EventTracker

Actionable Security Intelligence

Integrate Infoblox DDI

Publication Date: January 12, 2016

Abstract

This guide provides instructions to configure Infoblox device to send the syslog events to EventTracker.

Scope

The configurations detailed in this guide are consistent with **EventTracker** version 7.X and later, and **Infoblox DDI with NIOS version 7.0.x and later**.

Audience

Administrators, who are responsible for monitoring Infoblox devices using EventTracker Manager.

Table of Contents

Overview

Infoblox is a critical technology with DNS, DHCP, IPAM functionalities which provides maximum protection and offers minimum attack surface.

EventTracker compiles and inspects critical events to provide an administrator's insight on user behavior, device anomalies, configuration changes etc.

Prerequisites

- **EventTracker v7.x or later** should be installed.
- **Infoblox Grid Manager** with **NIOS version 7.0.X**.

Configure Infoblox to send syslog to EventTracker

All Infoblox devices are managed using Infoblox Grid Manager.

1. Logon to **Infoblox Grid Manager** using valid credentials.

Figure 1

2. Navigate to **Grid>Grid Manager>Members** to access active grid member settings.

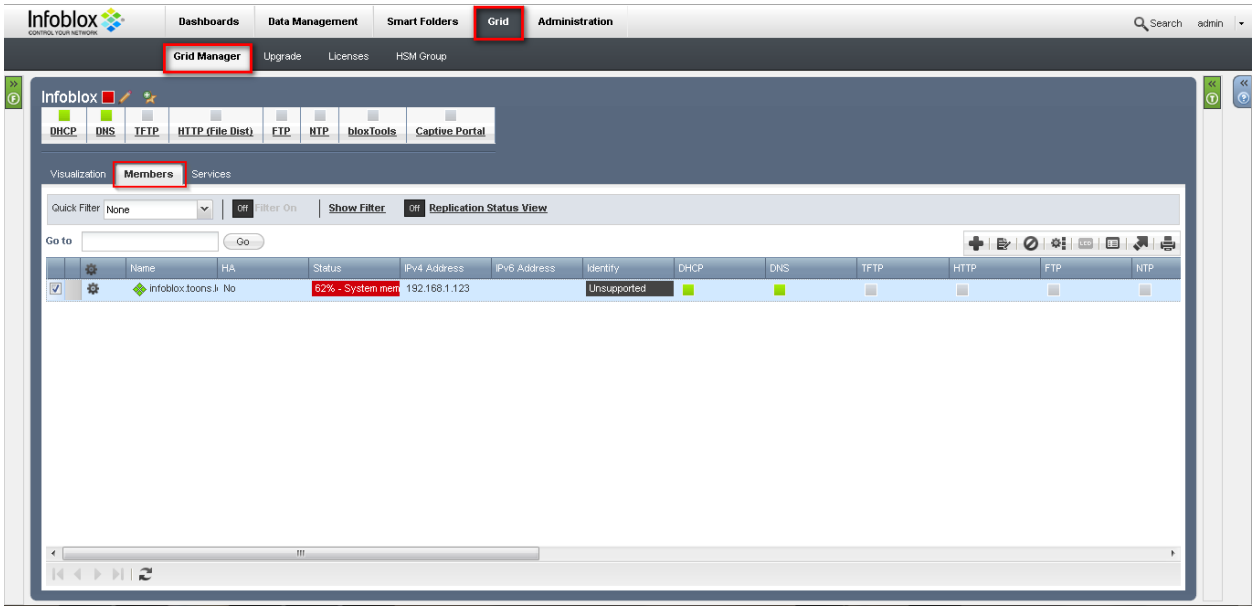

Figure 2

3. Click on the icon  to show available options for selected grid member.

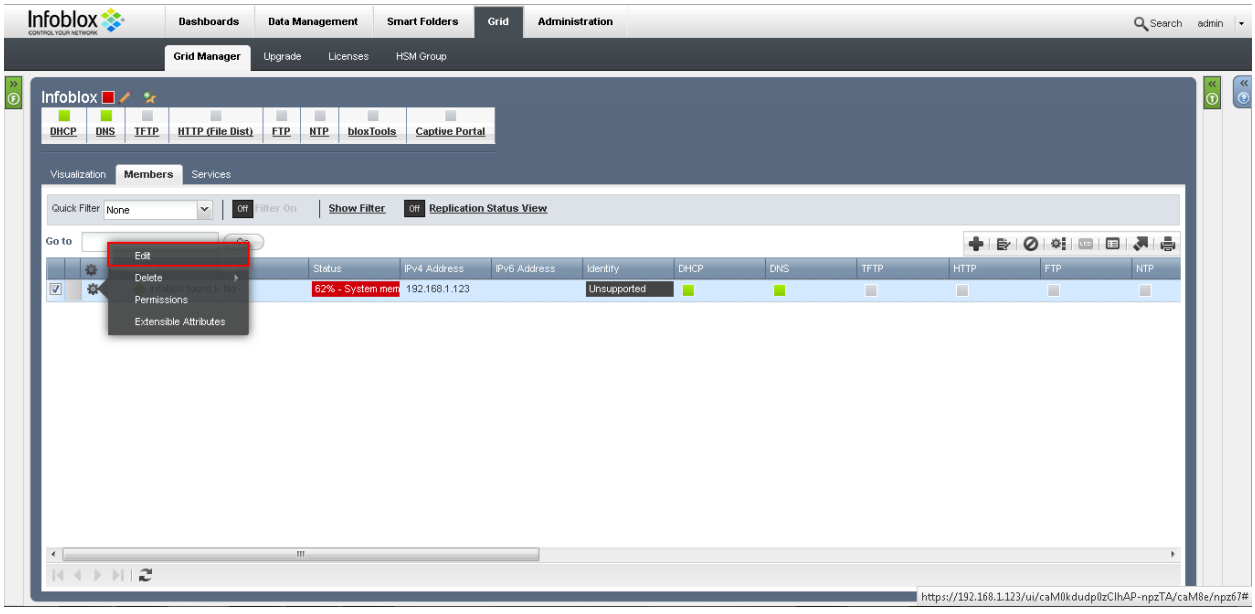

Figure 3

4. Click on **Edit** to change options for selected Grid Member.

   Grid Member Properties Editor pane is shown.

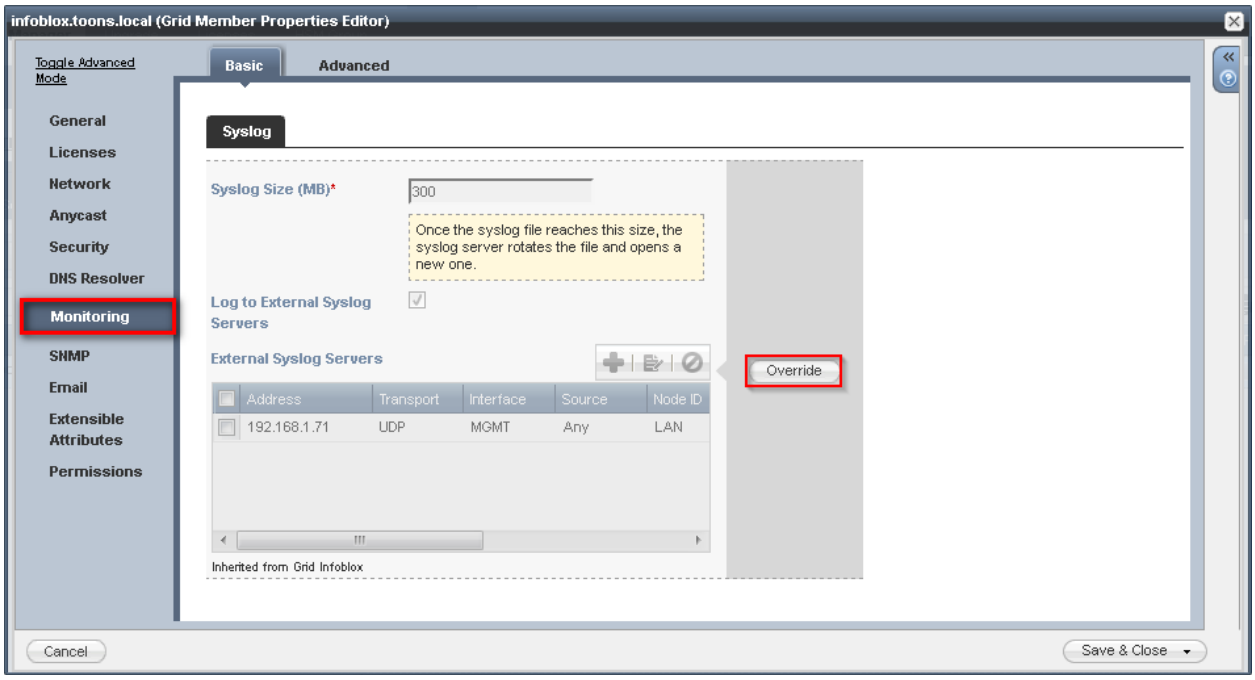

Figure 4

5. Select **Monitoring** and then click **Override** to enable customization of syslog settings.

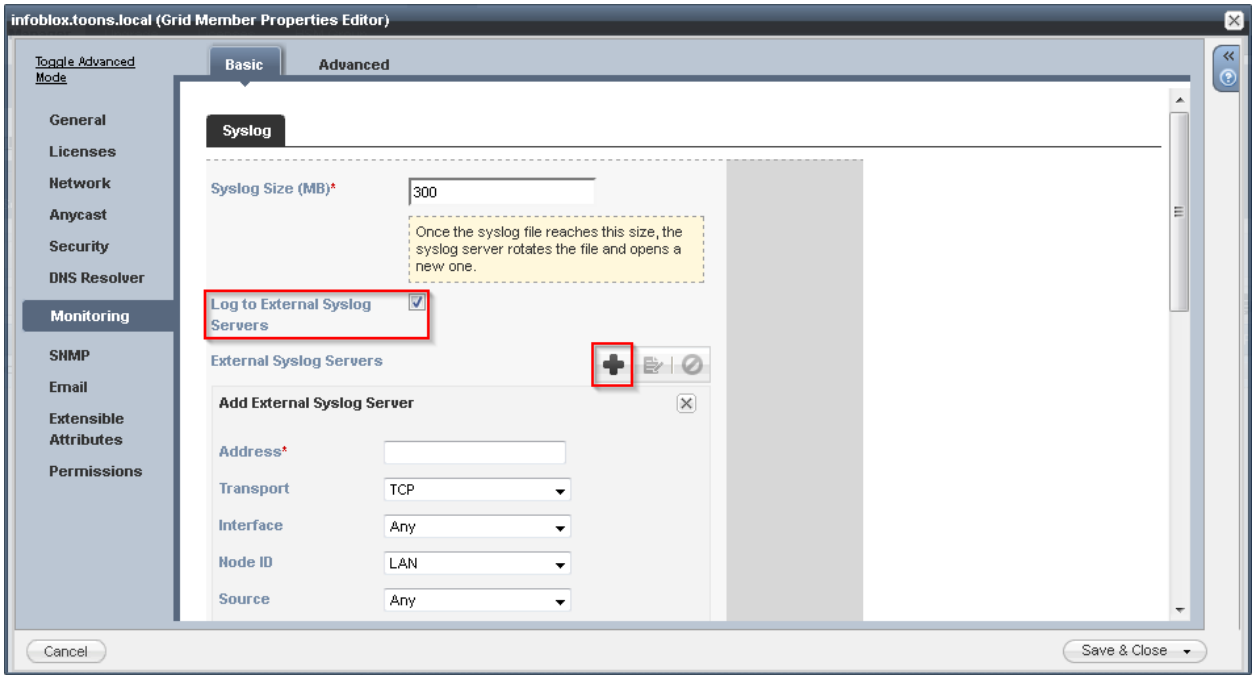

Figure 5

6. Select the checkbox beside **Log to External Syslog Servers** to enable syslog logging.
7. Click the icon  beside **External Log Servers** section to add new remote syslog server.

8. Fill the required details in **Add External Syslog Server** pane. As suggested below:

- **Address** – Fill in the **IP address** of syslog server
- **Transport** – Select **UDP**
- **Interface** – Select **Any** from dropdown
- **Node ID** - Select **LAN** from drop down
- **Source** - Select **Any** from drop down menu
- **Severity** - Select **Info** from drop down menu
- **Port** - Type **514**
- **Logging Category** - Select **Send All**

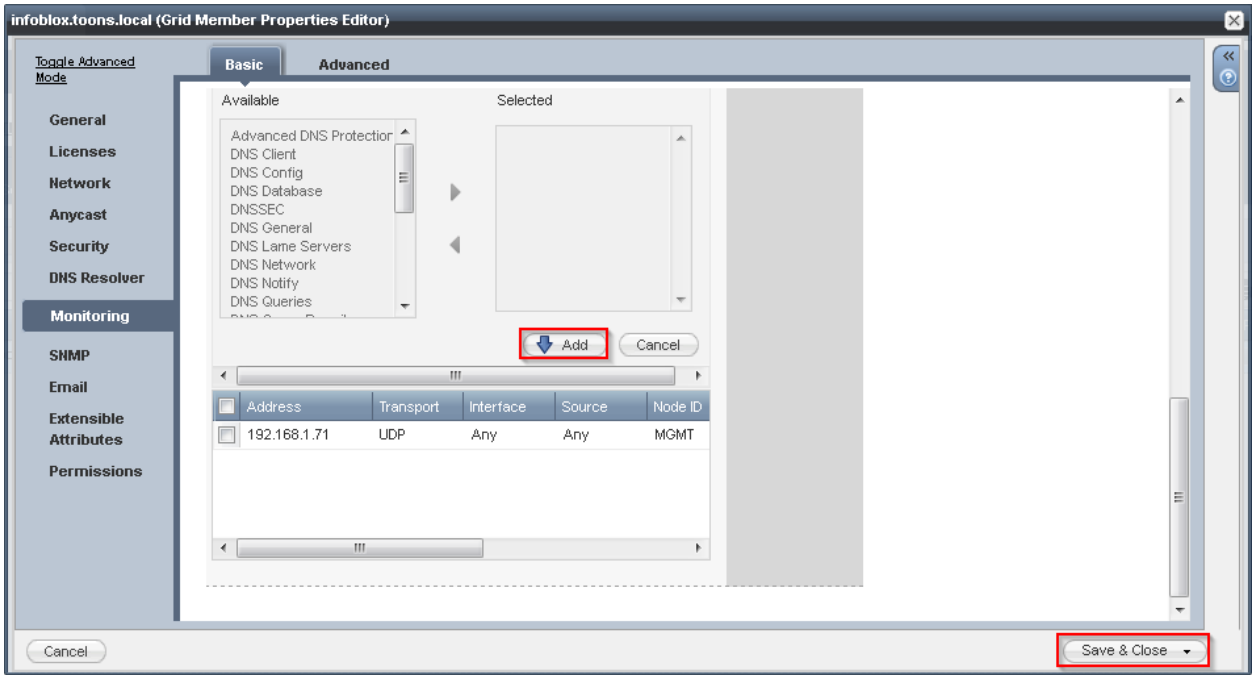

Figure 6

9. Click  to confirm configuration.
10. Select  to save the syslog configuration.

EventTracker Knowledge Pack (KP)

Once logs are received into EventTracker, Alerts and Reports can be configured into EventTracker. The following Knowledge Packs are available in EventTracker v7.x and later to support Infoblox monitoring.

Categories

- **Infoblox: Object created -** This category based report provides information related to the object created.
- **Infoblox: Object modified –** This category based report provides information related to the object modified.
- **Infoblox: Object deleted –** This category based report provides information related to the object deleted.
- **Infoblox: DHCP renew –** This category based report provides information related to the assignment and renewal of IP address to a system.
- **Infoblox: DHCP release –** This category based report provides information related to the release of IP address from a system.
- **Infoblox: DHCP expire –** This category based report provides information related to expire of lease-duration of IP address of a system.

Alerts

- **Infoblox: High CPU Usage Detected** – This alert is generated when CPU usage is critical.
- **Infoblox: High Disk Usage Detected** – This alert is generated when disk space usage is critical.
- **Infoblox: High Memory Usage Detected** – This alert is generated when memory usage is critical.
- **Infoblox: Object created deleted and modified** – This alert is generated when an object (DHCP range, A record, etc) is created, deleted or modified.

Reports

- **Infoblox - User Logon Details** – This report provides information related to user logon behavior which includes device address, username, group name, source address, console type, logon status, reason and authentication type fields.
- **Infoblox - Blacklist Ruleset Management Details** – This reports provides information related to change in blacklist rules which include device address, username and activity fields.
- **Infoblox - Administrative User Management Details** – This report provides information related to change in admin user accounts which includes device address, username and activity fields.

- **Infoblox – DHCP IP assignment details** – This report provides information related to assignment, release and expire of IP address to system which includes IP address, MAC address, lease-duration and status (assign, renew, release or expired) fields.
- **Infoblox – DHCP object created deleted and modified** – This report provides information related to the creation, deletion and modification of object (like DHCP range, A record, MX record) which includes object type, object name, action and messages (information about the changes) fields.

Filters

- **Infoblox: Called logs** – This filter can filter out the logs generated for function calls.

Import Infoblox Knowledge Pack into EventTracker

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

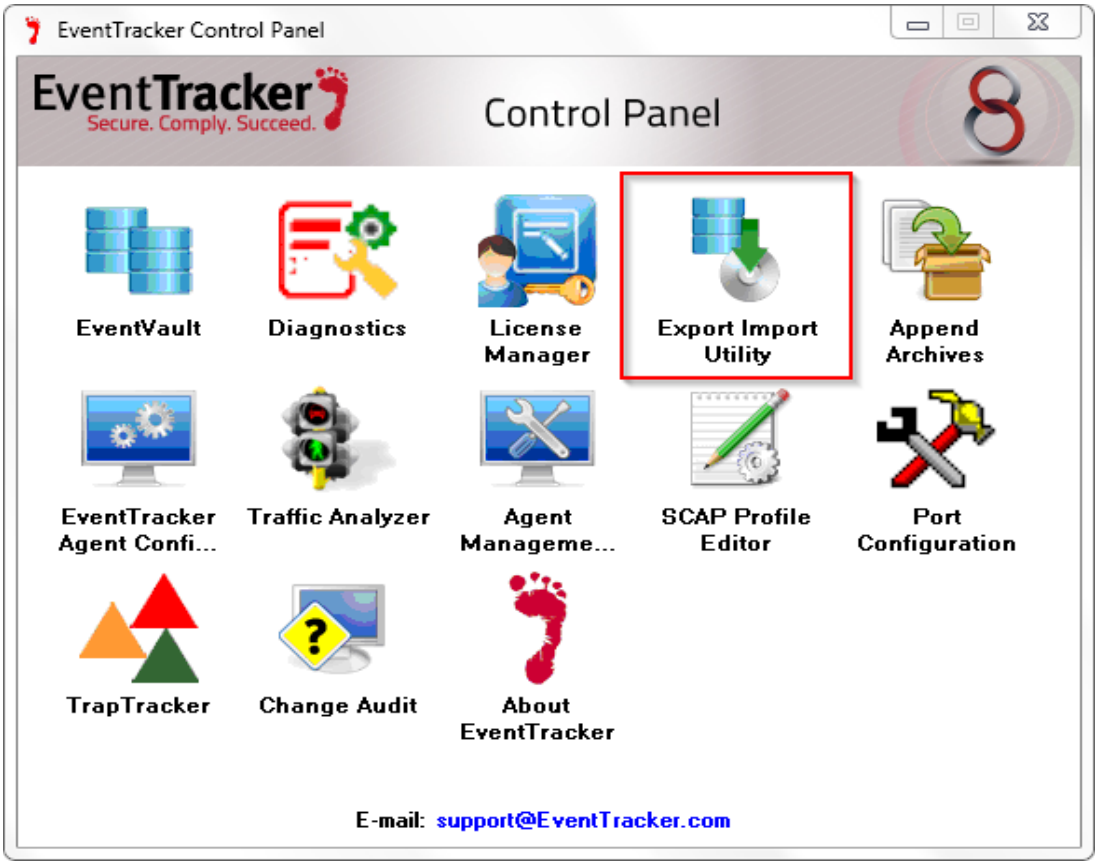

Figure 7

Import **Categories, Alerts, and Reports** as given below.

Import Category

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

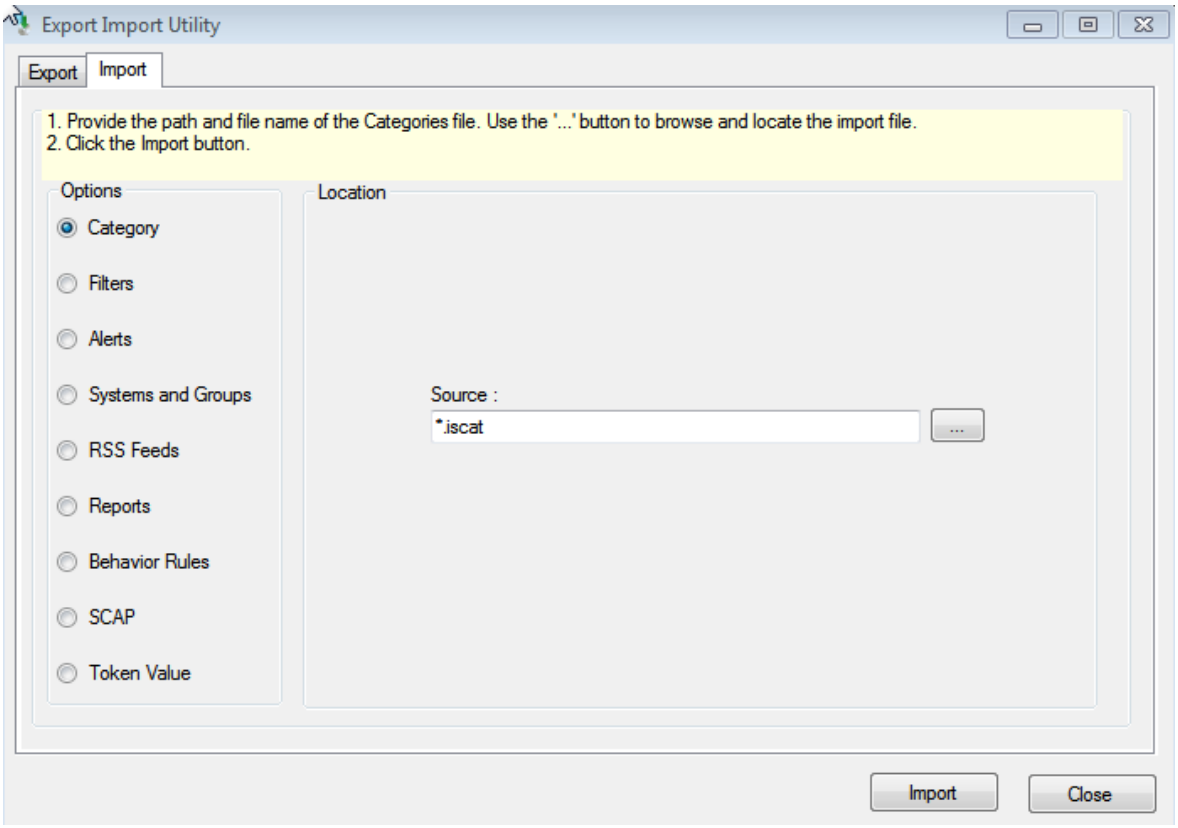

Figure 8

2. Locate **All Infoblox group of categories.iscat** file, and then click the **Open** button.
3. To import categories, click the **Import** button.
   EventTracker displays success message.

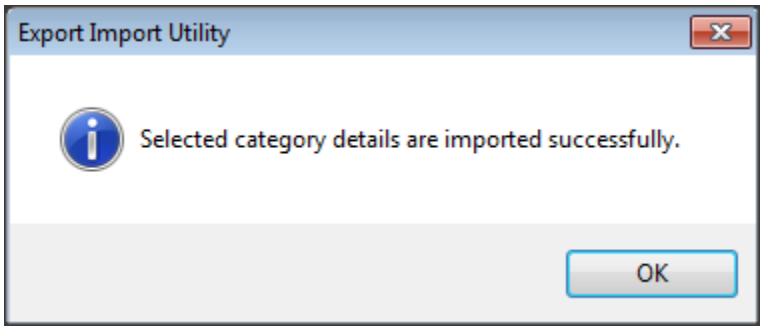

Figure 9

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

Import Alerts

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

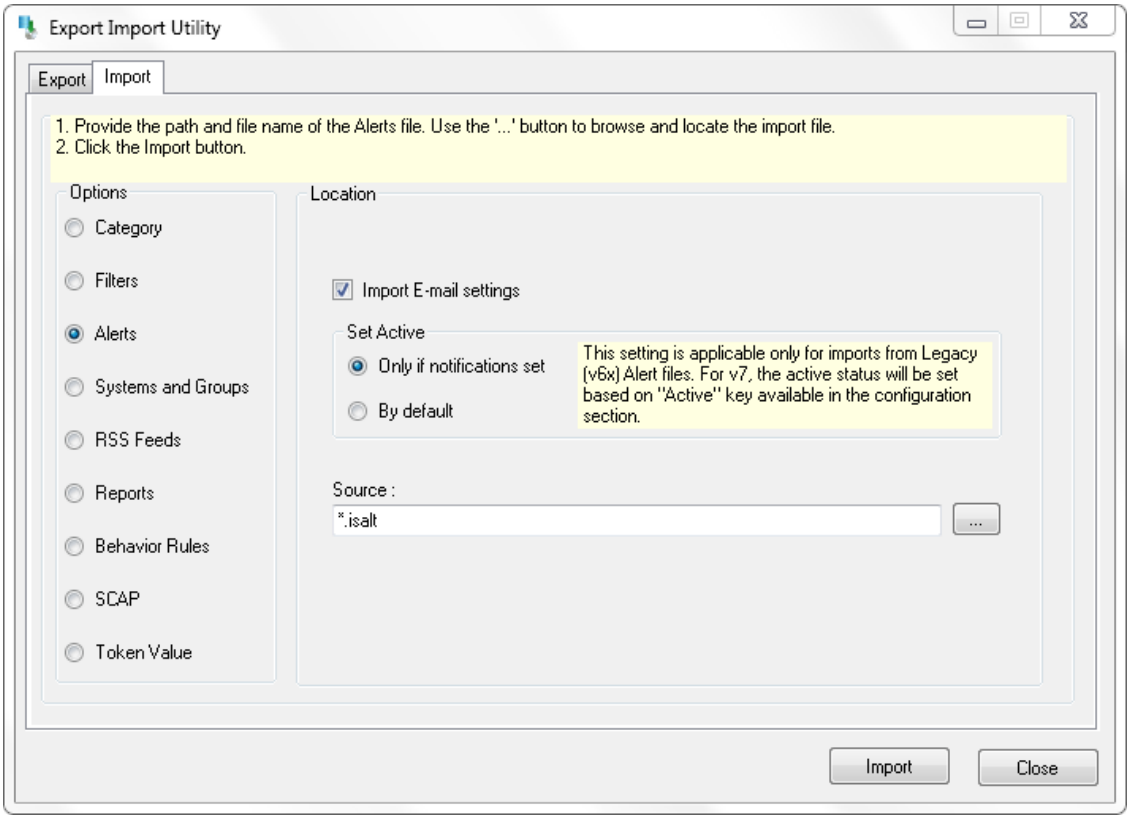

Figure 10

2. Locate **All Infoblox group of alerts.isalt** file, and then click the **Open** button.
3. To import alerts, click the **Import** button.
   EventTracker displays success message.

Figure 11

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

NOTE: You can select alert notification such as Beep, Email, and Message etc. Select the respective checkbox in the Alert management page, and then click the **Activate Now** button.

Import Parsing Rules

1. Click **Token Value** option, and then click the browse  button.
2. Locate **All Infoblox group of tokens.istoken** file, and then click the **Open** button.

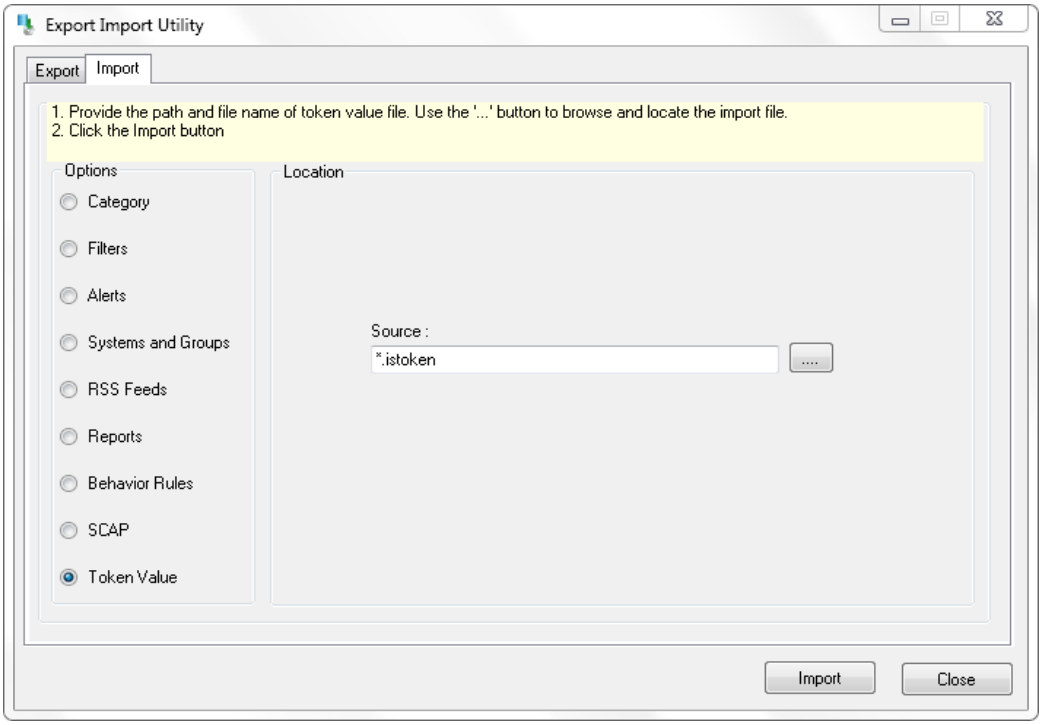

Figure 12

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

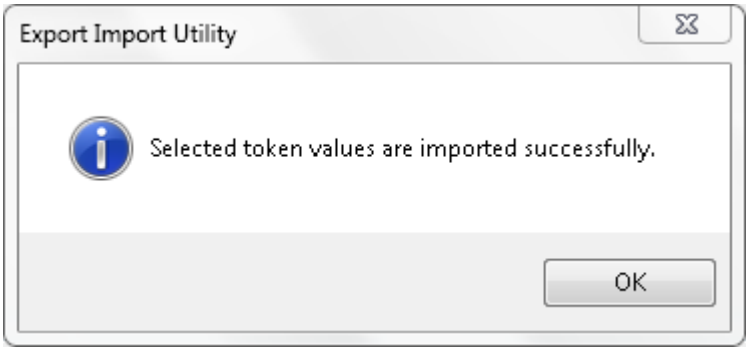

Figure 13

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'** icon.

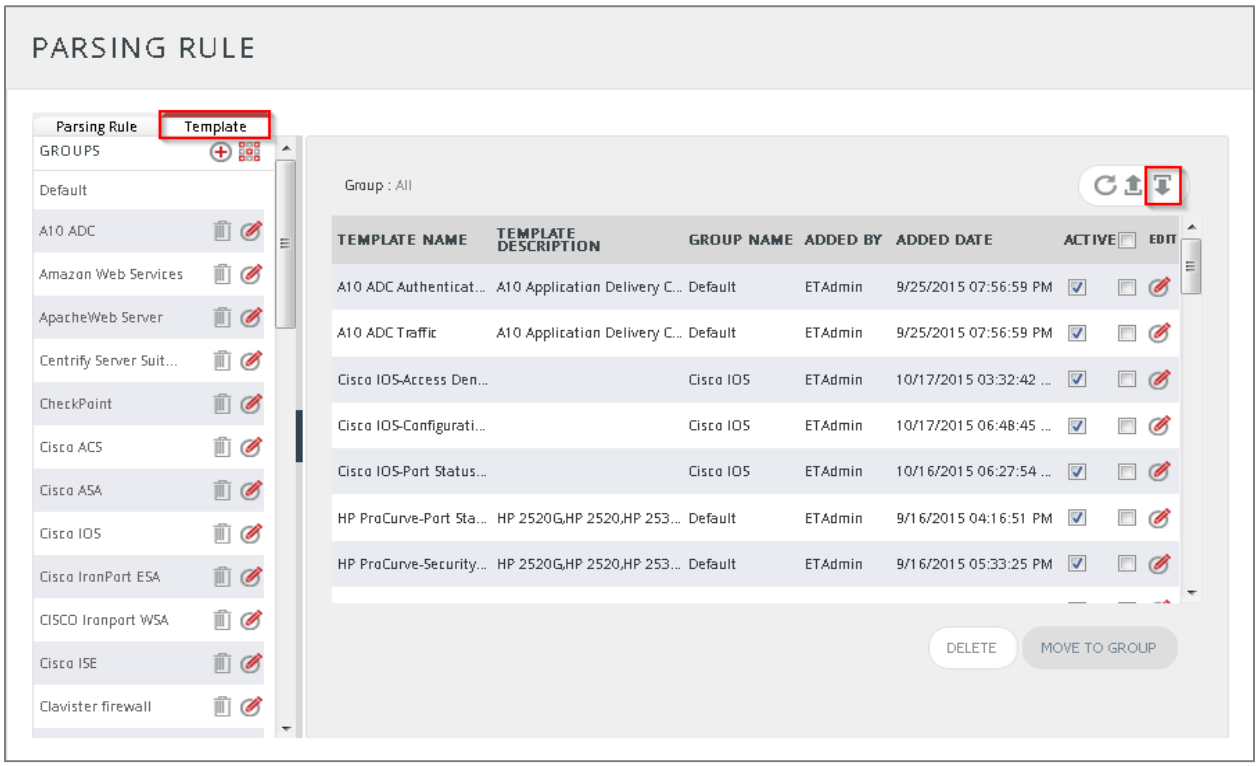

Figure 14

3. Click on **Browse** button.

Figure 15

4. Locate **Infoblox token template.ettd** file, and then click the **Open** button.

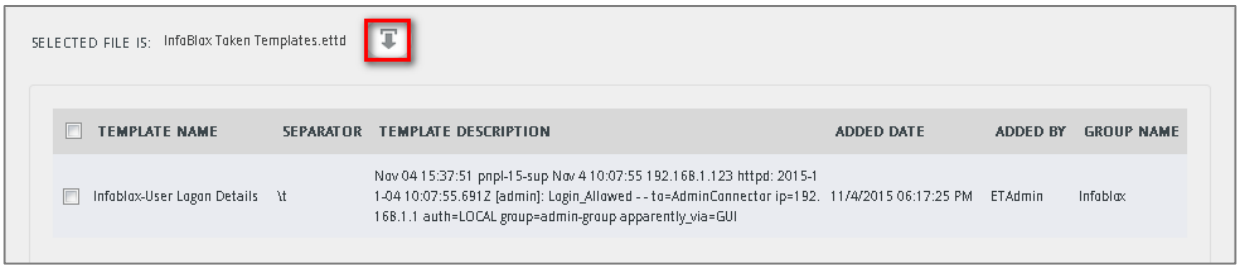

Figure 16

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

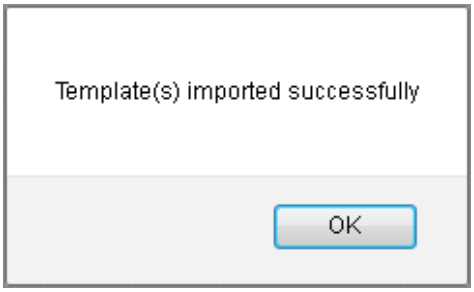

Figure 17

6. Click on **OK** button.

Import Flex Reports

1. Click **Reports** option, and then click the '**browse**' button.
2. Locate **All Infoblox group reports.issch** file, and then click the **Open** button.

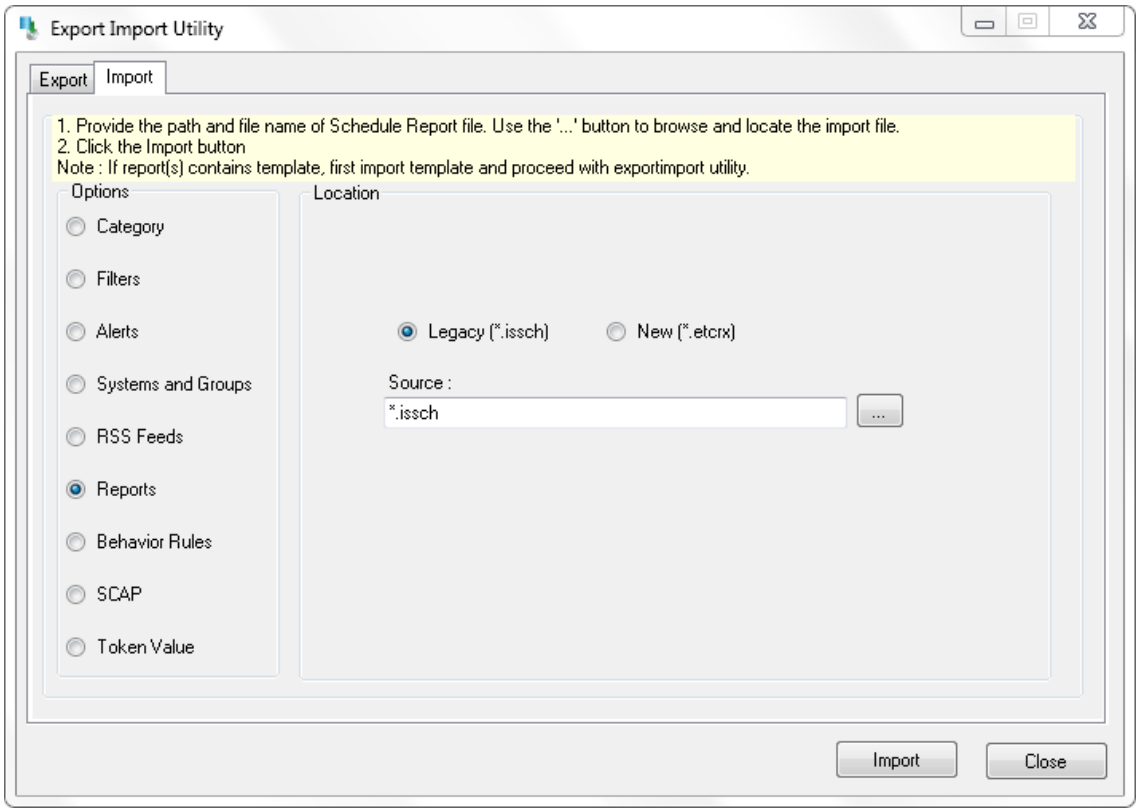

Figure 18

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

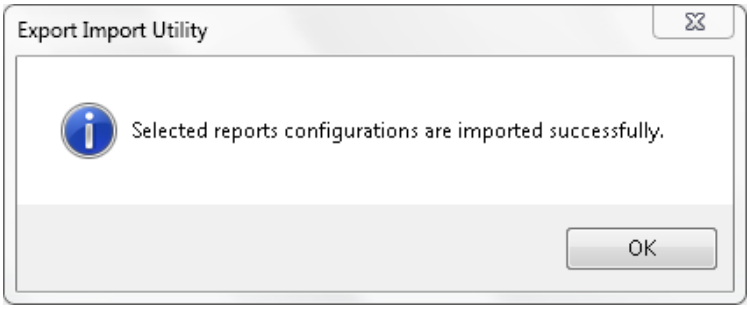

Figure 19

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

Import Filters

1. Click **Filters** option, and then click the '**browse**'  button.
2. Locate **All Infoblox group filters.issch** file, and then click the **Open** button.

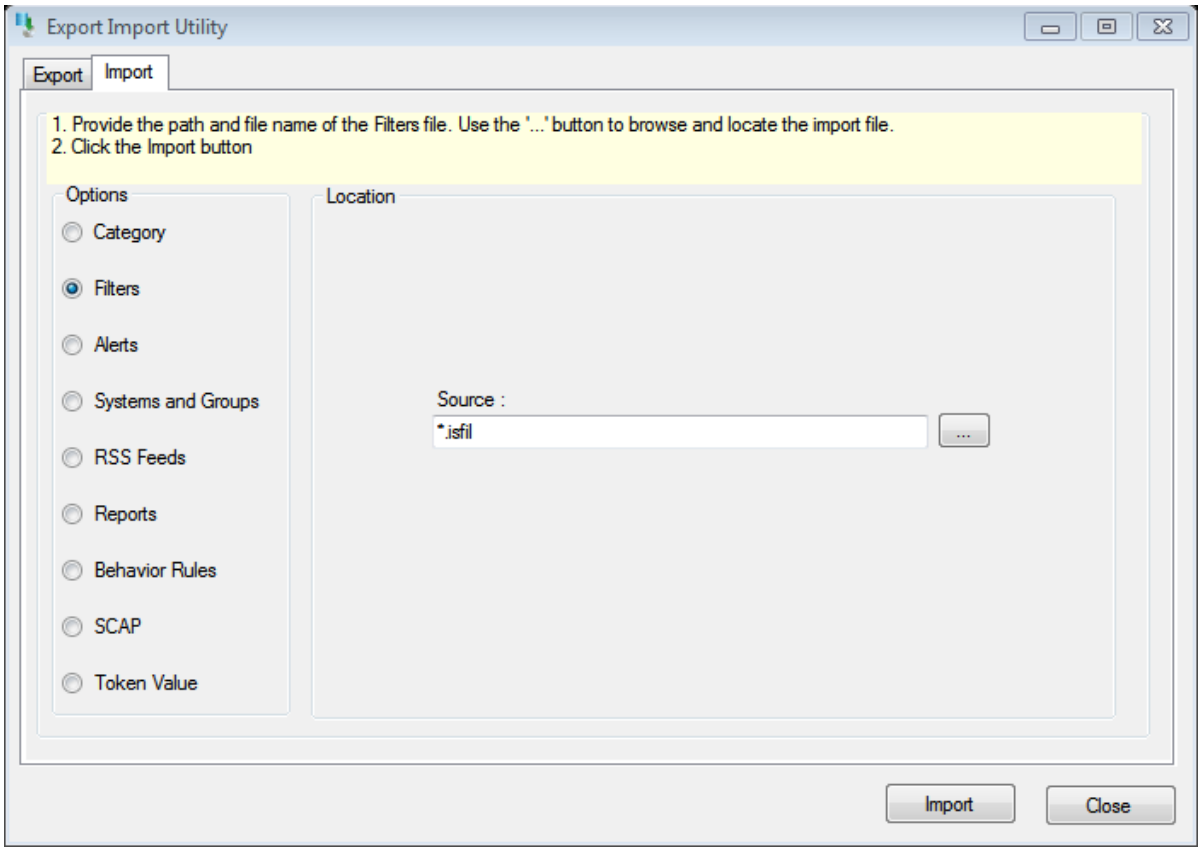

Figure 20

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

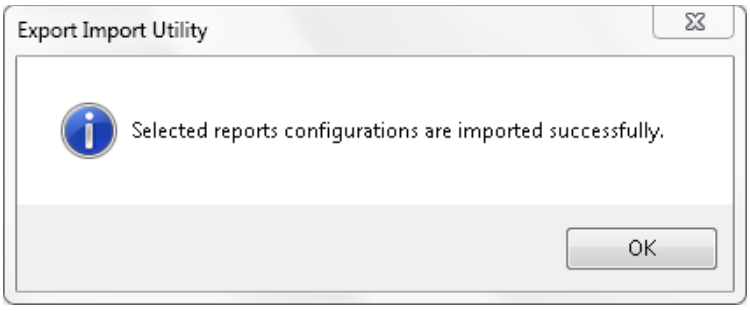

Figure 21

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

Verify Infoblox knowledge pack in EventTracker

Verify 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 **Infoblox** group folder to view the imported categories.

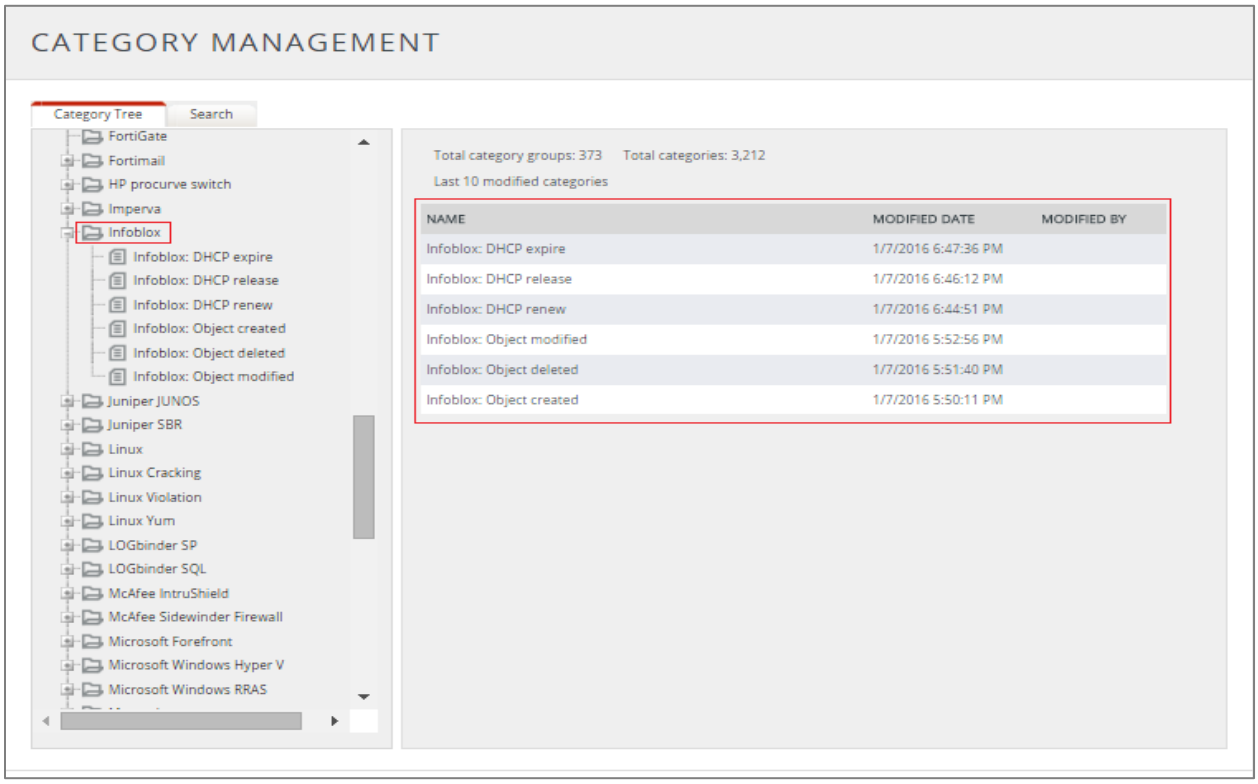

Figure 22

Verify Alerts

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

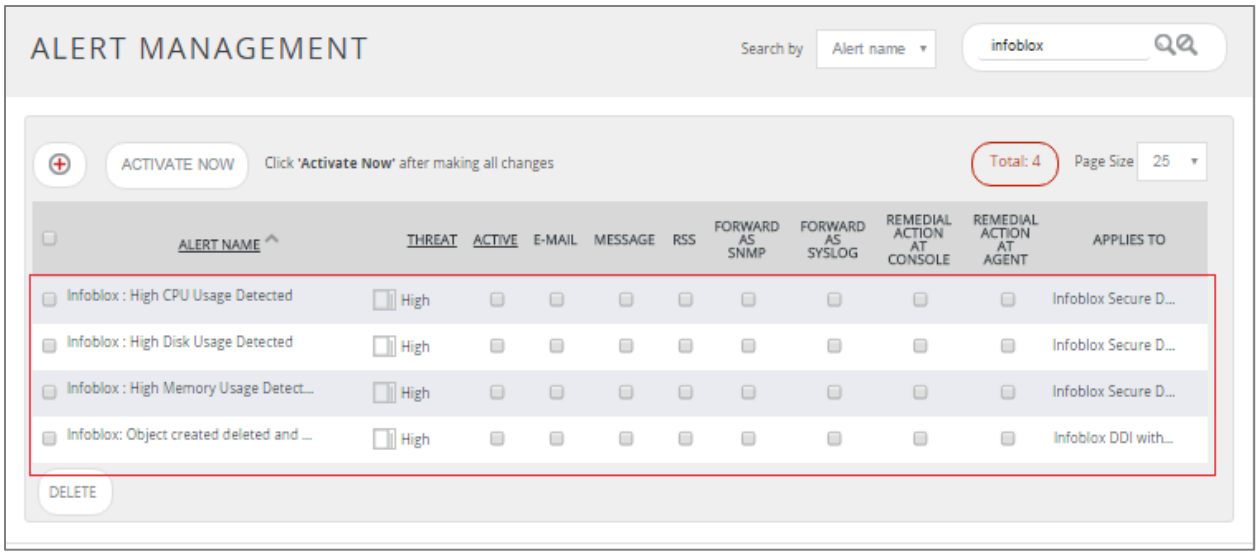

Figure 23

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

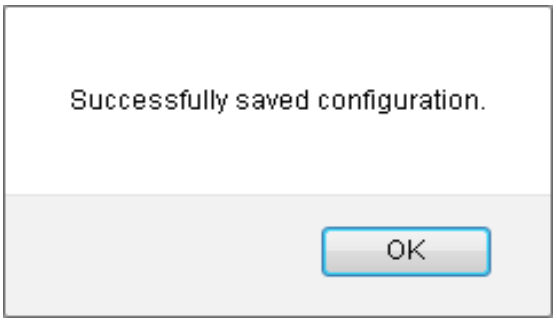

Figure 24

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

NOTE: Please specify appropriate **systems** in **Alert Configuration** for better performance.

Verify Parsing Rules

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Parsing Rules** from the dropdown options.
3. In **Token Value Group Tree** to view imported token values, scroll down and click **Infoblox group** folder.

Token values are displayed in the token value pane.

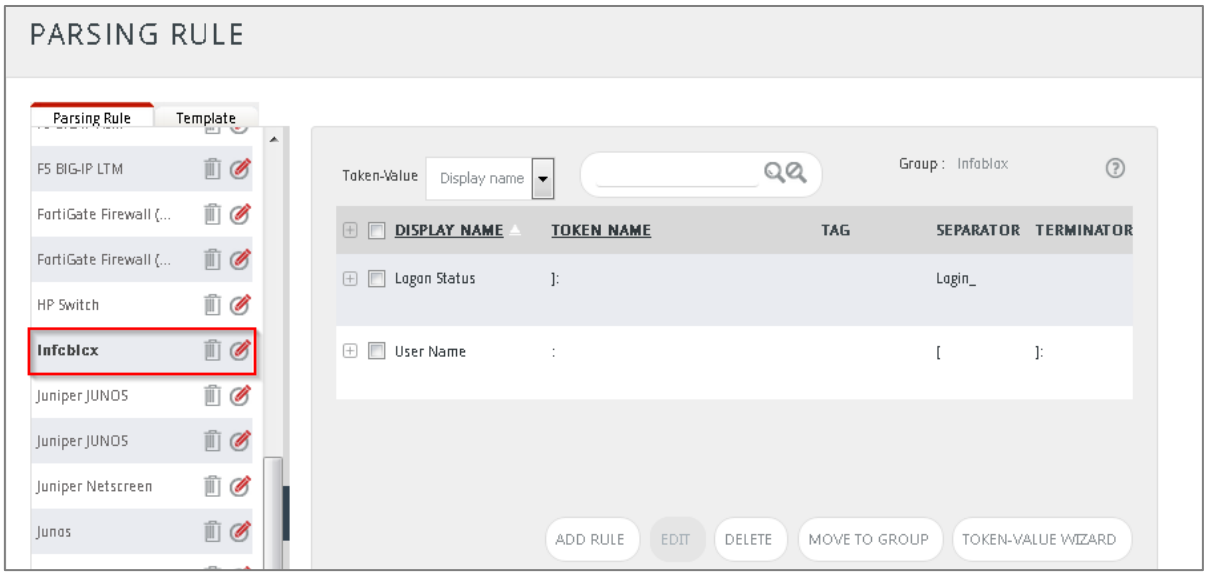

Figure 25

Verify Token Templates

1. Click the **Admin** menu, and then click **Parsing rule**.
2. Select **Template** tab.
3. In **Token Value Group Tree,** to view imported token values, scroll down and click **Infoblox group** folder.

   Imported token template is displayed in the template pane.

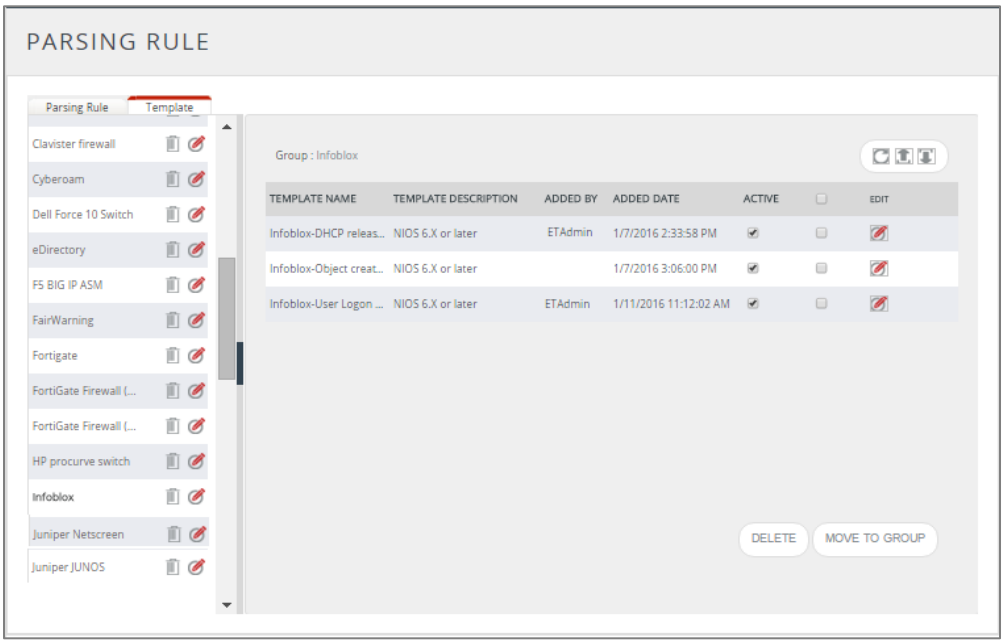

Figure 26

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 flex reports, scroll down and click **Infoblox group** folder.

   Imported Event Filters are displayed in the Event Filters Configuration pane.

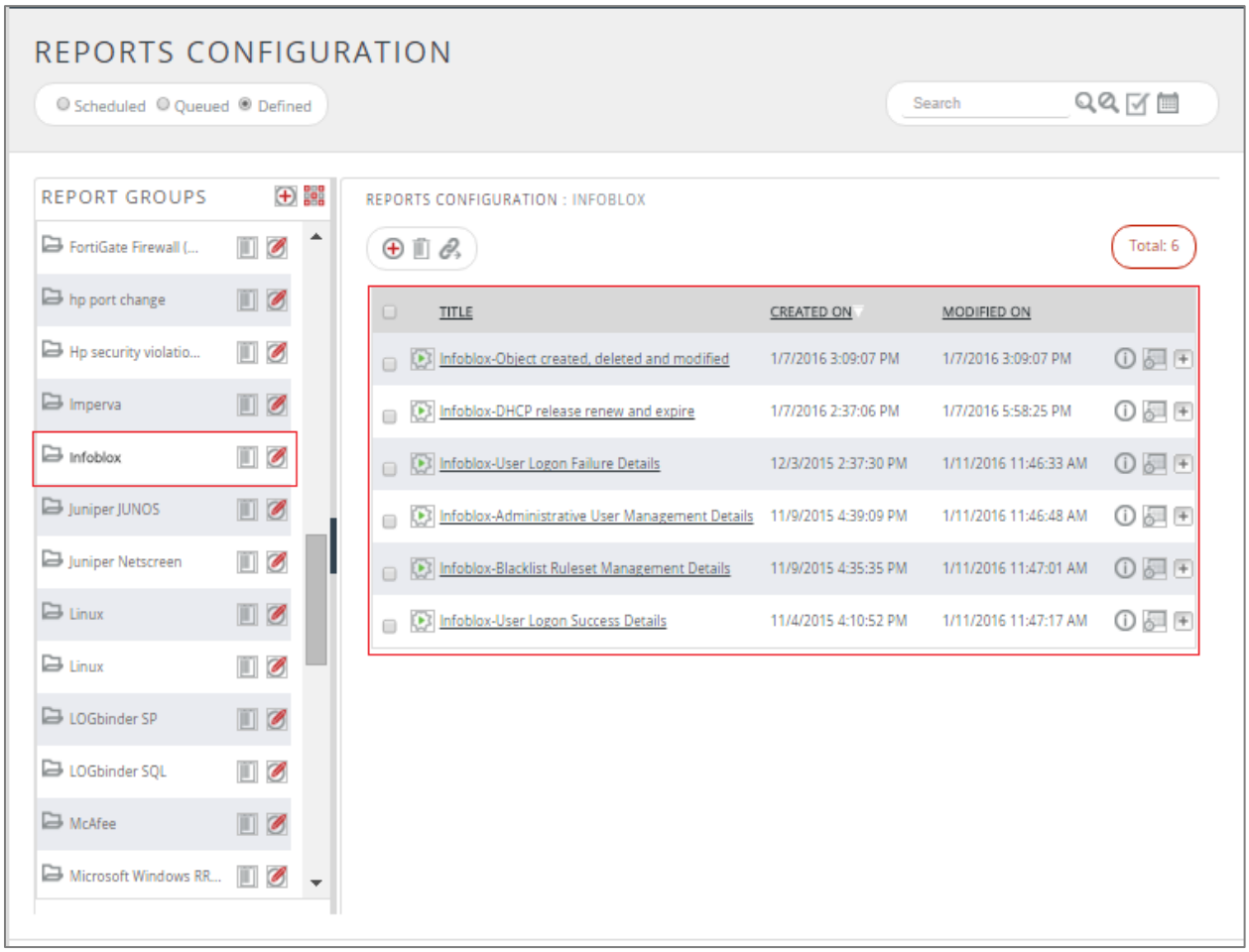

Figure 27

NOTE: Please specify appropriate **systems** in **Report Wizard** for better performance.

Verify Filters

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Event Filters**.
3. In **Event Filters Tree** to view imported **Event Filters**,

   Imported reports are displayed in the Reports Configuration pane.

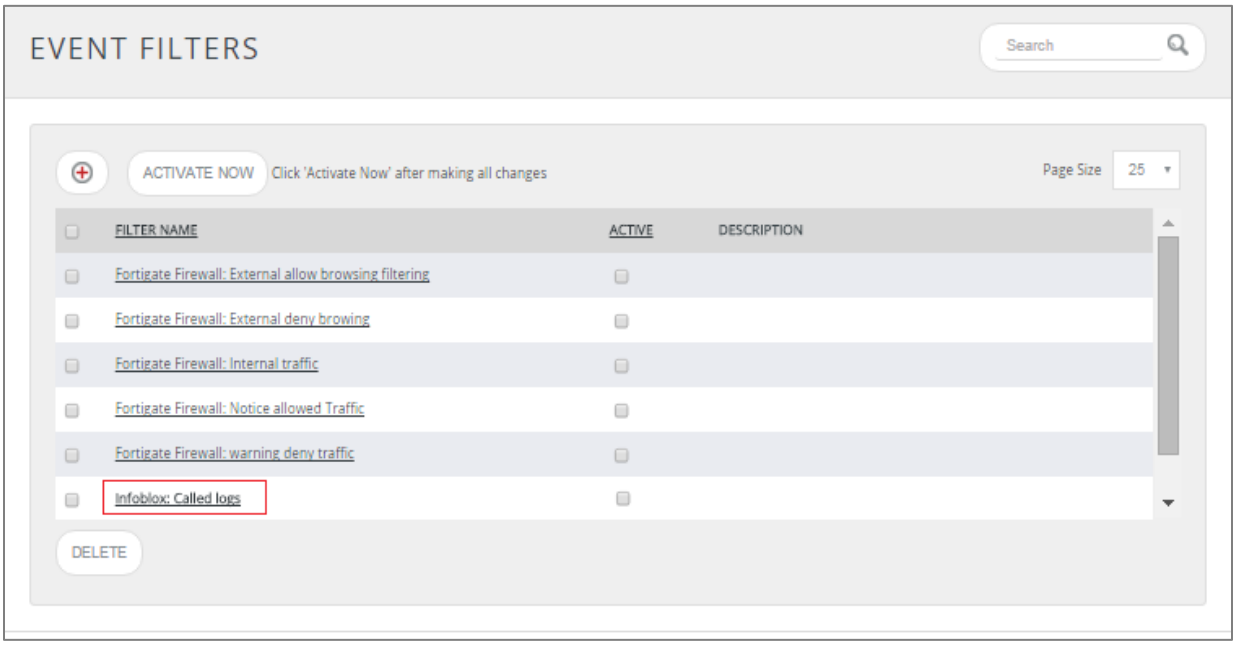

Figure 28

NOTE: Please specify appropriate **systems** in **Event Filters** for better performance.

Create Dashboards in EventTracker

Schedule Reports

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

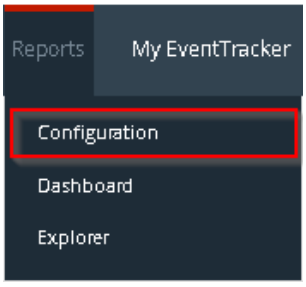

Figure 29

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

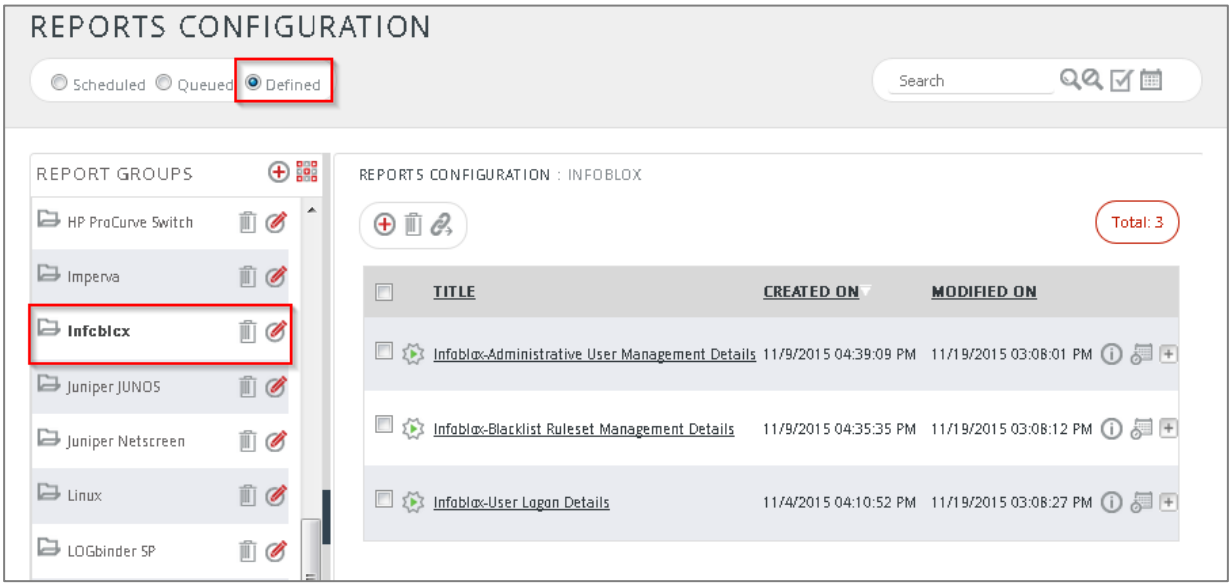

Figure 30

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

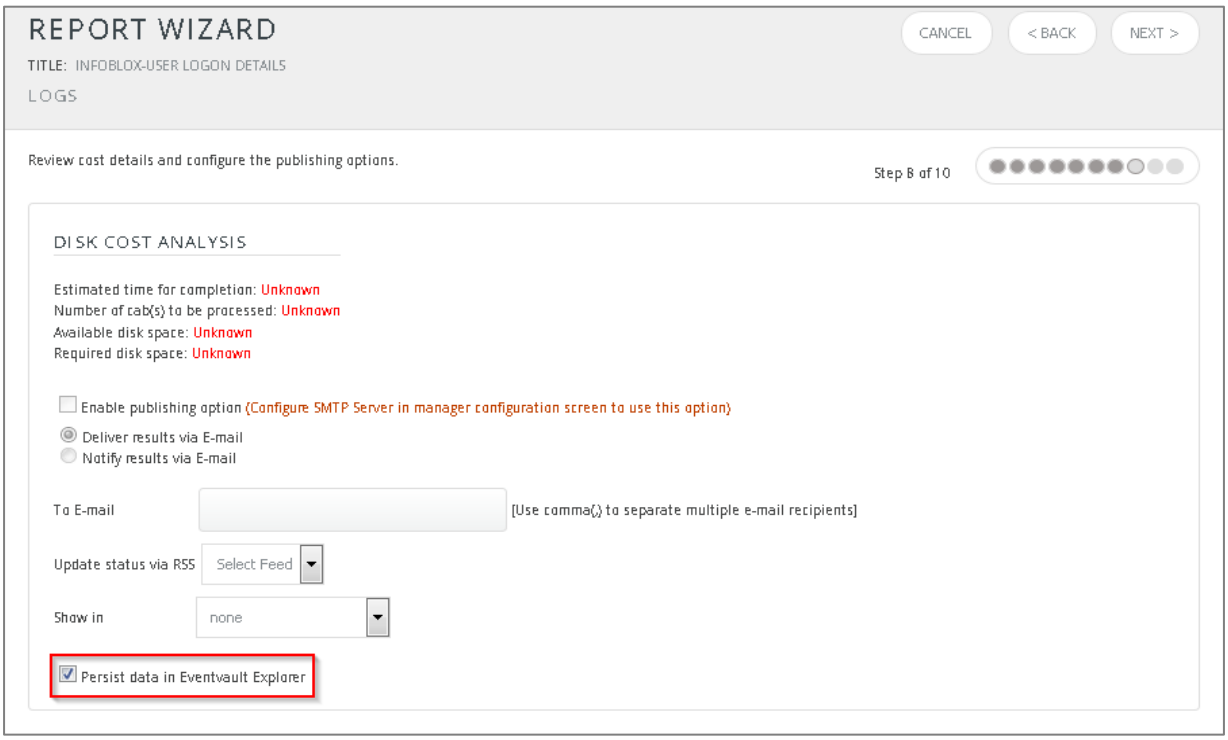

Figure 31

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

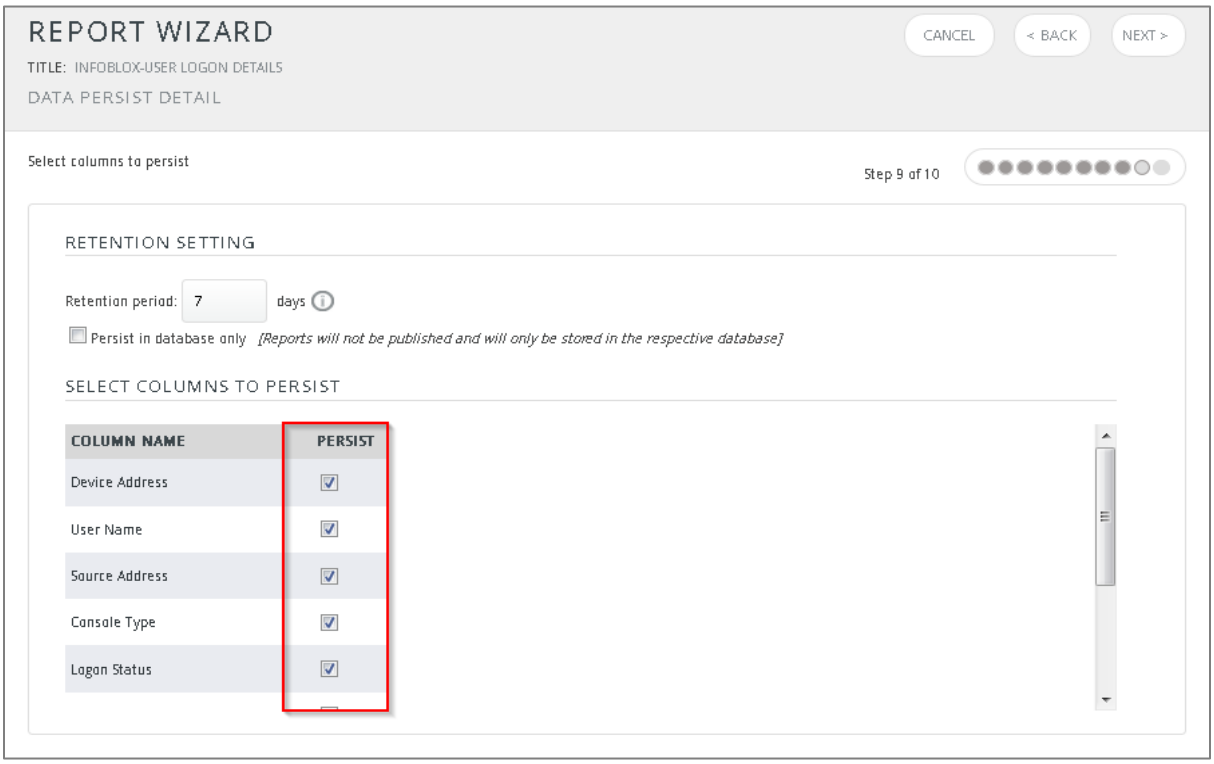

Figure 32

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 the scheduled time or generate report manually.

Create Dashlets

1. **EventTracker 8** is required to configure flex dashboard.
2. Open **EventTracker** in browser and logon.

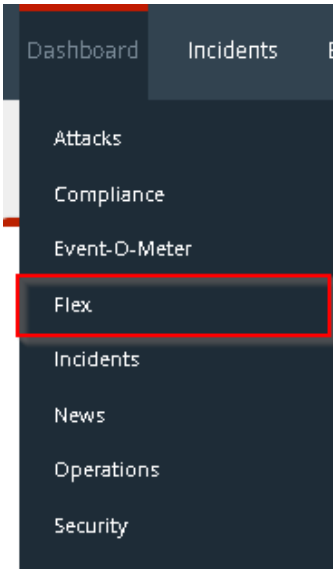

Figure 33

3. Navigate to **Dashboard>Flex**.

   Flex Dashboard pane is shown.

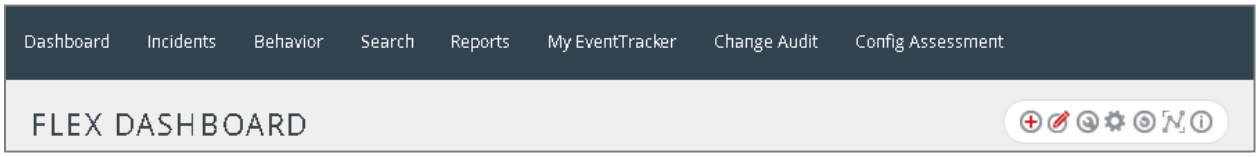

Figure 34

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

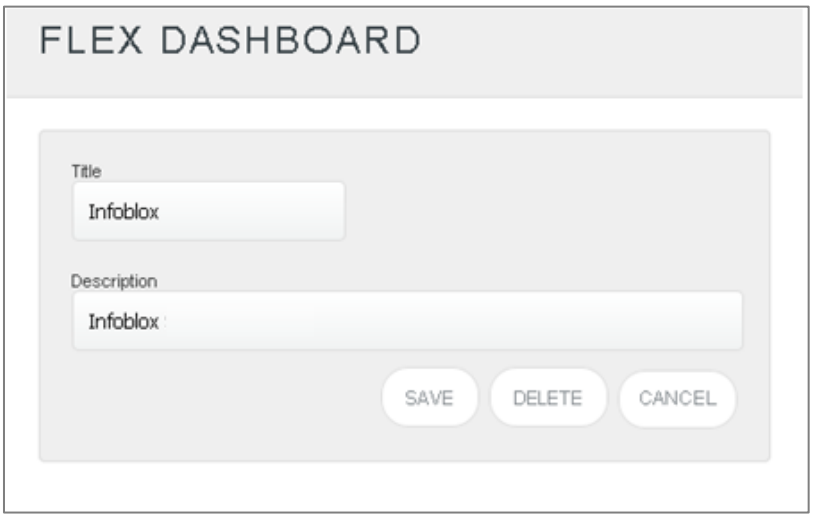

Figure 35

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

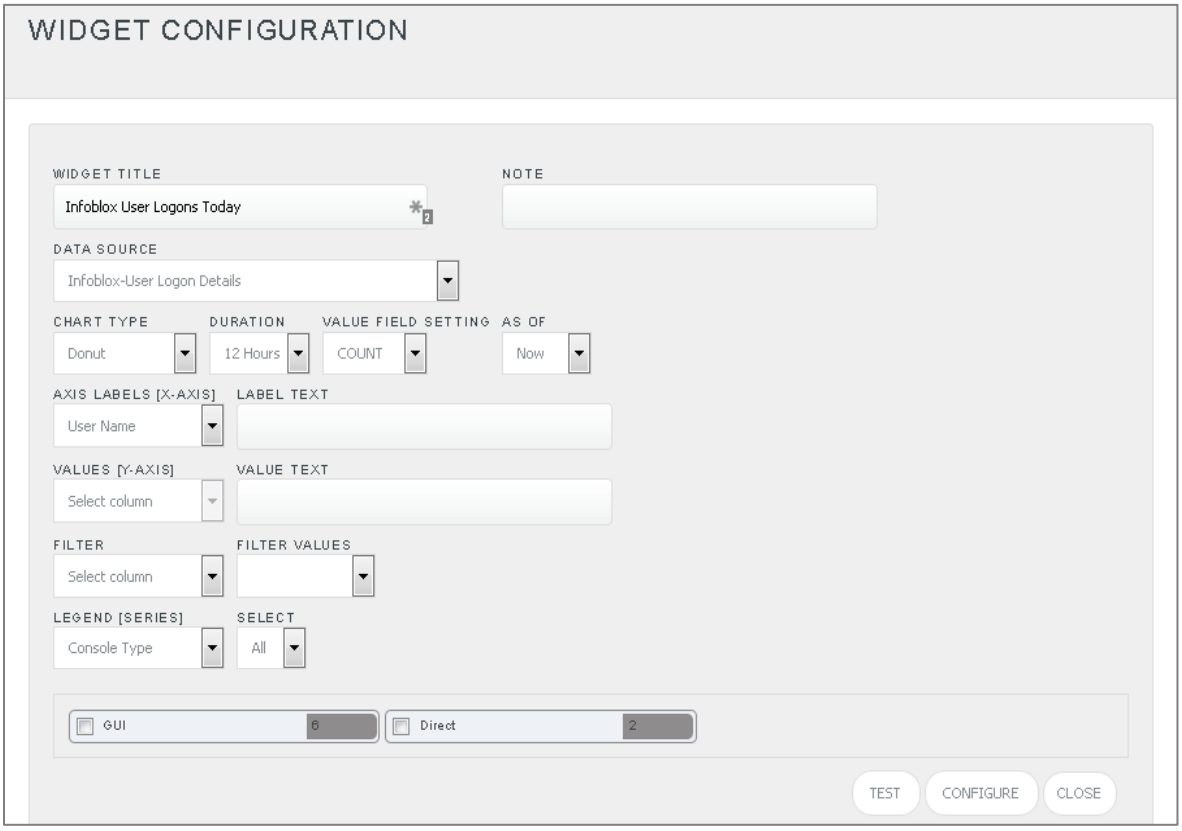

Figure 36

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.

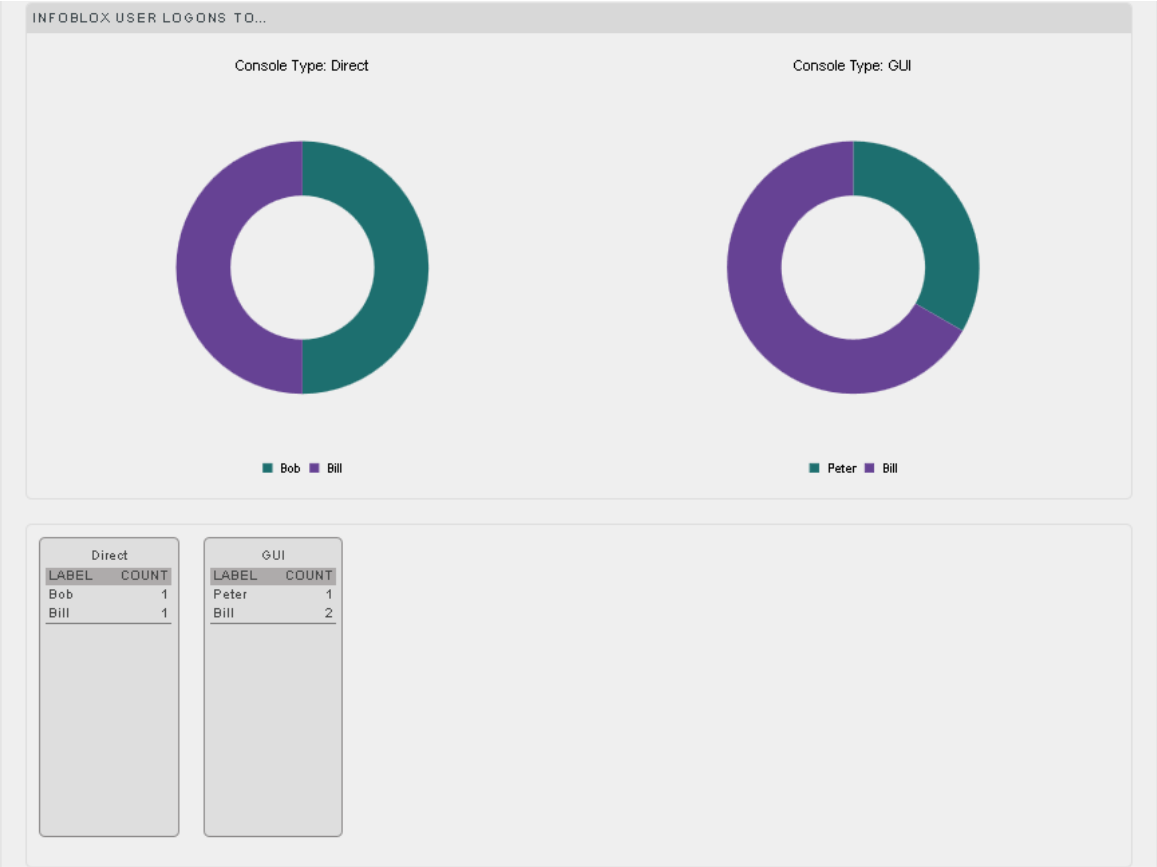

Figure 37

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

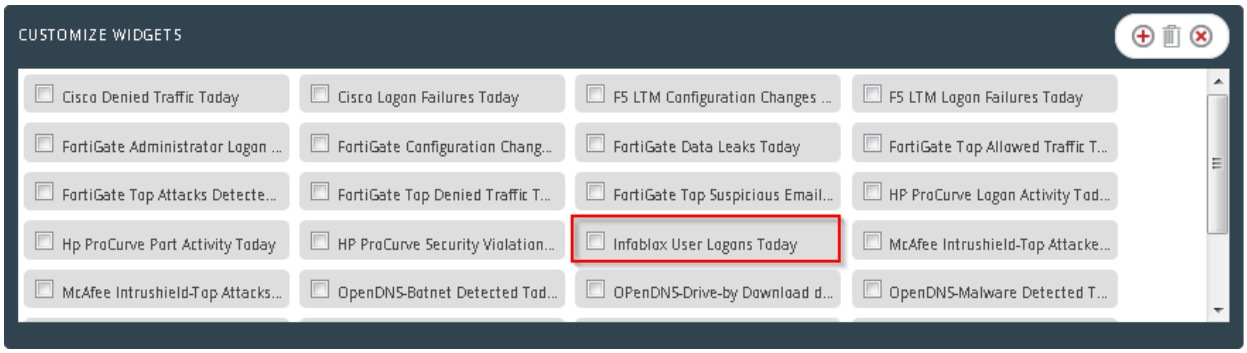

Figure 38

17. Click 'customize' to locate and choose created dashlet.
18. Click to add dashlet to earlier created dashboard.

Sample Dashboards

- **Infoblox User Logons Today**

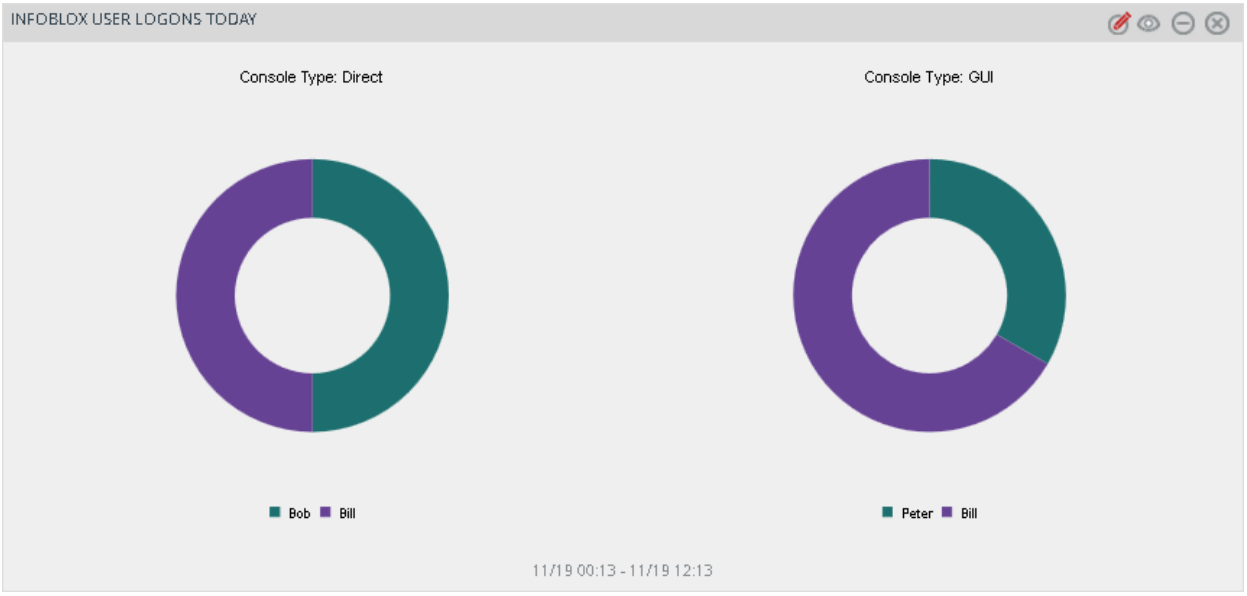

Figure 39

- **Infoblox DHCP IP assignment**

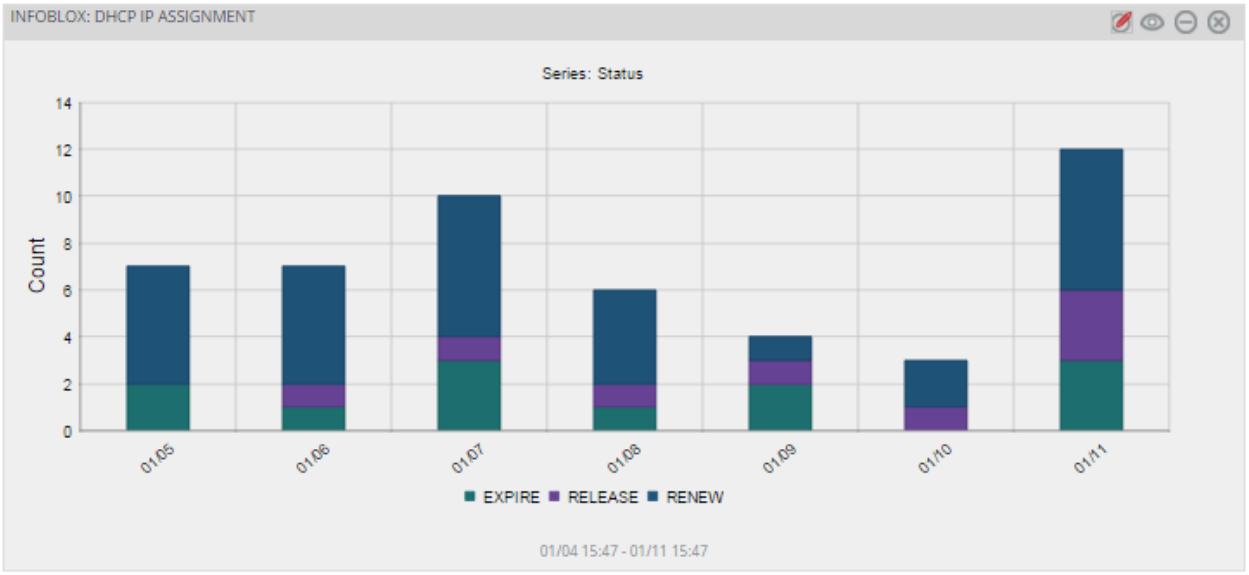

Figure 40

Sample Reports

- **Infoblox-User Logon Details**

Infoblox-User Logon Details

LogTime	Device Address	User Name	Source Address	Console Type	Authentication Type	Logon Status	Reason
11/04/2015 11:08:01 AM	192.168.1.123	Bill	192.168.1.1	GUI	LOCAL	Allowed	
11/04/2015 11:32:59 AM	192.168.1.123	Peter		Direct	Local	Allowed	
11/04/2015 11:37:22 AM	192.168.1.123	fhhdipjnf\133	192.168.1.1	GUI	Local	Denied	
11/04/2015 11:39:35 AM	192.168.1.123	Bob	192.168.1.1	GUI	Local	Denied	
11/04/2015 11:41:49 AM	192.168.1.123	Peter	192.168.1.52	GUI	Remote	Allowed	
11/04/2015 11:51:14 AM	192.168.1.123	admin	192.168.1.1	Direct	LOCAL	Allowed	
11/04/2015 12:16:21 PM	192.168.1.123	Bill	192.168.1.1	GUI	LOCAL	Allowed	
11/04/2015 12:51:57 PM	192.168.1.123	Peter	192.168.1.1	GUI	LOCAL	Allowed	
11/04/2015 01:55:14 PM	192.168.1.123	Peter	192.168.1.22	GUI	Remote	Allowed	
11/04/2015 02:13:44 PM	192.168.1.123	Bob	192.168.1.1	GUI	LOCAL	Allowed	
11/04/2015 03:37:51 PM	192.168.1.123	Peter	192.168.1.1	GUI	LOCAL	Allowed	
11/04/2015 03:44:30 PM	192.168.1.123	dzghhdz		Direct		Denied	invalid\040login\040or\040password
11/04/2015 03:45:41 PM	192.168.1.123	admin		GUI		Denied	invalid\040login\040or\040password
11/04/2015 03:45:48 PM	192.168.1.123	gsdagasrg		Direct		Denied	invalid\040login\040or\040password
11/04/2015 03:45:51 PM	192.168.1.123	gsdagasrg		Direct		Denied	failed\040logins\040exceed\040limit
11/04/2015 03:52:06 PM	192.168.1.123	Bob	192.168.1.27	GUI	Remote	Allowed	

Figure 41

- **Infoblox-DHCP IP assignment details**

Infoblox-DHCP IP assignment details

LogTime	IP address	MAC Address	Status	Lease Duration	By interface
01/07/2016 12:46:59 PM	192.168.10.200	00:50:79:66:68:00	RENEW	43200	eth1
01/07/2016 12:49:11 PM	192.168.10.200	00:50:79:66:68:00	RENEW	43067	eth1
01/07/2016 02:04:49 PM	192.168.10.200	00:50:79:66:68:00	RENEW	43200	eth1
01/07/2016 02:07:29 PM	192.168.10.197	00:50:79:66:68:01		43200	eth1
01/07/2016 02:11:06 PM	192.168.10.197	00:50:79:66:68:01	RENEW	43200	eth1
01/07/2016 02:21:42 PM	192.168.10.197	00:50:79:66:68:01	RELEASE		eth1
01/07/2016 03:31:09 PM	192.168.10.197	00:50:79:66:68:01		43200	eth1
01/07/2016 06:05:37 PM	192.168.10.198	00:50:56:c0:00:01	EXPIRE		
01/07/2016 06:22:49 PM	192.168.10.198	00:50:56:c0:00:01		43200	eth1

Figure 42