Integrate Juniper Secure Access VPN

EventTracker Enterprise
About this Guide

This guide will facilitate a Juniper Secure Access VPN user to send syslog to EventTracker Enterprise.

Scope

The configurations detailed in this guide are consistent with EventTracker Enterprise 7.x or later and Juniper Secure Access VPN.

Audience

Administrators who want to monitor Juniper Secure Access VPN using EventTracker 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.

© 2016 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

About this Guide ..............................................................................................................................................................1

Scope ............................................................................................................................................................................1

Audience ......................................................................................................................................................................1

Introduction ......................................................................................................................................................................3

Pre-requisites ..................................................................................................................................................................3

How to enable Juniper Secure Access VPN Event Logs and Send logs to EventTracker? .........................................3

EventTracker Knowledge Pack .......................................................................................................................................8

Categories .....................................................................................................................................................................9

Alerts ............................................................................................................................................................................9

Reports .......................................................................................................................................................................10

Behavior rules ............................................................................................................................................................14

Importing Juniper Secure Access VPN knowledge pack into EventTracker ..............................................................15

Category .....................................................................................................................................................................15

Alerts ..........................................................................................................................................................................17

Tokens ........................................................................................................................................................................18

Flex Reports ...............................................................................................................................................................19

Token Templates ..........................................................................................................................................................20

Behavior Rules ..........................................................................................................................................................21

Verifying Juniper Secure Access VPN knowledge pack in EventTracker ...................................................................23

Categories .....................................................................................................................................................................23

Alerts ..........................................................................................................................................................................23

Tokens ........................................................................................................................................................................25

Reports .......................................................................................................................................................................25

Token Template ..........................................................................................................................................................26

Behavior Rules ..........................................................................................................................................................27

Create Flex Dashboards in EventTracker .....................................................................................................................27

Schedule Reports ..........................................................................................................................................................27

Create Dashlets ..........................................................................................................................................................30

Sample Dashboards ......................................................................................................................................................34
Introduction

The Juniper Networks Secure Access SSL VPN device is suitable for large enterprises and service providers. It features best-in-class performance, scalability and redundancy for organizations with high-volume secure access and authorization requirements. The Juniper Secure Access VPN SSL VPN hardware platforms are designed to scale to the largest enterprise deployments and to optimize application delivery, with redundant, hot-swappable hard disks and fans, optional second power supply, as well as multiple Ethernet ports for redundant or meshed configurations.

Pre-requisites

- **EventTracker 7.x or later** should be installed.
- Port 514 must be opened on Juniper Networks Secure Access SSL VPN.
- Port 514 must not be used by other services of Juniper Networks Secure Access SSL VPN.
- An exception should be added into Windows Firewall on EventTracker machine for Syslog port 514.

How to enable Juniper Secure Access VPN Event Logs and Send logs to EventTracker?

To specify events log settings:

Login to the Juniper secure access VPN using the user credentials and follow the below steps:

**Step 1:** In the admin console, choose **System > Log/Monitoring**.
**Step 2:** Select the **Events Log, User Access Log, Admin Access Log, or Sensors Log** tab, and then choose **Settings**.

Here we have selected **User Access > Settings**.
In the **Maximum Log Size** field, specify the maximum file size for the local log file. (The limit is 500 MB.) The system log displays data up to the amount specified.

**NOTE: Maximum Log Size** is an internal setting that most closely corresponds with the size of logs formatted with the **Standard** format. If you choose to use a more verbose format such as **WELF**, your log files may exceed the limit that you specify here.

**Step 3:** Under **Select Events to Log**, select the checkbox for each type of event that you want to capture in the local log file:

- Login/Logout
- SAM/Java
- User Settings
- Secure Terminal
EventTracker: Integrate Juniper Secure Access VPN

- Network Connect
- File Requests

**NOTE:** If you disable the Statistics checkbox in the Events Log tab, the IVE does not write statistics to the log file, but continues to display them in the System > Log/Monitoring > Statistics tab. For more information, see Viewing system statistics.

**User Access > Settings > Select Events to Log**

![Figure 3](image)

**Step 4:** Under EventTracker servers, enter information about the EventTracker servers where you want to store your log files (optional):
- Enter the name or IP address of the EventTracker server.
EventTracker: Integrate Juniper Secure Access VPN

- Enter a facility for the server. The IVE provides 8 facilities (LOCAL0-LOCAL7) which you can map to facilities on your EventTracker server.
- (Central Manager only) Choose which filter you want to apply to the log file.
- Click Add.

**NOTE:** Make sure your EventTracker server accepts messages with the following settings: facility = LOG_USER and level = LOG_INFO.

**User Access > Settings > EventTracker servers**

![Image of EventTracker server settings](image)

*Figure 4*

**Step 5:** Click **Save Changes**.

**User Access > Settings > Save Changes.**
EventTracker Knowledge Pack

Once Juniper Secure Access VPN events are enabled and Juniper Secure Access VPN events are received in EventTracker, Alerts and Reports can be configured in EventTracker.

The following Knowledge Packs are available in EventTracker to support Juniper Secure Access VPN monitoring.
EventTracker: Integrate Juniper Secure Access VPN

Categories

- **Juniper Secure Access VPN: Cache cleaner activity**
  This category provides information related to cache cleaner which removes residual data, such as temporary files or application caches, left on a user’s machine after a secure access session on Juniper Secure Access VPN.

- **Juniper Secure Access VPN: User session status**
  This category provides information related to user session whether the user session has started or stopped on Juniper Secure Access VPN.

- **Juniper Secure Access VPN: User login failed**
  This category provides information related to login failed, when the admin tries to login but fails on Juniper Secure Access VPN.

- **Juniper Secure Access VPN: User login success**
  This category provides information related to login success, when the login of the admin is a success on Juniper Secure Access VPN.

- **Juniper Secure Access VPN: Primary authentication failed**
  This category provides information related to primary authentication, where the user tries to authenticate at the initial stage of authentication but fails on Juniper Secure Access VPN.

- **Juniper Secure Access VPN: Primary authentication successful**
  This category provides information related to primary authentication, where the user tries to authenticate at the initial stage of authentication and successfully authenticates on Juniper Secure Access VPN.

- **Juniper Secure Access VPN: File transfer activity**
  This category provides information related to file transfer activity, where the user tries to download or upload a file on Juniper Secure Access VPN.

Alerts

- **Juniper Secure Access VPN: Primary authentication failed** - This alert is generated when user tries to authenticate on the initial stage of authentication in Juniper secure access VPN.

```
<134>Juniper: 2008-08-21 08:01:22 - connect2a - [192.168.1.2]Root::jsmith(Intranet)|Employee| - Primary authentication failed for mpanko@juniper.net/acme AD from 172.5.6.87
```
• **Juniper Secure Access VPN: User login failed** - This alert is generated when admin tries to login but fails in Juniper secure access VPN.

```
```

• **Juniper Secure Access VPN: User login success** - This alert is generated when user successfully login to the Juniper Secure Access VPN.

**Logs Considered**

```
```

**Reports**

• **Juniper Secure Access VPN - File transfer activity** - This report provides information related to user activity, where the user tries to download or upload a file on Juniper Secure Access VPN.

**Logs considered**

```
<134>Juniper: 2008-08-21 08:01:22 - connect2a - [192.168.1.2] Root::jsmith(Intranet)[Employee] - Downloaded Windows file \GIZMOFILESERVER\public\andrey\Adj_Juniper.xls
<134>Juniper: 2008-08-21 08:01:22 - connect2a - [192.168.1.2] Root::jsmith(Intranet)[Employee] - Uploaded Windows file \GIZMOFILESERVER\public\AAA_HU\ldapbrowser\lib\ldap.jar.
```
Sample Report

• **Juniper Secure Access VPN - Primary authentication successful**: This report provides information related to primary authentication, where the user tries to authenticate at the initial stage of authentication on Juniper Secure Access VPN.

Logs considered

<134>Juniper: 2008-08-21 08:01:22 - connect2a - [192.168.1.2] Root::jsmith(Intranet)[Employee] - Primary authentication successful for mstest2/LOCAL-IVE from 10.2.6.15

Sample Report

• **Juniper Secure Access VPN - Primary authentication failed**: This report provides information related to primary authentication, where the user tries to authenticate at the initial stage of authentication but fails on Juniper Secure Access VPN.

Logs considered

<134>Juniper: 2008-08-21 08:01:22 - connect2a - [192.168.1.2] Root::jsmith(Intranet)[Employee] - Primary authentication failed for mpanko@juniper.net/acme AD from 172.5.6.87
EventTracker: Integrate Juniper Secure Access VPN

Sample Report

<table>
<thead>
<tr>
<th>Event Time</th>
<th>User Name</th>
<th>Source IP Address</th>
<th>Destination IP Address</th>
<th>Authentication Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>2008-08-21 08:01:22</td>
<td>jsmith</td>
<td>192.168.1.2</td>
<td>172.5.6.67</td>
<td><a href="mailto:mpanko@unipier.net">mpanko@unipier.net</a>/acme</td>
</tr>
<tr>
<td>2008-08-21 08:01:22</td>
<td>jsmith</td>
<td>192.168.1.2</td>
<td>172.5.6.67</td>
<td><a href="mailto:mpanko@unipier.net">mpanko@unipier.net</a>/acme</td>
</tr>
<tr>
<td>2008-08-21 08:01:22</td>
<td>jsmith</td>
<td>192.168.1.2</td>
<td>172.5.6.67</td>
<td><a href="mailto:mpanko@unipier.net">mpanko@unipier.net</a>/acme</td>
</tr>
</tbody>
</table>

Figure 8

- **Juniper Secure Access VPN-User login success**: This report provides information related to login success, i.e. when the login of the admin is a success on Juniper Secure Access VPN.

Logs considered


Sample Report

<table>
<thead>
<tr>
<th>Event Time</th>
<th>User Name</th>
<th>Source IP Address</th>
<th>Destination IP Address</th>
<th>Authentication Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>2008-08-21 08:01:22</td>
<td>jsmith</td>
<td>192.168.1.2</td>
<td>10.2.3.56</td>
<td>mtest2/mtest</td>
</tr>
<tr>
<td>2008-08-21 08:01:22</td>
<td>jsmith</td>
<td>192.168.1.2</td>
<td>10.2.3.56</td>
<td>mtest2/mtest</td>
</tr>
<tr>
<td>2008-08-21 08:01:22</td>
<td>jsmith</td>
<td>192.168.1.2</td>
<td>192.168.1.2</td>
<td>intranet.acme.net</td>
</tr>
<tr>
<td>2008-08-21 08:01:22</td>
<td>jsmith</td>
<td>192.168.1.2</td>
<td>192.168.1.2</td>
<td>intranet.acme.net</td>
</tr>
<tr>
<td>2008-08-21 08:01:22</td>
<td>jsmith</td>
<td>192.168.1.2</td>
<td>192.168.1.2</td>
<td>intranet.acme.net</td>
</tr>
</tbody>
</table>

Figure 9

- **Juniper Secure Access VPN-User login failed**: This report provides information related to login failed, i.e. when the admin tries to login but fails on Juniper Secure Access VPN.

Logs considered


Sample Report

**Juniper Secure Access VPN - User session status:** This report provides information related to user session, i.e. whether the user session has started or stopped on Juniper Secure Access VPN.

**Logs considered**


---

Sample Report

**Juniper Secure Access VPN - Cache cleaner activity:** This report provides information related to cache cleaner which removes residual data, such as temporary files or application caches, left on a user’s machine after a Secure Access session on Juniper Secure Access VPN.

**Logs considered**


<134>Juniper: 2008-07-09 08:04:31 - connect2a - [192.168.0.1] ABCD::bnelson(Users)[] - System process detected a Cache Cleaner time out on host 169.15.2.1 for user 'bnelson' (last update at 2008-07-11 07.00.19 -0700 PDT)
Sample Report

<table>
<thead>
<tr>
<th>Event Time</th>
<th>User Name</th>
<th>Source IP Address</th>
<th>Host IP Address</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>2008-07-09 08:04:31</td>
<td>bnelson</td>
<td>192.168.0.1</td>
<td>169.15.2.1</td>
<td>Cleaner time out</td>
</tr>
</tbody>
</table>

Figure 12

Behavior rules

**Juniper Secure Access VPN user logon success**

This behavior rule helps in identifying the connections from unknown or new IP addresses used to logon to Juniper Secure Access VPN.

![NEW IP ADDRESS OBSERVED][1]

Figure 13
Importing Juniper Secure Access VPN knowledge pack into EventTracker

1. Launch **EventTracker Control Panel**.

2. Double click **Export Import Utility**, and then click **Import** tab.

   Import **Token Templates/Category/Alert/Tokens/Flex Reports** as given below.

   **NOTE**: Importing should be in the same order as mentioned above.

   ![EventTracker Control Panel](image)

   Figure 14

**Category**

1. Click **Category** option, and then click the browse button.
2. Locate All Juniper Secure Access VPN group of Categories.iscat file, and then click the Open button.

3. To import categories, click the Import button.

   EventTracker displays success message.

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

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

![Image of Export Import Utility](image17.png)

**Figure 17**

2. Locate All Juniper Secure Access VPN Alerts.isalt file, and then click the Open button.

3. To import alerts, click the Import button.

EventTracker displays success message.

![Image of Alert Configuration Import](image18.png)

**Figure 18**

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

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

2. Locate **All Juniper Secure Access VPN Tokens.istoken** file, and then click the Open button.
3. To import tokens, click the Import button.
   
   EventTracker displays success message.

4. Click OK, and then click the Close button.
EventTracker: Integrate Juniper Secure Access VPN

Flex Reports

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

![Figure 21](image)

2. Locate **All Juniper Secure Access VPN Flex Report.issch** file, and then click the **Open** button.

3. To import scheduled reports, click the **Import** button.

   EventTracker displays success message.

![Figure 22](image)

4. Click **OK**, and then click the **Close** button.
EventTracker: Integrate Juniper Secure Access VPN

Token Templates

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

2. Select **Template** tab, and then click on 'Import' option.

3. Click on **Browse** button.

4. Locate **All Juniper Secure Access VPN Token Template.ettd** file, and then click the **Open** button
5. Now select the check box and then click on 'Import' option. EventTracker displays success message.

![Template(s) imported successfully](image)

6. Click on OK button.

**Behavior Rules**

1. Click Behavior Rules option, and then click the browse button.

2. Locate the All Juniper Secure Access VPN group of behavior rules.isrule file, and then click Open button.
3. To import categories, click the **Import** button.

EventTracker displays success message.

4. Click **OK**.
Verifying Juniper Secure Access VPN knowledge pack in EventTracker

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 Secure Access VPN group folder to view the imported categories.

![Image of Category Management]

Figure 29

Alerts

1. Logon to EventTracker Enterprise.
2. Click the Admin menu, and then click Alerts.
3. In **Search** field, type "Juniper Secure Access VPN", and then click the **Go** button.

Alert Management page will display all the imported **Juniper Secure Access VPN** alerts.

![Alert Management Page](image)

**Figure 30**

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

EventTracker displays message box.

![Message Box](image)

**Figure 31**

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.
Tokens

1. Logon to EventTracker Enterprise.

2. Click the Admin menu, and then click Parsing Rules.

The imported Juniper Secure Access VPN tokens are added in Token-Value Groups list.

![Parsing Rule](image)

Figure 32

Reports

1. Logon to EventTracker Enterprise.

2. Click the Reports menu, and then select Configuration.

3. In Reports Configuration pane, select Defined option.

   EventTracker displays Defined page.

4. In search box enter Juniper Secure Access VPN, and then click the Search button.

   EventTracker displays Flex reports of Juniper Secure Access VPN.
Token Template

1. Logon to EventTracker Enterprise.
2. Click the Admin menu, and then click Parsing Rules.
EventTracker: Integrate Juniper Secure Access VPN

Behavior Rules

1. Select **Behavior Rules** from **Admin** drop-down.

![Figure 35](image)

Create Flex Dashboards in EventTracker

Schedule Reports

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

![Figure 36](image)

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

4. Click on 'schedule' to plan a report for later execution.
5. Choose appropriate time for report execution and in Step 8 check **Persist data in Eventvault explorer** box.
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.

![Dashboard pane](Figure 40)

3. Navigate to **Dashboard>Flex**.
   Flex Dashboard pane is shown.
4. Fill suitable title and description and click **Save** button.
5. Click 🎨 to configure a new flex dashlet. Widget configuration pane is shown.
6. Locate earlier scheduled report in **Data Source** dropdown.
7. Select **Chart Type** from dropdown.
8. Select extent of data to be displayed in **Duration** dropdown.
9. Select computation type in **Value Field Setting** dropdown.
10. Select evaluation duration in **As Of** dropdown.
11. Select comparable values in **X Axis** with suitable label.
12. Select numeric values in **Y Axis** with suitable label.
13. Select comparable sequence in **Legend**.
14. Click **Test** button to evaluate. Evaluated chart is shown.
3. If satisfied, click **Configure** button

![Figure 43](image)

4. Click ‘customize’ 🚀 to locate and choose created dashlet.
5. Click ✖️ to add dashlet to earlier created dashboard.
Sample Dashboards


Figure 45