

# EventTracker: DLA Extension for Linux Audit Report

---

## *Integration Guide*

*Auditd Reports*

# About This Guide

## Abstract

Modern Linux kernel (2.6.x) comes with Auditd daemon. During startup it writes audit records on the disk and the rules in /etc/audit.rules files are read by this daemon. The changes such as setup audit file log location and other options, you can open this file. To get started with Auditd, default file are good enough. This document is designed to help Install, Configure, and Schedule Audit report generation on Linux and configure DLA Extension report in EventTracker.

## Purpose

The purpose of this document is to help users to Install Configure and Schedule Audit report generation on Linux and configure DLA Extension report in EventTracker.

## Intended Audience

EventTracker users who wish to generate Audit report for Linux machines and transferring those reports to EventTracker via DLA Extension.

*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, Inc. must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Prism Microsystems, Inc. and Prism Microsystems, Inc. cannot guarantee the accuracy of any information presented after the date of publication.*

*This document is for informational purposes only. Prism Microsystems, Inc. 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 Guide 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, Inc. 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, Inc. 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.*

*© 2013 Prism Microsystems, Inc. All rights reserved.*

*The names of actual companies and products mentioned herein may be the trademarks of their respective owners.*

## Table of Contents

Install and Configure Auditd in Linux .....	3
Install Auditd package if not installed .....	3
Configure Auditd .....	3
Setup Audit Rules .....	3
Generate audit report .....	4
Transfer audit report to EventTracker Manager .....	4
Configure DLA-Extension to Import Audit Report to EventTracker.....	6

# Install and Configure Auditd in Linux

## Install Auditd package if not installed

- yum install audit
- chkconfig Auditd on

## Configure Auditd

Modify Auditd .conf .Following parameter should be setup correctly.

```
log_file = /var/log/audit/audit.log
log_format = RAW
priority_boost = 3
flush = sync
freq = 20
#num_logs = 4
dispatcher = /sbin/audispd
disp_qos = lossy
max_log_file = 5
max_log_file_action = keep_logs
space_left = 75
space_left_action = SYSLOG
action_mail_acct = root
admin_space_left = 50
admin_space_left_action = syslog
disk_full_action = SUSPEND
disk_error_action = SUSPEND
```

## Setup Audit Rules

Modify audit.rules for the file and folder you want to enable auditing. Start AuditD and configure to start automatically on system startup.

```
# chkconfig AuditD on
# /etc/init.d/AuditD start
```

## Generate audit report

Using aureport, different reports can be generated and exported to file. Below are some examples.

```
aureport --success > /home/auditsuccess.log
aureport --failed > /home/auditfailed.log
aureport -f -i --failed --summary > /home/fileaccessfailure.log
aureport -l -l > /home/loginreport.log
aureport -l -i --failed > /home/Loginfailure.log
aureport -l -i --success > /home/Loginsuccess.log
```

## Transfer audit report to EventTracker Manager

Audit report files should be transferred to EventTracker Manager System at scheduled interval. It can be daily, Weekly. It can be done by creating shell script and scheduling it to run in cron. Below is the sample script.

```
e=`date +%m%d%Y%H`
cd /var/log/audit
mv /var/log/audit/audit.log /home/auditlog/audit${e}.log
rcAuditD restart
cd /home/auditlog/

# summary report of all events
aureport -if /home/auditlog/audit${e}.log >
/home/auditlog/AuditSummary${e}.txt
# Summary report for Success events
aureport --success -if /home/auditlog/audit${e}.log >
/home/auditlog/AuditSummary${e}.txt
# Summary report for failed events
aureport --failed -if /home/auditlog/audit${e}.log >
/home/auditlog/AuditFailedSummary${e}.txt
# Failed File Summary Report
aureport -f -i --failed -if /home/auditlog/audit${e}.log >
/home/auditlog/FailedFileSummary${e}.txt
```

# Transferring files to EventTracker Server

```
HOST='ServerName'  
USER='ftpuser'  
PASSWD='FtpUserpassword'  
ftp -nvA <<EOF  
open $HOST  
user $USER $PASSWD  
cd /DLAExtension/AuditD  
lcd /home/auditlog/  
prompt off  
put audit$.log  
mput *.txt  
EOF  
rm /home/auditlog/*.txt
```

**NOTE:** - Audit log path, and ftp server info must be changed accordingly.

# Configure DLA-Extension to Import Audit Report to EventTracker

1. Open **EventTracker Enterprise**.
2. Type valid user credentials and then click **Login**.
3. Click the **Admin** dropdown, and then click **Manager**.

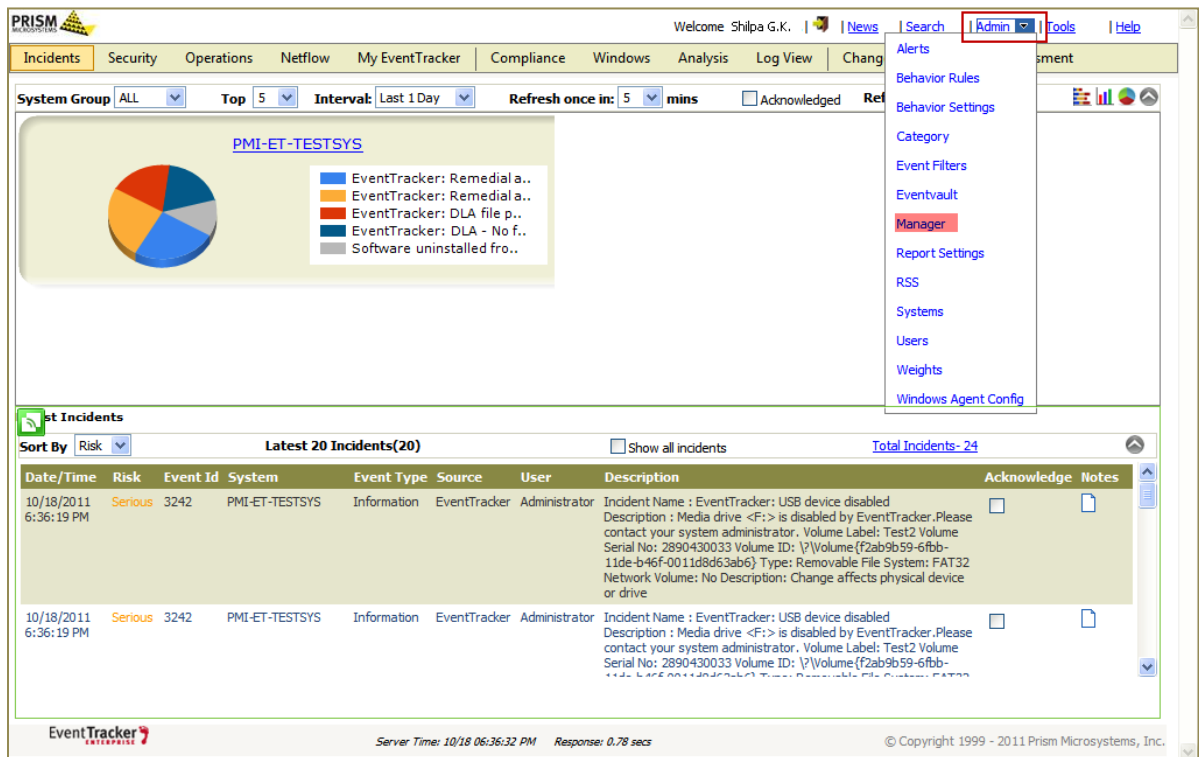


Figure 1: Incidents Dashboard

EventTracker displays the **Manager Configuration** page.

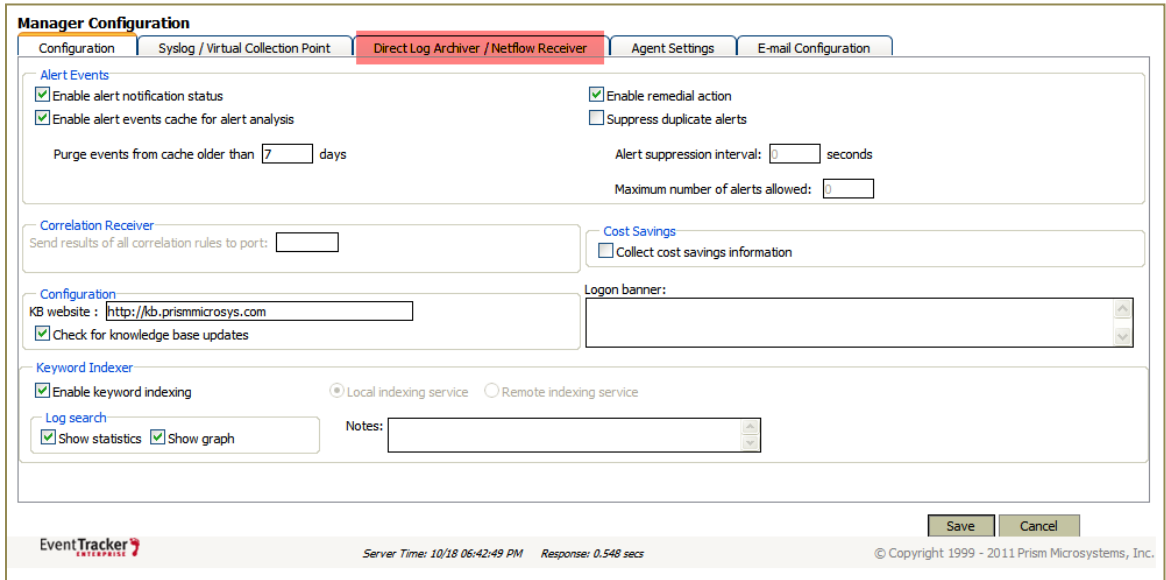


Figure 2: Manager Configuration

4. Click **Direct Log Archive/NetFlow Receiver** tab.
5. Select **Direct log file archiving from external sources** option, and then select VCP port from **Associated virtual collection point** dropdown.

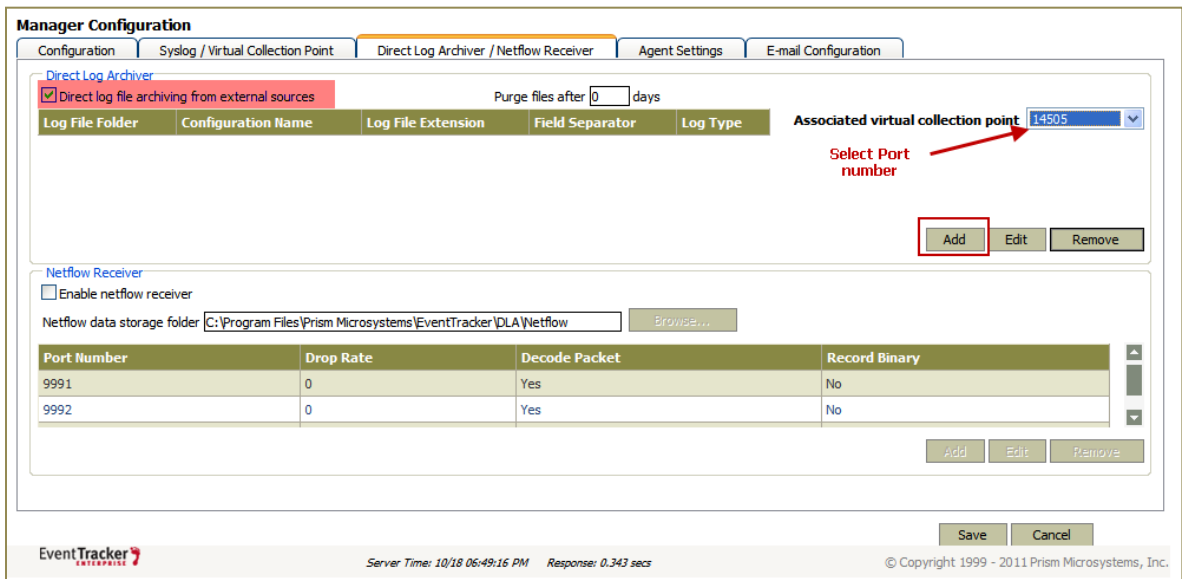


Figure 3

6. Click the **Add** button.
- EventTracker displays the Direct Archiver Configuration pop-up window.



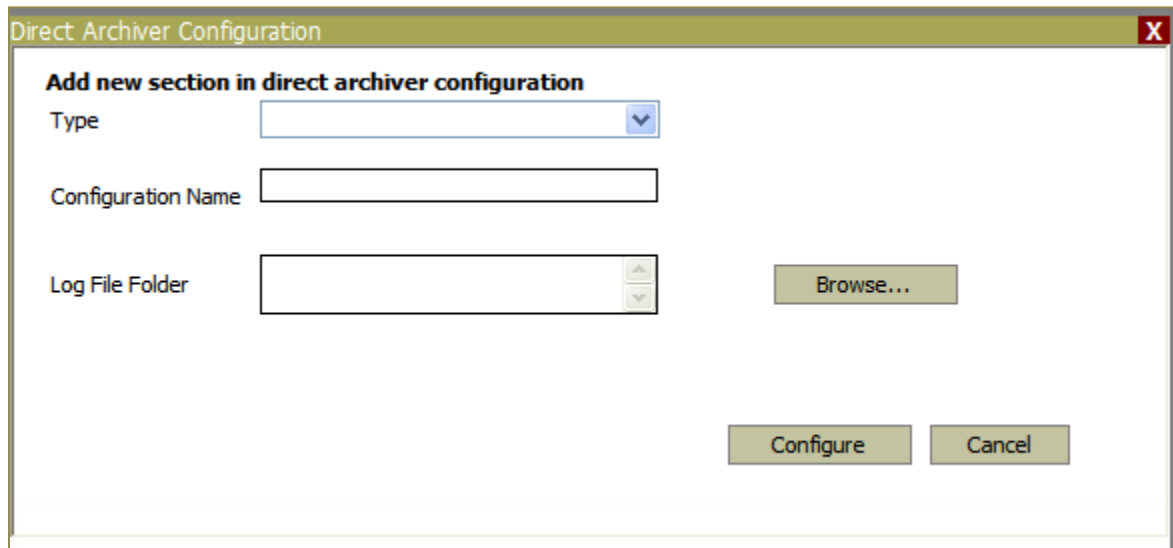


Figure 4

- Select **DLA-Extension** from Type dropdown.
- Type [AuditD.ini](#) as Configuration Name.
- Click the **Browse** button and select path of audit report file.
- Click the **Configure** button.  
Refer Figure 5.

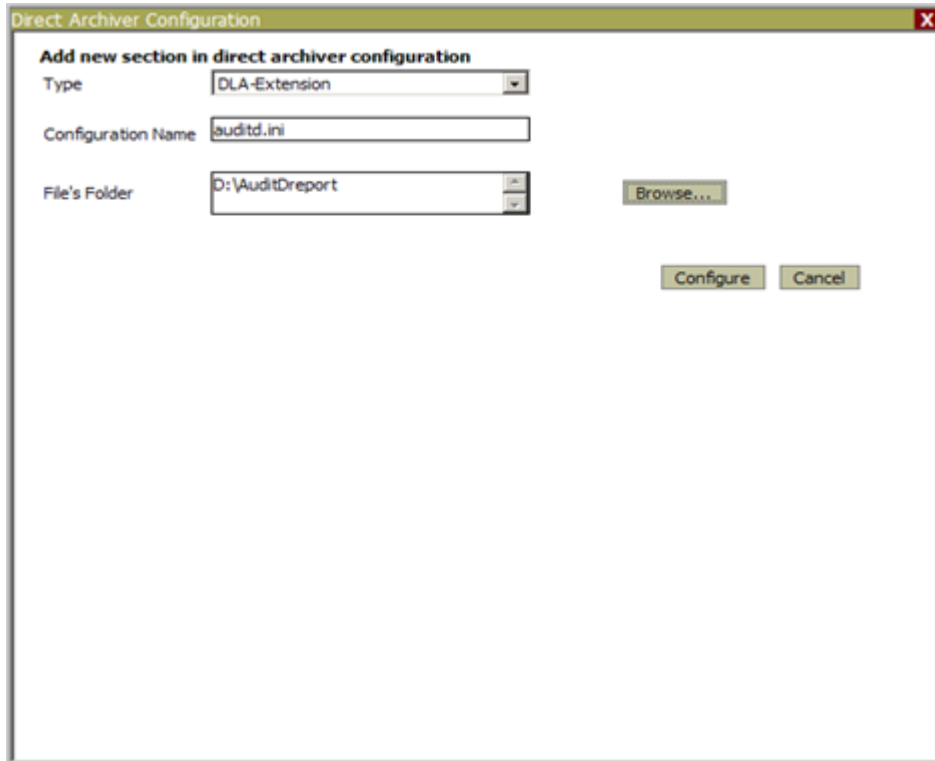


Figure 5

EventTracker displays the Direct Archiver Configuration pop-up window.

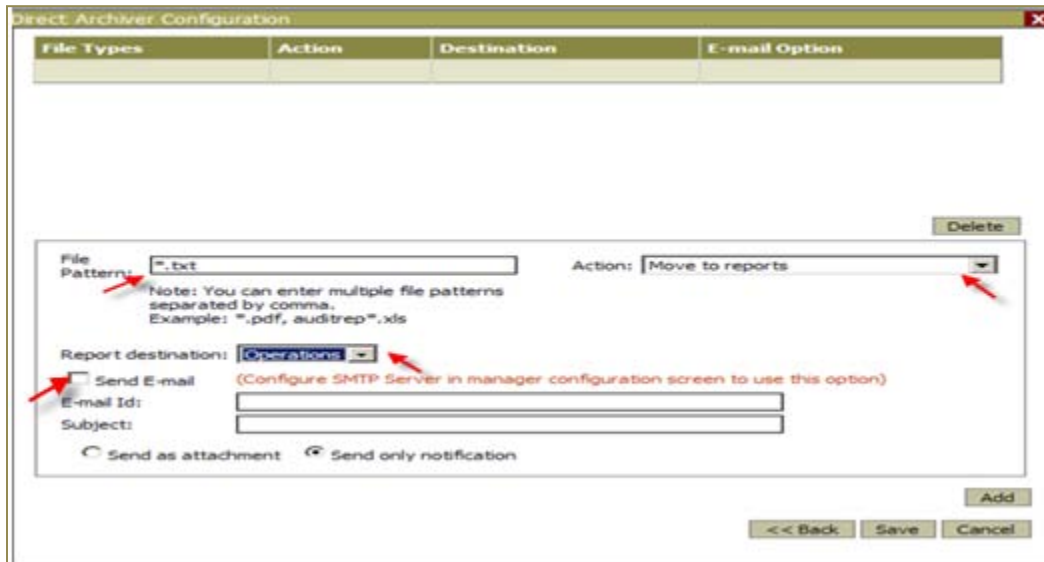


Figure 6

- Type **\*.txt** in File Pattern text box.
- Select **Move to Reports** from Action dropdown.(This can be customized accordingly)

- Select **Operation** from Report Destination dropdown.(This can be customized accordingly)
- Select **Send E-mail** to receive the report via e-mail.
- Type a valid sender e-mail address in the **E-mail Id** field, and a brief description in the **Subject** field.
- Select **Send as attachment** option to receive reports as email attached or select **Send only notification** options to receive email notification.
- Click the **Add** button, and then click the **Save** button.

EventTracker displays the **Manager Configuration** window.

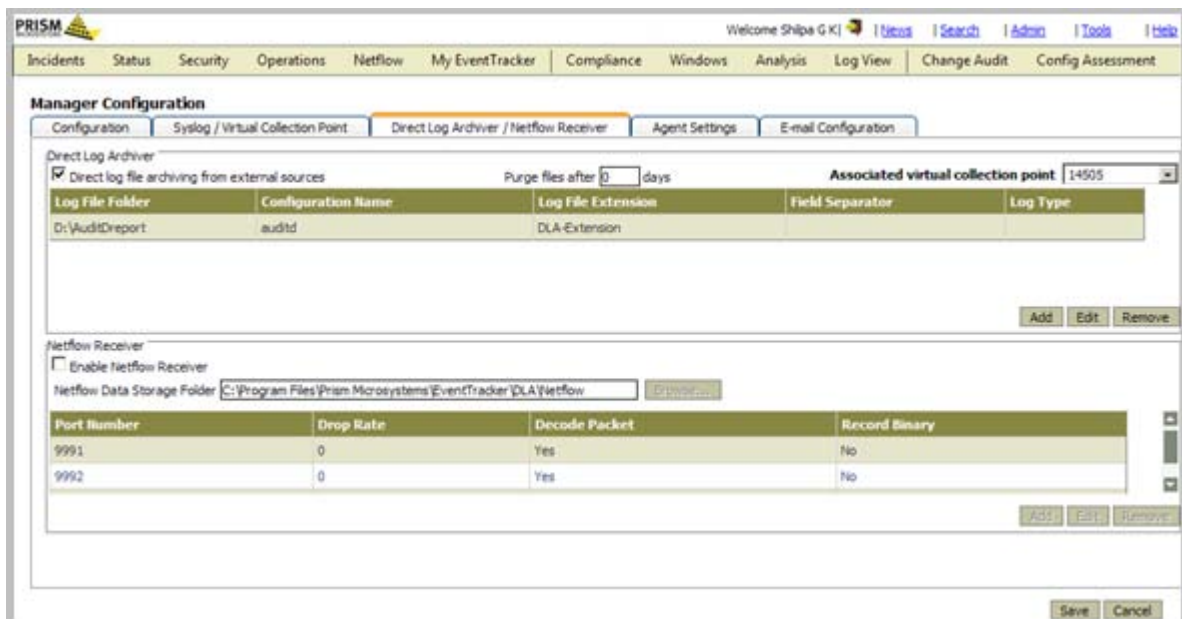


Figure 7

**NOTE:**

EventTracker displays Audit reports in 'Operation' dashboard in EventTrackerWeb.

- Click **Operations** tab, and then select **Reports**.

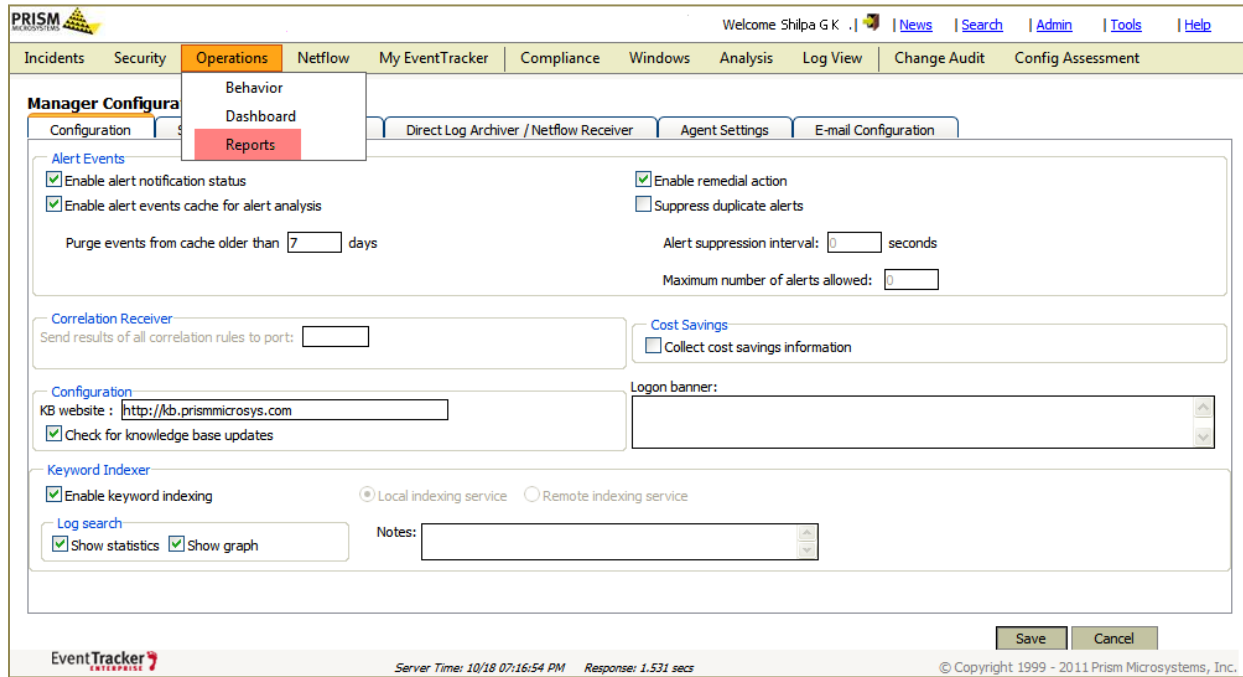


Figure 8

- Audit reports will be displayed in Reports page.

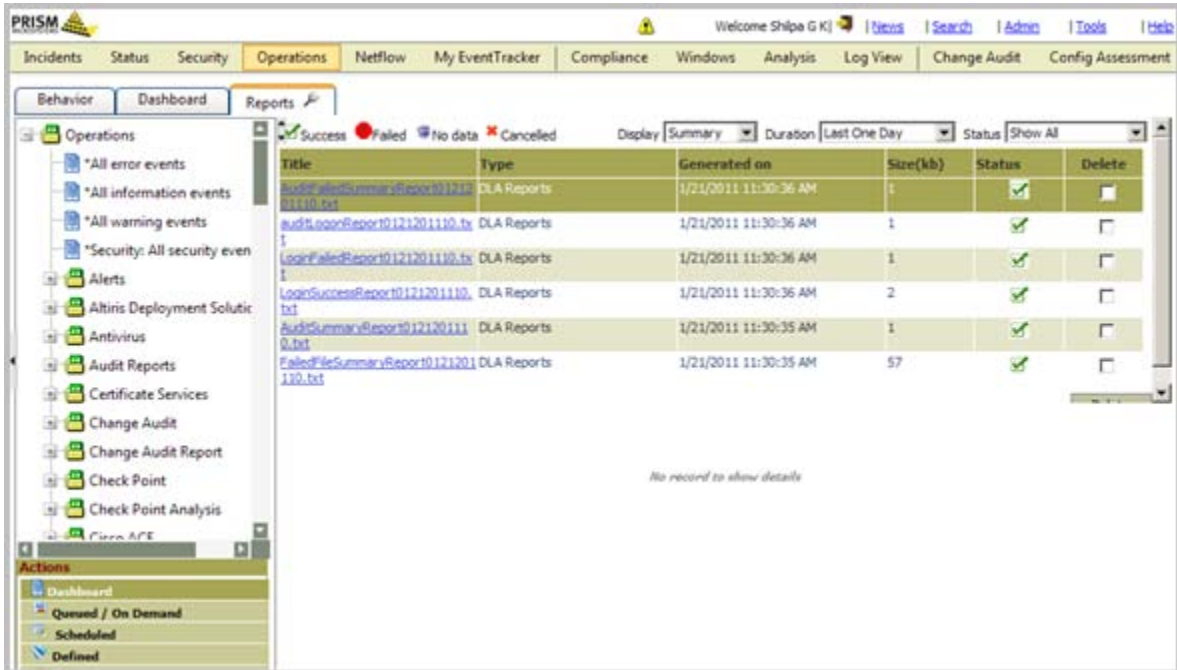


Figure 9: Operations >> Reports

- Click the report title to view the report.