Common Event Format Configuration Guide

LOGbinder

LOGbinder SP 3.5

Date: Wednesday, January 09, 2013

LOGbinder SP™

CEF Connector Configuration Guide

This document is provided for informational purposes only, and the information herein is subject to change without notice. Please report any errors herein to HP. HP does not provide any warranties covering this information and specifically disclaims any liability in connection with this document.

Certified CEF:

The event format complies with the requirements of the HP ArcSight Common Event Format. The HP ArcSight CEF connector will be able to process the events correctly and the events will be available for use within HP's ArcSight product. In addition, the event content has been deemed to be in accordance with standard SmartConnector requirements. The events will be sufficiently categorized to be used in correlation rules, reports and dashboards as a proof-of-concept (POC) of the joint solution

LOGbinder SP v3.5

11/13/2012

Revision History

Date	Description
11/13/2012	First edition of this Configuration Guide.
01/09/2013	Version 3.5 Certified by HP Enterprise Security

CEF Connector Support Information when an issue is outside of the ArcSight team's ability

In some cases the ArcSight customer service team is unable to help with issues that lie within the configuration itself in which case, the certified vendor should be contacted for assistance:

Tamas Lengyel Customer Support

Phone -1-866-749-2048 x.805

Email – Support@logbinder.com

Instructions –

If you are having problems installing or configuring LOGbinder SP, please
Refer to the "Getting Started Guide" that was included in the software download.
Contact a member of our support team and open a ticket by emailing Support@LOGbinder.com.

LOGbinder SP Configuration Guide

This guide provides information for configuring LOGbinder SP for syslog event collection. This Connector is supported on Windows based platforms. In order to use LOGbinder SP you must have a system with the following requirements:

SharePoint Services 3.0, Office SharePoint Server 2007, SharePoint Foundation, or SharePoint Server 2010
.Net Framework 3.5 SP1 or later
Windows Server 2003 32/64 bit or 2008 32/64 bit

Overview

LOGbinder SP is a small, efficient Windows service that monitors the internal SharePoint audit log without making any changes to your SharePoint installation. LOGbinder SP quickly installs on your SharePoint Server and allows you to quickly configure auditing on any or all of the server's site collections.

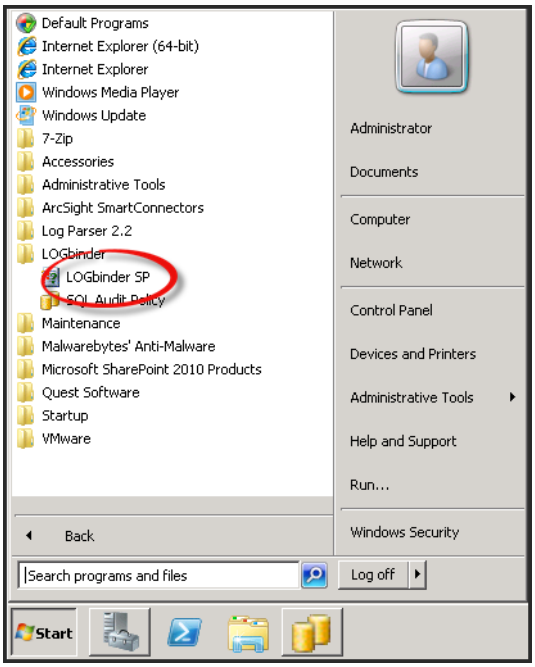
LOGbinder begins watching the SharePoint audit log. For each SharePoint audit event LOGbinder SP resolves the user and object IDs and other cryptic codes, producing an easy to understand, plain-English translation of the SharePoint audit event and reports it to the Windows Security, a custom LOGbinder SP event log, or for ArcSight CEF over Syslog.

From that point you can track SharePoint audit activity and use your log management solution to collect, monitor, report and securely archive your SharePoint audit logs. LOGbinder SP can periodically prune old SharePoint audit events from the SharePoint content database thus conserving expensive SQL server storage.

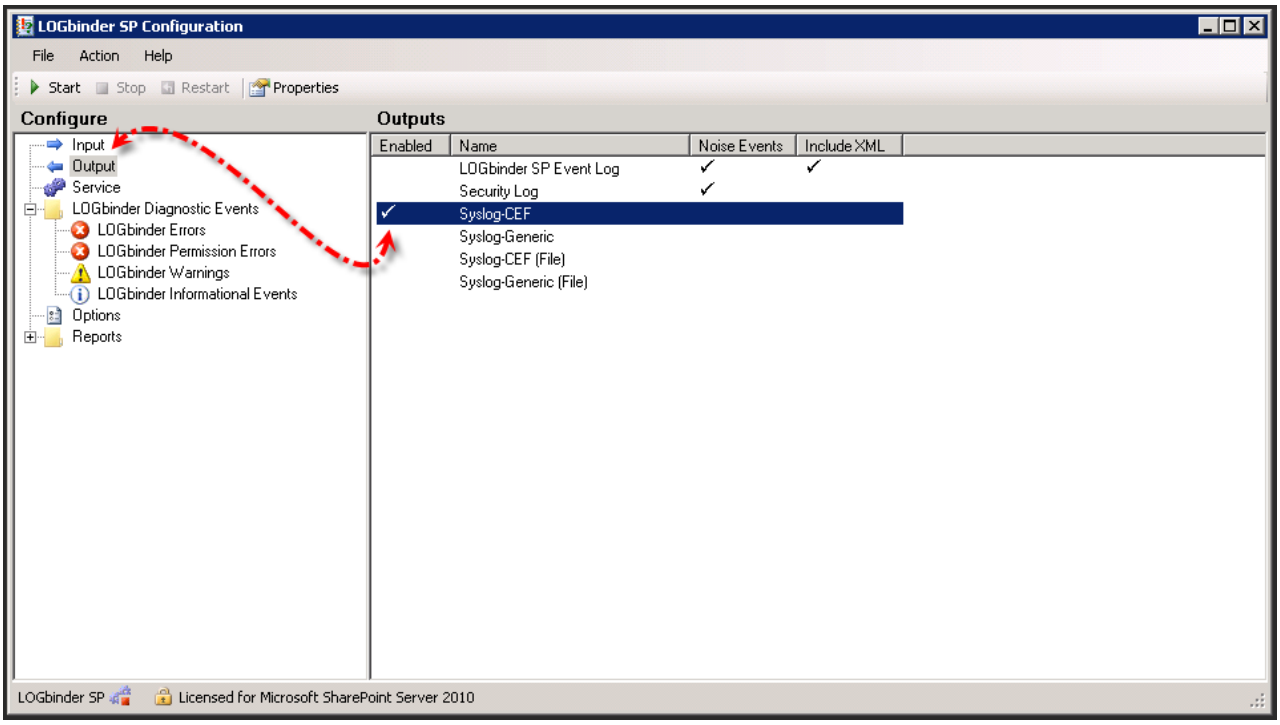
Configuration

If you have any questions regarding the installation of LOGbinder SP, please download the latest "Getting Started Guide" from http://www.logbinder.com/support/default.aspx .

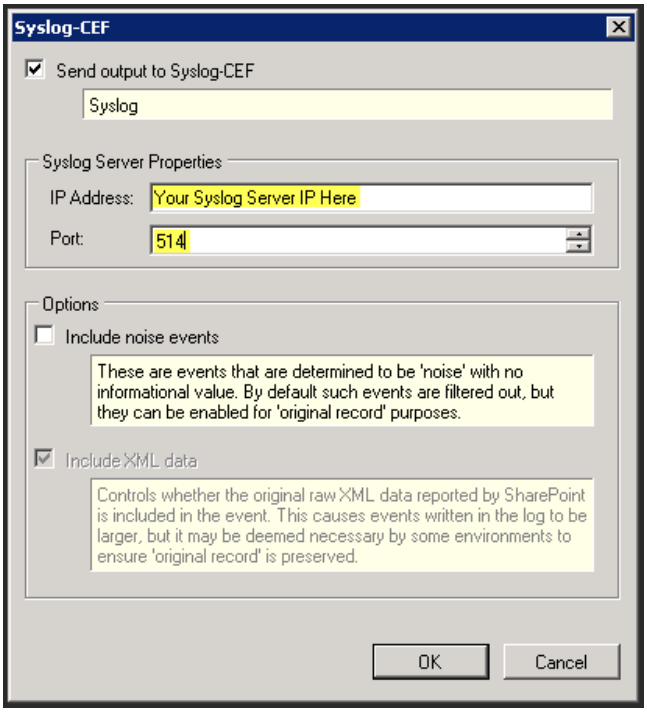
Once installed, open the LOGbinder Configurator from the Start Menu under LOGbinder.



Select “Outputs” from the left menu and then double click on “Syslog-CEF”.

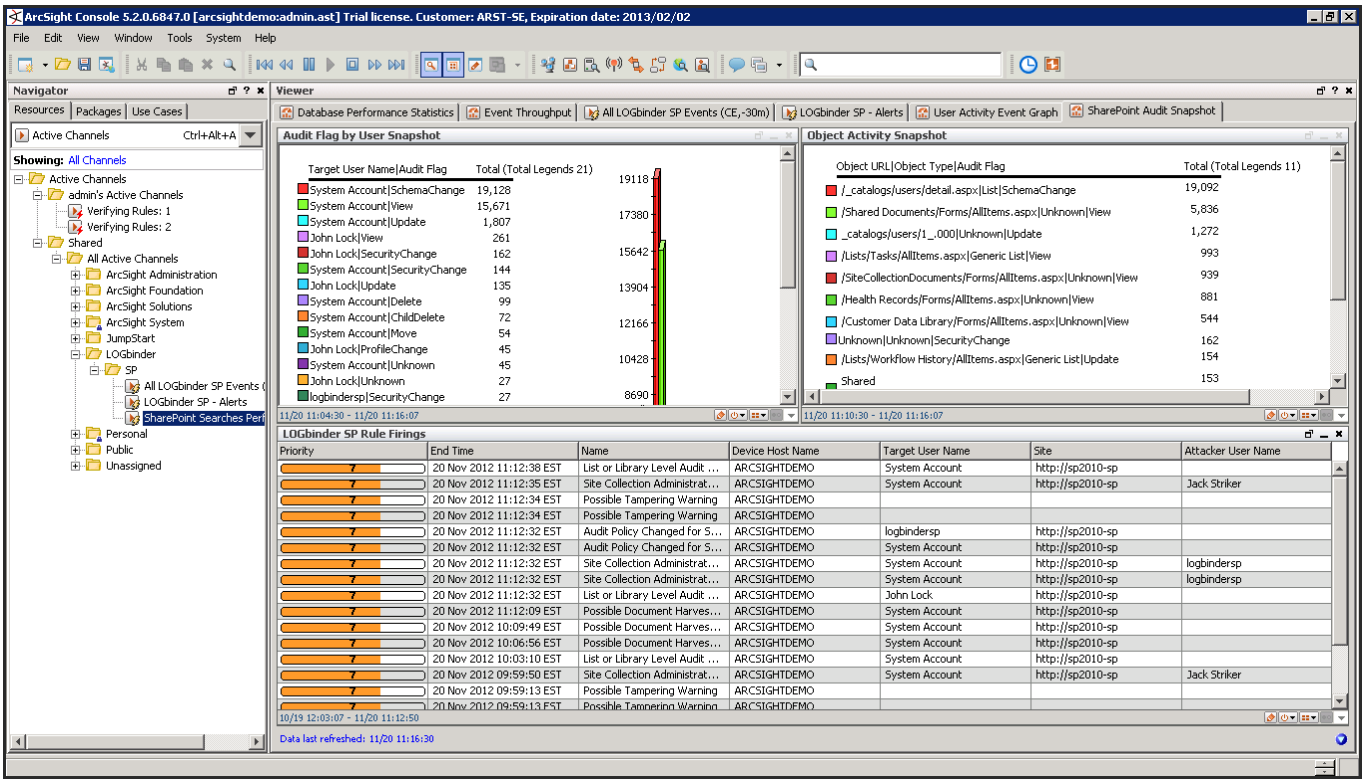


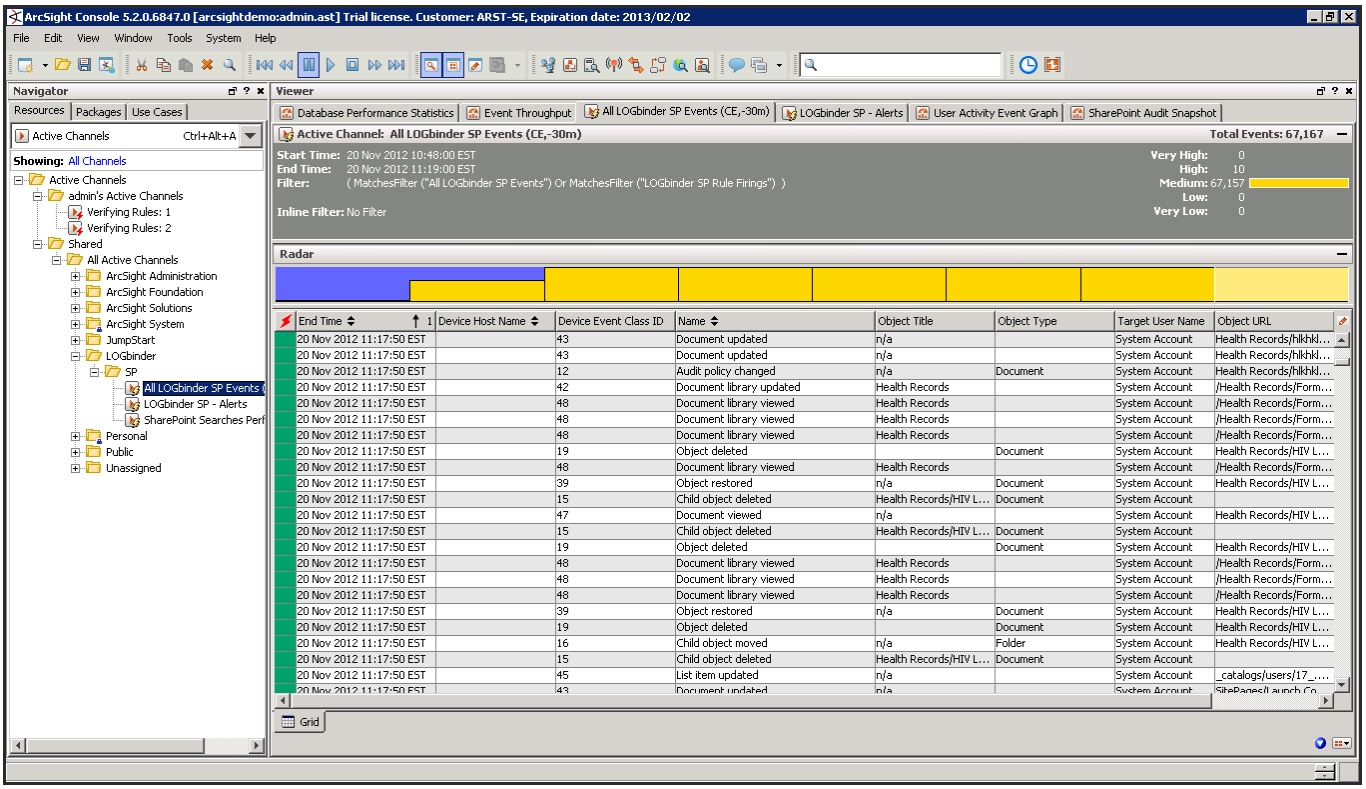
Enter the information for your syslog server and then click on “OK”.



Once the service is restarted the settings will be applied and you should begin receiving SharePoint events.

Screen Shot


ArcSight Console 5.2.0.6847.0 [arcsightdemo:admin.ast] Trial license. Customer: ARST-SE, Expiration date: 2013/02/02
File Edit View Window Tools System Help
Navigator
Resources Packages Use Cases
Active Channels Ctrl+Alt+A
Showing: All Channels
Active Channels
admin's Active Channels
Verifying Rules: 1
Verifying Rules: 2
Shared
All Active Channels
ArcSight Administration
ArcSight Foundation
ArcSight Solutions
ArcSight System
JumpStart
LOGbinder
SP
All LOGbinder SP Events (
LOGbinder SP - Alerts
SharePoint Searches Perf
Personal
Public
Unassigned
Viewer
Database Performance Statistics
Event Throughput
All LOGbinder SP Events (CE,-30m)
LOGbinder SP - Alerts
User Activity Event Graph
SharePoint Audit Snapshot
Audit Flag by User Snapshot
Target User Name|Audit Flag
Total (Total Legends 21)
System Account|SchemaChange 19,128
System Account|View 15,671
System Account|Update 1,807
John Lock|View 261
John Lock|SecurityChange 162
System Account|SecurityChange 144
John Lock|Update 135
System Account|Delete 99
System Account|ChildDelete 72
System Account|Move 54
John Lock|ProfileChange 45
System Account|Unknown 45
John Lock|Unknown 27
logbindersp|SecurityChange 27
19118
17380
15642
13904
12166
10428
8690
11/20 11:04:30 - 11/20 11:16:07
Object Activity Snapshot
Object URL|Object Type|Audit Flag
Total (Total Legends 11)
/_catalogs/users/detail.aspx|List|SchemaChange 19,092
/Shared Documents/Forms/AllItems.aspx|Unknown|View 5,836
catalogs/users/1.000|Unknown|Update 1,272
/Lists/Tasks/AllItems.aspx|Generic List|View 993
/SiteCollectionDocuments/Forms/AllItems.aspx|Unknown|View 939
/Health Records/Forms/AllItems.aspx|Unknown|View 881
/Customer Data Library/Forms/AllItems.aspx|Unknown|View 544
Unknown|Unknown|SecurityChange 162
/Lists/Workflow History/AllItems.aspx|Generic List|Update 154
Shared 153
11/20 11:10:30 - 11/20 11:16:07
LOGbinder SP Rule Firings
Priority
End Time
Name
Device Host Name
Target User Name
Site
Attacker User Name
20 Nov 2012 11:12:38 EST List or Library Level Audit ... ARCSIGHTDEMO System Account http://sp2010-sp
20 Nov 2012 11:12:35 EST Site Collection Administrat... ARCSIGHTDEMO System Account http://sp2010-sp Jack Striker
20 Nov 2012 11:12:34 EST Possible Tampering Warning ARCSIGHTDEMO
20 Nov 2012 11:12:34 EST Possible Tampering Warning ARCSIGHTDEMO
20 Nov 2012 11:12:32 EST Audit Policy Changed for S... ARCSIGHTDEMO logbindersp http://sp2010-sp
20 Nov 2012 11:12:32 EST Audit Policy Changed for S... ARCSIGHTDEMO System Account http://sp2010-sp
20 Nov 2012 11:12:32 EST Site Collection Administrat... ARCSIGHTDEMO System Account http://sp2010-sp logbindersp
20 Nov 2012 11:12:32 EST Site Collection Administrat... ARCSIGHTDEMO System Account http://sp2010-sp logbindersp
20 Nov 2012 11:12:32 EST List or Library Level Audit ... ARCSIGHTDEMO John Lock http://sp2010-sp
20 Nov 2012 11:12:09 EST Possible Document Harves... ARCSIGHTDEMO System Account http://sp2010-sp
20 Nov 2012 10:09:49 EST Possible Document Harves... ARCSIGHTDEMO System Account http://sp2010-sp
20 Nov 2012 10:06:56 EST Possible Document Harves... ARCSIGHTDEMO System Account http://sp2010-sp
20 Nov 2012 10:03:10 EST List or Library Level Audit ... ARCSIGHTDEMO System Account http://sp2010-sp
20 Nov 2012 09:59:50 EST Site Collection Administrat... ARCSIGHTDEMO System Account http://sp2010-sp Jack Striker
20 Nov 2012 09:59:13 EST Possible Tampering Warning ARCSIGHTDEMO
10/19 12:03:07 - 11/20 11:12:50
Data last refreshed: 11/20 11:16:30


ArcSight Console 5.2.0.6847.0 [arcsightdemo:admin.ast] Trial license. Customer: ARST-SE, Expiration date: 2013/02/02
File Edit View Window Tools System Help
Navigator
Resources Packages Use Cases
Active Channels Ctrl+Alt+A
Showing: All Channels
Active Channels
admin's Active Channels
Verifying Rules: 1
Verifying Rules: 2
Shared
All Active Channels
ArcSight Administration
ArcSight Foundation
ArcSight Solutions
ArcSight System
JumpStart
LOGbinder
SP
All LOGbinder SP Events (
LOGbinder SP - Alerts
SharePoint Searches Perf
Personal
Public
Unassigned
Viewer
Database Performance Statistics
Event Throughput
All LOGbinder SP Events (CE,-30m)
LOGbinder SP - Alerts
User Activity Event Graph
SharePoint Audit Snapshot
Active Channel: All LOGbinder SP Events (CE,-30m)
Total Events: 67,167
Start Time: 20 Nov 2012 10:48:00 EST
End Time: 20 Nov 2012 11:19:00 EST
Filter: (MatchesFilter ("All LOGbinder SP Events") Or MatchesFilter ("LOGbinder SP Rule Firings"))
Inline Filter: No Filter
Very High: 0
High: 10
Medium: 67,157
Low: 0
Very Low: 0
Radar
End Time
Device Host Name
Device Event Class ID
Name
Object Title
Object Type
Target User Name
Object URL
20 Nov 2012 11:17:50 EST 43 Document updated n/a System Account Health Records/hlkhkl...
20 Nov 2012 11:17:50 EST 43 Document updated n/a System Account Health Records/hlkhkl...
20 Nov 2012 11:17:50 EST 12 Audit policy changed n/a Document System Account Health Records/hlkhkl...
20 Nov 2012 11:17:50 EST 42 Document library updated Health Records System Account /Health Records/Form...
20 Nov 2012 11:17:50 EST 48 Document library viewed Health Records System Account /Health Records/Form...
20 Nov 2012 11:17:50 EST 48 Document library viewed Health Records System Account /Health Records/Form...
20 Nov 2012 11:17:50 EST 48 Document library viewed Health Records System Account /Health Records/Form...
20 Nov 2012 11:17:50 EST 19 Object deleted Document System Account Health Records/HIV L...
20 Nov 2012 11:17:50 EST 48 Document library viewed Health Records System Account /Health Records/Form...
20 Nov 2012 11:17:50 EST 39 Object restored n/a Document System Account Health Records/HIV L...
20 Nov 2012 11:17:50 EST 15 Child object deleted Health Records/HIV L... Document System Account
20 Nov 2012 11:17:50 EST 47 Document viewed n/a System Account Health Records/HIV L...
20 Nov 2012 11:17:50 EST 15 Child object deleted Health Records/HIV L... Document System Account
20 Nov 2012 11:17:50 EST 19 Object deleted Document System Account Health Records/HIV L...
20 Nov 2012 11:17:50 EST 48 Document library viewed Health Records System Account /Health Records/Form...
20 Nov 2012 11:17:50 EST 48 Document library viewed Health Records System Account /Health Records/Form...
20 Nov 2012 11:17:50 EST 48 Document library viewed Health Records System Account /Health Records/Form...
20 Nov 2012 11:17:50 EST 39 Object restored n/a Document System Account Health Records/HIV L...
20 Nov 2012 11:17:50 EST 19 Object deleted Document System Account Health Records/HIV L...
20 Nov 2012 11:17:50 EST 16 Child object moved n/a Folder System Account Health Records/HIV L...
20 Nov 2012 11:17:50 EST 15 Child object deleted Health Records/HIV L... Document System Account
20 Nov 2012 11:17:50 EST 45 List item updated n/a System Account _catalogs/users/17_....
Grid

Events

All LOGbinder SP SharePoint event ID's and descriptions can be found at http://www.ultimatewindowssecurity.com/securitylog/encyclopedia/default.aspx

Device Event Mapping to ArcSight Data Fields

Information contained within vendor-specific event definitions is sent to the ArcSight SmartConnector, then mapped to an ArcSight data field.

The following table lists the mappings from ArcSight data fields to the supported vendor-specific event definitions.

LOGbinder SP Connector Field Mappings

Vendor Event ID	Vendor-Specific Event Definition	ArcSight Event Data Field
10	**Noise entry**	name
	Message	message
	Occurred: 11/11/2011 8:08:37 PM	receiptTime
	Details:	filePermission
11	**Audit policy changed**	name
	Occurred: 11/22/2011 8:08:37 PM	receiptTime
	Site: http://sp2010-sp	requestUrl
	User: logbindersp	destinationUserName
	New audit policy: Check Out; Check In; Delete; Update; Profile Change;	deviceCustomString3
12	**Audit policy changed**	name
	Occurred: 11/21/2011 8:45:51 PM	receiptTime
	Site: http://sp2010-sp	requestUrl
	User: System Account	destinationUserName
	Object	
	Type: Document	fileType
	Subtype: n/a	deviceCustomString1
	URL: Shared Documents/FinancialReport.xlsx	filePath
	Title: n/a	fileName
	Description: n/a	message
	New audit policy:	deviceCustomString3
13	**Document checked in**	name
	Occurred: 11/24/2011 1:13:04 PM	receiptTime
	Site: http://sp2010-sp	requestUrl

Vendor Event ID	Vendor-Specific Event Definition	ArcSight Event Data Field
	User: Randy F. Smith	destinationUserName
	Object	
	URL: Shared Documents/FinancialData.xlsx	filePath
	Title: n/a	fileName
	Version: 1.0	fileId
14	**Document checked out**	name
	Occurred: 11/24/2011 1:11:43 PM	receiptTime
	Site: http://sp2010-sp	requestUrl
	User: Randy F. Smith	destinationUserName
	Object	
	URL: Shared Documents/Security_settings_2011-11-22T012342.xlsx	filePath
	Title: n/a	fileName
	Version: 1.0	fileId
15	**Child object deleted**	name
	Occurred: 11/21/2011 1:05:02 AM	receiptTime
	Site: http://sp2010-sp	requestUrl
	User: System Account	destinationUserName
	Parent Object	
	Type: List	fileType
	Subtype: Document Library	deviceCustomString1
	URL: /Shared Documents/Forms/AllItems.aspx	filePath
	Title: Shared Documents	fileName
	Child Object	
	Type: Document	oldFileType
	URL: Shared Documents/PatientRecords.xls	oldFilePath
16	**Child object moved**	name
	Occurred: 11/21/2011 5:52:16 PM	receiptTime
	Site: http://sp2010-sp	requestUrl
	User: System Account	destinationUserName
	Parent Object	
	Type: List	fileType
	Subtype: Document Library	deviceCustomString1
	URL: /Shared Documents/Forms/AllItems.aspx	filePath
	Title: Shared Documents	fileName
	Description: Share a document with the team by adding it to this document library.	message
	Child Object	

Vendor Event ID	Vendor-Specific Event Definition	ArcSight Event Data Field
	Type: Document	oldFileType
	Title: n/a	oldFileName
	Original location: Shared Documents/CustomerProfile.xlsx	oldFilePath
	New location: Customer Data Library/CustomerProfile.xlsx	deviceCustomString2
17	**Object copied**	name
	Occurred: 11/20/2011 9:28:32 PM	receiptTime
	Site: http://sp2010-sp	requestUrl
	User: System Account	destinationUserName
	Object	
	Type: Document	fileType
	Title: n/a	fileName
	Description: n/a	message
	Original location: Shared Documents/Auditing_settings.xlsx	filePath
	New location: http://sp2010-sp/Customer%20Data%20Library/Auditing_settings.xlsx	oldFilePath
18	**Custom Event**	name
	Occurred: 11/21/2011 1:05:02 AM	receiptTime
	Site: http://sp2010-sp	requestUrl
	User: John Smith	destinationUserName
	Details:	filePermission
	Message:	message
19	**Object deleted**	name
	Occurred: 11/21/2011 1:05:02 AM	receiptTime
	Site: http://sp2010-sp	requestUrl
	User: John Smith	destinationUserName
	Object	
	Type: Document	fileType
	URL: Shared Documents/FinancialReport.txt	filePath
	Versions deleted: All versions deleted	fileId
	Recycled: Item in end-user Recycle Bin	oldFileId
20	**SharePoint audit logs deleted**	name
	Occurred: 11/23/2011 1:00:04 AM	receiptTime
	Site: http://sp2010-sp	requestUrl

Vendor Event ID	Vendor-Specific Event Definition	ArcSight Event Data Field
	User: logbindersp	destinationUserName
	Logs deleted: 538	deviceCustomNumber1
	Last Date: 11/22/2011 12:00:00 AM	deviceCustomDate1
	Audit logs created before this date have been removed from SharePoint.	message
	Purge by LOGbinder	filePermission
21	**Object moved**	name
	Occurred: 11/21/2011 5:52:16 PM	receiptTime
	Site: http://sp2010-sp	requestUrl
	User: System Account	destinationUserName
	Object	
	Type: Document	fileType
	Title: n/a	fileName
	Original location: Shared Documents/Auditing_settings.xlsx	oldFilePath
	New location: http://sp2010-sp/Customer%20Data%20Library/Auditing_settings.xlsx	filePath
22	**Object profile changed**	name
	Occurred: 11/21/2011 3:15:29 PM	receiptTime
	Site: http://sp2010-sp	requestUrl
	User: System Account	destinationUserName
	Object	
	Type: List	fileType
	Subtype: Generic List	deviceCustomString1
	URL: /Lists/Tasks/AllItems.aspx	filePath
	Title: Tasks	fileName
	Description: Use the Tasks list to keep track of work that you or your team needs to complete.	message
	Profile details: <ContentType	filePermission
23	**SharePoint object structure changed**	name
	Occurred: 11/21/2011 3:15:28 PM	receiptTime
	Site: http://sp2010-sp	requestUrl
	User: System Account	destinationUserName
	Object	
	Type: List	fileType
	Subtype: Generic List	deviceCustomString1
	URL: /Lists/Tasks/AllItems.aspx	filePath

Vendor Event ID	Vendor-Specific Event Definition	ArcSight Event Data Field
	Title: Tasks	fileName
	Description: Use the Tasks list to keep track of work that you or your team needs to complete.	message
	Details:	filePermission
24	**Search performed**	name
	Occurred: 1/11/2011 8:04:15 AM	receiptTime
	Site: http://sp2010-sp	requestUrl
	User: System Account	destinationUserName
	Search: query='this is a search';constraint=' site:"http://sp2010-sp" '	message
25	**SharePoint group created**	name
	Occurred: 11/22/2011 12:05:49 AM	receiptTime
	Site: http://sp2010-sp	requestUrl
	User: System Account	destinationUserName
	Group	
	ID: 27	fileId
	Name: TestGroup	fileName
	Initial members: System Account	filePermission
26	**SharePoint group deleted**	name
	Occurred: 11/22/2011 12:07:25 AM	receiptTime
	Site: http://sp2010-sp	requestUrl
	User: System Account	destinationUserName
	Group	
	ID: 27	fileId
	Message	message
27	**SharePoint group member added**	name
	Occurred: 11/22/2011 10:46:34 PM	receiptTime
	Site: http://sp2010-sp	requestUrl
	User: Randy F. Smith	sourceUserName
	Group	
	ID: 22	fileId
	Name: Customer Information	fileName
	Member	
	ID: 26	destinationUserId
	Name: SP2010\wsmith	destinationUserName
28	**SharePoint group member removed**	name

Vendor Event ID	Vendor-Specific Event Definition	ArcSight Event Data Field
	Occurred: 11/22/2011 12:07:11 AM	receiptTime
	Site: http://sp2010-sp	requestUrl
	User: System Account	sourceUserName
	Group	
	ID: 27	fileId
	Name: n/a	fileName
	Member	
	ID: 17	destinationUserId
	Name: Jack Striker	destinationUserName
29	**Unique permissions created**	name
	Occurred: 11/22/2011 12:40:43 AM	receiptTime
	Site: http://sp2010-sp	requestUrl
	User: System Account	destinationUserName
	Parent Object	
	Type: Web	fileType
	Subtype: n/a	deviceCustomString1
	URL: http://sp2010-sp	filePath
	Title: SP2010	fileName
	Description: ddddddddddddddddddd	message
	Object	
	URL: Lists/My List	oldFilePath
	Message	filePermission
30	**Unique permissions removed**	name
	Occurred: 11/22/2011 12:54:47 AM	receiptTime
	Site: http://sp2010-sp	requestUrl
	User: System Account	destinationUserName
	Parent Object	
	Type: Web	fileType
	Subtype: n/a	deviceCustomString1
	URL: Lists/My List	filePath
	Title: n/a	fileName
	Description: n/a	message
	Object	
	URL: Lists/My List	oldFilePath
	Message	filePermission
31	**Permissions updated**	name
	Occurred: 11/22/2011 5:02:59 PM	receiptTime

Vendor Event ID	Vendor-Specific Event Definition	ArcSight Event Data Field
	Site: http://sp2010-sp	requestUrl
	User: System Account	destinationUserName
	Object	
	Type: Web	fileType
	Subtype: n/a	deviceCustomString1
	URL: http://sp2010-sp	filePath
	Title: SP2010	fileName
	Description: ddddddddddddddddddd	message
	Target	
	Name: Customer Information	oldFileName
	Type: Group	oldFileType
	Permissions	
	Role name: Read	oldFilePermission
	Role description: Can view pages and list items and download documents.	oldFileId
	Message	filePermission
32	**Permissions removed**	name
	Occurred: 11/22/2011 1:21:21 AM	receiptTime
	Site: http://sp2010-sp	requestUrl
	User: System Account	destinationUserName
	Object	
	Type: Web	fileType
	Subtype: n/a	deviceCustomString1
	URL: http://sp2010-sp	filePath
	Title: SP2010	fileName
	Description: ddddddddddddddddddd	message
	Target	
	Name: Jack Striker	oldFileName
	Type: User	oldFileType
33	**Unique permission levels created**	name
	Occurred: 11/22/2011 12:59:06 AM	receiptTime
	Site: http://sp2010-sp	requestUrl
	User: System Account	destinationUserName
	Object	
	Type: Web	fileType
	URL: http://sp2010-sp	filePath
	Title: SP2010	fileName
	Description: ddddddddddddddddddd	message

Vendor Event ID	Vendor-Specific Event Definition	ArcSight Event Data Field
	Message	filePermission
34	**Permission level created**	name
	Occurred: 11/22/2011 12:59:06 AM	receiptTime
	Site: http://sp2010-sp	requestUrl
	User: System Account	destinationUserName
	Object	
	Type: Web	fileType
	URL: http://sp2010-sp	filePath
	Title: SP2010	fileName
	Description: ddddddddddddddddddd	message
	Permission Level Details	
	ID: 1073741930	oldFileId
	Name: SomeAccess	oldFileName
	Type: None	oldFileType
	Description: n/a	oldFilePermission
	Permissions	
	List permissions: View Items; Edit Items; Open Items	deviceCustomString1
	Site permissions: Open; View Pages	deviceCustomString2
	Personal permissions: n/a	deviceCustomString3
35	**Permission level deleted**	name
	Occurred: 11/22/2011 1:04:19 AM	receiptTime
	Site: http://sp2010-sp	requestUrl
	User: System Account	destinationUserName
	Object	
	Type: Web	fileType
	URL: http://sp2010-sp	filePath
	Title: SP2010	fileName
	Description: ddddddddddddddddddd	message
	Permission Level Details	
	ID: 1073741930	oldFileId
	Message:	filePermission
36	**Permission level modified**	name
	Occurred: 11/22/2011 1:04:07 AM	receiptTime
	Site: http://sp2010-sp	requestUrl
	User: System Account	destinationUserName
	Object	
	Type: Web	fileType

Vendor Event ID	Vendor-Specific Event Definition	ArcSight Event Data Field
	URL: http://sp2010-sp	filePath
	Title: SP2010	fileName
	Description: ddddddddddddddddddd	message
	Permission Level Details	
	ID: 1073741930	oldFileId
	Name: SomeAccess	oldFileName
	Type: n/a	oldFileType
	Description: n/a	oldFilePermission
	Permissions	
	List permissions: View Items; Add Items; Edit Items; Open Items	deviceCustomString1
	Site permissions: Open; View Pages	deviceCustomString2
	Personal permissions: n/a	deviceCustomString3
37	**SharePoint site collection administrator added**	name
	Occurred: 11/22/2011 5:22:19 PM	receiptTime
	Site: http://sp2010-sp	requestUrl
	User: System Account	sourceUserName
	Administrator	
	ID: 28	destinationUserId
	Name: Randy F. Smith	destinationUserName
38	**SharePoint site collection administrator removed**	name
	Occurred: 2/12/2011 2:56:02 AM	receiptTime
	Site: http://sp2010-sp	requestUrl
	User: System Account	sourceUserName
	Administrator	
	ID: 20	destinationUserId
	Name: NT AUTHORITY\system	destinationUserName
39	**Object restored**	name
	Occurred: 11/21/2011 10:25:13 PM	receiptTime
	Site: http://sp2010-sp	requestUrl
	User: System Account	destinationUserName
	Object	
	Type: List	fileType
	URL: /Customer Data Library/Forms/AllItems.aspx	filePath
	Title: Customer Data Library	fileName
	Description: n/a	message
	Message:	filePermission

Vendor Event ID	Vendor-Specific Event Definition	ArcSight Event Data Field
40	**Site Collection Updated**	name
	Occurred: 11/22/2011 1:23:43 AM	receiptTime
	Site: http://sp2010-sp	requestUrl
	User: System Account	destiantionUserName
41	**Point Web Updated**	name
	Occurred: 11/21/2011 10:25:13 PM	receiptTime
	Site: http://sp2010-sp	requestUrl
	User: System Account	destinationUserName
	Object	
	URL: /Customer Data Library/Forms/AllItems.aspx	filePath
	Title: Customer Data Library	fileName
	Description: n/a	message
42	**Document library updated**	name
	Occurred: 11/22/2011 1:23:43 AM	receiptTime
	Site: http://sp2010-sp	requestUrl
	User: System Account	destinationUserName
	Object	
	URL: /Shared Documents/Forms/AllItems.aspx	filePath
	Title: Shared Documents	fileName
	Description: Share a document with the team by adding it to this document library.	message
	Library item updated: Security_settings_2011-11-22T012342.xlsx	oldFileName
43	**Document updated**	name
	Occurred: 11/22/2011 1:23:43 AM	receiptTime
	Site: http://sp2010-sp	requestUrl
	User: System Account	destinationUserName
	Object	
	URL: Shared Documents/Security_settings_2011-11-22T012342.xlsx	filePath
	Title: n/a	fileName
	Version: n/a	fileId
44	**List updated**	name
	Occurred: 11/21/2011 1:04:52 AM	receiptTime
	Site: http://sp2010-sp	requestUrl
	User: System Account	destinationUserName

Vendor Event ID	Vendor-Specific Event Definition	ArcSight Event Data Field
	Object	
	Type: Generic List	fileType
	URL: /Long Running Operation Status/AllItems.aspx	filePath
	Title: Long Running Operation Status	fileName
	Description: n/a	message
45	**List item updated**	name
	Occurred: 11/21/2011 7:06:02 PM	receiptTime
	Site: http://sp2010-sp	requestUrl
	User: System Account	destinationUserName
	Object	
	URL: Lists/My List/2_.000	filePath
	Title: asdfasdfddd	fileName
46	**Folder updated**	name
	Occurred: 2/12/2011 3:17:41 AM	receiptTime
	Site: http://sp2010-sp	requestUrl
	User: System Account	destinationUserName
	Object	
	URL: asdf/Lists/Team Discussion	filePath
	Version: 1.0	fileId
47	**Document viewed**	name
	Occurred: 11/22/2011 5:03:00 PM	receiptTime
	Site: http://sp2010-sp	requestUrl
	User: System Account	destinationUserName
	Object	
	URL: _catalogs/masterpage/v4.master	filePath
	Title: <asp:ContentPlaceHolder id="PlaceHolderPageTitle" runat="server"/>	fileName
	Version: 1.0	fileId
48	**Document library viewed**	name
	Occurred: 11/20/2011 5:55:56 PM	receiptTime
	Site: http://sp2010-sp	requestUrl
	User: System Account	destinationUserName
	Object	
	URL: /SitePages/Forms/AllPages.aspx	filePath
	Title: Site Pages	fileName
	Description: Use this library to create and store pages on this site.	message

Vendor Event ID	Vendor-Specific Event Definition	ArcSight Event Data Field
49	**List viewed**	name
	Occurred: 11/22/2011 1:13:04 AM	receiptTime
	Site: http://sp2010-sp	requestUrl
	User: System Account	destinationUserName
	Object	
	Type: Generic List	fileType
	URL: /Lists/My List/AllItems.aspx	filePath
	Title: My List	fileName
	Description: this is my list	message
50	**Object viewed**	name
	Occurred: 11/22/2011 1:13:04 AM	receiptTime
	Site: http://sp2010-sp	requestUrl
	User: System Account	destinationUserName
	Object	
	Type: Generic List	fileType
	URL: /Lists/My List/AllItems.aspx	filePath
	Title: My List	fileName
	Description: this is my list	message
51	**Workflow accessed**	name
	Occurred: 11/22/2011 1:13:04 AM	receiptTime
	Site: http://sp2010-sp	requestUrl
	User: System Account	destiantionUserName
	Object	
	Type: Generic List	fileType
	URL: /Lists/My List/AllItems.aspx	filePath
	Title: My List	fileName
	Description: this is my list	message
	Message	filePermission
52	**Information management policy created**	name
	Occurred: 11/21/2011 3:15:28 PM	receiptTime
	Site: http://sp2010-sp	requestUrl
	User: System Account	destinationUserName
	Object	
	Type: List	fileType
	Subtype: Generic List	deviceCustomString1
	URL: /Lists/Tasks/AllItems.aspx	filePath

Vendor Event ID	Vendor-Specific Event Definition	ArcSight Event Data Field
	Title: Tasks	fileName
	Description: Use the Tasks list to keep track of work that you or your team needs to complete.	message
	Policy details: <data ContentTypeId="0x01080030F71437AD53BC458A9F8A6F248E9D21" ContentTypeName="Task"><p:Policy xmlns:p="office.server.policy" id="" local="true" /></data>	filePermission
53	**Information management policy changed**	name
	Occurred: 11/21/2011 3:15:28 PM	receiptTime
	Site: http://sp2010-sp	requestUrl
	User: System Account	destinationUserName
	Object	
	Type: List	fileType
	Subtype: Generic List	deviceCustomString1
	URL: /Lists/Tasks/AllItems.aspx	filePath
	Title: Tasks	fileName
	Description: Use the Tasks list to keep track of work that you or your team needs to complete.	message
	Policy details: <data ContentTypeId="0x01080030F71437AD53BC458A9F8A6F248E9D21" ContentTypeName="Task"><p:Policy xmlns:p="office.server.policy" id="" local="true"><p:Name>Task</p:Name><p:Description></p:Description><p:Statement></p:Statement></p:Policy></data>	filePermission
54	**Site collection information management policy created**	name
	Occurred: 12/6/2011 3:23:02 AM	receiptTime
	Site: http://sp2010-sp	requestUrl
	User: Randy F. Smith	destinationUserName
	Policy details: <data><p:Policy xmlns:p="office.server.policy" local="false" id="ba091f4a-b41f-4748-93f1-6d9a310f7ffe"><p:Name></p:Name><p:Description></p:Description><p:Statement></p:Statement></p:Policy></data>	filePermission
55	**Site collection information management policy changed**	name

Vendor Event ID	Vendor-Specific Event Definition	ArcSight Event Data Field
	Occurred: 12/6/2011 3:23:02 AM	receiptTime
	Site: http://sp2010-sp	requestUrl
	User: Randy F. Smith	destinationUserName
	Policy details: <data><p:Policy xmlns:p="office.server.policy" local="false" id="ba091f4a-b41f-4748-93f1-6d9a310f7ffe"><p:Name>TestPolicy</p:Name><p:Description>this is the description</p:Description><p:Statement>this is the statement</p:Statement><p:PolicyItems><p:PolicyItem featureId="Microsoft.Office.RecordsManagement.PolicyFeatures.PolicyAudit" UniqueId="16076acb-9910-46eb-a5ca-c7ddfe5fb2ee"><p:Name>Auditing</p:Name><p:Description>Audits user actions on documents and list items to the Audit Log.</p:Description><p:CustomData><Audit><View /></Audit></p:CustomData></p:PolicyItem></p:PolicyItems></p:Policy></data>	filePermission
56	**Export of objects started**	name
	Occurred: 11/21/2011 1:04:53 AM	receiptTime
	Site: http://sp2010-sp	requestUrl
	Requested by: SP2010\Administrator	destinationUserName
	Message:	message
57	**Export of objects completed**	name
	Occurred: 11/21/2011 1:04:58 AM	receiptTime
	Site: http://sp2010-sp	requestUrl
	Requested by: SP2010\Administrator	destinationUserName
	Total number of items: 7	deviceCustomNumber1
	Size: n/a	fileHash
	Message:	message
58	**Import of objects started**	name
	Occurred: 11/21/2011 1:04:58 AM	receiptTime
	Site: http://sp2010-sp	requestUrl
	Requested by: SP2010\Administrator	destinationUserName
	Size: n/a	fileHash
	Message:	message

Vendor Event ID	Vendor-Specific Event Definition	ArcSight Event Data Field
59	**Import of objects completed**	name
	Occurred: 11/21/2011 1:05:01 AM	receiptTime
	Site: http://sp2010-sp	requestUrl
	Requested by: SP2010\Administrator	destinationUserName
	Total number of items: 7	deviceCustomNumber1
	Message	message
60	**Possible tampering warning**	name
	There may have been potential tampering of %1	fileName
	Details: %2	message
	Message	filePermission
61	**Retention policy processed**	name
	Occurred: 5/28/2011 11:00:26 PM	receiptTime
	Site: https://arcit.sharepoint.xyz.abc.com	requestUrl
	User: System Account	destinationUserName
	Object	
	Type: Document	fileType
	URL: ABC/General Documents on Budget Documents.docx	filePath
	Title: Home	fileName
	Description: n/a	message
	Action: Delete Previous Drafts	deviceAction
62	**File Fragment Written**	name
	Occurred: 5/28/2011 11:00:26 PM	receiptTime
	Site: https://arcit.sharepoint.xyz.abc.com	requestUrl
	User: System Account	destinationUserName
	Object	
	URL: ABC/General Documents on Budget Documents.docx	filePath
	Title: Home	fileName