

Integrate SpamTitan Gateway

EventTracker v9.2 and above

Abstract

This guide provides instructions to configure SpamTitan Gateway to send its logs to EventTracker.

Scope

The configuration details in this guide are consistent with EventTracker version v9.2 or above and **SpamTitan Gateway**

Audience

Administrators who are assigned the task to monitor SpamTitan Gateway events using EventTracker.

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

This document is for informational purposes only. Netsurion 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 Netsurion, if its content is unaltered, nothing is added to the content and credit to Netsurion is provided.

Netsurion 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 Netsurion, 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.

© 2020 Netsurion. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Table of Contents

1. Overview.....	3
2. Prerequisites.....	3
3. Integration of SpamTitan Gateway with EventTracker	3
3.1 Configuring SpamTitan Gateway to send the logs to EventTracker	3
4. EventTracker Knowledge Pack	4
4.1 Category.....	4
4.2 Alerts.....	5
4.3 Report	5
4.4 Dashboards	7
5. Importing SpamTitan Gateway knowledge pack into EventTracker	10
5.1 Category.....	11
5.2 Alerts.....	12
5.3 Token template.....	13
5.4 Knowledge Object.....	14
5.5 Report	16
5.6 Dashboards	17
6. Verifying SpamTitan Gateway knowledge pack in EventTracker	20
6.1 Category.....	20
6.2 Alerts.....	21
6.3 Token templates	22
6.4 Knowledge Object.....	23
6.5 Report	24
6.6 Dashboards	25

1. Overview

SpamTitan Gateway is a powerful Anti-Spam appliance that equips network administrators with extensive tools to control mail flow and protect against unwanted email and malware.

EventTracker helps to monitor events from SpamTitan Gateway. EventTracker's reports provide detailed information of all events, alerts are helpful to determine and stop the attack and suspicious activities in real-time, and dashboards will help you to analyze all the security-related events in a single console. Also, we can create and save log search rules/queries under the saved search feature for real-time and historical log search.

2. Prerequisites

- Admin privileges for **SpamTitan Gateway** to configure logging.
- **EventTracker** should be installed in the system.
- Syslog Port 514 should be open.

3. Integration of SpamTitan Gateway with EventTracker

SpamTitan Gateway logs we can get by using syslog.

3.1 Configuring SpamTitan Gateway to send the logs to EventTracker

Syslog is the de facto standard for forwarding log messages in an IP network. All system log messages are written to local log files on SpamTitan Gateway using syslog and logs can be viewed in the Logs tab.

Besides, the log output can also be sent to a remote syslog server. This is useful for administrators who want to use EventTracker to view and analyze log files.

Go to **Settings > Remote syslog** to specify a remote syslog server for mail, interface, and messages log files. The remote servers defined must run a logging daemon compatible with the syslog protocol.

To specify a remote server:

1. Click **Enable** to turn the remote syslog status to ON.
2. Enter the **EventTracker's address** in the **syslog Server:** field.

Note:

To specify a port, put a colon after the remote syslog address, and add the port number. For example, **192.168.3.120:5826**

3. Click **Save**.

The screenshot displays a configuration interface for Syslog. It consists of three vertically stacked sections, each with an orange header bar:

- Remote Mail Syslog:** The 'Status' is 'ON' (in green). There is a 'Syslog Server' input field and buttons for 'Disable' and 'Save'.
- Remote Interface Syslog:** The 'Status' is 'ON' (in green). There is a 'Syslog Server' input field and buttons for 'Disable' and 'Save'.
- Remote Messages Syslog:** The 'Status' is 'ON' (in green). There is a 'Syslog Server' input field and buttons for 'Disable' and 'Save'.

Figure 1

4. 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 to support SpamTitan Gateway.

4.1 Category

Saved searches are designed to quickly parse/filter logs and allow the user to see only specific events related to:

- **SpamTitan Gateway - Infected Emails:** This category for SpamTitan Gateway allows users to quickly filter and display the events related to Infected emails.
- **SpamTitan Gateway - Noqueue Email:** Using this category for SpamTitan Gateway we can quickly filter and display the events related to Noqueue emails.

- **SpamTitan Gateway - Passed Emails:** This category provides quick search and filter related to the Passed email events.
- **SpamTitan Gateway - Spam Emails:** This category for SpamTitan Gateway allows users to quickly filter and display the events related to Spam emails.
- **SpamTitan Gateway - Virus detected in the mail:** This category provides the quick filter and logs search related to Virus detected events.

4.2 Alerts

Alerts are triggered when an event received is identified as critical and requires immediate notification. Such as

- **SpamTitan Gateway - Virus detected in Infected mails:** This alert is triggered by EventTracker when SpamTitan Gateways detect any Virus/Malware in mails.
- **SpamTitan Gateway - Mail with Coronavirus/Covid-19 subject:** This alert is triggered by EventTracker when SpamTitan Gateways mail subject contains information of Coronavirus or Covid-19.

4.3 Report

- **SpamTitan Gateway - Passed Emails:** This report provides detailed information on SpamTitan Gateway Passed emails events generated by SpamTitan Gateway. This report contains information such as Source IP addresses, Mail sender information, Mail recipient, Mail Header information, Mail Subject, etc.

LogTime	Source IP	Mail Sender	Mail Recipient	From Header	Mail Subject	Rate
07/13/2020 03:22:02 PM	192.28.153.136	673-UWY-229.0.464899.0.0.30 9332.9.13623248@bounce1.xyz.com	Robert.p@contoso.com	Silicon Valley Business Journal <reply@news.bounce1.xyz.com>	Coronavirus Global News.	none
07/13/2020 03:22:02 PM	192.1688.153.136	673-UWY-229.0.464899.0.0.30 9332.9.13623248@yahoo.com	Peter.p@contoso.com	Silicon Valley Business Journal <reply@news.yahoo.com>	Covid-19 Vaccene update.	none

Figure 2

- **SpamTitan Gateway - Spam Emails:** This report provides detailed information on SpamTitan Gateway events generated by SpamTitan Gateway. This report contains information such as Source IP addresses, Source Port, Destination IP address, Mail Sender and Recipient address, Reason, Size, Action taken on spam mail, Quarantine details, etc.

LogTime	Source IP Address	Source Port	Destination IP	Sender Address	Recipient address	Reason	Size	Action	Quarantine	Hits
07/13/2020 03:22:01 PM	21.11.10.890	36912	21.11.10.890	bounce-9493_HTML-61583723-560396-7234512-22@bounce.replyien.com	tim.cook@contoso.com	NoBounceInbound,Quarantined	86058	Blocked	C/spam-CQmVjvelsddx	4.93
07/13/2020 03:22:02 PM	22.11.10.20	36912	22.11.10.20	Corona-VirusHTML-61583723-560396-7234512-22@abc.replycom	tim.cook@contoso.com	NoBounceInbound,Quarantined	86058	Blocked	C/spam-CQmVjvelsddx	4.93

Figure 3

- SpamTitan Gateway - Infected Emails with Virus:** This report provides detailed information on SpamTitan Gateway Response events generated by SpamTitan Gateway. This report contains information such as Scanner name, Sender-Recipient address, source IP address, source port, Virus name, size, hits and action taken on the mail, etc.

LogTime	Scanner	Recipient address	Sender Address	Source IP	Source Port	Destination IP	Virus Details	Size	Hits	Action	Quarantine	Reason
07/13/2020 04:42:42 PM	BitDefender	Pter.s@contoso.com	grace.quintero@zoom.net	200.7.100.32	57045	123.81.234.10	Trojan.Cryxos.4060	141392	-	Blocked	H/virus-H5wyjc3l8_n7	DiscardedInbound,Quarantined
07/13/2020 04:42:42 PM	BitDefender	adam.s@contoso.com	Hunter.X@Yamaha.net	12.7.100.20	57045	230.81.234.113	Trojan.Cryxos.4058	141392	-	Blocked	H/virus-H5wyjc3l8_n7	DiscardedInbound,Quarantined

Figure 4

- SpamTitan Gateway - Noqueue Emails:** This report provides detailed information on SpamTitan Gateway Noqueue events generated by SpamTitan Gateway. This report contains information such as Action taken on Noqueue mails, Protocol types, Mail Recipient and Sender addresses, source IP address, etc.

LogTime	Action	Protocol	Recipient address	Sender Address	Source IP
07/13/2020 03:22:02 PM	filter	ESMTP	Admin.Server@contoso.com	673-UWY-229.0.464899.0.0.309332.9.13623248@bounce1.token.com	192.168.15.16
07/13/2020 03:22:02 PM	filter	ESMTP	Robert.wilson@contoso.com	673-UWY-229.0.464899.0.0.309332.9.13623248@bounce12.gmail.com	192.168.15.16
07/13/2020 04:42:42 PM	filter	ESMTP	Admin.Server@contoso.com	673-UWY-229.0.464899.0.0.309332.9.13623248@bounce1.token.com	192.168.15.16

Figure 5

4.4 Dashboards

- SpamTitan Gateway - All Events

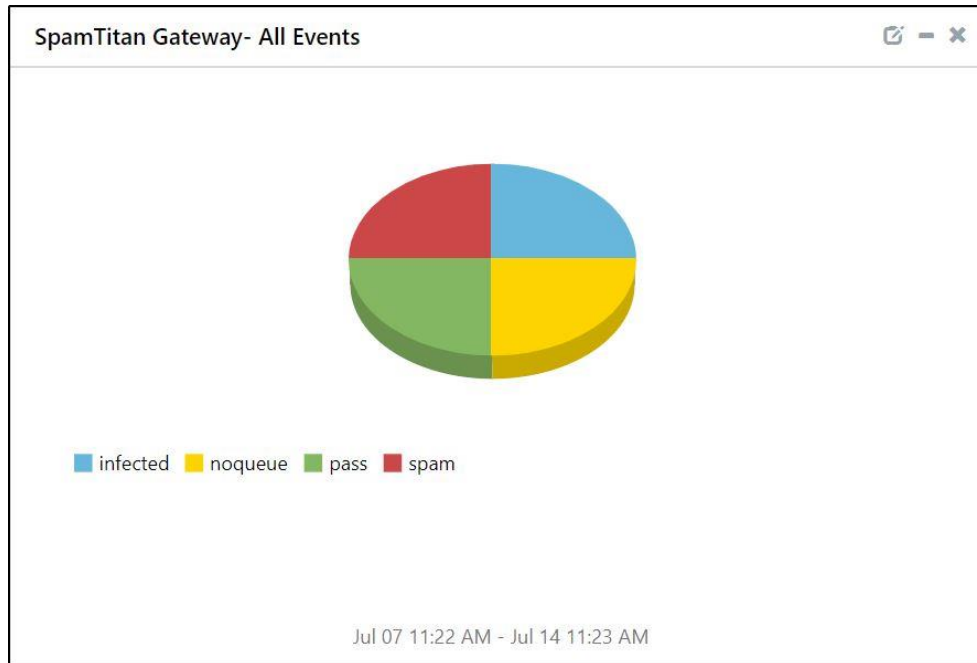


Figure 6

- SpamTitan Gateway - Action taken on mails



Figure 7

- **SpamTitan Gateway - Virus detected in infected mails**

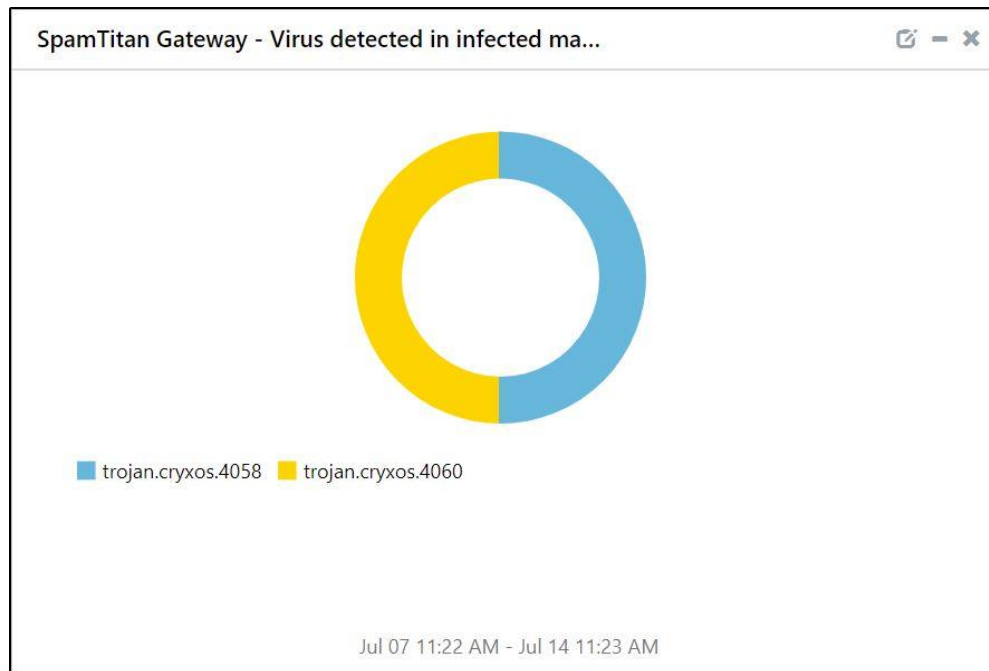


Figure 8

- **SpamTitan Gateway – Virus detected by Source IP**

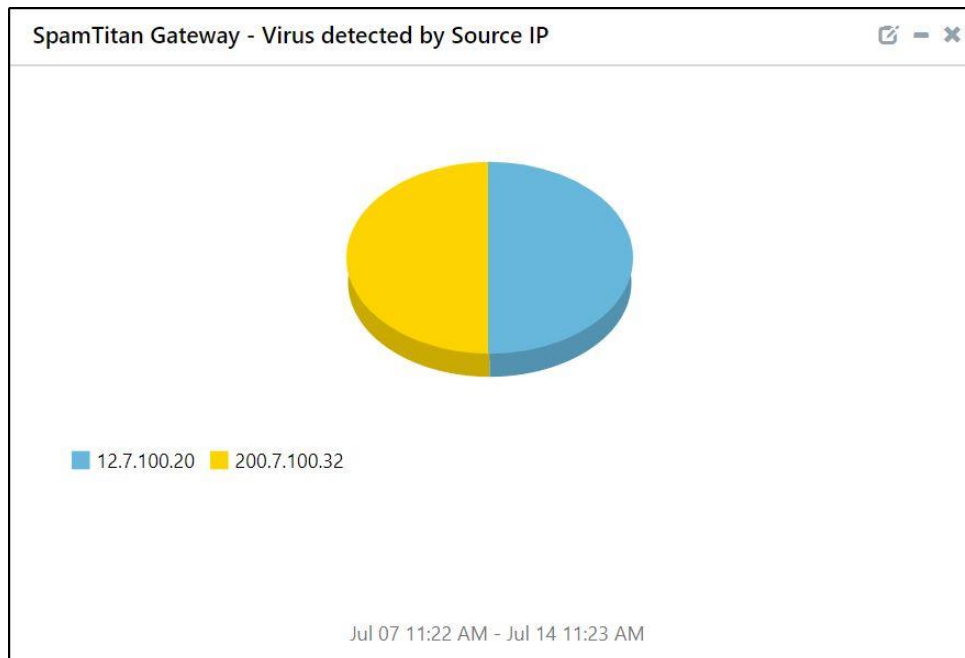


Figure 9

- SpamTitan Gateway – Top Suspicious Mail Sender



Figure 10

- SpamTitan Gateway – Top Suspicious mail Recipient

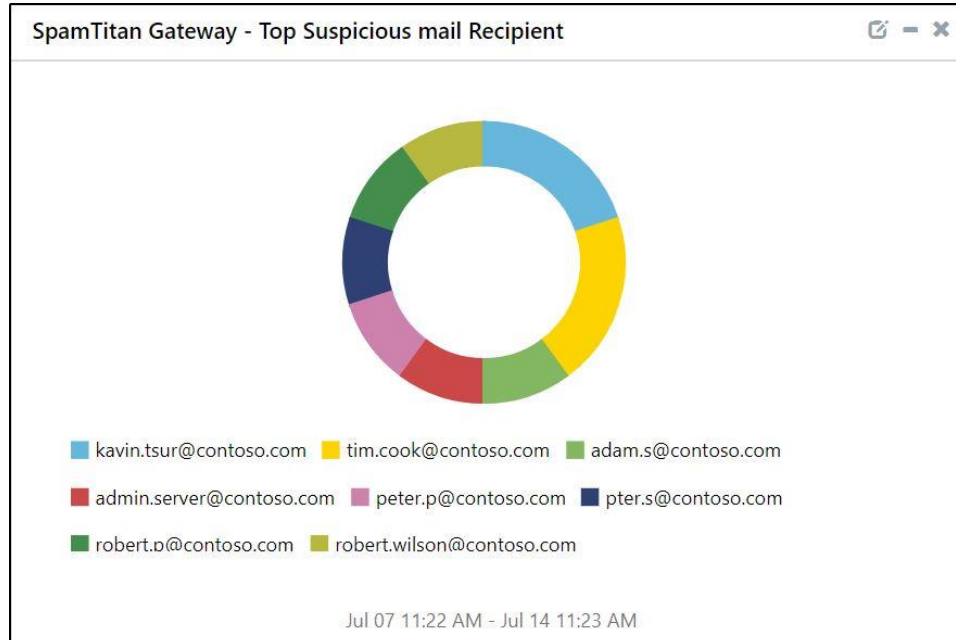
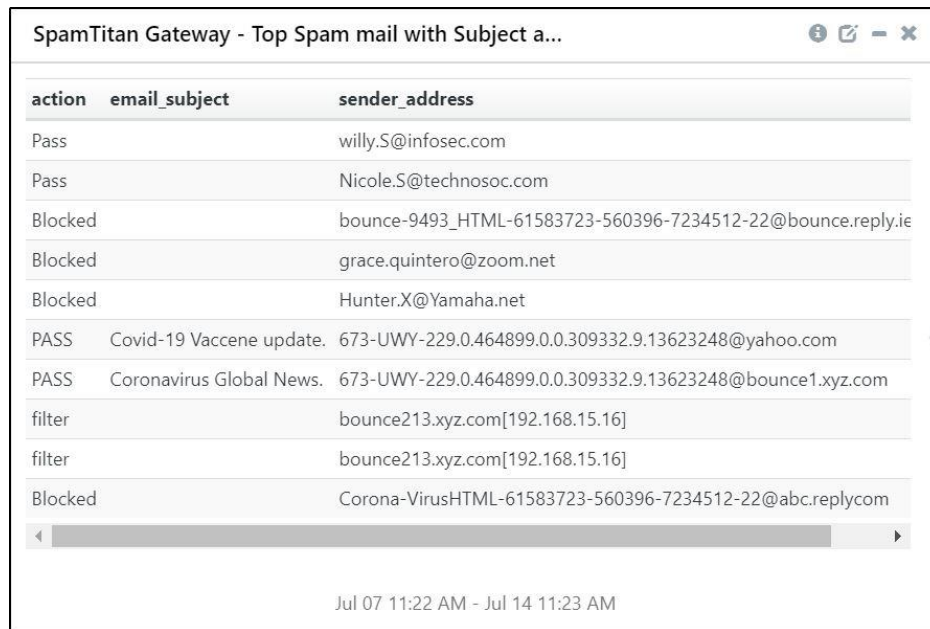


Figure 11

- **SpamTitan Gateway - Top Spam mail with Subject and Sender SpamTitan Gateway**



action	email_subject	sender_address
Pass		willy.S@infosec.com
Pass		Nicole.S@technosoc.com
Blocked		bounce-9493_HTML-61583723-560396-7234512-22@bounce.reply.ie
Blocked		grace.quintero@zoom.net
Blocked		Hunter.X@Yamaha.net
PASS	Covid-19 Vaccene update.	673-UWY-229.0.464899.0.0.309332.9.13623248@yahoo.com
PASS	Coronavirus Global News.	673-UWY-229.0.464899.0.0.309332.9.13623248@bounce1.xyz.com
filter		bounce213.xyz.com[192.168.15.16]
filter		bounce213.xyz.com[192.168.15.16]
Blocked		Corona-VirusHTML-61583723-560396-7234512-22@abc.replycom

Jul 07 11:22 AM - Jul 14 11:23 AM

Figure 12

5. Importing SpamTitan Gateway knowledge pack into EventTracker

NOTE: Import knowledge pack items in the following sequence:

- Category
- Alert
- Token template
- Knowledge Object
- Report
- Dashboard

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

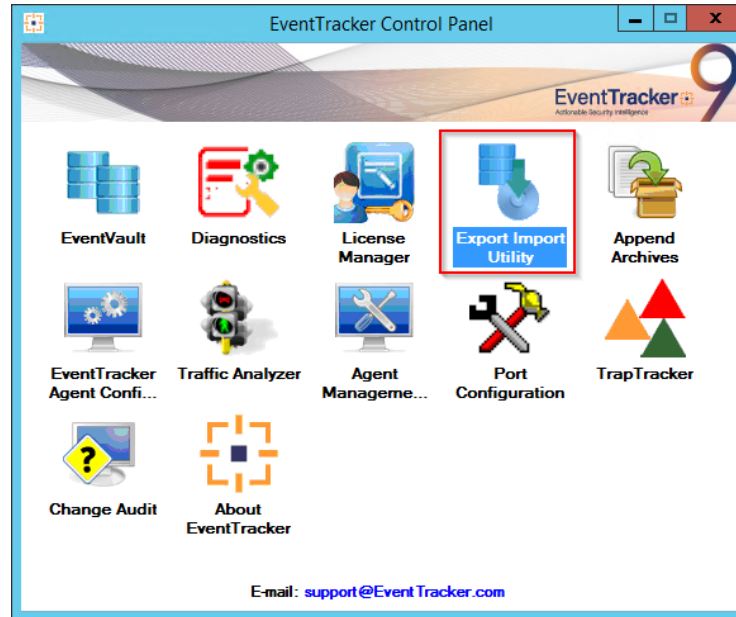


Figure 13

3. Click the **Import** tab.

5.1 Category

1. Click **Category** option, and then click **Browse**. ...

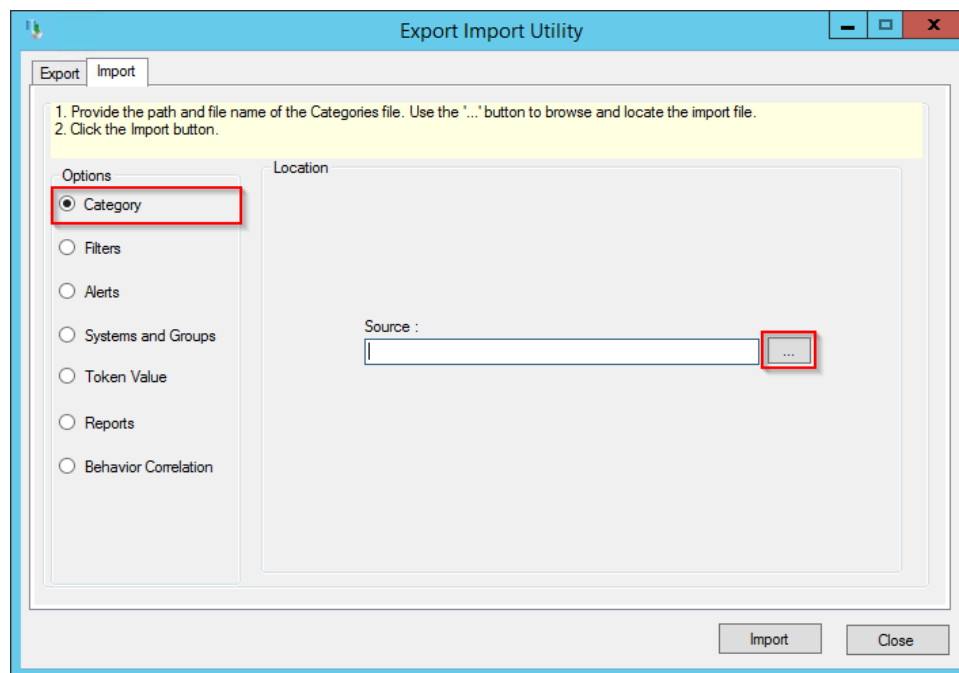


Figure 14

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

EventTracker displays a success message.

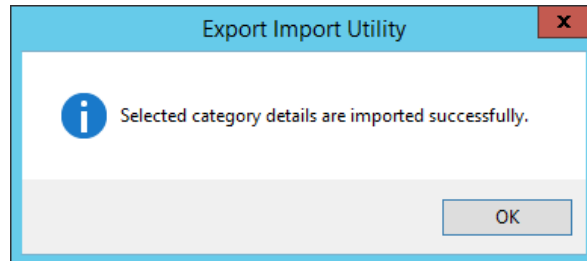



Figure 15

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

5.2 Alerts

1. Once you have opened "Export-Import Utility" via "EventTracker Control Panel", click **Alert** option, and then click Browse. 
2. Navigate to the knowledge pack folder and select the file with the extension ".isalt", e.g. "Alerts_SpamTitan Gateway.isalt" and then click "Import".

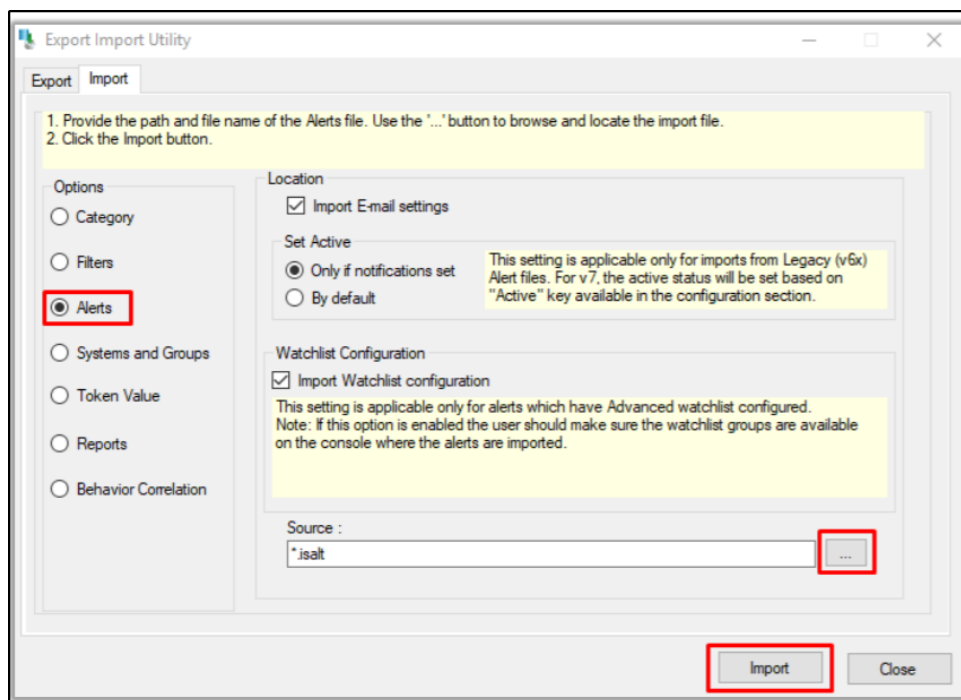


Figure 16

3. EventTracker displays a success message:

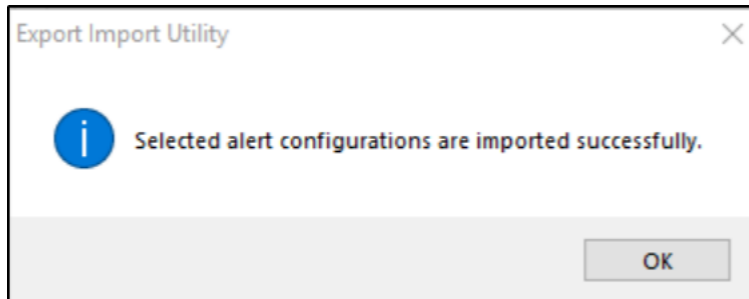


Figure 17

5.3 Token template

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

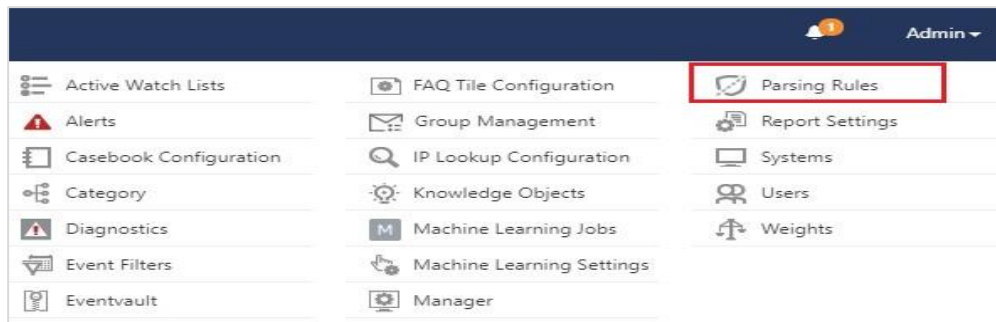


Figure 18

2. Click **Template**.

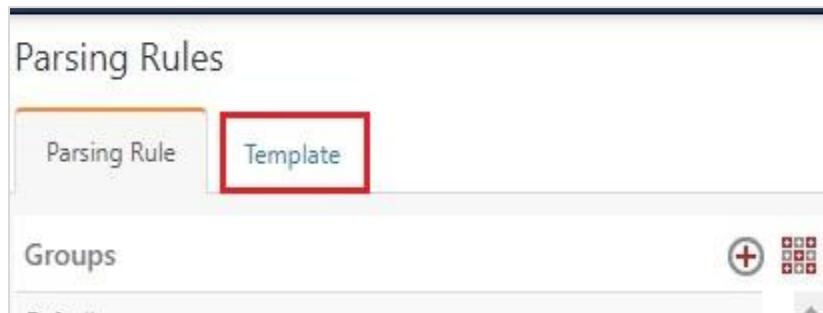


Figure 19

3. To import the token template, click **Import**.



Figure 20

4. Locate the **Templates_SpamTitan Gateway.ettd** type file by clicking the **Browse** button, enable all the templates and click **import**.



Figure 21

5. Click **OK**.

5.4 Knowledge Object

1. Click **Knowledge objects** under the Admin option in the EventTracker manager page.

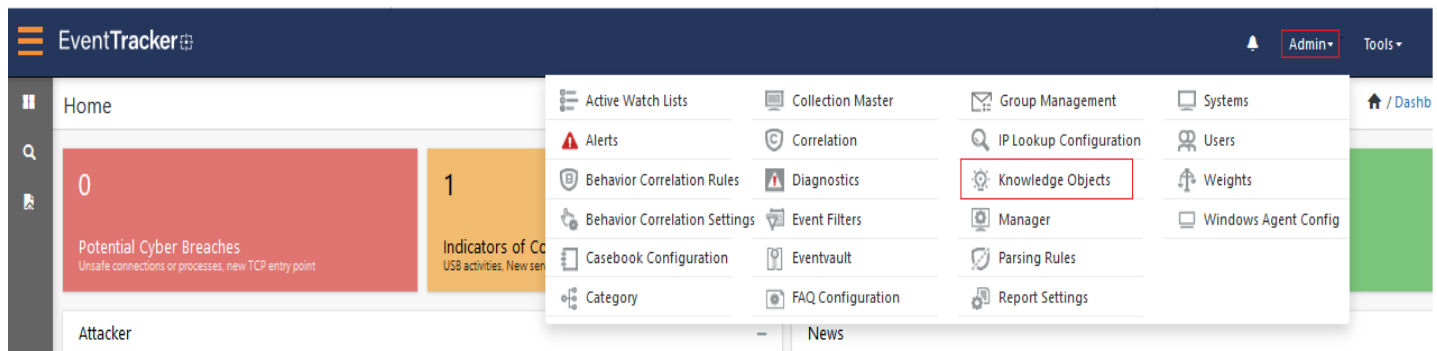


Figure 22

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

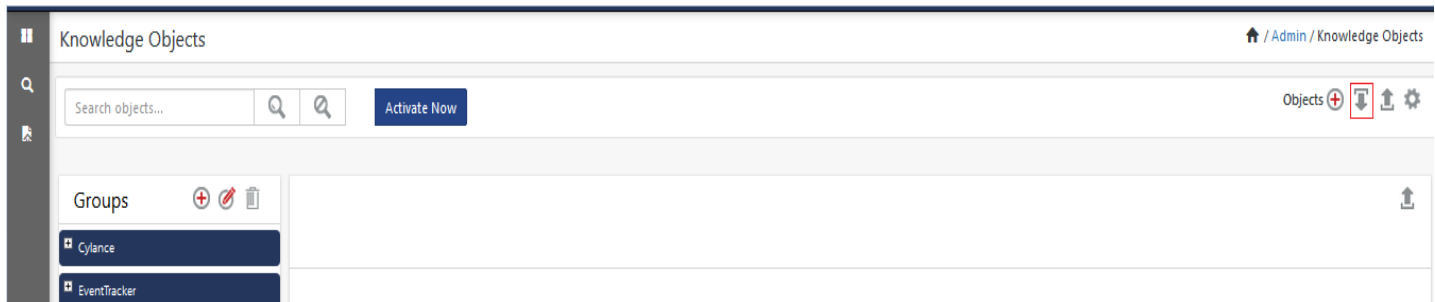


Figure 23

3. Click **Browse**.

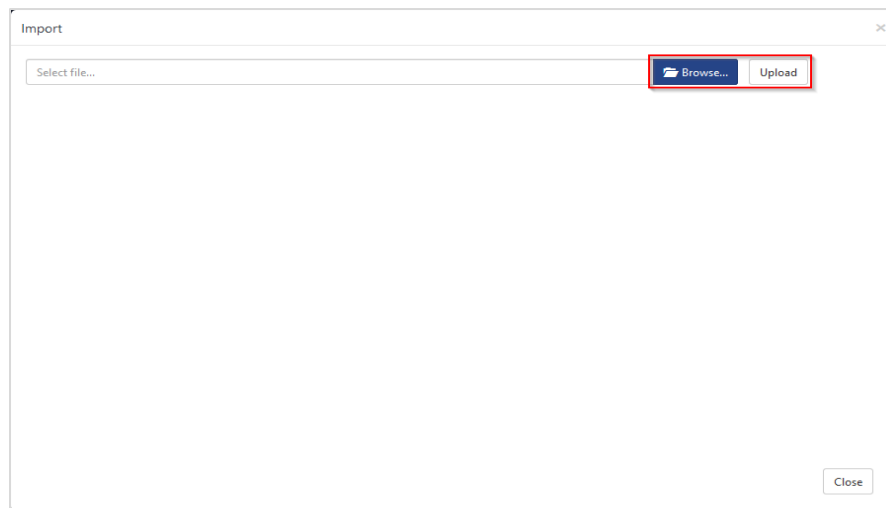


Figure 24

4. Locate the file named **KO_SpamTitan Gateway.etko**.

5. Now select the checkbox and then click  **Import**.

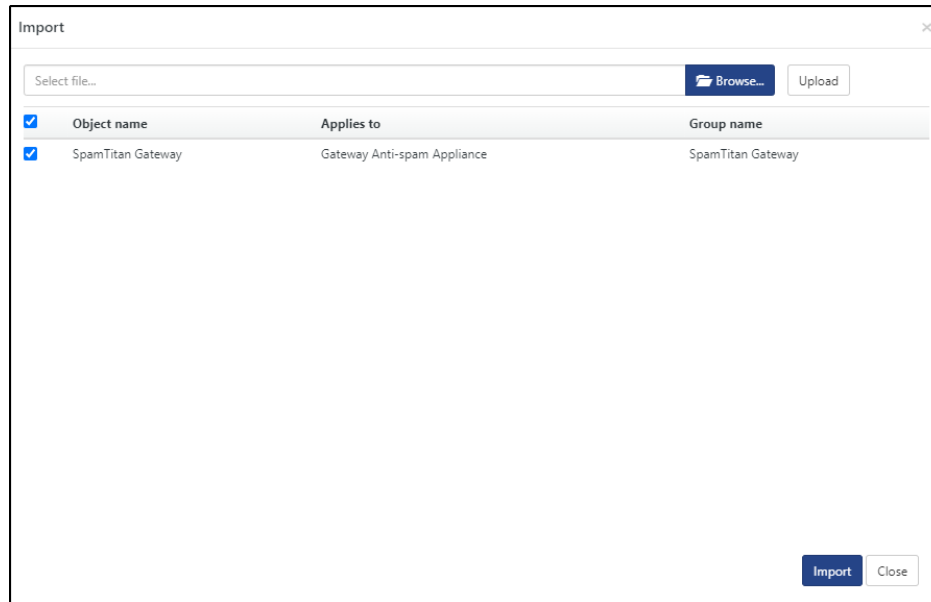


Figure 25

6. Knowledge objects are now imported successfully.

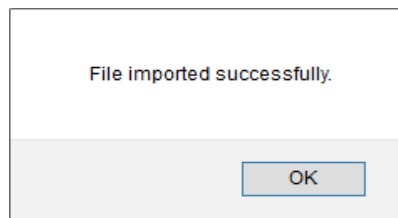


Figure 26

5.5 Report

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

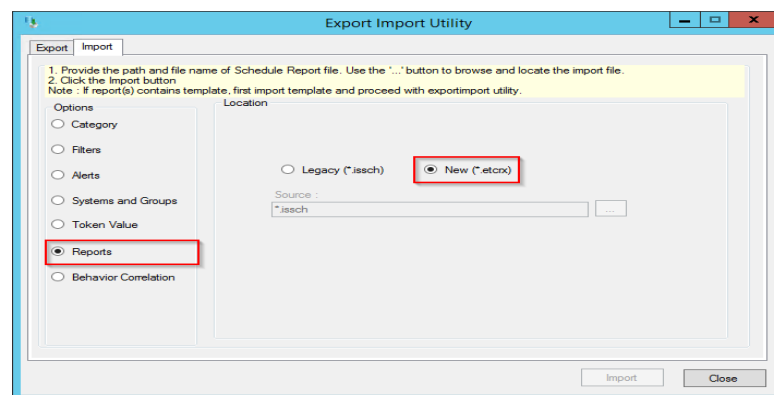


Figure 27

2. Locate the file named **Reports_SpamTitan Gateway.etcx** and select the checkbox.

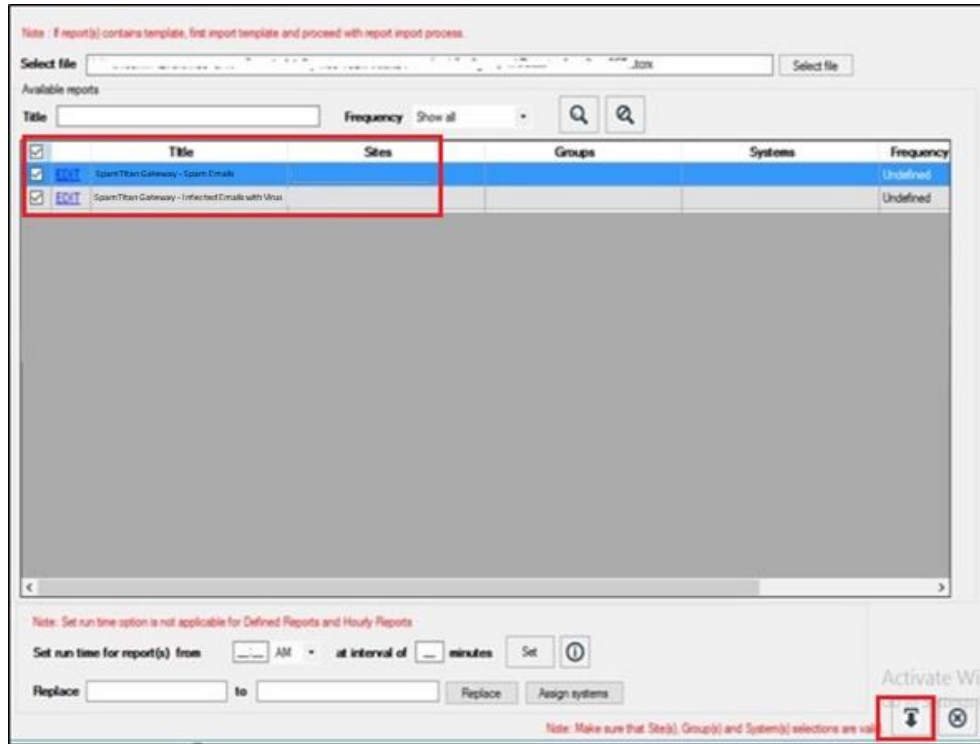



Figure 28

3. Click **Import**  to import the report. EventTracker displays a success message.

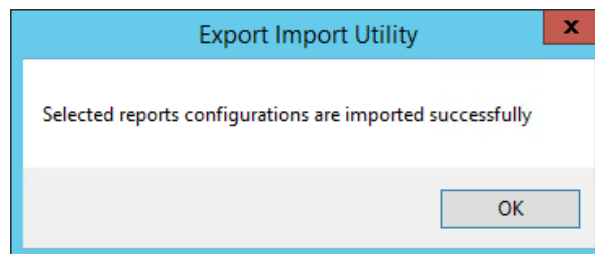


Figure 29

5.6 Dashboards

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

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

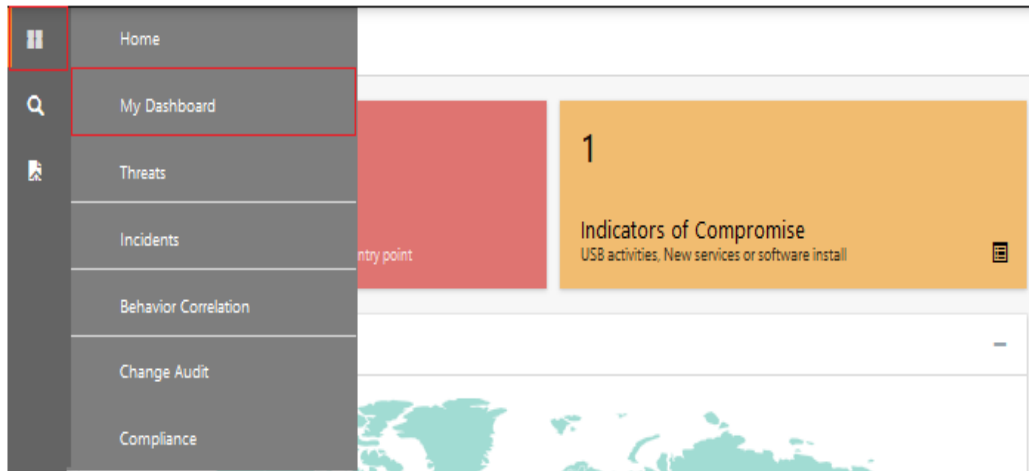


Figure 30


2. Navigate to **My Dashboard** option as shown above.
3. Click **Import**  as shown below:



Figure 31

4. Import dashboard file **Dashboard_SpamTitan Gateway.etwd** and select **Select All** checkbox.
5. Click **Import** as shown below.

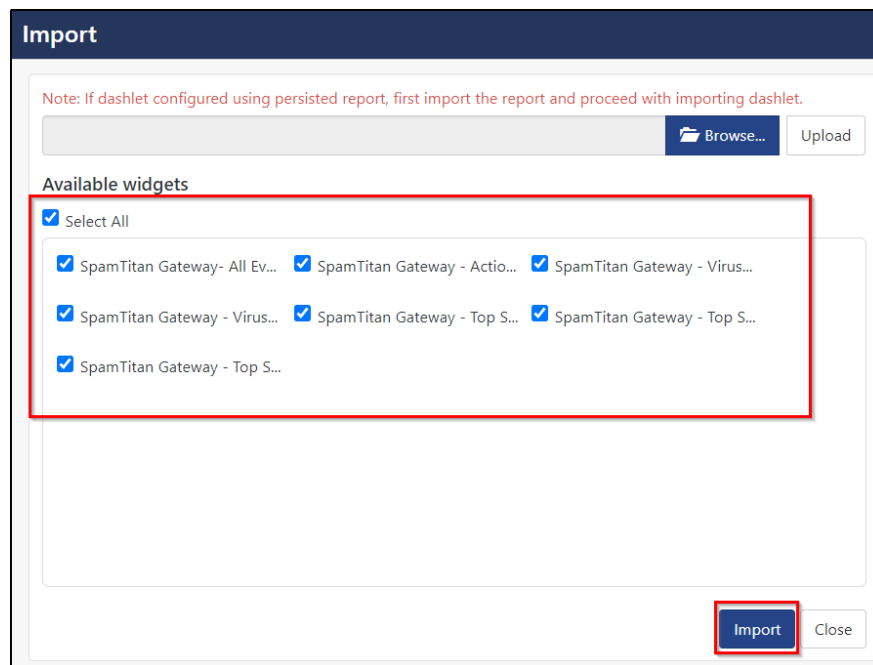


Figure 32

6. Import is now completed successfully.

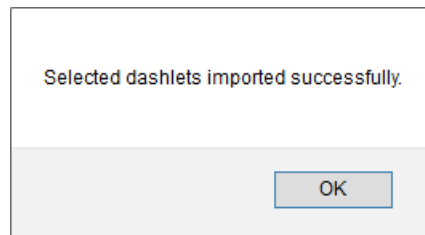



Figure 33

7. **My Dashboard** page selects to  add a dashboard.

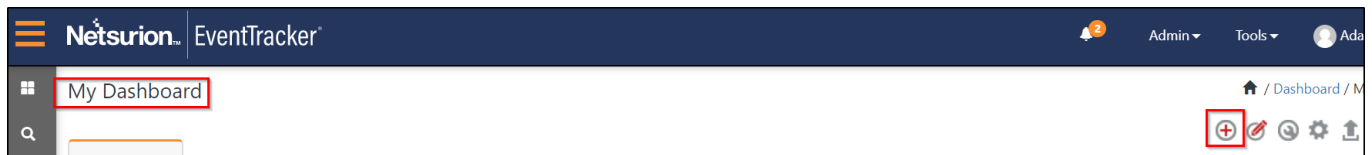


Figure 34

8. Choose an appropriate name for **Title** and **Description**. Click **Save**.

Figure 35

9. In **My Dashboard** page  select to add dashlets.

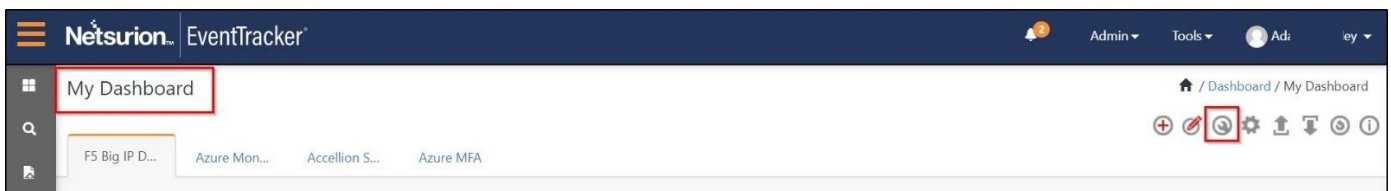


Figure 36

10. Select imported dashlets and click **Add**.

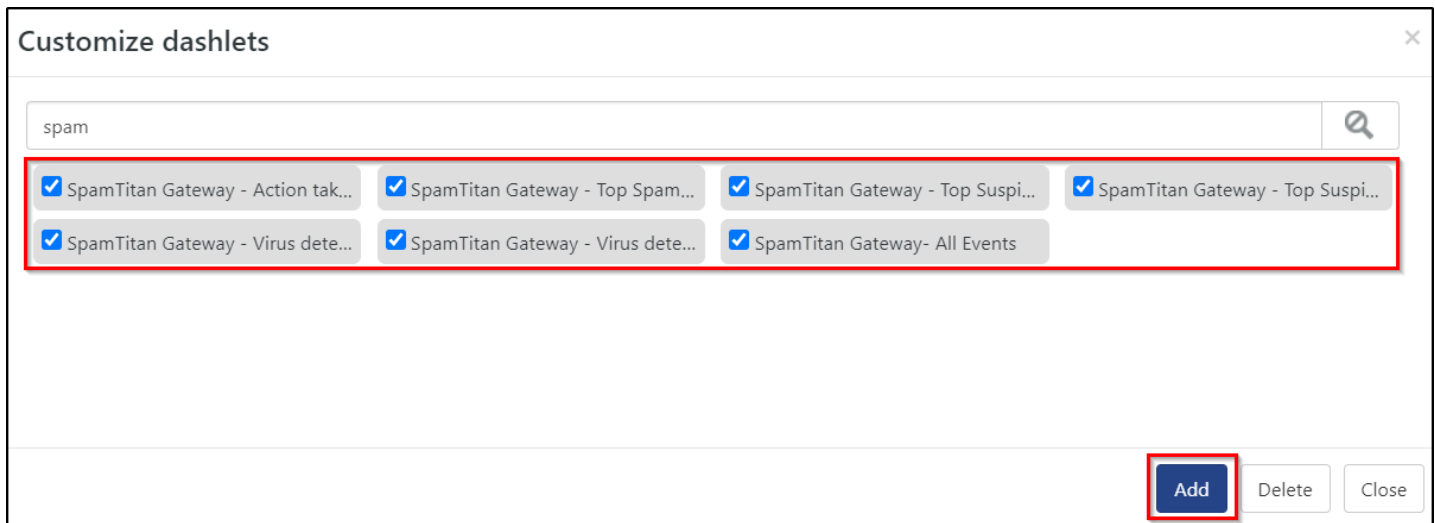


Figure 37

6. Verifying SpamTitan Gateway knowledge pack in EventTracker

6.1 Category

1. Login to **EventTracker**.
2. Click **Admin** dropdown, and then click **Category**.

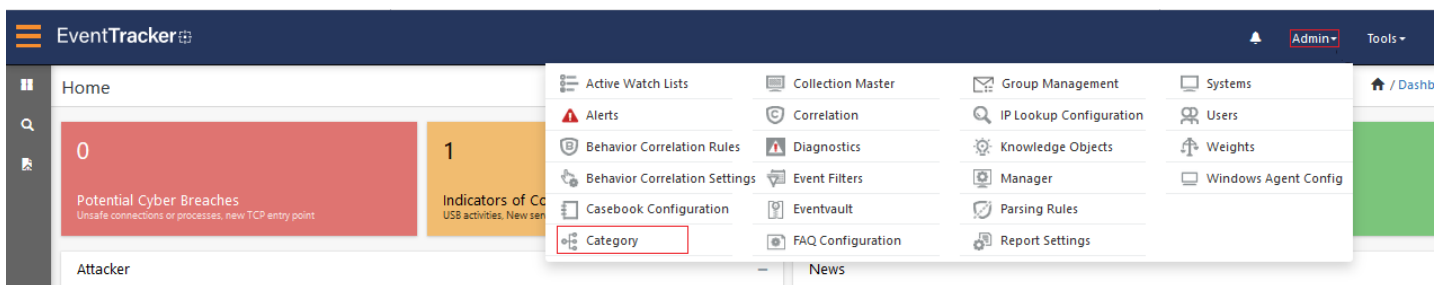


Figure 38

3. In **Category Tree** to view the imported category, scroll down and expand the **SpamTitan Gateway** group to view the imported category.

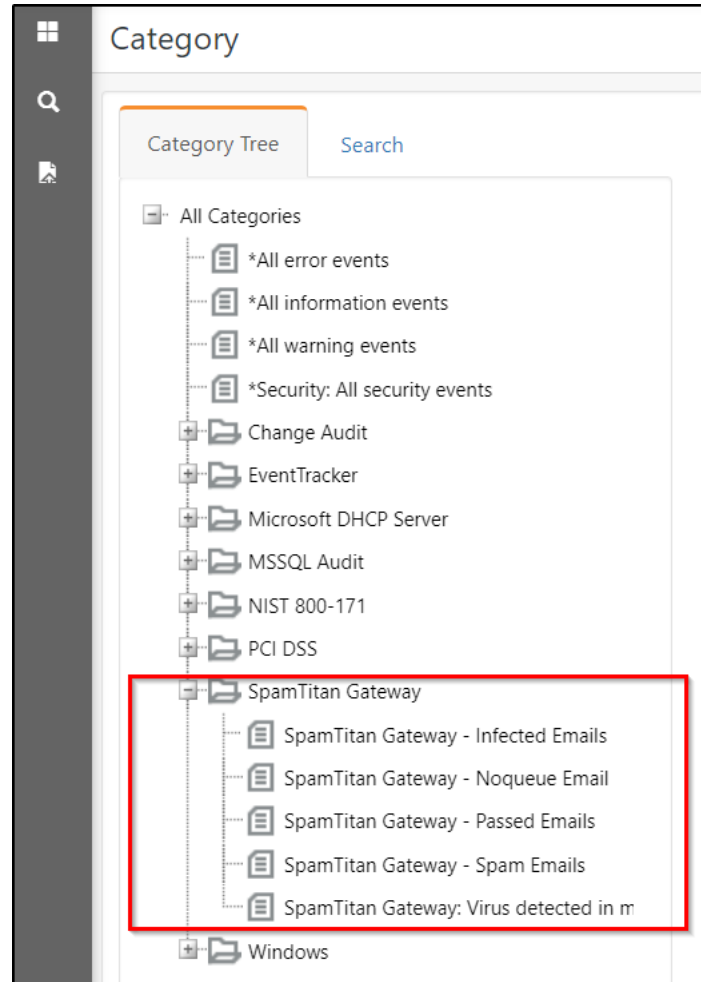


Figure 39

6.2 Alerts

1. In the EventTracker Manager web interface, click the Admin dropdown, and then click **Alerts**.
2. In search box enter “e.g. **SpamTitan**” and then click Search. EventTracker displays an alert related to **SpamTitan Gateway**:

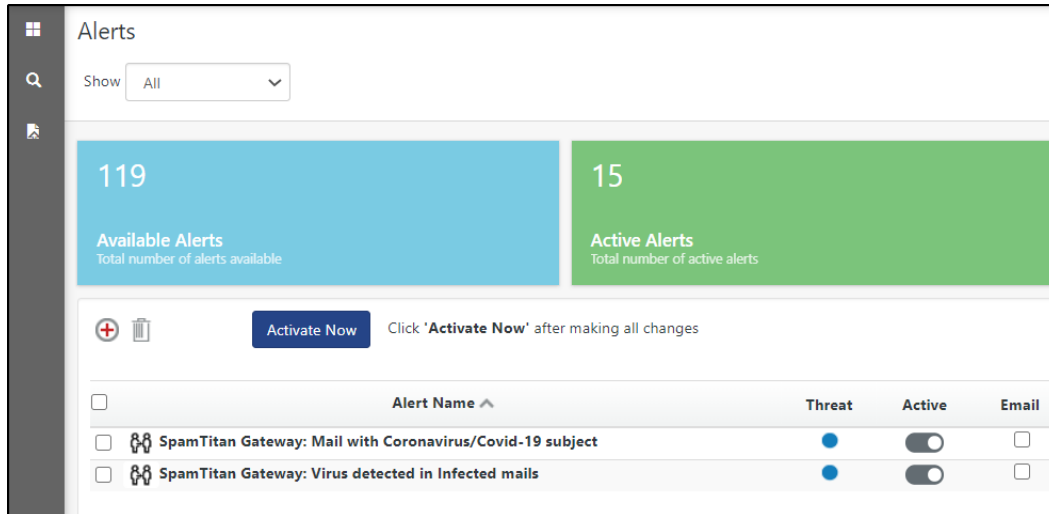


Figure 40

6.3 Token templates

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

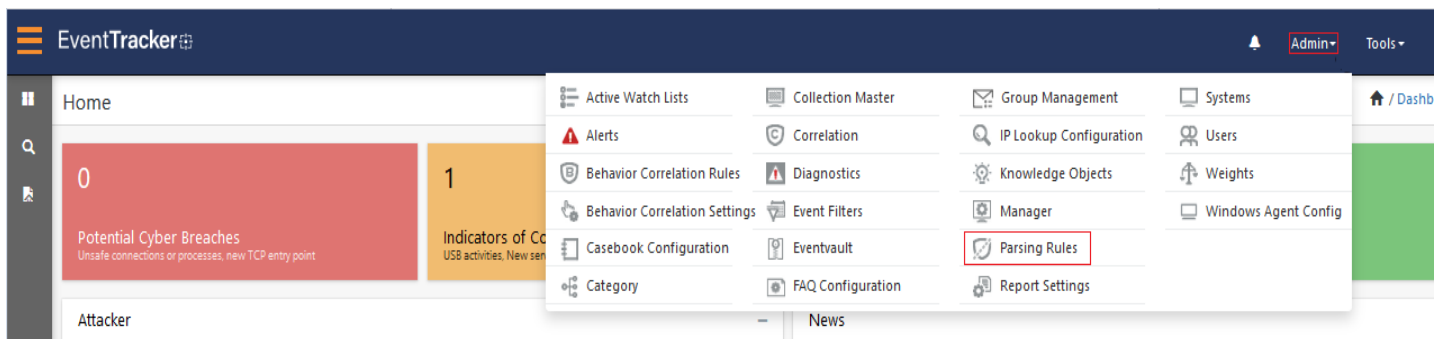


Figure 41

2. On the **Template** tab, click on the **SpamTitan Gateway** group folder to view the imported token values.

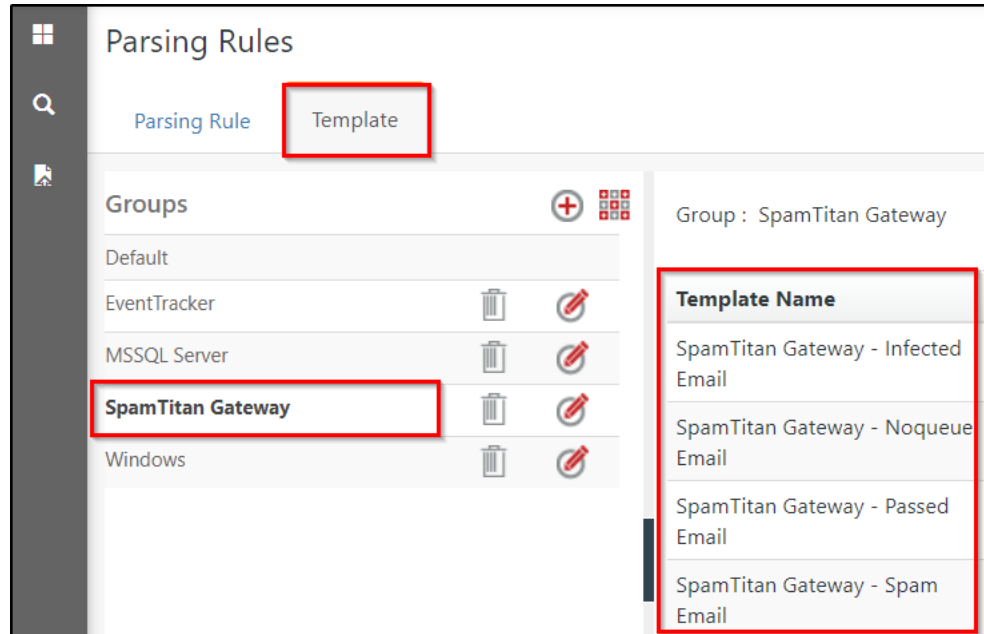


Figure 42

6.4 Knowledge Object

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

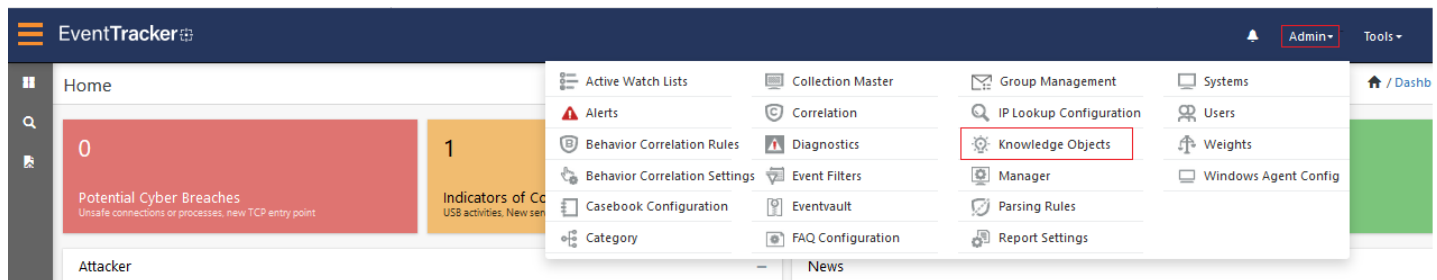


Figure 43

2. In the Knowledge Object tree, expand the **SpamTitan Gateway** group folder to view the imported knowledge object.

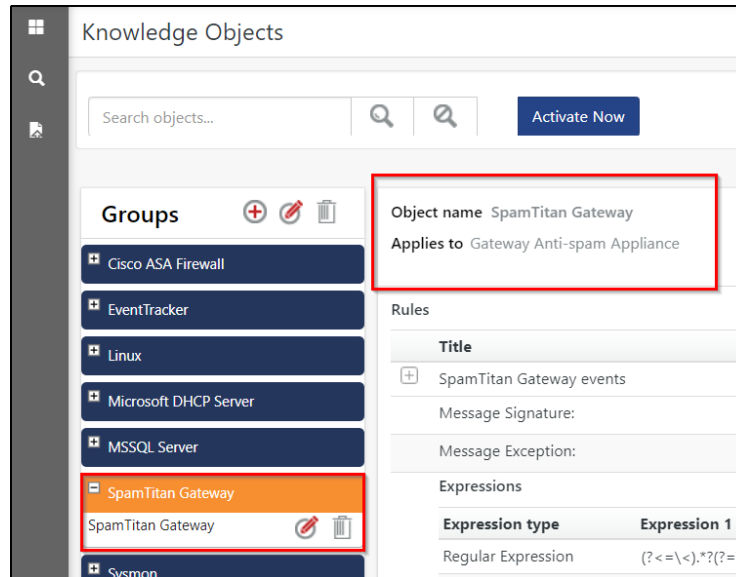


Figure 44

3. Click **Activate Now** to apply imported knowledge objects.

6.5 Report

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

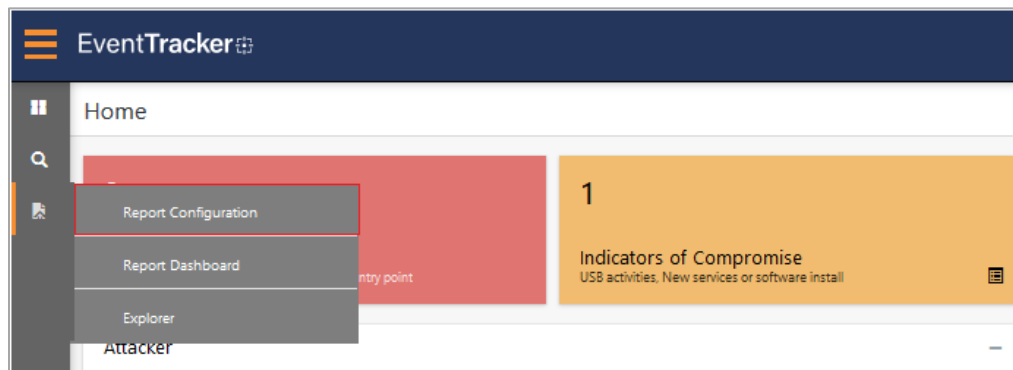


Figure 45

2. In **Reports Configuration** pane, select the **Defined** option.
3. Click on the **SpamTitan Gateway** group folder to view the imported reports.

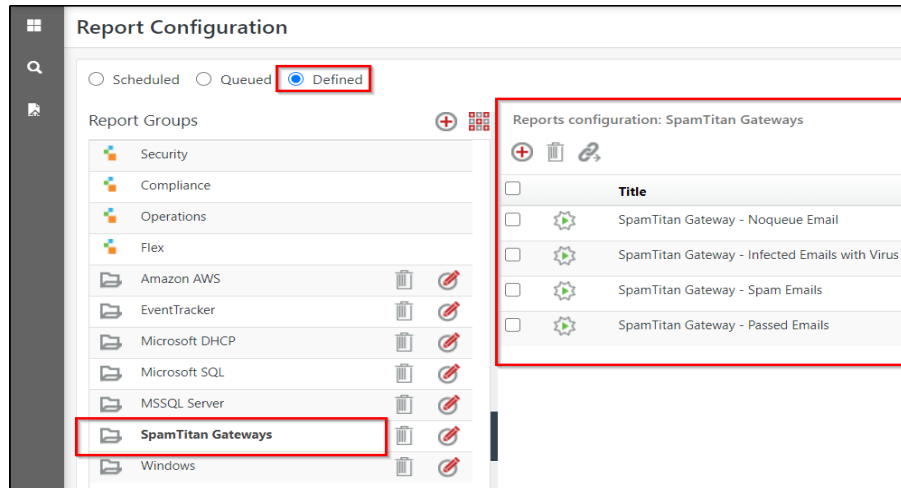


Figure 46

6.6 Dashboards

1. In the EventTracker web interface, Click **Home** and select **“My Dashboard”**.

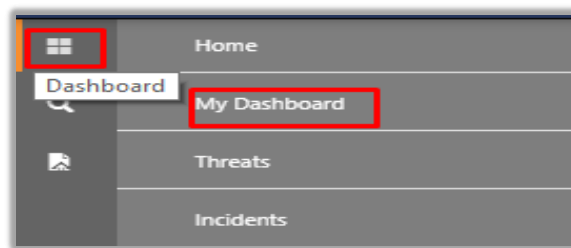


Figure 47

2. In the **“SpamTitan Gateway”** dashboard you should be now able to see something like this.

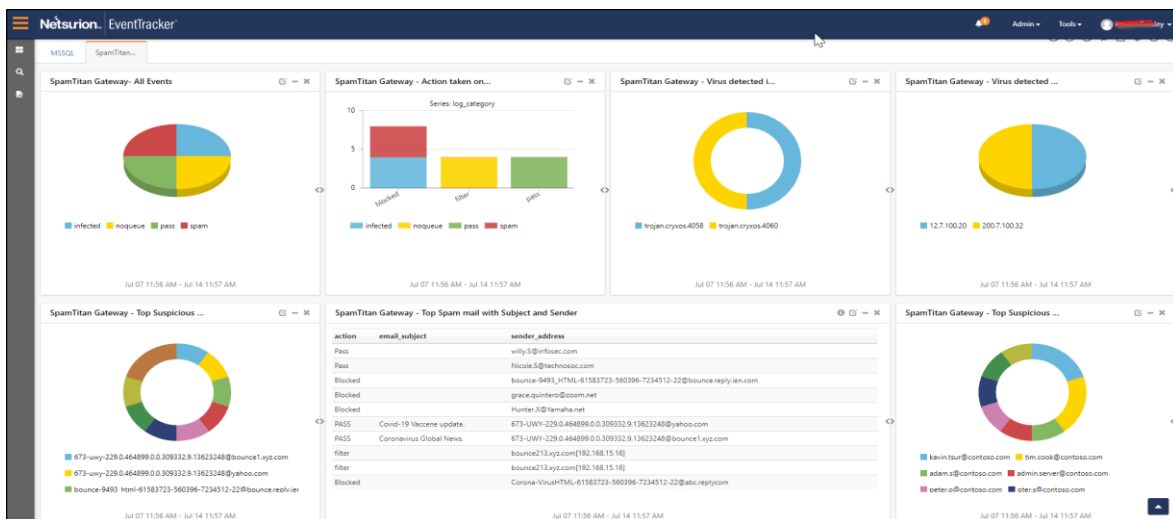


Figure 48