Abstract

This guide provides instructions to configure HP ProCurve Switch to send the event logs to EventTracker. Once events are configured to send to EventTracker Manager, alerts, dashboards and reports can be configured into EventTracker.

Scope

The configurations detailed in this guide are consistent with EventTracker Enterprise version 7.X and later, and HP 2520G, HP 2520, HP 2530, HP 2615, HP 2620, HP 2910al, HP 2915, HP 2920, HP 3500, HP 3500yl, HP 3800, HP 5400zl, HP 6200yl and HP 8200zl.

Audience

HP ProCurve Switch users, who wish to forward event logs to EventTracker Manager and monitor events using EventTracker.
# Table of Contents

Abstract ........................................................................................................................................... 1
Scope .................................................................................................................................................. 1
Audience............................................................................................................................................ 1
Overview .......................................................................................................................................... 3
Prerequisites .................................................................................................................................... 3
Enable Syslog forwarding on HP ProCurve Switch ........................................................................... 3
  Configure Syslog Server .................................................................................................................. 3
EventTracker Knowledge Pack (KP) .................................................................................................... 3
  Categories ......................................................................................................................................... 4
Alerts ................................................................................................................................................... 4
Reports ................................................................................................................................................ 4
Knowledge Objects ............................................................................................................................ 4
Import Knowledge Pack into EventTracker ....................................................................................... 5
  Import Categories ............................................................................................................................. 6
Import Alerts ....................................................................................................................................... 7
Import Flex Reports ............................................................................................................................ 8
Import Token Templates ..................................................................................................................... 9
Import Knowledge Object .................................................................................................................. 10
Verify Knowledge Pack in EventTracker .......................................................................................... 12
  Verify Categories ............................................................................................................................. 12
Verify Alerts ....................................................................................................................................... 13
Verify Flex Reports ............................................................................................................................ 14
Verify Token Templates ..................................................................................................................... 15
Verify Knowledge Object .................................................................................................................. 16
Create Dashboards in EventTracker ................................................................................................. 17
  Schedule Reports .............................................................................................................................. 17
Create Dashlets ................................................................................................................................. 20
Sample Reports ................................................................................................................................. 24
Sample Dashboards ........................................................................................................................... 27
Overview

Hp ProCurve switches are a series of layer 2 and layer 3 switches ideal for high-performance and secure Gigabit connectivity. EventTracker aggregates and deduces informative events to provide an insight on user behavior and security violations.

Prerequisites

- EventTracker v7.x and later should be installed.
- Console access by telnet or ssh must be enabled on ProCurve switch.

Enable Syslog forwarding on HP ProCurve Switch

Configure Syslog Server

- Telnet/SSH to switch console.
- Logon with Admin account.
- Enter Config Mode.
- Type following commands:

```
logging facility syslog
logging 192.168.X.X
```

(192.168.X.X is ip address of EventTracker manager)

- Save configuration and exit.

NOTE: Please add port 514 to firewall exception, if applicable.

EventTracker Knowledge Pack (KP)

Once logs are received in EventTracker; categories, alerts, reports and dashboards can be configured in EventTracker.

The following Knowledge Packs are available in EventTracker v7 and later to support HP ProCurve switch monitoring:
Categories

- **HP ProCurve Console Session Established** - This category based report provides information related to launch of console sessions.
- **HP ProCurve Security Violation Detected** - This category based report provides information related to network security violations.
- **HP ProCurve System Authentication Failed** - This category based report provides information related to system authentication failure.
- **HP ProCurve System Configuration Changed** - This category based report provides information related to switch configuration file modification.
- **HP ProCurve User Logon Failed** - This category based report provides information related to user logon failure.

Alerts

- **HP ProCurve System Authentication Failed** - This alert is generated when system authentication fails.
- **HP ProCurve User Logon Failed** - This alert is generated when user logon fails.

Reports

- **HP ProCurve-Port Status Change Details** - This report provides information related to status change of switch port.
- **HP ProCurve-Security Violation Details** - This report provides information related to security violations detected.
- **HP ProCurve-User Logon Details** - This report provides information related to user logon and logoff.

Knowledge Objects

- **HP ProCurve-Port Status Change Details** - This KO assists in evaluation of switch port status.
- **HP ProCurve-Security Violation Details** - This KO assists in evaluation of potential security breach.
- **HP ProCurve-User Logon Details** - This KO assists in evaluation of user logon activities.
Import Knowledge Pack into EventTracker

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

3. Import Categories/Alerts/Templates/Flex Reports/Knowledge Objects as given below.
Import Categories

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

![Figure 2](image)

2. Locate applicable ‘**All HP ProCurve Switch categories.iscat**’ file, and then click the **Open** button.
3. To import categories, click the **Import** button.
   EventTracker displays success message.

![Figure 3](image)

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

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

![Figure 4](image)

2. Locate applicable ‘All HP ProCurve Switch alerts.isalt’ file, and then click the *Open* button.
3. To import alerts, click the *Import* button.
   EventTracker displays success message.

![Figure 5](image)

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

1. Click **Scheduled Reports** option, and then click the ‘browse’ button.

2. Locate applicable ‘All HP ProCurve Switch reports.issch’ file, and then click the **Open** button.

   ![Figure 6]
   
   To import scheduled reports, click the **Import** button. EventTracker displays success message.

   ![Figure 7]

3. Click **OK**, and then click the **Close** button.
Import Token Templates

1. Click the **Admin** menu, and then click **Parsing rule**.
2. Select **Template** tab, and then click on ‘Import’ option.

![Parsing Rule](image)

**Figure 8**

3. Click on **Browse** button.

![Browse](image)

**Figure 9**

4. Locate applicable ‘All HP ProCurve Switch token templates.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.

**Import Knowledge Object**

1. Click the Admin menu, and then click Knowledge Objects.
2. Click on ‘Import’ option.
3. In **IMPORT** pane click on **Browse** button.

4. Locate applicable ‘**All HP ProCurve Switch knowledge objects.etko**’ file, and then click the **UPLOAD** button.
5. Now select the check box and then click on ‘MERGE’ option. EventTracker displays success message.

6. Click on OK button.

Verify 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 HP ProCurve Switch group folder.
Verify Alerts

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Alerts**.
3. In the **Search** box, type ‘**HP ProCurve**’, and then click the **search** button. Alert Management page will display all the imported alerts.

4. To activate the imported alerts, select the respective checkbox in the **Active** column and then click the **Activate Now** button.

   EventTracker displays message box.
5. Click OK.

**NOTE:** Please specify appropriate systems in alert configuration for better performance.

**Verify Flex Reports**

1. Logon to EventTracker Enterprise.
2. Click the Reports menu, and then Configuration.
4. In Report Groups Tree to view imported Scheduled Reports, scroll down and click HP ProCurve Switch group folder.

Scheduled Reports are displayed in the Reports configuration pane.
NOTE: Please specify appropriate systems in report wizard for better performance.

Verify Token Templates

1. Click the Admin menu, and then click Parsing rule.
2. Select Template tab.
3. Scroll and find imported HP ProCurve Switch token templates.
### Verify Knowledge Object

1. Click the **Admin** menu, and then click **Knowledge Objects**.
2. Scroll down and select **HP ProCurve Switch** in **Objects** pane. Imported HP ProCurve object details are shown.

---

**Table:**

<table>
<thead>
<tr>
<th>Rule Description</th>
<th>Value</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wasteguard Attacks</td>
<td>XTM 6 series or later</td>
<td>9/1/2015 10:31:22 AM</td>
</tr>
<tr>
<td>All ACC Traffic</td>
<td>All Application Delivery Controller AVT tunnel Series</td>
<td>9/1/2015 11:23:42 AM</td>
</tr>
<tr>
<td>All ACC Authentication Failure</td>
<td>All Application Delivery Controller AVT tunnel Series</td>
<td>9/1/2015 11:23:42 AM</td>
</tr>
<tr>
<td>HP ProCurve-Port Status Change Details</td>
<td></td>
<td>9/1/2015 04:18:51 PM</td>
</tr>
<tr>
<td>HP ProCurve-Security Violation Details</td>
<td></td>
<td>9/1/2015 05:35:35 PM</td>
</tr>
<tr>
<td>HP ProCurve-User Login Details</td>
<td></td>
<td>9/1/2015 08:15:40 PM</td>
</tr>
</tbody>
</table>
Create Dashboards in EventTracker

Schedule Reports

1. Open EventTracker in browser and logon.

2. Navigate to Reports>Configuration.
3. Select **HP ProCurve Switch** in report groups. Check **defined** dialog box.

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

4. Click + to add a new dashboard.
   Flex Dashboard configuration pane is shown.
5. Fill fitting title and description and click **Save** button.
6. Click 🌟 to configure a new flex dashlet.
   Widget configuration pane is shown.

![Figure 29](image-url)

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 30**

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

**Figure 31**

17. Click ‘customize’ to locate and choose the created dashlet.

18. Click to add dashlet to earlier created dashboard.
## Sample Reports

1. **HP ProCurve-User Logon Details**

<table>
<thead>
<tr>
<th>Event Time</th>
<th>Switch Address</th>
<th>Logon Status</th>
<th>User Name</th>
<th>Source Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mar 10 09:39:47</td>
<td>10.1.52.23</td>
<td>logout</td>
<td>Jack</td>
<td>192.168.5.23</td>
</tr>
<tr>
<td>Mar 10 09:20:51</td>
<td>10.1.52.23</td>
<td>login</td>
<td>Mary</td>
<td>192.168.6.10</td>
</tr>
<tr>
<td>Mar 10 10:01:55</td>
<td>10.1.51.85</td>
<td>logout</td>
<td>Ken</td>
<td>192.168.5.3</td>
</tr>
<tr>
<td>Mar 10 10:42:59</td>
<td>10.1.52.23</td>
<td>login</td>
<td>Mary</td>
<td>192.168.5.16</td>
</tr>
<tr>
<td>Mar 10 11:24:03</td>
<td>10.1.52.23</td>
<td>login</td>
<td>Jack</td>
<td>192.168.5.20</td>
</tr>
<tr>
<td>Mar 10 12:05:07</td>
<td>10.1.51.85</td>
<td>login</td>
<td>John</td>
<td>192.168.5.12</td>
</tr>
<tr>
<td>Mar 10 12:46:11</td>
<td>10.1.51.85</td>
<td>logout</td>
<td>John</td>
<td>192.168.5.55</td>
</tr>
<tr>
<td>Mar 10 13:27:16</td>
<td>10.1.51.85</td>
<td>logout</td>
<td>Jim</td>
<td>192.168.5.88</td>
</tr>
<tr>
<td>Mar 10 14:08:19</td>
<td>10.1.51.85</td>
<td>login</td>
<td>Jack</td>
<td>192.168.5.21</td>
</tr>
<tr>
<td>Mar 10 11:12:14</td>
<td>10.1.52.23</td>
<td>login</td>
<td>Jim</td>
<td>192.168.4.21</td>
</tr>
<tr>
<td>Mar 10 13:44:41</td>
<td>10.1.52.23</td>
<td>logout</td>
<td>Jack</td>
<td>192.168.3.34</td>
</tr>
<tr>
<td>Mar 10 16:17:08</td>
<td>10.1.51.85</td>
<td>logout</td>
<td>John</td>
<td>192.168.4.22</td>
</tr>
<tr>
<td>Mar 10 18:49:35</td>
<td>10.1.51.85</td>
<td>logout</td>
<td>Jack</td>
<td>192.168.3.35</td>
</tr>
<tr>
<td>Mar 10 21:22:02</td>
<td>10.1.52.23</td>
<td>login</td>
<td>Jack</td>
<td>192.168.4.23</td>
</tr>
<tr>
<td>Mar 10 23:54:29</td>
<td>10.1.51.85</td>
<td>login</td>
<td>Jim</td>
<td>192.168.3.36</td>
</tr>
<tr>
<td>Mar 11 02:26:56</td>
<td>10.1.51.85</td>
<td>logout</td>
<td>John</td>
<td>192.168.4.24</td>
</tr>
<tr>
<td>Mar 11 04:59:23</td>
<td>10.1.51.85</td>
<td>logout</td>
<td>Mary</td>
<td>192.168.3.37</td>
</tr>
<tr>
<td>Mar 11 07:31:50</td>
<td>10.1.51.85</td>
<td>login</td>
<td>Mary</td>
<td>192.168.4.25</td>
</tr>
<tr>
<td>Mar 11 10:06:17</td>
<td>10.1.52.23</td>
<td>logout</td>
<td>Jack</td>
<td>192.168.3.36</td>
</tr>
<tr>
<td>Mar 11 12:36:44</td>
<td>10.1.51.85</td>
<td>login</td>
<td>Ken</td>
<td>192.168.4.26</td>
</tr>
<tr>
<td>Mar 11 15:03:11</td>
<td>10.1.52.23</td>
<td>logout</td>
<td>Jane</td>
<td>192.168.3.38</td>
</tr>
<tr>
<td>Mar 11 17:41:38</td>
<td>10.1.51.85</td>
<td>logout</td>
<td>Ken</td>
<td>192.168.4.27</td>
</tr>
<tr>
<td>Mar 11 20:14:05</td>
<td>10.1.52.23</td>
<td>login</td>
<td>Jack</td>
<td>192.168.3.40</td>
</tr>
</tbody>
</table>
## 2. HP ProCurve – Security Violation Details

<table>
<thead>
<tr>
<th>Event Time</th>
<th>Component Violated</th>
<th>Switch Address</th>
<th>Switch Port</th>
<th>User Name</th>
<th>Source Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mar 10 08:39:47</td>
<td>Port</td>
<td>10.1.51.65</td>
<td>21</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mar 10 09:20:50</td>
<td>snmp</td>
<td>10.1.52.23</td>
<td></td>
<td></td>
<td>EdgeSwitch 10.1.1.2</td>
</tr>
<tr>
<td>Mar 10 13:01:55</td>
<td>snmp</td>
<td>10.1.51.65</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mar 10 13:42:59</td>
<td>Port</td>
<td>10.1.52.23</td>
<td>19</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mar 10 11:24:03</td>
<td>snmp</td>
<td>10.1.51.65</td>
<td></td>
<td></td>
<td>10.1.1.11</td>
</tr>
<tr>
<td>Mar 10 12:05:07</td>
<td>snmp</td>
<td>10.1.51.65</td>
<td></td>
<td></td>
<td>10.1.1.52</td>
</tr>
<tr>
<td>Mar 10 12:46:11</td>
<td>Port</td>
<td>10.1.52.23</td>
<td>21</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mar 10 13:27:15</td>
<td>snmp</td>
<td>10.1.52.23</td>
<td></td>
<td></td>
<td>EdgeSwitch 10.1.1.2</td>
</tr>
<tr>
<td>Mar 10 14:08:19</td>
<td>Port</td>
<td>10.1.52.23</td>
<td></td>
<td></td>
<td>10.1.1.1</td>
</tr>
<tr>
<td>Mar 10 11:12:14</td>
<td>Port</td>
<td>10.1.51.65</td>
<td></td>
<td></td>
<td>20</td>
</tr>
<tr>
<td>Mar 10 13:44:41</td>
<td>snmp</td>
<td>10.1.52.23</td>
<td></td>
<td></td>
<td>10.1.1.55</td>
</tr>
<tr>
<td>Mar 10 13:17:08</td>
<td>snmp</td>
<td>10.1.51.65</td>
<td></td>
<td></td>
<td>10.1.1.1</td>
</tr>
<tr>
<td>Mar 10 18:49:35</td>
<td>Port</td>
<td>10.1.52.23</td>
<td></td>
<td></td>
<td>11</td>
</tr>
<tr>
<td>Mar 10 21:22:02</td>
<td>Port</td>
<td>10.1.51.65</td>
<td></td>
<td></td>
<td>EdgeSwitch 10.1.1.2</td>
</tr>
<tr>
<td>Mar 10 23:54:29</td>
<td>snmp</td>
<td>10.1.51.65</td>
<td></td>
<td></td>
<td>10.1.1.1</td>
</tr>
<tr>
<td>Mar 11 00:26:58</td>
<td>Port</td>
<td>10.1.52.23</td>
<td></td>
<td></td>
<td>21</td>
</tr>
<tr>
<td>Mar 11 04:59:23</td>
<td>snmp</td>
<td>10.1.51.65</td>
<td></td>
<td></td>
<td>EdgeSwitch 10.1.1.2</td>
</tr>
<tr>
<td>Mar 11 07:31:50</td>
<td>snmp</td>
<td>10.1.52.23</td>
<td></td>
<td></td>
<td>10.1.1.41</td>
</tr>
<tr>
<td>Mar 11 10:04:17</td>
<td>Port</td>
<td>10.1.52.23</td>
<td></td>
<td></td>
<td>11</td>
</tr>
<tr>
<td>Mar 11 12:36:44</td>
<td>Port</td>
<td>10.1.52.23</td>
<td></td>
<td></td>
<td>EdgeSwitch 10.1.1.2</td>
</tr>
<tr>
<td>Mar 11 15:09:11</td>
<td>snmp</td>
<td>10.1.51.65</td>
<td></td>
<td></td>
<td>10.1.1.1</td>
</tr>
<tr>
<td>Mar 11 17:41:38</td>
<td>snmp</td>
<td>10.1.51.65</td>
<td></td>
<td></td>
<td>5</td>
</tr>
<tr>
<td>Mar 11 20:14:05</td>
<td>snmp</td>
<td>10.1.51.65</td>
<td></td>
<td></td>
<td>EdgeSwitch 10.1.1.47</td>
</tr>
</tbody>
</table>
### HP ProCurve - Port Status Change Details

<table>
<thead>
<tr>
<th>Event Time</th>
<th>Switch Address</th>
<th>Switch Port</th>
<th>Port Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mar 10 08:35:47</td>
<td>10.1.51.55</td>
<td>41</td>
<td>on-line</td>
</tr>
<tr>
<td>Mar 10 08:20:51</td>
<td>10.1.51.55</td>
<td>10</td>
<td>off-line</td>
</tr>
<tr>
<td>Mar 10 08:01:55</td>
<td>10.1.51.55</td>
<td>19</td>
<td>off-line</td>
</tr>
<tr>
<td>Mar 10 04:29:50</td>
<td>10.1.52.23</td>
<td>41</td>
<td>on-line</td>
</tr>
<tr>
<td>Mar 10 11:24:03</td>
<td>10.1.52.23</td>
<td>42</td>
<td>on-line</td>
</tr>
<tr>
<td>Mar 10 12:05:07</td>
<td>10.1.51.55</td>
<td>28</td>
<td>off-line</td>
</tr>
<tr>
<td>Mar 10 12:46:11</td>
<td>10.1.51.55</td>
<td>37</td>
<td>off-line</td>
</tr>
<tr>
<td>Mar 10 13:27:16</td>
<td>10.1.62.23</td>
<td>42</td>
<td>off-line</td>
</tr>
<tr>
<td>Mar 10 14:08:18</td>
<td>10.1.51.55</td>
<td>43</td>
<td>on-line</td>
</tr>
<tr>
<td>Mar 10 10:12:14</td>
<td>10.1.51.55</td>
<td>46</td>
<td>on-line</td>
</tr>
<tr>
<td>Mar 10 13:44:41</td>
<td>10.1.51.55</td>
<td>55</td>
<td>off-line</td>
</tr>
<tr>
<td>Mar 10 16:17:08</td>
<td>10.1.51.55</td>
<td>10</td>
<td>on-line</td>
</tr>
<tr>
<td>Mar 10 18:49:35</td>
<td>10.1.52.23</td>
<td>17</td>
<td>off-line</td>
</tr>
<tr>
<td>Mar 10 21:22:02</td>
<td>10.1.51.55</td>
<td>24</td>
<td>off-line</td>
</tr>
<tr>
<td>Mar 10 23:54:29</td>
<td>10.1.52.23</td>
<td>31</td>
<td>on-line</td>
</tr>
<tr>
<td>Mar 11 02:26:56</td>
<td>10.1.51.55</td>
<td>38</td>
<td>off-line</td>
</tr>
<tr>
<td>Mar 11 04:59:23</td>
<td>10.1.52.23</td>
<td>45</td>
<td>on-line</td>
</tr>
<tr>
<td>Mar 11 07:31:50</td>
<td>10.1.52.23</td>
<td>41</td>
<td>off-line</td>
</tr>
<tr>
<td>Mar 11 10:04:17</td>
<td>10.1.52.23</td>
<td>25</td>
<td>on-line</td>
</tr>
<tr>
<td>Mar 11 12:36:44</td>
<td>10.1.51.55</td>
<td>8</td>
<td>off-line</td>
</tr>
<tr>
<td>Mar 11 15:05:11</td>
<td>10.1.52.23</td>
<td>7</td>
<td>on-line</td>
</tr>
<tr>
<td>Mar 11 17:41:38</td>
<td>10.1.51.55</td>
<td>23</td>
<td>off-line</td>
</tr>
<tr>
<td>Mar 11 20:46:05</td>
<td>10.1.52.23</td>
<td>39</td>
<td>on-line</td>
</tr>
</tbody>
</table>
Sample Dashboards

1. HP ProCurve Security Violations Today

![Graph showing security violations today](image)

Figure 32

2. HP ProCurve Port Activity Today

![Graph showing port activity today](image)

Figure 33
3. HP ProCurve Logon Activity Today

Figure 34