

Integrate SonicWall Spam Filter

EventTracker v8.x and above

Abstract

This guide provides instructions to configure a **SonicWall Spam Filter** 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 **SonicWall Spam Filter v 9.0 and later**.

Audience

Administrators who are assigned the task to monitor SonicWall Spam Filter 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.

© 2018 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 SonicWall Spam Filter with EventTracker manager 3
- EventTracker Knowledge Pack..... 4
 - Categories 5
 - Alerts 5
 - Flex Reports 5
- Import SonicWall Spam Filter knowledge pack into EventTracker 8
 - Category 9
 - Alerts 10
 - Token Templates 11
 - Knowledge Objects 12
 - Flex Reports 14
- Verify SonicWall Spam Filter knowledge pack in EventTracker 17
 - Categories 17
 - Alerts 17
 - Token Template..... 19
 - Knowledge Objects 19
 - Flex Reports 20
- Create Dashlets 21
 - Sample Flex Dashboards 25

Overview

The **SonicWall Email Security** appliances deliver a multi-layered protection against advanced email-borne threats from a hardened Linux based system. It integrates with Capture Advanced Threat Protection sandbox, uses multiple AV engines for comprehensive malware scanning, real-time threat intelligence feeds from SonicWall Capture Labs, enables email fraud prevention with SPF, DKIM and DMARC, delivers dynamic Advanced Reputation Management (ARM) and offers DLP with Email Encryption and Compliance add-on.

EventTracker helps to monitor events from SonicWall Spam Filter. It's knowledge object and flex reports will help you to analyze mail traffic, threat detection and to monitor policy or configuration changes.

Prerequisites

- EventTracker v8.x or above should be installed.
- SonicWall Spam Filter v 9.0 and later should be configured for forwarding logs.
- Create a rule in EventTracker Manager firewall for inbound and outbound to allow UDP port 514.

Integration of SonicWall Spam Filter with EventTracker manager

To configure a SonicWall Spam Filter to forward logs to a syslog server,

- Logon to **SonicWall Email Security** web interface.
- Navigate to **System Monitoring** and click on **Configure System Logging** at the bottom of the page. A pop window will appear as shown below.

Severity level: **SYSLOG_INFORMATION**

Local:
(Log to Event Viewer on Windows installations)

Remote:
(Send syslog messages to remote servers)

Server 1 name and UDP port: **10.xx.xx.54** **514**
(Example: 192.168.1.1 and port 514; also supports FQDN such as *myserver.example.com*)

Server 2 name and UDP port:
(Example: 192.168.1.1 and port 514; also supports FQDN such as *myserver.example.com*)

Send message details:
(Send a syslog message for every email)

Save **Cancel**

Figure.1

- From the drop down choose **SYSLOG_INFORMATION** as the **Severity Level**.
- Check the **Remote checkbox** option.
- In the **Server 1 name and UDP port**, enter the **EventTracker Manager IP Address** and Port as **514** as shown in the above image.
- Check the **Send message details** checkbox
- Click on **Save**.

Logs will now be forwarded to EventTracker.

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 SonicWall Spam Filter.

Categories

- **SonicWall Spam Filter-Threat detected-** This category based report provides information related to all the threat emails that is detected by the SonicWall Spam Filter.
- **SonicWall Spam Filter-Spam email detection-** This category based report provides information related to all the spam emails that is detected by the SonicWall Spam Filter.
- **SonicWall Spam Filter-Clean email traffic-** This category based report provides information related to all the clean emails that is passed through SonicWall Spam Filter.

Alerts

- **SonicWall Spam Filter: Threat detected:** This alert is generated when any threat is detected in the email traffic by the SonicWall Spam Filter.

Flex Reports

NOTE: Below reports would contain threat category fields in abbreviated forms,

Below given are possible abbreviated forms that would appear in the reports and alerts.

- ddh = Definate directory harvest attack
 - dsp= Definate spam
 - lsp = Likely spam
 - dvi = Definate virus
 - lvi = Likely virus
 - dph= Definate phishing
 - lph = Likely phishing
 - goo = good email (no Threat)
 - Ply = Policy threat
- **SonicWall Spam Filter-Threat detected-** This report gives the information about all the threat emails that is detected by the SonicWall Spam Filter.

LogTime	Computer	Sender Address	Recipient Address	Email Subject	Threat Category	Threat Name
04/27/2018 02:39:09 PM	SONICSF	winkster121.supply.com@gossips.com	accountwin.12@contoso.com	Save up to 85 percent on printer ink	ddh	-
04/27/2018 02:39:09 PM	SONICSF	remedy.12.elite@gossips.com	accountwin.12@contoso.com	FW: Your HSBC application documents	dvi	CVE-2017-11882.A.gen/Camelot
04/27/2018 02:39:09 PM	SONICSF	ajaxax.121@lipren2.com	accountwin.12@contoso.com	U.S Department of State	dph	-

Figure 2

Logs Considered

Apr 27 05:10:43 AM		Apr 16 16:50:01 bfgmailgateway Apr 16 16:50:01 junkmail id=EmailSecurity: sn=0040102820D0 Subject="Re: Re: new order 18141022/Cables" From=vatandl@server.vatamdownload.com To=	
add_info	+ - EmailSecurity:		
add_info1	+ - 0		
email_subject	+ - Re: Re: new order 18141022/Cables		
event_category	+ - 0		
event_computer	+ - SonicSF		
event_datetime	+ - 4/27/2018 5:10:43 AM		
event_datetime_utc	+ - 1524831043		
event_description	Apr 16 16:50:01 bfgmailgateway Apr 16 16:50:01 junkmail id=EmailSecurity: sn=0040102820D0 Subject="Re: Re: new order 18141022/Cables" From=vatandl@server.vatamdownload.com To=accountwin.12@contoso.com MfUniqueID=20180416204945000719 Threat= dvi VrsOrPolicyName=Exploit-CVE2017-11882.o		
event_id	+ - 3333		
event_log_type	+ - Application		
event_source	+ - syslog		
event_type	+ - Information		
event_user_domain	+ - N/A		
event_user_name	+ - N/A		
log_source	+ - Sonicwall Spam Filter Threat detection		
recipient_address	+ - accountwin.12@contoso.com		
sender_address	+ - vatandl@server.vatamdownload.com		
tags	+ - Sonicwall Spam Filter		
tags	+ - Threat detection		
threat_category	+ - dvi		
threat_name	+ - Exploit-CVE2017-11882.o		

Figure 3

- **SonicWall Spam Filter-Spam email detection** – This report gives the information about all the spam emails that is detected by the SonicWall Spam Filter.

LogTime	Computer	Sender Address	Recipient Address	Email Subject	Threat Category	Threat Name
04/27/2018 02:39:09 PM	SONICSF	pnpl.exer.dt@epof.com	accountwin.12@contoso.com	For You: See Inside	lsp	-
04/27/2018 02:39:09 PM	SONICSF	remedy.12.elite@gossips.com	accountwin.12@contoso.com	Dont pay a fortune for printer ink.	dsp	-

Figure 4

Logs Considered

```

- Apr 27 05:10:43 AM
Apr 17 13:42:01 bfgmailgateway Apr 17 13:42:01 junkmail id=EmailSecurity: sn=0040102820D0 Subject="For You: See Inside" From=pnpl.exer.dt@epof.com To=accountwin.12@contoso.co...

addl_info      +- EmailSecurity:
addl_info1     +- 0
email_subject  +- For You: See Inside
event_category +- 0
event_computer +- SonicSF
event_datetime +- 4/27/2018 5:10:43 AM
event_datetime_utc +- 1524831043
event_description
Apr 17 13:42:01 bfgmailgateway Apr 17 13:42:01 junkmail id=EmailSecurity: sn=0040102820D0 Subject="For You: See Inside" From=pnpl.exer.dt@epof.com To=accountwin.12@contoso.com
MIRUniqueID=20180417174102003754 Threat= lsp VrsOrPolicyName=-

event_id       +- 3333
event_log_type +- Application
event_source   +- syslog
event_type     +- Information
event_user_domain +- N/A
event_user_name +- N/A
log_source     +- Sonicwall Spam Filter Spam email detection
recipient_address +- accountwin.12@contoso.com
sender_address +- pnpl.exer.dt@epof.com
tags          +- Sonicwall Spam Filter
              +- Spam email
threat_category +- lsp
threat_name    +- -
    
```

Figure 5

- **SonicWall Spam Filter-Clean email traffic**-This report gives information about all the clean emails that is passed through SonicWall Spam Filter.

LogTime	Computer	Sender Address	Recipient Address	Email Subject
04/27/2018 02:39:09 PM	SONICSF	pnpl.exer.dt@epof.com	accountwin.12@contoso.com	Credit Card Payment Confirmation

Figure 6

Logs Considered

Apr 27 05:10:43 AM	Apr 17 13:42:01 bfgmailgateway Apr 17 13:42:01 junkmail id=EmailSecurity: sn=0040102820D0 Subject="Credit Card Payment Confirmation" From=pnplexer.dt@epof.com To=accountwin.1...
addl_info	+-- EmailSecurity:
addl_info1	+-- 0
email_subject	+-- Credit Card Payment Confirmation
event_category	+-- 0
event_computer	+-- SonicSF
event_datetime	+-- 4/27/2018 5:10:43 AM
event_datetime_utc	+-- 1524831043
event_description	Apr 17 13:42:01 bfgmailgateway Apr 17 13:42:01 junkmail id=EmailSecurity: sn=0040102820D0 Subject="Credit Card Payment Confirmation" From=pnplexer.dt@epof.com To=accountwin.12@contoso.com MIFUniquelD=20180417174113003755 Threat= goo VrsOrPolicyName=-
event_id	+-- 3333
event_log_type	+-- Application
event_source	+-- syslog
event_type	+-- Information
event_user_domain	+-- N/A
event_user_name	+-- N/A
log_source	+-- Sonicwall Spam Filter Clean email traffic
recipient_address	+-- accountwin.12@contoso.com
sender_address	+-- pnplexer.dt@epof.com
tags	+-- Sonicwall Spam Filter
tags	+-- Clean traffic
threat_category	+-- goo
threat_name	+-- -

Figure 7

Import SonicWall Spam Filter 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**.

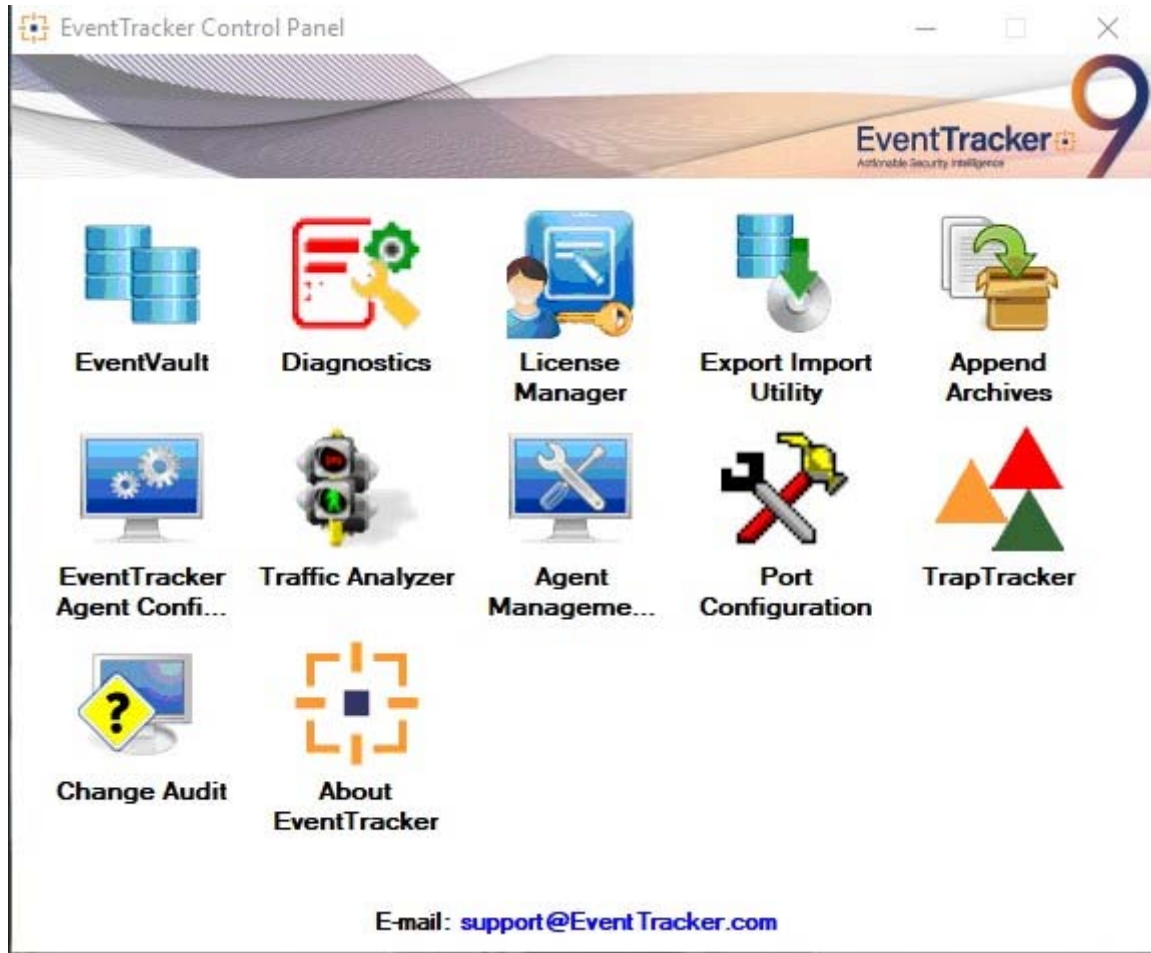



Figure 8

3. Click the **Import** tab.

Category

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

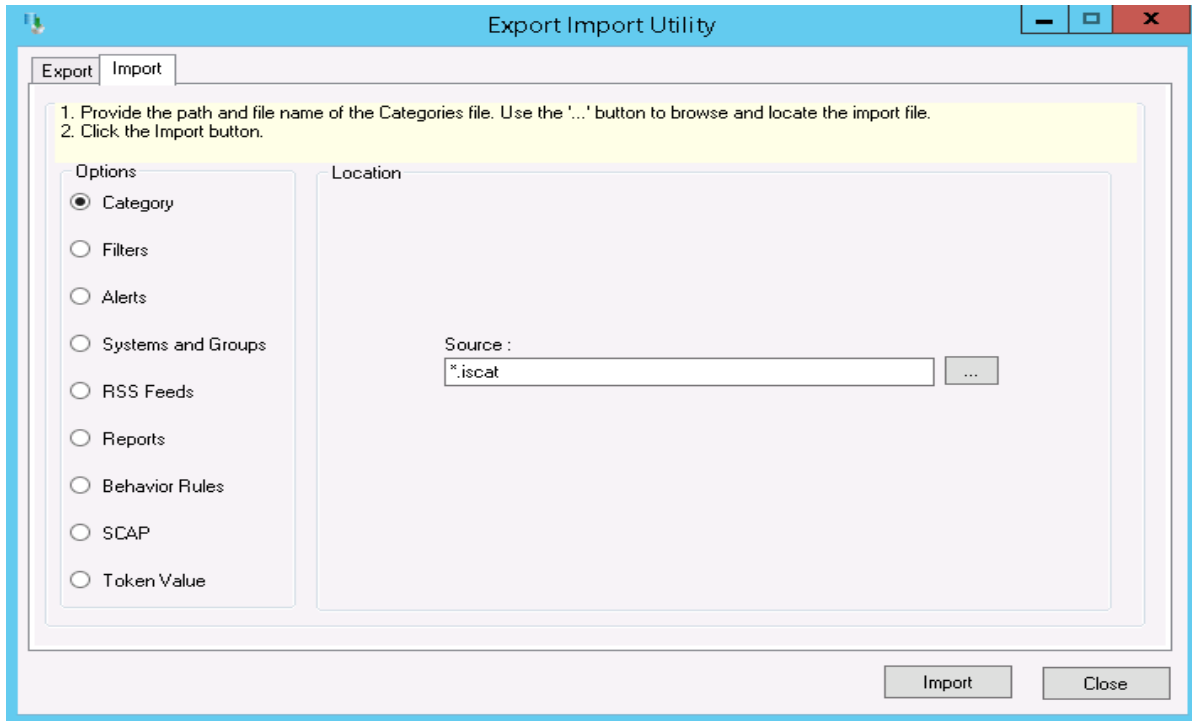


Figure 9

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

EventTracker displays success message.

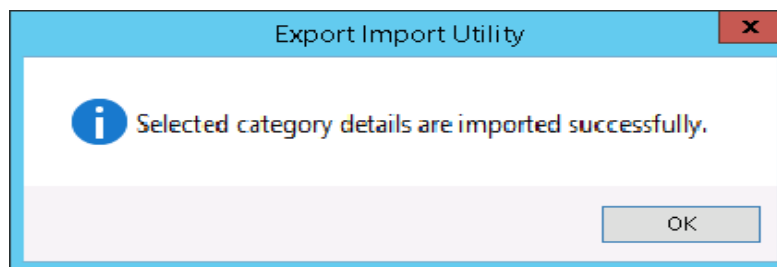



Figure 10

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

Alerts

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

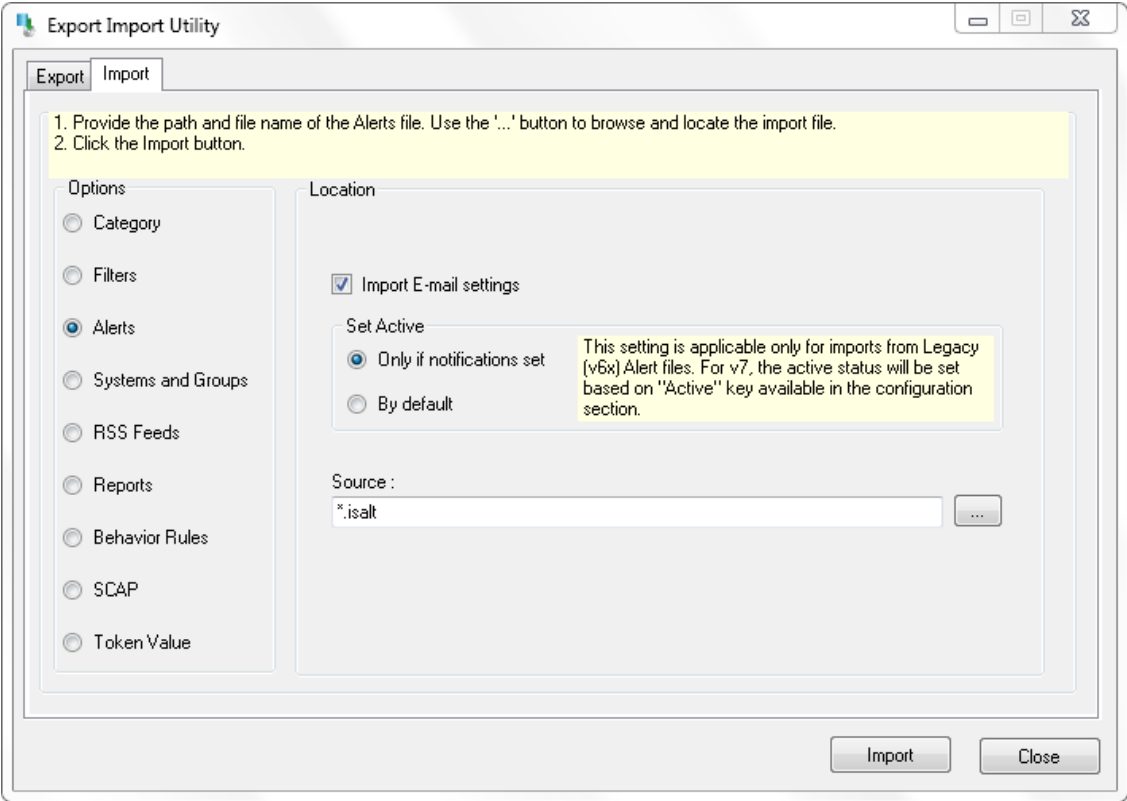


Figure 11

- 2. Locate **Alerts_Sonicwall Spam Filter.isalt** file, and then click the **Open** button.
- 3. To import alerts, click the **Import** button.
- 4. EventTracker displays success message.

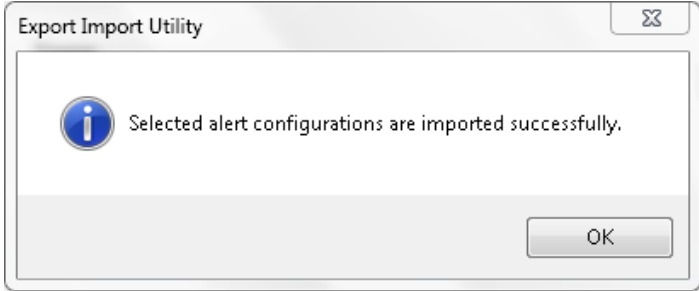


Figure 12

- 5. Click the **OK** button, and then click the **Close** button.

Token Templates

- 1. Click **Parsing rules** under **Admin** option in the EventTracker manager page.

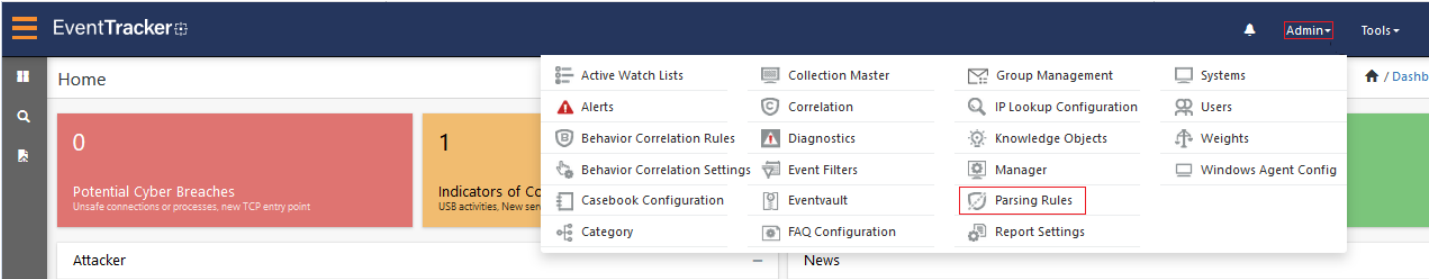



Figure 13

2. Move to **Template** and click on import configuration  icon on the top right corner.
3. In the popup window browse the file name **Template_Sonicwall Spam Filter.ettd**.

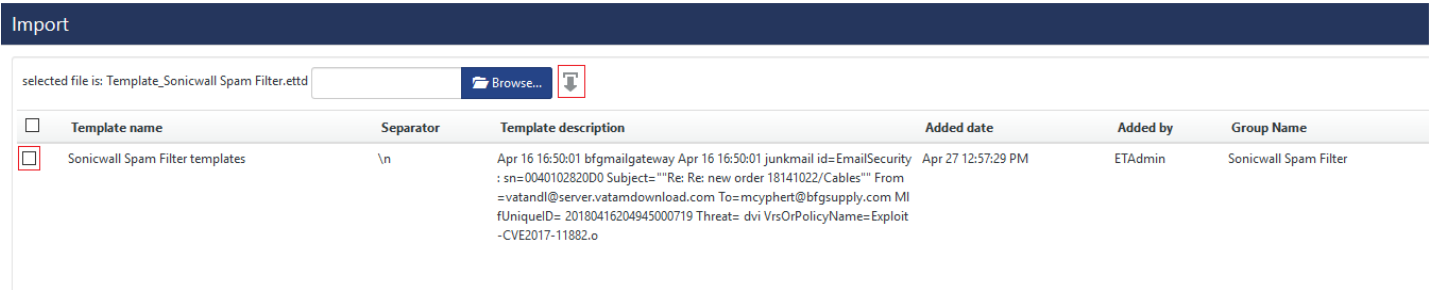



Figure 14

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.

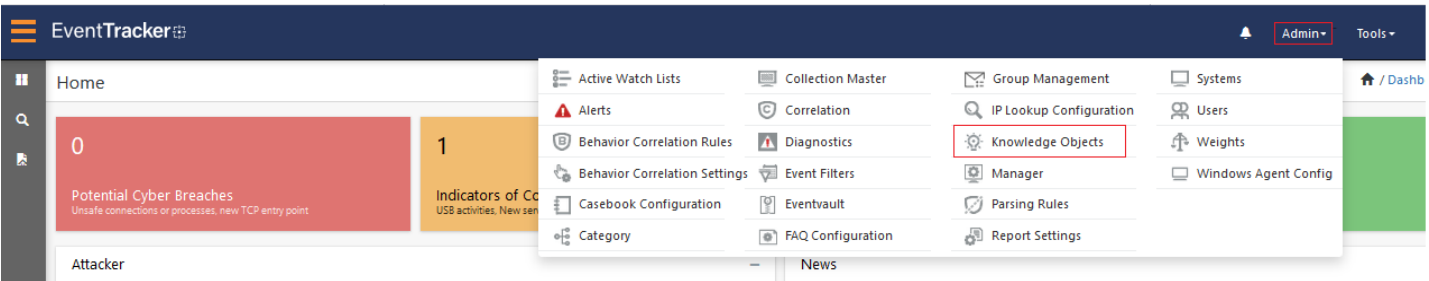


Figure 15

2. Click on **Import** button as highlighted in the below image.

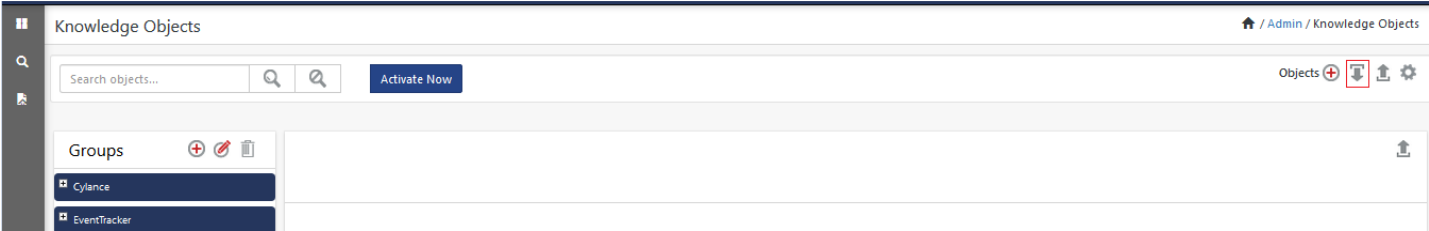


Figure 16

3. Click on **Browse**.

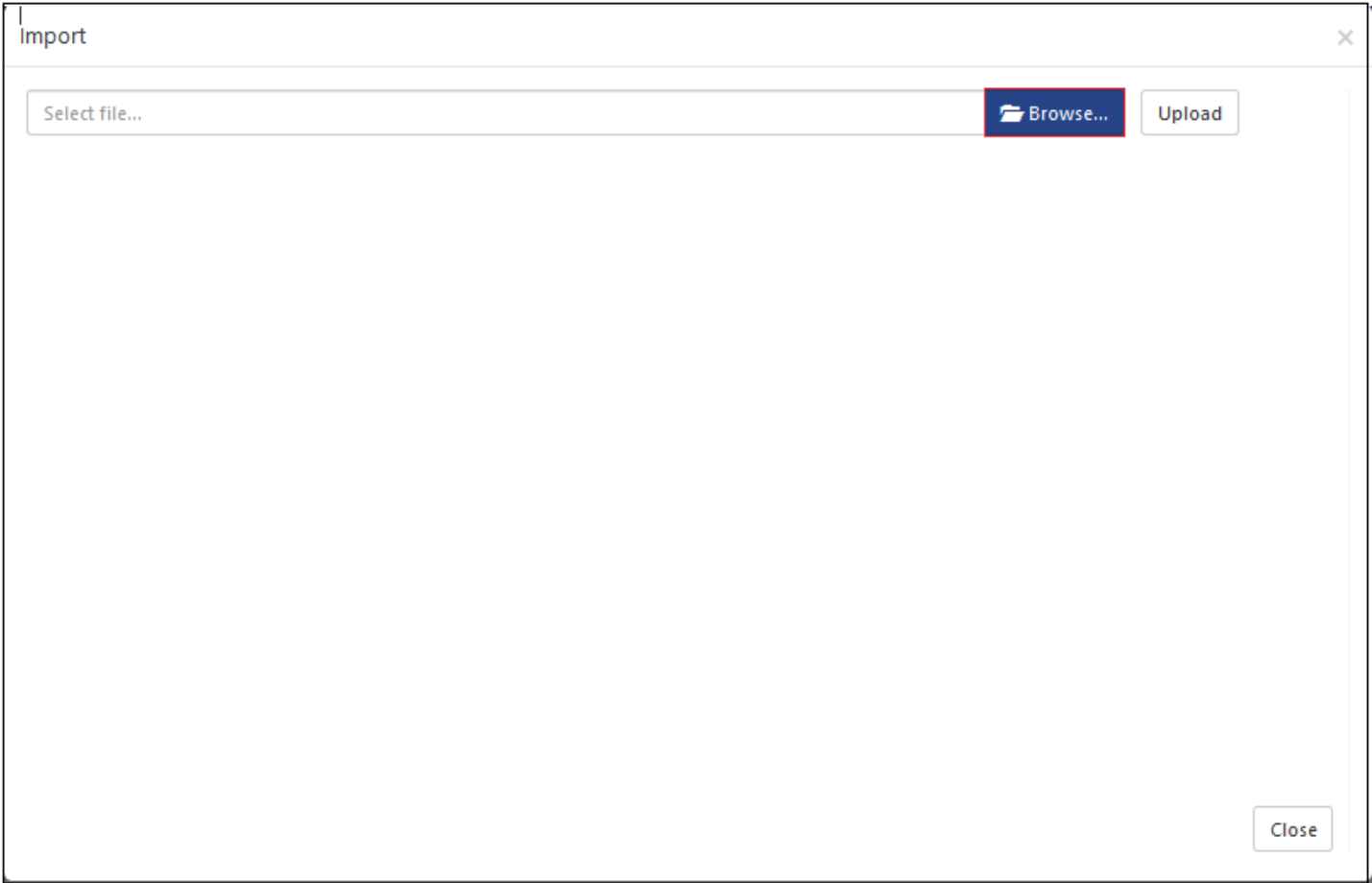


Figure 17

- 4. Locate the file named **KO_SonicWall Spam Filter.etko**.
- 5. Now select all the check box and then click on **Import** option.

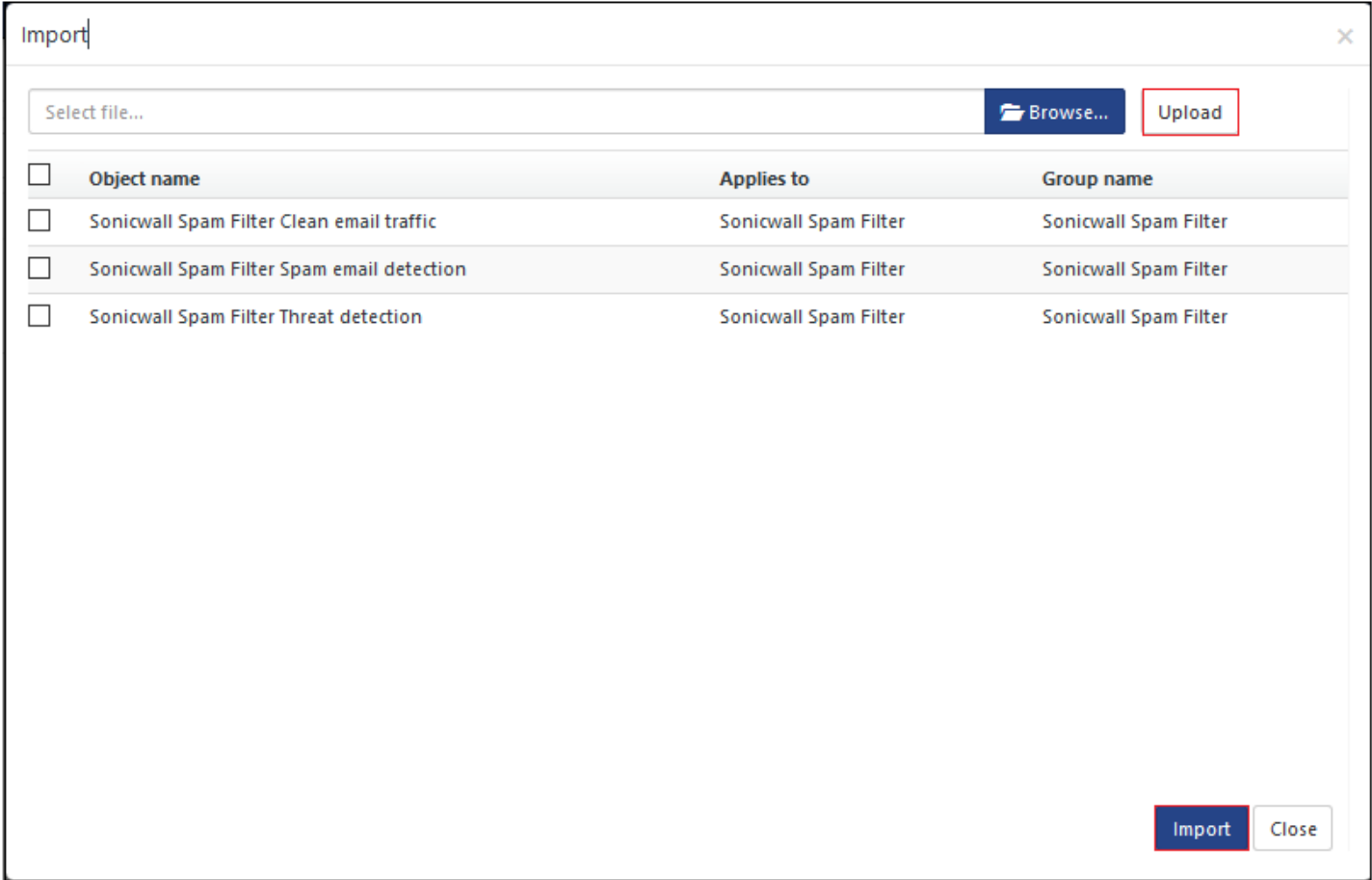


Figure 18

6. Knowledge objects are now imported successfully.

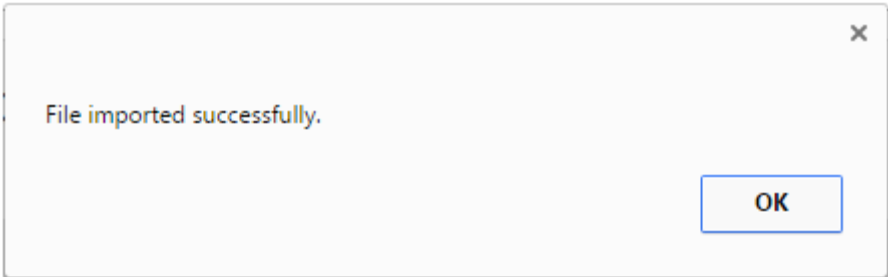


Figure 19

Flex Reports

On EventTracker Control Panel,

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

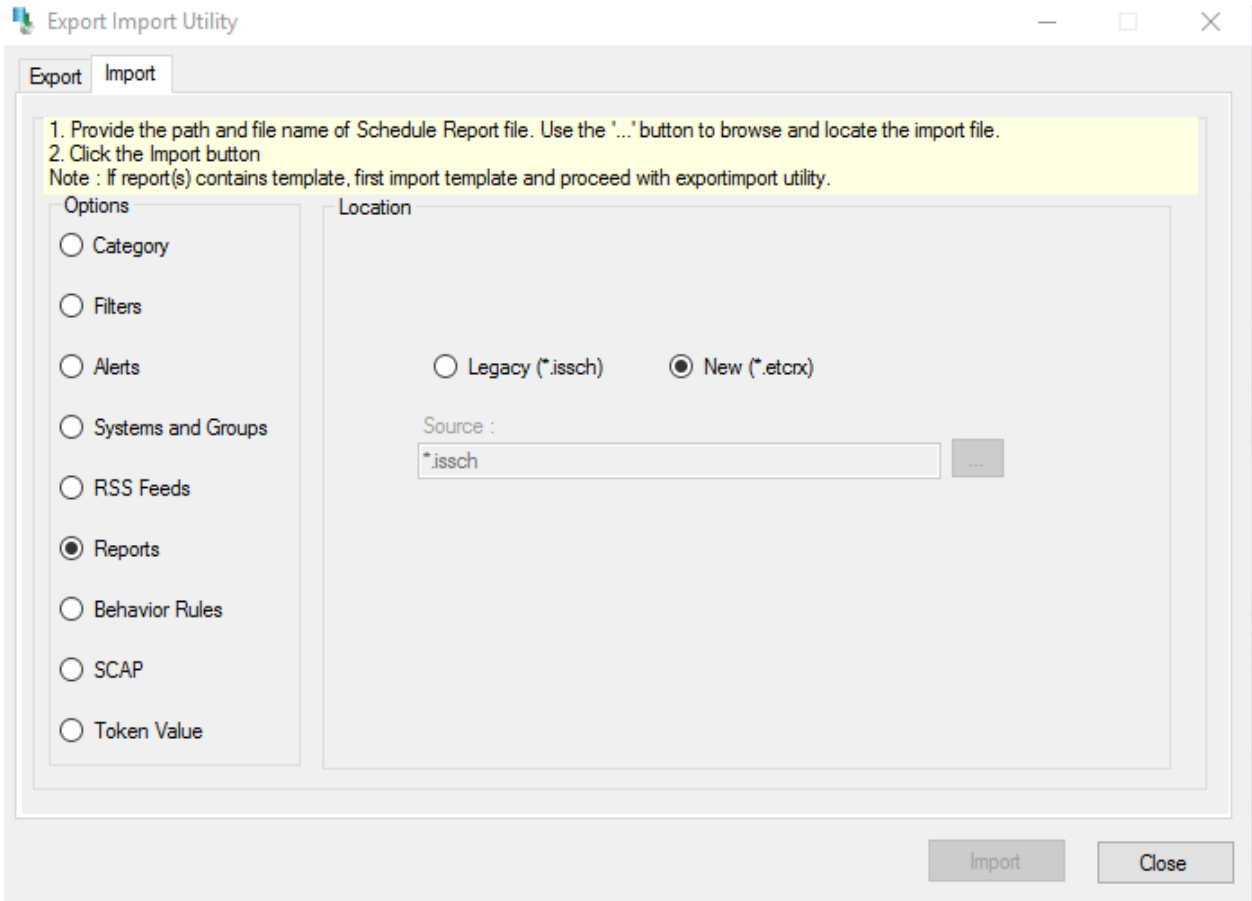


Figure 20

- 2. Locate the file named **Reports_SonicWall Spam Filter.etcrx**, and select all the check box.

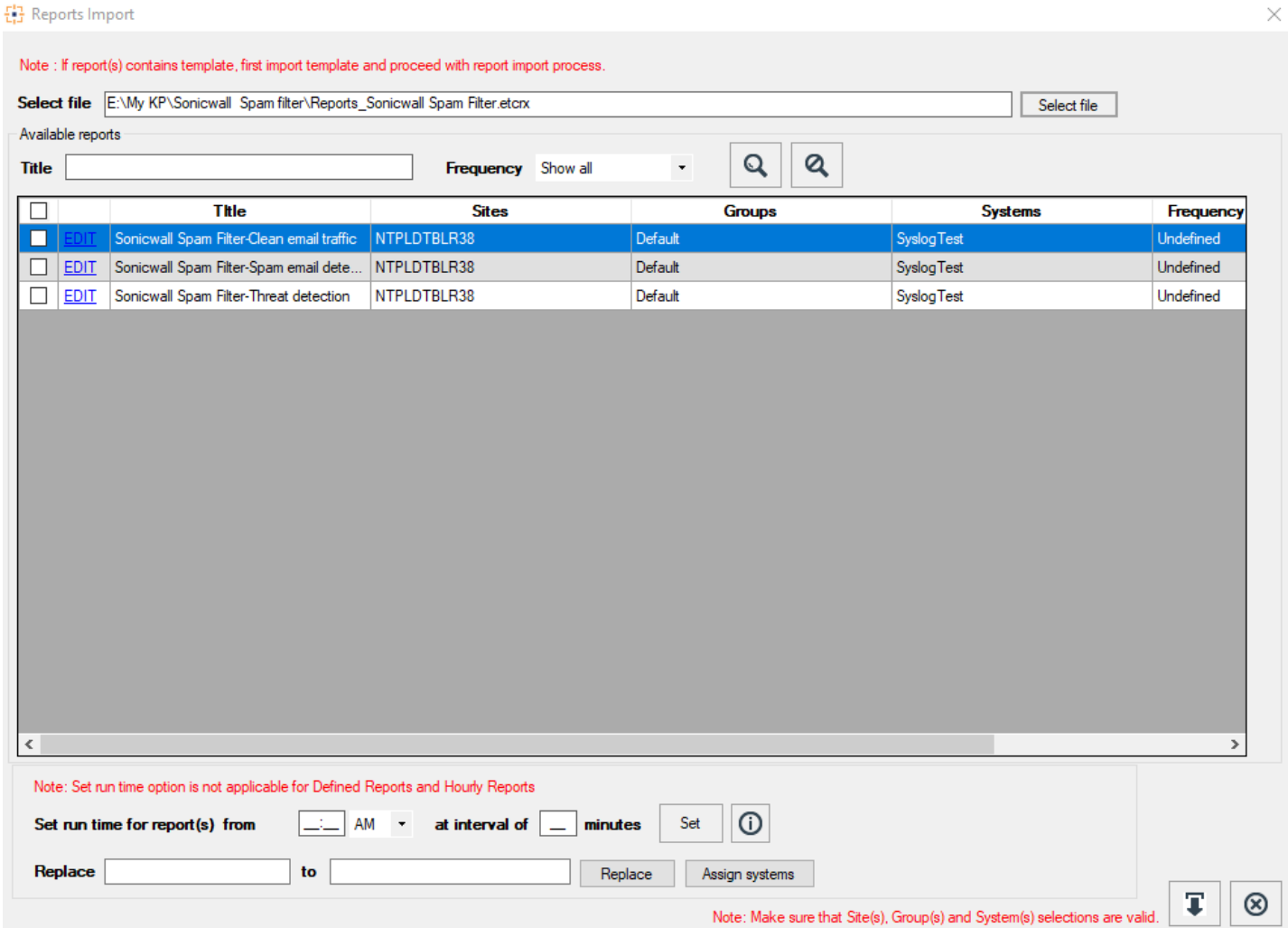


Figure 21

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

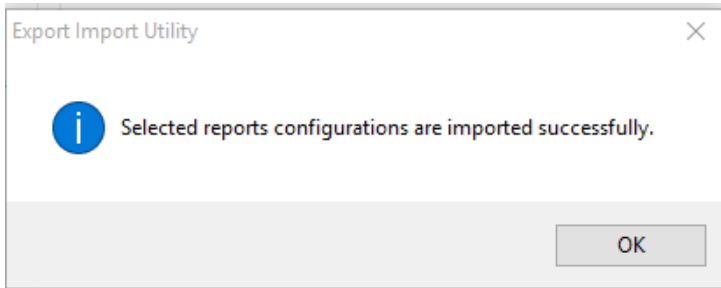


Figure 22

Verify SonicWall Spam Filter knowledge pack in EventTracker

Categories

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

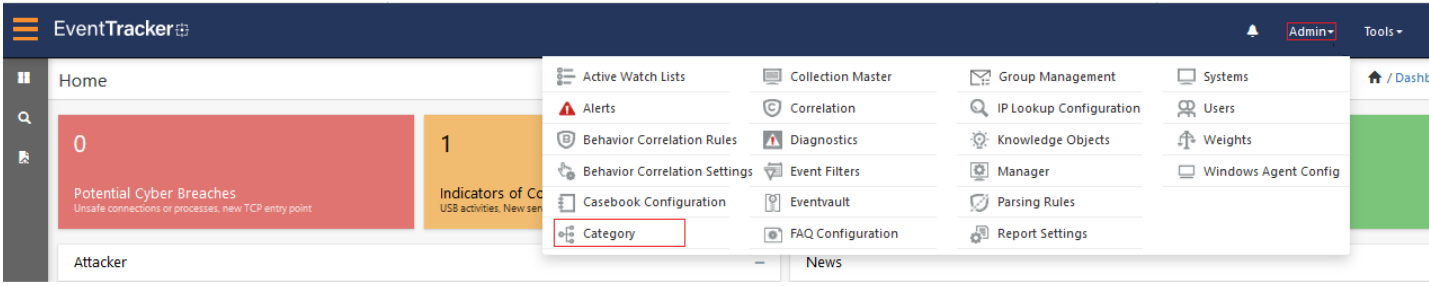


Figure 23

- 3. In **Category Tree** to view imported categories, scroll down and expand SonicWall Spam Filter group folder to view the imported categories.

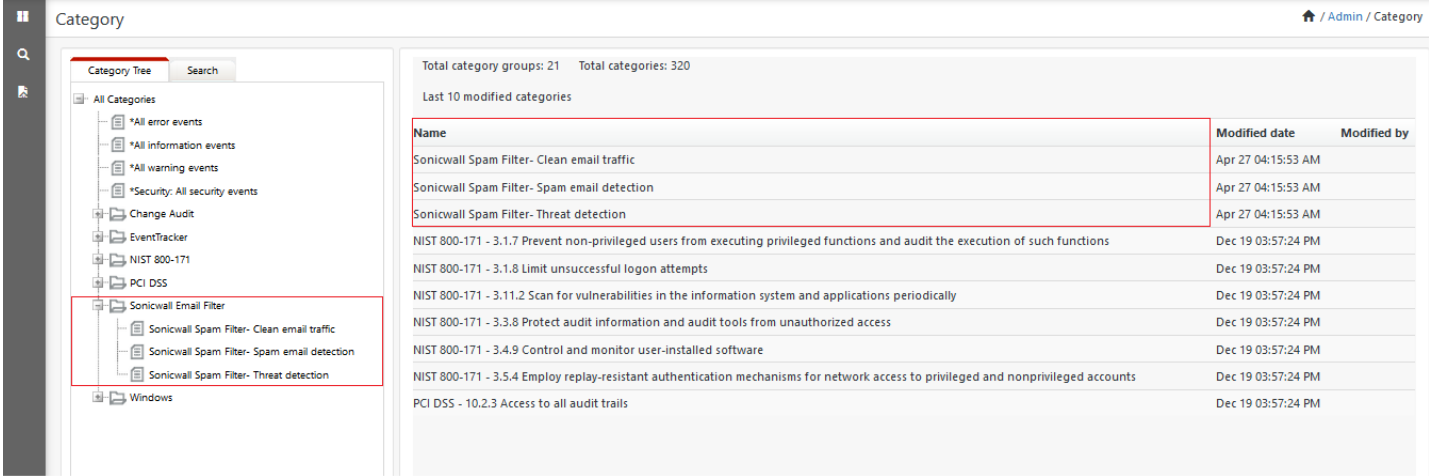


Figure 24

Alerts

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

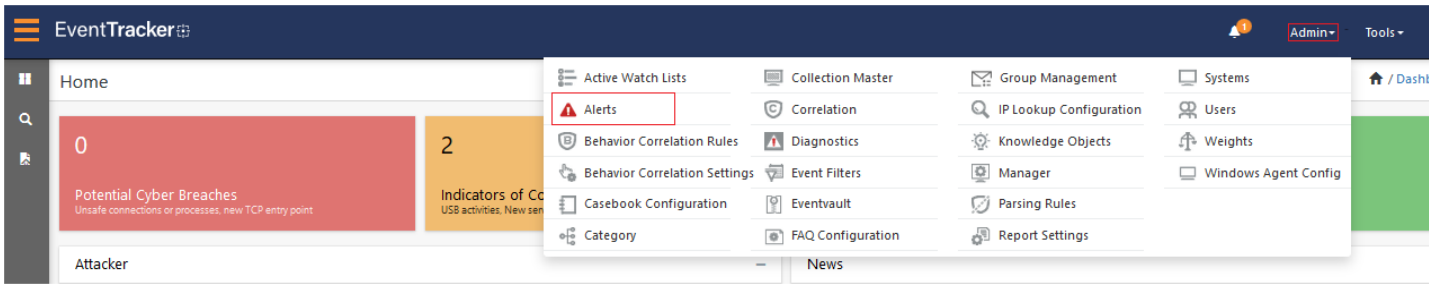


Figure 25

- 3. In the **Search** box, type '**Sonicwall Spam Filter**, and then click the **Go** button. Alert Management page will display all the imported alerts.

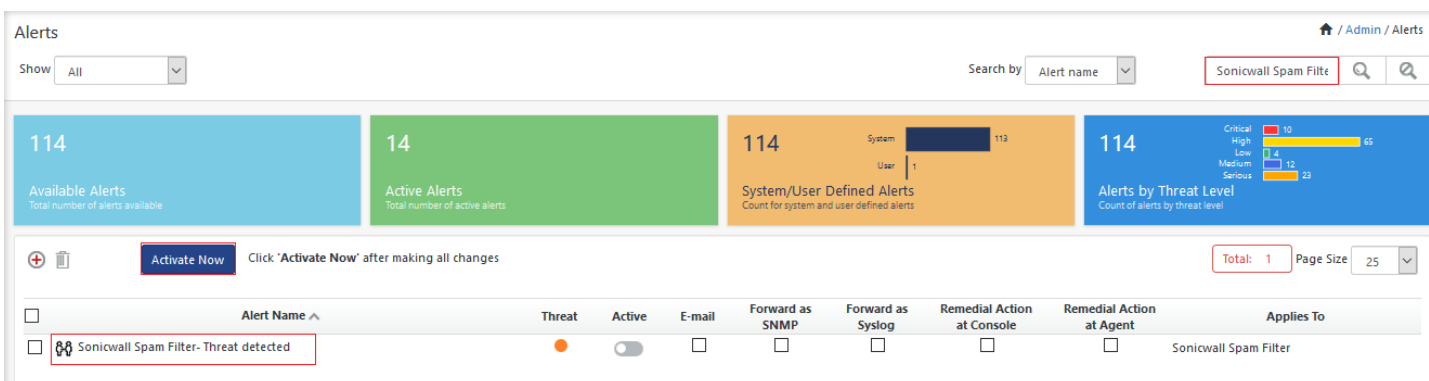


Figure 26

- 4. To activate the imported alerts, select the respective checkbox in the **Active** column. EventTracker displays message box.

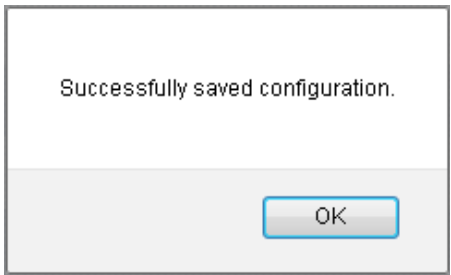


Figure 27

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

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

Token Template

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

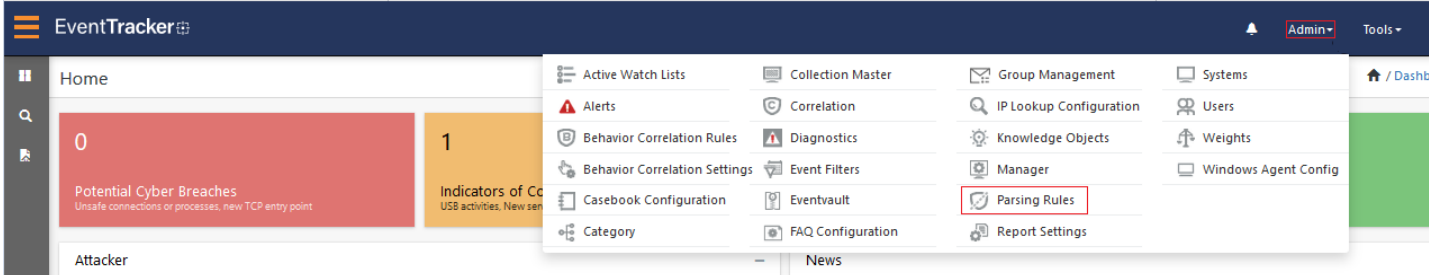


Figure 28

2. On **Template** tab, click on the SonicWall Spam Filter group folder to view the imported Templates.

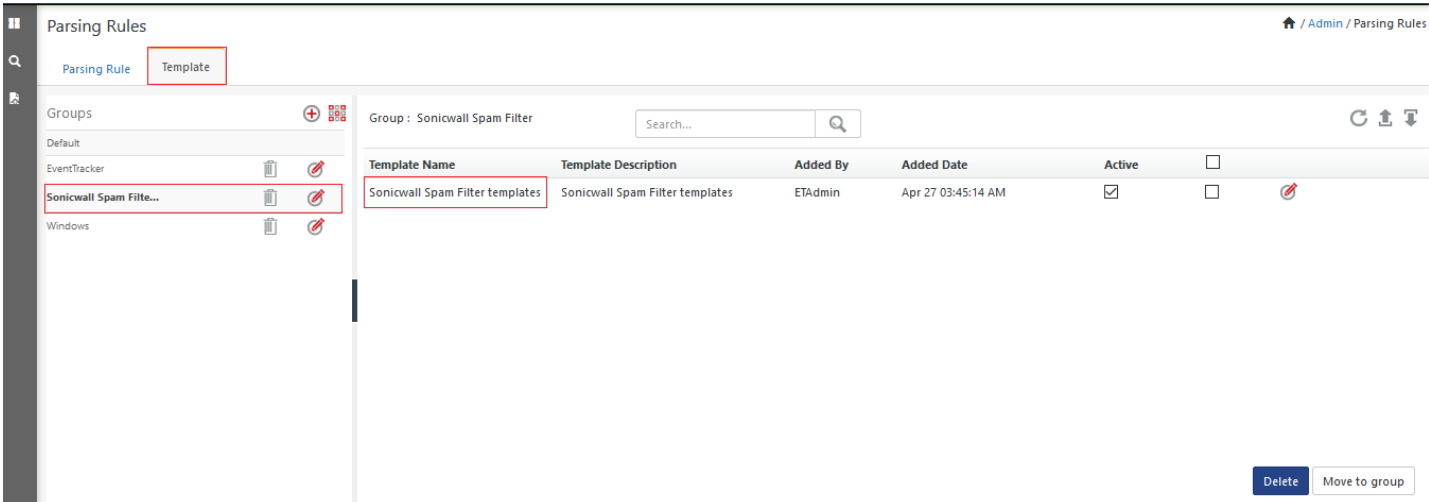


Figure 29

Knowledge Objects

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

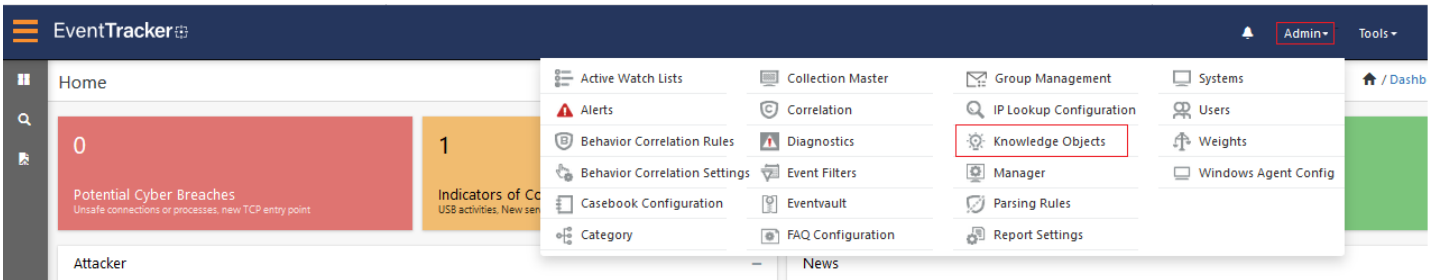


Figure 30

- 2. In the Knowledge Object tree, expand SonicWall Spam Filter group folder to view the imported Knowledge objects.

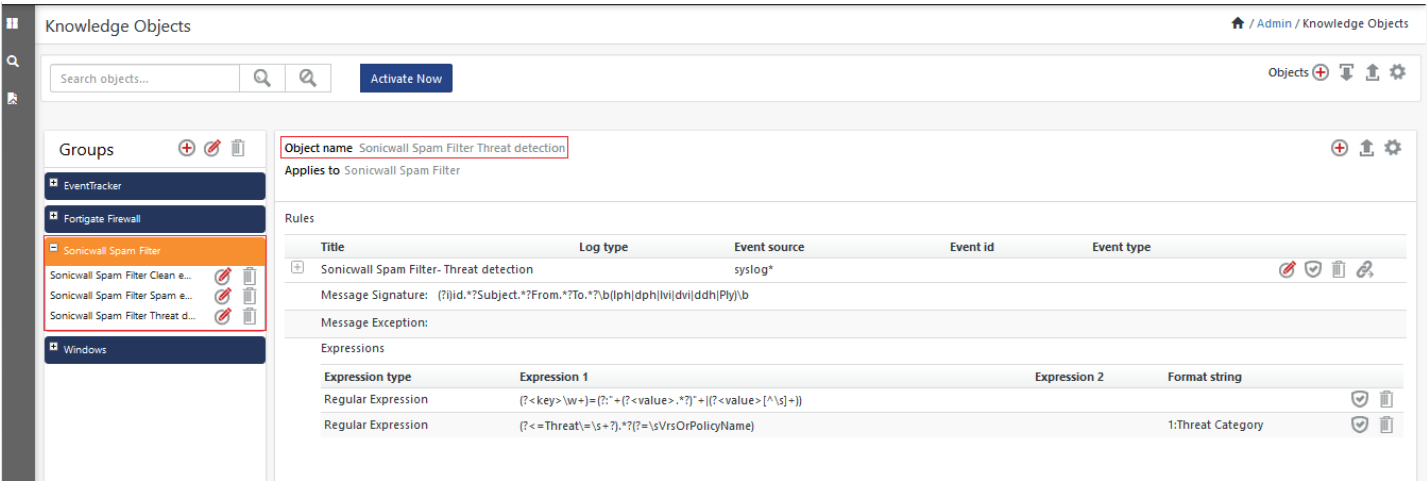


Figure 31

Flex Reports

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

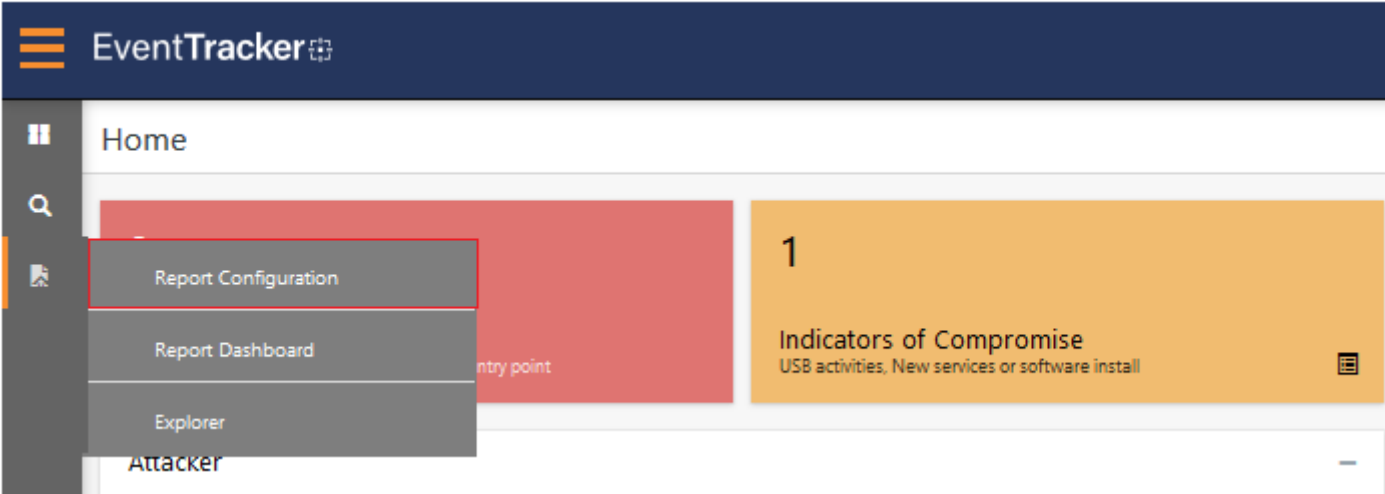


Figure 32

- 2. In **Reports Configuration** pane, select **Defined** option.
- 3. Click on the SonicWall Spam Filter group folder to view the imported SonicWall Spam Filter reports.

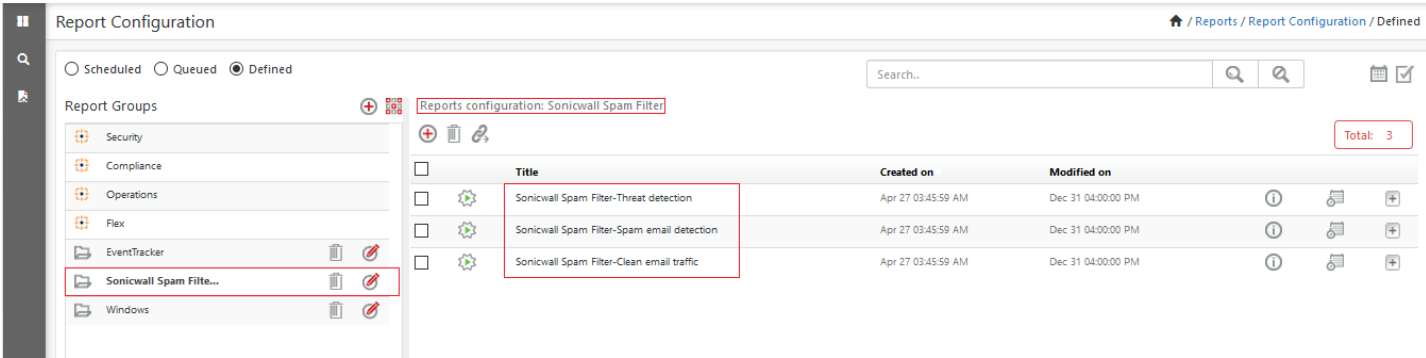


Figure 33

Create Dashlets

NOTE: Below steps given are specific to EventTracker 9 and later.

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

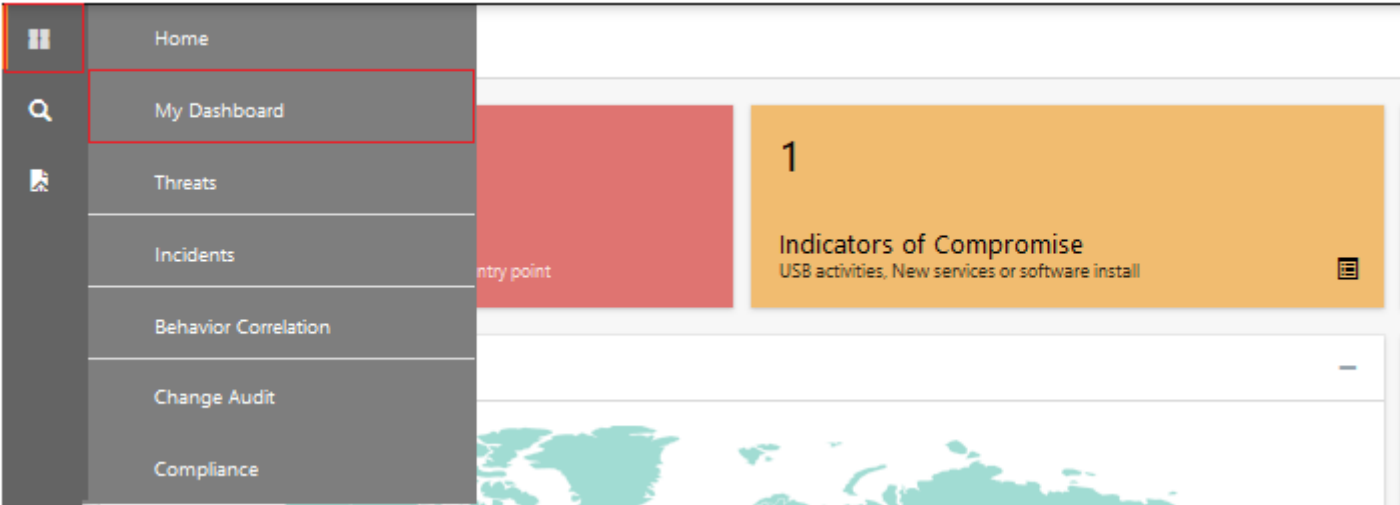


Figure 34

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


Add Dashboard

Title


Description


Save **Delete** **Cancel**

Figure 35

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

Dashlet configuration

Dashlet title 

Note 

Use SQL database

Duration



Lucene Query 

Chart Type Value field setting

Show 

View CIM field mapping

Axis Labels [X-Axis] Label Text

Values [Y-Axis] Value Text

Refine Refine values

Legend [Series] Select

Type to search...

accountwin.12@contoso... 2

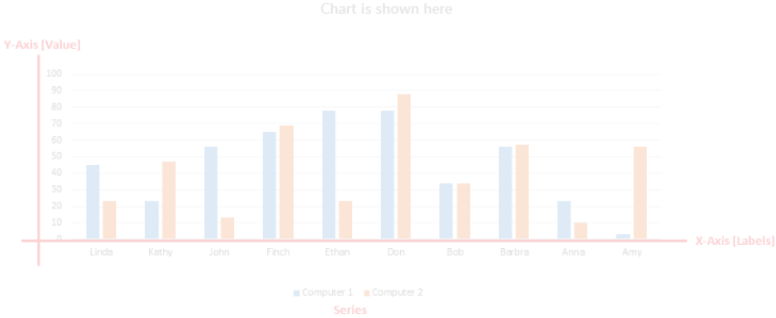


Figure 36

- 5. Select **Saved Search** option and choose the saved search associated with the dashboard that needs to be configured. If **Saved Search** is not required, a valid **lucene query** needs to be entered in the box provided below **Lucene Query** heading.
- 6. Click on **Get CIM Fields** tab to obtain all CIM fields that are mapped.
- 7. Select **Chart Type** from dropdown.
- 8. Select extent of data to be displayed in **Duration** dropdown.
- 9. Select comparable values in **X Axis** with suitable label.
- 10. Select numeric values in **Y Axis** with suitable label.
- 11. Select comparable sequence in **Legend**.
- 12. Click **Test** button to evaluate. Evaluated chart is shown.

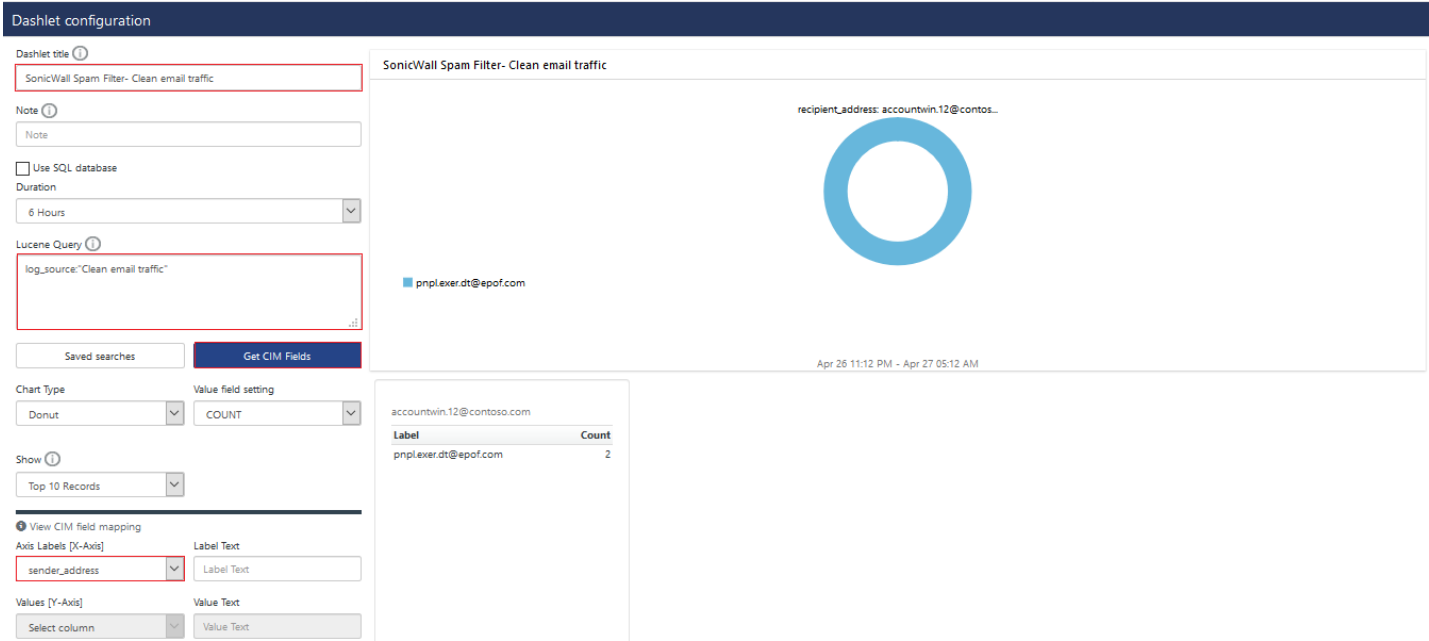


Figure 37

- 13. If satisfied, click **Configure** button.
- 14. Click 'customize' to locate and choose created dashlet.

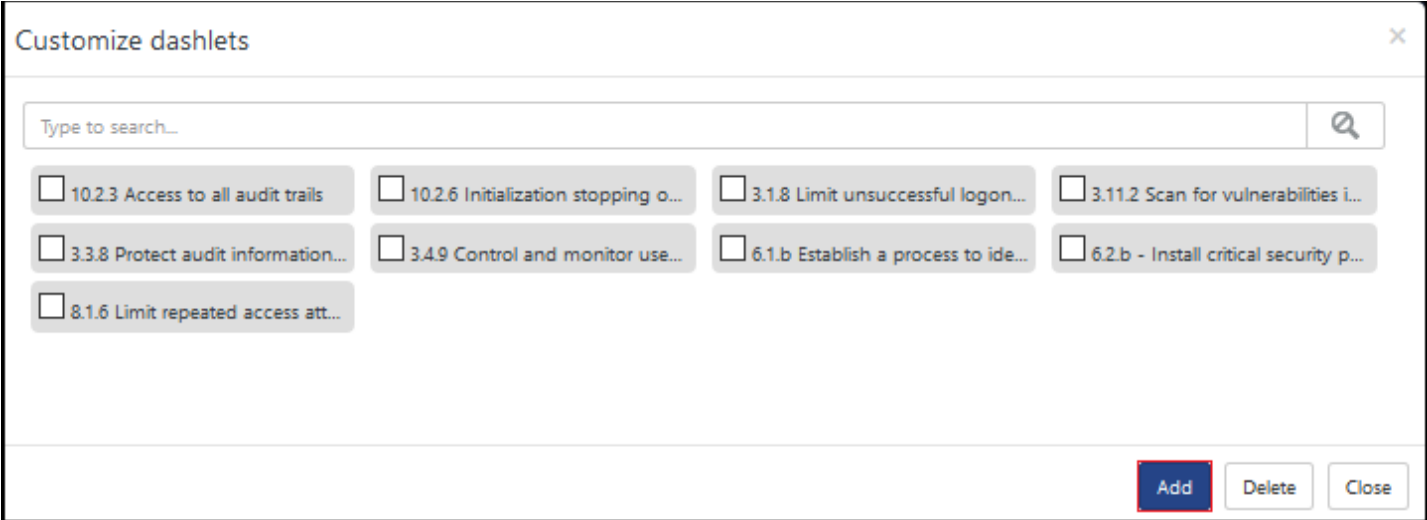



Figure 38

15. Click  to add dashlet to earlier created dashboard.

Sample Flex Dashboards

- **WIDGET TITLE:** SonicWall Spam Filter-Threat detection

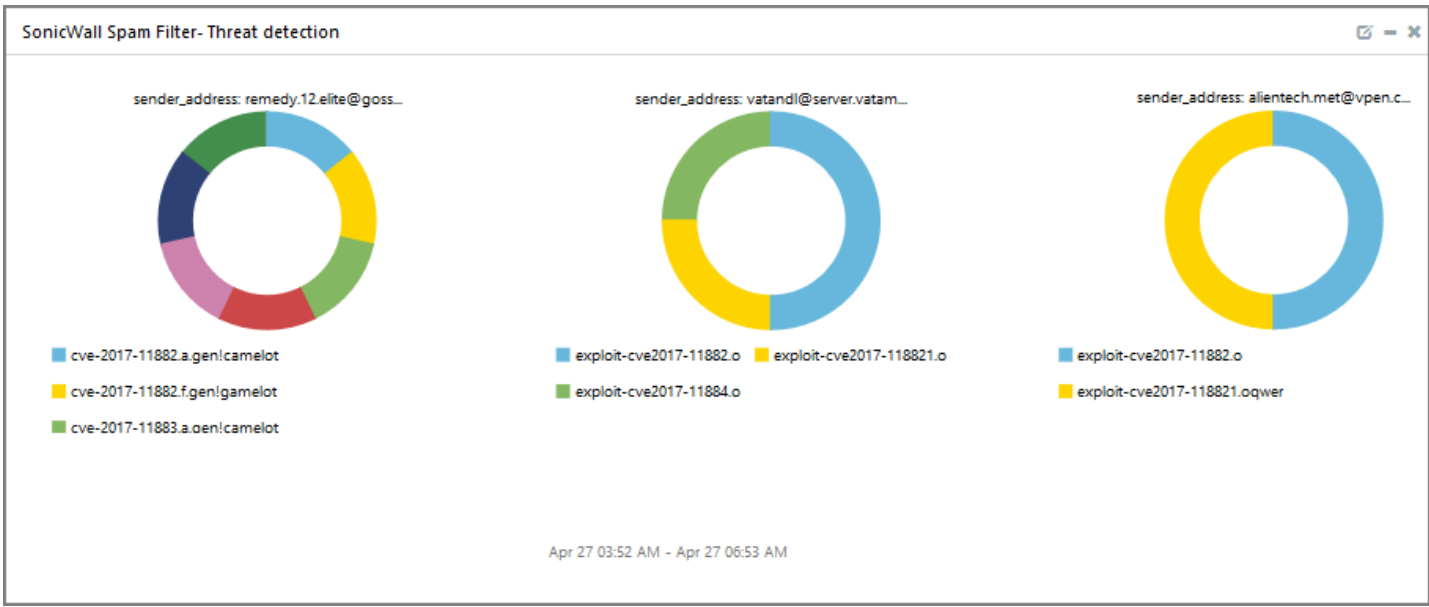


Figure 39

- **WIDGET TITLE:** SonicWall Spam Filter-Spam email detection

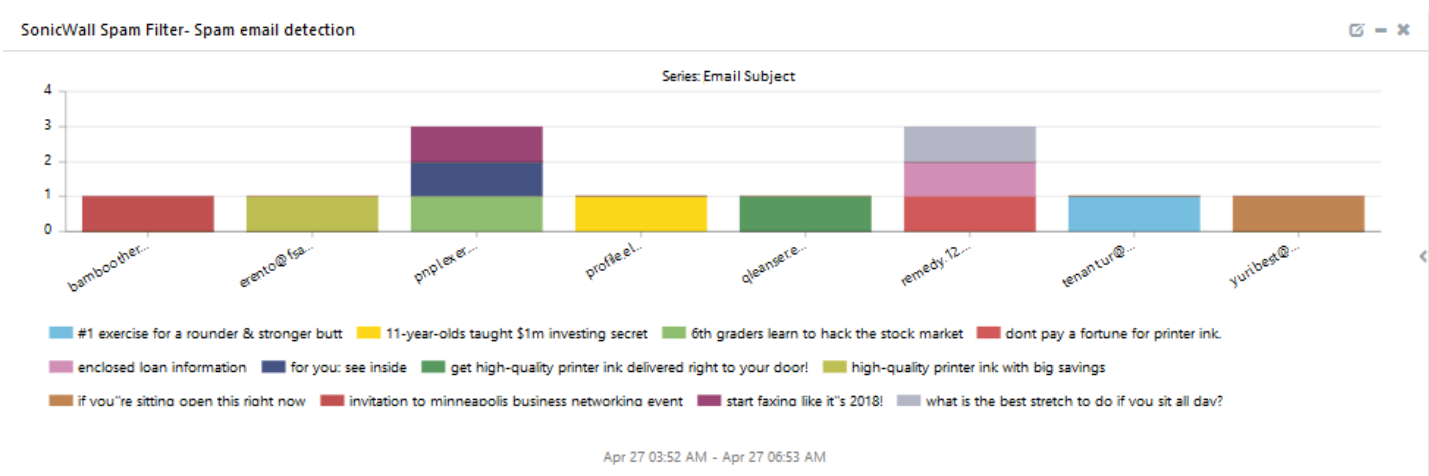


Figure 40