

# How To - Monitor USB device and CD/DVD for Linux OS Using rsyslog

---

*EventTracker Enterprise*

Publication Date: July 16, 2015

EventTracker  
8815 Centre Park Drive  
Columbia MD 21045  
[www.eventtracker.com](http://www.eventtracker.com)

# About this guide

This guide provides instructions to configure **Linux Operating System** to send the syslog events for USB device and CD/DVD insertion to EventTracker Enterprise.

## Scope

The configurations detailed in this guide are consistent with **EventTracker Enterprise** version **7.x and later**, and **Linux RHEL/CentOS 6 and later**.

## Audience

**Linux Operating System** users, who wish to forward syslog messages for USB device and CD/DVD insertion to EventTracker Enterprise.

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

*This document is for informational purposes only. Prism Microsystems 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 Prism, as long as its content is unaltered, nothing is added to the content and credit to Prism is provided.*

*Prism Microsystems 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 Prism Microsystems, 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.*

*© 2015 Prism Microsystems Corporation. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.*

# Table of Contents

- About this guide ..... 1
  - Scope ..... 1
  - Audience..... 1
- Prerequisite ..... 3
- Configuration ..... 3
  - Forward events to EventTracker..... 3
- Import Knowledge Pack for USB device and CD/DVD into EventTracker ..... 4
  - Import Alerts..... 4
  - Import Token Value ..... 5
  - Import Flex Reports ..... 7
- Verify Knowledge Pack for USB device and CD/DVD into EventTracker ..... 8
  - Verify Alerts ..... 8
  - Verify Token Values..... 9
  - Verify Flex Reports ..... 10
- Sample Reports ..... 11

## Prerequisite

1. EventTracker Enterprise 7.x and later should be installed.
2. Linux RHEL/CentOS 6 and later should be installed.
3. An exception should be added into Windows Firewall on EventTracker machine for syslog port 514.

## Configuration

In Linux operating system, the USB device insertion is detected automatically, but CD/DVD drive has to be mounted. These devices write logs into `/var/log/messages` file.

For mounting the CD/DVD drive, use the following configuration steps:

1. First, insert the CD or DVD in the server / laptop or desktop drive.
2. Login to the Linux machine as root.
3. Open terminal and enter the following command-

```
#mount -t iso9660 -o ro device dir
```

Specify the **device directory** like `/dev/cdrom /mnt/cdrom`

## Forward events to EventTracker

To forward USB device and CD/DVD drive messages to EventTracker Enterprise, rsyslog has to be configured.

Use the following steps to configure rsyslog in Linux OS.

1. Log on to **Linux** machine as root user.
2. Open **Terminal** window.
3. Open and edit file `/etc/rsyslog.conf` in **vi** Editor.
4. Add following line at the end of the file.

```
msg, contains, "New USB device found, idVendor=" @@10.18.1.94:514  
:msg, contains, ": Mounting volume" @@10.18.1.94:514
```

**NOTE:** **10.18.1.94** mentioned above should be replaced with the IP address of EventTracker machine's IP. 514 is the default port for syslog.

4. Save the file.

5. Restart the rsyslog service.

#### # service rsyslog restart

6. Now, logon to EventTracker Enterprise and verify the events.


## Import Knowledge Pack for USB device and CD/DVD into EventTracker

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

Import **Alerts/Tokens/Flex Reports** as given below.

**NOTE-** To get the Alert, Tokens and Flex Report files please contact Technical Support via e-mail at [support@eventtracker.com](mailto:support@eventtracker.com).

### Import Alerts

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

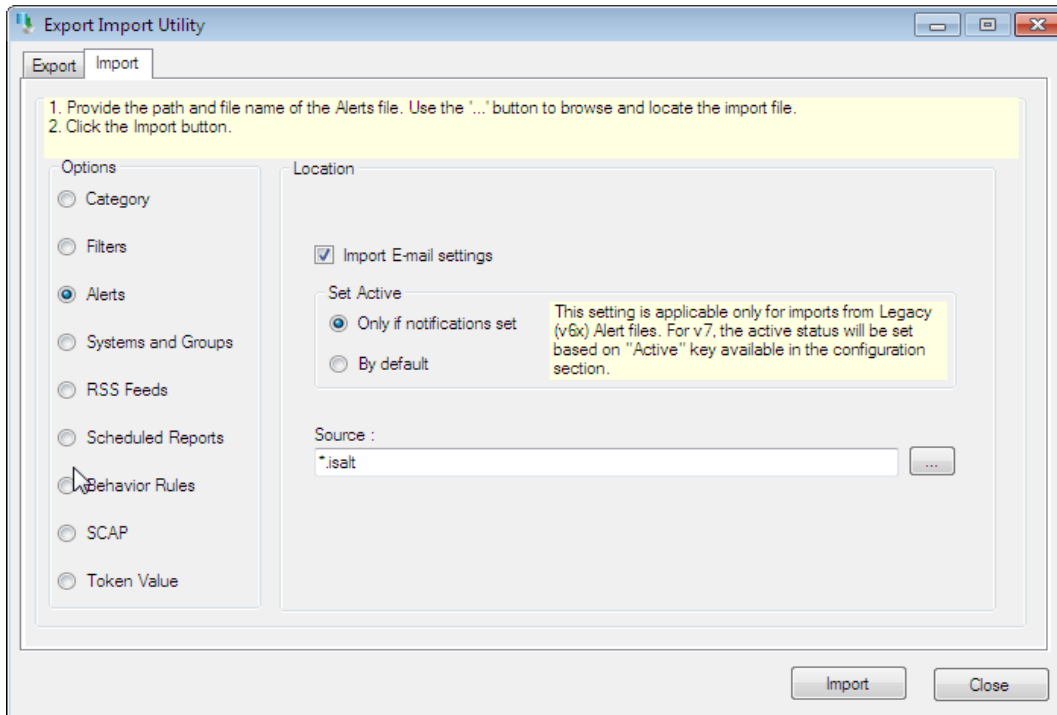


Figure 1

2. Locate **Linux USB device and CD DVD Alert.isalt** file, and then click the **Open** button.
3. To import alerts, click the **Import** button.

EventTracker displays success message.

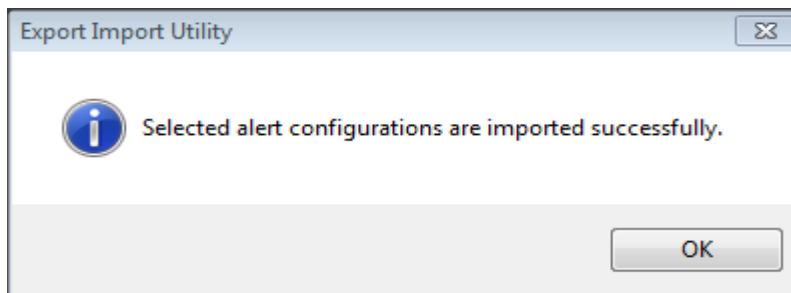



Figure 2

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 **Linux USB device and CD DVD Tokens.istoken** file, and then click the **Open** button.

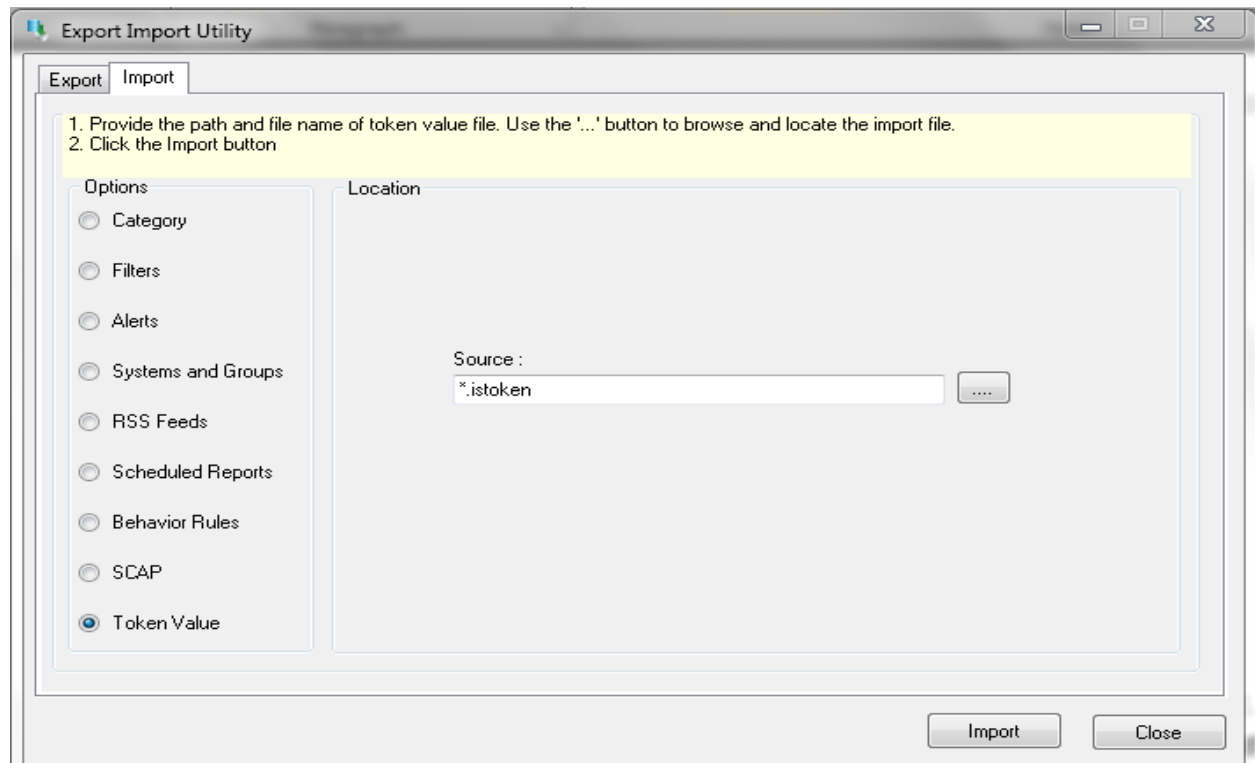


Figure 3

3. To import token value, click the **Import** button.

EventTracker displays success message.

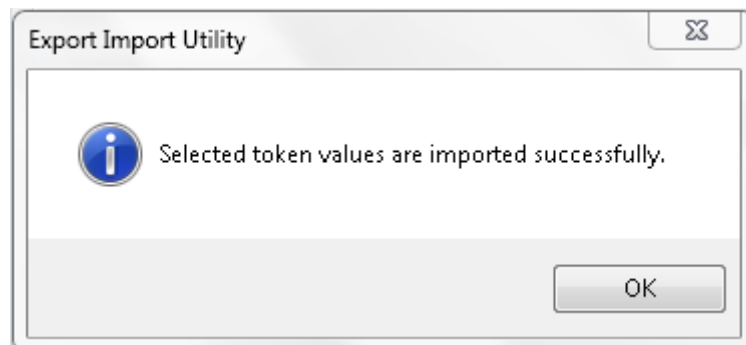



Figure 4

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 **Linux USB device and CD DVD Flex Reports.issch** file, and then click the **Open** button.

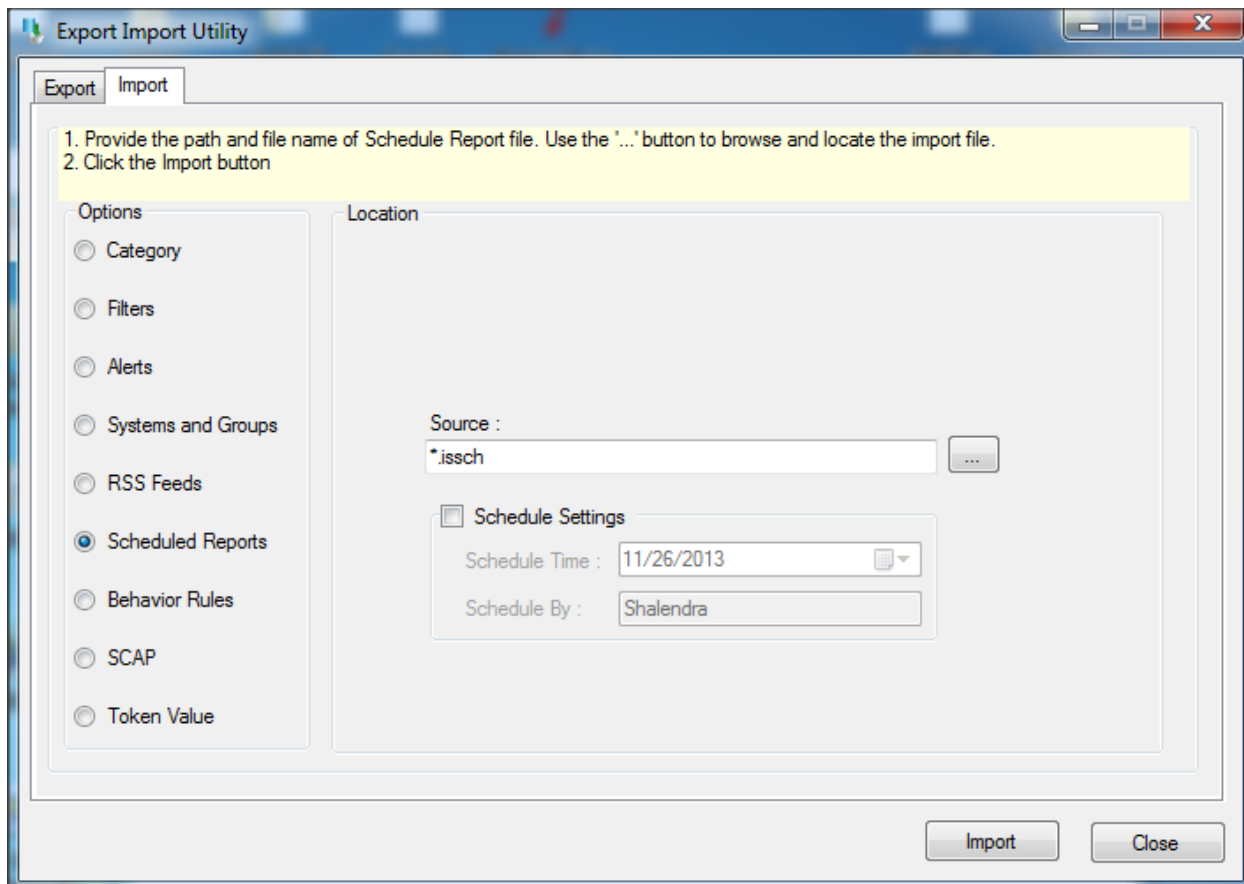


Figure 5

3. To import scheduled reports, click the **Import** button.

EventTracker displays success message.

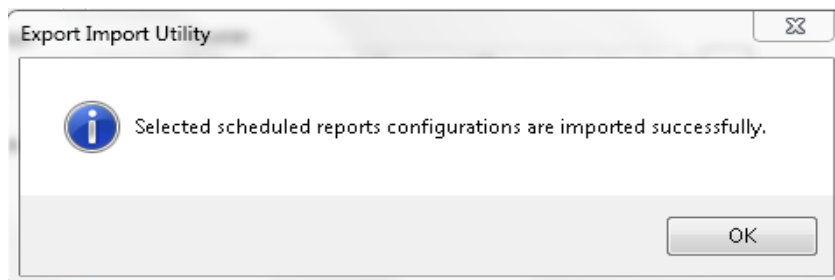


Figure 6



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

## Verify Knowledge Pack for USB device and CD/DVD into EventTracker

### Verify Alerts

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Alerts**.
3. In **Search** field, type '**Linux**', and then click the **Go** button.

Alert Management page will display all the imported Linux alerts.

ALERT MANAGEMENT linux 🔍

**ACTIVATE NOW** Click 'Activate Now' after making all changes Page Size 25 ▼

<input type="checkbox"/>	<u>ALERT NAME</u> ^	THREAT	ACTIVE	E-MAIL	MESSAGE	RSS	FORWARD AS SNMP	FORWARD AS SYSLOG	REMEDIAL ACTION AT CONSOLE	REMEDIAL ACTION AT AGENT	APPLIES TO
<input type="checkbox"/>	Linux High CPU Usage Alert	High	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	RHEL/CentOS 6.x
<input type="checkbox"/>	Linux High Memory Usage Alert	High	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	RHEL/CentOS 6.x
<input type="checkbox"/>	Linux High Process Usage Alert	High	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	RHEL/CentOS 6.x
<input type="checkbox"/>	Linux Low Disk Space Alert	High	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	RHEL/CentOS 6.x
<input type="checkbox"/>	Linux: CD/DVD insertion detected	Serious	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	RHEL/CentOS 6 a...
<input type="checkbox"/>	Linux: USB device insertion detected	Serious	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	RHEL/CentOS 6 a...

Figure 7

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

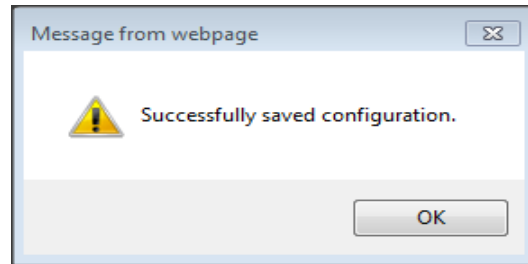


Figure 8

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 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 **Linux** group folder. Token values are displayed in the token value pane.

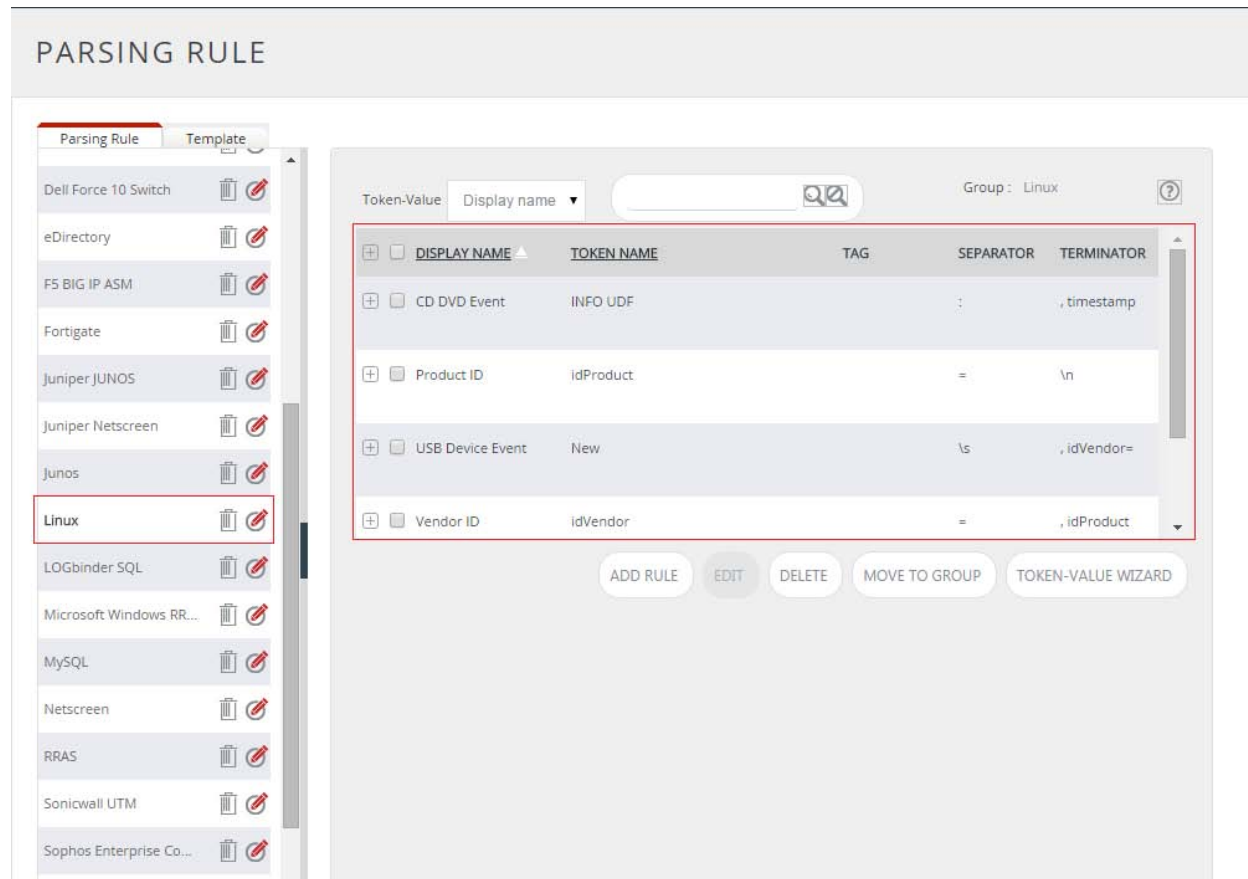


Figure 9

## 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 **Linux** group folder. Scheduled Reports are displayed in the Reports configuration pane.

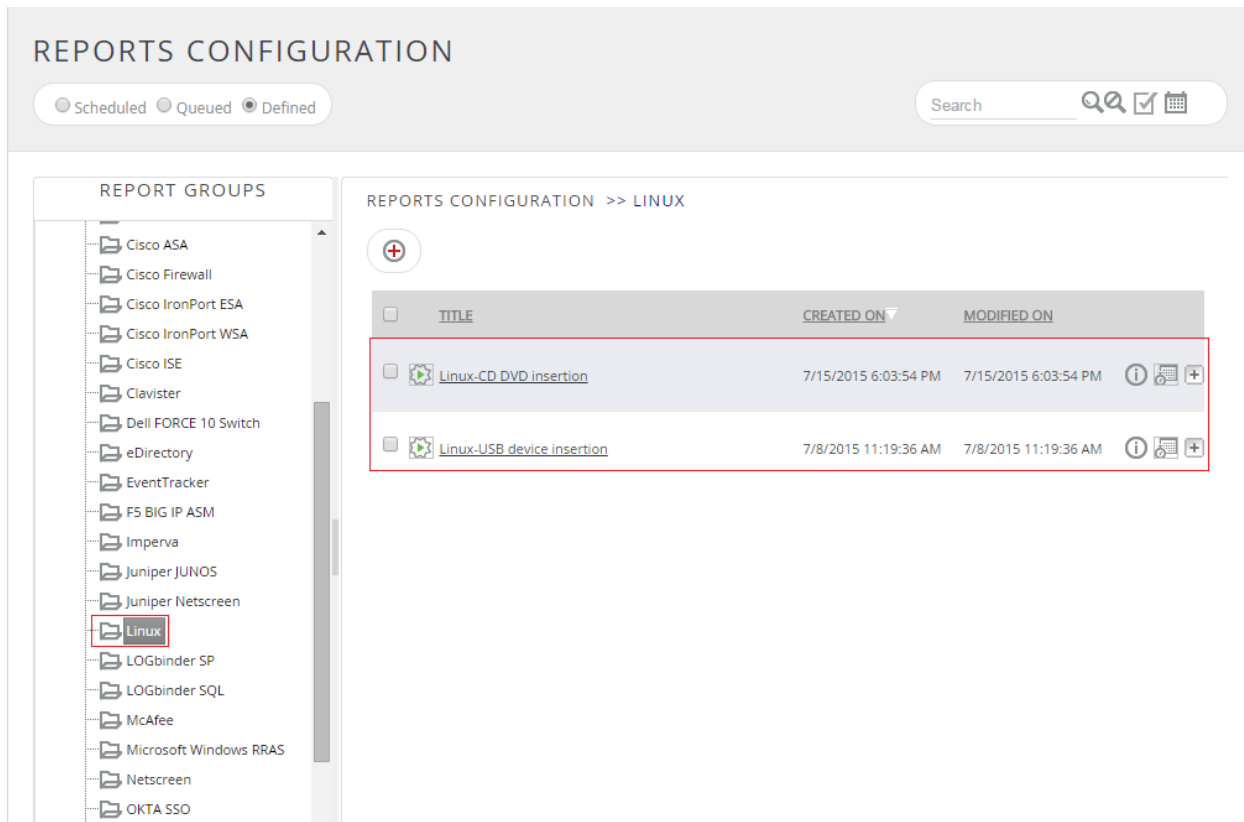


Figure 10

## Sample Reports

### 1. Linux-USB device insertion

**Linux-USB device insertion**

LogTime	Computer	USB Event	Product ID	Vendor ID
07/11/2015 12:02:19 PM	10.10.1.126-syslog	USB device found	5a07	03f0
07/12/2015 10:10:03 PM	10.10.1.132-syslog	USB device found	4b05	03f1
07/13/2015 11:02:13 PM	10.10.1.45-syslog	USB device found	5a07	08z3
07/14/2015 09:11:25 PM	10.10.1.66-syslog	USB device found	3d09	05f8
07/15/2015 03:25:20 PM	10.10.1.80-syslog	USB device found	1g06	09f0
07/16/2015 06:13:17 PM	10.10.1.89-syslog	USB device found	4j07	08f0

Figure 11

### 2. Linux-CD DVD insertion

## Linux-CD DVD insertion

LogTime	Computer	CD DVD Event
07/15/2015 06:07:35 PM	10.10.1.29-syslog	Mounting volume 'UDF Volume'
07/15/2015 03:14:30 PM	10.10.1.31-syslog	Mounting volume 'Sample Volume'
07/16/2015 04:16:17 PM	10.10.1.09-syslog	Mounting volume 'Financial Data'
07/16/2015 06:07:35 PM	10.10.1.45-syslog	Mounting volume 'Blank'
07/17/2015 04:27:16 PM	10.10.1.85-syslog	Mounting volume 'Jurassic Park'
07/17/2015 06:07:36 PM	10.10.1.56-syslog	Mounting volume 'Democracy'

Figure 12