# EventTracker

Actionable Security Intelligence

# Monitoring SharePoint 2007/ 2010/ 2013 Server using EventTracker

Publication Date: June 12, 2012

### Abstract

EventTracker allows you to effectively manage your systems and provides operational efficiencies – reducing IT costs and freeing resources for other duties that increase the business value of your organization. EventTracker's built-in knowledge pack enables you to gather business intelligence providing increased security, performance, availability, and reliability of your systems.

With EventTracker, you can monitor all of your servers running SharePoint from a single view. EventTracker checks the status and availability of SharePoint Servers, critical server processes, and it centrally consolidates all the event logs. Through consolidated logging you can monitor the performance, availability, and security of your servers running SharePoint, alerting you to events that have a direct impact on server availability while filtering out events that require no action. Through alerts, knowledge base solutions, and reports, EventTracker helps you correct problems long before a catastrophic failure occurs. EventTracker also includes reports that allow you to summarize server availability

### Scope

The configurations detailed in this guide are consistent with **EventTracker** version 7.X and later, SharePoint 2007/2010/2013.

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.

© 2017 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
Monitoring SharePoint Server	3
Event Log Consolidation	4
Turn on Appropriate Diagnostics Logging on SharePoint Server	4
Install EventTracker agent on SharePoint Servers	6
Enable IIS Logging on SharePoint Web Application Server	6
Enabling Log File Monitoring in EventTracker Agent	
Install 'LOGbinder SP' on SharePoint Server	10
Monitoring uptime status of SharePoint Server	11
Monitoring Disk and Memory Problem on SharePoint Server	13
Monitoring Microsoft Office SharePoint Server services	13
Monitoring Microsoft Office SharePoint Server	15
Monitoring SharePoint Audit Trail Integrity**	16
Monitoring any Access Control changes done by authorized user or administrator in S collection**	
Monitoring any Information Management Policy Changes**	19
Monitoring Item updates done in SharePoint Site Collection**	19
Monitoring Generic Object Changes done in SharePoint Site Collection**	21
SharePoint Alerts/Categories/Reports in EventTracker SharePoint Audit Log Alerts in EventTracker	
SharePoint Audit Log Pre-defined Alerts in EventTracker	24
SharePoint Audit Log Pre-defined Categories in EventTracker	25
SharePoint Audit Log Reports in EventTracker	26



# **Monitoring SharePoint Server**

EventTracker allows you to effectively manage your systems and provides operational efficiencies – reducing IT costs and freeing resources for other duties that increase the business value of your organization. EventTracker's built-in knowledge base enables you to gather business intelligence providing increased security, performance, availability, and reliability of your systems.

With EventTracker you can monitor all of your servers running Microsoft Office SharePoint Server from a single view. EventTracker checks the status and availability of SharePoint Server's critical processes and it centrally consolidates all the event logs, Web Server, and Database Server logs. Through consolidated logging you can monitor the performance, availability, and security of your servers running SharePoint, alerting you to events that have a direct impact on server availability while filtering out events that require no action. Through alerts, knowledge base solutions, and reports, EventTracker helps you correct problems long before a catastrophic failure occurs. EventTracker also includes reports that allow you to summarize server availability.

#### Critical components to be monitored include:

- Monitoring uptime status of 'SharePoint Servers'.
- Monitoring disk and memory problem on 'SharePoint Server'.
- Monitoring 'SharePoint Server' and its dependency component service and related services (Single Sign On, Load Balancer, Launcher and Search, IIS, SQL Server).
- Monitoring 'Microsoft Office SharePoint Server' and related events.
- 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'\*\*.

\*\* Requires **LOGbinder SP** installed and configured to monitor SharePoint sites.



# **Event Log Consolidation**

Based on audit settings, Microsoft logs the necessary audit, availability, and performance events. EventTracker collects all events to a centralized server. Either you can collect all the events or you can filter any events you don't care about. EventTracker Knowledgebase (<u>http://kb.eventtracker.com/</u>) helps you to search for events that can be chosen or filtered from the available repository. All these events are received in real-time and you can configure any event to generate an alert. You can write intensive pattern matching rules using industry standard regular expressions that parse the information within the complex event description or you can create an alert when a sequence of events occurs within a predefined time frame. Once EventTracker consolidates the event logs, you can generate hundreds of reports on various conditions.

#### To monitor SharePoint Server following things need to be checked:

- Turn on appropriate diagnostics logging on SharePoint Server.
- Install EventTracker agent on SharePoint Servers.
- Enable IIS logging on SharePoint Web Application Server.
- Enabling 'Log File Monitoring' in EventTracker agent.
- Install LOGbinder SP on SharePoint Server.
- Configure 'LOGbinder SP' to export SharePoint audit logs to windows 'Event Viewer'.

### Turn on Appropriate Diagnostics Logging on SharePoint Server

To enable diagnostic logging in SharePoint Server you need to be a member of **Farm Administrator's Group**.

Follow the steps given below to add a user in **Farm** administrators group:

- 1. Login to SharePoint Server Central Administration website.
- 2. Click on Monitoring.
- 3. Click Diagnostics logging.
- 4. Check the All categories option,
- 5. Select **Warning** as the **Least critical event to report to report to the eventlog** from the dropdown.
- 6. Click **OK**.



# Monitoring SharePoint 2007/2010/2013 Server

Site Actions 🔸 😏			System Account +		
SharePoint 2010	Central Administratio	n → Diagnostic Logging	I Like It Tags & Notes		
			0		
Home Application Management System Settings Monitoring Backup and Restore Security Upgrade and Migration General Application Settings Configuration Wizards	Event Throttling Use these settings to control the sevenity of events captured in the Windows event log and the trace logs. As the sevenity decreases, the number of events logged will increase. You can change the settings for any single category, or for all categories. Updating all categories will lose the changes to individual categories.	Select a category       Event Levent Le	vel Trace Leve		

Figure 1



### Install EventTracker agent on SharePoint Servers

Installation procedure is identical for Windows XP/Vista/7/2008/2003/2012 systems. To install EventTracker Agent, please refer <u>Agent Deployment Manual</u>.

# Enable IIS Logging on SharePoint Web Application Server

IIS logging should be configured properly for **Exchange web access** and **Exchange ActiveSync** usage monitoring.

Configure IIS logging using the steps below:

- 1. Click Start > All Programs > Administrative Tools > Internet Information Services (IIS) Manager.
- 2. In the Connections pane, navigate to Default website, and then click Logging.

Def	ault Web	Site Hom	e				
Filter:		• 00 <u>Go</u> • 5	Show All   Gr	oup by: Area	í .	-	
ASP.NET							
.NET Authorizati	.NET Compilation	.NET Error Pages	.NET Globalization	.NET Profile	.NET Roles	.NET Trust Levels	
.NET Users	Application Settings	Connection Strings	Machine Key	Pages and Controls	Providers	Session State	
SMTP E-mail							
<u></u>	J	0		404			
uthentication	Compression	Default Document	Directory Browsing	Error Pages	Failed Request Tracing Rules	Handler Mappings	
		3					
ITTP Redirect	HTTP Respo	ISAPI Filters	Logging	MIME Types	Modules	Output Caching	
0	9						
Request Filtering	SSL Settings						

Figure 2

- 3. Select log file format as **W3C** from **Format** dropdown.
- Click the Select Fields button.
   W3C Logging Fields dialog box appears on the screen.



5. Check all the field options, and then click **OK**.

3C Logging Fields		? ×
🖌 Date ( date )		
🔽 Time ( time )		
🔽 Client IP Adcress ( c-ip )		
🔽 User Name ( cs-username )		
🖌 Service Name ( s-sitename )		
🖌 Server Name ( s-computername )		
🖌 Server IP Address ( s-ip )		
🖌 Server Port ( s-port )		
🖌 Method ( cs-method )		
🖌 URI Stem ( cs-uri-stem )		
🖌 URI Query ( cs-uri-query )		
🖌 Protocol Status ( sc-status )		
🖌 Protocol Substatus ( sc-substatus	;)	
🖌 Win32 Status ( sc-win32-status )		
Bytes Sent (sc-bytes)		
🖌 Bytes Received ( cs-bytes )		
🖌 Time Taken ( time-taken )		
Protocol Version ( cs-version )		
Host ( cs-host )		
User Agent ( cs(User-Agent) )		
🖌 Cookie ( cs(Cookie) )		
🖌 Referer ( cs(Referer) )		

Figure 3

6. In the Actions pane, click the Apply button



S S PRISMTESTI-VMI + Sites + Default Web Site +	- 18 1 10
Ele Yew Help	Actions         Image: Apply         Image: Cancel         Disable         View Log Files         Image: Provide the state of t

Figure 4

# Enabling Log File Monitoring in EventTracker Agent

Logfile monitoring should be enabled for EventTracker agent to start retrieving the events from IIS log.

Follow the steps given below to enable Logfile Monitoring:

- 1. Open EventTracker Control Panel.
- 2. Double click EventTracker Agent Configuration.
- 3. In EventTracker Agent Configuration dialog box, click the Logfile Monitor tab.



### Monitoring SharePoint 2007/2010/2013 Server

🚰 Event Tracker Agent Configuration	×
Eile Help	
- Select Systems	
WIN2K3X64	
Apply the following settings to specified Agents	
Manager destinations:	
WIN2K3X64, 192.168.1.8	_
Services   Log Backup   Processes   Network Connections	1
Managers Event Filters System Monitor Monitor Apps	
Logfile Monitor File Transfer Config Assessment	
Contraction Contraction Contraction Contraction Contraction	
Search log files (various formats supported) for matching patterns specified	
here. Both individual files as well as folders can be monitored for matching entries. Matches cause an event to be generated.	
Logfile Name File Type	
Add File Name View File Details Delete File Name Search Strings	
<u>Save</u> <u>C</u> lose	

Figure 5: Logfile Monitor

- 4. Check the Logfile Monitor option.
- 5. Click the Add File Name button to add SMTP log that you wish to monitor.
- 6. In Enter File name dialog box, select the IISW3C as the 'Log File Type' from the dropdown.
- 7. Browse or type the path to the SMTP logs, and then click **OK**.



Enter File name		×
along with the strings the	omplete path of the log file or folder that needs to be monitored at need to be searched.	
Get All Existing Lo	j Files	
Select Log File Type	IISW3C 💌	1
This is the IIS W3C Ex Enter File name	······································	and a second sec
c:\inetpub\logs\LogFi	es\W3SVC1\*.log	
	OK Cancel	l

Figure 6: Enter file name

# Install 'LOGbinder SP' on SharePoint Server

Visit <a href="http://www.logbinder.com/support/LOGbinderSPGettingStartedv3.pdf">http://www.logbinder.com/support/LOGbinderSPGettingStartedv3.pdf</a>:

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



# Monitoring uptime status of SharePoint Server

SharePoint Server 'Uptime' status can be monitored using StatusTracker component available in EventTracker. Following are the components which should be configured in status tracker to monitor the sever status.

- System availability Status tracker alerts when SharePoint Server is not reachable or down.
- **Ports monitoring** Status Tracker alerts when SharePoint Server ports are not available or down. Following are the ports which should be always up and running.

Protocol	Port	Usage	Comment
ТСР	80	http	Client to SharePoint web server traffic (SharePoint – Office Web Apps communication)
ТСР	443	https/ssl	Encrypted client to SharePoint web server traffic (Encrypted SharePoint – Office Web Apps communication)
ТСР	1433	SQL Server default communication port.	May be configured to use custom port for increased security
UDP	1434	SQL Server default port used to establish connection	May be configured to use custom port for increased security
ТСР	445	SQL Server using named pipes	When SQL Server is configured to listen for incoming client connections by using named pipes over a NetBIOS session, SQL Server communicates over TCP port 445
ТСР	25	SMTP for e-mail integration	Cannot be configured
ТСР	16500-16519	Ports used by the search index component	Intra-farm only Inbound rule Added to Windows firewall by SharePoint
ТСР	22233-22236	Ports required for the AppFabric Caching Service	Distributed Cache
ТСР	808	Windows Communication Foundation communication	WCF
ТСР	32843	Communication between Web servers and service applications	http (default) To use custom port, see references section
ТСР	32844	Communication between Web servers and service applications	https



Protocol	Port	Usage	Comment
ТСР	32845	net.tcp binding: TCP 32845 (only if a third party has implemented this option for a service application)	Custom Service Applications
ТСР	5725	User Profile Synchronization Service(FIM)	Synchronizing profiles between SharePoint 2013 and Active Directory Domain Services (AD DS) on the server that runs the Forefront Identity Management agent
TCP + UDP	389	User Profile Synchronization Service(FIM)	LDAP Service
TCP + UDP	88	User Profile Synchronization Service(FIM)	Kerberos
TCP + UDP	53	User Profile Synchronization Service(FIM)	DNS
UDP	464	User Profile Service(FIM)	Kerberos change password
ТСР	809	Office Web Apps	Intra-farm Office Web Apps communication.

Following are the Knowledge packs available, which can be used for monitoring Exchange server and generating reports on that.

• EventTracker: StatusTracker resource down – This predefined alert and category enables you to be alerted and generating reports for resource downtime status when SharePoint Server system or SharePoint services ports are down.



# Monitoring Disk and Memory Problem on SharePoint Server

EventTracker agent can be configured to monitor disk space, CPU usage, and memory usage threshold. Once Disk space, Memory usage or CPU usage on SharePoint Server exceeds the threshold limit then it generates warning events.

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

- **EventTracker: Disk space low**: This event logged by EventTracker when the disk space is below the defined threshold.
- **EventTracker: Runaway processes:** This Event logged by EventTracker when system resource usage by processes cross the configured threshold.
- System: Disk bad block: All events related to bad sectors found on Hard Disc.

# Monitoring Microsoft Office SharePoint Server services

You can monitor the availability of services used by SharePoint Server and its dependency component. If any of these services are not available – SharePoint Server does not behave properly. EventTracker agent continuously checks the status of Windows services.

SharePoint Server Services 2013		
SharePoint Server Search 15	Performs host deployment and management for SharePoint 2013 search	
SharePoint Search Host Controller	Administers and crawls content from repositories	
SharePoint Timer Service V4	Sends notifications and performs scheduled tasks for SharePoint 2013	
SharePoint Tracing Service V4	Manages trace output	
SharePoint User Code Host V4	Executes user code in a sandbox	
Document Conversions Launcher	Schedules and initiates document conversions	
Document Conversions Load Balancer	Balances the document conversion requests from across the server farm	



SharePoint Server Services 2010			
SharePoint 2010 Administration	Performs administrative tasks for SharePoint		
SharePoint 2010 Timer	SharePoint 2010 Timer		
SharePoint 2010 Tracing	Manages trace output		
SharePoint 2010 User Code Host	SharePoint 2010 User Code Host		
SharePoint 2010 VSS Writer	SharePoint 2010 VSS Writer		
SharePoint Foundation Search V4	Provides full-text indexing and search to SharePoint user and help content.		
SharePoint Server Search 14	SharePoint Server Search 14		
Document Conversions Launcher for Microsoft SharePoint Server 2010	Manages the Microsoft Exchange Information Store. This includes mailbox databases and public folder databases. If this service is stopped, mailbox databases and public folder databases on this computer are unavailable. If this service is disabled, any service that explicitly depends on it will fail to start.		
Document Conversions Load Balancer for Microsoft SharePoint Server 2010	Load Balancer for Microsoft Office Server Document Conversions Services		

SharePoint Server Services 2007			
Windows SharePoint Services Administration	Performs administrative tasks for Windows SharePoint Services		
Windows SharePoint Services Search	Provides full-text indexing and search to SharePoint user and help content.		
Windows SharePoint Services Timer	Sends notifications and performs scheduled tasks for Windows SharePoint Services.		
Windows SharePoint Services Tracing	Manages trace output		
Windows SharePoint Services VSS Writer	Windows SharePoint Services VSS Writer		



IIS Services				
World Wide Web Publishing Service	Provides Web connectivity and administration through the Internet Information Services Manager			
IIS Admin Service	Enables this server to administer the IIS metabase. The IIS metabase stores configuration for the SMTP and FTP services. If this service is stopped, the server will be unable to configure SMTP or FTP. If this service is disabled, any services that explicitly depend on it will fail to start.			

SQL Se	ervices
MSSQLSERVER	Provides storage, processing and controlled access of data, and rapid transaction processing

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

- **Service Downtime:** This report will provide you the resource downtime status when SharePoint Server system or SharePoint services ports are down
- **Critical service not running:** If any of the SharePoint services are stopped then this alert will notify you the status.

# Monitoring Microsoft Office SharePoint Server

You can see events generated by SharePoint Server in EventTracker once EventTracker agent is deployed to SharePoint Servers.

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

- All SharePoint Server events: All diagnostics events logged by SharePointServer.
- SharePoint database activity: All events logged by SharePoint Server related to database activity.
- SharePoint office activity: All events logged by SharePoint Server related to SharePoint search services.
- **SharePoint Policy:** All SharePoint policy events.
- SharePoint Services: All SharePoint services related events.



# 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 :**

Summany Banart(c)

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 audt 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 audt policy: Check Out; Check In; View; Delete; Update; Frofile Change; Schema Change; Security Change; Undelete; Copy; Move; Search
				New audt policy: Check Out; Check In; View; Delete; Update; Frofile Change; Child Delete; Schema Change; Security Change; Undelete; Workflow; Copy; Move;
4/16/2012 3:48	System Account	http://leo:24956	Site collection audit policy changed	Search

Reports

EventTracker

# 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	<b>1</b>	30(1)
SharePoint site collection administrator added	1	37(1)
SharePoint group member removed	i1	28(1)
SharePoint group created	1	25(1)

#### **Detail Report :**

Event Time	Sharepoint User	Sharepoint Site	Operation Performed	Updated configuration
		COLUMN STATES		Administrator
				ID: 11
1/16/2012 3:49	deepak@prismcomm.com	http://leo:24956	SharePoint site collection administrator removed	Name: anand
	_			Administrator
				ID: 8
/16/2012 3:49	deepak@prismcomm.com	http://leo:24956	SharePoint site collection administrator removed	Name: admin
				Administrator
				ID: 23
				Name: deepak@prismmicrosys.com
/16/2012 3:50	deepak@prismcomm.com	http://leo:24956	SharePoint site collection administrator adde	ed
				Group
				ID: n/a
				Name: n/a
				Member
				ID: 23 Name: prismmembershipprovider:deepak@pris mmicrosys.com
/16/2012 3.50	System Account	http:///eu.24956	SharePoint group member added	
				Group
				ID: n/a
				Name: n/a
				Member
				ID: 25 Name: prismmembershipprovider:deepak@pris mcomm.com
4/16/2012 3:54	System Account	http://leo:24956	SharePoint group member added	
				Group
				ID: 32
				Name: PrismMktg
				deepak@prismcomm.com
/16/2012 3:54	deepak@prismcomm.com	http://leo:24956	SharePoint group created	



# 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 :

Sharepoint User	Sharepoint Site	Operation Performed	Sharepoint Object
			Object
			URL: _catalogs/users/11000
			Title: n/a
deepak@prismcomm.com	http://leo:24956	List item updated	For more information, see http://logbinder.com/support
			Object
			URL: _catalogs/users/8000
			Title: n/a
deensk@price.com	http://decr.24956	List item undeted	For more information, see http://logbinder.com/support
deepungepromeonini.com	140.00024000	Eist itom apaatoa	Object
			URL: _catalogs/users/23000
			Title: n/a
			nue. Iva
deepak@prismcomm.com	http://leo:24956	List item updated	For more information, see http://logbinder.com/support
			Object
			URL: _catalogs/users/32000
			Title: n/a
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.
	LH. M	(the second second	For more information, see http://logbinder.com/support
deepak@prismconm.com	пцр. мео. 24956	List updated	Object
			URL: _catalogs/users/32000
			Title: n/a
			Version: n/a
			Y CI SION, H/A
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
deepak@prismcomm.com	http://leo:24956	Folder updated	For more information, see http://logbinder.com/support
			Object
			URL: Mktgsite/Lists/Calendar
			Version: 1.0
	http://leo:24956	Folder updated	For more information, see http://logbinder.com/support
deepak@prismcomm.com			
	deepak@prismcomm.com deepak@prismcomm.com deepak@prismcomm.com deepak@prismcomm.com deepak@prismcomm.com	deepak@prismcomm.com http://leoi24956 deepak@prismcomm.com http://leoi24956 deepak@prismcomm.com http://leoi24956 deepak@prismcomm.com http://leoi24956 deepak@prismcomm.com http://leoi24956	deepak@prismcomm.com       http://leo:24956       List item updated         deepak@prismcomm.com       http://leo:24956       List updated         deepak@prismcomm.com       http://leo:24956       List updated

Type: n/a

# EventTracker 🕃

Actionable Security Intelligence

# 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://leo: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
				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
/16/2012 4:17	deepak@prismcomm.com	http://leo:24956	Child object deleted	
				Object
				Type: Document
				URL: Deepak Doc/PrismMembersPub.zip
				Versions deleted: All versions deleted
				Recycled: Item in end-user Recycle Bin
1/16/2012 4:17	deepak@prismcomm.com	http://leo: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/1000
1/16/2012 4:25	deepak@prismcomm.com	http://leo:24956	Child object deleted	
				Object
				Type: List Item
				URL: Lists/Test1list/1000
				Versions deleted: n/a
				Recycled: n/a
/16/2012 4:25	deepak@prismcomm.com	http://leo:24956	Object deleted	
				Parent Object
				Type: Web
				Subtype: n/a
				URL: http://leo:24956
				Title: SugarInfo
				Child Object
				Type: List
				URL: Lists/Test1list
/16/2012 4:26	deepak@prismcomm.com	http://leo:24956	Child object deleted	
				Object
				Type: List
				URL: Lists/Test1list
				Versions deleted: All versions deleted
				Versions deleted: All versions deleted Recycled: Item in end-user Recycle Bin

# EventTracker:

Actionable Security Intelligence

# 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.

RISM						Welco	me Sonal Kharat.	I News	Search	Admin   ]	iools   H	elp
Incidents	Status	Security	Operations	Netflow	My EventTracker	Compliance Window:	: Analysis	Log View	Change Aud	dit Confi	g Assessmer	nt
ystem Group	WORKG	SROUP	Top 5	Minterval:	Last 1 Day 💌	Refresh once in: 5 💌 n	nins 📃 Ackn	owledged F	Refreshed at: 4	:22:42 PM		
				LOGbinder:	SharePoint si SharePoint au LOGbinder set	Share	Point Alerts					
atest Inciden ort By Time	~		Latest 20	) Incidents(3)		Show all incident	s	Tot	al Incidents- 30			8
Date/Time		Event Id Sy		Event Type	a second second	Description				Acknowled	lge Notes	^
6/5/2012 2:42:04 PM	Medium	553 LE	0	Information	LOGbndSE N/A	Incident Name : LOGB Description : LOGBind http://leo/MySite adju Update, Profile Chang Change, Undelete, W http://leo/MySite char http://logbinder.com/	er settings changed sted: Check Out, ( e, Child Delete, Sc orkflow, Copy, Mov iged to UseCustom	d Settings for Check In, View hema Change ve, Search. P	w, Delete, e, Security folicy for			
5/5/2012 1:00:38 PM	Medium	38 LE	0	Audit Success	LOGbndSC Admin	istrator Incident Name : LOGb removed Description : SharePoi Occurred: 6/5/2012 1: deepak@prismcomm.c deepak@prismcoms.c htp://logbinder.com/	nt site collection ac 00:31 PM Site; htt om Administrator I s.com For more inf	dministrator n :p://leo:2495 D: 23 Name:	emoved 6 User:		۵	^
6/5/2012 12:59:39 PM	Medium	11 LE	0	Audit Success	LOGbndSC Admin	istrator Incident Name : LOGb Description : Site colle 12:59:38 PM Site: http policy: Check Out; Ch Schema Change; Secu Search For more infor	ction audit policy d h://leo:16145 User eck In; View; Delet rity Change; Unde	hanged Occu : System Acc e; Update; C lete; Workflo	rred: 6/5/2012 ount New audit hild Delete; w; Copy; Move;		D	<ul> <li>III</li> </ul>
	cker								1957050 <sup>(2</sup>			

Figure 7

- 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

Alert Management Search: Go Show All Page Size: 25 V									age Size: 25 😵	
Alert Name≜	Threat level	Active	Веер	E-mail	Message	R55	Forward as SNMP	Forward as SYSLOG	Remedial Action at Console	Remedial Action at Agent
LOGbinder: LOGbinder setting changed	High									
LOGbinder: Possible audit trail tampering	Critical	~								
LOGbinder: SharePoint audt logs deleted	High									
LOGbinder: SharePoint audit policy change	High	~								
LOGBinder: SharePoint site collection administrator added	High									
LOGbinder: SharePoint site collection administrator removed	High									
	***	lick 'Activ	ate Now'	after mal	cing all chan	ides A	ctivate Now		Add alert	Delete

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.

Incidents	Status Sec	urity Operations	Netflow	My EventTracker	Compliance	Windows	Analysis	Log View	Change Audit	Config Assessment	
Category	v Managemer	nt									
Category Tree Search				Total category groups : 210				Total categories : 1,950			
	binder SP			Last 10 modified cate	egories						
	OGbinder: Logbir			Name				Modified dat	e	Modified by	
- DGbinder: LOGbinder setting changed				LOGbinder: LOGbinder setting changed				6/5/2012 2:43:56 PM		deepak	
	OGbinder: LOGbi	nder warning		LOGbinder: Logbinder error			6/5/2012 2:42:58 PM		deepak		
				LOGbinder: LOGbinder warning				6/5/2012 12:52:57 PM			
				LOGbinder: Noise events			6/5/2012 12:52:57 PM				
	OGbinder: ShareP	oint audit log de etec		LOGbinder: SharePoint access control change			6/5/2012 12:52:57 PM				
- D L	OGbinder: Sharep	oint audit policy char	nge	LOGbinder: SharePoint	audit log deleted			6/5/2012 12:5	2:57 PM		
	and the second	oint container object		LOGbinder: Sharepoint -	audit policy changed			6/5/2012 12:5	2:57 PM		
				LOGbinder: SharePoint	container object upd	ate		6/5/2012 12:5	2:57 PM		
		oint document updat	e —	LOGbinder: SharePoint	document update			6/5/2012 12:5	2:57 PM		
	OGbinder: ShareP	oint Import-Export		LOGbinder: SharePoint :	Import-Export			6/5/2012 12:5	2:57 PM		
📄 L	OGbinder: ShareP	oint Information mar	iag								
📄 L	OGbinder: ShareP	oint list update									
	OGbinder: ShareP	oint object changes									
			×								
Event	Tracker 🦻			er Time: 06/05 04:36:30 PM	Response: 0.31 secs				D Copyright 1999 - 2		

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 A		Welcome Sonal Kharat.	I <u>News</u>	<u>Search</u>   <u>Admi</u>	n   <u>Tools</u>	<u>Help</u>
Incidents Status Security	Operations Netflow My EventTracker Compliance V	Vindows Analysis	Log View	Change Audit	Config Assess	ment
Analysis	Defined analysis Search ShowAll ShowAll					^
	Title	Crea	ted on <b>▼</b>	Delete		
Detail	LOGbinder SP SharePoint Generic Object Changes	3/1/2				
Trend	LOGbinder SP Sharepoint Information Management Policy Changes	3/1/2	011 1:33:33 PM			
Summary	LOGbinder SP SharePoint View Events report		3/1/2	011 11:52:19 AM		
Detail	LOGbinder SP SharePoint Item updates		3/1/2	011 11:47:44 AM		
🖃 🎦 Cost Savings	LOGbinder SP SharePoint Access Control changes		3/1/2	011 11:45:22 AM		
Summary     Person Hour	LOGbinder SP Sharepoint Audit Trail Setting Changes		3/1/2	011 11:41:39 AM		
Actions Desoldward Desoldward Queued Scheduled Exceptions	New	Edit Delate	Schedule	Add to que	ie Run no	₩.
Event Tracker 7	Server Time: (6/05 04:58:32 PM Response: 0.31 secs		(	D Copyright 1999 - 2	012 Prism Microsy	stems, Inc.

Figure 10

