

Integrate Symantec Endpoint Protection EventTracker Enterprise

Publication Date: Sept. 7, 2016

EventTracker
8815 Centre Park Drive
Columbia MD 21045
www.eventtracker.com

About this Guide

This guide will facilitate a **Symantec Endpoint Protection** user to send syslog logs to **EventTracker Enterprise**.

Scope

The configurations detailed in this guide are consistent with **EventTracker Enterprise 7.x or later, Symantec Endpoint Protection 12.1.6**.

Note: The integration steps mentioned the “**Configuration**” section are only for 12.1.4 and 12.1.6. Hence to know the integration steps for 10.0 and later version, please contact the EventTracker support (support@eventtracker.com).

Audience

Administrators who want to monitor **Symantec Endpoint Protection** using EventTracker Enterprise.

The information contained in this document represents the current view of Prism Microsystems Inc. on the issues discussed as of the date of publication. Because Prism Microsystems must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Prism Microsystems, and Prism Microsystems cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. Prism Microsystems MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from Prism, as long as its content is unaltered, nothing is added to the content and credit to Prism is provided.

Prism Microsystems may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Prism Microsystems, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

© 2016 Prism Microsystems Corporation. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Table of Contents

- About this Guide 1
 - Scope..... 1
 - Audience..... 1
- Introduction 3
- Prerequisites..... 3
- Configuration 3
- Importing Symantec Endpoint Protection knowledge pack into EventTracker 14
 - Category 15
 - Alerts..... 17
 - Flex Reports..... 18
 - Templates 19
- Verifying Symantec Endpoint Protection knowledge pack in EventTracker 20
 - Categories 20
 - Alerts..... 21
 - Reports..... 23
 - Template 23
- Create Flex Dashboards in EventTracker 24
 - Schedule Reports..... 24
 - Create Dashlets..... 27
- Sample Dashboards..... 30

Introduction

EventTracker support for Symantec's Antivirus and IDS/IPS events is now available. Symantec's security policy will consist of specific rules enabled with logging used to capture and send to EventTracker. These events will be auto-identified, if enabled, and parsed into the EventTracker report tables for later review.

Prerequisites

Prior to configuring Symantec Endpoint Protection and EventTracker, ensure that you meet the following prerequisites:

- Symantec Endpoint Protection 12.1.6 is installed and configured.
- Administrative user on Symantec Endpoint Protection Server.
- EventTracker v7.0 or later should be installed.
- Administrative access on EventTracker.

Configuration

You must enable and configure Syslog on Symantec Endpoint Protection prior to configuring EventTracker.

To specify events log settings:

1. To login to **Symantec Endpoint Protection Manager** Console in manager machine, select the **Start** button, select **All Programs**, and then select **Symantec Endpoint Protection Manager**.



Figure 1

Login page of Symantec Endpoint Protection Manager Console displays.

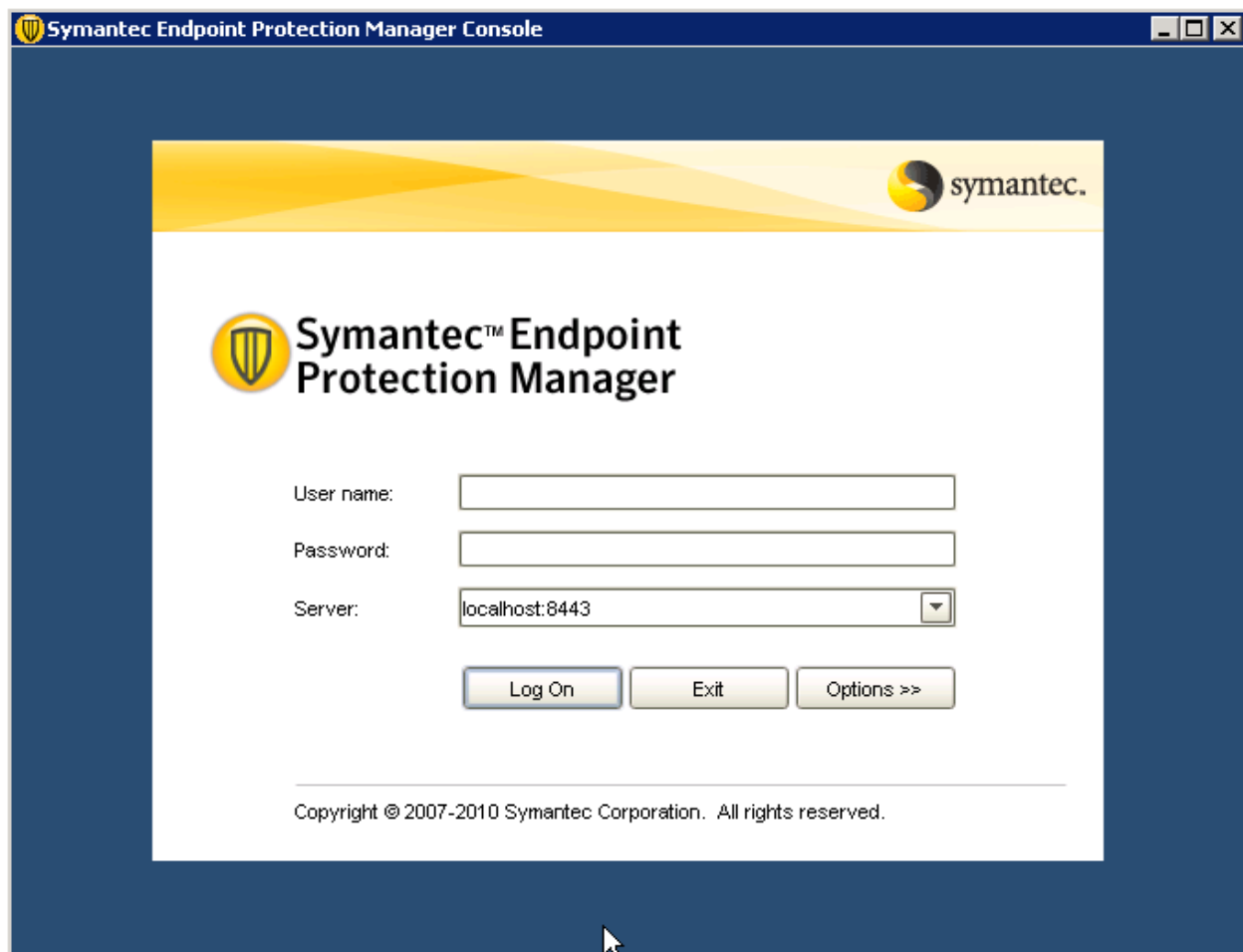


Figure 2

2. Enter valid **User name:** and **Password:** and then click the **Log On** button.
Symantec Endpoint Protection Manager displays.
3. In left pane, select **Admin**, select **Servers** node, and then select respective site node.

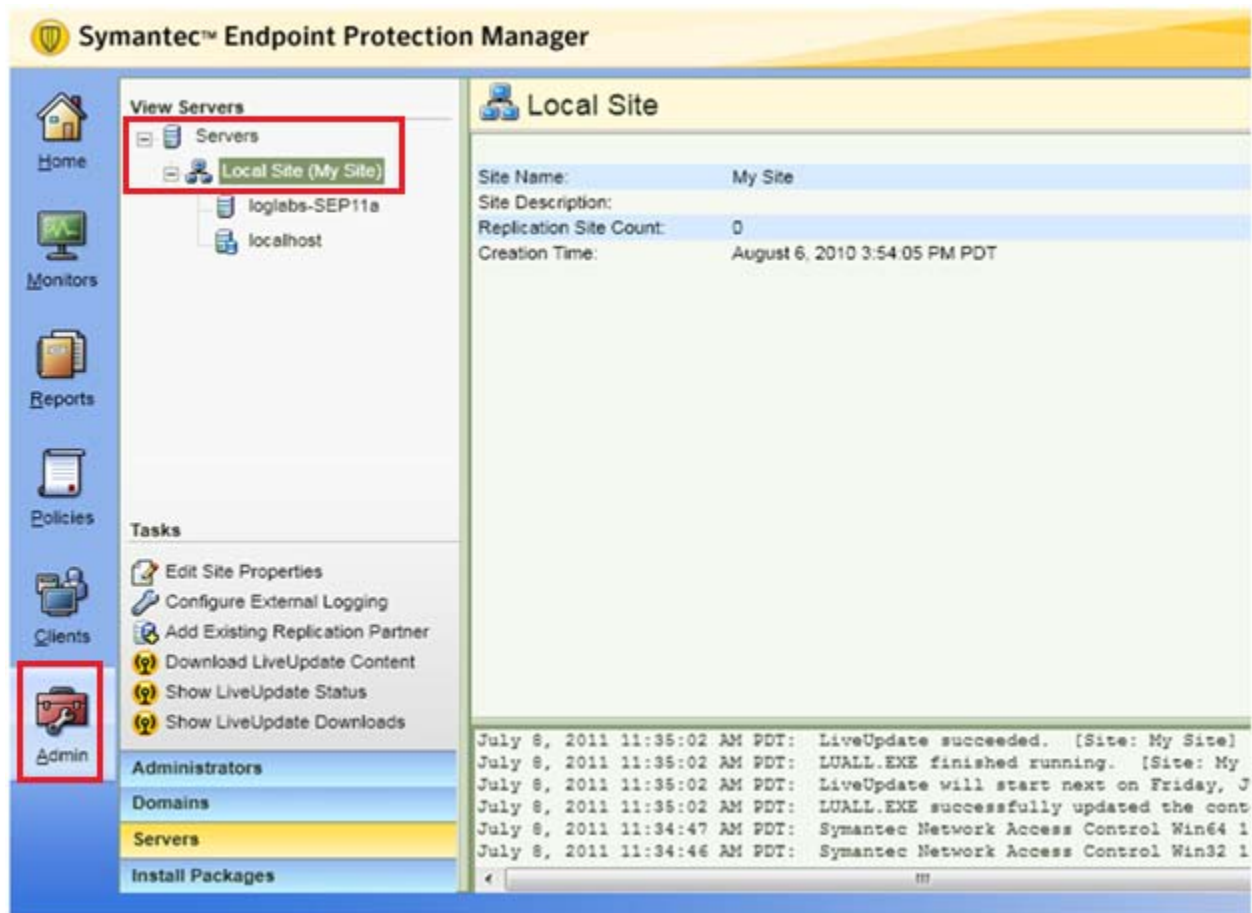


Figure 3

4. In **Tasks** pane, select **Servers**, and then select **Configure External Logging**.

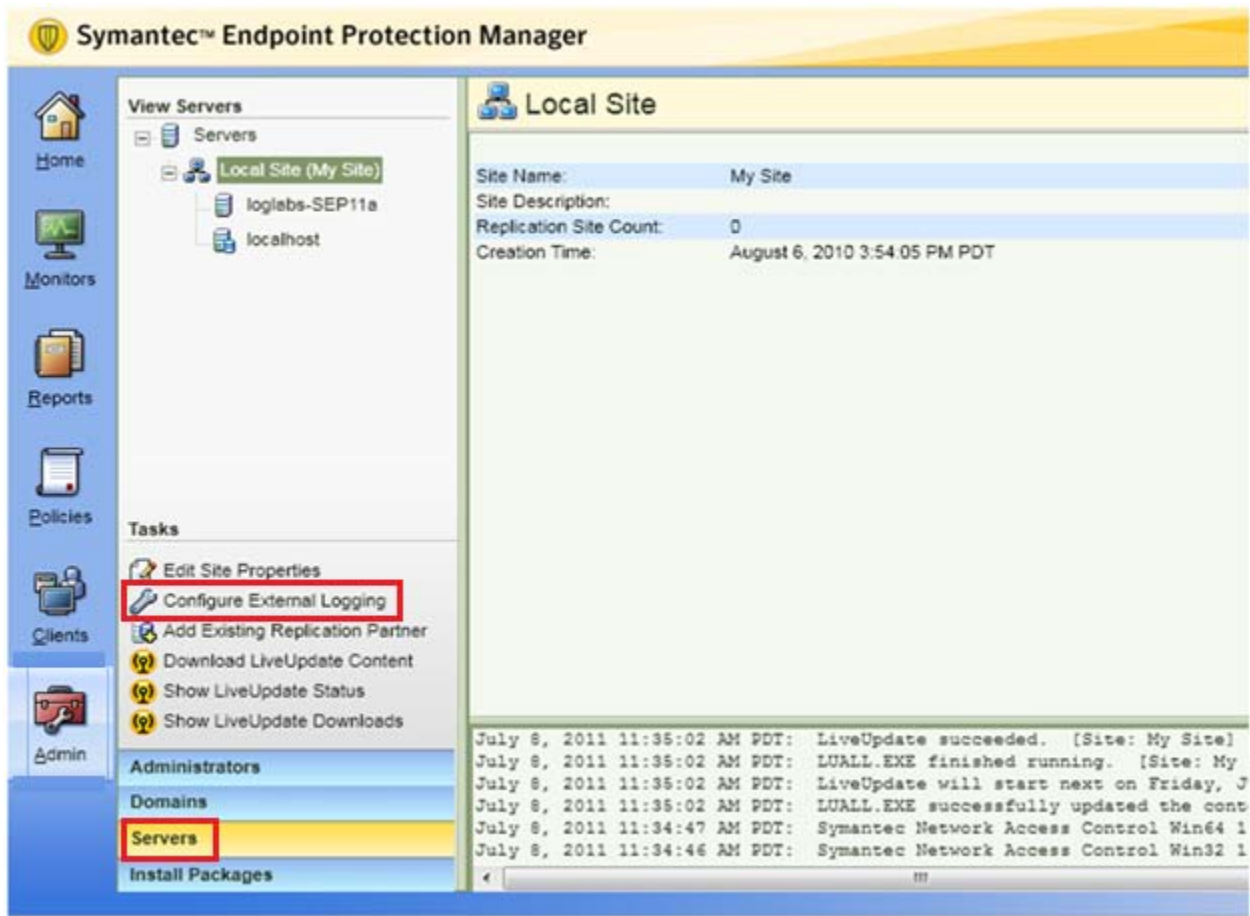


Figure 4

External Logging for Local Site window displays.

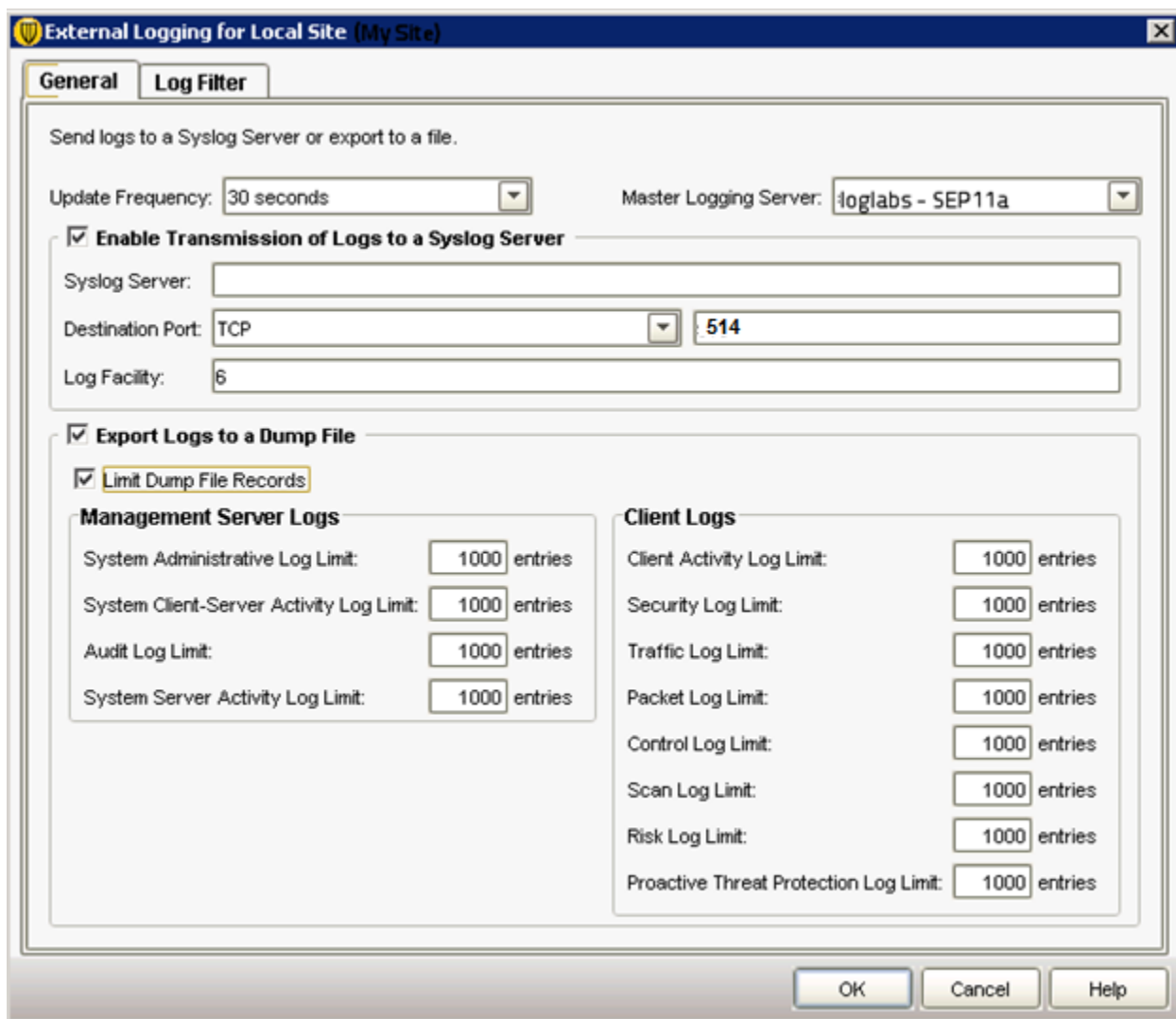


Figure 5

5. Click **Enable Transmission of Logs to a Syslog Server** option.
6. Enter EventTracker IP address.
7. Click **Export Logs to a Dump File** option, and then click **Limit Dump File Records** option.
8. Enter the required limit entries.
9. Click **Log Filter** tab; check the required log types that have to be sent to EventTracker.

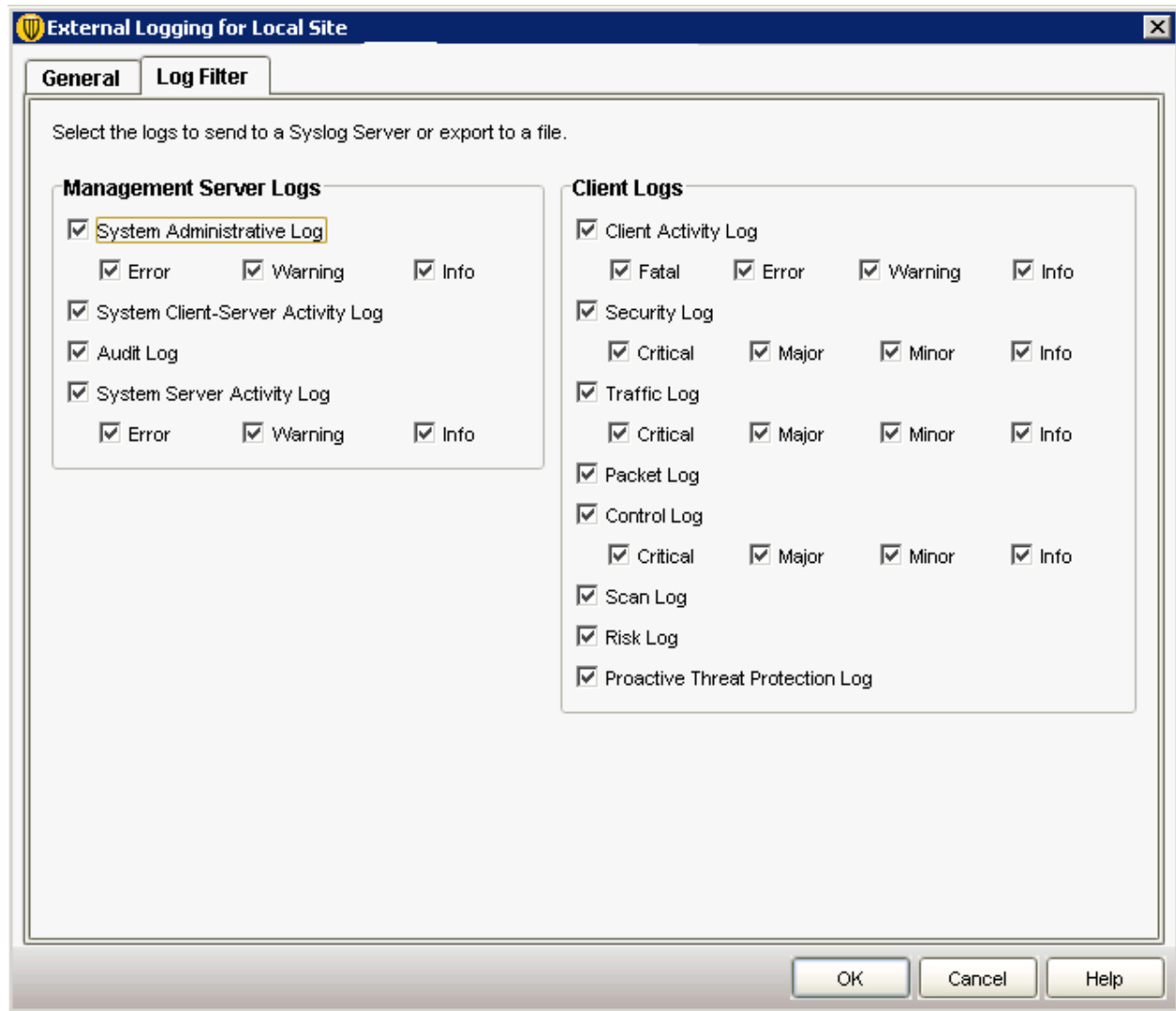


Figure 6

EventTracker Knowledge Pack

Once Symantec endpoint Protection events are enabled and Symantec endpoint Protection events are received in EventTracker, Alerts and Reports can be configured in EventTracker.

The following Knowledge Packs are available in EventTracker to support Symantec endpoint Protection monitoring.

Categories

- **SEP: Administrator account locked** - This category provides information related to administrator account locked.
- **SEP: Administrator account unlocked** - This category provides information related to administrator account unlocked.
- **SEP: Administrator logon failed** - This category provides information related to administrator logon failed.
- **SEP: Administrator logon success** - This category provides information related to administrator logon success.
- **SEP: Administrator property changed** - This category provides information related to administrator property changed.
- **SEP: Administrator password changed** - This category provides information related to administrator password changed.
- **SEP: Administrator renamed** - This category provides information related to administrator renamed.
- **SEP: Auto protect disabled** - This category provides information related to auto protect disabled.
- **SEP: Auto protect enabled** - This category provides information related to auto protect enabled.
- **SEP: Backup restore error** - This category provides information related to backup restore error.
- **SEP: Checksum error** - This category provides information related to checksum error.
- **SEP: Web attack blocked** - This category provides information related to web attack blocked.
- **SEP: Whitelist failure** - This category provides information related to whitelist failure.
- **SEP: Virus detected** - This category provides information related to virus detected.
- **SEP: Auto protect disabled** - This category provides information related to auto protect disabled.
- **SEP: User created** - This category provides information related to user created.
- **SEP: User deleted** - This category provides information related to user deleted.
- **SEP: Threat whitelisted** - This category provides information related to threat whitelisted.
- **SEP: Service shutdown** - This category provides information related to service shutdown.
- **SEP: Security risk found** - This category provides information related to security risk found.
- **SEP: Remediation action failed** - This category provides information related to remediation action failed.
- **SEP: Remediation action pending** - This category provides information related to remediation action pending.

- **SEP: Remediation action successful** - This category provides information related to remediation action successful.
- **SEP: RDP allowed** - This category provides information related to RDP allowed.
- **SEP: No update found** - This category provides information related to no update found.
- **SEP: Live update started** - This category provides information related to live update started.
- **SEP: New virus definition file loaded** - This category provides information related new virus definition file loaded.
- **SEP: Intrusion prevention disabled** - This category provides information related to intrusion prevention disabled.
- **SEP: Intrusion prevention enabled** - This category provides information related to intrusion prevention enabled.
- **SEP: Configuration changed** - This category provides information related to configuration changed.
- **SEP: Scan aborted** - This category provides information related to scan aborted.
- **SEP: Scan completed** - This category provides information related to scan completed.
- **SEP: Scan delayed** - This category provides information related to scan delayed.
- **SEP: Scan restarted** - This category provides information related to scan restarted.
- **SEP: Scan stopped** - This category provides information related to scan stopped.
- **SEP: Domain deleted** - This category provides information related to user domain deleted.
- **SEP: Domain disabled** - This category provides information related to domain disabled.

Alerts

- **SEP: Live update started**

This alert is generated when live update have been started.

- **SEP: No update found**

This alert is generated when no updates are to be found.

- **SEP: Remediation action failed**

This alert is generated when remediation action fails.

- **SEP: Remediation action pending**

This alert is generated when remediation action is pending.

- **SEP: Scan stopped**

This alert is generated when scan is stopped.

- **SEP: Security risk found**

This alert is generated when security risk is found.

- **SEP: Administrator account locked**

This alert is generated when administrator account has been locked.

- **SEP: Administrator logon failed**

This alert is generated when administrator has failed to logon.

- **SEP: Administrator password changed**

This alert is generated when administrator changes the password.

- **SEP: Administrator property changed**

This alert is generated when administrator changes the property.

- **SEP: Auto protect disabled**

This alert is generated when auto protect is disabled.

- **SEP: Intrusion prevention disabled**

This alert is generated when intrusion prevention is disabled.

- **SEP: Domain disabled**

This alert is generated when domain is disabled.

- **SEP: Service shutdown**

This alert is generated when service is shutdown.

- **SEP: Virus detected**

This alert is generated when virus is detected.

- **SEP: Whitelist failure**

This alert is generated when whitelist fails.

- **SEP: Web attack blocked**

This alert is generated when web attack is blocked.

Reports

- **SEP-Agent created and deleted**

This report is generated when a new agent or client machine has been added or deleted.

- **SEP-Application blocked**

This report is generated when an application has been blocked.

- **SEP-Auto-protect disabled**

This report is generated when an auto protect was disabled.

- **SEP-Device disabled**

This report is generated when the device has been disabled.

- **SEP-Intrusion prevention disabled**

This report is generated when intrusion prevention has been disabled.

- **SEP-Security risk detected**

This report is generated when a security risk has been detected.

- **SEP-Virus detected**

This report has been generated when a virus has been detected in the system.

- **SEP-Web attack blocked**

This report has been generated when a web attack has been blocked.

- **SEP-Virus deletion failed**

This report has been generated when a virus has been detected and SEP tries to delete it but fails to delete.

- **SEP-At Risk Computers**

This report has been generated when a computer has been detected as a risk.

- **SEP-New Risks Detected in the Network**

This report has been generated when a risk has been detected in a network.

- **SEP-TruScan Proactive Threat Detection Over Time**

This report has been generated when a threat has been detected over a period amount of time during a scan.

- **SEP-TruScan Proactive Threat Distribution**

This report has been generated when a threat has been distributed during a scan.

- **SEP-Detected Risks Not Confirmed**

This report has been generated when a risk has been detected but it has not been confirmed as a risk.

- **SEP-Confirmed Risks**

This report has been generated when a risk has been detected and has been confirmed as a risk.

- **SEP-Permitted Applications**

This report has been generated when an application has been given permission.

Importing Symantec Endpoint Protection knowledge pack into EventTracker

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

Import


1. **Templates**
2. **Category**
3. **Alerts**
4. **Parsing rules**
5. **Flex Reports**

NOTE: Importing should be in the same order as mentioned above.



Figure 28

Category

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

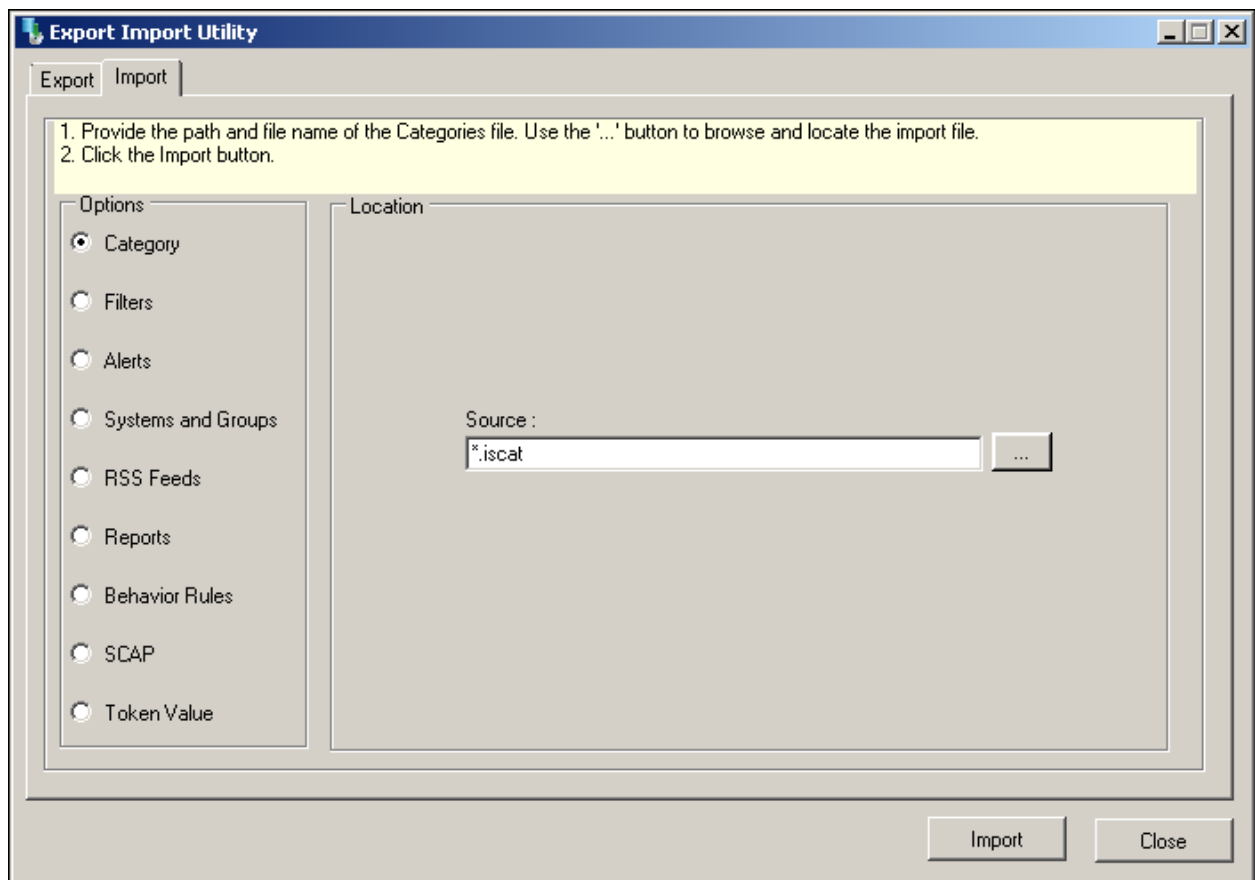


Figure 29

2. Locate **All Symantec Endpoint Protection Categories.iscat** file, and then click the **Open** button.
3. To import categories, click the **Import** button.

EventTracker displays success message.

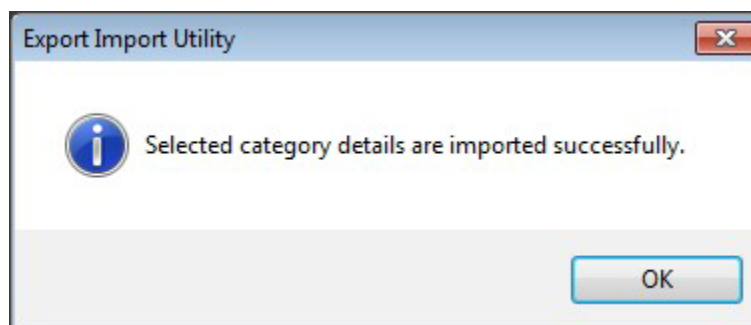



Figure 30

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

Alerts

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

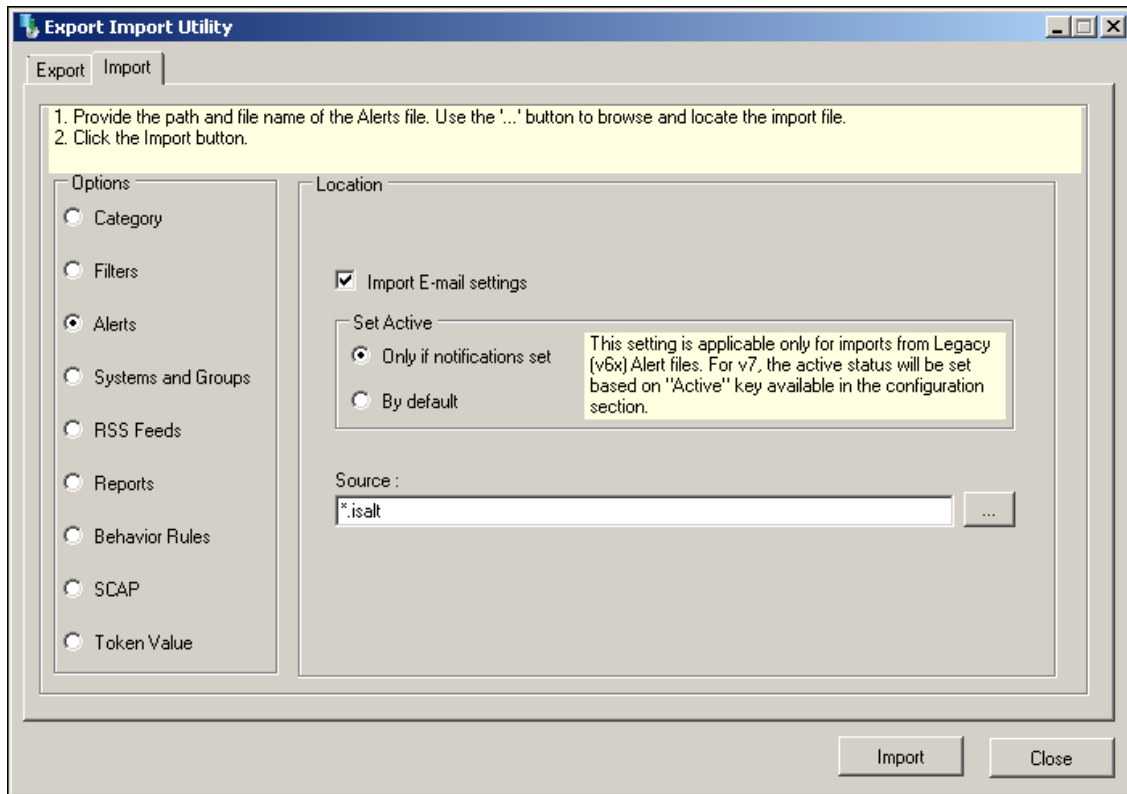


Figure 31

2. Locate **All Symantec Endpoint Protection Alerts.isalt** file, and then click the **Open** button.
3. To import alerts, click the **Import** button.

EventTracker displays success message.

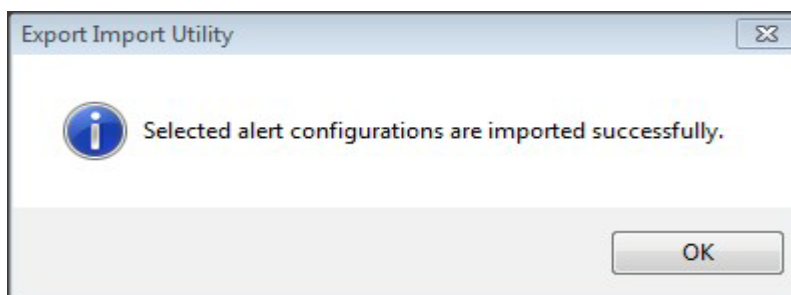


Figure 32

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

Flex Reports

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

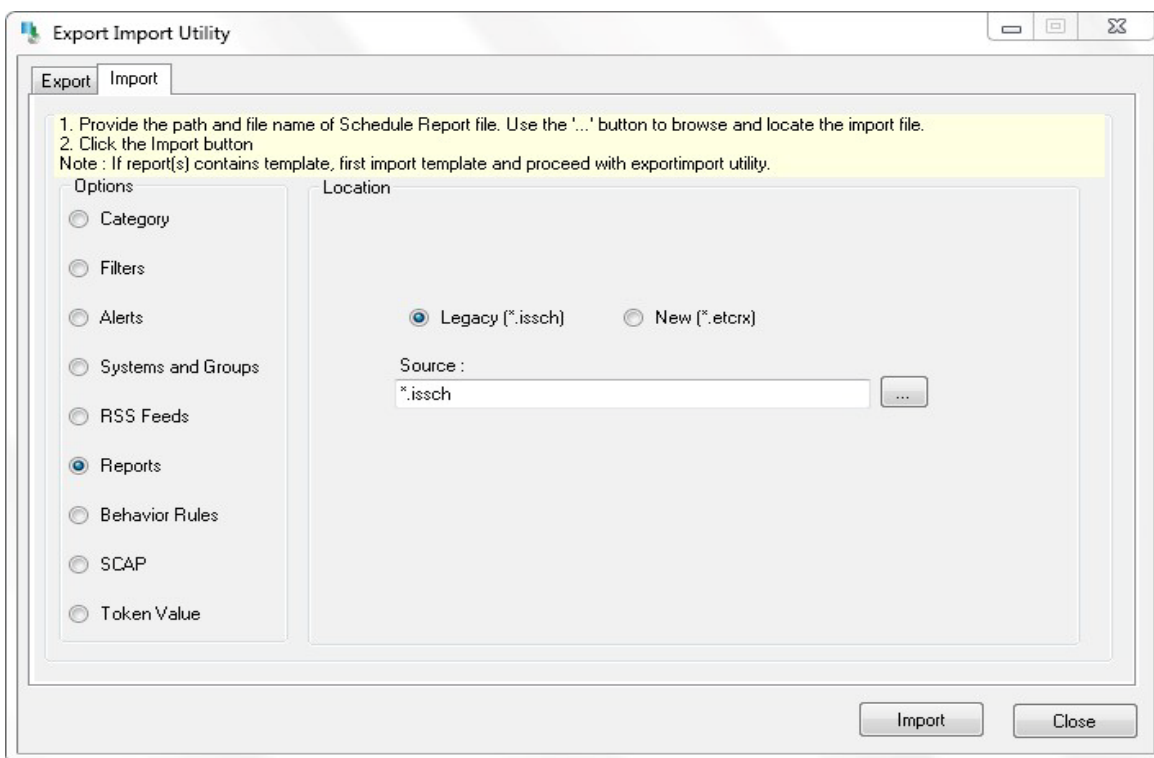


Figure 35

2. Locate **All Symantec Endpoint Protection Report.issch** file, and then click the **Open** button.
3. To import scheduled reports, click the **Import** button.

EventTracker displays success message.

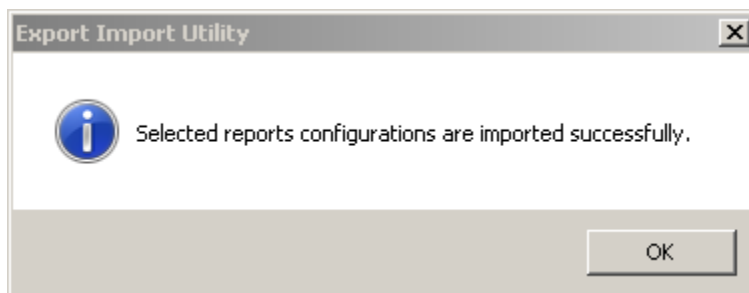



Figure 36

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

Templates

1. Click the **Admin** menu, and then click **Parsing rule**.
2. Select **Template** tab, and then click on  'Import' option.

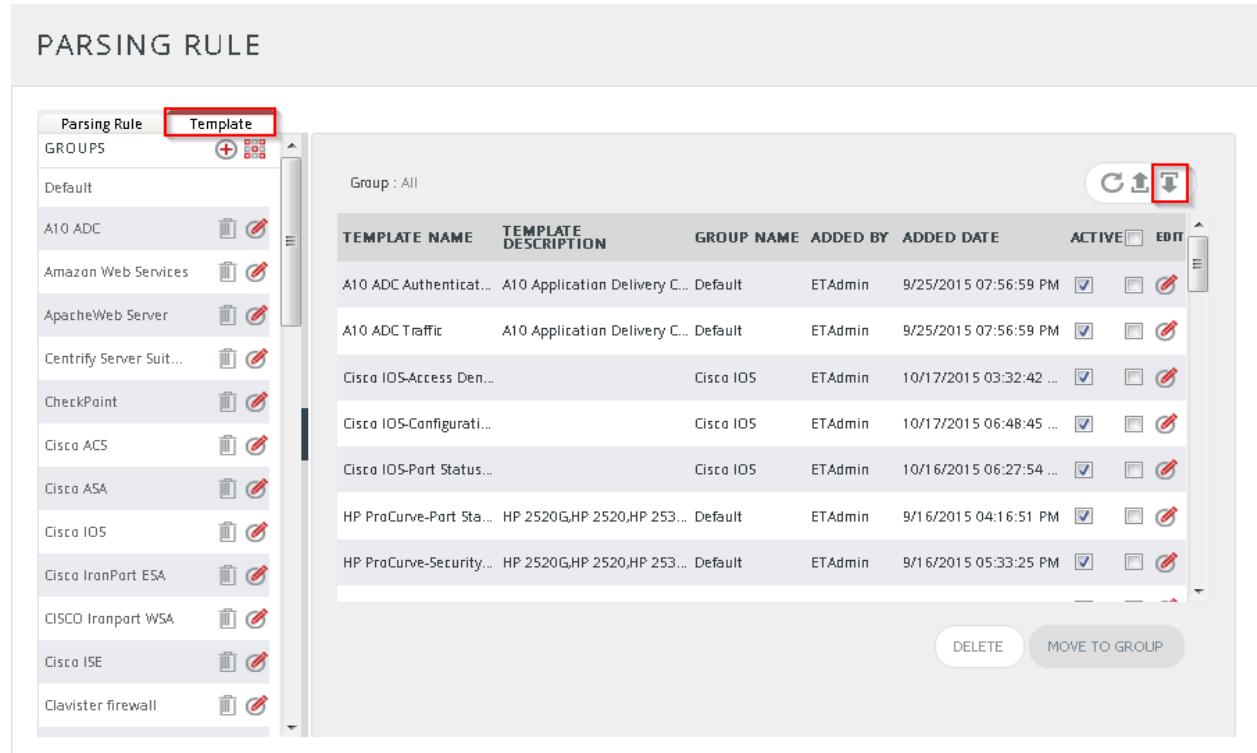


Figure 37

3. Click on **Browse** button.

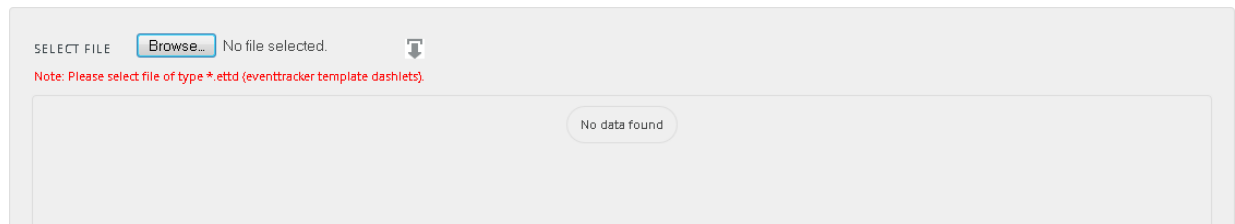


Figure 38

4. Locate **All Symantec Endpoint Protection Template.ettd** file, and then click the **Open** button

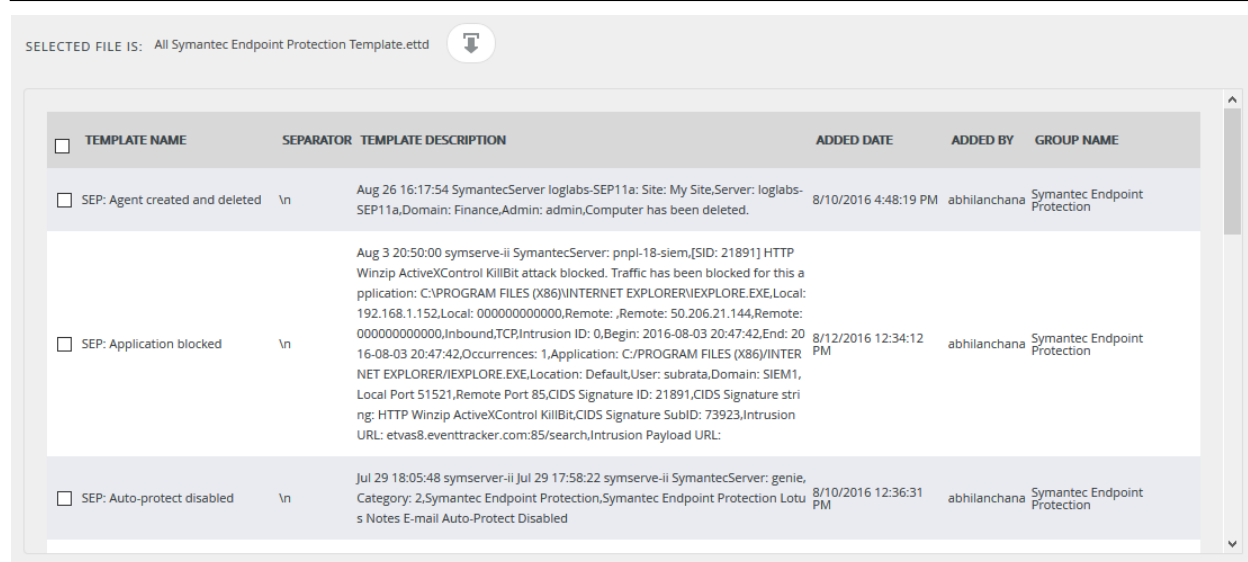



Figure 39

- Now select the check box and then click on  'Import' option. EventTracker displays success message.

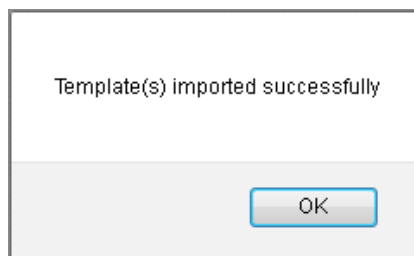


Figure 40

- Click on **OK** button.

Verifying Symantec Endpoint Protection knowledge pack in EventTracker Categories

- Logon to **EventTracker Enterprise, Web interface**.
- Click the **Admin** menu, and then click **Categories**.
- In **Category Tree** to view imported categories, scroll down and expand **Symantec Endpoint Protection** group folder to view the imported categories.

CATEGORY MANAGEMENT

Category Tree Search

Total category groups: 354 Total categories: 3,122

Last 10 modified categories

NAME	MODIFIED DATE	MODIFIED BY
SEP: Administrator account unlocked	8/16/2016 5:58:16 PM	ETAdmin
SEP: Virus detected	8/16/2016 4:49:28 PM	ETAdmin
SEP: Application blocked	8/16/2016 3:36:57 PM	ETAdmin
SEP: Administrator account locked	8/12/2016 5:09:57 PM	ETAdmin
SEP: Administrator log on failed	8/12/2016 5:09:57 PM	ETAdmin
SEP: Administrator log on success	8/12/2016 5:09:57 PM	ETAdmin
SEP: Administrator password changed	8/12/2016 5:09:57 PM	ETAdmin
SEP: Administrator property changed	8/12/2016 5:09:57 PM	ETAdmin
SEP: Administrator renamed	8/12/2016 5:09:57 PM	ETAdmin
SEP: All events	8/12/2016 5:09:57 PM	ETAdmin

Figure 41

Alerts

1. Logon to **EventTracker Enterprise** web interface.
2. Click the **Admin** menu, and then click **Alerts**.
3. In **Search** field, type '**SEP**', and then click the **Go** button.

Alert Management page will display all the imported **Symantec Endpoint Protection** alerts.

ALERT MANAGEMENT Search by Alert name

Click 'Activate Now' after making all changes Total: 20 Page Size 25

<input type="checkbox"/>	ALERT NAME ^	THREAT	ACTIVE	E-MAIL	MESSAGE	RSS	FORWARD AS SNMP	FORWARD AS SYSLOG	REMEDIAL ACTION AT CONSOLE	REMEDIAL ACTION AT AGENT	APPLIES TO
<input type="checkbox"/>	SEP: Administrator account locked	☐ Serious	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Symantec Endpoi...
<input type="checkbox"/>	SEP: Administrator log on failed	☐ Serious	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Symantec Endpoi...
<input type="checkbox"/>	SEP: Administrator password changed	☐ Serious	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Symantec Endpoi...
<input type="checkbox"/>	SEP: Administrator property changed	☐ Serious	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Symantec Endpoi...
<input type="checkbox"/>	SEP: Application blocked	☐ High	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Symantec Endpoi...
<input type="checkbox"/>	SEP: Auto protect disabled	☐ Serious	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Symantec Endpoi...
<input type="checkbox"/>	SEP: Device disable	☐ High	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Symantec Endpoi...
<input type="checkbox"/>	SEP: Domain disabled	☐ Critical	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Symantec Endpoi...
<input type="checkbox"/>	SEP: Intrusion prevention disabled	☐ Serious	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Symantec Endpoi...
<input type="checkbox"/>	SEP: Live update started	☐ Serious	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Symantec Endpoi...

Figure 42

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

EventTracker displays message box.



Figure 43

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

NOTE:

You can select alert notification such as Beep, Email, and Message etc. For this, select the respective checkbox in the Alert management page, and then click the **Activate Now** button.

Reports

1. Logon to **EventTracker Enterprise**.
2. Click the **Reports** menu, and then select **Configuration**.
3. In **Reports Configuration** pane, select **Defined** option.
EventTracker displays **Defined** page.
4. In search box enter **SEP**, and then click the **Search** button.
EventTracker displays Flex reports of **Symantec Endpoint Protection**.

The screenshot shows the 'REPORTS CONFIGURATION' page for 'SYMANTEC ENDPOINT PROTECTION'. At the top, there are radio buttons for 'Scheduled', 'Queued', and 'Defined' (which is selected). A search bar contains the text 'SEP'. Below the search bar, there are two main sections: 'REPORT GROUPS' on the left and 'REPORTS CONFIGURATION : SYMANTEC ENDPOINT PROTECTION' on the right. The 'REPORTS CONFIGURATION' section shows a table of reports with columns for 'TITLE', 'CREATED ON', and 'MODIFIED ON'. A red box highlights the following reports in the table:

TITLE	CREATED ON	MODIFIED ON
SEP-At Risk Computers	11/5/2013 3:34:45 PM	8/31/2016 3:07:59 PM
SEP-New Risks Detected in the Network	11/5/2013 2:25:29 PM	8/31/2016 3:07:42 PM
SEP-TruScan Proactive Threat Detection Over Time	10/31/2013 6:23:45 PM	8/31/2016 3:08:25 PM
SEP-TruScan Proactive Threat Distribution	10/31/2013 6:10:27 PM	8/31/2016 3:09:22 PM
SEP-Detected Risks Not Confirmed	10/31/2013 6:03:21 PM	8/31/2016 3:25:55 PM
SEP-Confirmed Risks	10/31/2013 5:19:48 PM	8/31/2016 3:26:27 PM
SEP-Permitted Applications	10/31/2013 4:14:56 PM	8/31/2016 3:26:57 PM

Figure 45

Template

1. Logon to **EventTracker Enterprise** web interface.
2. Click the **Admin** menu, and then click **Parsing Rules** and click **Template**.

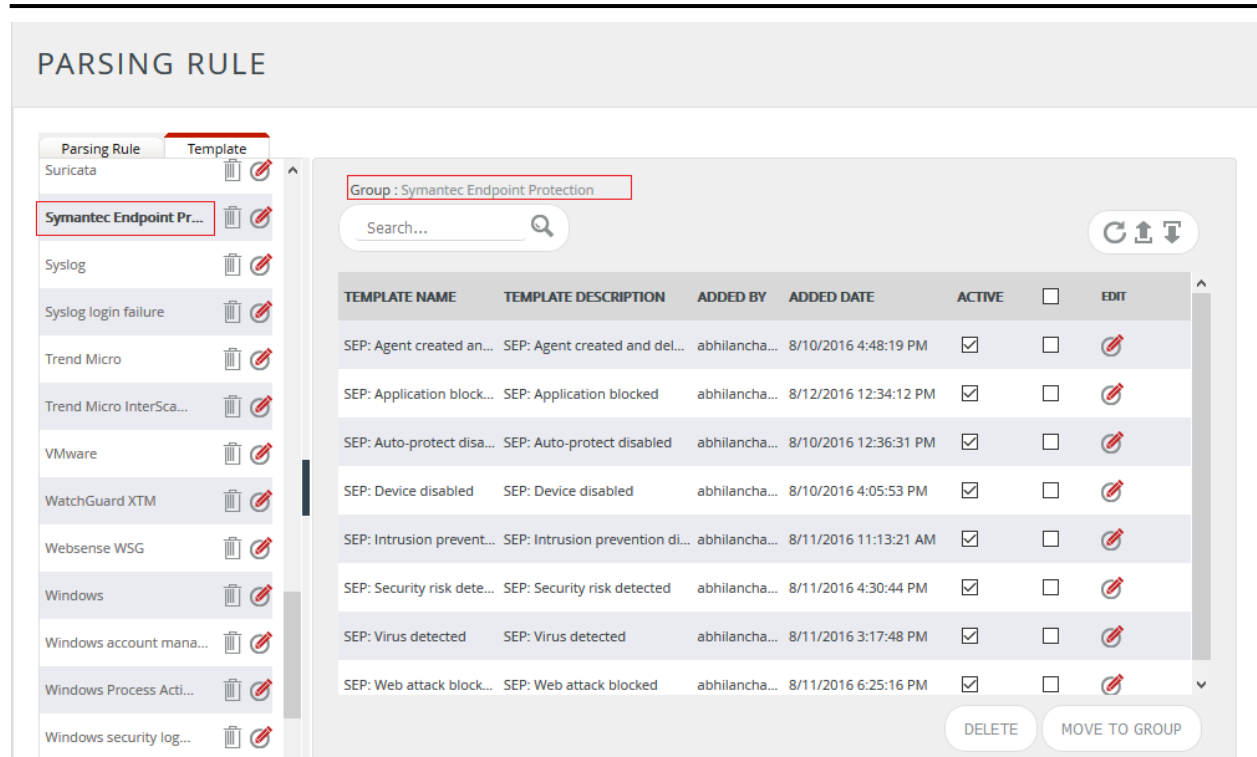


Figure 46

Create Flex Dashboards in EventTracker

NOTE: To configure the flex dashboards schedule and generate the reports. Flex dashboard feature is available from EventTracker Enterprise v8.0 and later.

Schedule Reports

1. Open **EventTracker** in browser and logon.

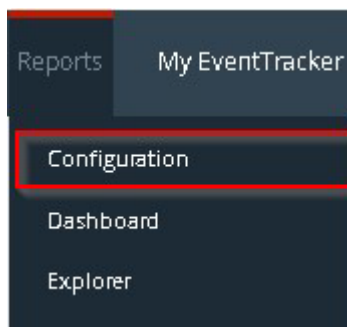





Figure 47

2. Navigate to **Reports>Configuration**.

REPORTS CONFIGURATION

Scheduled Queued Defined

Search   

REPORT GROUPS

- Suricata
- Symantec EndPoint Pr...**
- Syslog
- syslog login failure
- Teradata Database
- Trend Micro
- Trend Micro InterSca...
- Vipre Antivirus
- VMware
- WatchGuard XTM
- Websense WSG

REPORTS CONFIGURATION : SYMANTEC ENDPOINT PROTECTION

Total: 17






























<input type="checkbox"/>	TITLE	CREATED ON	MODIFIED ON	
<input type="checkbox"/>	 SEP-At Risk Computers	11/5/2013 3:34:45 PM	8/31/2016 3:07:59 PM	  
<input type="checkbox"/>	 SEP-New Risks Detected in the Network	11/5/2013 2:25:29 PM	8/31/2016 3:07:42 PM	  
<input type="checkbox"/>	 SEP-TruScan Proactive Threat Detection Over Time	10/31/2013 6:23:45 PM	8/31/2016 3:08:25 PM	  
<input type="checkbox"/>	 SEP-TruScan Proactive Threat Distribution	10/31/2013 6:10:27 PM	8/31/2016 3:09:22 PM	  
<input type="checkbox"/>	 SEP-Detected Risks Not Confirmed	10/31/2013 6:03:21 PM	8/31/2016 3:25:55 PM	  
<input type="checkbox"/>	 SEP-Confirmed Risks	10/31/2013 5:19:48 PM	8/31/2016 3:26:27 PM	  
<input type="checkbox"/>	 SEP-Permitted Applications	10/31/2013 4:14:56 PM	8/31/2016 3:26:57 PM	  

Figure 48

3. Select **Symantec Endpoint Protection** in report groups. Check **defined** dialog box.
4. Click on 'schedule'  to plan a report for later execution.

REPORT WIZARD

TITLE: SEP- APPLICATION BLOCKED

LOGS

CANCEL < BACK NEXT >

Review cost details and configure the publishing options. Step 8 of 10

DISK COST ANALYSIS

Estimated time for completion: 00:00:42(HH:MM:SS)
Number of cab(s) to be processed: 6
Available disk space: 235 GB
Required disk space: 50 MB

Enable publishing option (Configure SMTP Server in manager configuration screen to use this option)
 Deliver results via E-mail
 Notify results via E-mail

To E-mail: [Use comma(,) to separate multiple e-mail recipients]

Update status via RSS: ▼

Show in: ▼

Persist data in Eventvault Explorer

Figure 49

REPORT WIZARD

TITLE: SEP- APPLICATION BLOCKED

DATA PERSIST DETAIL

CANCEL < BACK NEXT >

Select columns to persist Step 9 of 10

RETENTION SETTING

Retention period: days ⓘ

Persist in database only [Reports will not be published and will only be stored in the respective database]

SELECT COLUMNS TO PERSIST

COLUMN NAME	PERSIST
Client System Name	<input checked="" type="checkbox"/>
User Name	<input checked="" type="checkbox"/>
Local Address	<input checked="" type="checkbox"/>
Local Port	<input checked="" type="checkbox"/>
Remote Address	<input checked="" type="checkbox"/>
Remote Port	<input checked="" type="checkbox"/>

Figure 50

5. Check column names to persist using **PERSIST** checkboxes beside them. Choose suitable **Retention period**.
6. Proceed to next step and click **Schedule** button.
7. Wait till the reports get generated.

Create Dashlets

1. Open **EventTracker** in browser and logon.

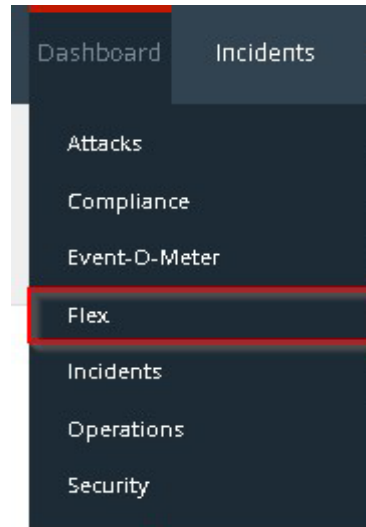


Figure 51

3. Navigate to **Dashboard>Flex**.
Flex Dashboard pane is shown.


FLEX DASHBOARD

Title
Symantec Endpoint Protection

Description
Symantec Endpoint Protection

SAVE DELETE CANCEL

Figure 52

4. Fill suitable title and description and click **Save** button.
5. Click  to configure a new flex dashlet. Widget configuration pane is shown.

WIDGET CONFIGURATION

WIDGET TITLE: SEP-Device disabled

NOTE: [Empty]

DATA SOURCE: SEP-Device disabled

CHART TYPE: Donut

DURATION: 1 Week

VALUE FIELD SETTING: COUNT

AS OF: Recent

AXIS LABELS [X-AXIS]: Device Name

LABEL TEXT: [Empty]

VALUES [Y-AXIS]: Select column

VALUE TEXT: [Empty]

FILTER: Domain Name

FILTER VALUES: Select column

LEGEND [SERIES]: Select column

SELECT: All

TEST CONFIGURE CLOSE

Figure 53

6. Locate earlier scheduled report in **Data Source** dropdown.
7. Select **Chart Type** from dropdown.
8. Select extent of data to be displayed in **Duration** dropdown.
9. Select computation type in **Value Field Setting** dropdown.
10. Select evaluation duration in **As Of** dropdown.
11. Select comparable values in **X Axis** with suitable label.
12. Select numeric values in **Y Axis** with suitable label.
13. Select comparable sequence in **Legend**.
14. Click **Test** button to evaluate. Evaluated chart is shown.

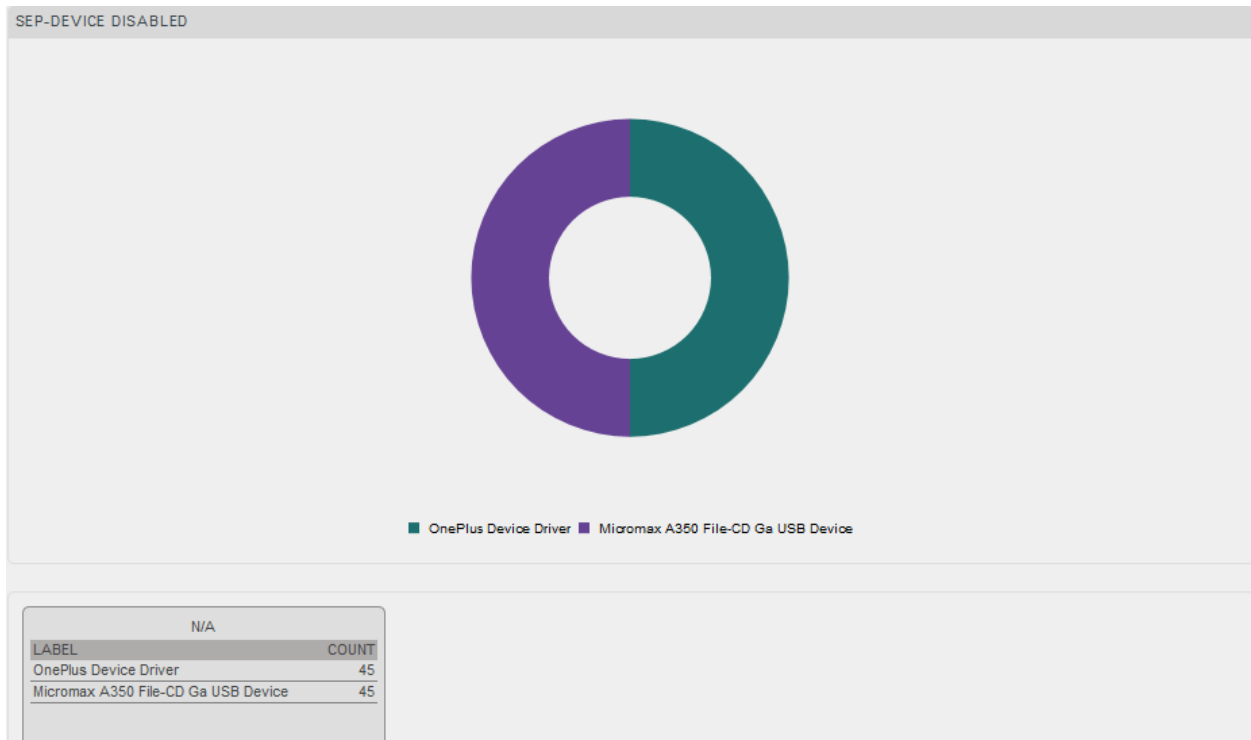


Figure 54

2. If satisfied, click **Configure** button

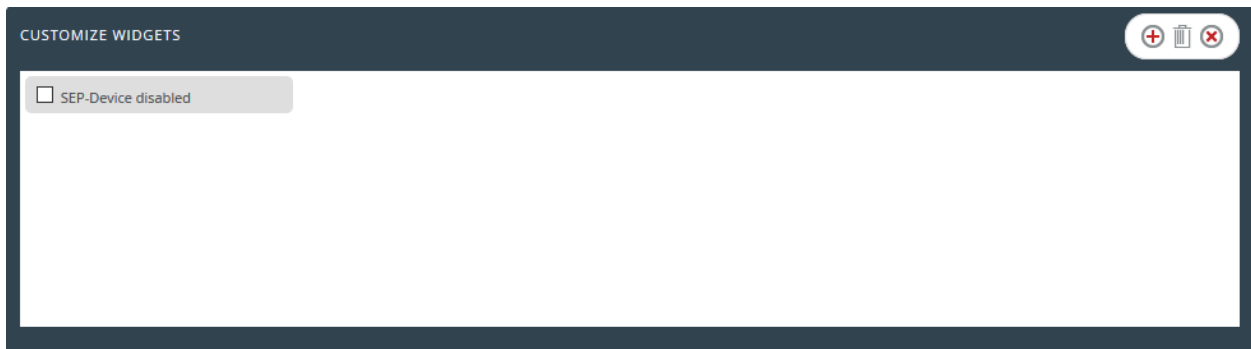




Figure 55

3. Click 'customize'  to locate and choose created dashlet.
4. Click  to add dashlet to earlier created dashboard.

Sample Dashboards

For below dashboard **DATA SOURCE: SEP-Device disabled**

- **WIDGET TITLE:** SEP-Device disabled
CHART TYPE: Donut
AXIS LABELS [X-AXIS]: Device Name
FILTER: Domain name

1. SEP-Device disabled

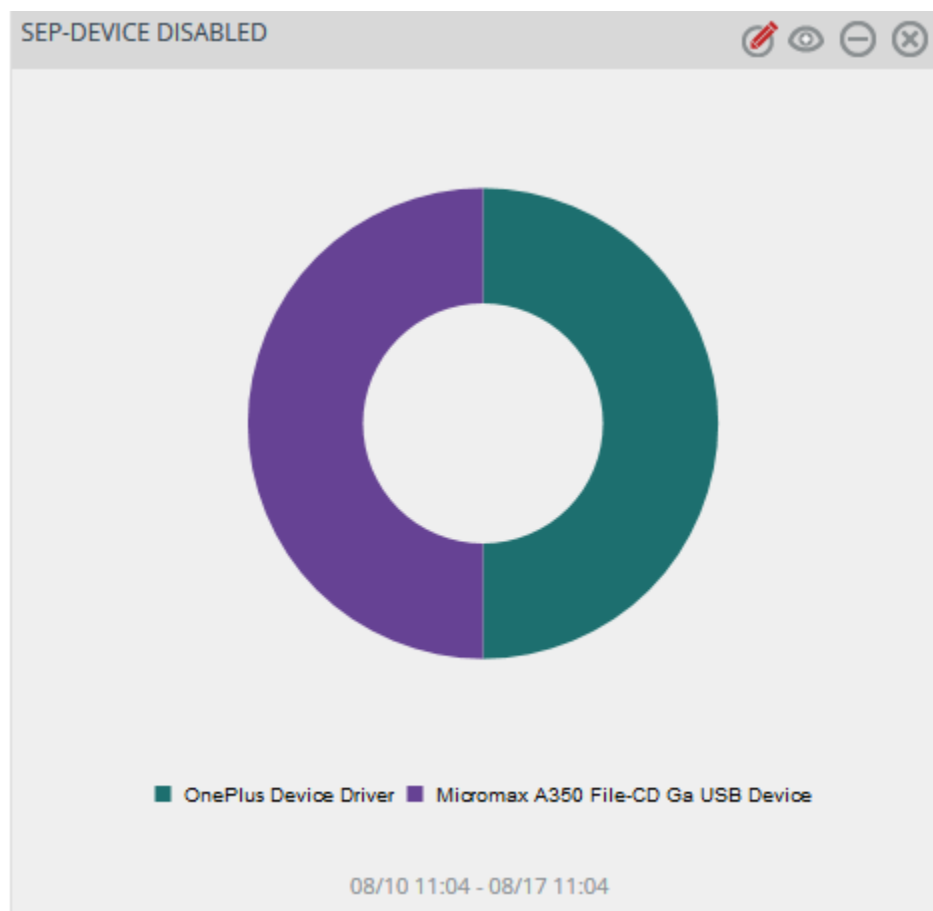


Figure 56