

# Integrating LOGbinder SP

*EventTracker v7.x*

# Abstract

This guide provides instructions to configure Microsoft SharePoint to send the event logs to EventTracker Enterprise using LOGbinder SP.

## Scope

The configurations detailed in this guide are consistent with **EventTracker Enterprise v7.x** and later, SharePoint 2007/2010.

## Audience

Microsoft SharePoint users, who wish to forward audit events to EventTracker manager using LOGbinder SP.

*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.*

*© 2014 Prism Microsystems Corporation. All rights reserved.*

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

# Contents

Abstract.....	1
Scope .....	1
Audience.....	1
Overview.....	3
Critical components to be monitored include:.....	3
Install 'LOGbinder SP' on SharePoint Server .....	3
Monitoring SharePoint Audit Trail Integrity.....	4
LOGbinder SP Sharepoint Audit Trail Setting Changes.....	5
Monitoring any Access Control changes done by authorized user or administrator in SharePoint Site collection.....	6
LOGbinder SP SharePoint Access Control Changes .....	7
Monitoring any Information Management Policy Changes .....	8
Monitoring Item updates done in SharePoint Site Collection .....	8
LOGbinder SP SharePoint Item Updates.....	9
Monitoring Generic Object Changes done in SharePoint Site Collection .....	10
LOGBinder SP SharePoint Generic Object Changes .....	11
SharePoint Alerts/Categories/Reports in EventTracker.....	12
SharePoint Audit Log Alerts in EventTracker .....	12
SharePoint Audit Log Pre-defined Alerts in EventTracker .....	13
SharePoint Audit Log Pre-defined Categories in EventTracker .....	14
Following predefined categories are present in the EventTracker:.....	14
SharePoint Audit Log Reports in EventTracker .....	16

# Overview

LOGbinder SP translates cryptic SharePoint audit data into easy-to-understand messages and sends them to EventTracker. LOGbinder SP does not require an agent to be installed on your SharePoint servers, nor does it make intrusive changes to your SharePoint environment. It simply bridge the gap by bringing application security intelligence on SharePoint to your security operations center. LOGbinder SP is a small, efficient Windows service that runs on any Windows server that is a member of your SharePoint farm. This can be an existing SharePoint server or a dedicated server – even a VM. It just needs to be a member of the farm so that LOGbinder can interface with the SharePoint API.

EventTracker is an enterprise-class platform that seamlessly combines SIEM, Log Management, File Integrity Monitoring, machine Analytics and so forth. It is designed to address an ever-changing landscape of threats and challenges, with a full suite of high-performance tools for security, compliance, and operations. EventTracker delivers comprehensive, useful and actionable insight into what is really going on in and around an enterprise IT environment.

## Critical components to be monitored include:

- Monitoring 'SharePoint Audit Trail Integrity'.
- Monitoring any access control changes done by authorized user or administrator in 'SharePoint Site Collection'.
- Monitoring any 'Information Management Policy Changes'.
- Monitoring any item updates in 'SharePoint Site Collection'.
- Object Changes done in 'SharePoint Site Collection'.

## Install 'LOGbinder SP' on SharePoint Server

Visit <http://www.logbinder.com/support> and click on LOGbinder SP Getting Started Guide under Support Documentation -

- To install LOGbinder SP on SharePoint server
- To configure 'LOGbinder SP' to export SharePoint audit logs to windows 'Event Viewer'

## Monitoring SharePoint Audit Trail Integrity

It is very important to monitor SharePoint audit log integrity. Audit policy changes can result in important security events no longer being recorded in the audit log. Audit log deletion or tempering can be done to hide any user activity in SharePoint.

Following are the knowledge packs available in EventTracker, which can be used for alerting and reporting.

- **LOGbinder SP: Possible audit trail tampering** - This report includes events which could indicate tampering, which could affect the integrity of the audit.
- **LOGbinder SP: SharePoint Audit Logs Deleted** - This report includes information related to SharePoint audit log deletion. Audit logs created before this date have been removed from SharePoint.
- **LOGbinder SP: SharePoint Audit Policy Change** - This report includes changes in Site collection or SharePoint audit policy changes.

## LOGbinder SP Sharepoint Audit Trail Setting Changes

Summary Report(s) :

Sharepoint User	Total Event Occured	Event Id(Total Count)
deepak@prismcomm.com	2	11(2)
System Account	1	11(1)
Sharepoint Site	Total Event Occured	Event Id(Total Count)
http://leo:24956	3	11(3)
Operation Performed	Total Event Occured	Event Id(Total Count)
Site collection audit policy changed	3	11(3)

Detail Report :

Event Time	Sharepoint User	Sharepoint Site	Operation Performed	Updated configuration
4/16/2012 3:47	deepak@prismcomm.com	http://leo:24956	Site collection audit policy changed	New audit policy: View; Delete; Update; Profile Change; Schema Change; Security Change; Undelete; Copy; Move; Search
4/16/2012 3:47	deepak@prismcomm.com	http://leo:24956	Site collection audit policy changed	New audit policy: Check Out; Check In; View; Delete; Update; Profile Change; Schema Change; Security Change; Undelete; Copy; Move; Search
4/16/2012 3:48	System Account	http://leo:24956	Site collection audit policy changed	New audit policy: Check Out; Check In; View; Delete; Update; Profile Change; Child Delete; Schema Change; Security Change; Undelete; Workflow; Copy; Move; Search

Reports

Figure 1

# Monitoring any Access Control changes done by authorized user or administrator in SharePoint Site collection

It is very important to monitor any access control changes done in SharePoint Server which could result in a user being granted more or less authority to objects in SharePoint. This includes changes to site collection administrators, group changes and object permission changes.

Following are the knowledge packs available in EventTracker which can be used for reporting.

- **LOGbinder SP: SharePoint access control change** - This report includes changes to site collection administrators, group changes and object permission changes.

# LOGbinder SP SharePoint Access Control Changes

Summary Report(s) :

Sharepoint User	Total Event Occured	Event Id(Total Count)
deepak@prismcomm.com	17	31(8), 29(2), 38(2), 30(1), 28(1), 27(1), 25(1), 37(1)
System Account	2	27(2)
Sharepoint Site	Total Event Occured	Event Id(Total Count)
http://leo:24956	19	31(8), 27(3), 29(2), 38(2), 30(1), 28(1), 25(1), 37(1)
Operation Performed	Total Event Occured	Event Id(Total Count)
Permissions updated	8	31(8)
SharePoint group member added	3	27(3)
Unique permissions created	2	29(2)
SharePoint site collection administrator removed	2	38(2)
Unique permissions removed	1	30(1)
SharePoint site collection administrator added	1	37(1)
SharePoint group member removed	1	28(1)
SharePoint group created	1	25(1)

Detail Report :

Event Time	Sharepoint User	Sharepoint Site	Operation Performed	Updated configuration
4/16/2012 3:49	deepak@prismcomm.com	http://leo:24956	SharePoint site collection administrator removed	Administrator ID: 11 Name: anand
				Administrator ID: 8 Name: admin
4/16/2012 3:49	deepak@prismcomm.com	http://leo:24956	SharePoint site collection administrator removed	Administrator ID: 23 Name: deepak@prismmicrosys.com
				Group ID: n/a Name: n/a Member ID: 23 Name: prismmembershipprovider:deepak@prismmicrosys.com
4/16/2012 3:50	System Account	http://leo:24956	SharePoint group member added	Group ID: n/a Name: n/a Member ID: 25 Name: prismmembershipprovider:deepak@prismcomm.com
				Group ID: 32 Name: PrismMktg deepak@prismcomm.com
4/16/2012 3:54	deepak@prismcomm.com	http://leo:24956	SharePoint group created	

Figure 2



# Monitoring any Information Management Policy Changes

Information management policies enable you to control who can access your organizational information, what they can do with it, and how long to retain it. It is very important to keep track of any changes done in information management policy in SharePoint Server.

Following are the knowledge packs available in EventTracker, which can be used for reporting.

- **LOGbinder SP: SharePoint Information management policy changes** - This report includes changes to Information management policy changes

# Monitoring Item updates done in SharePoint Site Collection

It is very important to keep track of any changes made by users in SharePoint site collections items (Documents, lists and SharePoint container object updates).

Following are the knowledge packs available in EventTracker, which can be used for reporting.

- **LOGbinder SP: SharePoint container object Update** - This report includes SharePoint audit events concerning updates to site collections, webs, document libraries and folders
- **LOGbinder SP: SharePoint document update** - This report lists document level access events except for view events. It includes Document check in, Check out, Document updates and deletion events.
- **LOGbinder SP: SharePoint list update** - This report lists SharePoint audit events concerning updates to Lists, List Items and deletion.

# LOGbinder SP SharePoint Item Updates

Summary Report(s) :

Sharepoint User	Total Event Occured	Event Id(Total Count)
deepak@prismcomm.com	25	43(8), 45(5), 19(3), 44(3), 42(2), 46(2), 13(1), 14(1)
System Account	4	45(2), 44(1), 43(1)
Sharepoint Site	Total Event Occured	Event Id(Total Count)
http://leo.24956	29	43(9), 45(7), 44(4), 19(3), 42(2), 46(2), 13(1), 14(1)
Operation Performed	Total Event Occured	Event Id(Total Count)
Document updated	9	43(9)
List item updated	7	45(7)
List updated	4	44(4)
Object deleted	3	19(3)
Folder updated	2	46(2)
Document library updated	2	42(2)
Document checked out	1	14(1)
Document checked in	1	13(1)

Detail Report :

Event Time	Sharepoint User	Sharepoint Site	Operation Performed	Sharepoint Object
				Object URL: _catalogs/users/11_000 Title: n/a
4/16/2012 3:49	deepak@prismcomm.com	http://leo.24956	List item updated	For more information, see http://logbinder.com/support Object URL: _catalogs/users/8_000 Title: n/a
4/16/2012 3:49	deepak@prismcomm.com	http://leo.24956	List item updated	For more information, see http://logbinder.com/support Object URL: _catalogs/users/23_000 Title: n/a
4/16/2012 3:50	deepak@prismcomm.com	http://leo.24956	List item updated	For more information, see http://logbinder.com/support Object URL: _catalogs/users/32_000 Title: n/a
4/16/2012 3:54	deepak@prismcomm.com	http://leo.24956	List item updated	For more information, see http://logbinder.com/support Object Type: Generic List URL: /_catalogs/users/detail.aspx Title: User Information List Description: All people.
4/16/2012 3:54	deepak@prismcomm.com	http://leo.24956	List updated	For more information, see http://logbinder.com/support Object URL: _catalogs/users/32_000 Title: n/a Version: n/a
4/16/2012 3:54	deepak@prismcomm.com	http://leo.24956	Document updated	For more information, see http://logbinder.com/support Object URL: Mktgsite/Lists/Team Discussion Version: 1.0
4/16/2012 3:56	deepak@prismcomm.com	http://leo.24956	Folder updated	For more information, see http://logbinder.com/support Object URL: Mktgsite/Lists/Calendar Version: 1.0
4/16/2012 3:56	deepak@prismcomm.com	http://leo.24956	Folder updated	For more information, see http://logbinder.com/support Object Type: n/a

Figure 3

# Monitoring Generic Object Changes done in SharePoint Site Collection

Following are the knowledge packs available in EventTracker, which can be used for reporting.

- **LOGbinder SP: SharePoint object changes** - This report lists SharePoint audit events for certain change operations dealing with various object types. It includes Child object deleted, Child object moved, Object copied, Object deleted, Object moved, Object profile changed, SharePoint object structure changed, Object restored, List item updated and Workflow accessed.

# LOGBinder SP SharePoint Generic Object Changes

Summary Report(s) :

Sharepoint User	Total Event Occured	Count)
deepak@prismcomm.com	7	15(3), 19(3), 39(1)
Sharepoint Site	Total Event Occured	Count)
http://Meo:24956	7	15(3), 19(3), 39(1)
Operation Performed	Total Event Occured	Count)
Object deleted	3	19(3)
Child object deleted	3	15(3)
Object restored	1	39(1)

Detail Report :

Event Time	Sharepoint User	Sharepoint Site	Operation Performed	Sharepoint Object
4/16/2012 4:17	deepak@prismcomm.com	http://Meo:24956	Child object deleted	Parent Object Type: List Subtype: Document Library URL: /Deepak Doc/Forms/AllItems.aspx Title: Deepak Doc Child Object Type: Document URL: Deepak Doc/PrismMembersPub.zip
				Object Type: Document URL: Deepak Doc/PrismMembersPub.zip Versions deleted: All versions deleted Recycled: Item in end-user Recycle Bin
4/16/2012 4:17	deepak@prismcomm.com	http://Meo:24956	Object deleted	Parent Object Type: List Subtype: Generic List URL: /Lists/Test1list/AllItems.aspx Title: Test1list Child Object Type: List Item URL: Lists/Test1list/1_000
				Object Type: List Item URL: Lists/Test1list/1_000 Versions deleted: n/a Recycled: n/a
4/16/2012 4:25	deepak@prismcomm.com	http://Meo:24956	Child object deleted	Parent Object Type: Web Subtype: n/a URL: http://Meo:24956 Title: SugarInfo Child Object Type: List URL: Lists/Test1list
				Object Type: List URL: Lists/Test1list Versions deleted: All versions deleted Recycled: Item in end-user Recycle Bin
4/16/2012 4:26	deepak@prismcomm.com	http://Meo:24956	Object deleted	

Figure 4

# SharePoint Alerts/Categories/Reports in EventTracker

## SharePoint Audit Log Alerts in EventTracker

In Incidents dashboard, EventTracker displays the SharePoint incidents that are generated for past 24 hours in the managed systems. **Latest Incidents** pane will list the latest 20 incidents.

If the LOGbinder alerts are activated in the Alerts management page, then those alerts can be seen in the Incident dashboard.

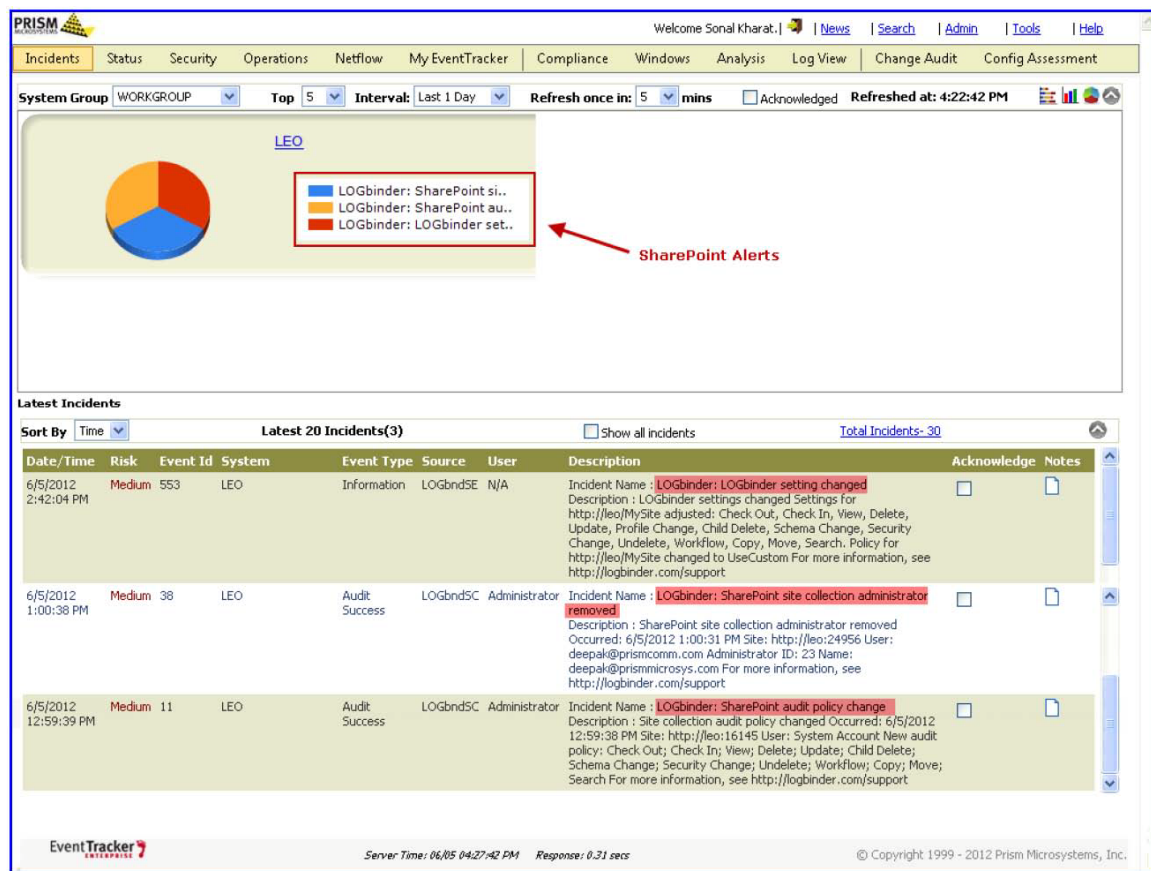


Figure 5

- To view the total incidents occurred on a particular system, click the system name on the 'Incidents dashboard' top pane.
- Click any sector of pie chart/ bar of bar graph on the 'Incidents dashboard' top pane to view details of that particular Incident(s).

EventTracker will display the **Search Incidents** window that shows the detailed search results for the selected incident.

## SharePoint Audit Log Pre-defined Alerts in EventTracker

Following SharePoint alerts are present in the EventTracker **Alert Management** page:

- LOGbinder: LOGbinder setting changed
- LOGbinder: Possible audit trail tampering
- LOGbinder: SharePoint audit logs deleted
- LOGbinder: SharePoint audit policy change
- LOGbinder: SharePoint site collection administrator added
- LOGbinder: SharePoint site collection administrator removed

The screenshot shows the EventTracker Alert Management page. At the top, there is a navigation bar with links: Incidents, Status, Security, Operations, Netflow, My EventTracker, Compliance, Windows, Analysis, Log View, Change Audit, and Config Assessment. Below this is a search bar with a 'Go' button and a 'Show All' button. The main table lists several alerts with columns for Alert Name, Threat level, Active, Beep, E-mail, Message, RSS, Forward as SNMP, Forward as SYSLOG, Remedial Action at Console, and Remedial Action at Agent. The alerts are: LOGbinder: LOGbinder setting changed (High), LOGbinder: Possible audit trail tampering (Critical), LOGbinder: SharePoint audit logs deleted (High), LOGbinder: SharePoint audit policy change (High), LOGbinder: SharePoint site collection administrator added (High), and LOGbinder: SharePoint site collection administrator removed (High). At the bottom of the table, there is a message: '\*\*\*Click 'Activate Now' after making all changes' and buttons for 'Activate Now', 'Add alert', and 'Delete'.

Alert Name▲	Threat level	Active	Beep	E-mail	Message	RSS	Forward as SNMP	Forward as SYSLOG	Remedial Action at Console	Remedial Action at Agent
LOGbinder: LOGbinder setting changed	High	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LOGbinder: Possible audit trail tampering	Critical	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LOGbinder: SharePoint audit logs deleted	High	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LOGbinder: SharePoint audit policy change	High	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LOGbinder: SharePoint site collection administrator added	High	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LOGbinder: SharePoint site collection administrator removed	High	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

\*\*\*Click 'Activate Now' after making all changes

Activate Now Add alert Delete

EventTracker 7  
Server Time: 06/05 04:46:18 PM Response: 0.46 secs  
© Copyright 1999 - 2012 Prism Microsystems, Inc.

Figure 8

Custom alert(s) can also be added using **Add Alert** button.

## SharePoint Audit Log Pre-defined Categories in EventTracker

In EventTracker, LOGbinder categories are grouped under **LOGbinder SP** group.

In **Category Management** page, the last 10 modified categories can be viewed in the right pane.

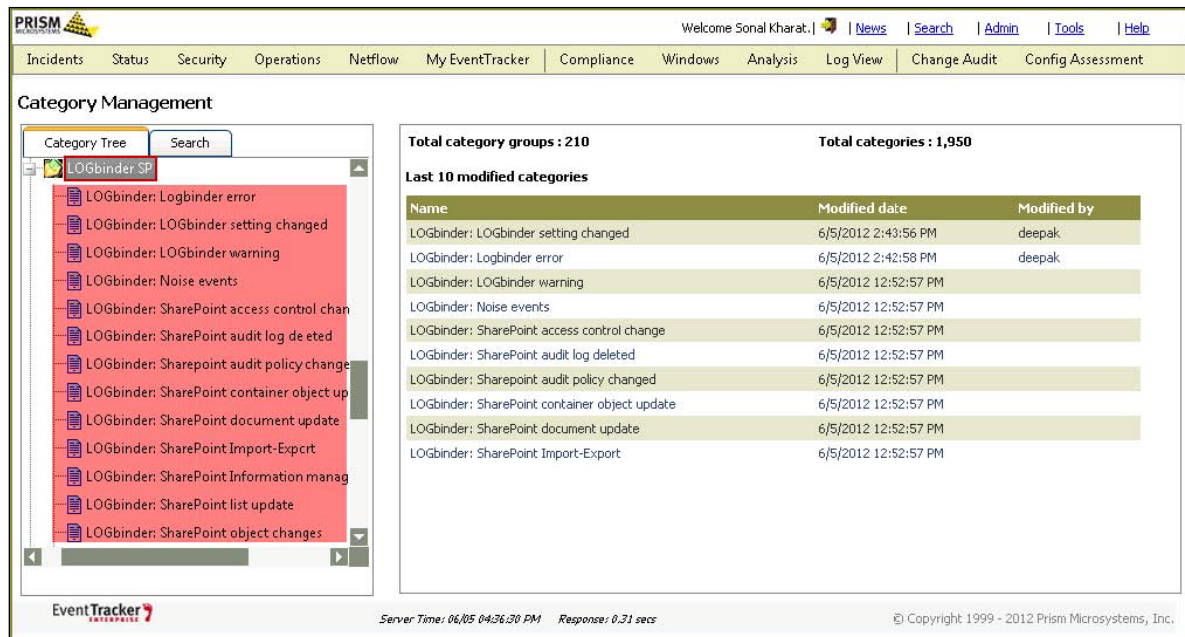


Figure 9

Following predefined categories are present in the EventTracker:

- LOGbinder: LOGbinder error
- LOGbinder: LOGbinder setting changed
- LOGbinder: LOGbinder warning
- LOGbinder: Noise events
- LOGbinder: SharePoint access control change
- LOGbinder: SharePoint audit log deleted
- LOGbinder: SharePoint audit policy changed
- LOGbinder: SharePoint container object update
- LOGbinder: SharePoint document update

- LOGbinder: SharePoint Import-Export
- LOGbinder: SharePoint Information management policy changes
- LOGbinder: SharePoint list update
- LOGbinder: SharePoint object changes
- LOGbinder: SharePoint search events
- LOGbinder: Site collection administrator added
- LOGbinder: Site collection administrator



## SharePoint Audit Log Reports in EventTracker

In EventTracker, SharePoint analysis reports can be scheduled for a specific time, executed immediately, or can be queued up for report generation.

PRISM  
MICROSYSTEMS

Welcome Sonal Kharat. | [News](#) | [Search](#) | [Admin](#) | [Tools](#) | [Help](#)

Incidents Status Security Operations Netflow My EventTracker Compliance Windows Analysis Log View Change Audit Config Assessment

Analysis

- Logs
  - Summary
  - Detail
  - Trend
- Alerts
  - Summary
  - Detail
- Cost Savings
  - Summary
  - Person Hour
- Suspicious Traffic
- Log Volume

Actions

- Dashboard
- On Demand
- Queued
- Scheduled
- Defined
- Exceptions

Defined analysis

Search

Title	Created on ▼	Delete
LOGbinder SP SharePoint Generic Object Changes	3/1/2011 1:35:26 PM	<input type="checkbox"/>
LOGbinder SP Sharepoint Information Management Policy Changes	3/1/2011 1:33:33 PM	<input type="checkbox"/>
LOGbinder SP SharePoint View Events report	3/1/2011 11:52:19 AM	<input type="checkbox"/>
LOGbinder SP SharePoint Item updates	3/1/2011 11:47:44 AM	<input type="checkbox"/>
LOGbinder SP SharePoint Access Control changes	3/1/2011 11:45:22 AM	<input type="checkbox"/>
LOGbinder SP Sharepoint Audit Trail Setting Changes	3/1/2011 11:41:39 AM	<input type="checkbox"/>

EventTracker  
ENTERPRISE

Server Time: 16/05 04:58:32 PM Response: 0.31 secs

© Copyright: 1999 - 2012 Prism Microsystems, Inc.

Figure 10