

Integrate Symantec Data Loss Prevention

EventTracker v8.x and above

Publication Date: April 8, 2019

Abstract

This guide provides instructions to configure Symantec Data Loss Prevention to generate logs for critical events. Once EventTracker is configured to collect and parse these logs, dashboard and reports can be configured to monitor Symantec DLP usage.

Scope

The configurations detailed in this guide are consistent with **EventTracker Enterprise** version 8.x and later, and Symantec DLP.

Audience

IT Admins, Symantec Data Loss Prevention administrators and EventTracker users who wish to forward logs to EventTracker Manager and monitor events using EventTracker Enterprise.

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.

© 2019 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
Scope	1
Audience	1
Overview	3
Prerequisites	3
Configure Symantec DLP Syslog	3
EventTracker Agent LFM Configuration	6
EventTracker Knowledge Pack (KP) Alert	14 14
Reports	14
Dashboards	16
Import Knowledge Pack into EventTracker Category	18 19
Alerts	19
Knowledge Objects	20
Flex Reports	22
Dashlets	23
Verify Knowledge Pack in EventTracker	26
Category	26
Alerts	27
Knowledge Object	28
Flex Reports	28
Dashlets	29



Overview

EventTracker Knowledge pack for Symantec DLP captures important and critical activities in Symantec DLP alerts, Symantec DLP Audit logs, Symantec DLP Access logs and Symantec DLP policy name details. Monitoring these activities is critical from a security aspect and is required for compliance and operational reasons.

The Symantec Data Loss Prevention Enforce Server is the central management platform that enables you to define, deploy, and enforce data loss prevention and security policies. The Enforce Server administration console provides a centralized, web-based interface for deploying detection servers, authoring policies, remediating incidents, and managing the system.

As your data spreads across a wider range of devices and storage environments, the ability to consistently define and enforce policies becomes even more critical. Symantec DLP features a unified management console, the DLP Enforce Platform, and a business intelligence reporting tool, IT Analytics for DLP, which allows you to write policies once and then enforce them everywhere, and measurably reduce information risks.

EventTracker helps you to monitor day to day activities like alerts, user audits, access log and policy violation.

Prerequisites

- EventTracker v8.x or above should be installed.
- EventTracker Agent should be installed on Symantec DLP enforce server system.
- **Symantec DLP** 14.5 or above versions. For all version, we need to customize the syslog format according to policy rule and policy name.

Configure Symantec DLP Syslog

- 1. Logon to the Symantec DLP enforce server.
- 2. Click Manage go to policies and go to Response rules.





3. Creating new response rule by clicking Add Response Rule.





4. Check Automated Response and click next.



Figure 3

- 5. Fill details for Configure Response Rule.
 - i) Rule Name: we can give the Response Rule name as per Policies Names.
 - ii) Description: Description should give overview about Rule Name.
 - iii) Actions: Add Condition as Log to a Syslog Server for Actions.
 - iv) Host: Mention EventTracker installed host IP Address.
 - v) Port: Mention EventTracker syslog port (514) number.
 - vi) Message: Follow below message for logging syslogs.
 - vii) Level: Select 7 debugging form level.



🔇 Symantec Da	ata Loss Prevention Home Incidents - Manage	e 🗸 System 👻
Manage > Polici	es > Response Rules > Configure Response Rule	
Save Cano	e	
General Rule Name	Forward syslogs to EventTracker	
Used in activ	This Rule will Trigger syslog message to EventTracker	
Conditions	;	Add Condition
Actions	og to a Syslog Server 💌	Add Action
All: Log to	a Syslog Server	×
Host:	192.168.10.13	Insert Variable
Port:	514	Application Name Application User Attachment File Name
Message:	ID:\$INCIDENT_ID\$,Policy Rule;\$RULE\$\$,Severity:\$SEVERITY\$,Match count:\$MATCH_COUNT\$,Policy Name:\$POLICY\$,Application Name:\$APPLICATION_UAME\$,Application User Name:\$APPLICATION_USER\$,Attachment File Name:\$ATACHMENT_FILENAME\$,Machine IP:\$MACHINE_IP\$,Destination IP:\$DESTINATION_IP\$,Endpoint User Name:\$ENDPOINT_USERNAME\$,Endpoint Machine:\$ENDPOINT_USERNAME\$,Endpoint Location:\$ENDPOINT_LOCATION\$,Attachment:\$ATTACHMENT _FILENAME\$,Blocked:\$BLOCKED\$,URL:\$URL\$,Protocol:\$PROT OCOL\$,status:\$STATUS\$	Blocked Data Owner Data Owner Email Destination IP Device Instance ID Endpoint Location Endpoint Machine Endpoint Username Incident ID Incident Snapshot Machine IP Match Count Occurred On

Figure 4

Use below log format.

Log Format:

ID:\$INCIDENT_ID\$,PolicyRule:\$RULES\$,Severity:\$SEVERITY\$,Matchcount:\$MATCH_COUNT\$,PolicyName:\$POLICY\$,ApplicationName:\$APPLICATION_NAME\$,ApplicationUserName:\$APPLICATION_USER\$,AttachmentFileName:\$ATTACHMENT_FILENAME\$,MachineIP:\$MACHINE_IP\$,DestinationIP:\$DESTINATION_IP\$,EndpointUserName:\$ENDPOINT_USERNAME\$,EndpointMachine:\$ENDPOINT_MACHINE\$,EndpointLocation:\$ENDPOINT_LOCATION\$,Attachment:\$ATTACHMENT_FILENAME\$,Blocked:\$BLOCKED\$,URL:\$URL\$,Protocol:\$PROTOCOL\$,status:\$STATUS\$

- 6. After configuring response rule click Save.
- 7. **Response Rule** must map with **Policy Rule**. Whenever user violated the **Policy Rule** it will trigger **Response Rule** and **Response Rule** send syslog to EventTracker.



Follow the process given below for mapping **Response Rule** to **Policy Rule**. Same process needs to be followed for other **Policy rules**.

i) Click Manage go to Policies and go to Policy List.



ii) Click any one Policy Rule for mapping Response Rule.

V Sym	intec Data Lo	ss Prevention Home Incidents + Mar	age • System •			ଡ କ ଷ
Manage	 Policies > 6 	Policy List				Admin 💌
Q.	en 💟im	eent (Propi () immediatele	O have O hord X him			Yriw acre
Showin	o 1 to 12 of 12	entries				
	Status 0	Name 0	Description 0	Policy Group 0	Last Modified	0
	0	Cormon Spyware Upload Sites	This policy detects access to common spyware upload websites.	Developers	3.4y 10, 2018 8:06:36 AM IST	/ X 🖯 🖉



iii) After clicking **Policy Rule** go to **Response** and **choose response rule** and select Response Rule.

<u> </u>		1
🕐 Symantec Data	Loss Prevention Home Incidents - Manage - System -	
Manage > Policies	Policy List > Configure Policy	
Save Cancel		
General		
Name	General Data Protection Regulation (Banking and Finance)	
Description	This template focuses on GDPR banking and finance related keyw	
Policy Label	syslog forwarded	
Policy Group	Default Policy Group	
Status	Active [suspend]	
Last Modified	3/26/19 4:15 PM by SIT	
Detection	Groups Response	
<choose< td=""><td>response rule></td><td></td></choose<>	response rule>	
	Figure 7	

iv) Click save.

Note: Repeat same process for mapping Response Rule to all Policy Rules.

EventTracker Agent LFM Configuration

1. Logon to Symantec DLP enforce server host.



2. Navigate to <%EventTracker install directory%>\Prism Microsystems\EventTracker\Agent\.

Name	Date modified	Туре	Size
🔐 ET82UA16-010-log.txt	9/20/2016 3:01 PM	TXT File	1 KB
🔐 ET82UA16-011-log.txt	9/20/2016 3:03 PM	TXT File	1 KB
📔 ET82UA16-012-log.txt	9/20/2016 3:03 PM	TXT File	2 KB
📔 ET82UA16-015-log.txt	9/20/2016 3:06 PM	TXT File	1 KB
📔 ET82UA16-018-log.txt	9/20/2016 3:07 PM	TXT File	2 KB
📔 ET82UA16-020-log.txt	9/20/2016 3:08 PM	TXT File	2 KB
TR2UA16-022-log.txt	9/20/2016 3:09 PM	TXT File	2 KB
😽 etaconfig.exe	9/19/2016 6:59 AM	Application	2,301 KB
etaconfig.exe.manifest	3/1/2016 12:48 AM	MANIFEST File	3 KB
🔄 etaconfig.ini	1/17/2017 12:09 PM	Configuration sett	63 KB
🛐 EtaDataDispatcher.exe	9/6/2016 4:04 PM	Application	793 KB
🚳 etagent.dll	9/17/2016 1:48 AM	Application extens	1,424 KB
📧 etagent.exe	9/8/2016 6:43 AM	Application	447 KB

Figure 8

3. Right-click etaconfig.exe and select Run as administrator.

EventTracker Agent Configuration
File Help
Select Systems
DLP
Apply the following settings to specified Agents
Manager destinations:
192.168.1.14
Log Backup Performance Network Connections Managers Event Filters System Monitor Monitor Processes Services Logfile Monitor File Transfer syslog FTP server Suspicious Activity
Logfile Monitor 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
C:\Symantec_DLP\SymantecDLP\Protect\logs\tomcat\L TEXTLINE
I
Save Close
stringled Litzberg

Figure 9

Symantec DLP audit logs has (.txt) and (.log) file extensions.

Below process is for (.txt) audit logs.

1. Select Logfile Monitor tab and click Add File Name.



e	Enter File name	x
You can configur along with the str	e the complete path of the log file or folder that needs to be monitor ings that need to be searched.	red
🔽 Get All E <u>x</u> ist	ing Log Files	
Select <u>L</u> og File	Type TEXTLINE	•
This is a generic CRLF or CR) in event computer	: text file, where the TEXT value is any separate line (separated by the text file.Provided event source and system name will be reflecte name and event source in the event property.	d as:
Enter File name	e	
		(m)
Event Source		
System Name		
	0K Cancel	

Figure 10

- 2. Select Get All Existing Log Files Checkbox.
- 3. Select Text line from Select Log File Type drop-down.
- 4. Click browse and browse to the earlier selected log file path.
- 5. Click **OK** to continue.

e	Select Folder/File Name	
Select Drive Name:	V	
Select Folder Name:	Show all the files.	
	OK Cancel	

Figure 11

e	Enter File name	x		
You can configu along with the st	re the complete path of the log file or folder that needs to be monitore rings that need to be searched.	ed		
🔽 Get All E <u>x</u> is	sting Log Files			
Select <u>L</u> og File	Type TEXTLINE	•		
This is a generi CRLF or CR) in event computer	This is a generic text file, where the TEXT value is any separate line (separated by CRLF or CR) in the text file. Provided event source and system name will be reflected as event computer name and event source in the event property.			
Enter File nam	Enter File name			
C:\Symantec_E	DLP\SymantecDLP\Protect\logs\tomcat\localhost_access_log*.t>	<u>.</u>		
Event Source	Symantec DLP			
System Name				
	OK Cancel]		



6. Click Add String for adding the Search String.



Search String ×				
Search Strings for : C:\Symantec_DLP\SymantecDLP\Protect\logs\tomcat\localhost_ Use a ' * ' in any column to match every entry in the file				
Column Name	Search String			
Add String	Edit String	Delete String		
	OK	Cancel		

Figure 13

- 7. Select text from Select Field Name.
- 8. Mention * for Enter Search String.
- 9. Check Current Date Time.
- 10. Click **Ok** to Continue.

Enter Search String
You can configure the strings that need to be searched in the selected log file(s). If any record matching the search string is found, an event will be generated.
Select <u>F</u> ield Name:
This is a generic text file, where the TEXT value is any separate line (separated by CRLF or CR) in the text file.
Enter Search String
" You can extend date and time from the parsing file by Decelecting this check boy
Current Date Time
No of Field
Colort Data and Time formationly
Format value
,
OK Cancel

Figure 14

11. Click Ok to Accepting Search String.



Search String			
Search Strings for : C:\Symantec_DLP\SymantecDLP\Protect\logs\tomcat\localhost_ Use a ' * ' in any column to match every entry in the file			
Column Name	Search String		
Text	Text *		
, Add String	Edit String	Delete String	
	ОК	Cancel	



12. Click **Save** from **EventTracker Agent Configuration** for completing LFM configuration for (.txt) audit logs.

4	EventTracker Agent Configuration	
File	Help	
_ Se	elect Systems	
	LP Agent b	ased system
	Apply the following settings to specified Agents	
<u>M</u> an	nager destinations:	
192	2.168.1.14	
_	Log Backup Performance Network C	onnections
м	fanagers Event Filters System Monitor Monitor Process	es Service
L	_ogfile Monitor File Transfer syslog FTP server Sus	picious Activity
F	✓ Loafile Monitor	
e e	Search log files (various formats supported) for matching patterns : here. Both individual files as well as folders can be monitored for m entries. Matches cause an event to be generated	specified natching
S H e	Search log files (various formats supported) for matching patterns : Free. Both individual files as well as folders can be monitored for m entries. Matches cause an event to be generated.	specified hatching File Type
e e	Search log files (various formats supported) for matching patterns : refer. Both individual files as well as folders can be monitored for m entries. Matches cause an event to be generated. Logfile Name C:\Symantec_DLP\SymantecDLP\Protect\logs\tomcat\	specified hatching File Type
e e	Search log files (various formats supported) for matching patterns a nere. Both individual files as well as folders can be monitored for m entries. Matches cause an event to be generated. Logfile Name C:\Symantec_DLP\SymantecDLP\Protect\logs\tomcat\L C:\Symantec_DLP\SymantecDLP\Protect\logs\tomcat\L	specified natching File Type TEXTLINE TEXTLINE TEXTLINE
e e	Search log files (various formats supported) for matching patterns : Search log files (various formats supported) for matching patterns : ener. Both individual files as well as folders can be monitored for matching. Matches cause an event to be generated. Logfile Name Image: C:\Symantec_DLP\SymantecDLP\Protect\logs\tomcat\L Image: C:\Symantec_DLP\SymantecDLP\SymantecDLP\Protect\logs\tomcat\L Image: C:\Symantec_DLP\SymantecDLP\SymantecDLP\Protect\logs\tomcat\L Image: C:\Symantec_DLP\SymantecDLP\Protect\logs\tomcat\L Image: C:\Symantec_DLP\SymantecDLP\Protect\logs\tomcat\L Image: C:\Symantec_DLP\SymantecDLP\Protect\logs\tomcat\L Image: C:\Symantec_DLP\SymantecDLP\Protect\logs\tomcat\L Image: C:\Symantec_DLP\SymantecDLP\Protect\logs\tomcat\L Image: C:\Symantec_DLP\SymantecDLP\Protect\logs\tomcat\L Image: C:\SymantecDLP\SymantecDLP\Protect\logs\tomcat\L Image: C:\SymantecDLP\SymantecDLP\SymantecDLP\SymantecDLP\SymantecDLP\SymantecDLP\S	specified hatching

Figure 16

Below Process is for (.log) audit logs.

1. Select Logfile Monitor tab and click Add File Name.



ę.	Enter File name 🛛 🗙							
You can configure the complete path of the log file or folder that needs to be monitored along with the strings that need to be searched.								
🔽 Get All E <u>x</u> ist	🔽 Get All Existing Log Files							
Select <u>L</u> og File ⁻	Type TEXTLINE							
This is a generic CRLF or CR) in t event computer	text file, where the TEXT value is any separate line (separated by he text file.Provided event source and system name will be reflected as name and event source in the event property.							
Enter File name	,							
Event Source								
System Name								
	OK Cancel							

Figure 17

- 2. Select Get All Existing Log Files Checkbox.
- 3. Select Text line from Select Log File Type drop-down.
- 4. Click browse and browse to the earlier selected log file path.
- 5. Click **OK** to continue.

Select Folder/File Name						
Select Drive Name:	•					
Select Folder Name:	✓ Show all the files. Iocalhost.2018-06-14.log Iocalhost.2018-06-15.log Iocalhost.2018-06-16.log Iocalhost.2018-06-17.log Iocalhost.2018-06-17.log Iocalhost.2018-06-18.log Iocalhost.2018-06-18.log Iocalhost.2018-06-18.log Iocalhost.2018-06-18.log Iocalhost.2018-06-18.log Iocalhost.2018-06-18.log Iocalhost.2018-06-18.log Iocalhost.2018-06-19.log Iocalhost.2018-06-21.log	×				
	OK Cancel					

Figure 18

e	Enter File name	x					
You can configure the complete path of the log file or folder that needs to be monitored along with the strings that need to be searched.							
Get All Existing Log Files							
Select <u>L</u> og File T	ype TEXTLINE	•					
This is a generic text file, where the TEXT value is any separate line (separated by CRLF or CR) in the text file.Provided event source and system name will be reflected as event computer name and event source in the event property.							
Enter File name							
C:\Symantec_DL	_P\SymantecDLP\Protect\logs\tomcat\localhost*.log	<u>.</u>					
Event Source	Symantec DLP						
System Name							
	OK Cancel						

Figure 19



6. Click Add String for adding the Search String.

	Search String	x					
Search Strings for : C:\Symantec_DLP\SymantecDLP\Protect\logs\tomcat\localhost_ Use a '*' in any column to match every entry in the file							
Column Name	Search String						
Add String	Edit String	Delete String					
	OK	Cancel					

Figure 20

- 7. Select text from Select Field Name.
- 8. Mention * for Enter Search String.
- 9. Check Current Date Time.
- 10. Click **OK** to Continue.

Enter Search String							
You can configure the strings that need to be searched in the selected log file(s). If any record matching the search string is found, an event will be generated.							
Select <u>F</u> ield Name: Text This is a generic text file, where the TEXT value is any separate line (separated by CRLF or CR) in the text file.							
Enter Search String * You can select date and time from the parsing file by Deselecting this checkbox. Current DateTime							
No of Fields Date Field Time Field Select Date and Time format value Format value							
OK Cancel							

Figure 21

11. Click OK to Accepting Search String.



Search String							
Search Strings for : C:\Symantec_DLP\SymantecDLP\Protect\logs\tomcat\localhost_ Use a *** in any column to match every entry in the file							
Column Name	Search String						
Text	*						
Add String	Edit String	Delete String					
	ОК	Cancel					



12. Click **Save** from **EventTracker Agent Configuration** for completing LFM configuration for **(.log)** audit logs.

EventTracker Agent Configuration
File Help
Select Systems
DLP Agent based system
Apply the following settings to specified Agents
Manager destinations:
192.168.1.14
Log Backup Performance Network Connections Managers Event Filters System Monitor Monitor Processes Services Logfile Monitor File Transfer syslog FTP server Suspicious Activity
here. Both individual files as well as folders can be monitored 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
U:\Symantec_DLP\SymantecDLP\Protect\logs\tomcat\L TEXTLINE C:\Symantec_DLP\SymantecDLP\Protect\logs\tomcat\L TEXTLINE
Add File Name View File Details Delete File Name Search Strings
Save

Figure 23



EventTracker Knowledge Pack (KP)

Once logs are received in EventTracker; alert, reports and dashboards can be configured in EventTracker.

The following Knowledge Packs are available in EventTracker v9.x and later to support Symantec DLP.

Alert

- Symantec DLP: Audit Changes This alert will trigger whenever policy rule is updated, Policy rule is changed.
- **Symantec DLP: Authentication Failed** This alert will trigger whenever Symantec DLP enforce server user authentication failed, and user not found.
- Symantec DLP: Policy Violations This alert will trigger whenever response rule match with severity is high or severe or critical.

Reports

• Symantec DLP Policy Violation – This report provides information related to what are the user and system violated in the mentioned policy.

LogTime		Policy Name	Policy Rule	Match coun	t Endpoint User Name	Sender IP Address	Destination IP Address	Application Name	Endpoint Name	Endpoint Location
04/02/2019 04:45:33 PM	86813	General Data Protection Regulation (Banking and Finance)	Polish Tax Identification Number	4	CONT\CLARKK	192.168.50.11	null	Mozilla Firefox	CONTOSO12	Off the Corporate Network
04/02/2019 04:45:33 PM	86789	General Data Protection Regulation (Banking and Finance)	Polish Tax Identification Number	4	CONTOUack	192.168.200.122	null	Mozilla Firefox	CONTOSO221	Off the Corporate Network
04/02/2019 04:45:33 PM	86790	General Data Protection Regulation (Banking and Finance)	Hungarian Social Security Number	13	CONT\CLARKK	192.168.200.142	null	Microsoft Internet Explorer	CONTOSO43	Off the Corporate Network
04/02/2019 04:45:33 PM	86804	General Data Protection Regulation (Banking and Finance)	Polish Tax Identification Number	4	CONT\spinch	172.200.90.110	null	Mozilla Firefox	CONTOSO32	Off the Corporate Network
04/02/2019 04:45:33 PM	86806	General Data Protection Regulation (Banking and Finance)	Netherlands Tax Identification Number	12	CONT\MARYJ	172.40.80.110	127.0.0.1	NVIDIA GeForce Experience	CONTOSO10	Off the Corporate Network
04/02/2019 04:45:33 PM	86814	General Data Protection Regulation (Banking and Finance)	Polish Tax Identification Number	4	CONT\CLARKK	192.168.50.21	null	Mozilla Firefox	CONTOSO42	Off the Corporate Network
04/02/2019 04:45:35 PM	86813	General Data Protection Regulation (Banking and Finance)	Polish Tax Identification Number	4	CONT\CLARKK	192.168.50.11	null	Mozilla Firefox	CONTOSO12	Off the Corporate Network
04/02/2019 04:45:35 PM	86814	General Data Protection Regulation (Banking and Finance)	Polish Tax Identification Number	4	CONT\CLARKK	192.168.50.21	null	Mozilla Firefox	CONTOSO42	Off the Corporate Network
04/02/2019 04:45:35 PM	86806	General Data Protection Regulation (Banking and Finance)	Netherlands Tax Identification Number	12	CONT/MARYJ	172.40.80.110	127.0.0.1	NVIDIA GeForce Experience	CONTOSO10	Off the Corporate Network
04/02/2019 04:45:35 PM	86804	General Data Protection Regulation (Banking and Finance)	Polish Tax Identification Number	4	CONT\spinch	172.200.90.110	null	Mozilla Firefox	CONTOSO32	Off the Corporate Network



• Symantec DLP User Login and Logout - This report provides information related to the user login, logout and user authenticated.

LogTime	User Name	Thread ID	Authentication Type	Severity	Status
04/02/2019 04:45:33 PM	clarkk	8145	com.vontu.manager.ui.LogToServ erController	SEVERE	loggedin
04/02/2019 04:45:33 PM	maryj	8145	com.vontu.manager.ui.LogToServ erController	SEVERE	loggedout
04/02/2019 04:45:35 PM	clarkk	8145	com.vontu.manager.ui.LogToServ erController	SEVERE	loggedin
04/02/2019 04:45:35 PM	maryj	8145	com.vontu.manager.ul.LogToServ erController	SEVERE	loggedin

Figure 25



• **Symantec DLP Authentication Failed** - This report provides information related to the authentication failed for user and could not find the user.

LogTime	User Name	Thread ID	Authentication Type	Severity	Status
04/02/2019 04:45:33 PM	123	6974	com.vontu.login.spring.VontuForm AuthenticationProvider	WARNING	Form based authentication failed
04/02/2019 04:45:33 PM	maryj	8148	com.vontu.login.spring.VontuForm AuthenticationProvider	WARNING	Form based authentication failed
04/02/2019 04:45:33 PM	clarkk	8148	com.vontu.login.AuthenticationSer viceBase	SEVERE	Could not find a user with the name
04/02/2019 04:45:33 PM	maryj	8145	com.vontu.login.spring.VontuForm AuthenticationProvider	WARNING	Form based authentication failed
04/02/2019 04:45:33 PM	clarkk	7565	com.vontu.login.spring.VontuForm AuthenticationProvider	WARNING	Form based authentication failed
04/02/2019 04:45:33 PM	maryj	6960	com.vontu.login.AuthenticationSer viceBase	SEVERE	Could not find a user with the name

Figure 26

 Symantec DLP Web Activities - This report provides information related to the accessing (access log) Symantec DLP detail IP address, web request method, and browser details.

LogTime	User IP Address	Web Request Method	Accessed URL	Status Code	Web Browser Details
04/02/2019 04:45:33 PM	172.80.200.110	GET	https://192.168.100.122/ProtectMa nager/Logon	304	Mozilla/5.0 (Windows NT 10.0; WOW64; rv:67.0) Gecko/20100101 Firefox/67.0
04/02/2019 04:45:33 PM	172.80.200.110	GET	https://192.168.100.122/ProtectMa nager/Logon	304	Mozilla/5.0 (Windows NT 10.0; WOW64; rv:67.0) Gecko/20100101 Firefox/67.0
04/02/2019 04:45:34 PM	172.80.200.110	GET	https://192.168.100.122/ProtectMa nager/Logon	304	Mozilla/5.0 (Windows NT 10.0; WOW64; rv:67.0) Gecko/20100101 Firefox/67.0
04/02/2019 04:45:34 PM	172.80.200.110	GET	https://192.168.100.122/ProtectMa nager/Logon	304	Mozilla/5.0 (Windows NT 10.0; WOW64; rv:67.0) Gecko/20100101 Firefox/67.0
04/02/2019 04:45:34 PM	172.80.200.110	GET	https://192.168.100.122/ProtectMa nager/Logon	304	Mozilla/5.0 (Windows NT 10.0; WOW64; rv:67.0) Gecko/20100101 Firefox/67.0



• Symantec DLP Audit Activities – This report provides information related to policy changed, policy updated.

LogTime	User Name	Thread ID	Authentication Type	Severity	Policy Name	Activity	
04/02/2019 04:45:33 PM	clarkk	4604	com.vontu.manager	INFO		POLICY_UPDATE	
04/02/2019 04:45:33 PM	clarkk	80	com.vontu.manager.mail.ReportMail er	INFO		Scheduled report sent	
04/02/2019 04:45:33 PM	clarkk	80	com.vontu.manager.report.saved.s chedule.job.ScheduledReportJob	INFO		Running scheduled report	
04/02/2019 04:45:33 PM	clarkk	80	com.vontu.manager.mail.ReportMail er	INFO		Scheduled report sent	
04/02/2019 04:45:33 PM	Maryj	80	com.vontu.manager.report.saved.s chedule.job.ScheduledReportJob	INFO		Running scheduled report	
04/02/2019 04:45:33 PM	clarkk	4604	com.vontu.manager	INFO		POLICY_UPDATE	
04/02/2019 04:45:33 PM	clarkk	4604	com.vontu.manager	INFO	Network Security policy	Policy changed	
04/02/2019 04:45:33 PM	maryj	80	com.vontu.manager.mail.ReportMail er	INFO		Scheduled report sent	
04/02/2019 04:45:33 PM	clarkk	80	com.vontu.manager.report.saved.s chedule.job.ScheduledReportJob	INFO		Running scheduled report	
04/02/2019 04:45:33 PM	clarkk	80	com.vontu.manager.mail.ReportMail er	INFO		Scheduled report sent	





Dashboards

• Symantec DLP Audit Activity – This dashboard shows information about policy updated, policy changed, and Schedule report sent by the user.





 Top System Violated DLP Policies – This dashboard shows information about which host, or user violated DLP policies.





• Symantec DLP Web Activities – This dashboard shows information about what are the IP Address accessed by Symantec DLP portal, web request methods, URL and web browser detail.





• Symantec DLP User Login and Logout – This dashboard shows information about which user is authenticated, login and logout.





• Symantec DLP Authentication Failed – This dashboard shows information for which user authentication failed and user could not find.





Figure 33

Import Knowledge Pack into EventTracker

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



Figure 34

3. Import Tokens/Flex Reports as given below.



Category

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

🖢 Expo	rt Import Utility				-		×
Export	Import						
1. Pro 2. Clic	ovide the path and file name ok the Import button.	ne of the Categori	es file. Use the '' button to bro	wse and locate the import file			
Opti	ons	Location					
•	Category						
OF	liters						
0/	Verts						
0 9	Systems and Groups		Source : *.iscat				
01	Token Value						
OF	Reports						
0	Behavior Correlation						
					mport	Clos	e



- 2. Locate Category_Symantec DLP.iscat file, and then click the open button.
- 3. To import category, click the Import button.
 - EventTracker displays success message.





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

Alerts

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

Netsurion EventTracker

ort Import		
. Provide the path and file na . Click the Import button.	me of the Alerts file. Use the '' button	to browse and locate the import file.
Options	Location	
Category		
Filters	✓ Import E-mail settings	
Alerts	Set Active	
Systems and Groups	 Only if notifications set By default 	This setting is applicable only for imports from Legacy (v6k) Alert files. For v7, the active status will be set based on "Active" key available in the configuration section.
RSS Feeds	- · ·	socion.
Reports	Source :	
	*.isalt	
Behavior Rules		
SCAP		
🔿 Token Value		

Figure 37

- 2. Locate Alerts_Symantec DLP.isalt file, and then click the Open button.
- 3. To import alerts, click the **Import** button. EventTracker displays success message.

Export Imp	port Utility Σ	3
1	Selected alert configurations are imported successfully.	
	ОК	



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

Knowledge Objects

- 1. Click Knowledge objects under Admin option in the EventTracker manager page.
- 2. Locate the file named KO_Symantec DLP.etko.



Import		×
KD_Symantec DLP.etko 📨 Browse	Upload	
		a 1
		Close

Figure 39

3. Now select all the check box and then click \blacksquare 'Import' option.

Import		×
Selec	t file	🚝 Browse Upload
\checkmark	Object name	Applies to Group name
\checkmark	Symantec DLP Audit Changes	Symantec DLP
\checkmark	Symantec DLP Authentication Failed	Symantec DLP
\checkmark	Symantec DLP Policy Violation	Symantec DLP
\checkmark	Symantec DLP User Login Logout	Symantec DLP
Ŋ	Symantec DLP Web Activities	Symantec DLP Import Close



4. Knowledge objects are now imported successfully.



File imported successfully.	
ОК	

Figure 41

Flex Reports

1. Click **Reports** option and select new (.etcrx) from the option.

💺 Export Import Utility	_		\times
Export Import			
Import	t	Clo	se



2. Locate the file named Reports_Symantec DLP.etcrx and select all the check box.



{]} I	Reports Import X								
Ma	Nato (Kanada) and in the fact in a dama data and an an disand an an								
Note : in reportion contrains tempore, inst import tempore and proceed with report import process.									
Se	Select file E\PRODUCT\Symantec DLP\Symantec DLP KP items\Reports_Symantec DLP.etcx Select file								
Av	Available reports								
Tit	le		Frequency Show all	- <i>Q Q</i>					
		Title	Sites	Groups	Systems	Frequency			
	EDIT	Symantec DLP - Audit Changes	NTPLDTBLR46	Default	Symantec DLP	Undefined			
	EDIT	Symantec DLP - Authentication Failed	NTPLDTBLR46	Default	Symantec DLP	Undefined			
	<u>EDIT</u>	Symantec DLP - Policy violation	NTPLDTBLR46	Default	Symantec DLP	Undefined			
	EDIT	Symantec DLP - User Login Logout	NTPLDTBLR46	Default	Symantec DLP	Undefined			
	EDIT	Symantec DLP - Web Activities	NTPLDTBLR46	Default	Symantec DLP	Undefined			
٢									
	Note: Set	run time option is not applicable for Defined	Reports and Hourly Reports						
	Set run t	time for report(s) from	M • at interval of minute	es Set ()					
	Replace	to	Rep	lace Assign systems					
				Note: Make sure that Site(s)), Group(s) and System(s) selections are va	id. 📕 🗵			

Figure 43

3. Click the **Import** button to import the reports. EventTracker displays success message.





Dashlets

In EventTracker 9.0, we have added new feature which will help to import/export of dashlet. Following is the procedure to do that:

1. Login into EventTracker Enterprise Web console.



	EventTracker 🕀					
1	Username					
	Password					
		Login				
log	8,333,946 logs processed since install on Dec 30, 2017					
35,002 logs processed today						
Co	ntact Us	FAQ	Help			

Figure 45

2. Go to My Dashboard option.

Dashboard
Behavior Correlation
Compliance
My Dashboard
Home
Incidents
Threats
Q Search
Reports

Figure 46



3. Click import button and select .etwd File.





4. Click upload and select Dashboard which you want to import.



👂 Import dashlets - Mozilla Firefox	-]	Х
() localhost:8080/EventTracker/Flex/ImportWidget.aspx	•••	⊌	☆	≡
Import				^
Note: If dashlet configured using persisted report, first import the report and proceed wi dashlet.	th imp	ortin	9	
🚔 Brow	vse	U	pload	
Available widgets				
Select All				
🗹 Top System Violated DLP P 🗹 Symantec DLP Web Activiti 🗹 Symantec DLF	User	Login	L	
Symantec DLP Authenticati 🗹 Symantec DLP Audit Change				
	Impo	rt	Close	·]

Figure 49

5. Click Import button. It will upload all selected dashboards.

Verify Knowledge Pack in EventTracker

Category

- 1. Logon to EventTracker Enterprise.
- 2. Click the Admin menu, and then click Category.

≡	Event Tracker ⊕				📣 🖌 Admin 🗸	Tools -
	Home		Active Watch Lists	Event Filters	😥 Parsing Rules	
Q		_	Alerts	Eventvault	Report Settings	_
	0	0	Behavior Correlation Rules	FAQ Tile Configuration	Systems	
<u>~</u>			🗞 Behavior Correlation Settings	Group Management	Q Users	
	Potential Cyber Breaches Unsafe connections or processes, new TCP ent	Indicators of Co USB activities, New	Casebook Configuration	Q IP Lookup Configuration	🕀 Weights	orting Syste
			● Category	· . Knowledge Objects	Windows Agent Config	_
	Attacker		Diagnostics	🔯 Manager		

Figure 50

3. Click the search, and then search with Symantec DLP.



Category			
Category Tree	bearch		
Symantec DLP		Q	Q
Category			
Symantec DLP Au	dit Activit	ies	
Symantec DLP Au	thenticati	on Failed	
Symantec DLP Po	licy Violat	ion	
✓ Symantec DLP Use	er Login a	nd Logou	ıt
Symantec DLP We	b Activiti	es	

Figure 51

1. Logon to EventTracker Enterprise.

Alerts

2. Click the Admin menu, and then click Alerts.

≡	Event Tracker ⊕					🔎 🛛 Admin-	Tools 🕶
	Home		Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dasht
٩			Alerts	Correlation	Q IP Lookup Configuration	Q Users	_
	0	2	Behavior Correlation Rule	s 🛕 Diagnostics	· Knowledge Objects	T Weights	
~			🇞 Behavior Correlation Sett	ngs 🧔 Event Filters	Manager	Windows Agent Config	
	Potential Cyber Breaches Indicators of Co Unsafe connections or processes, new TCP entry point USB activities. New ser		Casebook Configuration	Eventvault	😥 Parsing Rules		
			● Category	FAQ Configuration	Report Settings		
	Attacker			- News			



3. In the **Search** box, type **'Symantec DLP'**, and then click the **Go** button. Alert Management page will display all the imported alerts.

Alerts								🕈 / Admin / Alerts
Show All						Search by	Alert name 🗸	Symantec DLP Q Q
134	39			134	System User	31	134	Critical 15 Low 15 74 Serious 19
Available Alerts Total number of alerts available	Active Alerts Total number of active alerts			System/User Count for syste	Defined Alert: m and user defin	5 ied alerts	Alerts by Count of a	Threat Level lerts by threat level
Activate Now Click 'Activate No	w' after making all changes							Total: 2 Page Size 25 V
Alert Name A	Threat	Active	E-mail	Forward as SNMP	Forward as Syslog	Remedial Action at Console	Remedial Action at Agent	Applies To
🗌 양청 Symantec DLP: Audit Changes	•							14.5 above
다 않 Symantec DLP: Authnetication Failed	•							14.5 above



4. To activate the imported alerts, select the respective checkbox in the Active column.



EventTracker displays message box.





5. Click **OK**, and then click the **Activate Now** button.

NOTE: Specify appropriate **systems** in **alert configuration** for better performance.

Knowledge Object

- 1. Logon to EventTracker Enterprise.
- 2. Click the Admin menu, and then click Knowledge Object.
- In Knowledge Object Group Tree to view imported knowledge object, scroll down and click Symantec
 DLP group folder.

Knowledge Object are displayed in the pane.

Knowledge Objects			🟫 / Admin / Knowledge Objects
Symantec DLP Q. Q.	Activate Now		Objects 🔶 ፒ 🏦
Groups 🕑 Ø 📋			Î
Symantec DLP Audit Cha Symantec DLP Authentic Symantec DLP Policy Viol Symantec DLP User Logi Symantec DLP Web Activi		Select Object from the left panel.	

Figure 55

Flex Reports

- 1. Logon to EventTracker Enterprise.
- 2. Click the Reports menu, and then Configuration.
- 3. Select **Defined** in report type.
- 4. In **Report Groups Tree** to view imported Scheduled Reports, scroll down and click **Symantec DLP** group folder.



Reports are displayed in the Reports configuration pane.

Report Configuration 🔶 / Reports / Reports / Report Configuration / Defined														
O Sched	O Scheduled O Queued							Symantec DLP		Q	Q	Ċ	1	
Report Groups 🕀 🎬 Reports configuration: Symantec DLP												_		
🔁 se	🕀 Security ^			÷	⊕ III ∂,							Total:	5	
🔁 o	🔁 Compliance					Title		Created on	Modified on					
€ 3 o	perations				£3	Symantec DLP - Web Activities		Mar 29 02:56:49 PM	Mar 29 03:32:23 PM		i	5	+	
🔁 FI	🔁 Flex		🗆 🄅	£\$3	Symantec DLP - Audit Changes		Mar 29 01:01:26 PM	Mar 29 01:10:26 PM		(j	5	+		
	II Compliance Repor	Ē	0		2	Symantec DLP - User Login Logout		Mar 29 11:35:04 AM	Mar 29 11:46:22 AM		i	5	+	
D AI	rubaOS	Ē	0		£3	Symantec DLP - Authentication Failed		Mar 29 11:24:20 AM	Mar 29 11:46:33 AM		(j)	5	+	
В	omgar	Ē	0			233	Symantec DLP - Policy violation		Mar 27 02:25:44 PM	Mar 29 11:46:56 AM		Û	5	(F)
	🔁 Dell Equallogic 📋 🧭		0		\mathcal{M}	-,				0	6			
F 1	all Units	前	CAR.	-										

Figure 56

Dashlets

- 1. Logon to EventTracker Enterprise.
- 2. Click the Dashboard menu, and then My Dashboard.
- 3. Then click **Customize Dashlet** button (a) and search for **"Symantec DLP"**

Customize dashlets			×
Symantec			Q
Symantec DLP Audit Changes	Symantec DLP Authentication F	Symantec DLP User Login Logout	Symantec DLP Web Activities
			Add Delete Close

Figure 57

