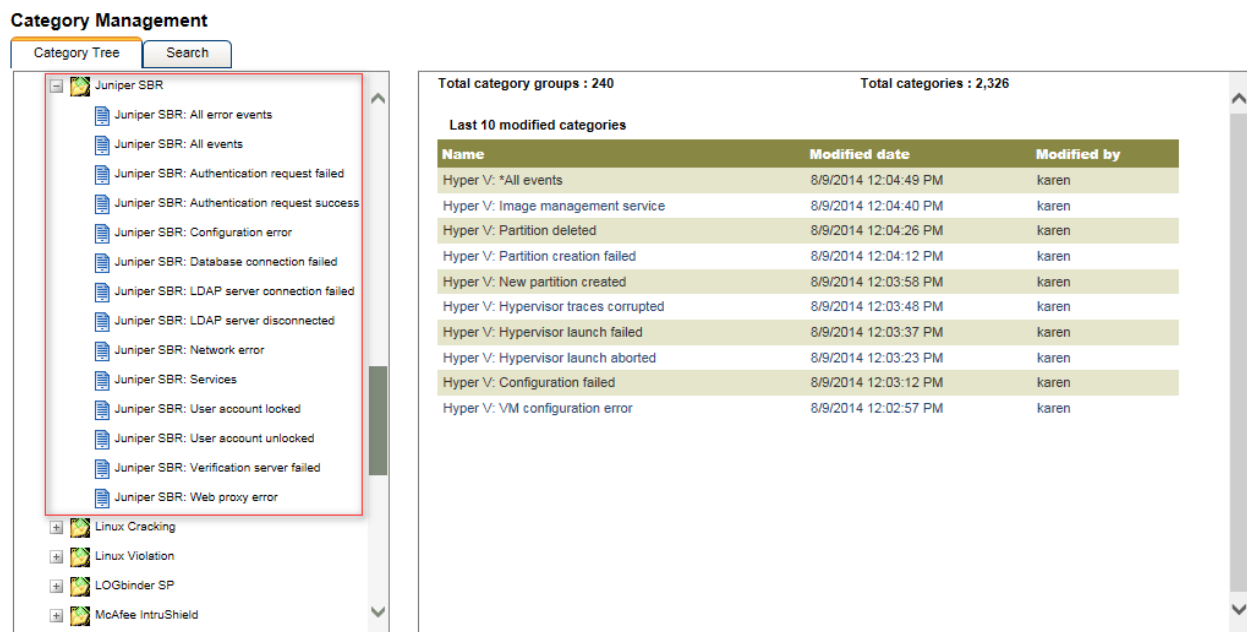


Figure 4

Verify alerts

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

Alert Management page will display all the imported alerts.

Alert Management Search: Juniper SBR Go Show All 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
Juniper SBR: Authentication request failed	Medium	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Juniper SBR: LDAP server connection failed	Serious	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Juniper SBR: Services	Serious	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Juniper SBR: User account locked	High	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

Activate Now Add alert Delete

Figure 5

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

EventTracker displays message box.

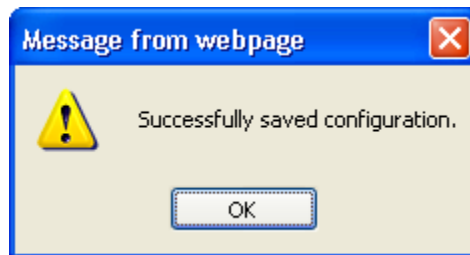


Figure 6

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

EventTracker Knowledge Pack

Categories

EventTracker can alert on critical events such as virus detection, login failures etc.

- **Juniper SBR Authentication request failed:** This category based report provides information related to authentication request failed.
- **Juniper SBR Authentication request success:** This category based report provides information related to authentication request success.
- **Juniper SBR Configuration error:** This category based report provides information related to configuration error.
- **Juniper SBR Database connection failed:** This category based report provides information related to database connection failed.
- **Juniper SBR LDAP server connection failed:** This category based report provides information related to LDAP server connection failed.
- **Juniper SBR LDAP server disconnected:** This category based report provides information related to LDAP server disconnected.
- **Juniper SBR Network error:** This category based report provides information related to network connection failed.
- **Juniper SBR Services:** This category based report provides information related to services started or stopped.
- **Juniper SBR User account locked:** This category based report provides information related to when user account locked.
- **Juniper SBR User account unlocked:** This category based report provides information related to user account unlocked.
- **Juniper SBR Verification server failed:** This category based report provides information related to verification server failed.
- **Juniper SBR Web proxy error:** This category based report provides information related to web proxy error.

Alerts

- **Juniper SBR Authentication request failed:** This alert is generated when authentication request failed.
- **Juniper SBR Database connection failed:** This alert is generated when database connection failed.
- **Juniper SBR Network Error:** This alert is generated when network connection failed.
- **Juniper SBR Verification server failed:** This alert is generated when verification server failed.