EventTracker

Actionable Security Intelligence

Integrate HP ProCurve Switch

Publication Date: September 24, 2015

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

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 firwall 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.

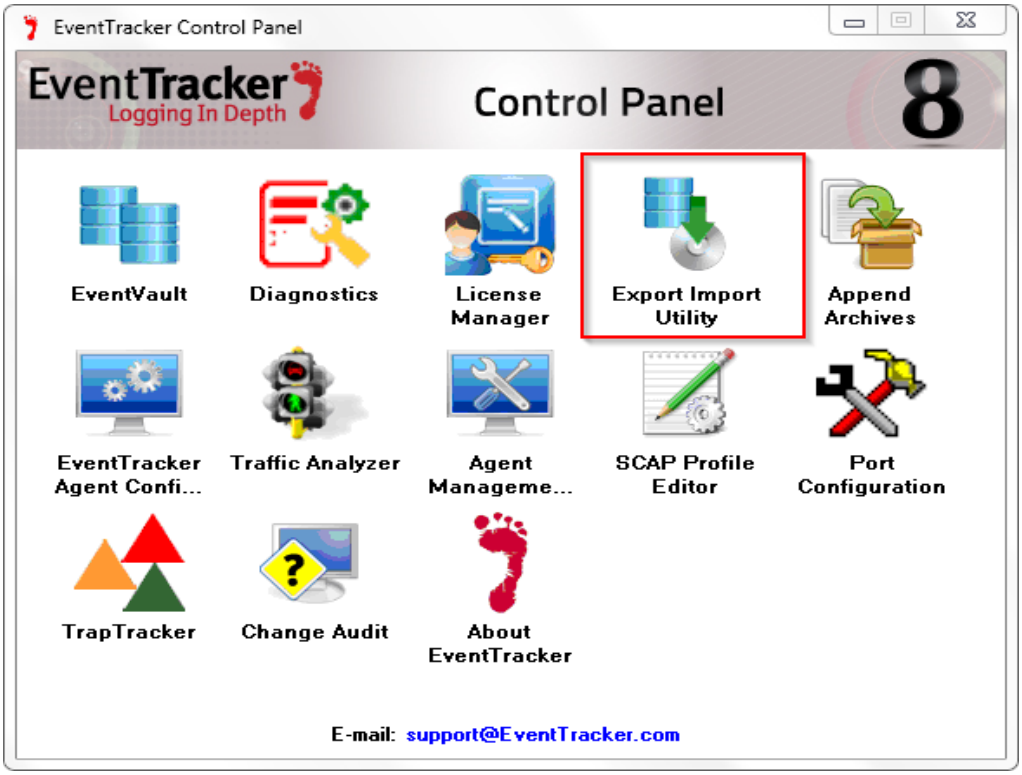

Figure 1

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

Import Categories

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

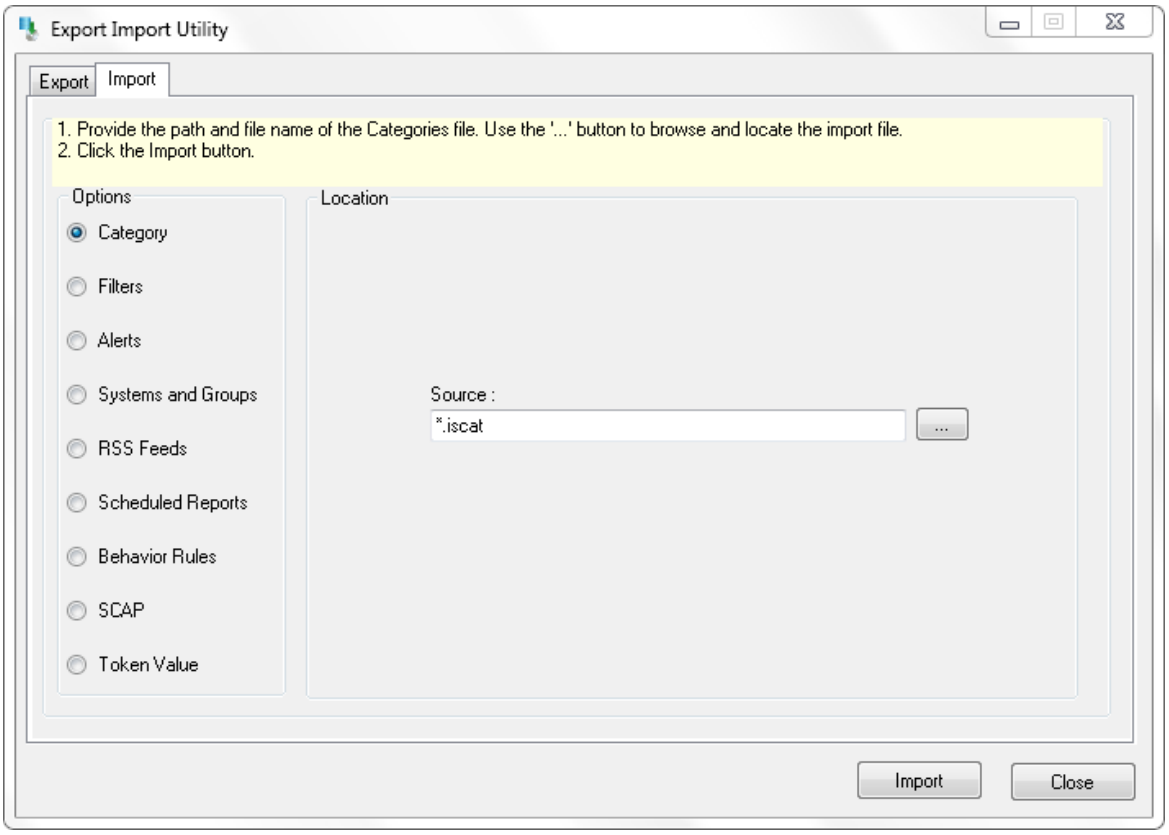

Figure 2

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.

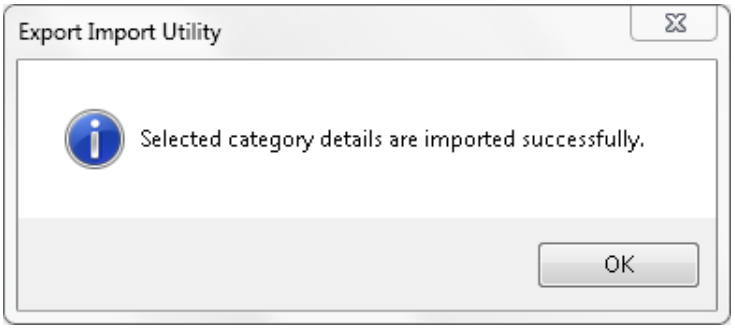

Figure 3

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

Import Alerts

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

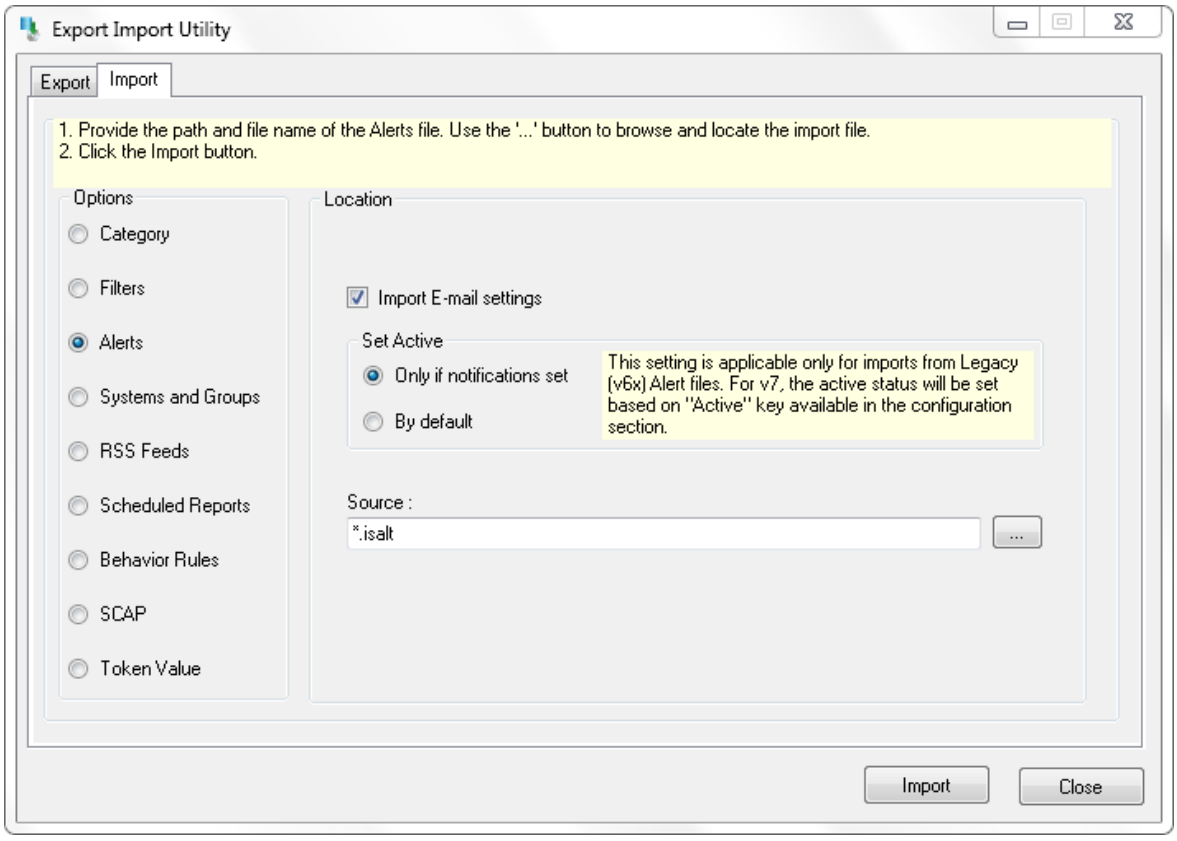

Figure 4

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

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.

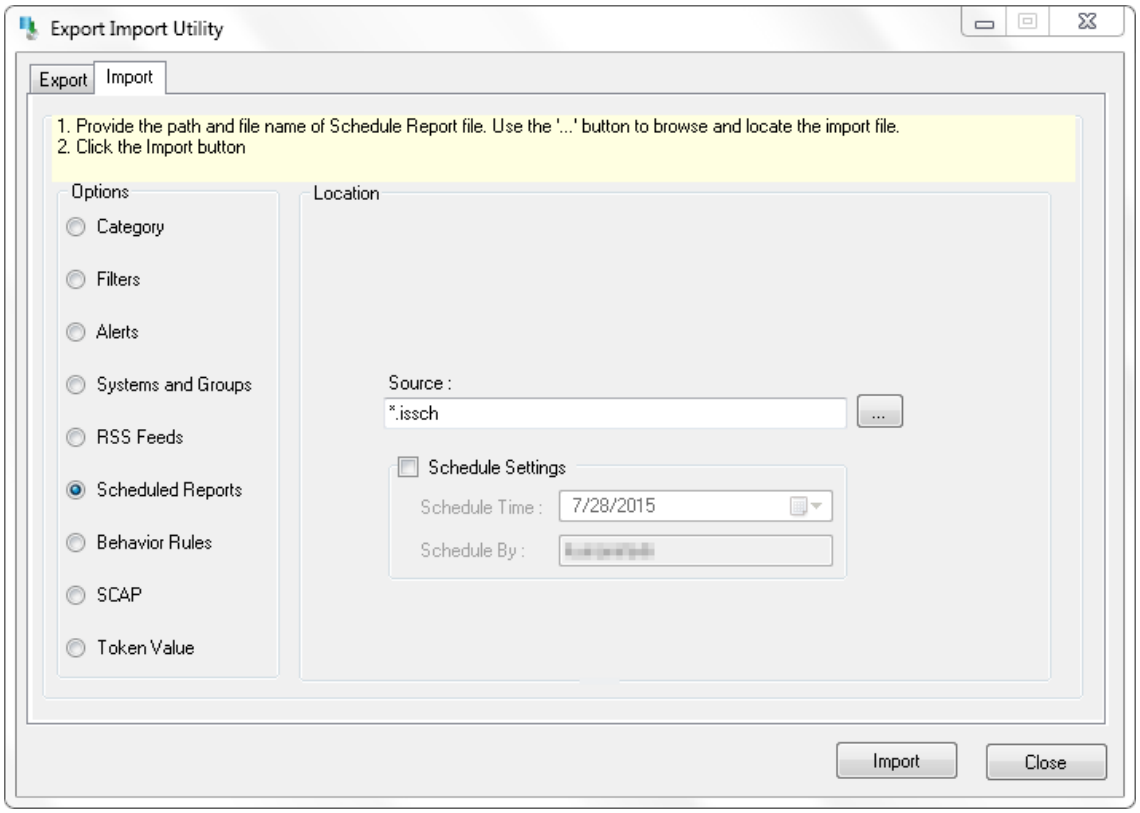

Figure 6

3. To import scheduled reports, click the **Import** button.
   EventTracker displays success message.

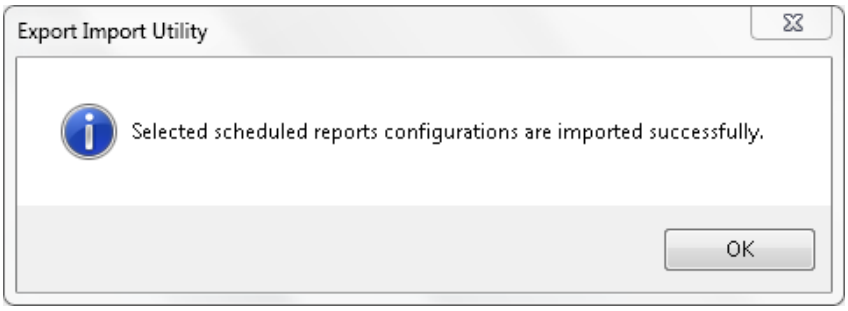

Figure 7

4. 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.

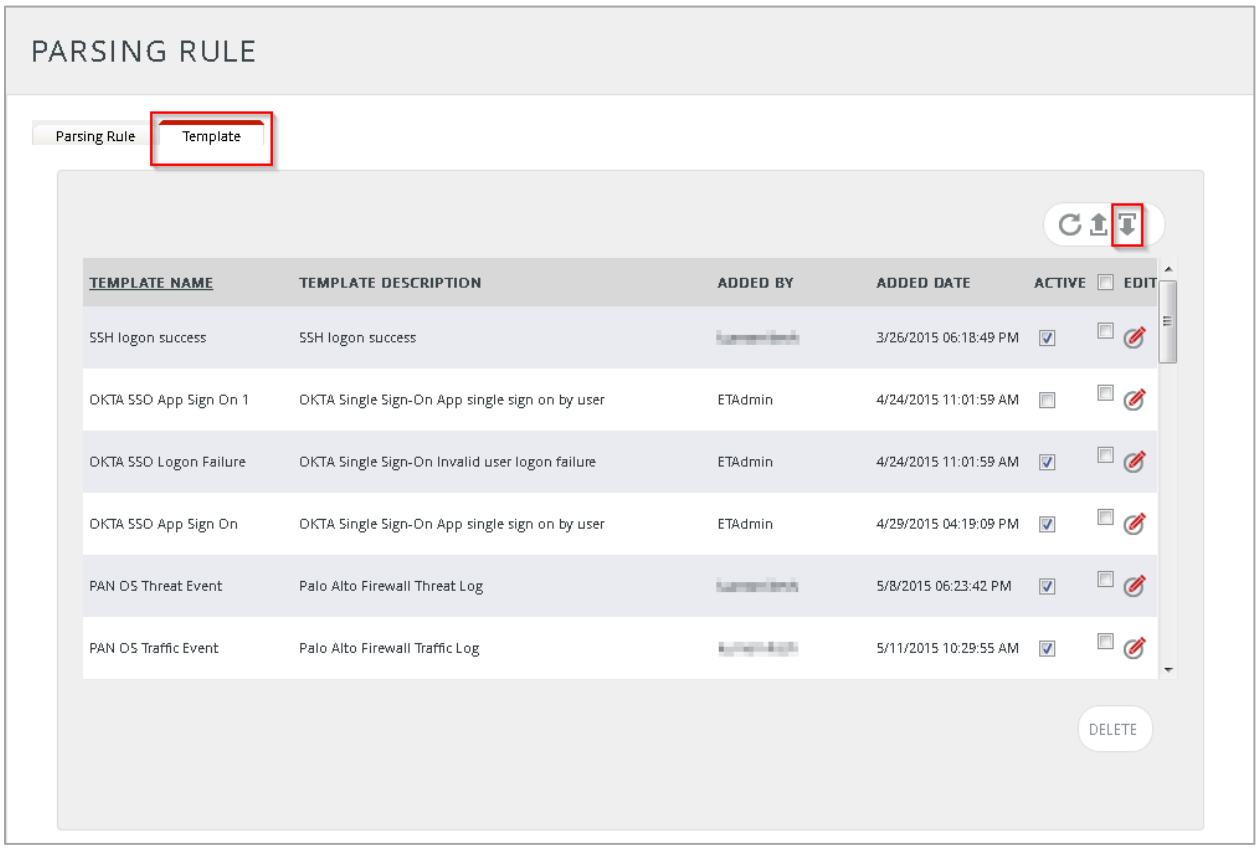

Figure 8

3. Click on **Browse** button.

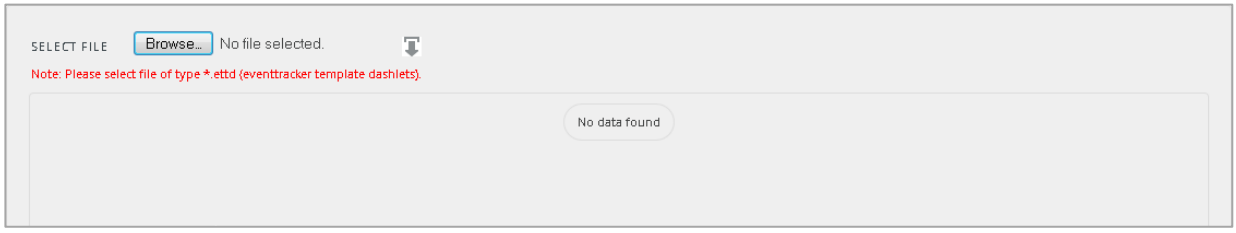

Figure 9

4. Locate applicable **'All HP ProCurve Switch token templates.ettd'** file, and then click the **Open** button.

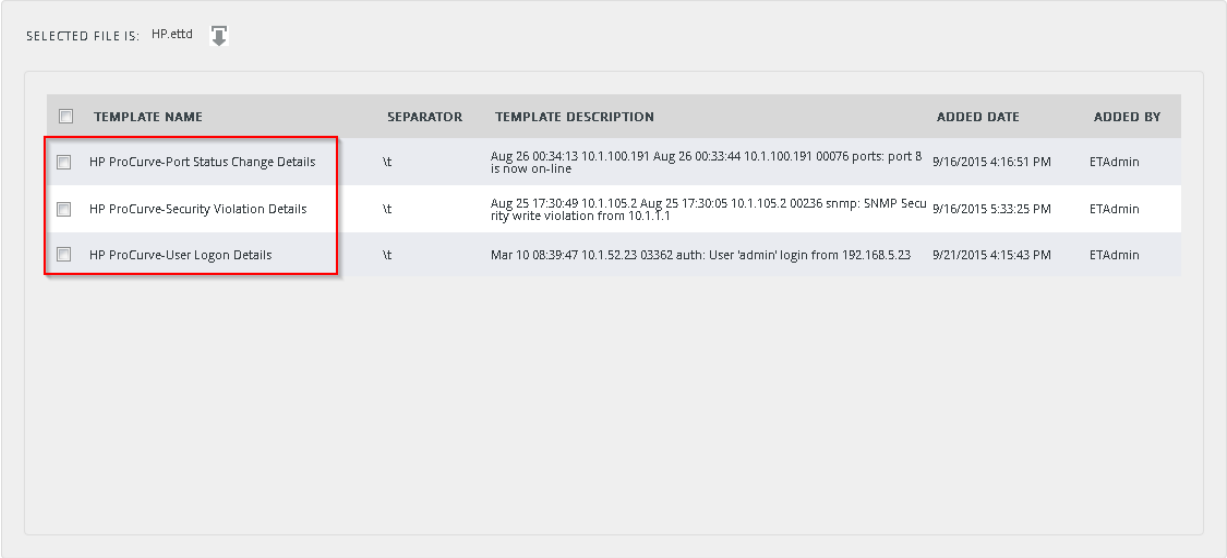

Figure 10

5. Now select the check box and then click on ‘**Import**’ option EventTracker displays success message.

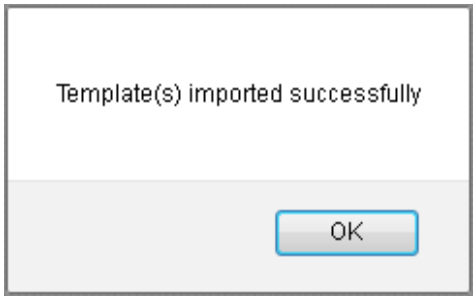

Figure 11

6. Click on **OK** button.

Import Knowledge Object

1. Click the **Admin** menu, and then click **Knowledge Objects**.
2. Click on ‘**Import**’ option.

Figure 12

3. In **IMPORT** pane click on **Browse** button.

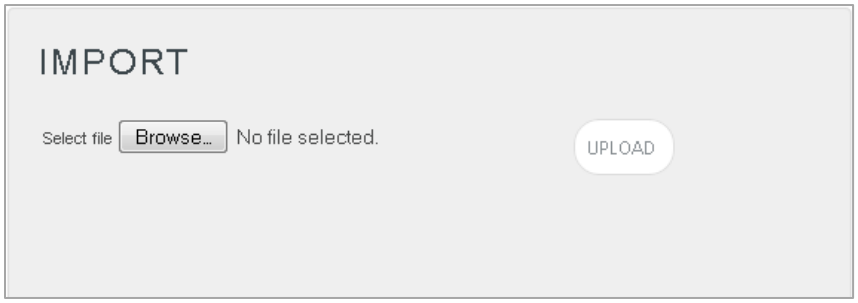

Figure 13

4. Locate applicable **'All HP ProCurve Switch knowledge objects.etko'** file, and then click the **UPLOAD** button.

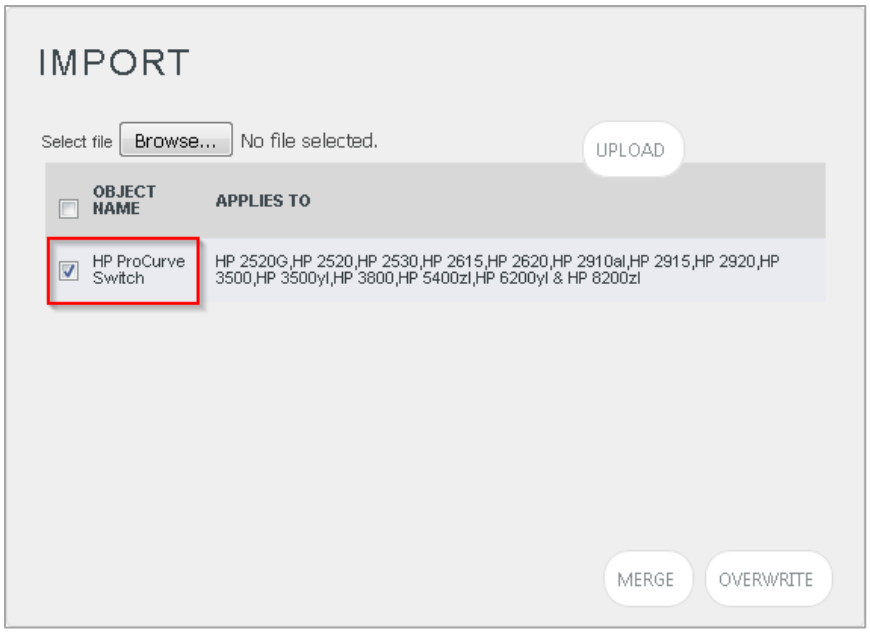

Figure 14

5. Now select the check box and then click on '**MERGE**' option. EventTracker displays success message.

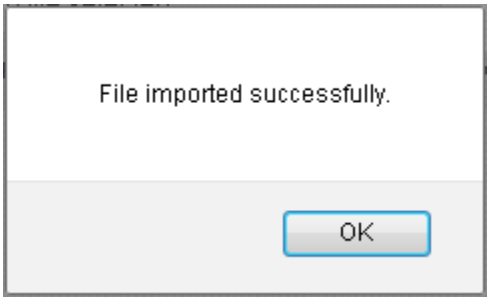

Figure 15

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.

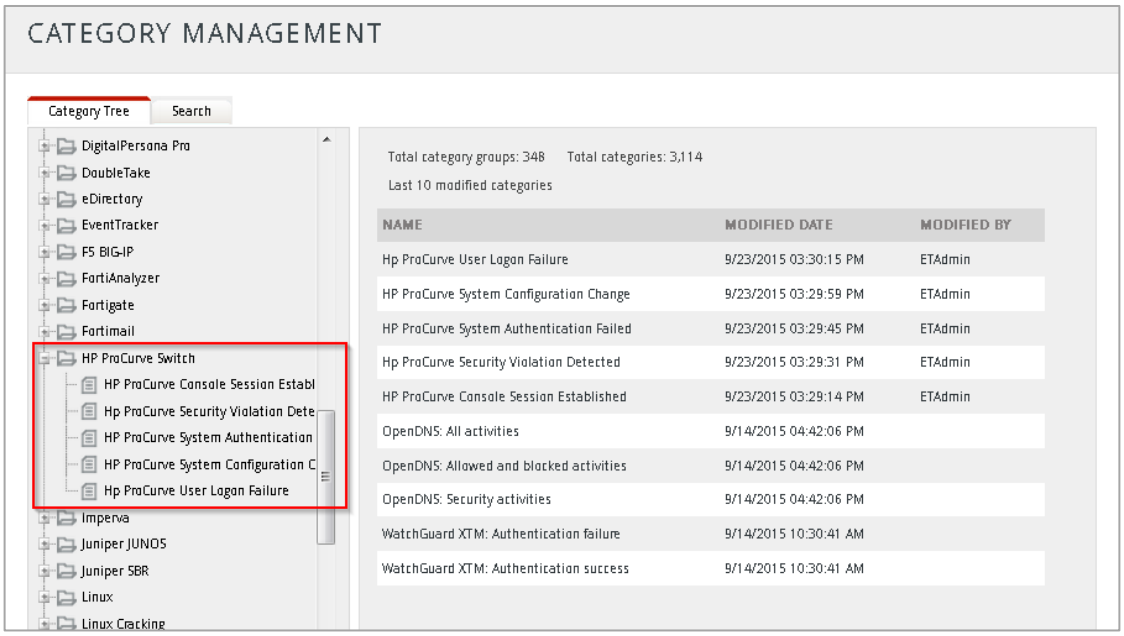

Figure 16

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.

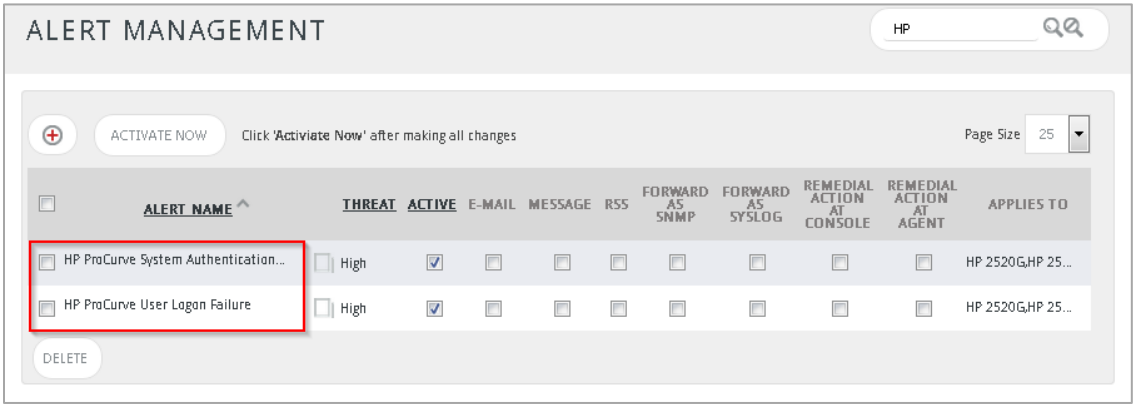

Figure 17

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.

Figure 18

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**.
3. Select **Defined** in report type.
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.

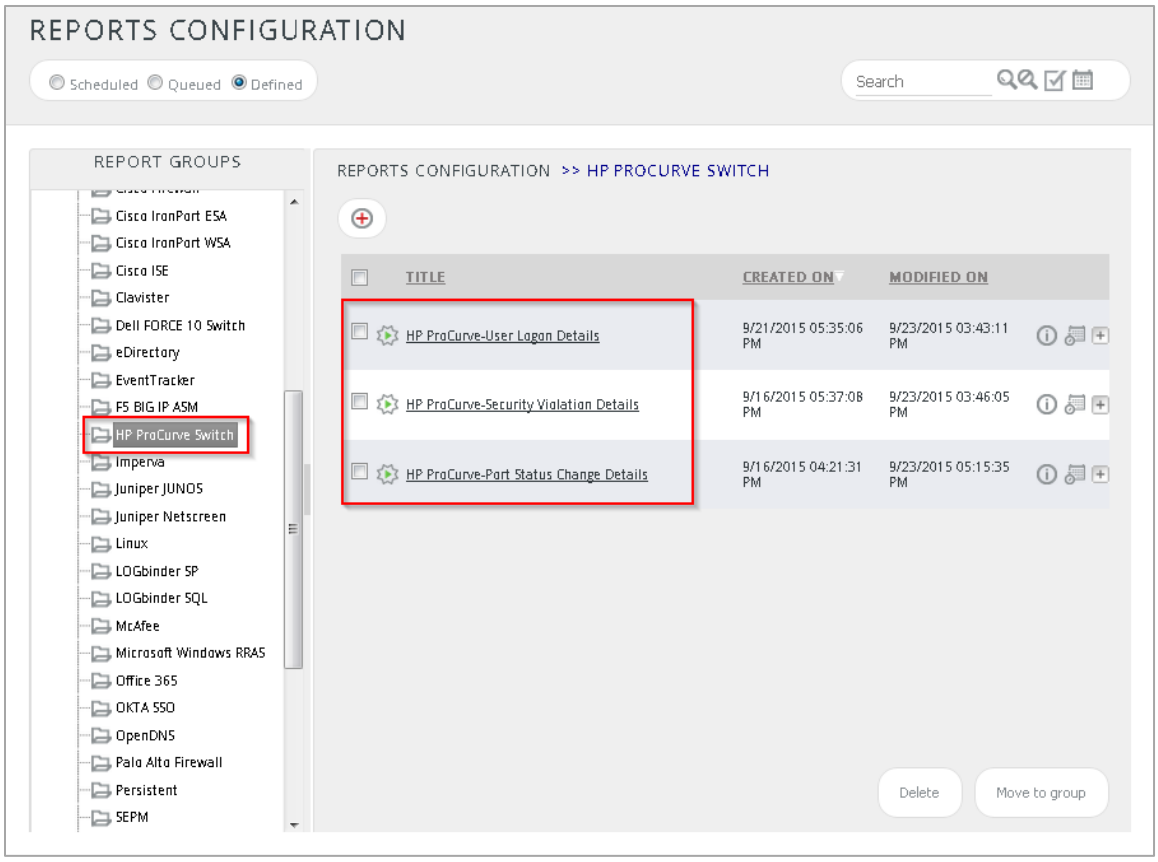

Figure 19

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.

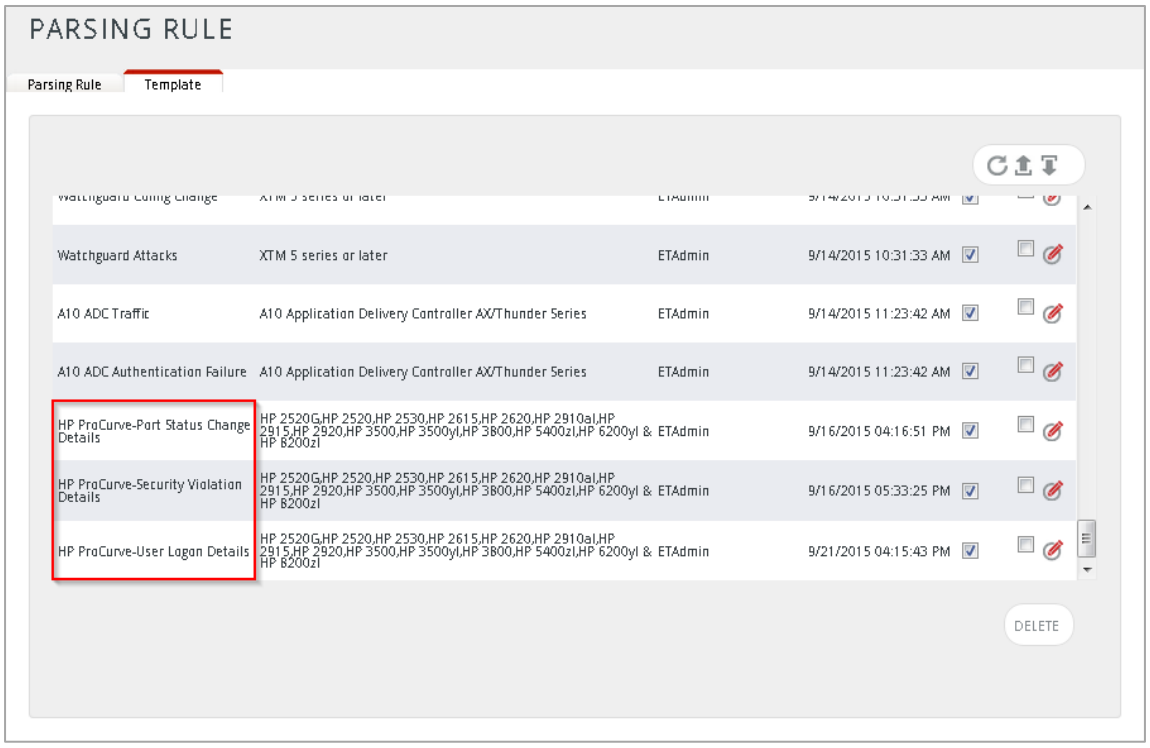

Figure 20

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.

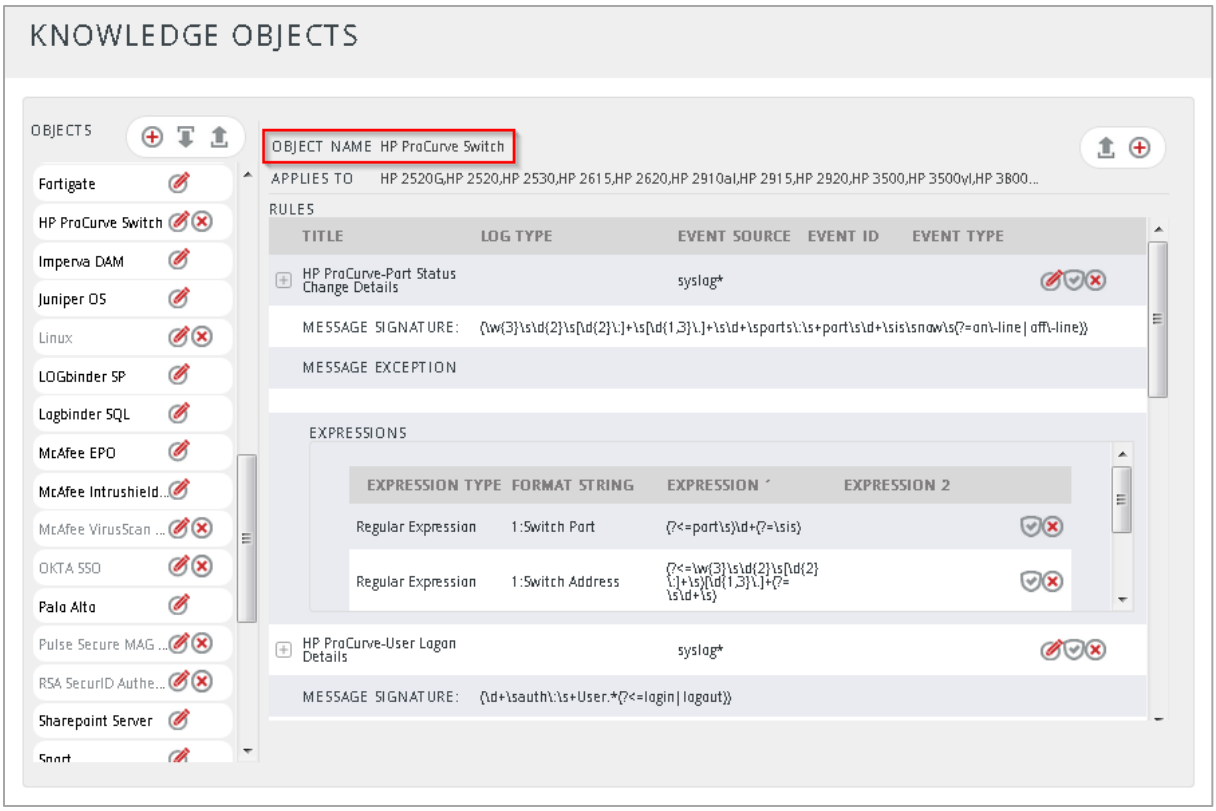

Figure 21

Create Dashboards in EventTracker

Schedule Reports

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

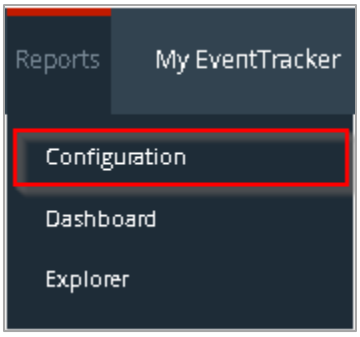

Figure 22

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

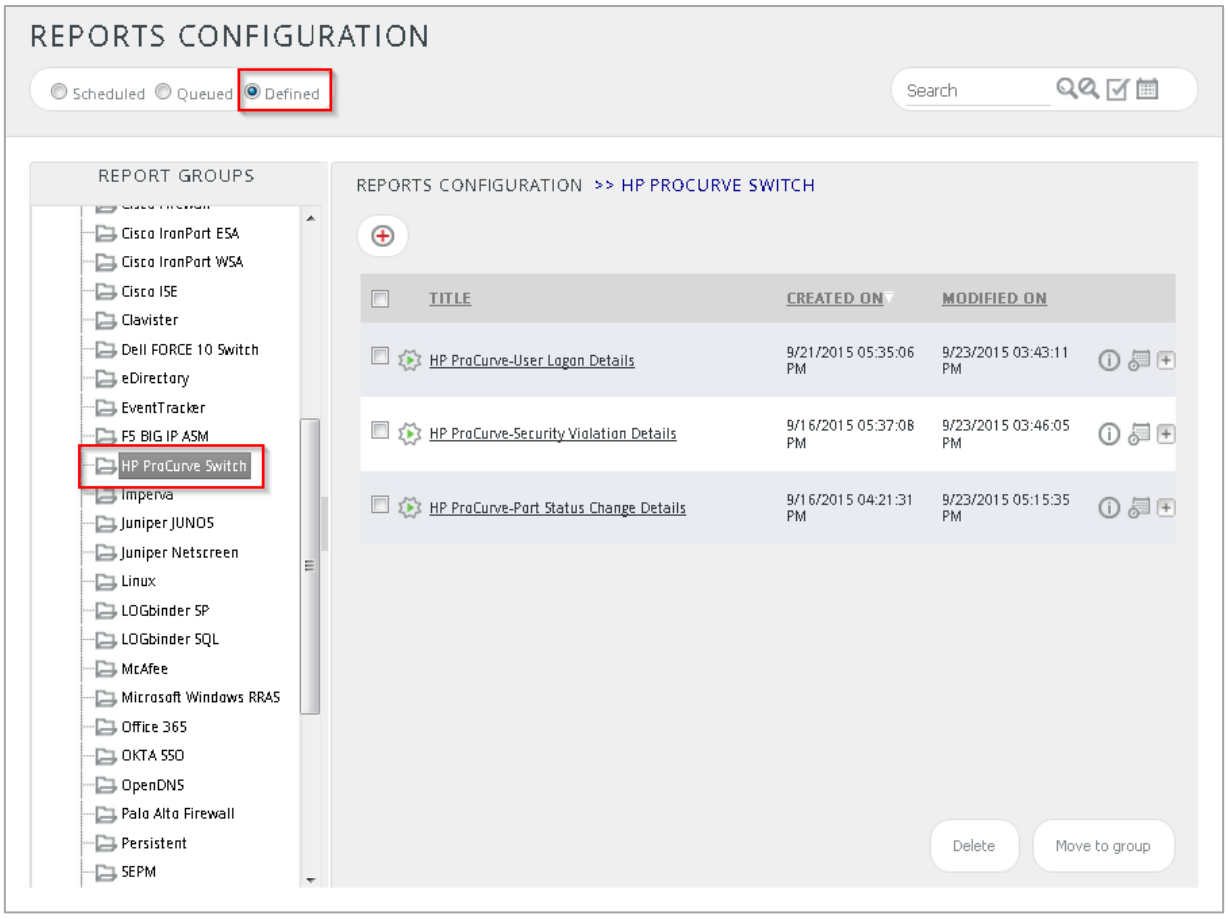

Figure 23

3. Select **HP ProCurve Switch** in report groups. Check **defined** dialog box.
4. Click on '**schedule**'  to plan a report for later execution.

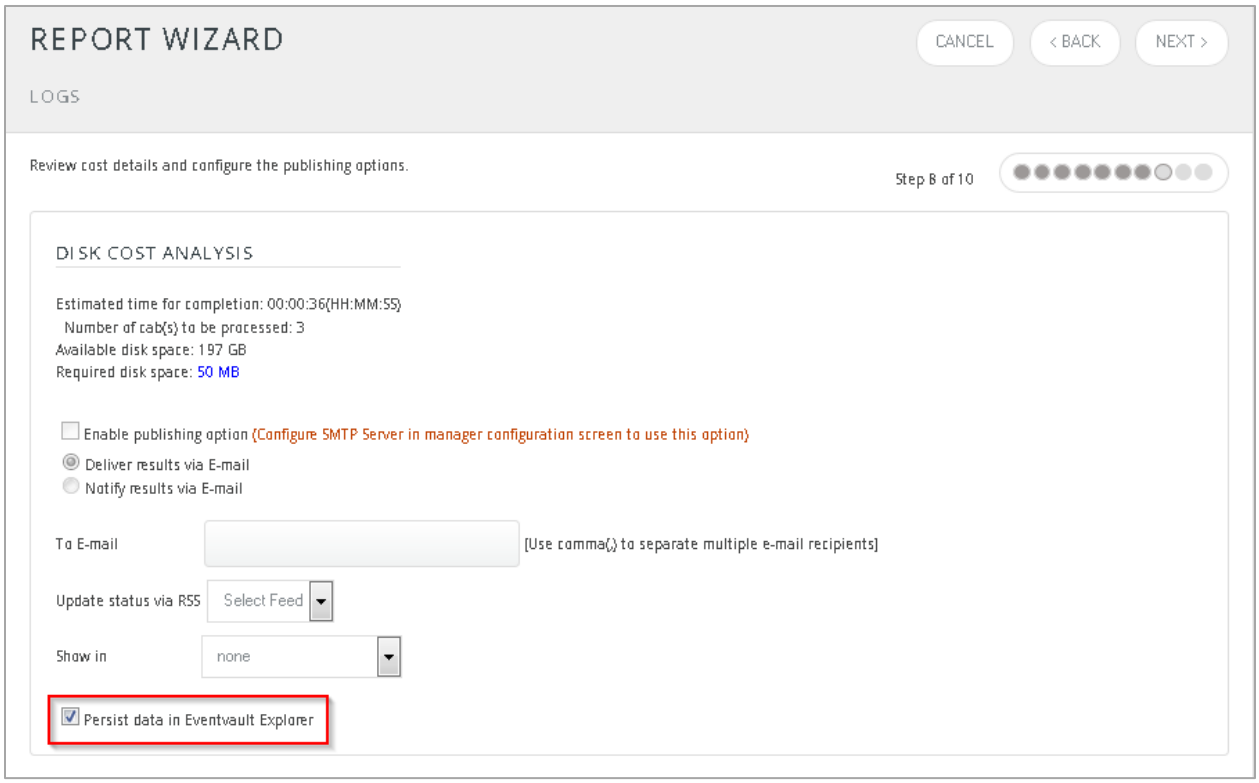

Figure 24

5. Choose appropriate time for report execution and in **Step 8** check **Persist data in Eventvault explorer** box.

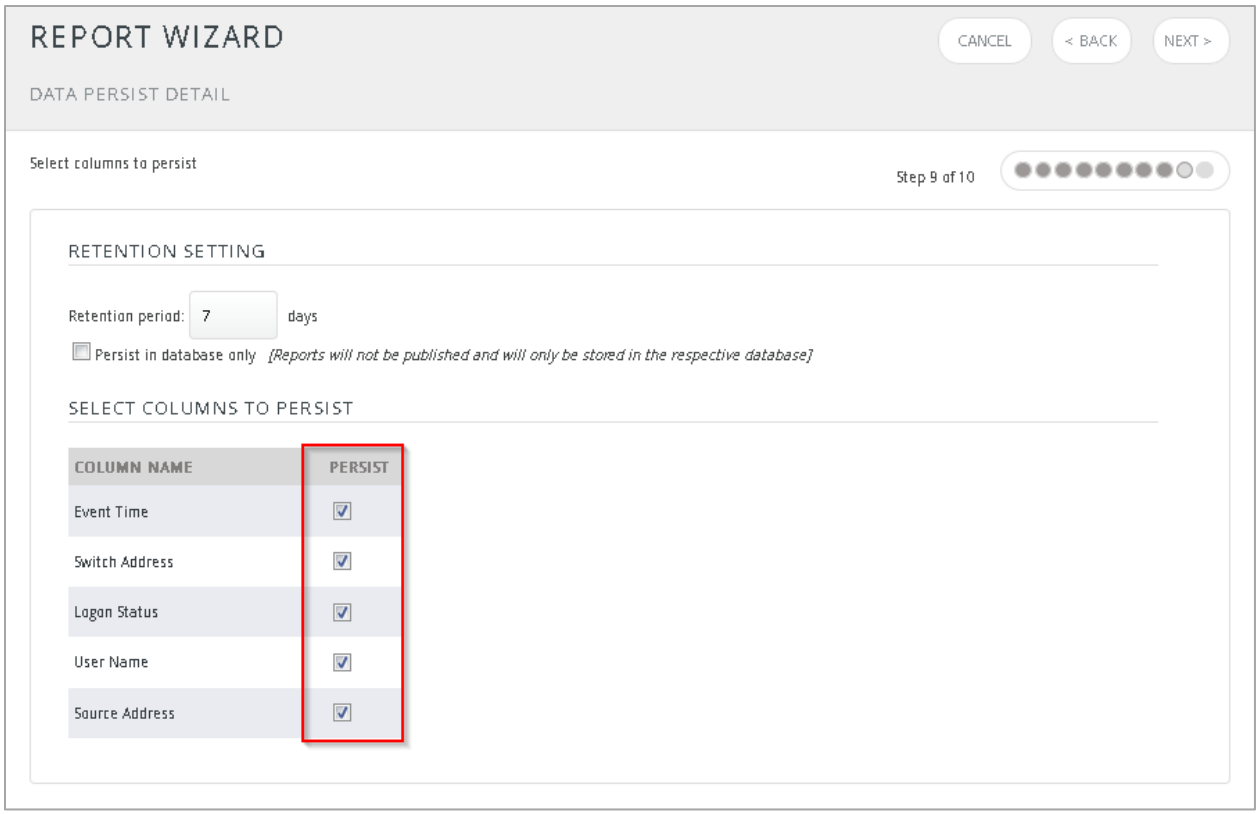

Figure 25

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.

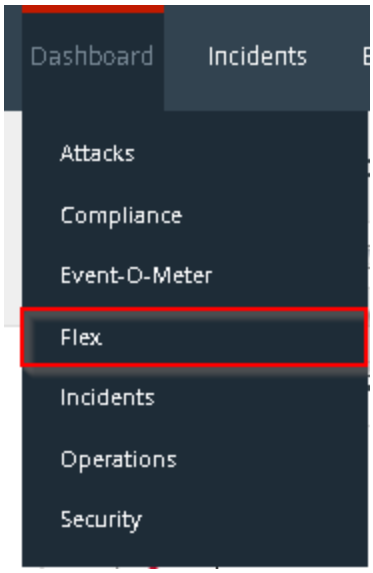

Figure 26

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

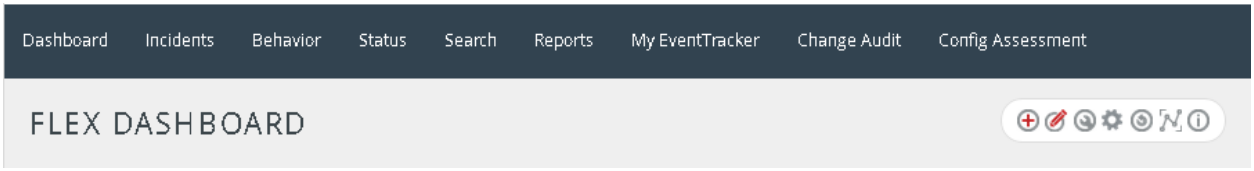

Figure 27

4. Click ⊕ to add a new dashboard.
   Flex Dashboard configuration pane is shown.

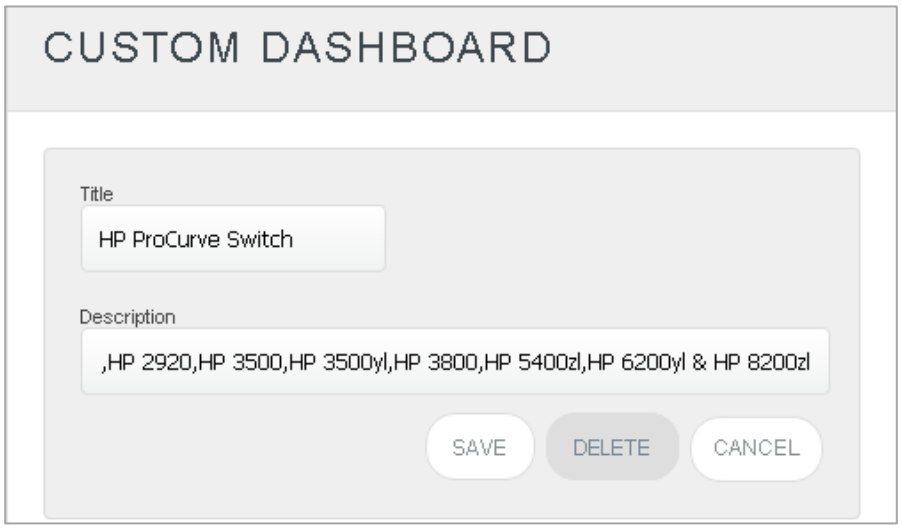

Figure 28

5. Fill fitting title and description and click **Save** button.
6. Click ⚙ to configure a new flex dashlet.
   Widget configuration pane is shown.

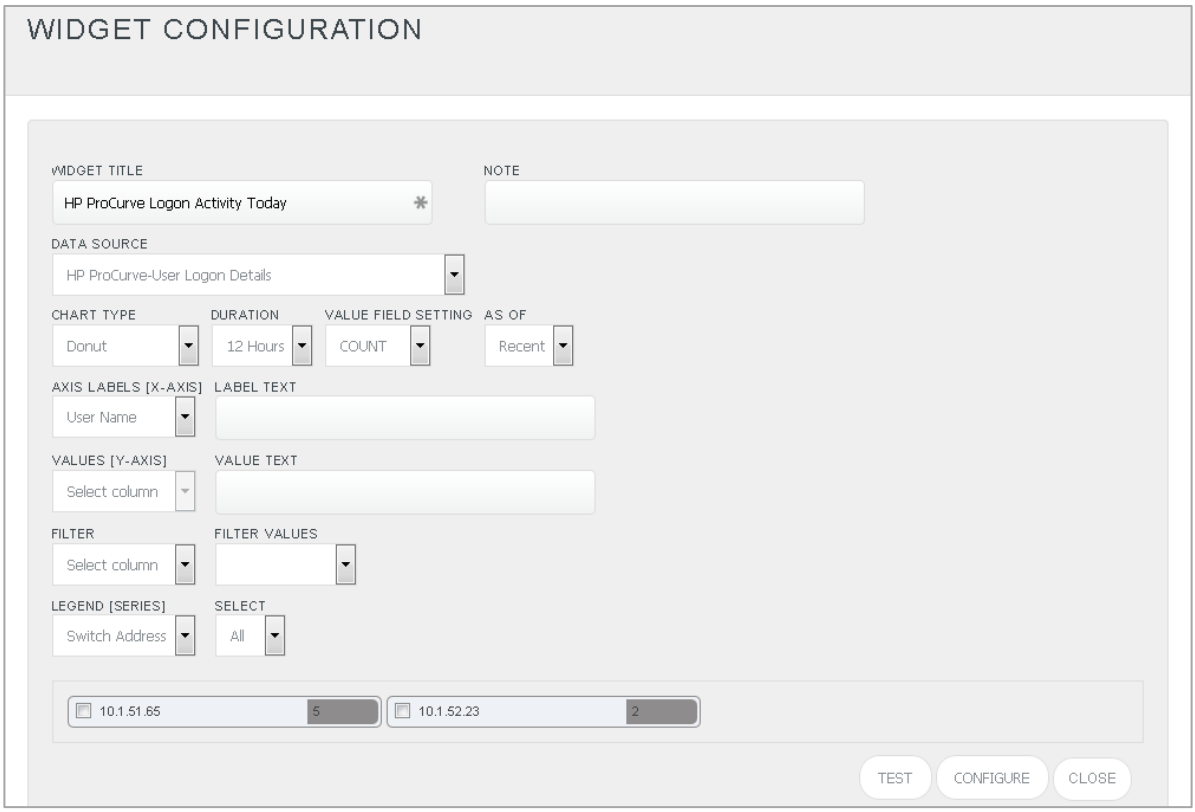

Figure 29

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.

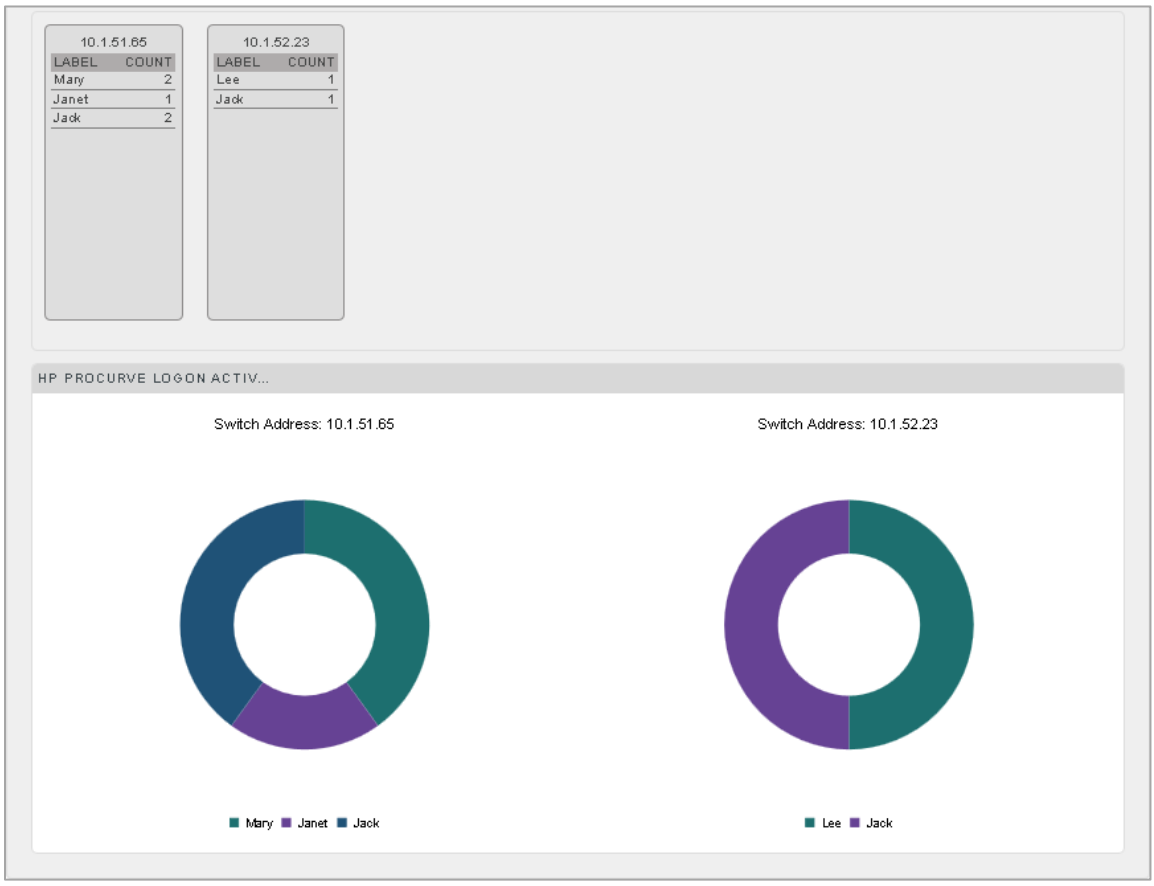

Figure 30

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

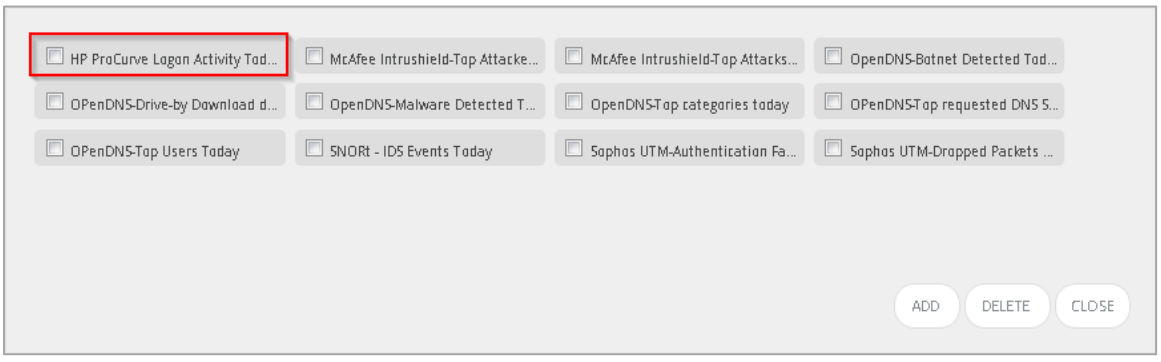

Figure 31

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**

HP ProCurve-User Logon Details

Event Time	Switch Address	Logon Status	User Name	Source Address
Mar 10 08:39:47	10.1.52.23	logout	Jack	192.168.5.23
Mar 10 09:20:51	10.1.52.23	login	Mary	192.168.5.10
Mar 10 10:01:55	10.1.51.65	logout	Kris	192.168.5.3
Mar 10 10:42:59	10.1.52.23	login	Mary	192.168.5.16
Mar 10 11:24:03	10.1.52.23	login	Jack	192.168.5.29
Mar 10 12:05:07	10.1.51.65	login	John	192.168.5.42
Mar 10 12:46:11	10.1.51.65	logout	John	192.168.5.55
Mar 10 13:27:15	10.1.51.65	logout	Jim	192.168.5.68
Mar 10 14:08:19	10.1.51.65	login	Jack	192.168.5.81
Mar 10 11:12:14	10.1.52.23	logout	Mary	192.168.4.21
Mar 10 13:44:41	10.1.52.23	logout	Jack	192.168.3.34
Mar 10 16:17:08	10.1.51.65	logout	John	192.168.4.22
Mar 10 18:49:35	10.1.51.65	logout	Jack	192.168.3.35
Mar 10 21:22:02	10.1.52.23	login	Jack	192.168.4.23
Mar 10 23:54:29	10.1.51.65	login	Jim	192.168.3.36
Mar 11 02:26:56	10.1.51.65	logout	John	192.168.4.24
Mar 11 04:59:23	10.1.51.65	logout	Mary	192.168.3.37
Mar 11 07:31:50	10.1.51.65	login	Mary	192.168.4.25
Mar 11 10:04:17	10.1.52.23	logout	Jack	192.168.3.38
Mar 11 12:36:44	10.1.51.65	login	Kris	192.168.4.26
Mar 11 15:09:11	10.1.52.23	logout	Jane	192.168.3.39
Mar 11 17:41:38	10.1.51.65	logout	Kris	192.168.4.27
Mar 11 20:14:05	10.1.52.23	login	Jack	192.168.3.40

2. HP ProCurve – Security Violation Details

HP ProCurve-Security Violation Details

Event Time	Component Violated	Switch Address	Switch Port	User Name	Source Address
Mar 10 08:39:47	Port	10.1.51.65	21		
Mar 10 09:20:51	snmp	10.1.52.23		EdgeSwitch	10.1.1.2
Mar 10 10:01:55	snmp	10.1.51.65			10.1.1.20
Mar 10 10:42:59	Port	10.1.52.23	19		
Mar 10 11:24:03	snmp	10.1.51.65			10.1.1.11
Mar 10 12:05:07	snmp	10.1.51.65			10.1.1.52
Mar 10 12:46:11	Port	10.1.52.23	21		
Mar 10 13:27:15	snmp	10.1.52.23		EdgeSwitch	10.1.1.2
Mar 10 14:08:19	Port	10.1.52.23			10.1.1.1
Mar 10 11:12:14	Port	10.1.51.65	20		
Mar 10 13:44:41	snmp	10.1.52.23			10.1.1.55
Mar 10 16:17:08	snmp	10.1.51.65			10.1.1.1
Mar 10 18:49:35	Port	10.1.52.23	11		
Mar 10 21:22:02	Port	10.1.51.65		EdgeSwitch	10.1.1.2
Mar 10 23:54:29	snmp	10.1.51.65			10.1.1.1
Mar 11 02:26:56	Port	10.1.52.23	21		
Mar 11 04:59:23	snmp	10.1.51.65		EdgeSwitch	10.1.1.2
Mar 11 07:31:50	snmp	10.1.52.23			10.1.1.41
Mar 11 10:04:17	Port	10.1.52.23	11		
Mar 11 12:36:44	Port	10.1.52.23		EdgeSwitch	10.1.1.2
Mar 11 15:09:11	snmp	10.1.51.65			10.1.1.1
Mar 11 17:41:38	snmp	10.1.51.65	5		
Mar 11 20:14:05	snmp	10.1.51.65		EdgeSwitch	10.1.1.47

3. HP ProCurve – Port Status Change Details

HP ProCurve-Port Status Change Details

Event Time	Switch Address	Switch Port	Port Status
Mar 10 08:39:47	10.1.51.65	41	on-line
Mar 10 09:20:51	10.1.51.65	10	off-line
Mar 10 10:01:55	10.1.51.65	19	off-line
Mar 10 10:42:59	10.1.52.23	41	on-line
Mar 10 11:24:03	10.1.52.23	42	on-line
Mar 10 12:05:07	10.1.51.65	28	off-line
Mar 10 12:46:11	10.1.51.65	37	off-line
Mar 10 13:27:15	10.1.52.23	42	off-line
Mar 10 14:08:19	10.1.51.65	43	on-line
Mar 10 11:12:14	10.1.51.65	46	on-line
Mar 10 13:44:41	10.1.51.65	55	off-line
Mar 10 16:17:08	10.1.51.65	10	on-line
Mar 10 18:49:35	10.1.52.23	17	off-line
Mar 10 21:22:02	10.1.51.65	24	off-line
Mar 10 23:54:29	10.1.52.23	31	on-line
Mar 11 02:26:56	10.1.51.65	38	off-line
Mar 11 04:59:23	10.1.52.23	45	on-line
Mar 11 07:31:50	10.1.52.23	41	off-line
Mar 11 10:04:17	10.1.52.23	25	on-line
Mar 11 12:36:44	10.1.51.65	9	off-line
Mar 11 15:09:11	10.1.52.23	7	on-line
Mar 11 17:41:38	10.1.51.65	23	off-line
Mar 11 20:14:05	10.1.52.23	39	on-line

Sample Dashboards

1. **HP ProCurve Security Violations Today**

Figure 32

2. **HP ProCurve Port Activity Today**

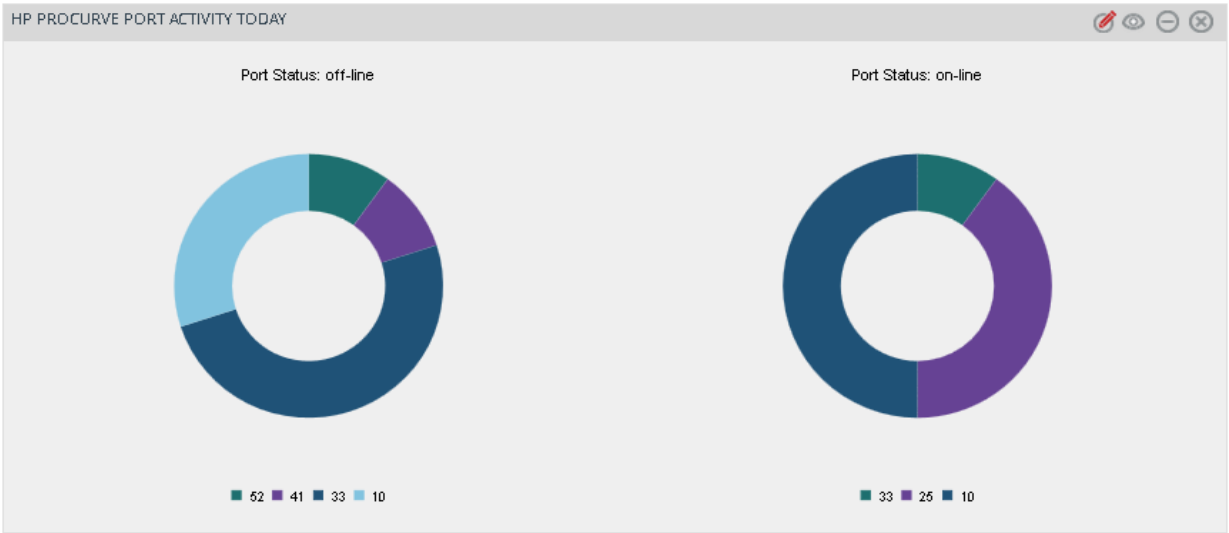

Figure 33

3. HP ProCurve Logon Activity Today

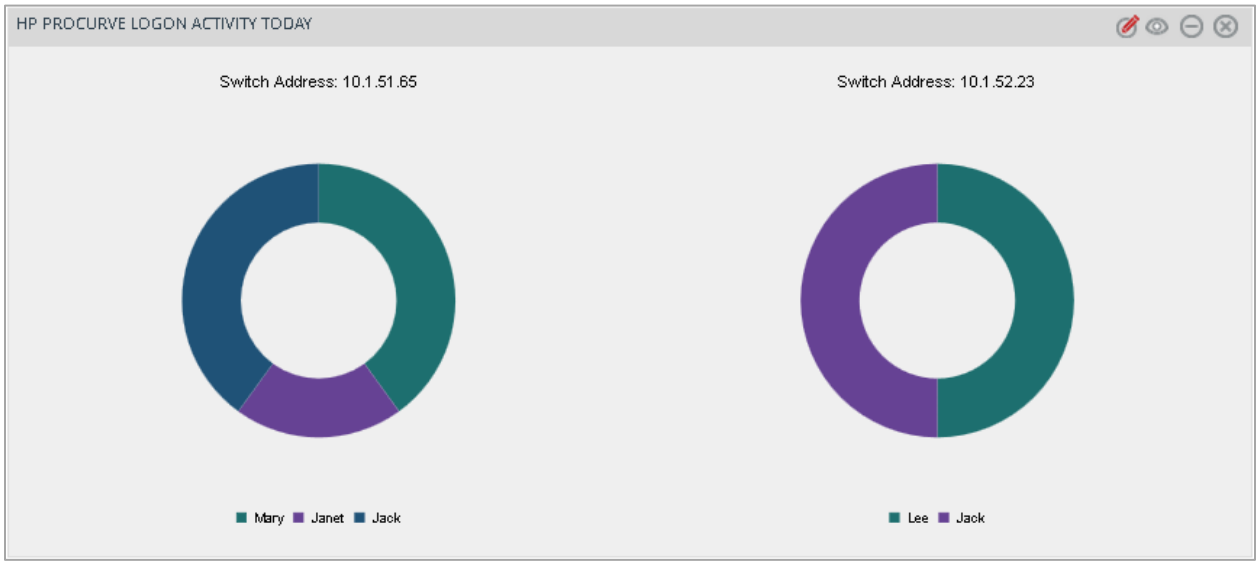

Figure 34