

Integrate Sophos Email Appliance

EventTracker v8.x and above

Abstract

This guide provides instructions to configure a **Sophos Email Appliance** to send its syslog to EventTracker Enterprise

Scope

The configurations detailed in this guide are consistent with EventTracker Enterprise version v8.x or above and Sophos Email Appliance v 4.2.x.x.

Audience

Administrators who are assigned the task to monitor Sophos Email Appliance events using EventTracker.

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

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

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

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

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

© 2017 EventTracker Security LLC. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Table of Contents

Abstract	1
Scope	1
Audience	1
Overview	3
Prerequisites	3
Integration of Sophos Email Appliance with EventTracker manager	3
Configuring Log Delivery	3
EventTracker Knowledge Pack.....	4
Flex Reports	4
Categories	6
Knowledge Objects.....	6
Import Sophos Email Appliance knowledge pack into EventTracker	7
Category	7
Token Templates	8
Knowledge Objects.....	9
Flex Reports	10
Verify Sophos Email Appliance knowledge pack in EventTracker	13
Categories	13
Token Template.....	14
Knowledge Objects.....	15
Flex Reports	16
Create Dashlets.....	17
Sample Flex Dashboards	21

Overview

Sophos Email Appliance is an appliance for filtering email. It provides tools for routing incoming and outgoing mail, configuring policies for email processing, monitoring mail flow, and allowing end-user access to message quarantine.

EventTracker helps to monitor events from Sophos Email Appliance. It's knowledge object and flex reports will help you to analyse mail traffic, admin activities and to monitor policy or configuration changes.

Prerequisites

- EventTracker v8.x or above should be installed.
- Sophos Email Appliance should be configured for forwarding logs.

Integration of Sophos Email Appliance with EventTracker manager

Configuring Log Delivery

To configure a Sophos Email Appliance to forward logs to a syslog server,

- Logon to Sophos Email Appliance
- Use the **Configuration > System > Alerts & Monitoring** page to do the following:
- Select the Enable Syslog check box.
- In the **Hostname/IP** text box, enter the IP address of the **EventTracker**.
- In the **Port** text box, enter the port number **514**.
- Select a Protocol option button to select whether the appliance will send syslog data using **UDP**.
- Select the check box next to each log:
 1. System status log
 2. Message policy log
 3. Mail transfer agent log

EventTracker Knowledge Pack

Once logs are received by EventTracker manager, knowledge packs can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker Enterprise to support Sophos Email Appliance.

Flex Reports

- **Sophos Email Appliance-Configuration changes** – This report gives the information about configurations changed by the users.

LogTime	Computer	Source IP Address	User Name	Object Name	Old Value	New Value
12/11/2017 04:59:13 PM	SOPHOUS_EA	192.0.2.96	admin	proxy_enabled	0	1
12/11/2017 04:59:13 PM	SOPHOUS_EA	192.0.2.96	admin	Rule_config	0	1
12/11/2017 04:59:13 PM	SOPHOUS_EA2	192.0.2.96	admin	proxy_enabled	0	1
12/11/2017 04:59:13 PM	SOPHOUS_EA3	192.0.2.96	admin	Rule_config	0	1
12/11/2017 04:59:13 PM	SOPHOUS_EA4	192.0.2.96	admin	proxy_enabled	1	0
12/11/2017 04:59:13 PM	SOPHOUS_EA2	192.0.2.96	admin	Rule_config	0	1

Figure 1

Logs Considered

12/18/2017 4:19:33 PM [3333](#) NTPPLDTBLR38 / [Sophou...](#) N/A N/A Syslog
 Event Type: Information Description: Jan 11 03:36:54 somehost3 admin-ui[1652]: [NOTICE] [192.0.2.96] admin/en: config: option "Rule_config" set to "1" (was "0")
 Log Type: Application
 Category Id: 0

Figure 2

- **Sophos Email Appliance-Policy Changes** – This report gives the information about the message policies changed by the users.

LogTime	Computer	Source IP Address	Source User Name	Policy Detail	Old Value	New Value	EventDescription
12/11/2017 04:59:13 PM	SOPHOUS_EA	192.0.2.96	admin	outbound virus action	quarantine	discard	Jan 11 03:57:11 somehost admin-ui[1200]: [NOTICE] [192.0.2.96] admin/en: policy: outbound virus action set to discard (was quarantine)
12/11/2017 04:59:13 PM	SOPHOUS_EA	192.0.2.96	admin	inbound spam action	quarantine	discard	Jan 11 03:57:11 somehost admin-ui[1200]: [NOTICE] [192.0.2.96] admin/en: policy: inbound spam action set to discard (was quarantine)

Figure 3

Logs Considered

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
<input type="checkbox"/> 12/18/2017 4:19:34 PM	3333	NTPPLDTBLR38 / Sophou...	N/A	N/A	Syslog

Event Type: Information Description: Jan 11 03:57:11 somehost admin-ui[1200]: [NOTICE] [192.0.2.96] admin/en: policy: outbound spam action set to discard (was quarantine)
 Log Type: Application
 Category Id: 0

Figure 4

- **Sophos Email Appliance-Allowed email traffic details** -This report gives information about the messages which were delivered (allowed) by the message policy rules.

LogTime	Computer	Mail Subject	Sender Address	Recipient Address	Direction	Spam Score	Rule Name	Untrusted Relay Address	Remote IP Address
12/11/2017 04:59:12 PM	SOPHOUS_EA	?q?Stores_that_have_not_transmitted	support@cotoso.com	TransmissionReport@cotoso.co	inbound	0.110	allowed_fw		10.66.100.4
12/11/2017 04:59:12 PM	SOPHOUS_EA	?q?KACE_-_BOS/POS_Last_Reboot_time	root@kbox.contoso.com	POShelpdesk@cotoso.com	inbound	0.079	allowed_fw		10.66.100.45
12/11/2017 04:59:12 PM	SOPHOUS_EA	?q?[VMware_vCenter_-_Alarm_alarm.VmCPUUsageAlarm]_alarm.VmCPUUsageAlarm_changed_status_from_Yellow_to_Red	pci-vcenter6@cotoso.com	udf.alert@gmail.com	outbound	0.078	allowed_fw	10.66.100.96	10.66.100.96
12/11/2017 04:59:12 PM	SOPHOUS_EA	?q?[VMware_vCenter_-_Alarm_alarm.VmCPUUsageAlarm]_alarm.VmCPUUsageAlarm_changed_status_from_Yellow_to_Red	pci-vcenter6@cotoso.com	support@cotoso.com	outbound	0.002	allowed_fw	10.66.100.96	10.66.100.96
12/11/2017 04:59:12 PM	SOPHOUS_EA	?q?KACE_-_BOS/POS_Last_Reboot_time	root@confotoso.com	POShelpdesk@cotoso.com	inbound	0.079	allowed_fw		10.66.100.45

Figure 5

Logs Considered

12/18/2017 2:50:54 PM 3333 NTPLDTBLR38 / Sophou... N/A N/A Syslog

Event Type: Information
 Log Type: Application
 Category Id: 0

Description:
 Nov 30 08:00:24 es4000 Nov 30 13:00:24 q=5A2000E8_2077_3625_1 f=<root@contosodata.com>; t=<POShelpdesk@tester.com>; t=<ccleveng@udfinc.com>; t=<gdavid@udfinc.com>; b=ok action=deliver h=HTML_NO_HTTP h=BODYTEXT_SIZE_10000_LESS h=BODYTEXT_SIZE_3000_LESS h=BODYTEXT_SIZE_400_LESS h=BODY_SIZE_10000_PLUS h=DATE_TZ_NA h=HAS_X_PHP_SCRIPT h=NO_CTA_URI_FOUND h=NO_REAL_NAME h=NO_URI_FOUND h=NO_O_URI_HTTPS h=__CT h=__CTYPE_HAS_BOUNDARY h=__CTYPE_MULTIPART h=__CTYPE_MULTIPART_MIXED h=__HAS_ATTACHMENT h=__HAS_ATTACHMENT1 h=__HAS_FROM h=__HAS_HTML h=__HAS_MSGID h=__HAS_X_PHP_ORIG_SCRIPT h=__MIME_HTML h=__MIME_TEXT_H h=__MIME_TEXT_H1 h=__MIME_TEXT_H2 h=__MIME_TEXT_P h=__MIME_TEXT_P1 h=__MIME_TEXT_P2 h=__MIME_VERSION h=__SANE_MSGID h=__SUBJ_ALPHA_END h=__TAG_EXIST h=__TO_MALFORMED_2 h=__TO_NO_NAME inbound p=0.079 S=?q?KACE_-_BOS/POS_Last_Reboot_time fur= r=10.66.100.45 tm=0.44 a=a/eom

Figure 6

- **Sophos Email Appliance-Blocked or quarantine email traffic details**-This report gives information about the messages which were discarded or quarantined by the message policy rules.

LogTime	Computer	Mail Subject	Sender Address	Recipient Address	Direction	Spam Score	Action	Rule Name	Remote IP Address	Untrusted Relay Address
12/11/2017 04:59:12 PM	SOPHOUS_EA	?q?[Fixed]UDFPCI_ET_Alert_System_Performance_Metrics	pci.monitor@cotoso.com	support@cotoso.com	outbound	0.802	reject	blocker_spam	10.66.100.23	10.66.100.23
12/11/2017 04:59:12 PM	SOPHOUS_EA	?q?UDFPCI_ET_Alert_System_Performance_Metrics	pci.monitor@cotoso.com	support@cotoso.com	outbound	0.902	discard	blocker_spam	10.66.100.23	10.66.100.23
12/11/2017 04:59:12 PM	SOPHOUS_EA	?q?[VMware_vCenter_-_Alarm_alarm.VmCPUUsageAlarm]_alarm.VmCPUUsageAlarm_changed_status_from_Green_to_Red	pci-vcenter6@cotoso.com	support@cotoso.com	outbound	0.755	quarantine	Quarantine	10.66.100.96	10.66.100.96
12/11/2017 04:59:12 PM	SOPHOUS_EA	?q?cotoso_Daily_-_Windows_Active_Directory_Object_Access_Report_[Success]	cotoso@eventtracker.com	pcireports@cotoso.com	outbound	0.952	discard	blocker_spam	10.66.100.70	10.66.100.70
12/11/2017 04:59:13 PM	SOPHOUS_EA	one	junk@example.com	tester2@host.example	inbound	0.708	quarantine	Quarantine	192.0.2.107	
12/11/2017 04:59:13 PM	SOPHOUS_EA	?q?This_should_exceed	junk@example.com	tester1@host.example	inbound	0.902	Reject	blocker_spam	192.0.2.107	

Figure 7

Logs considered

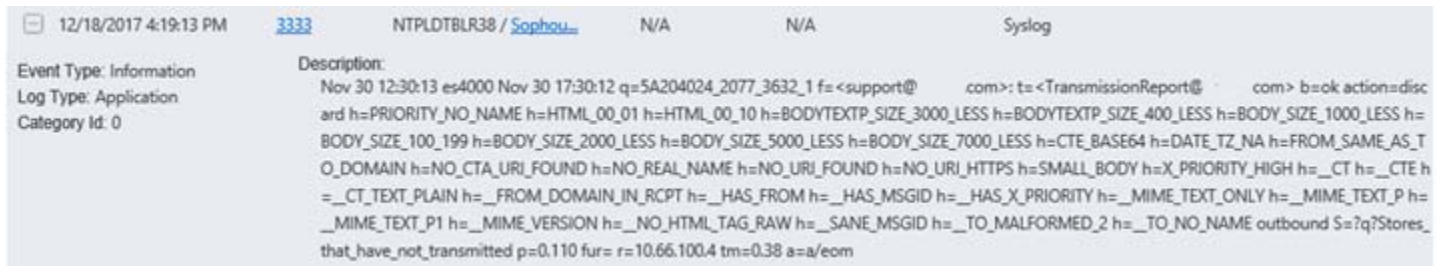


Figure 8

Categories

- **Sophos Email Appliance: Configuration Changes** - This category based report provides information related to configuration changes in Sophos Email Appliance.
- **Sophos Email Appliance: Policy Changes** – This category based report provides information related to the modification of Sophos Email Appliance policies.
- **Sophos Email Appliance: Admin User Login Details** – This category based report provides information related to admin logon activity.
- **Sophos Email Appliance: Allowed Email Traffic Details** – This category based report provides information related to email delivered by message policy rules.
- **Sophos Email Appliance: Blocked or Quarantine Email Traffic Details** – This category based report provides information related to the messages which were discarded or quarantined by the message policy rules.

Knowledge Objects

- **Sophos Email Appliance Admin User Login Details**– This knowledge object will help us to analyze logs related to Sophos Email Appliance’s admin logon details.
- **Sophos Email Appliance Configuration Changes**– This knowledge object will help us to analyze logs related to configuration changes made by users.
- **Sophos Email Appliance Email Traffic Details**– This knowledge object will help us to analyze logs related to the email filter.
- **Sophos Email Appliance Policy Changes**– This knowledge object will help us to analyze logs related to the policy rules modified by the user.

Import Sophos Email Appliance knowledge pack into EventTracker

NOTE: Import knowledge pack items in the following sequence:

- Categories
- Alerts
- Token templates
- Knowledge Objects
- Flex Reports

1. Launch **EventTracker Control Panel**.
2. Double click **Export Import Utility**.

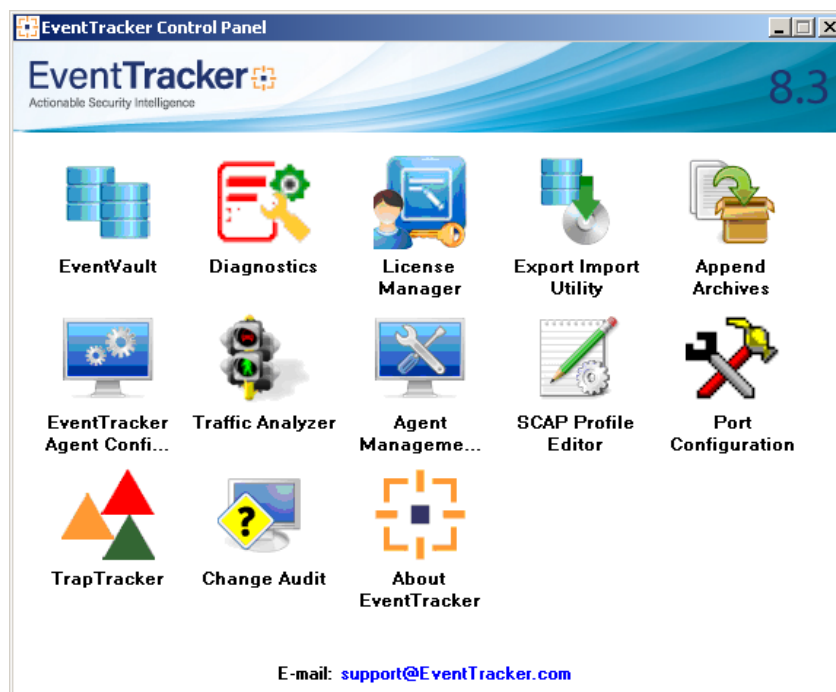



Figure 9

3. Click the **Import** tab.

Category

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

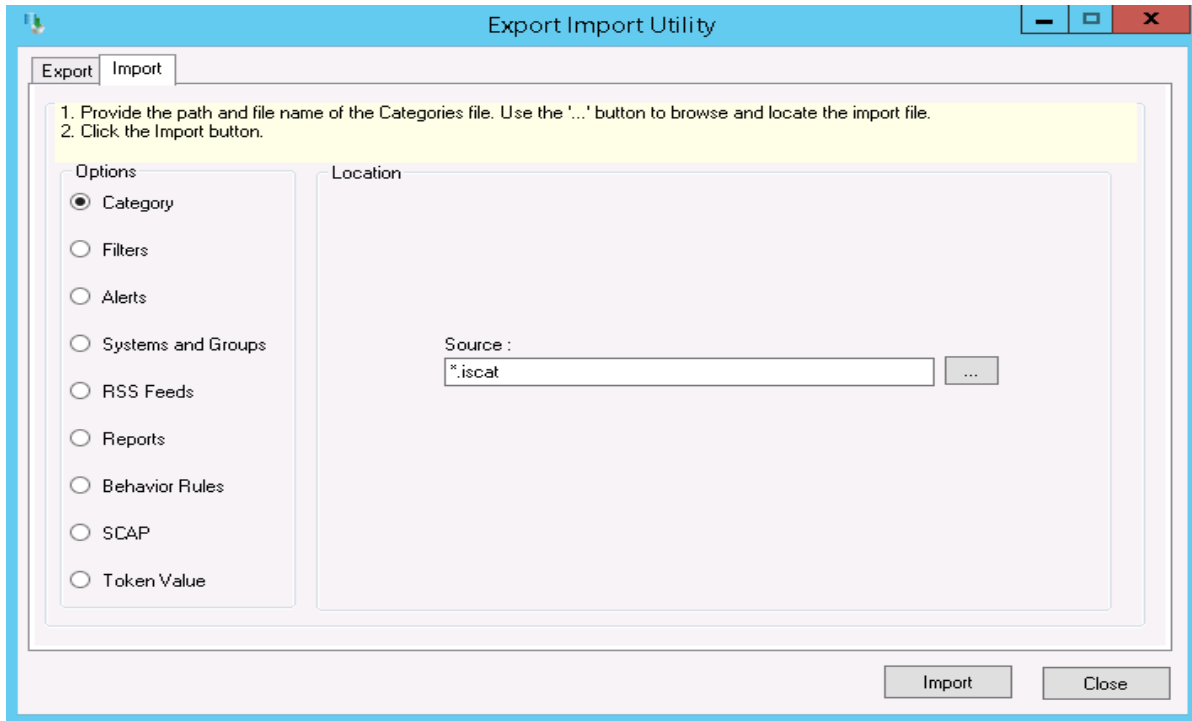


Figure 10

2. Locate .iscat file, and then click the **Open** button.
3. To import categories, click the **Import** button.

EventTracker displays success message.

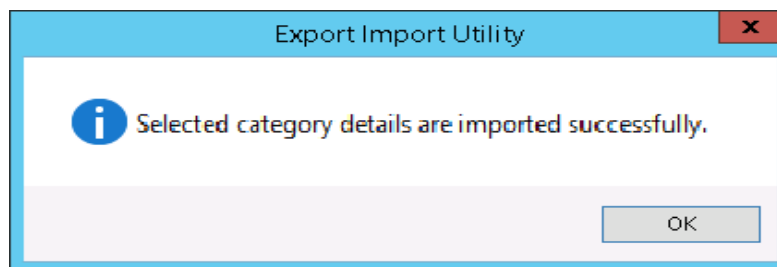


Figure 11

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

Token Templates



1. Click **Parsing rules** under **Admin** option in the EventTracker manager page.
2. Move to **Template** and click on import configuration  icon on the top right corner.
3. In the popup window browse the file named **TokenTemplate_Sophos Email Appliance.ettd**.



Figure 12

4. Now select all the check box and then click on  Import option.

Knowledge Objects

1. Click **Knowledge objects** under Admin option in the EventTracker manager page.
2. Locate the file named **KO_Sophos Email Appliance.etko**.

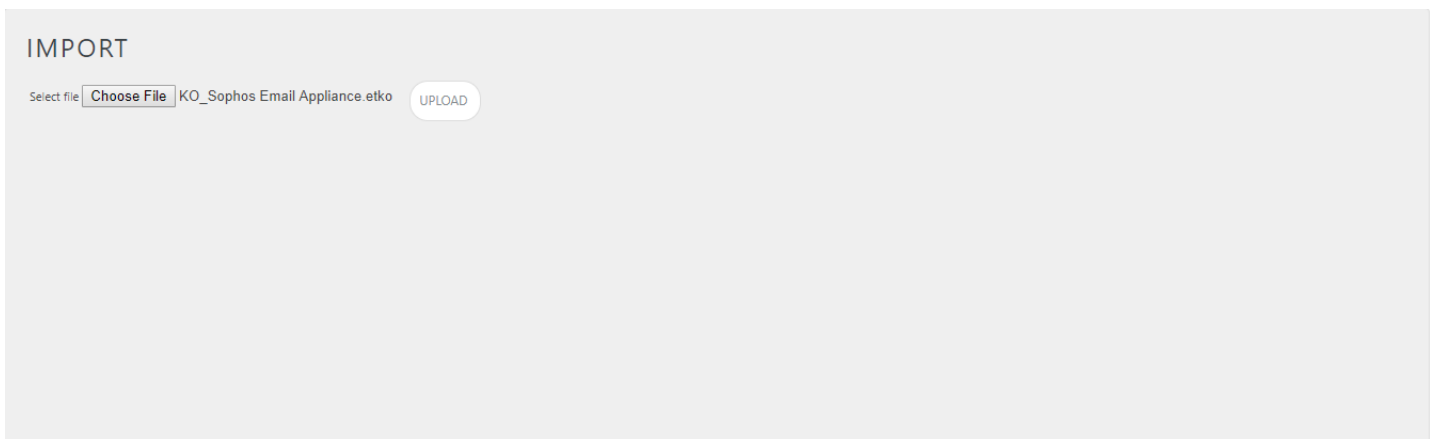



Figure 13

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

<input checked="" type="checkbox"/> OBJECT NAME	APPLIES TO	GROUP NAME
<input checked="" type="checkbox"/> Sophos Email Appliance Admin User Login Details	Sophos Email Appliance V4.2.XX and later	Sophos Email Appliance
<input checked="" type="checkbox"/> Sophos Email Appliance Configuration Changes	Sophos Email Appliance V4.2.XX and later	Sophos Email Appliance
<input checked="" type="checkbox"/> Sophos Email Appliance Email Traffic Details	Sophos Email Appliance V4.2.XX and later	Sophos Email Appliance
<input checked="" type="checkbox"/> Sophos Email Appliance Policy Changes	Sophos Email Appliance V4.2.XX and later	Sophos Email Appliance

Figure 14

4. Knowledge objects are now imported successfully.

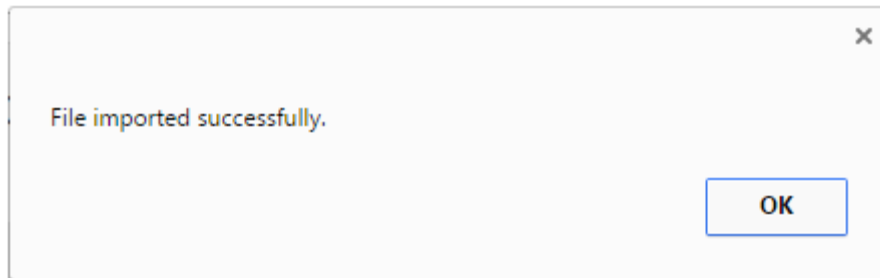


Figure 15

Flex Reports

On EventTracker Control Panel,

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

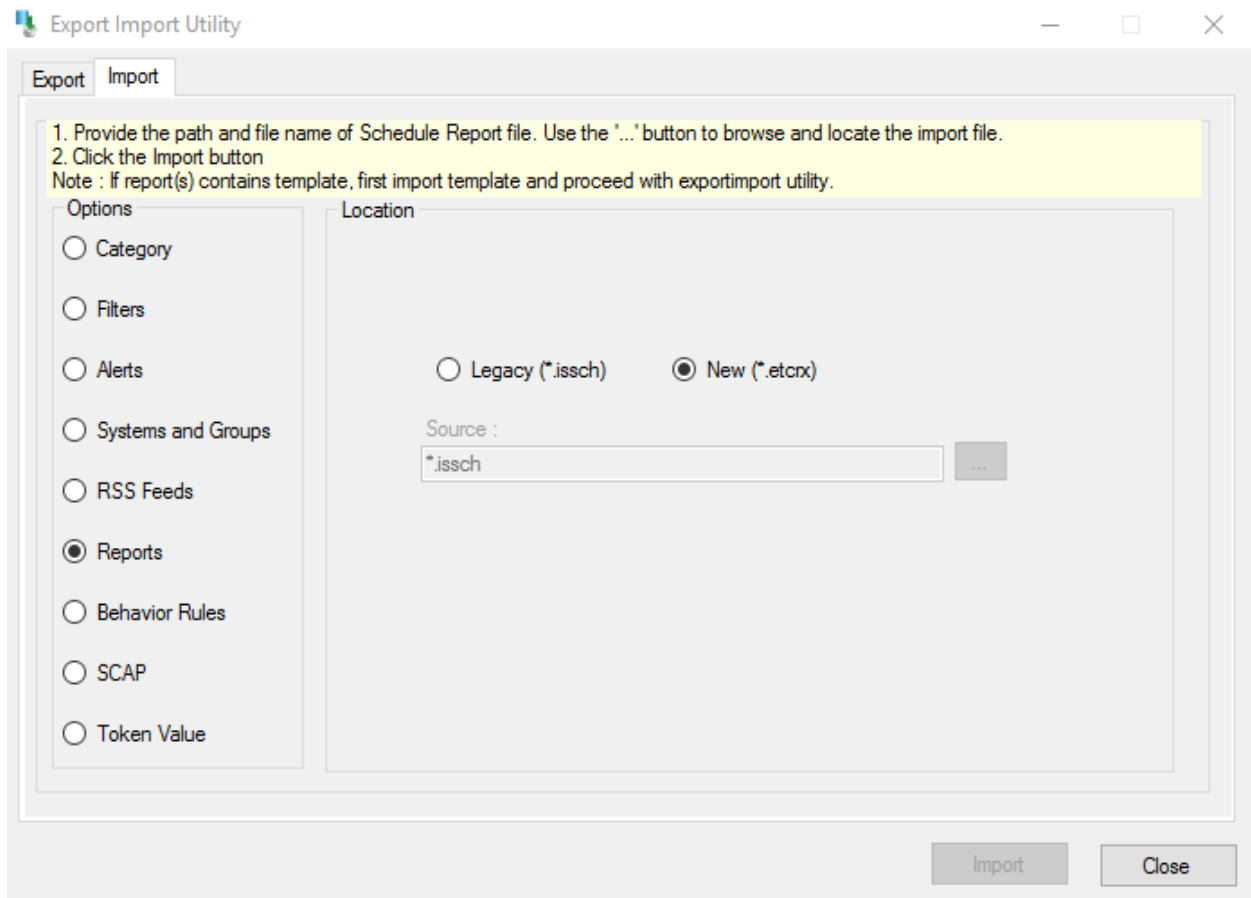


Figure 16

2. Locate the file named **FlexReports_Sophos Email Appliance.etcrx**, and select all the check box.

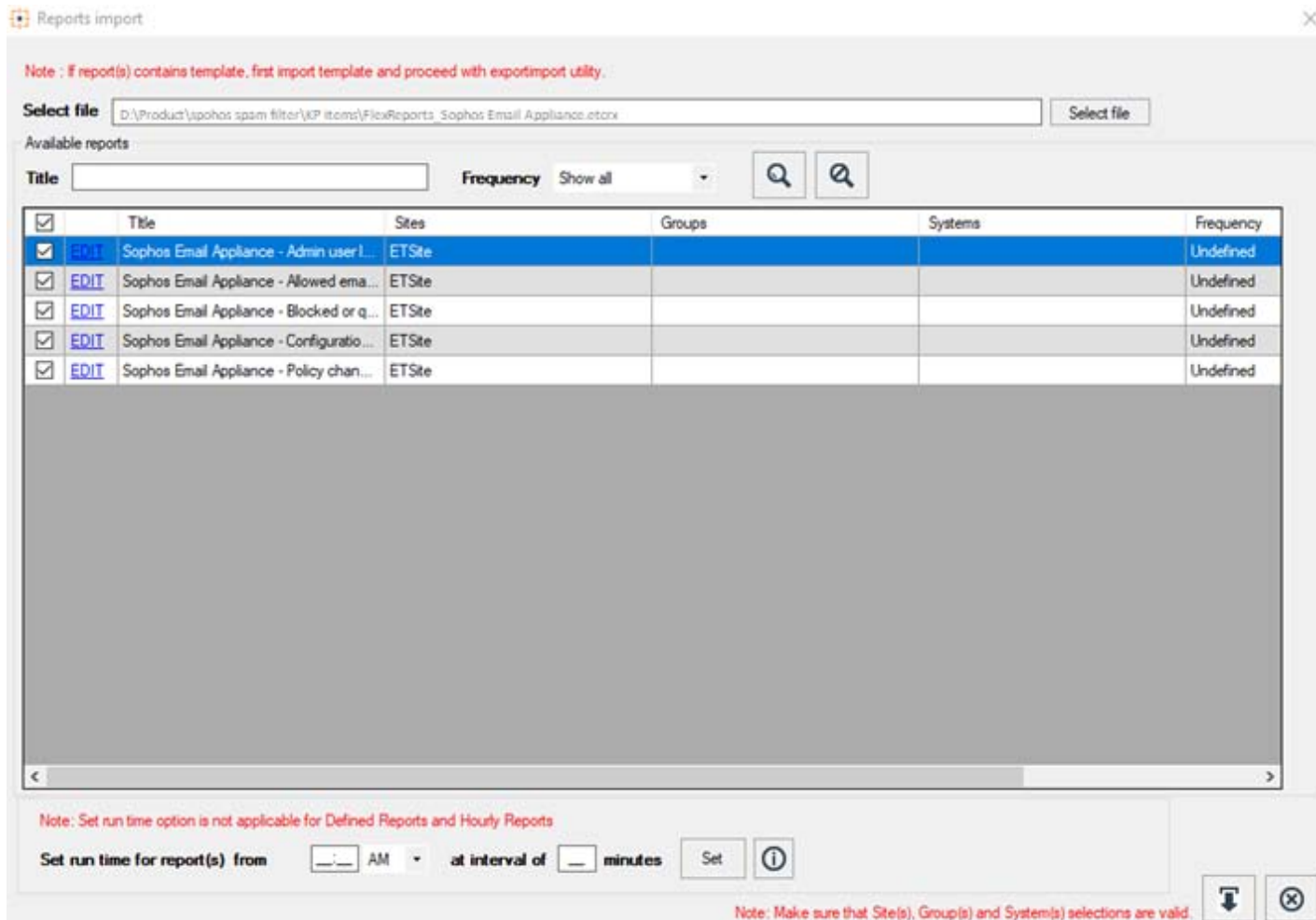


Figure 17

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

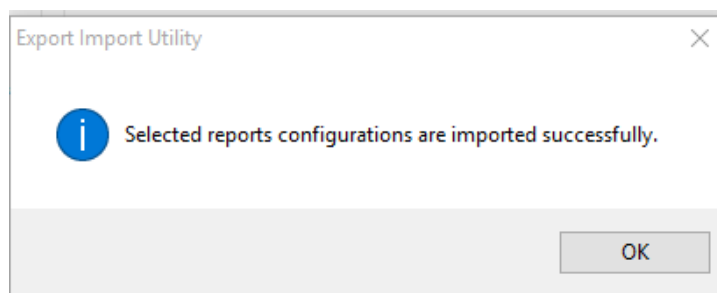


Figure 18

Verify Sophos Email Appliance knowledge pack in EventTracker

Categories

1. Logon to **EventTracker Enterprise**.
2. Click **Admin** dropdown, and then click **Categories**.

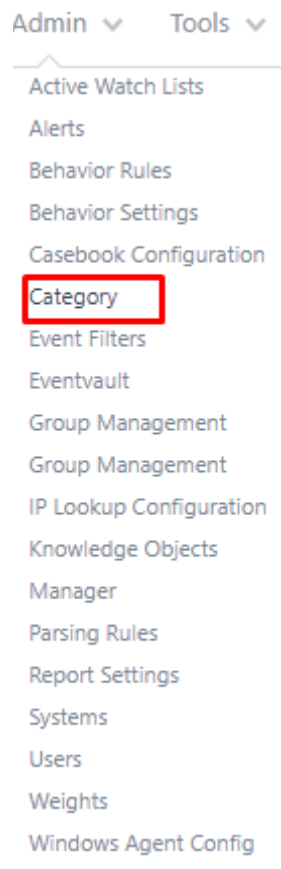


Figure 19

3. In **Category Tree** to view imported categories, scroll down and expand Sophos Email Appliance group folder to view the imported categories.

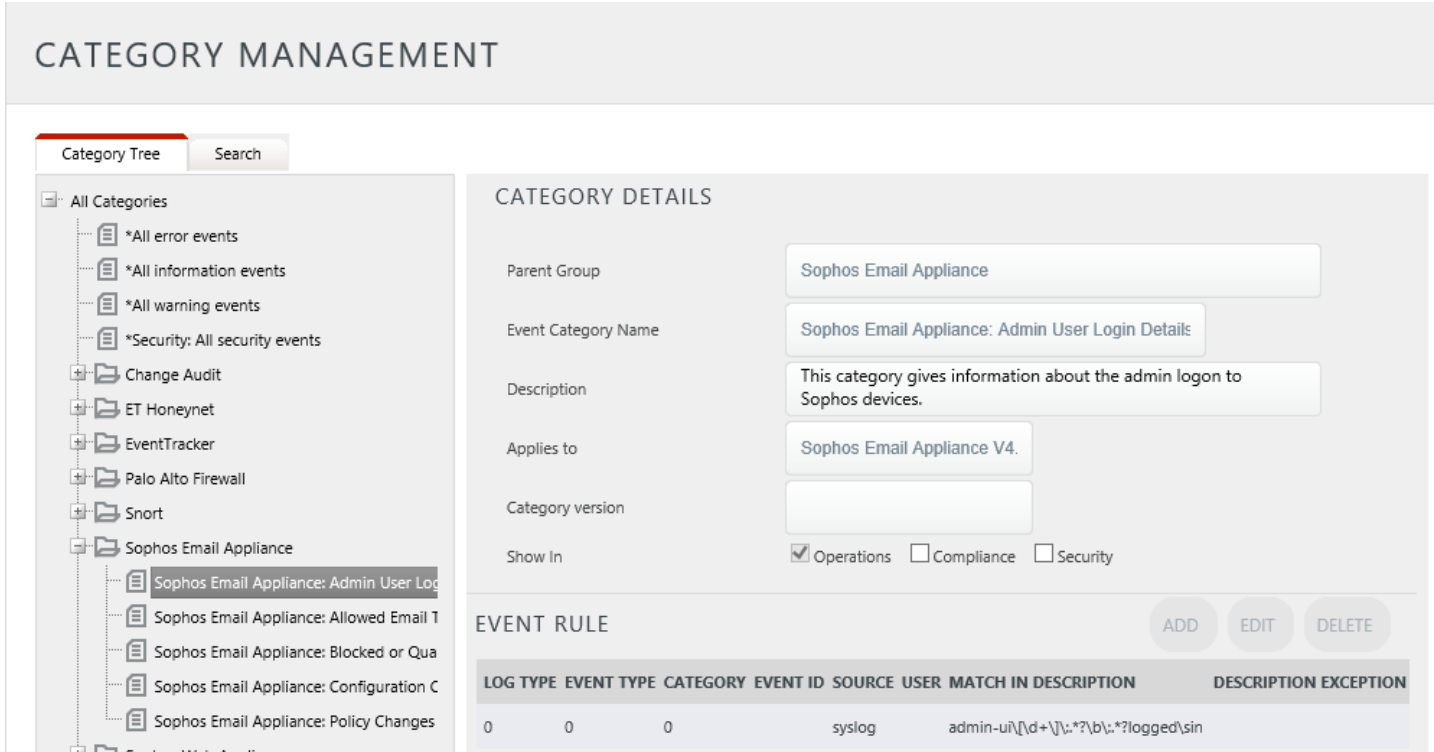


Figure 20

Token Template

1. In the **EventTracker Enterprise** web interface, click the **Admin** dropdown, and then click **Parsing rules**.

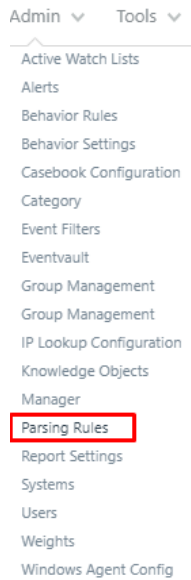


Figure 21

2. On **Template** tab, click on the Sophos Email Appliance group folder to view the imported Templates.

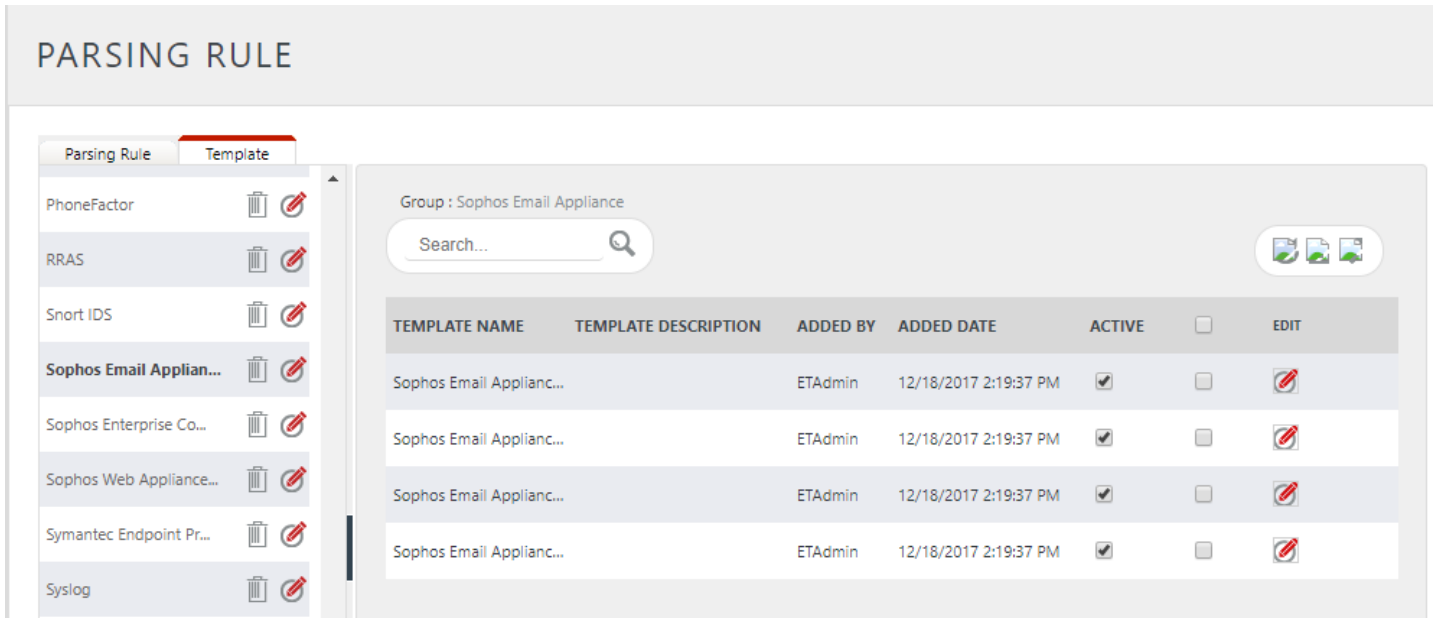


Figure 22

Knowledge Objects

1. In the **EventTracker Enterprise** web interface, click the **Admin** dropdown, and then click **Knowledge Objects**.

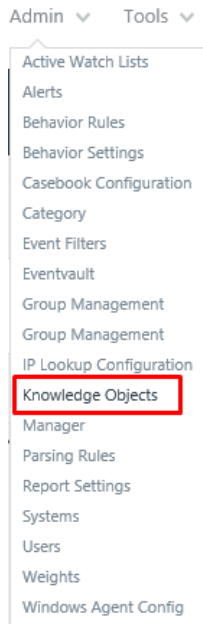


Figure 23

- In the Knowledge Object tree, expand Sophos Email Appliance group folder to view the imported Knowledge objects.

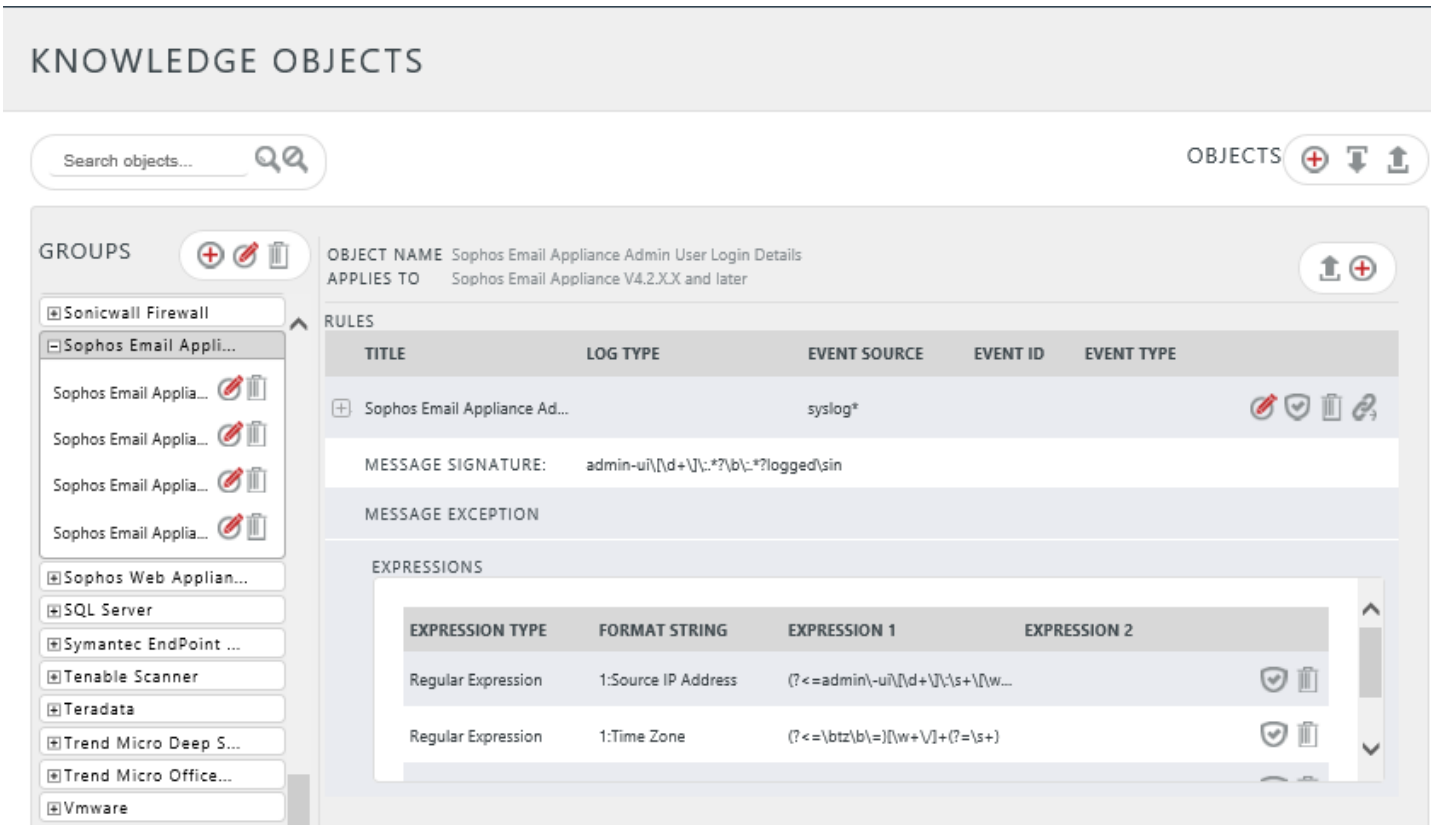


Figure 24

Flex Reports

- In the **EventTracker Enterprise** web interface, click the **Reports** menu, and then select **Report Configuration**.

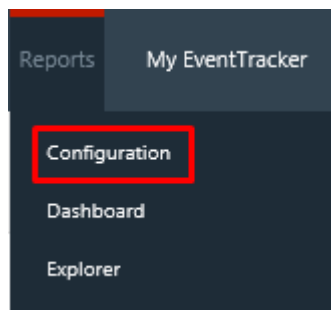


Figure 25

- In **Reports Configuration** pane, select **Defined** option.

3. Click on the Sophos Email Appliance group folder to view the imported Sophos Email Appliance reports.

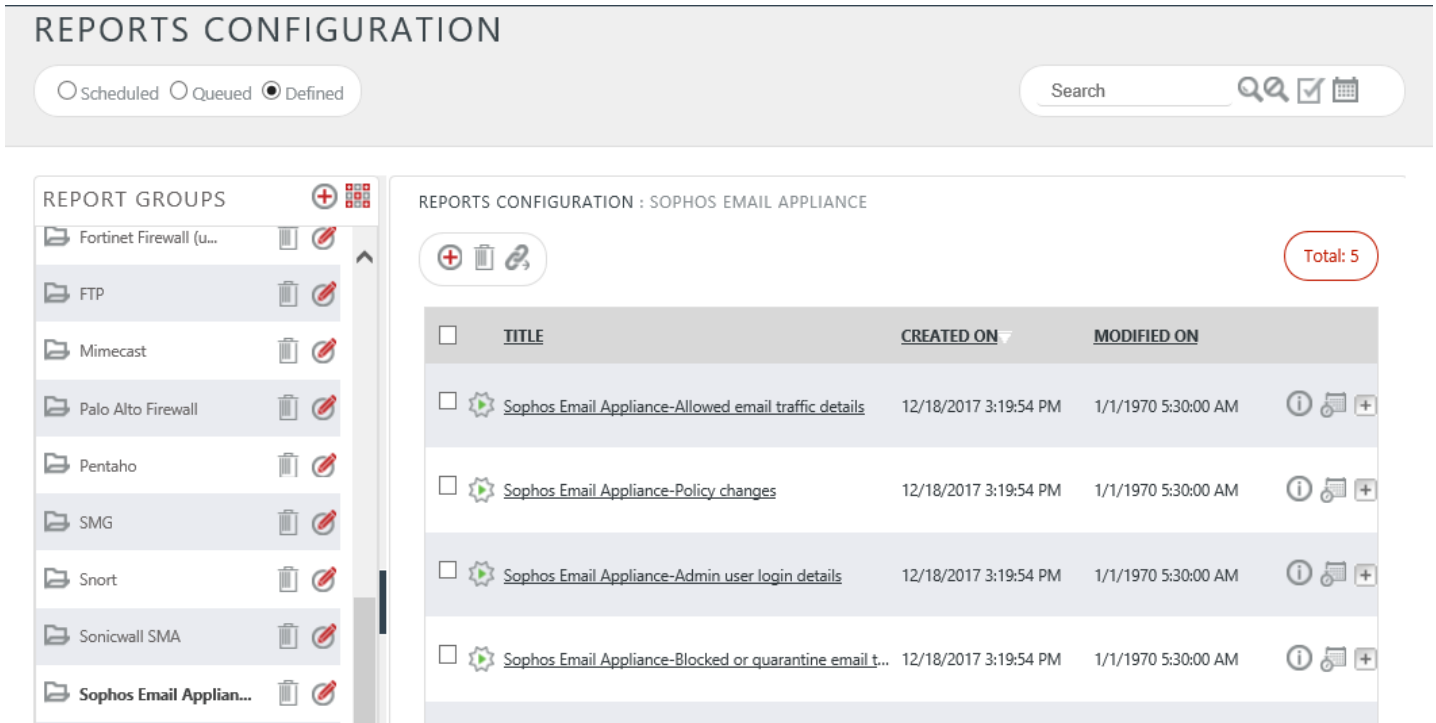


Figure 26

Create Dashlets

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

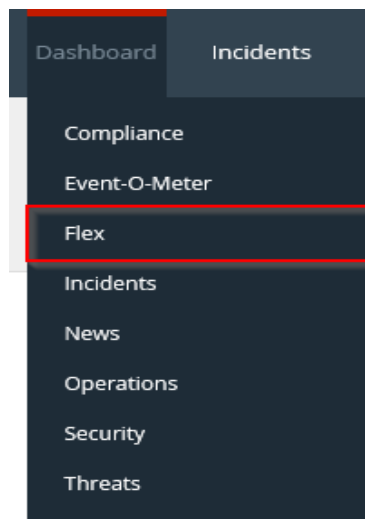


Figure 27

- 2. Navigate to **Dashboard>Flex**.
Flex Dashboard pane is shown.

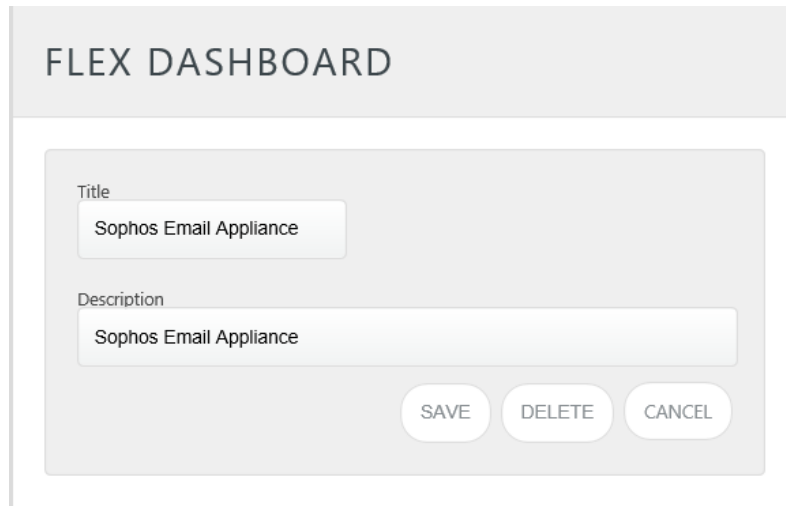



Figure 28

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

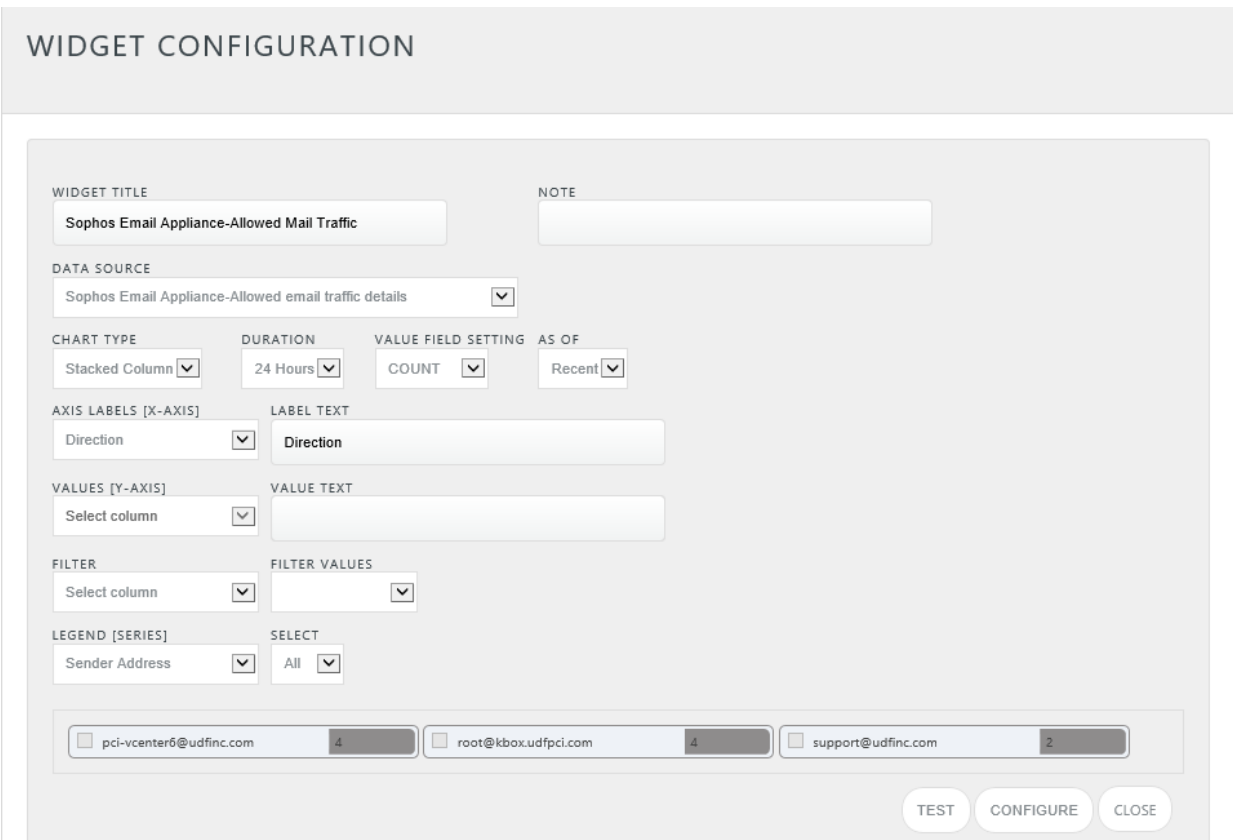


Figure 29

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

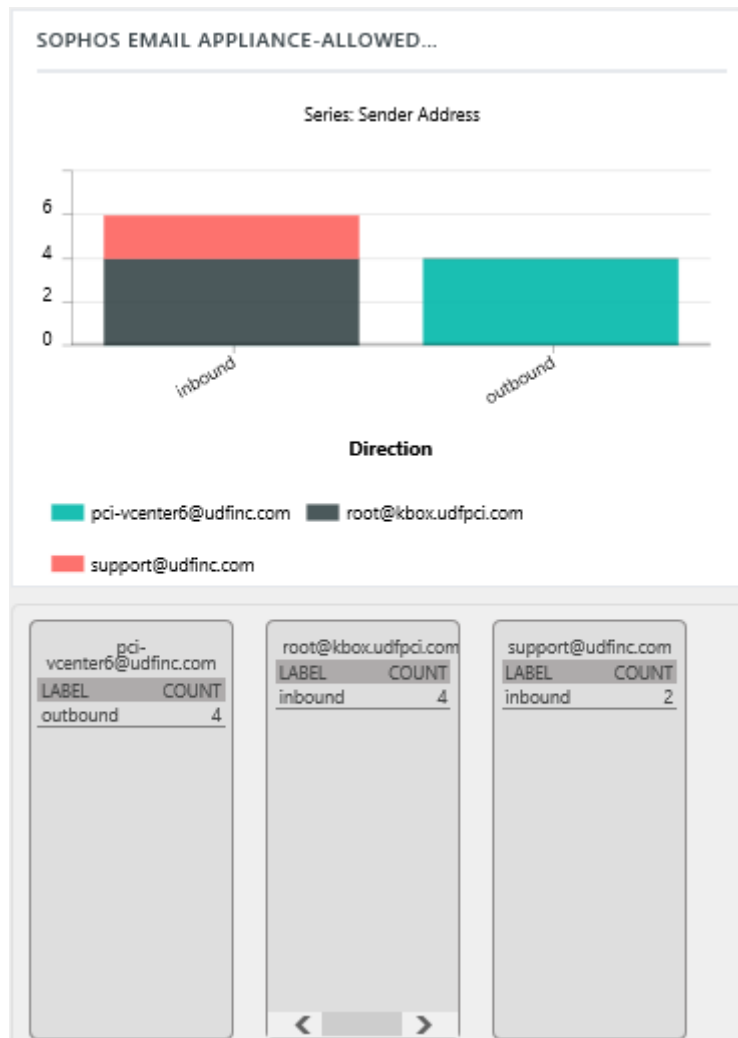


Figure 30

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

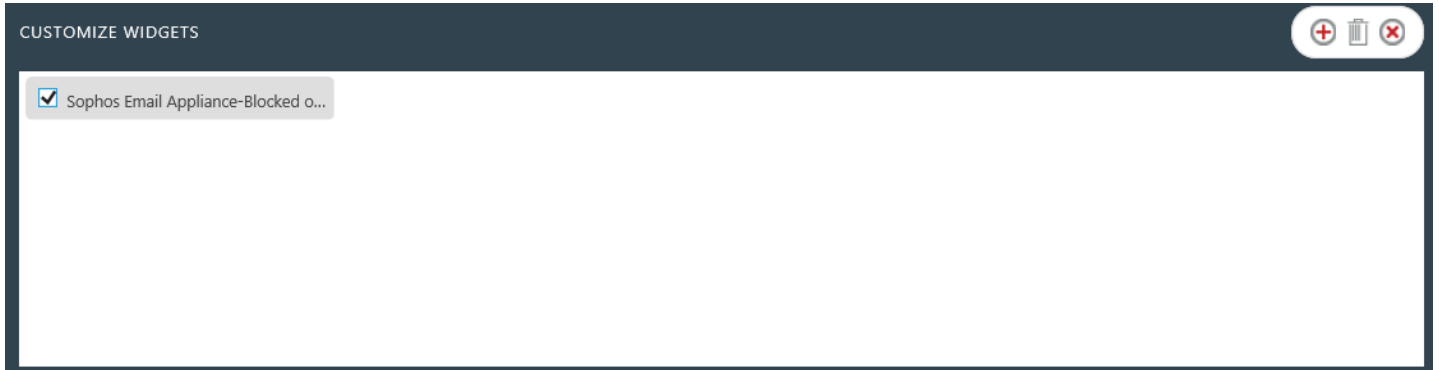




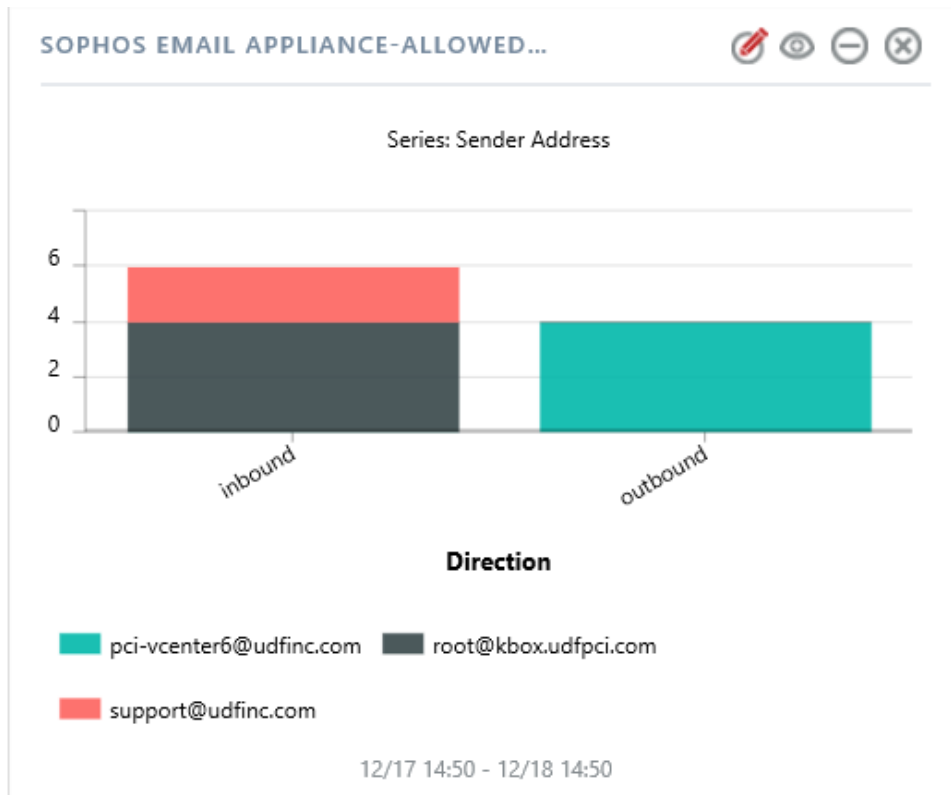
Figure 31

15. Click 'customize'  to locate and choose created dashlet.
16. Click  to add dashlet to earlier created dashboard.

Sample Flex Dashboards

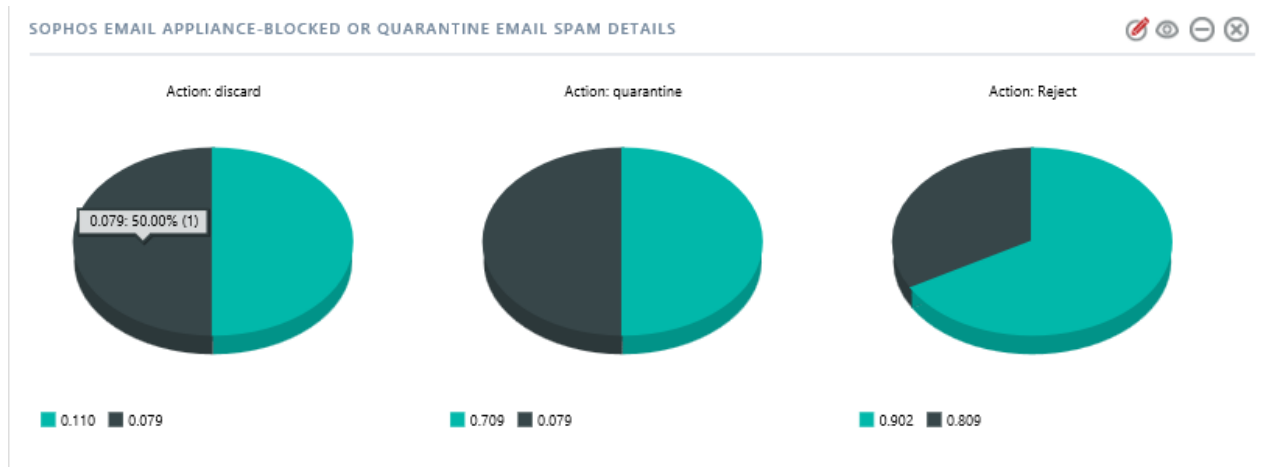
For below dashboard

- **WIDGET TITLE:** Sophos Email Appliance-Allowed Mail Traffic
- **DATA SOURCE:** Sophos Email Appliance-Allowed email traffic details
- **CHART TYPE:** Stacked Column
- **AXIS LABELS [X-AXIS]:** Direction
- **LEGEND[SERIES]:** Sender Address



For below dashboard

- **WIDGET TITLE:** Sophos Email Appliance-Blocked or Quarantine Email Spam Details
- **DATA SOURCE:** Sophos Email Appliance-Blocked or quarantine email traffic details
- **CHART TYPE:** Pie
- **AXIS LABELS [X-AXIS]:** Spam Score
- **LEGEND[SERIES]:** Action



For below dashboard

- **WIDGET TITLE:** Sophos Email Appliance-Suspicious Mail Sender Details
- **DATA SOURCE:** Sophos Email Appliance-Blocked or quarantine email traffic details
- **CHART TYPE:** Stacked Column
- **AXIS LABELS [X-AXIS]:** Action
- **LEGEND[SERIES]:** Sender Details

