EventTracker

Actionable Security Intelligence

Integrate Dell FORCE10 Switch

Publication Date: December 15, 2016

Abstract

This guide provides instructions to configure **Dell FORCE10 Switch** to send the syslog events to EventTracker.

Scope

The configurations detailed in this guide are consistent with **EventTracker** version 7.X and later, and **Dell FORCE10 Switch** and later.

Audience

Dell FORCE10 Switch users, who wish to forward syslog messages to EventTracker manager.

Table of Contents

Overview

The **Dell FORCE10 Switchs** are used as both distribution switches for large networks and core switches for smaller networks. Dell FORCE10 switches run the FTOS (the Force10 Operating System).

EventTracker supports **Dell FORCE10 Switch** and it forwards the syslog messages to EventTracker manager. EventTracker generates the alerts, reports and dashlets for critical logs.

Prerequisites

Prior to configuring the Dell FORCE10 Switch and EventTracker, ensure that you meet the following prerequisites:

- EventTracker 7.x and later should be installed.
- Console access to Dell FORCE10 Switch device.

Configuration

In **Dell FORCE10 Switch** logging is enabled by default and log messages are sent to configured syslog servers.

Configure Syslog logging

To enable and configure syslog servers for **Dell FORCE10 Switch**.

1. Enter Privileged Exec mode and type the command.
   FTOS>enable

2. Enter Global Config mode and type the command.
   FTOS#config

3. Enter the syslog server's address where logging messages will be sent.
   FTOS#logging 10.11.129.100

4. Type this command to enable console logging.
   FTOS#logging console

5. Type this command to copy system:running-config to nvram:startup-config.
   FTOS#do write

EventTracker Knowledge Pack

Once Dell FORCE10 Switch events are enabled and Dell FORCE10 Switch events are received in EventTracker. Alerts, reports and dashlets can be configured in EventTracker.

The following knowledge packs are available in EventTracker to support Dell FORCE10 Switch monitoring.

Categories

- **Dell FORCE10 Switch: User logoff -** This category based report provides information related to user logout.
- **Dell FORCE10 Switch: User logon success -** This category based report provides information related to user logon success.
- **Dell FORCE10 Switch: Authentication success -** This category based report provides information related to authentication success.
- **Dell FORCE10 Switch: Authentication failure -** This category based report provides information related to authentication failure.
- **Dell FORCE10 Switch: Interface status -** This category based report provides information related to interface status.
- **Dell FORCE10 Switch: Port channel details -** This category based report provides information related to port channel details.

Alerts

- **Dell FORCE10 Switch: User logon success -** This alert is generated when user logon succeeds.
- **Dell FORCE10 Switch: User logoff -** This alert is generated when user logoffs.
- **Dell FORCE10 Switch: Authentication failure -** This alert is generated when user authentication fails.

Import Dell FORCE10 Switch Knowledge Pack into EventTracker

1. Launch **EventTracker Control Panel**.
2. Double click **Export Import Utility**, and then click **Import** tab.
   Import **Category/Alert/Tokens/ Flex Reports/Behavior Rules** as given below.

Import Category

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

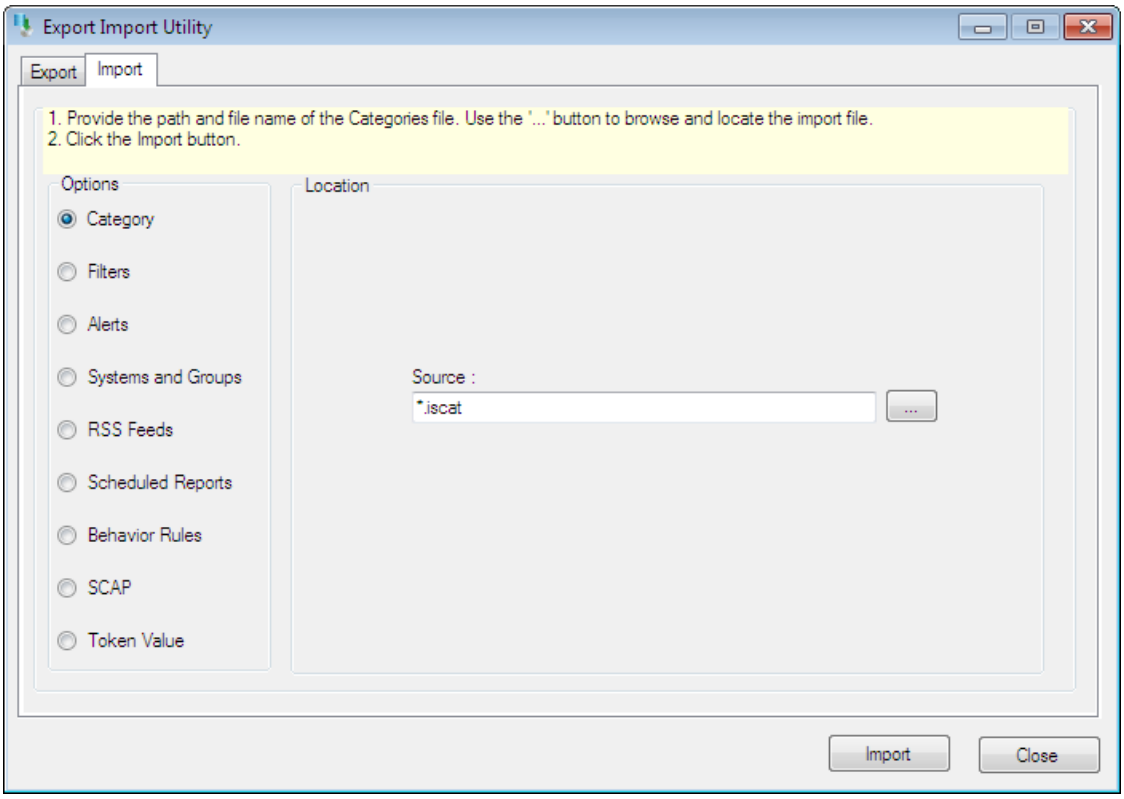

Figure 1

2. Locate **Dell FORCE10 Switch.iscat** file, and then click the **Open** button.
3. To import categories, click the **Import** button.
   EventTracker displays success message.

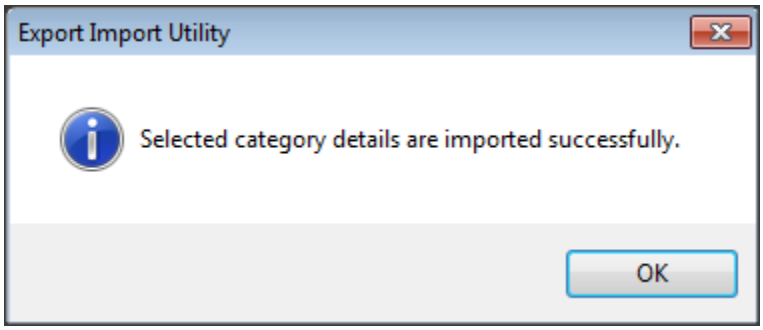

Figure 2

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

Import Alerts

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

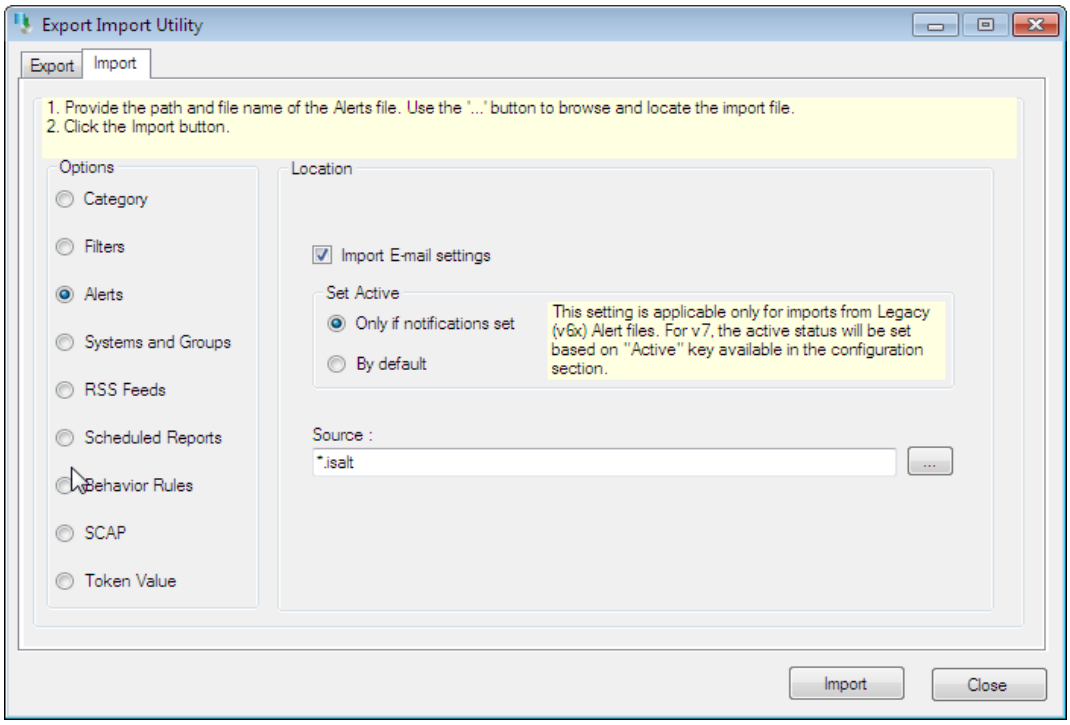

Figure 3

2. Locate **Dell FORCE10 Switch.isalt** file, and then click the **Open** button.

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

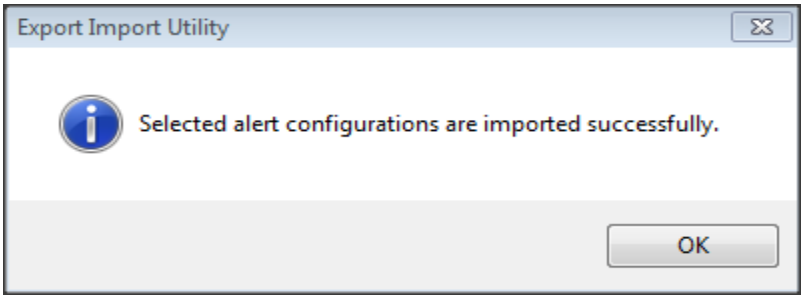

Figure 4

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

Import Token Value

1. Click **Token Value** option, and then click the browse ... button.
2. Locate **Dell FORCE10 Switch.istoken** file, and then click the **Open** button.

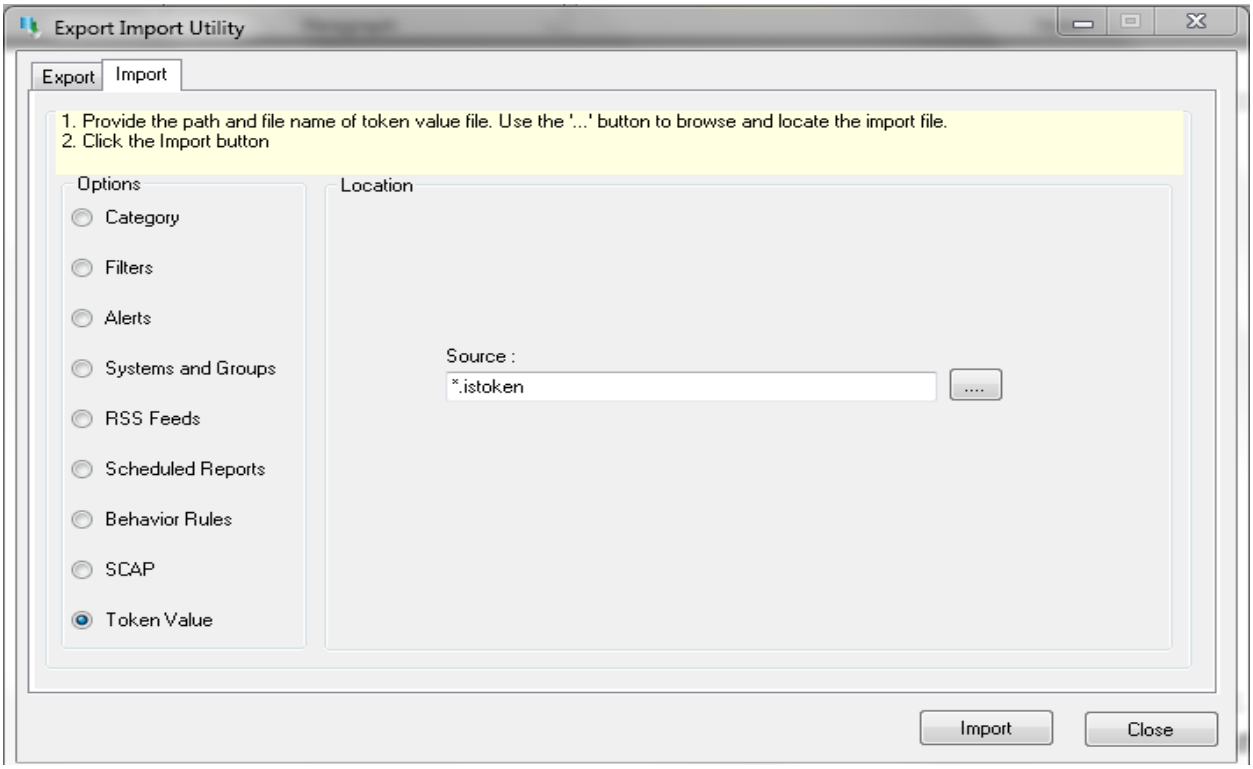

Figure 5

3. To import token value, click the **Import** button.
   EventTracker displays success message.

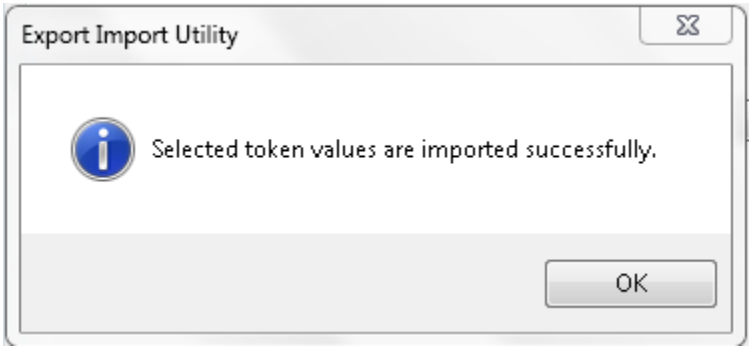

Figure 6

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 **Dell FORCE10 Switch.issch** file, and then click the **Open** button.

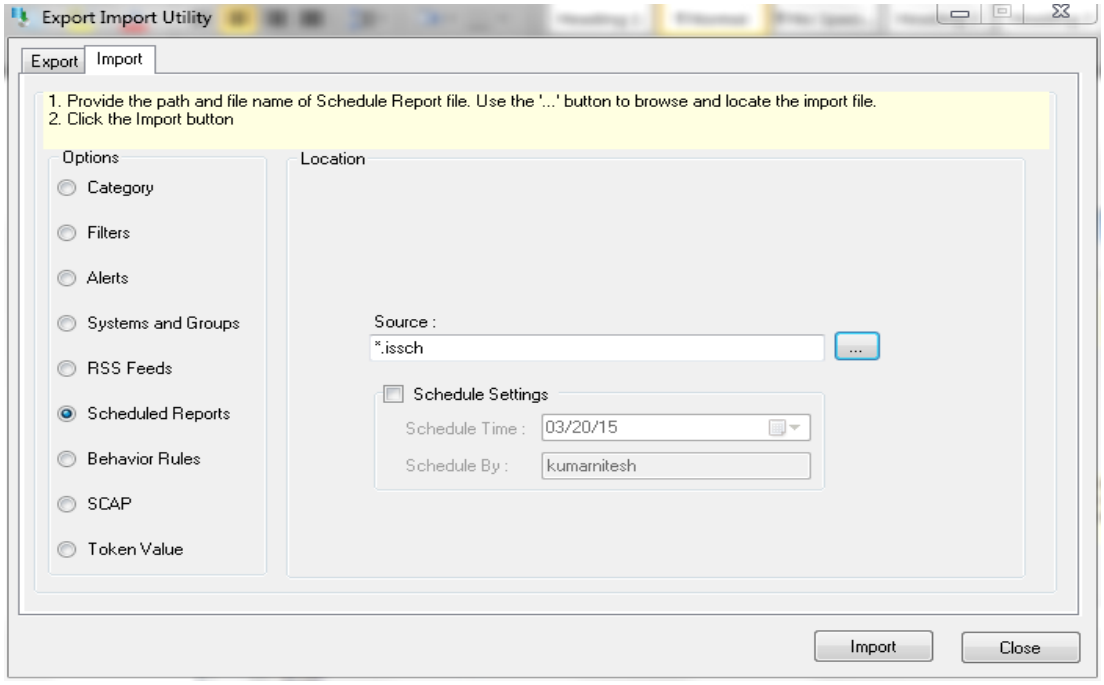

Figure 7

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

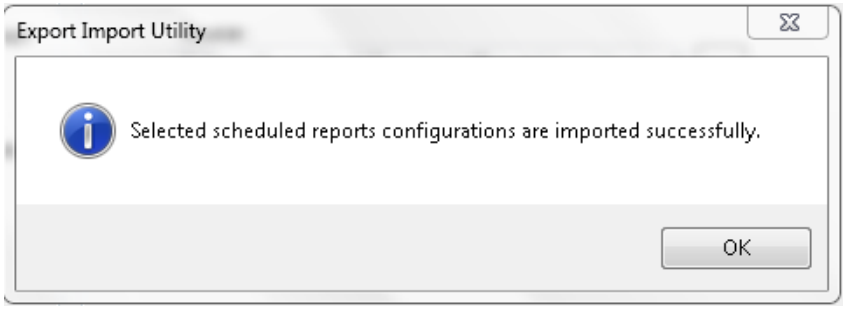

Figure 8

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

Import Behavior Rules

1. Click **Behavior Rules** option, and then click the browse ... button.
2. Locate **Dell FORCE10 Switch.isrule** file, and then click the **Open** button.

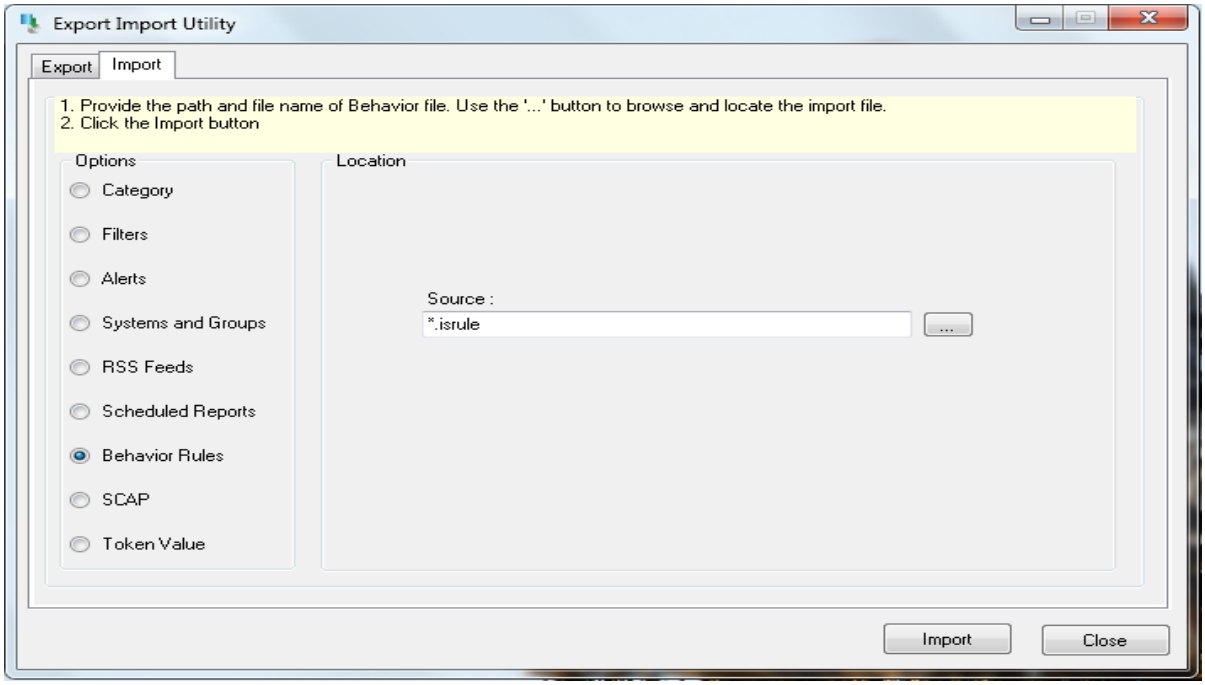

Figure 9

3. To import behavior rules, click the **Import** button.
   EventTracker displays success message.

Figure 10

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

Verify Dell FORCE10 Switch Knowledge Pack in EventTracker

Verify Dell FORCE10 Switch Categories

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Category**.
3. In **Category Tree** to view imported categories, scroll down and expand **Dell FORCE10 Switch** group folder to view the imported categories.

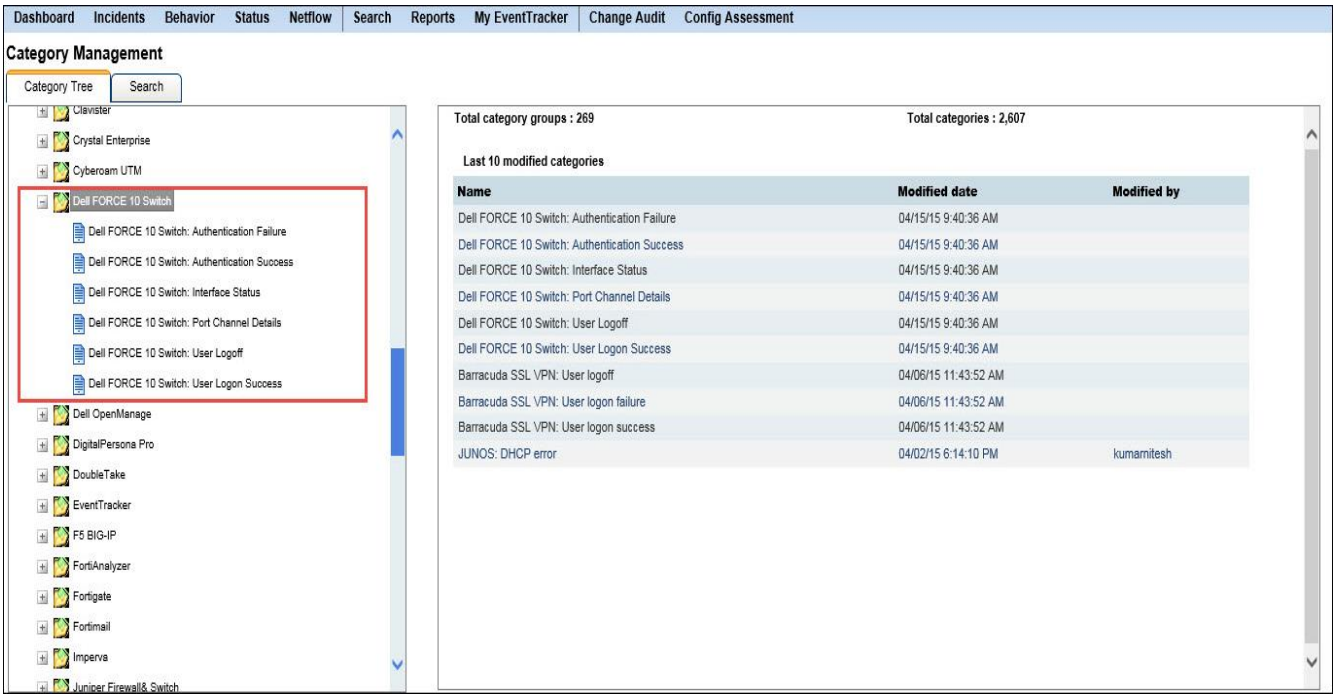

Figure 11

Verify Dell FORCE10 Switch Alerts

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Alerts**.
3. In **Search** field, type **'Dell FORCE10 Switch'**, and then click the **Go** button.
   Alert Management page will display all the imported Dell FORCE10 Switch alerts.

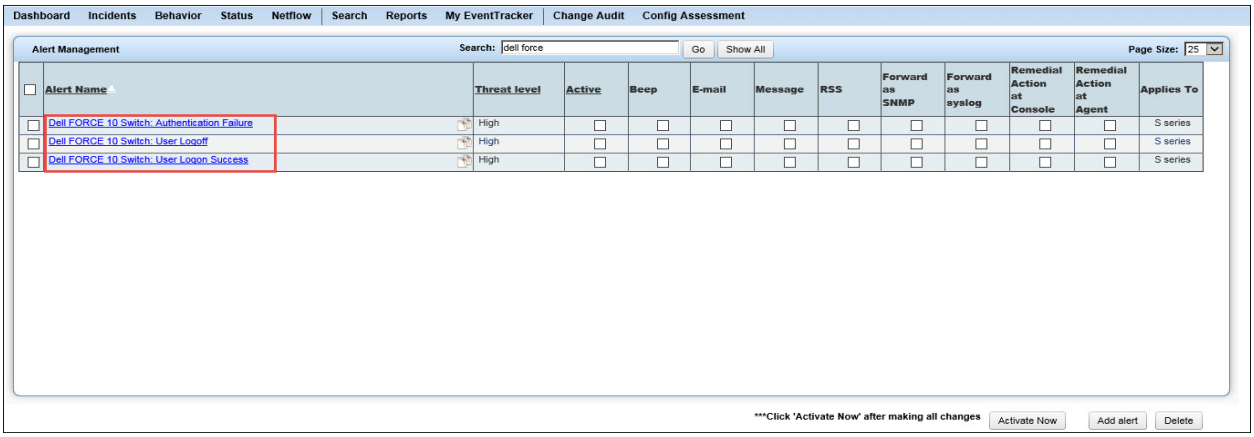

Figure 12

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

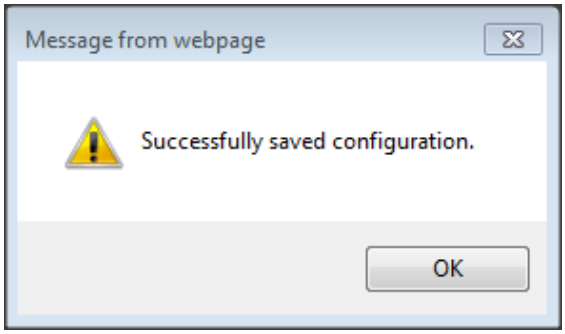

Figure 13

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.

Verify Dell FORCE10 Switch Token Values

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Parsing Rules**.
3. In **Token Value Group Tree** to view imported token values, scroll down and click **Dell FORCE10 Switch** group folder. Token values are displayed in the token value pane.

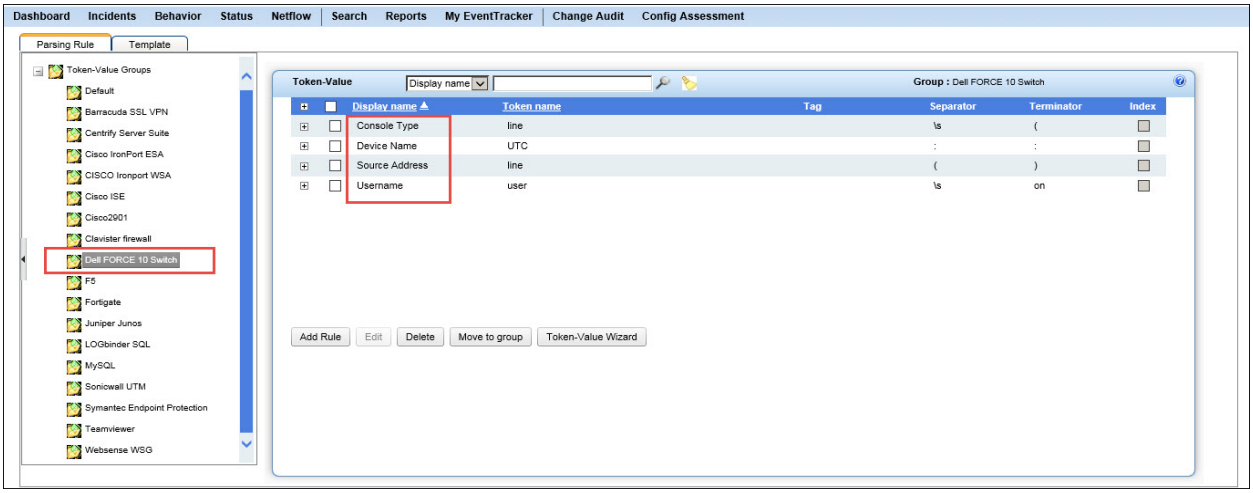

Figure 14

Verify Dell FORCE10 Switch 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 **Dell FORCE10 Switch** group folder. Scheduled Reports are displayed in the Reports configuration pane.

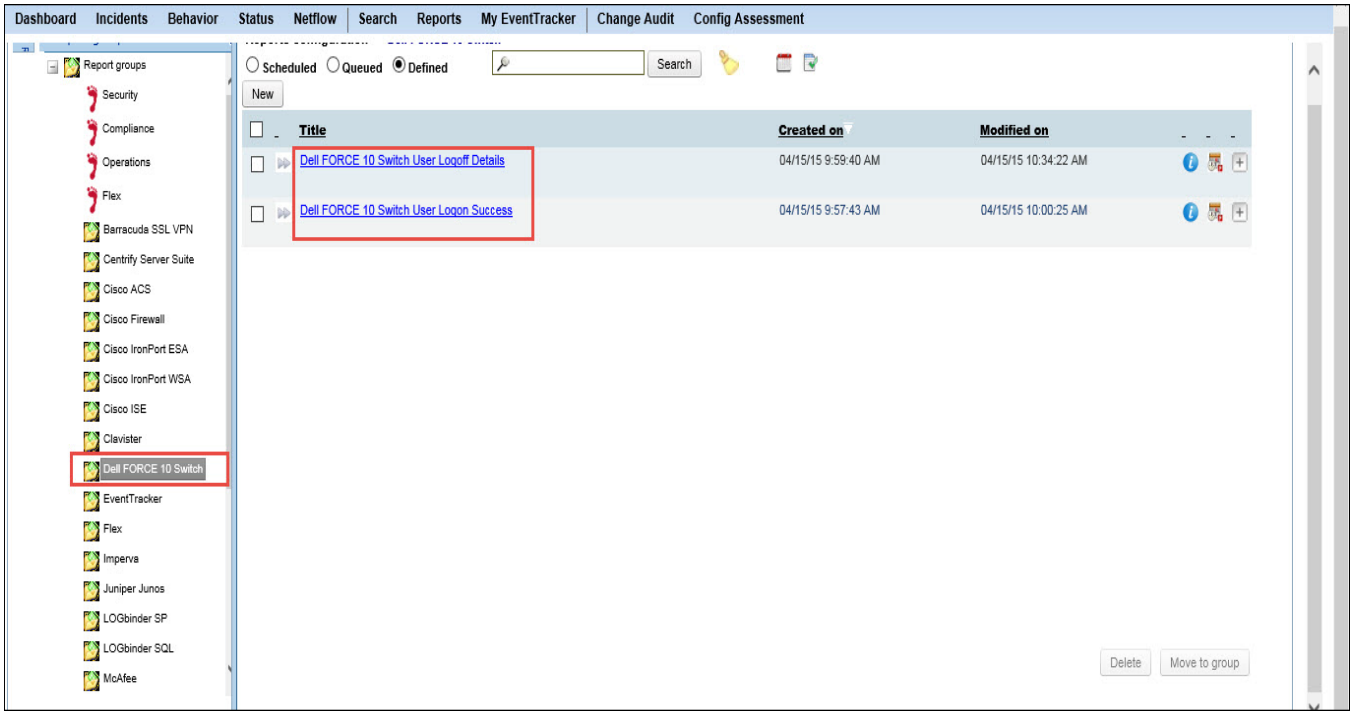

Figure 15

Verify Dell FORCE10 Switch Behavior Rules

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Behavior rules**.
3. **Behavior Rules** window will be displayed, where EventTracker displays the imported behavior rules.

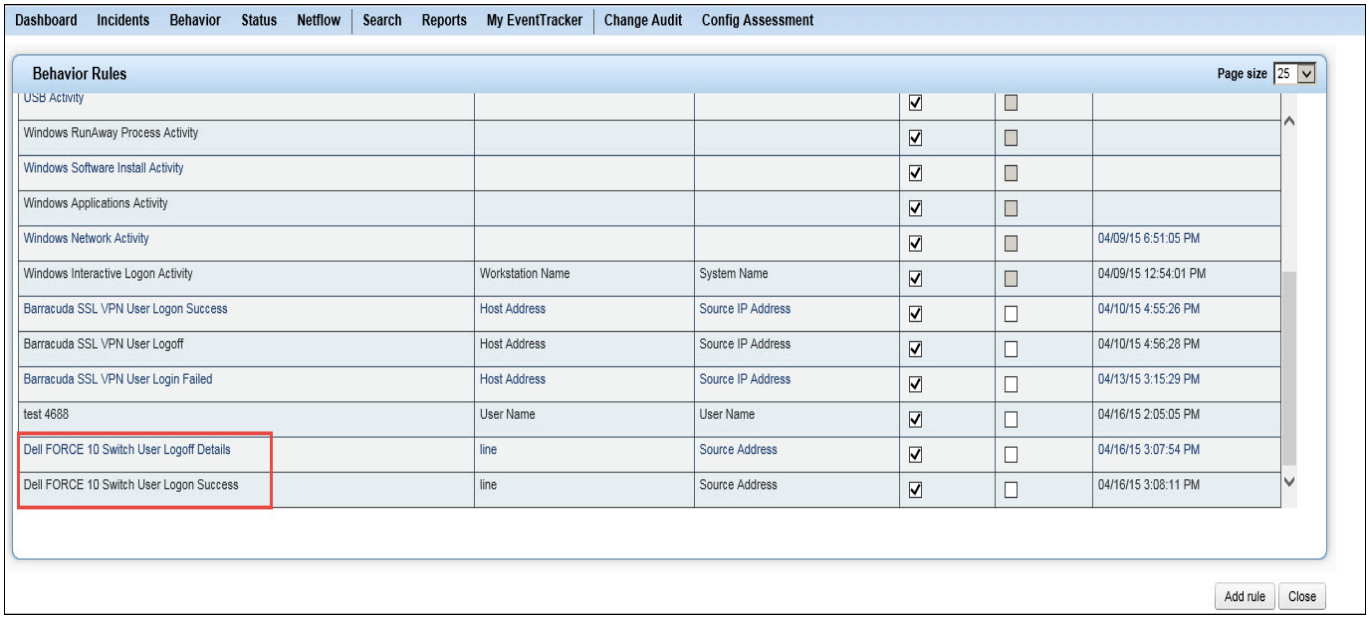

Figure 16

Configure Dell FORCE10 Switch dashboards

Configure Behavior Dashboard

1. Logon to **EventTracker Enterprise**.
2. Select **Behavior**, and then select **Security**. Click on the Down double arrow from the **Security** tab.
3. Select **Customize**.
   Available Dashlets window displays.

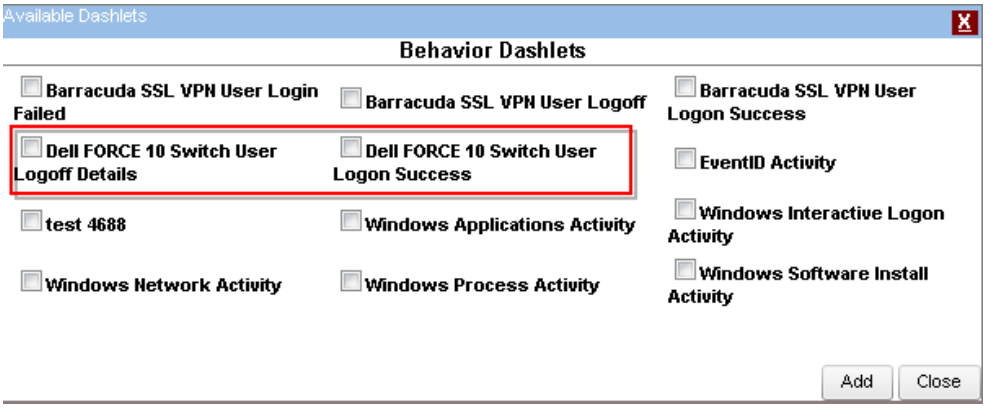

Figure 17

4. Select required behavior dashlets and click **Add**.

   Behavior dashboard will be displayed as shown below.

Figure 18

Click on available chart to view behavior details.

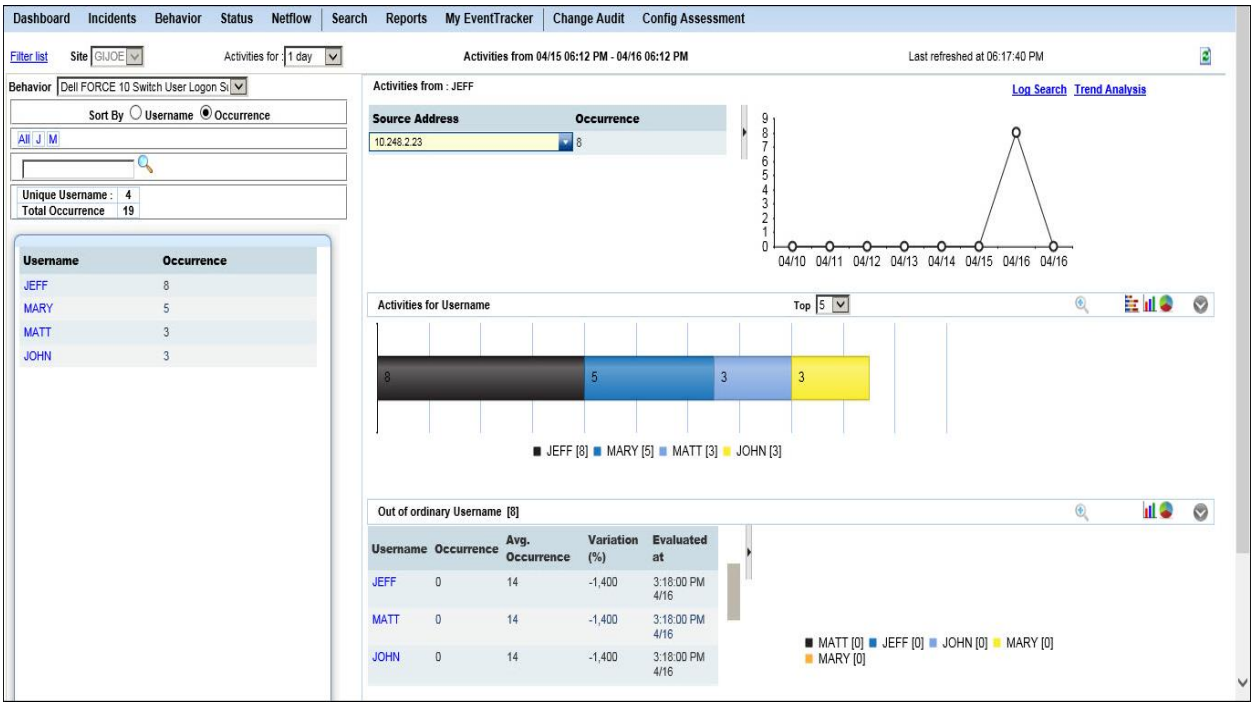

Figure 19

Configure Flex Dashboard

1. Logon to **EventTracker Enterprise**.
2. Select **Reports** then click **Configuration**.
3. Select **Dell FORCE10 Switch from the Report group** pane. Select **Defined** option.
4. Click on schedule icon of the report which you want to configure.
5. When you reach the **Step 8 of 10** Select **Persist data in Eventvault Explorer** option.
   Wait until your report gets generated.
6. Once your report gets generated, Click **Dashboard** select **Flex**
7. Click on the Down double arrow from the **security** tab then select configure.
8. EventTracker displays **Keyword flex** window where the generated reports are shown in **Available reports** section.
9. Expand the report and select the column name which you want to see in flex dashboard.
   For example: Please see the image below.

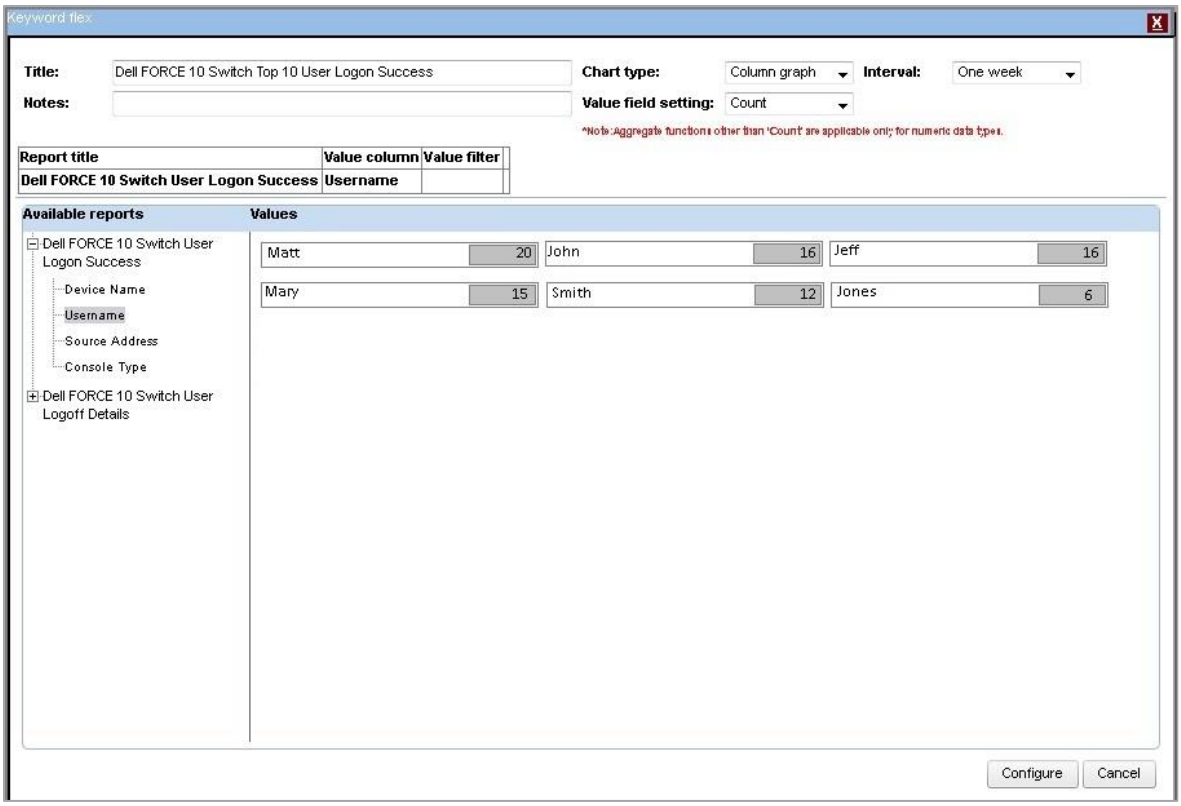

Figure 20

10. Give appropriate title name and notes.
11. Click **Configure**.
12. Again select **Flex** tab then click on the icon, select **Customize.**

    Available Dashlets window displays.

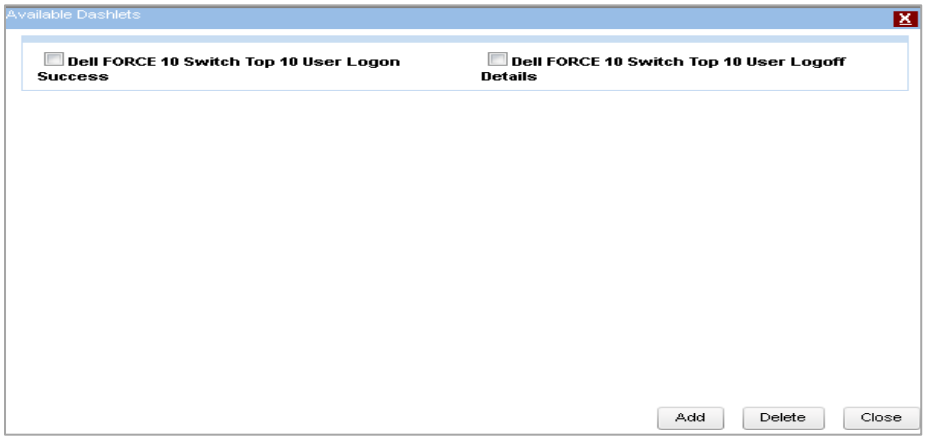

Figure 21

13. Select required flex dashlets and click **Add**.

Flex dashboard will be displayed as shown below.

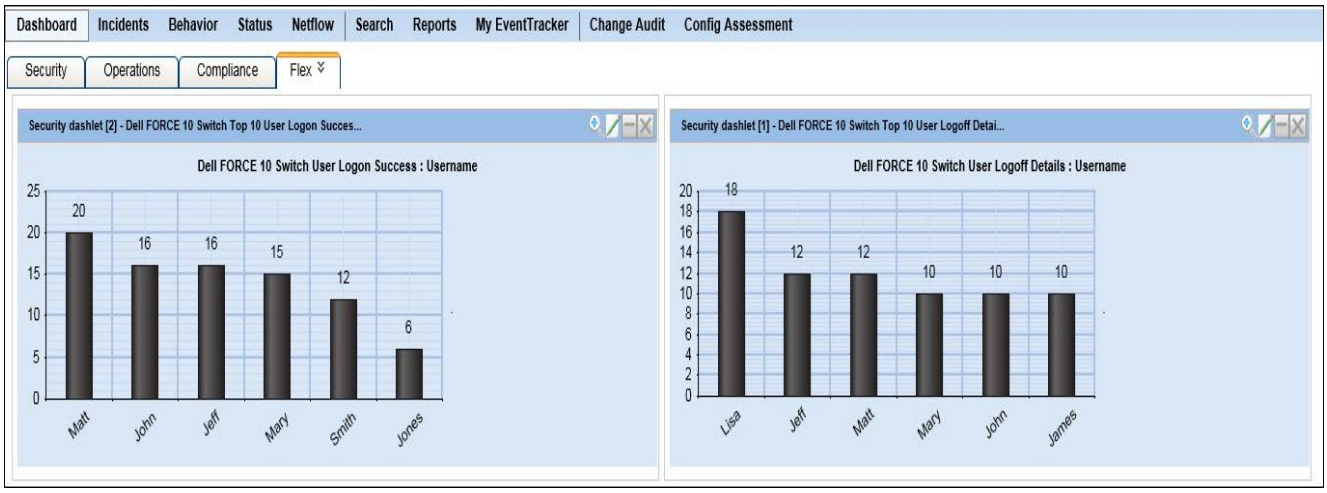

Figure 22

Sample Flex reports for Dell FORCE10 Switch using EventTracker

A. Flex Report for Dell FORCE10 Switch **User Logon Success**.

Dell FORCE 10 Switch User Logon Success

LogTime	Device Name	Username	Source Address	Console Type
04/15/2015 10:29:10 AM	CHIRPY-02	Jeff	10.248.2.23	vty0
04/14/2015 11:19:17 AM	CHIRPY-02	John	10.248.2.20	vty0
04/13/2015 10:29:20 AM	CHIRPY-02	Jeff	10.248.2.23	vty0
04/15/2015 04:12:20 PM	CHIRPY-01	Matt	10.248.2.27	console
04/13/2015 01:14:45 AM	CHIRPY-01	Mary	10.248.2.30	console
04/12/2015 04:12:52 AM	CHIRPY-01	Matt	10.248.2.27	console
04/15/2015 10:33:17 PM	CHIRPY-02	John	10.248.2.20	vty0
04/14/2015 11:41:13 PM	CHIRPY-01	Mary	10.248.2.30	console
04/13/2015 07:12:41 AM	CHIRPY-02	Jeff	10.248.2.23	vty0
04/15/2015 02:33:44 AM	CHIRPY-01	Matt	10.248.2.27	console
04/12/2015 07:12:51 PM	CHIRPY-02	John	10.248.2.20	vty0
04/15/2015 10:29:10 AM	CHIRPY-02	John	10.248.2.20	vty0
04/14/2015 06:22:11 AM	CHIRPY-02	John	10.248.2.20	vty0
04/15/2015 07:00:40 AM	CHIRPY-01	Mary	10.248.2.30	console
04/12/2015 03:12:30 PM	CHIRPY-02	Jeff	10.248.2.23	vty0
04/15/2015 10:19:33 PM	CHIRPY-01	Mary	10.248.2.30	console
04/15/2015 05:43:38 AM	CHIRPY-01	Matt	10.248.2.27	console
04/15/2015 07:37:49 PM	CHIRPY-01	Matt	10.248.2.27	console
04/13/2015 05:05:11 PM	CHIRPY-02	Jeff	10.248.2.23	vty0
04/15/2015 11:33:20 AM	CHIRPY-01	Mary	10.248.2.30	console
04/13/2015 07:23:10 PM	CHIRPY-02	John	10.248.2.20	vty0
04/15/2015 02:42:30 AM	CHIRPY-01	Matt	10.248.2.27	console
04/14/2015 09:13:52 PM	CHIRPY-02	Jeff	10.248.2.23	vty0
04/15/2015 07:22:30 AM	CHIRPY-02	Jeff	10.248.2.23	vty0
04/14/2015 05:14:13 PM	CHIRPY-02	John	10.248.2.20	vty0
04/15/2015 11:19:18 AM	CHIRPY-02	John	10.248.2.20	vty0

B. Flex Report for Dell FORCE10 Switch **User Logoff**.

Dell FORCE 10 Switch User Logoff Details

LogTime	Device Name	Username	Source Address	Console Type
04/15/2015 10:29:10 AM	CHIRPY-02	Jeff	10.248.2.23	vty0
04/14/2015 11:19:17 AM	CHIRPY-02	Jeff	10.248.2.23	vty0
04/13/2015 10:29:20 AM	CHIRPY-01	Mary	10.248.2.30	console
04/15/2015 04:12:20 PM	CHIRPY-02	John	10.248.2.20	vty0
04/13/2015 01:14:45 AM	CHIRPY-01	Matt	10.248.2.27	console
04/12/2015 04:12:52 AM	CHIRPY-02	Jeff	10.248.2.23	vty0
04/15/2015 10:33:17 PM	CHIRPY-01	Mary	10.248.2.30	console
04/14/2015 11:41:13 PM	CHIRPY-01	Matt	10.248.2.27	console
04/13/2015 07:12:41 AM	CHIRPY-01	Matt	10.248.2.27	console
04/15/2015 02:33:44 AM	CHIRPY-01	Matt	10.248.2.27	console
04/12/2015 07:12:51 PM	CHIRPY-01	Mary	10.248.2.30	console
04/15/2015 10:29:10 AM	CHIRPY-02	John	10.248.2.20	vty0
04/14/2015 06:22:11 AM	CHIRPY-02	Jeff	10.248.2.23	vty0
04/15/2015 07:00:40 AM	CHIRPY-02	John	10.248.2.20	vty0
04/12/2015 03:12:30 PM	CHIRPY-01	Matt	10.248.2.27	console
04/15/2015 10:19:33 PM	CHIRPY-02	John	10.248.2.20	vty0
04/15/2015 05:43:38 AM	CHIRPY-02	John	10.248.2.20	vty0
04/15/2015 07:37:49 PM	CHIRPY-01	Mary	10.248.2.30	console
04/13/2015 05:05:11 PM	CHIRPY-01	Mary	10.248.2.30	console
04/15/2015 11:33:20 AM	CHIRPY-02	John	10.248.2.20	vty0
04/13/2015 07:23:10 PM	CHIRPY-01	Matt	10.248.2.27	console
04/15/2015 02:42:30 AM	CHIRPY-02	Jeff	10.248.2.23	vty0
04/14/2015 09:13:52 PM	CHIRPY-02	John	10.248.2.20	vty0
04/15/2015 07:22:30 AM	CHIRPY-01	Matt	10.248.2.27	console
04/14/2015 05:14:13 PM	CHIRPY-02	Jeff	10.248.2.23	vty0
04/15/2015 11:19:18 AM	CHIRPY-01	Mary	10.248.2.30	console

C. Flex Report for Dell FORCE10 Switch **Authentication Success**.

Dell FORCE 10 Switch-Authentication Success

LogTime	Device Name	Source Address	Console Type
03/26/2015 04:51:52 PM	CHIRPY-01	10.5.1.45	vty0
03/24/2015 03:52:34 PM	CHIRPY-01	10.5.1.45	vty0
03/25/2015 09:14:14 PM	CHIRPY-02	10.5.1.69	vty0
03/26/2015 04:54:54 PM	CHIRPY-01	10.5.1.70	console
03/26/2015 07:24:04 PM	CHIRPY-02	10.5.1.84	console
03/26/2015 07:04:05 PM	CHIRPY-01	10.5.1.45	vty0
03/27/2015 05:04:54 PM	CHIRPY-02	10.5.1.69	vty0
03/26/2015 04:52:54 PM	CHIRPY-02	10.5.1.84	console
03/26/2015 04:54:24 PM	CHIRPY-02	10.5.1.84	console
03/26/2015 10:04:05 PM	CHIRPY-01	10.5.1.70	console
03/22/2015 08:51:04 PM	CHIRPY-02	10.5.1.69	vty0
03/27/2015 06:33:34 PM	CHIRPY-02	10.5.1.84	console
03/16/2015 08:09:53 PM	CHIRPY-02	10.5.1.69	vty0
03/26/2015 04:54:54 PM	CHIRPY-01	10.5.1.70	console
03/27/2015 06:51:43 PM	CHIRPY-02	10.5.1.84	console
03/21/2015 08:51:56 PM	CHIRPY-01	10.5.1.45	vty0
03/21/2015 04:53:34 PM	CHIRPY-02	10.5.1.69	vty0
03/22/2015 04:14:24 PM	CHIRPY-01	10.5.1.70	console
03/22/2015 08:51:23 PM	CHIRPY-01	10.5.1.70	console
03/22/2015 04:52:14 PM	CHIRPY-01	10.5.1.45	vty0
03/26/2015 04:51:54 PM	CHIRPY-01	10.5.1.70	console
03/22/2015 04:54:22 PM	CHIRPY-01	10.5.1.70	console
03/26/2015 04:34:14 PM	CHIRPY-02	10.5.1.84	console
03/16/2015 06:05:59 PM	CHIRPY-02	10.5.1.69	vty0
03/23/2015 07:34:23 PM	CHIRPY-02	10.5.1.84	console