

Integrate Dell PowerConnect Switch

EventTracker v8.x and above

Abstract

This guide provides instructions to forward syslog generated by Dell PowerConnect N20XX series to EventTracker. EventTracker is configured to collect and parse these logs to generate reports.

Scope

The configurations detailed in this guide are consistent with **EventTracker Enterprise** version 8.x and later, and **Dell PowerConnect N20XX series**.

Audience

IT Admins, Dell PowerConnect switch administrators and EventTracker users who wish to forward logs to EventTracker Manager and monitor events using EventTracker Enterprise.

The information contained in this document represents the current view of EventTracker. on the issues discussed as of the date of publication. Because EventTracker must respond to changing market conditions, it should not be interpreted to be a commitment on the part of EventTracker, and EventTracker cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. EventTracker 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 EventTracker, if its content is unaltered, nothing is added to the content and credit to EventTracker is provided.

EventTracker 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 EventTracker, 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.

© 2018 EventTracker Security LLC. 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
- Overview 3
- Prerequisites 3
- Configure Dell PowerConnect to forward logs to EventTracker 3
 - Configuration to enable Syslog forwarding 3
- EventTracker Knowledge Pack (KP) 5
 - Categories 5
 - Alerts 5
 - Flex Reports 5
- Import Dell PowerConnect Knowledge Pack into EventTracker 7
 - Import Categories 8
 - Import Alerts 9
 - Import Knowledge Objects 10
 - Import Token Templates 11
 - Import Flex Reports 12
- Verify Knowledge Pack in EventTracker 14
 - Verify Category 14
 - Verify Alerts 14
 - Verify Knowledge Object 15
 - Verify Token Templates 16
 - Verify Flex Reports 16
- Create Dashboards in EventTracker 17
 - Schedule Reports 17
 - Create Dashlet 19
 - Import Dashlet 21
- Sample Dashboards 23

Overview

Dell PowerConnect is switch series. EventTracker integrates with Dell PowerConnect switches using Syslog and provides reports, alerts and knowledge objects.

Prerequisites

- EventTracker v8.x or above should be installed.
- Dell PowerConnect switches should be configured for forwarding logs.
- Firewall Exception on port 514

Configure Dell PowerConnect Switches to forward logs to EventTracker

Dell PowerConnect switches supports forwarding logs to EventTracker via syslog.

Configuration to enable Syslog forwarding

Logs can be configured to be forwarded to EventTracker through the Remote Log Server page.

To display the Remote Log Server page,

- Login to OPENMANAGE portal.
- Click System→Logs→Remote Log Server

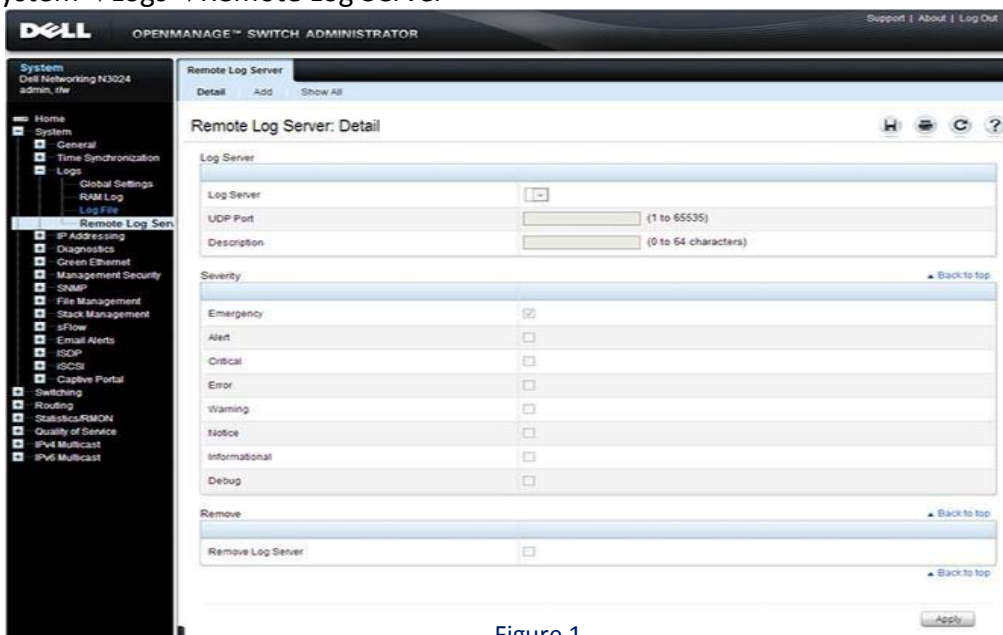


Figure 1

- **Adding EventTracker Server**

To add an EventTracker syslog server:

- Open the **Remote Log Server** page.
- Click **Add** to display the Add Remote Log Server page.
- Specify the IP address of EventTracker.
- Select the severity of the messages to send to the EventTracker.
- Click **Apply**.

Figure 2

- Click the **Show All** link to view or remove remote log servers configured on the system.

	Log Server	UDP Port	Description	Minimum Severity	Remove
1	192.168.2.7	514	RLOG_2	Info	<input type="checkbox"/> Edit

Figure 3

EventTracker Knowledge Pack (KP)

Once logs are received into EventTracker, Categories and Reports can be configured into EventTracker. The following Knowledge Packs are available in EventTracker Enterprise.

Categories

- **Dell PowerConnect - Login and logout** – This category based report provides information related to all the login and logout activities.
- **Dell PowerConnect - Port status change** – This category based report provides information related to all the port status changes.
- **Dell PowerConnect – Authentication failures** – This category based report provides information related to all the authentication failures.

Alerts

- **Dell PowerConnect: Authentication failures** : This alert is generated when any authentication failure occurs.

Flex Reports

- **Dell PowerConnect - Login and logout** - This report provides information related to all the login and logout activities.

Computer	User IP Address	Username	Action
POWERCONNECT	192.168.56.36	it1admin	logged out
POWERCONNECT	192.168.2.16	it1admin	logged in
POWERCONNECT	192.168.56.36	David	logged in

Figure 4

Logs considered:

```

- Apr 16 03:12:17 PM                               Apr 09 21:08:17 10.9.100.1 <190> Aug 16 13:24:27 Back Office network-1 CLI_WEB[emWeb]: cmd_logger_api.c(260) 6699526 %% [CLI:it1admin:10.11.5.48] User it1admin logged in to ...

action                +- logged in
event_category        +- 0
event_computer        +- PowerConnect
event_datetime        +- 4/16/2018 3:12:17 PM
event_datetime_utc    +- 1523871737
event_description      Apr 09 21:08:17 10.9.100.1 <190> Aug 16 13:24:27 Back Office network-1 CLI_WEB[emWeb]: cmd_logger_api.c(260) 6699526 %% [CLI:it1admin:10.11.5.48] User it1admin logged in to enable mode.
event_id              +- 3333
event_log_type        +- Application
event_source          +- syslog
event_type            +- Information
event_user_domain     +- N/A
event_user_name       +- N/A
log_source            +- Dell PowerConnect LoginLogout
service_name          +- Back Office network
src_ip_address        +- 10.11.5.48
src_user_name         +- it1admin

```

Figure 5

- **Dell PowerConnect - Port status change** - This report provides information related to all the port status changes.

LogTime	Computer	Port	State
04/16/2018 11:50:02 AM	POWERCONNECT	Gi1/0/7	Link Up
04/16/2018 11:50:02 AM	POWERCONNECT	Gi1/0/7	Link Down
04/16/2018 11:50:02 AM	POWERCONNECT	Gi1/0/7	Link Up
04/16/2018 11:50:02 AM	POWERCONNECT	Gi1/0/7	Link Down
04/16/2018 11:50:02 AM	POWERCONNECT	Gi1/0/7	Link Up

Figure 6

Logs considered:

```

- Apr 16 03:12:16 PM                               Apr 09 21:08:24 10.9.100.1 Apr 9 21:08:24 DELL_N20xx_Core_Stack-1 TRAPMGR[trapTask]: traputil.c(721) 65729 %% Link Up: Gi1/0/6

event_category        +- 0
event_computer        +- PowerConnect
event_datetime        +- 4/16/2018 3:12:16 PM
event_datetime_utc    +- 1523871736
event_description      Apr 09 21:08:24 10.9.100.1 Apr 9 21:08:24 DELL_N20xx_Core_Stack-1 TRAPMGR[trapTask]: traputil.c(721) 65729 %% Link Up: Gi1/0/6
event_id              +- 3333
event_log_type        +- Application
event_source          +- syslog
event_type            +- Information
event_user_domain     +- N/A
event_user_name       +- N/A
log_source            +- Dell PowerConnect Port Status
log_status            +- Link Up
src_host_name         +- DELL_N20xx_Core_Stack

```

Figure 7

- **Dell PowerConnect - Authentication failures** - This report provides information related to all the user authentication failures.

LogTime	Computer	Username	Action	Reason
04/16/2018 12:16:46 PM	POWERCONNECT	David	Failed to login	authentication failures
04/16/2018 12:17:10 PM	POWERCONNECT	it1admin	Failed to login	authentication failures
04/16/2018 12:17:10 PM	POWERCONNECT	David	Failed to login	authentication failures
04/16/2018 03:09:44 PM	POWERCONNECT	it1admin	Failed to login	authentication failures
04/16/2018 03:09:44 PM	POWERCONNECT	David	Failed to login	authentication failures
04/16/2018 03:09:49 PM	POWERCONNECT	it1admin	Failed to login	authentication failures
04/16/2018 03:12:14 PM	POWERCONNECT	it1admin	Failed to login	authentication failures
04/16/2018 03:12:14 PM	POWERCONNECT	David	Failed to login	authentication failures
04/16/2018 03:12:18 PM	POWERCONNECT	it1admin	Failed to login	authentication failures

Figure 8

Logs considered:

```

- Apr 16 03:09:44 PM      Apr 09 21:08:17 10.9.100.1 <190> Aug 16 08:12:59 Home network-1 USER_MGR[emWeb]: user_mgr.c(1793) 66 99475 %% User David Failed to login because of authentication failures

event_category          +- 0
event_computer          +- PowerConnect
event_datetime          +- 4/16/2018 3:09:44 PM
event_datetime_utc      +- 1523871584
event_description       Apr 09 21:08:17 10.9.100.1 <190> Aug 16 08:12:59 Home network-1 USER_MGR[emWeb]: user_mgr.c(1793) 66 99475 %% User David Failed to login because of authentication failures
event_id               +- 3333
event_log_type          +- Application
event_source            +- syslog
event_type              +- Information
event_user_domain       +- N/A
event_user_name         +- N/A
log_source              +- Dell PowerConnect Authentication Failures
src_user_name           +- David

```

Figure 9

Import Dell PowerConnect Switches Knowledge Pack into EventTracker

NOTE: Import knowledge pack items in the following sequence:

- Categories
- Knowledge Objects
- Alerts
- Token Templates
- Flex Reports

EventTracker displays success message.

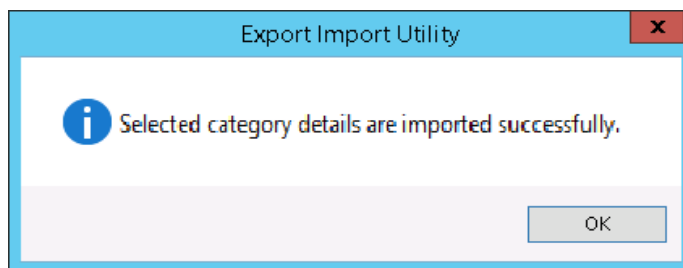



Figure 12

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

Import Alerts

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

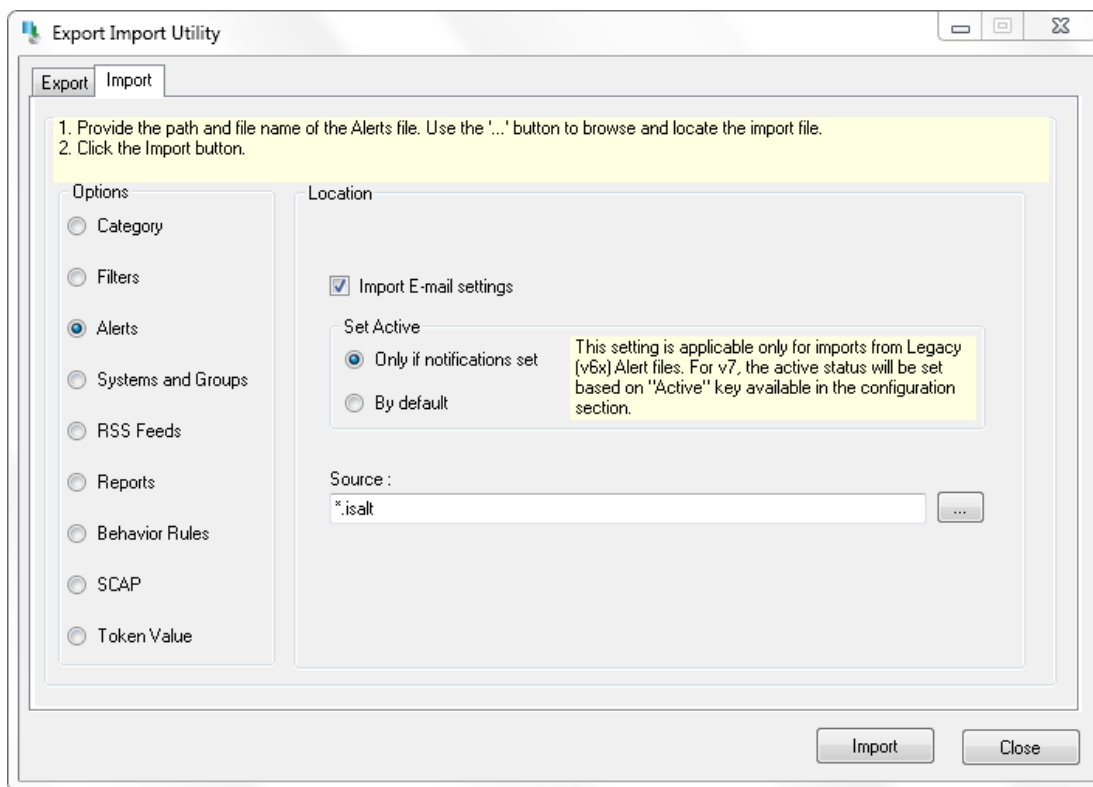


Figure 13

2. Locate **DellPowerConnect_Alerts.isalt** file, and then click the **Open** button.
 3. To import alerts, click the **Import** button.
- EventTracker displays success message.

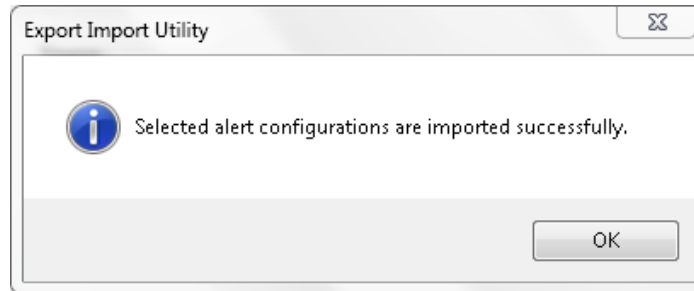


Figure 14

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

Import Knowledge Objects

- Click **Knowledge objects** under **Admin** option in the EventTracker Manager page.
- Click **Browse**.
- Locate the **KO_ DellPowerConnect.etko** file



Figure 15

- Now select all the files and then click on **Upload**.



Figure 16

Knowledge objects are now imported successfully.

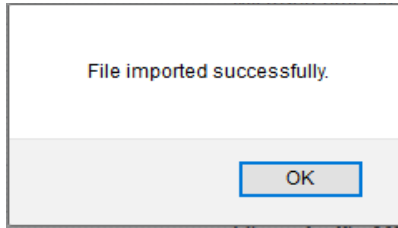


Figure 17

Import Token Templates

- Logon to **EventTracker Enterprise**.
- Click the **Admin** menu, and then click **Parsing Rules**.
- Select **Template** tab, locate the **Token_Template_DellPowerConnect.ettd** file.
- Click on the **Import** icon.

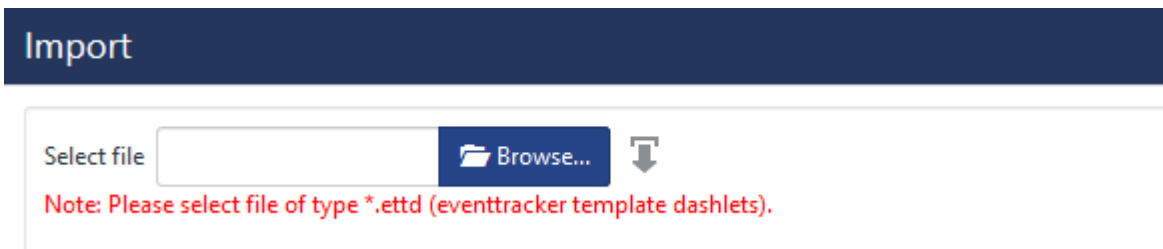


Figure 18

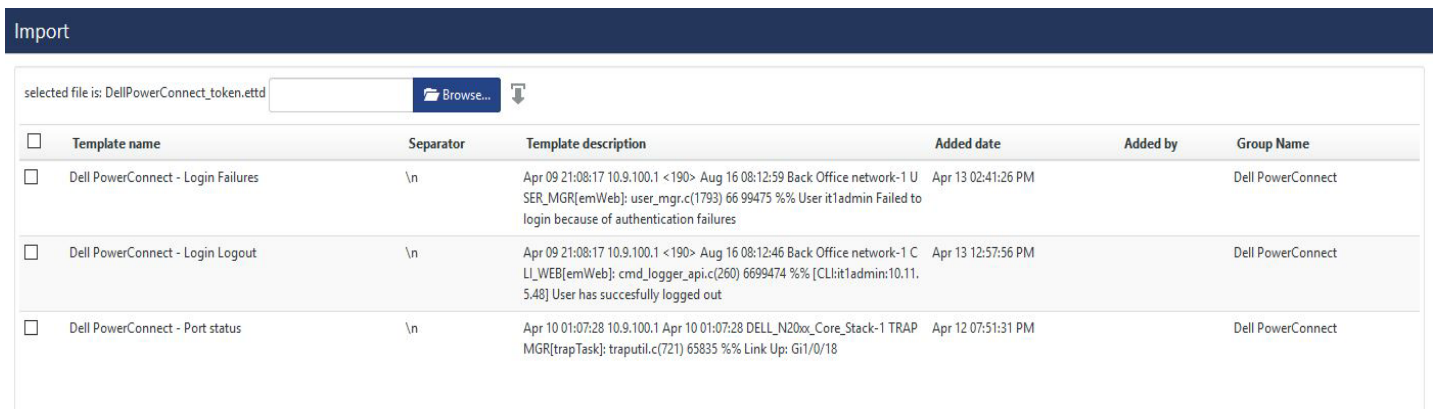


Figure 19

Templates are now imported successfully.

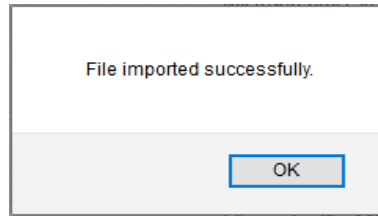


Figure 20

Import Flex Reports

- Launch **EventTracker Control Panel**.
- Double click **Export Import Utility**, and then click the **Import** tab.

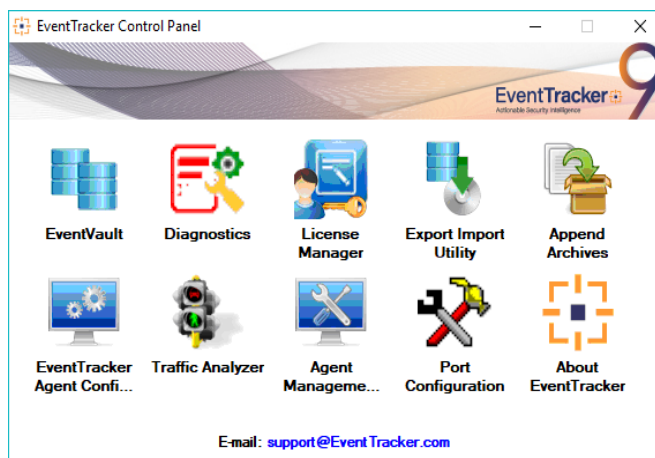


Figure 21

- Click **Reports** option, and select new (.etcrx) option.

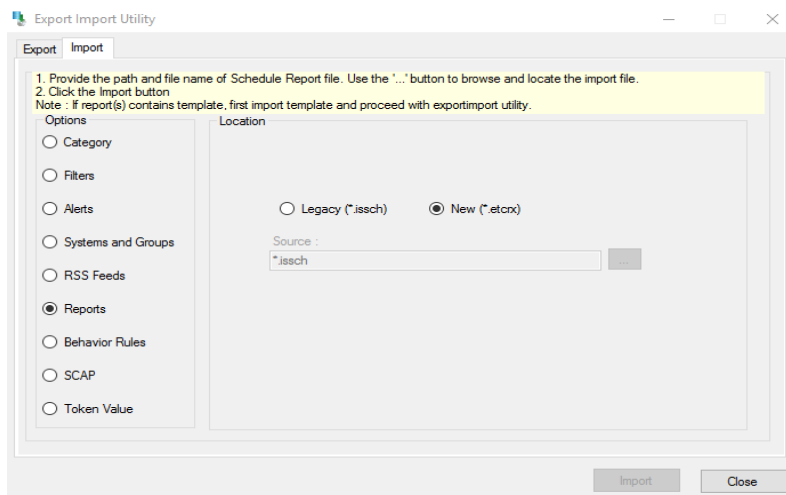


Figure 22

- And then locate the file.

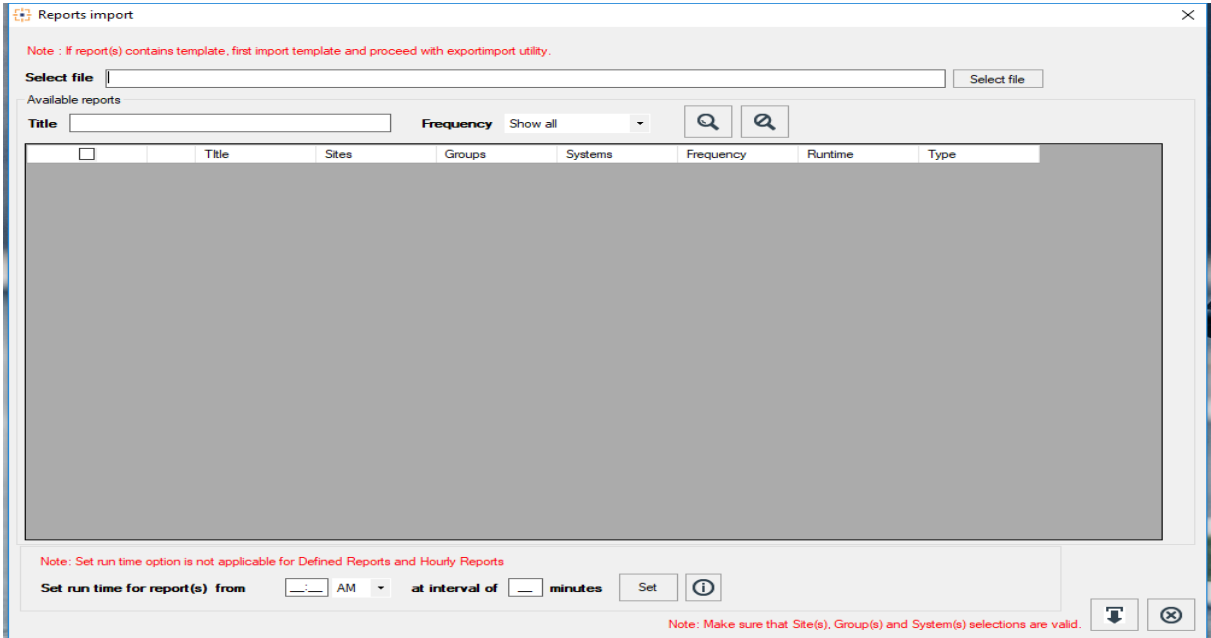


Figure 23

- Locate the file named **FlexReports_DellPowerConnect.etcx** and select all the check box.

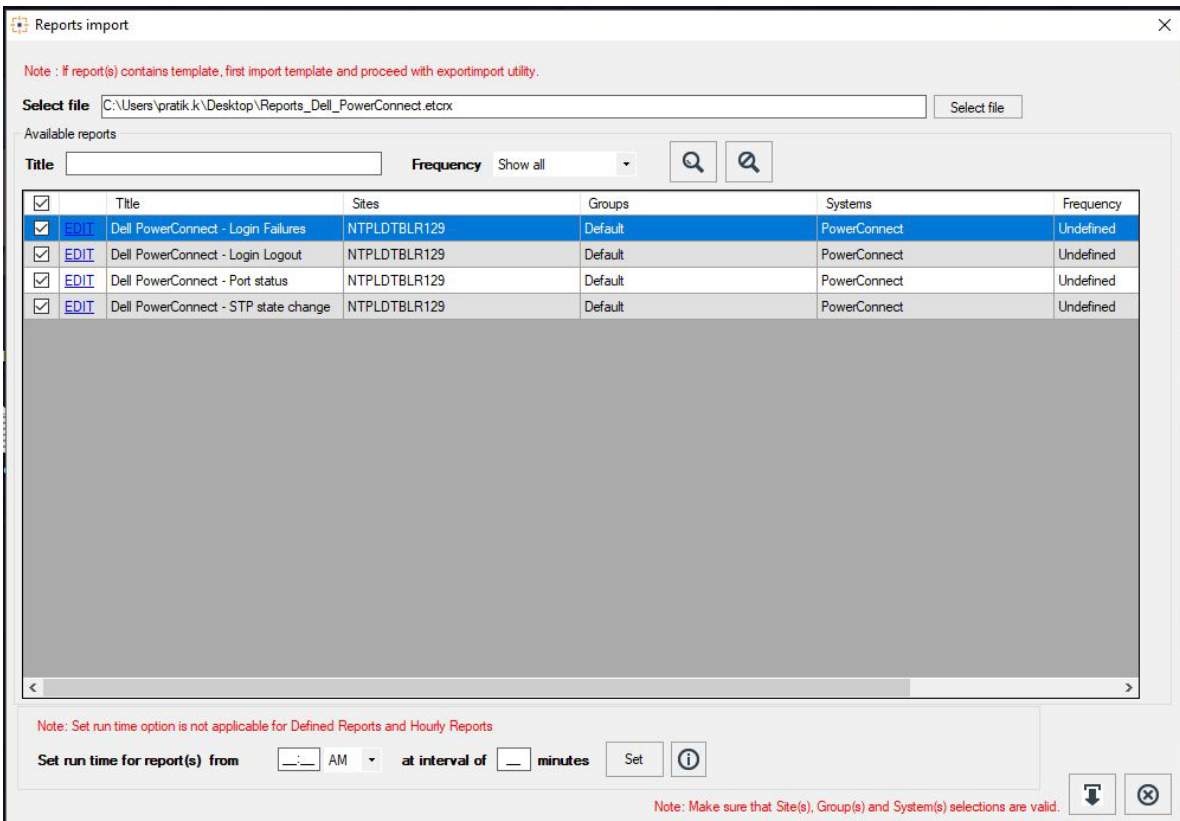


Figure 24

- Click the **Import** button to import the reports. EventTracker displays success message.

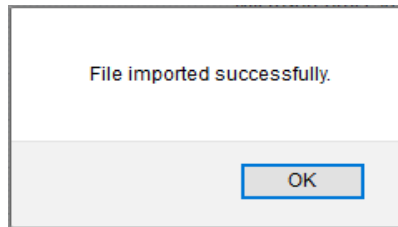


Figure 25

Verify Knowledge Pack in EventTracker

Verify Category

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Category**.
3. In **Category Group Tree** to view imported category, scroll down and click **Dell PowerConnect** group folder.

Categories are displayed in the pane.

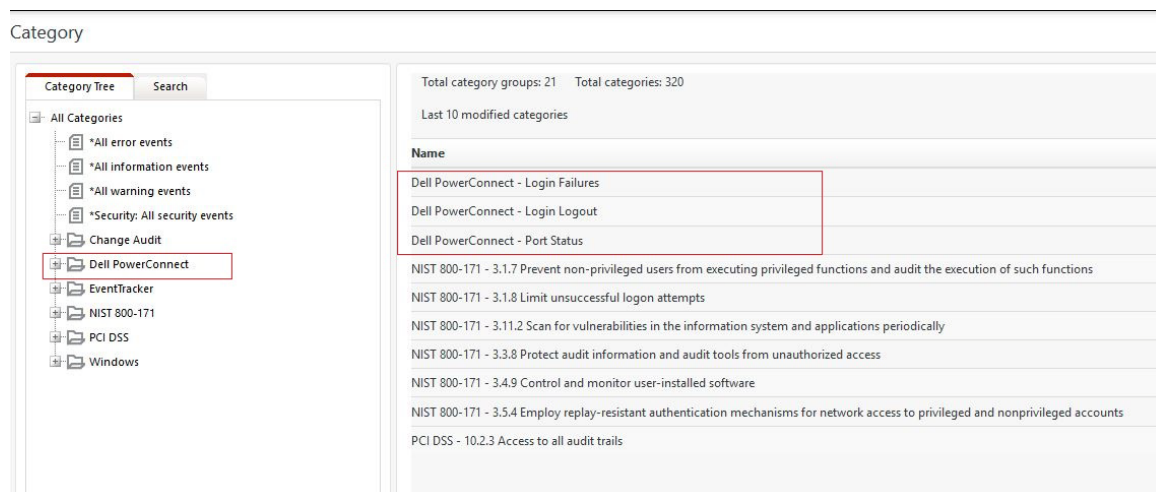


Figure 26

Verify Alerts

1. Logon to **EventTracker Enterprise**.

2. Click the **Admin** menu, and then click **Alerts**.
3. In the **Search** box, type "**Dell PowerConnect**", and then click the **Go** button.
Alert Management page will display all the imported alerts.

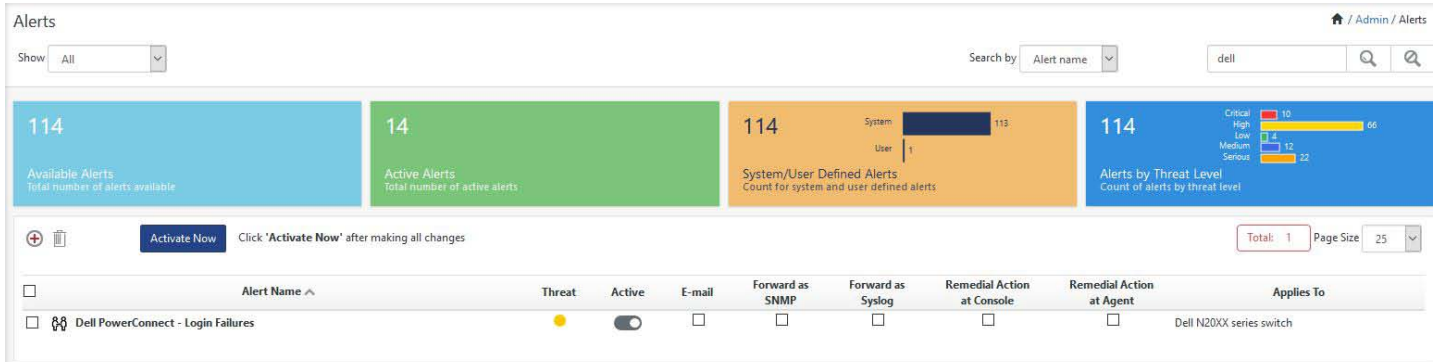


Figure 27

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

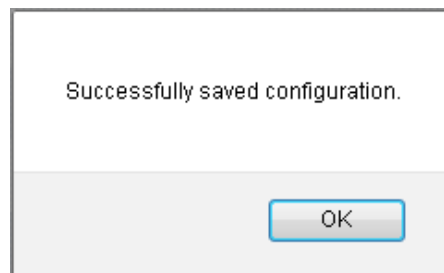


Figure 28

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

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

Verify Knowledge Object

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Knowledge Object**.
3. In **Knowledge Object Group Tree** to view imported knowledge object, scroll down and click **Dell PowerConnect** group folder.

Knowledge Object are displayed in the pane.

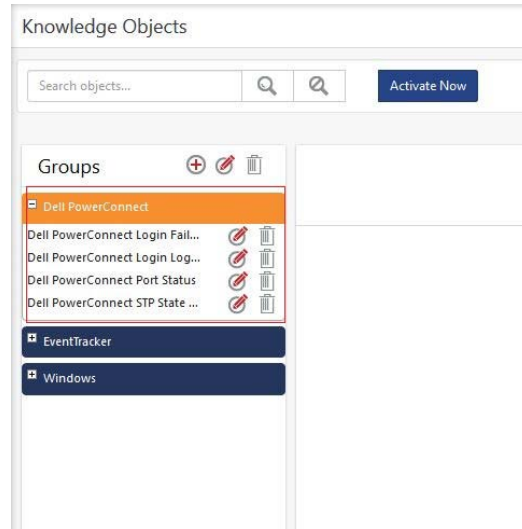


Figure 29

Verify Token Templates

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Parsing Rules**.
3. In **Parsing Rules** select **Template**, scroll down and click **Dell PowerConnect** group folder
Token templates are displayed in the pane.

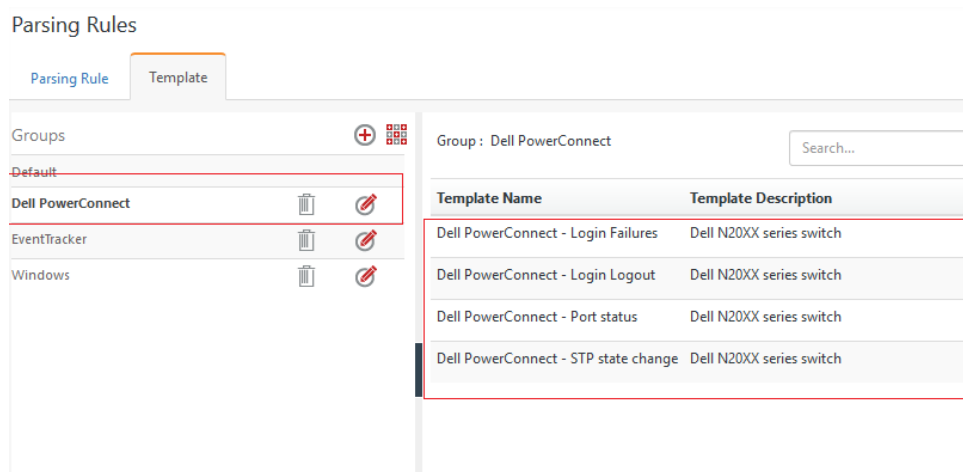


Figure 30

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 **Dell PowerConnect** group folder.

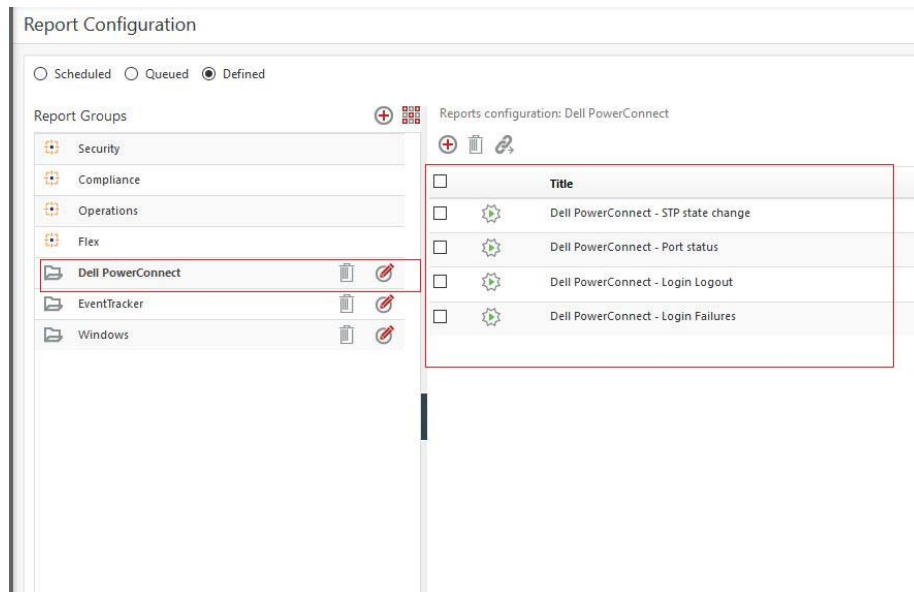


Figure 31

5. Reports are displayed in the Reports configuration pane.

NOTE: Please specify appropriate **systems** in **report wizard** for better performance.

Create Dashboards in EventTracker

NOTE: This is applicable for EventTracker 8.3. For EventTracker 9.x, import the dashboards (.etwd file).

Schedule Reports

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

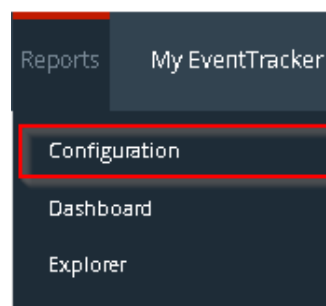


Figure 32

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

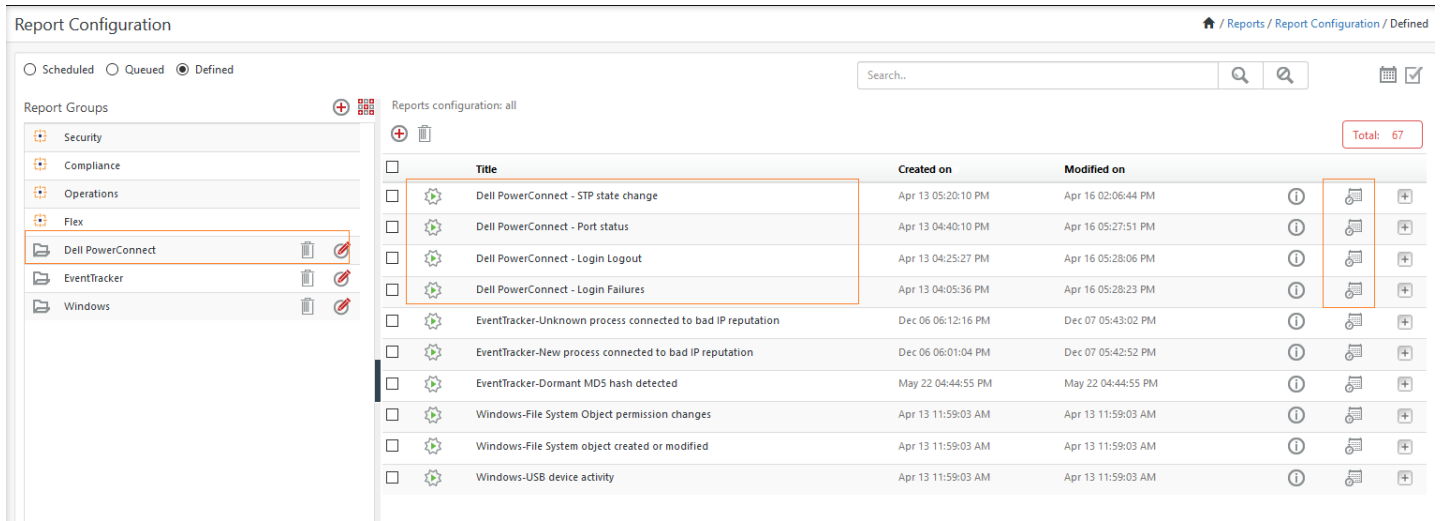



Figure 33

3. Select **Dell PowerConnect** 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.

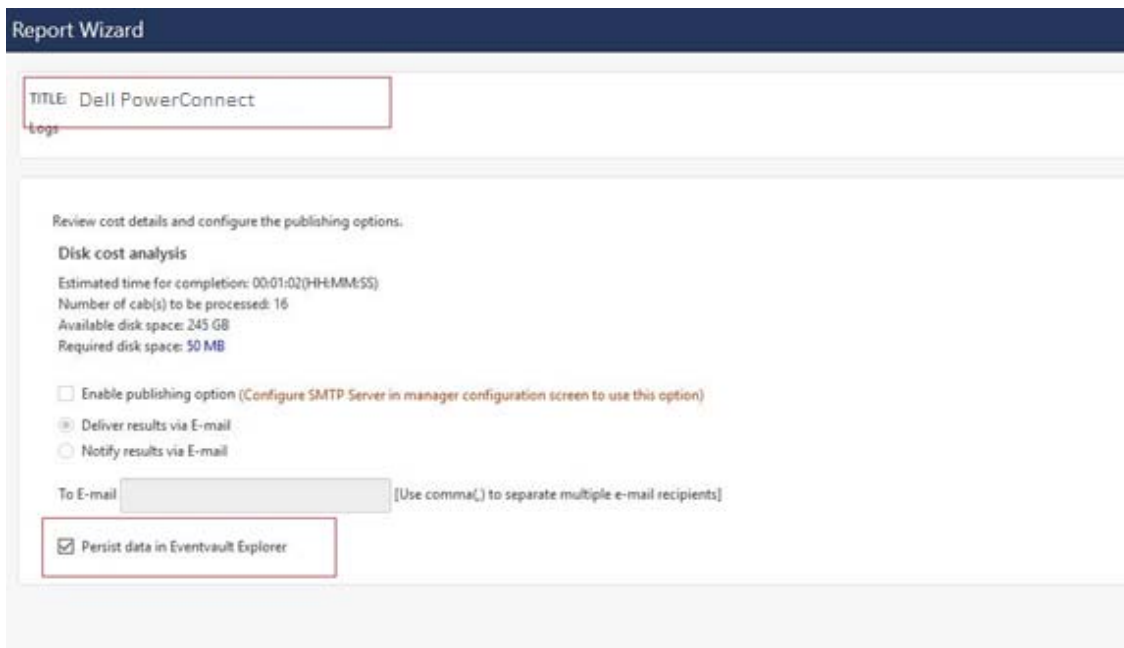


Figure 34

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 Dashlet

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

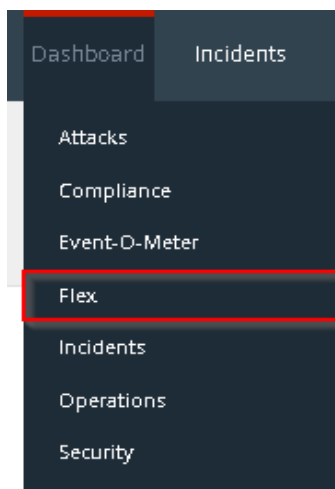


Figure 35

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

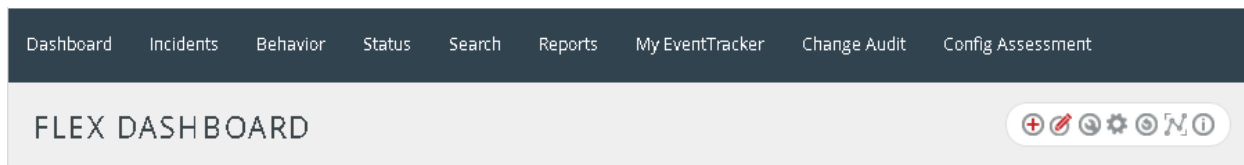



Figure 36

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

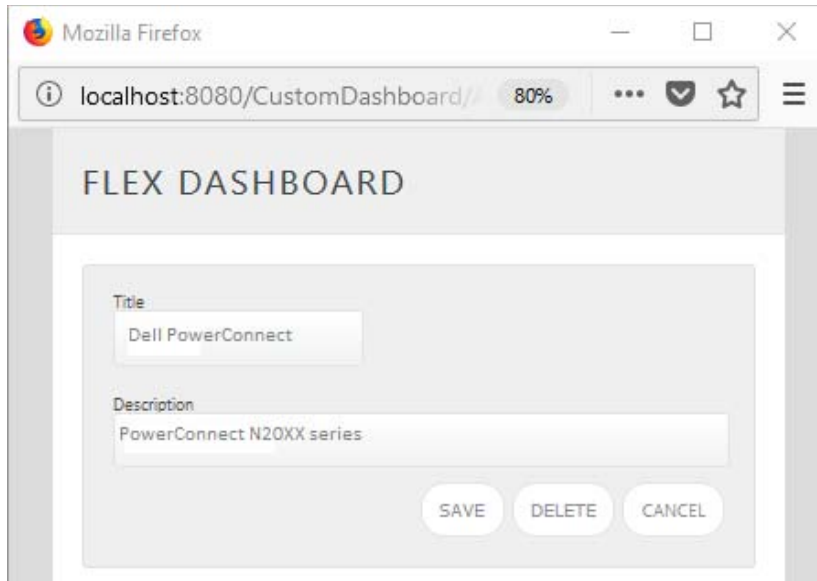



Figure 37

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

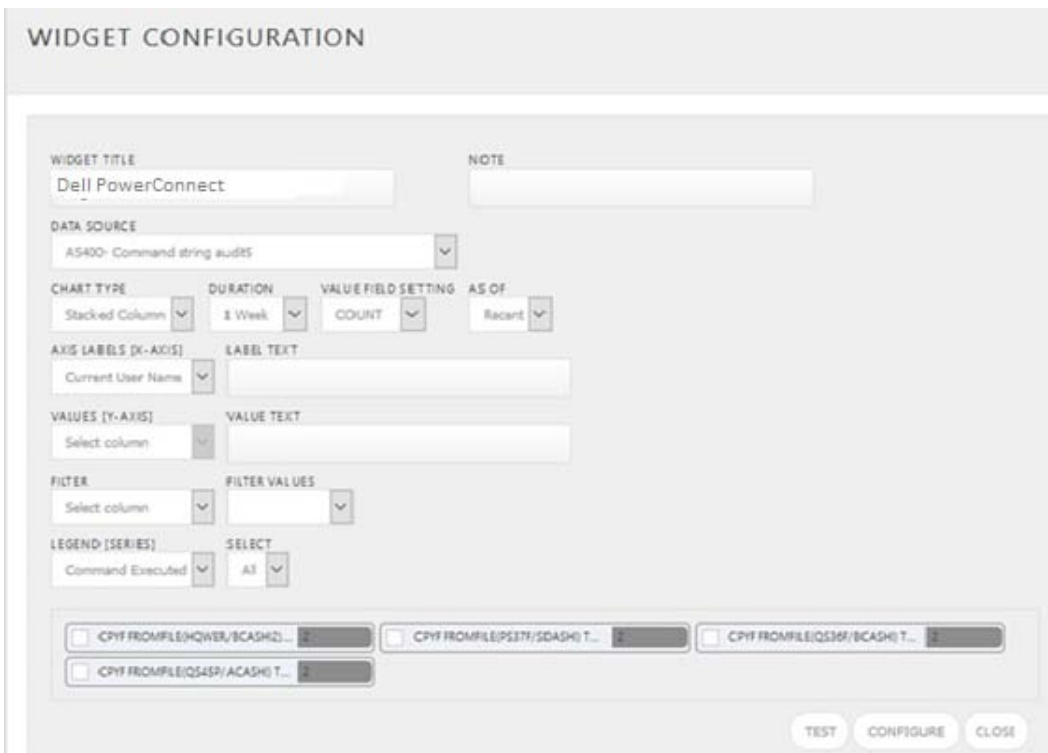




Figure 38

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.
15. If satisfied, Click **Configure** button.
16. Click 'customize'  to locate and choose created dashlet.
17. Click  to add dashlet to earlier created dashboard.

Import Dashlet

In EventTracker 9.0, we have added new feature which will help to import/export of dashlet. Following is procedure to do that:

1. Login into EventTracker Enterprise Web console.

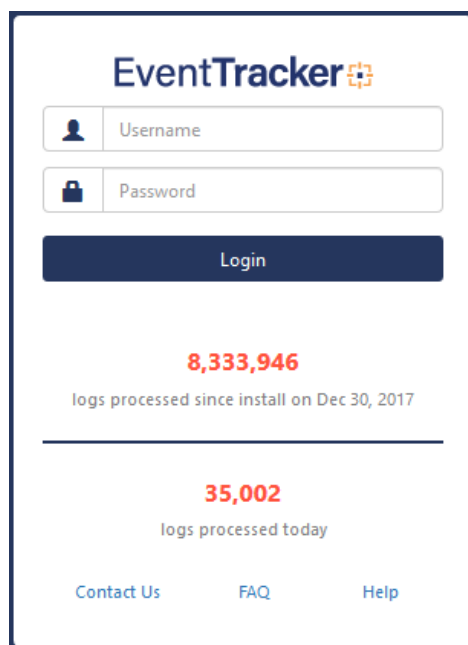


Figure 39

2. Go to **My Dashboard** option.

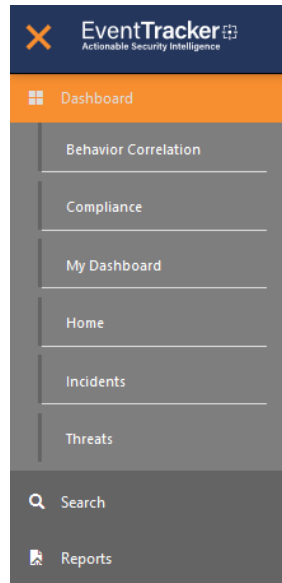


Figure 40

3. Click on import button and select Dell **PowerConnect.etwd** File.

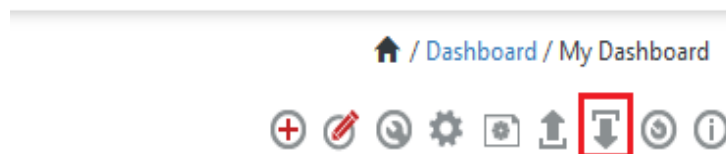


Figure 41

4. Click upload icon and select Dashboard which you want to import.

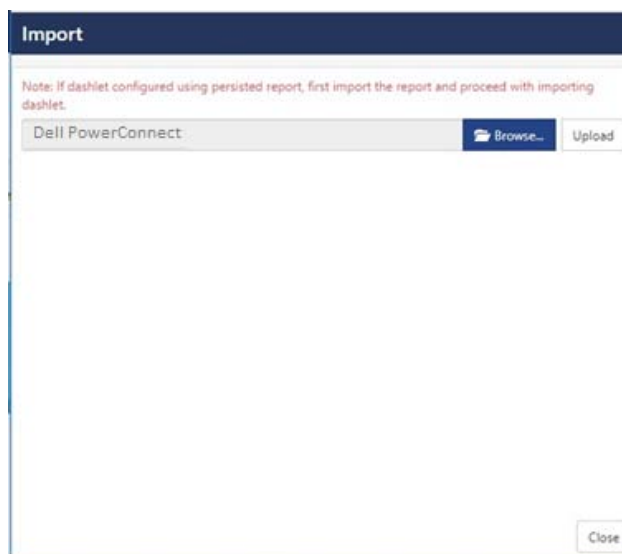


Figure 42

5. Click on **Import** button. It will upload the selected dashboard.

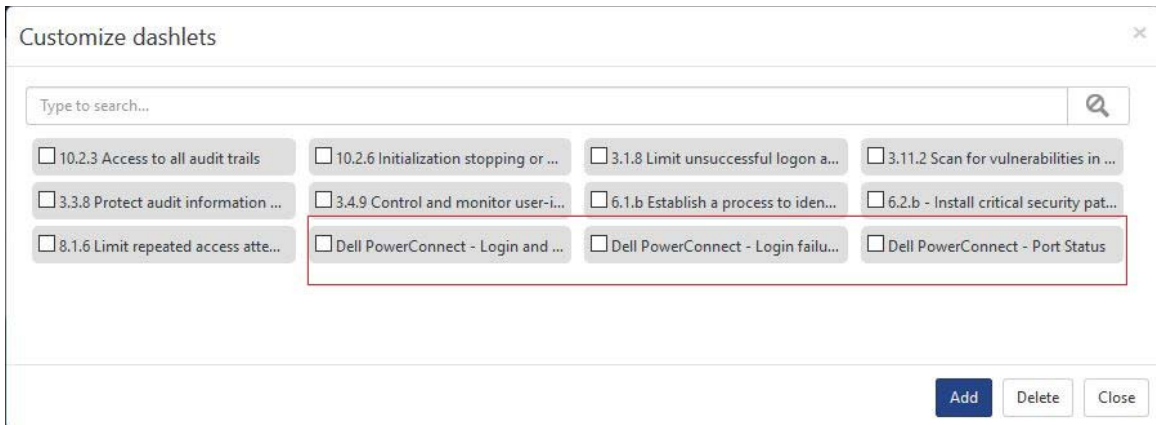


Figure 43

Sample Dashboards

- REPORT: Dell PowerConnect - Login failures**
WIDGET TITLE: Dell PowerConnect - Login failures
CHART TYPE: Donut
AXIS LABELS [X-AXIS]: Source user name



Figure 44

- **REPORT:** Dell PowerConnect - Login and Logout
WIDGET TITLE: Dell PowerConnect - Login failures
CHART TYPE: Donut
AXIS LABELS [X-AXIS]: Source user name
LEGEND [SERIES]: Action

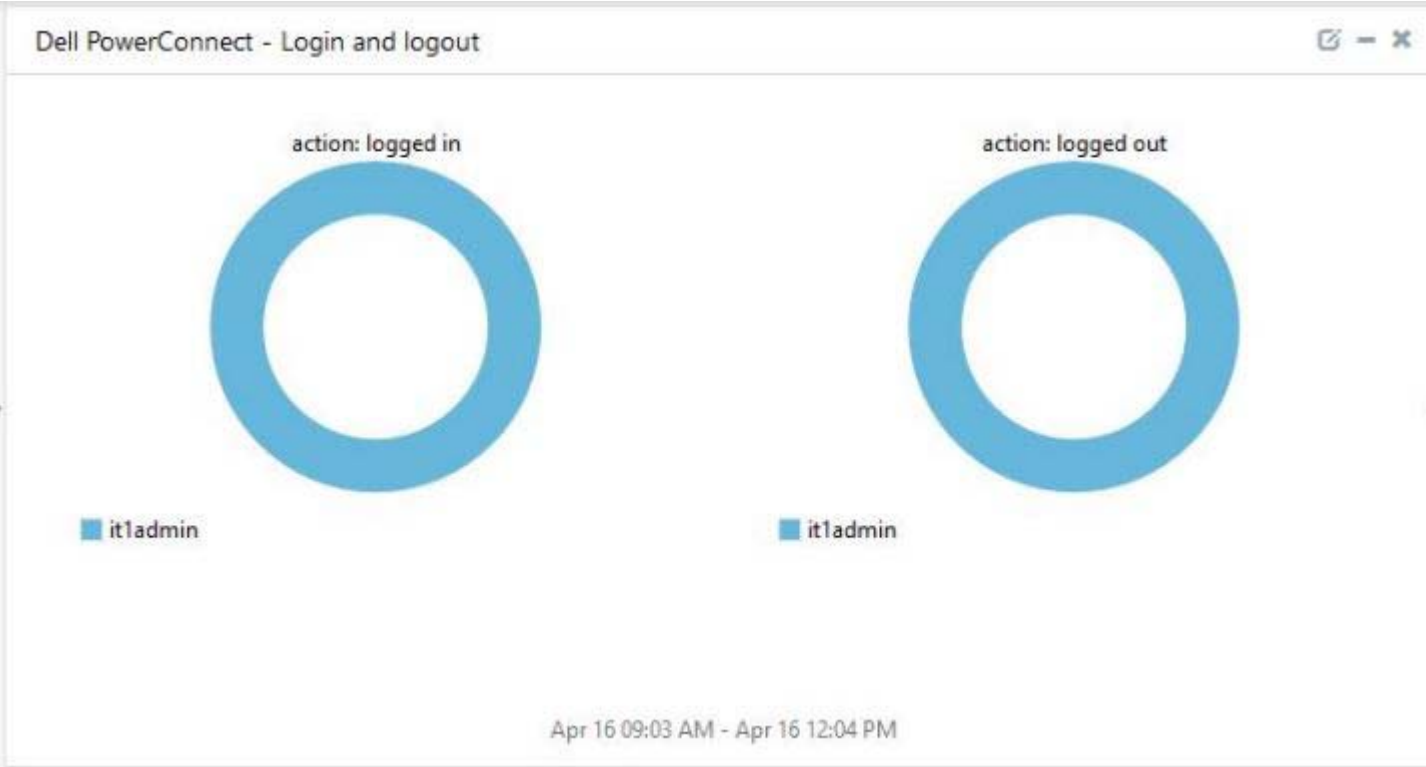


Figure 45

- **REPORT: Dell PowerConnect – Port Status Changes**
WIDGET TITLE: Dell PowerConnect – Port Status Changes
CHART TYPE: Donut
AXIS LABELS [X-AXIS]: Port Status Changes

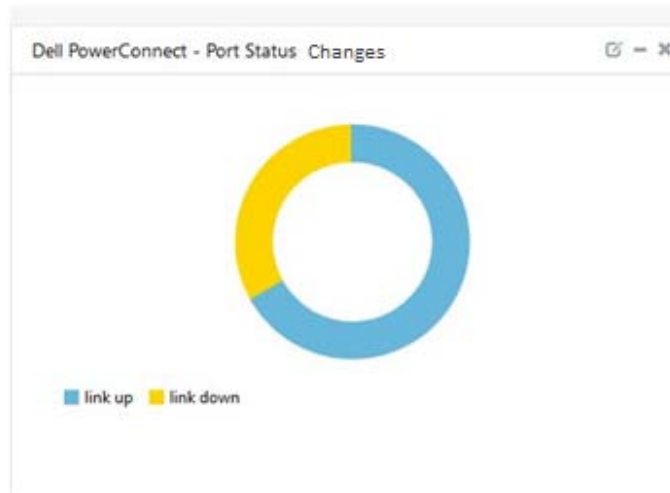


Figure 46