Integrate Trend Micro Worry-Free with EventTracker

EventTracker v9.x and above

Publication Date: October 25, 2019

Abstract

This guide provides instructions to configure **Trend Micro Worry-Free** to send the log to EventTracker. Once log source is being configured to send to EventTracker, alerts, and reports can be configured into EventTracker.

Scope

The configurations detailed in this guide are consistent with **EventTracker** version 9.x and later, **Trend Micro Worry-Free V9.0 or Later.**

Audience

Administrators who are responsible for monitoring Trend Micro Worry-Free which are running using EventTracker.

Table of Contents

1.Overview

Trend Micro Worry-Free Business Security is designed to protect physical and virtualized endpoints in small organizations. **EventTracker** collects the event logs delivered from Trend Micro Worry-Free and filters them out to get some critical event types for creating reports, dashboards, and alerts. Among the event types, we are considering: Application control, Behaviour monitoring, Device control, Network virus, Predictive machine learning, spyware, URL Filtering, Virus/Malware, Web Reputation, etc.

2.Prerequisites

- **EventTracker** agent must be installed in a host system/server.
- **Python** should be installed**. Python 2** is recommended.
- Install or upgrade **pip (Python package manager).**
- **Windows Powershell** ISE(x86) must be installed to run the Powershell script.
- Windows **Task scheduler** should be running to schedule the powershell script task.
- **end_customer.zip** and **vendor.zip** setup must be installed to perform the cspi_connection, logfeeder, enroll_users, get_customer, and query_logs.
- Firewall between Trend Micro Worry-Free and EventTracker should be off or exception for EventTracker ports.

3.Configuring Trend Micro Worry-Free to EventTracker

WFBS-SVC allows you to export logs to syslog format using the Log Forwarder API. You can then further analyze the exported data in your syslog management tool. This article contains a step-by-step guide on how to activate the Log Forwarder API in WFBS-SVC.

3.1 Environment setup

1. Install **Python** on Windows. **Python 2** is recommended.
2. Install or upgrade **pip (Python package manager)** on Windows. For more information, refer to Installing Python packages guide.
3. Install all required Python packages. Open Windows Command Prompt, locate pip.exe and key in the following commands:

    a. **# pip install pycrypto==2.6.1**

    b. **# pip install pytz**

3.2 Configuration

1. Download **end_customer.zip** or **vendor.zip** depending on your license and extract the files using the password "trend".

2. Configure **logfeeder.ini file**. Fill in all required information.

```
[cspi]
ACCESS_TOKEN = aaaaaaaa-bbbb-cccc-dddd-eeeeeeeeeeee
SECRET_KEY = ssssssssaaaaaaaammmmmmppppppplllllllleeeeee=
SERVER_HOSTNAME = cspi.trendmicro.com
SERVER_PORT = 443

[logfeeder]
public_file_path = ./my_public.key
password = my_password
log_types =
virus,spyware,wtp,url_filtering,behavior_monitoring,device_control,application_control,machine_l
earning,network_virus,dlp
storage_path = ./logs/
```

- **ACCESS_TOKEN** is one of the CSPI key pair provided by the Product Manager.
- **SECRET_KEY** is one of the CSPI key pair provided by the Product Manager.
- **SERVER_HOSTNAME** is the CSPI FQDN (no need to change).
- **SERVER_PORT** should be 443 (no need to change).
- **public_file_path** is the location of your public key (e.g. C:\my_public.key), Environment Variables are not supported.
- **password** is used to protect the log archives; the password is used to unzip the log archive. The "%" symbol is not supported in the password.
- **log_types** are the threat types which you would like to download from the log archive. There are 11 types of threats; each should be separated by a comma.
- **storage_path** is the location where you would like to keep log archives (e.g. C:\logs\), Environment Variables are not supported.

3.3 Script usage

1. For the MSP version, get the customer ID by name once you have received the CSPI key pair and public key. Run the following command:

```
# python get_customer_list.py apple
```

The result displays a list of customer IDs with 'apple' in the company name.

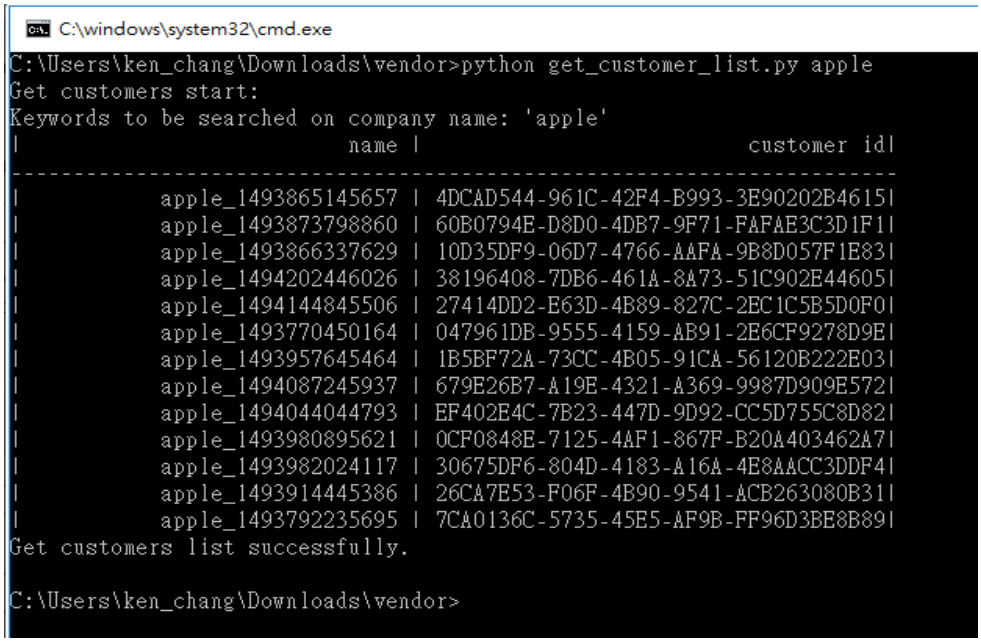

Figure 1

2. The MSP version supports automatic enrollment. Once you have received the CSPI key pair and public key, you can run the following command to automatically enroll the rest of the customers:

 # python enroll_users.py customer_id1 customer_id2

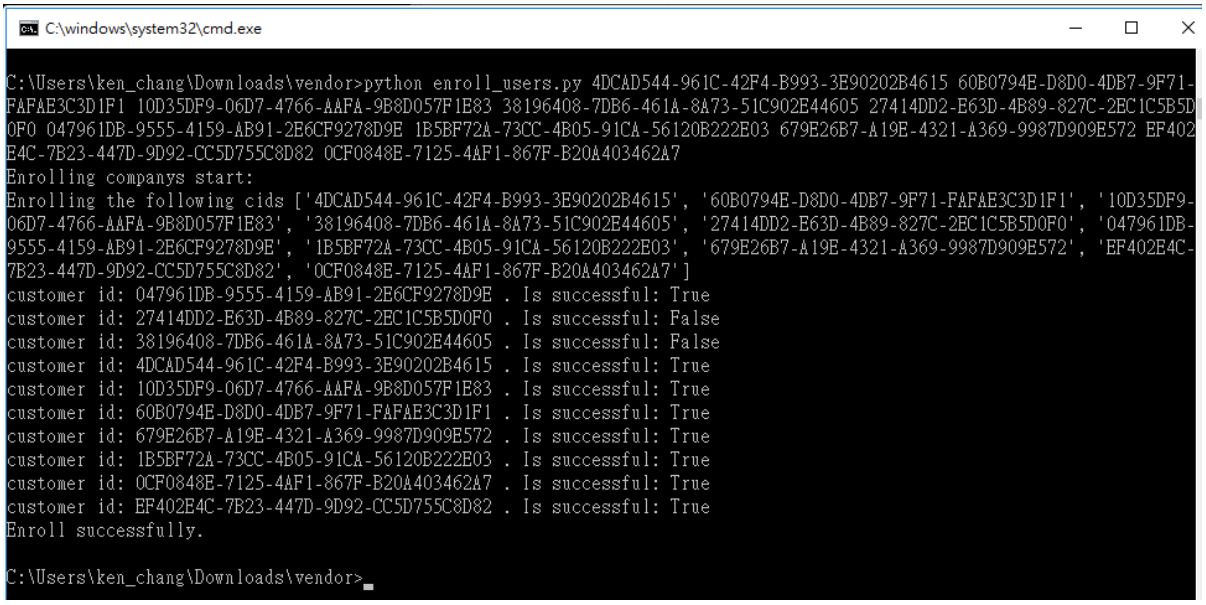

Figure 2

3. Subscribe the API.

Note: It takes one day to prepare the log archive of the previous day. Run the subscribe script in advance, at least one day, before running the query script.
Make sure to update logfeeder.ini first and that the entries are correct (e.g. CSPI keys, log_types or password).
Open Windows Command Prompt and run the following command:

 # python subscribe.py

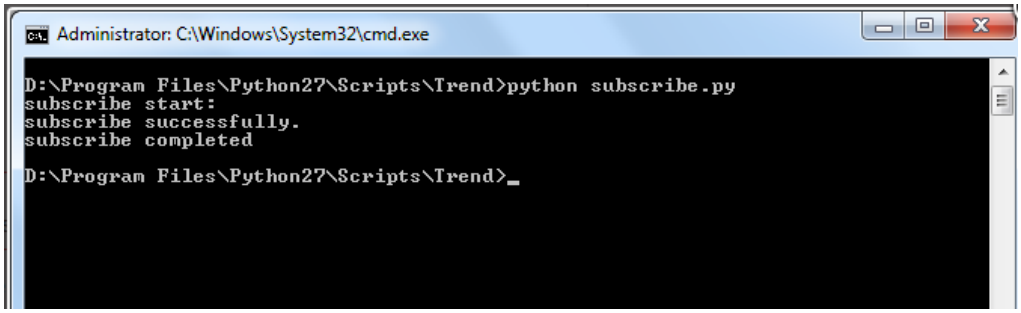

Figure 3

4. Query and download the log archive. Open Windows Command Prompt and run the following command:

 # python query_logs.py
Locate and extract the log archives using the password you configured in the **logfeeder.ini** file.

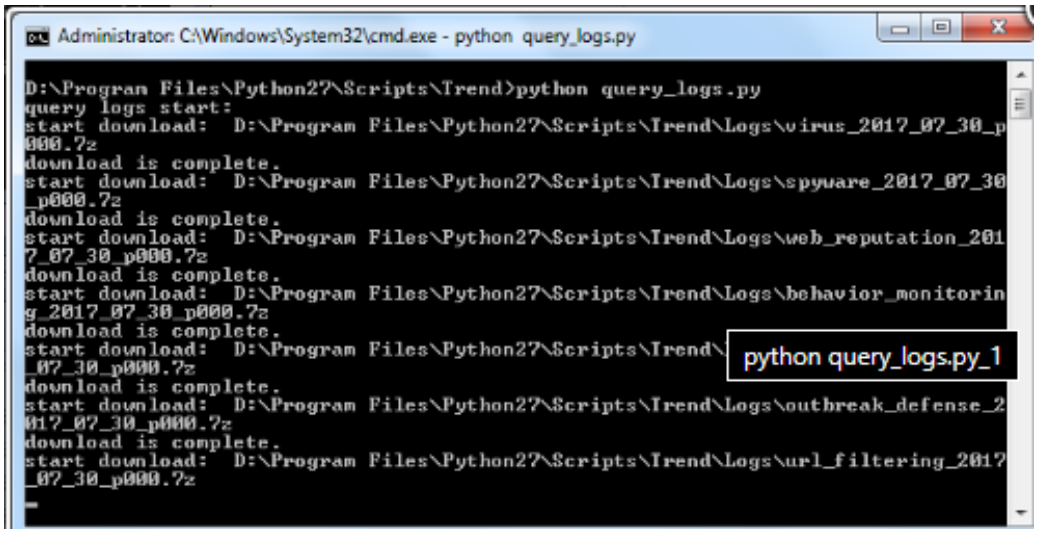

Figure 4

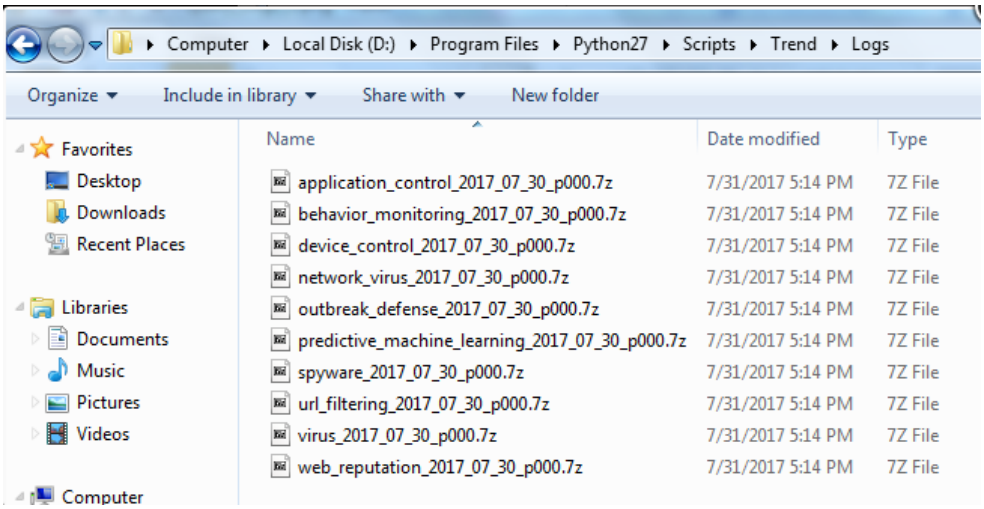

Figure 5

3.4 Run PowerShell script

PowerShell script needs to be deployed on the client's system to normalize the password-protected Trend micro Worry-Free log files**.**

Note: Please contact to support team for the Trend Micro Worry-Free Powershell script.

1. Launch the powershell ISE(x86).
2. Open the powershell script and provide the Password for Protected Zip File.

```
1  $ErrorActionPreference = "silentlycontinue"
2
3
4  $filepath="D:\TM_Logs_7Z\"
5  $zipFilePassword = "Password"
6  $7zipPath = "C:\Program Files\7-Zip\7z.exe"
7  $null > "$filepath\error.log"
8
```

Figure 6

3. Save the script.
4. Run powershell script as scheduled task in **Windows Task scheduler**.

3.5 Scheduling PowerShell script with task scheduler

3.5.1 Configure the task with task scheduler

1. Open Task Manager by clicking the Windows icon, and type "**task scheduler**".

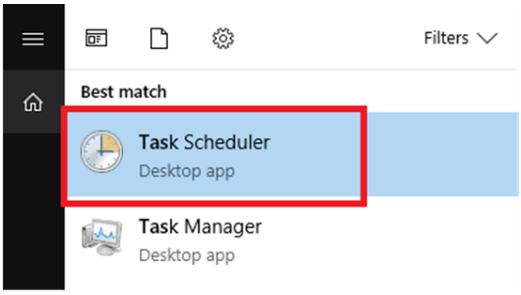

Figure 7

2. Once open, create a Task by clicking the "**Create Task**" link in the "**Actions section**".

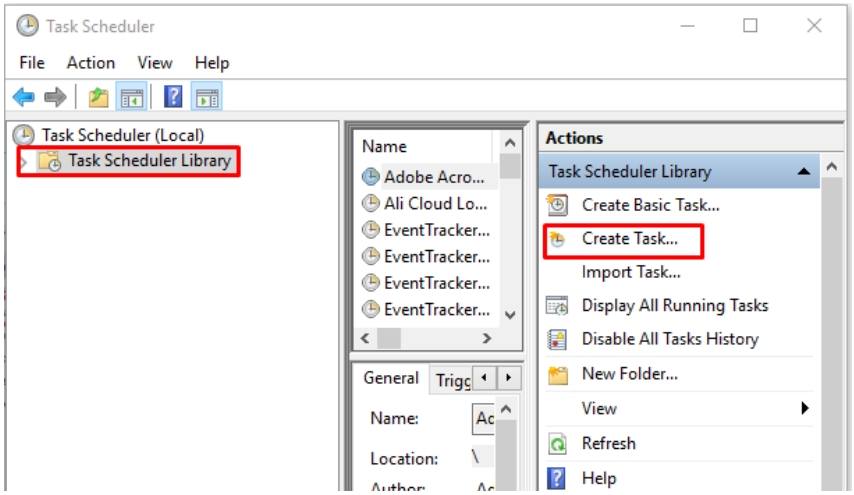

Figure 8

3. At the start, we are in the "**General**" tab. On the next screen add a name and make sure that the checkbox "**Run it with the highest privileges**" is checked.

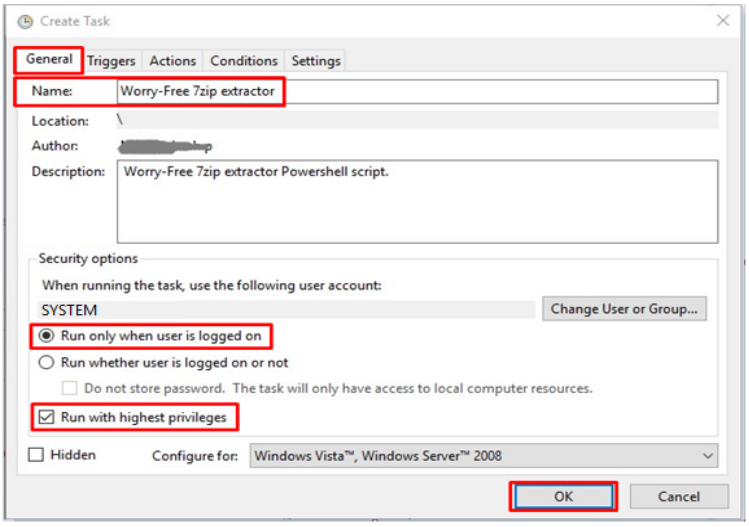

Figure 9

4. Move to the Triggers tab. Here we configure that it should execute every hour. To do so, we need to click the "**New**" button and then set as shown in the next image. Click **OK**.

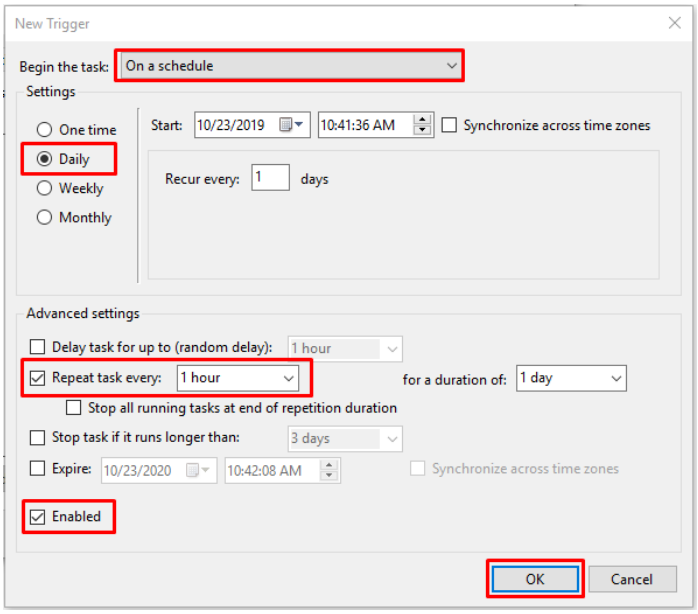

Figure 10

5. The "**Actions**" tab is the important one. We click on "**New**" on the program.

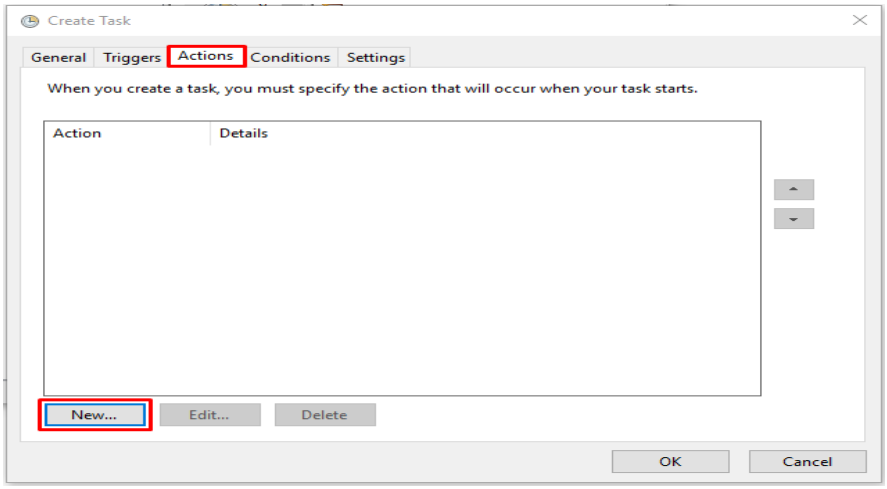

Figure 11

6. Select Actions tab, enter "**powershell.exe**" as program name and compose argument as given below:

powershell.exe -executionpolicy bypass -file "C:\Program Files (x86)\Prism Microsystems\EventTracker\Configuration Files\TM Worry-Free\Scripts\Worry-free.ps1"

EventTracker installation folder

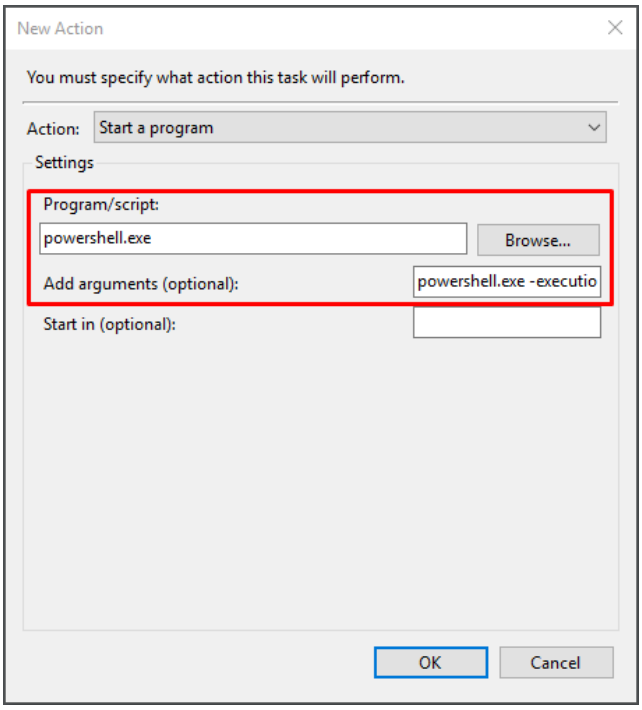

Figure 12

7. Click **OK** to save the task.

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 Trend Micro Worry-Free.

4.1 Flex Reports

- **Trend Micro Worry-Free - Action taken on malware-** This report provides information related to the action taken by the Trend Micro Worry-Free on malware, detected on the system along with file name, file path, and scan type. If the action fails, then this report provides the details for the reason.

TM Worry Free- Action taken on malware

LogTime	Computer	Action	Device_Name	Domain Name	File Name	Group Name	Label	Path	Scan Type	Virus/Malware
10/21/2019 12:41:25 PM	WORRYFREE	No action	030-WS773	contoso	ParalQUA_ex.dll	Device (Default)	-	C:\6.0.9_OnView BranchDeposit	Scheduled Scan	Possible_Virus
10/21/2019 02:49:12 PM	WORRYFREE	Access blocked	012-WFBS	Contoso	run.dll32	Laptops	-	C:\User\MyOffice Directory	Scheduled Scan	Wannacry
10/21/2019 02:49:13 PM	WORRYFREE	Access Blocked	030-WS76	Contoso	rundll32.exe	Device (Default)	-	C:\Tset\User\file1	Scheduled Scan	Anna Kournikova
10/21/2019 02:49:14 PM	WORRYFREE	Access blocked	019-WFBS	Contoso	run.dll32	Device (Default)	-	C:\User\MyOffice Directory	Scheduled Scan	Storm Worm
10/21/2019 02:49:24 PM	WORRYFREE	Access blocked	012-WFBS	Contoso	run.dll32	Device (Default)	-	C:\User\MyOffice Directory	Scheduled Scan	Wannacry
10/21/2019 02:49:25 PM	WORRYFREE	Access Blocked	030-WS76	Contoso	rundll32.exe	Desktops	-	C:\Tset\User\file1	Scheduled Scan	Anna Kournikova
10/21/2019 02:49:25 PM	WORRYFREE	Access blocked	019-WFBS	Contoso	run.dll32	Device (Default)	-	C:\User\MyOffice Directory	Scheduled Scan	Storm Worm

Figure 13

Sample Logs:

action	Access blocked
addl_info	run.dll32
device_name	019-WFBS
event_computer	WorryFree
event_description	<116>1 2019-09-10 19:00:33 10.30.12.161 WFBS-SVC-AC [LogVirus@1.3.6.1.4.1.6101 Action Taken="Access blocked" Device name="019-WFBS" Domain="Contoso" File name="run.dll32" Generated="2019-09-10T23:00:30-04:00" Group name="Device (Default)" IPv6 Address="-" Label="-" Path="C:\User\MyOffice Directory" Received="2019-09-10T19:00:33-04:00" Scan Type="Scheduled Scan" Virus/Malware Name="Storm Worm"]
event_id	3220
event_log_type	Application
event_source	TrendMicro
event_type	Information
event_user_domain	N/A
event_user_name	N/A
file_path	C:\User\MyOffice Directory
group_name	Device (Default)
log_source	TM Worry Free All Events
log_type	Virus
service_type	Scheduled Scan
src_domain_name	Contoso
threat_name	Storm Worm
tags	Trend Micro Worry Free

Figure 14

- **Trend Micro Worry-Free - Web reputation events-** This report provides detailed information related to web reputation events. Using this report, we can find out the computer on which this event was logged, the URL that triggered this event, what was the risk level of the URL that triggered the event and what action was taken by the trend micro worry-free.

TM Worry Free Web reputation events

LogTime	Computer	Action	Device_Name	Domain Name	Group Name	Label	Risk Level	URL	User
10/21/2019 02:49:11 PM	WORRYFREE	Access to a website was blocked	Win123	Contoso	Desktops	-	Medium	http://malwarelauncher.com/executefile+an	Joe Smith
10/21/2019 02:49:13 PM	WORRYFREE	Access to a website was blocked	Peachs-MacBook-Pro	-	Laptops	-	High	http://Uwatchfree.torentz.com/all+latest+ho	Randy Peter
10/21/2019 02:49:14 PM	WORRYFREE	Access to a website was blocked	Peachs-MacBook-Pro	-	Laptops	-	High	http://Uwatchfree.torentz.com/all+latest+bo	Hemilton
10/21/2019 02:49:24 PM	WORRYFREE	Access to a website was blocked	Win123	Contoso	Desktops	-	Medium	http://malwarelauncher.com/executefile+an	Joe Smith
10/21/2019 02:49:24 PM	WORRYFREE	Access to a website was blocked	Peachs-MacBook-Pro	-	Laptops	-	High	http://Uwatchfree.torentz.com/all+latest+ho	Randy Peter
10/21/2019 02:49:25 PM	WORRYFREE	Access to a website was blocked	Peachs-MacBook-Pro	-	Laptops	-	High	http://Uwatchfree.torentz.com/all+latest+bo	Hemilton

Figure 15

Sample Logs:

action	+ - Access to a website was blocked
device_name	+ - Peachs-MacBook-Pro
event_computer	+ - WorryFree
event_description	<116>1 2019-09-10 15:31:15 10.30.33.115 WFBS-SVC-AC [LogWebReputation@1.3.6.1.4.1.6101 Action="Access to a website was blocked" Device name="Peachs-MacBook-Pro" Domain="-" Generated="2019-09-10T15:01:58-04:00" Group name="Laptops" IPv6 Address="-" Label="-" Received="2019-09-10T15:31:15-04:00" Risk Level="High" URL="http://Uwatchfree.torentz.com/all+latest+bollywood+3idiots/access+download+path" User="Hemilton"]
event_id	+ - 3220
event_log_type	+ - Application
event_source	+ - TrendMicro
event_type	+ - Information
event_user_domain	+ - N/A
event_user_name	+ - N/A
group_name	+ - Laptops
log_source	+ - TM Worry Free All Events
log_type	+ - WebReputation
src_domain_name	+ - -
src_user_name	+ - Hemilton
threat_priority	+ - High
url_name	+ - http://Uwatchfree.torentz.com/all+latest+bollywood+3idiots/access+download+path
tags	+ - Trend Micro Worry Free

Figure 16

4.2 Dashboards

- **Trend Micro Worry-Free - All events**

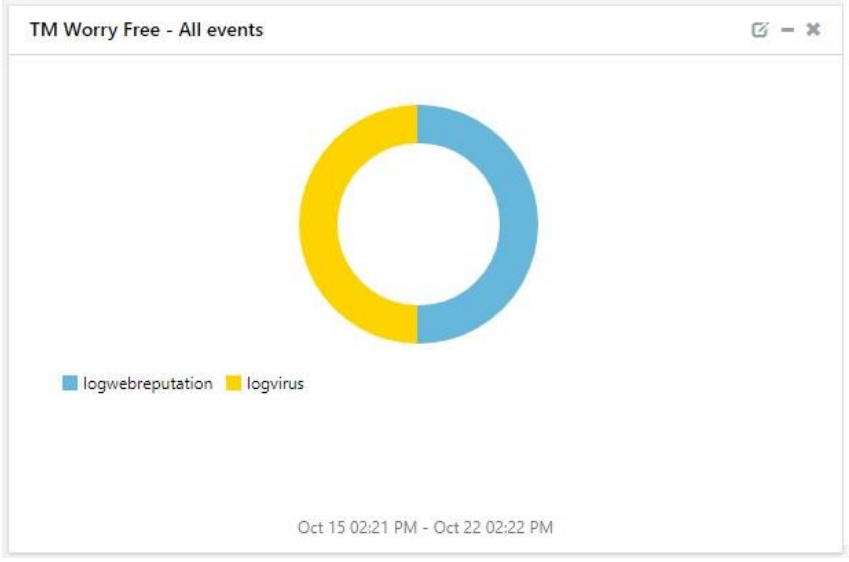

Figure 17

- **Trend Micro Worry-Free- Action taken on URL**

TM Worry Free - Action taken on URL

action	device_name	src_user_name	url_name
Access to a website was blocked	Peachs-MacBook-Pro	Hemilton	http://Uwatchfree.torentz.com/all+latest+bollywood+3idiots
Access to a website was blocked	Peachs-MacBook-Pro	Randy Peter	http://Uwatchfree.torentz.com/all+latest+hollywood+movies
Access to a website was blocked	Win123	Joe Smith	http://malwarelauncher.com/executefile+and+gameover
Access to a website was blocked	Peachs-MacBook-Pro	Hemilton	http://Uwatchfree.torentz.com/all+latest+bollywood+3idiots
Access to a website was blocked	Peachs-MacBook-Pro	Randy Peter	http://Uwatchfree.torentz.com/all+latest+hollywood+movies
Access to a website was blocked	Win123	Joe Smith	http://malwarelauncher.com/executefile+and+gameover
Access to a website was blocked	Peachs-MacBook-Pro	Hemilton	http://Uwatchfree.torentz.com/all+latest+bollywood+3idiots
Access to a website was blocked	Win123	Joe Smith	http://malwarelauncher.com/executefile+and+gameover
Access to a website was blocked	Peachs-MacBook-Pro	Randy Peter	http://Uwatchfree.torentz.com/all+latest+hollywood+movies
Access to a website was blocked	Peachs-MacBook-Pro	Hemilton	http://Uwatchfree.torentz.com/all+latest+bollywood+3idiots

Oct 15 02:21 PM - Oct 22 02:22 PM

Figure 18

- **TrendMicro Worry-Free- Action taken on malware**

TM Worry Free - Action taken on malware

action	addl_info	event_computer	file_path	service_type	threat_name
Access blocked	run.dll32	WorryFree	C:\User\MyOffice Directory	Scheduled Scan	Storm Worm
Access Blocked	rundll32.exe	WorryFree	C:\Tset\User\file1	Scheduled Scan	Anna Kournikova
Access blocked	run.dll32	WorryFree	C:\User\MyOffice Directory	Scheduled Scan	Wannacry
Access blocked	run.dll32	WorryFree	C:\User\MyOffice Directory	Scheduled Scan	Storm Worm
Access Blocked	rundll32.exe	WorryFree	C:\Tset\User\file1	Scheduled Scan	Anna Kournikova
Access blocked	run.dll32	WorryFree	C:\User\MyOffice Directory	Scheduled Scan	Wannacry
Access blocked	run.dll32	WorryFree	C:\User\MyOffice Directory	Scheduled Scan	Storm Worm
Access Blocked	rundll32.exe	WorryFree	C:\Tset\User\file1	Scheduled Scan	Anna Kournikova
Access blocked	run.dll32	WorryFree	C:\User\MyOffice Directory	Scheduled Scan	Wannacry
Access blocked	run.dll32	WorryFree	C:\User\MyOffice Directory	Scheduled Scan	Storm Worm

Oct 15 02:21 PM - Oct 22 02:22 PM

Figure 19

- **TrendMicro Worry-Free- Threats by devices/domain name**

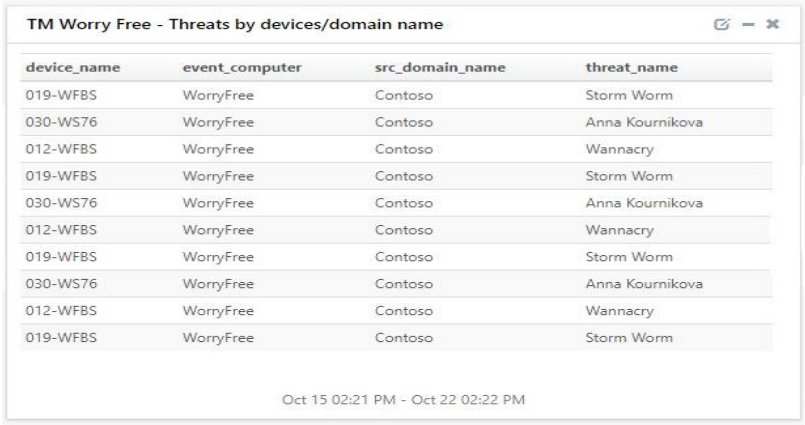

Figure 20

5 Importing Trend Micro Worry-Free knowledge pack into EventTracker

NOTE: Import knowledge pack items in the following sequence:

- Token Templets.
- Knowledge Object.
- Flex Reports.
- Dashboard.

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

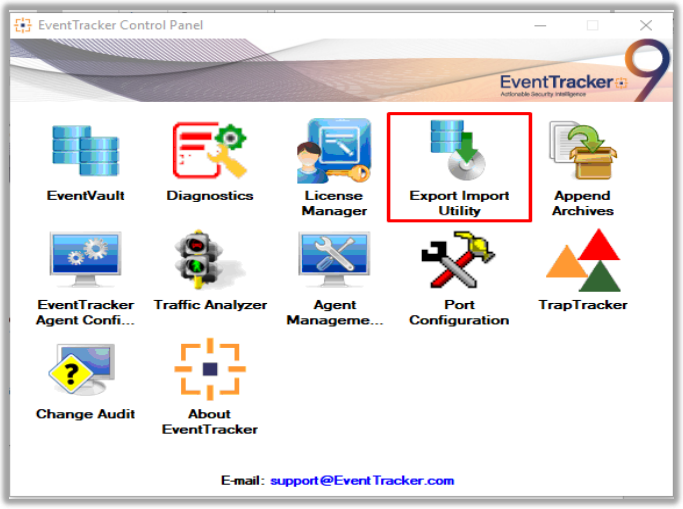

Figure 21

5.1 Token Template

1. Login to the **EventTracker Console.**
2. Click on **Admin >> Parsing Rules.**

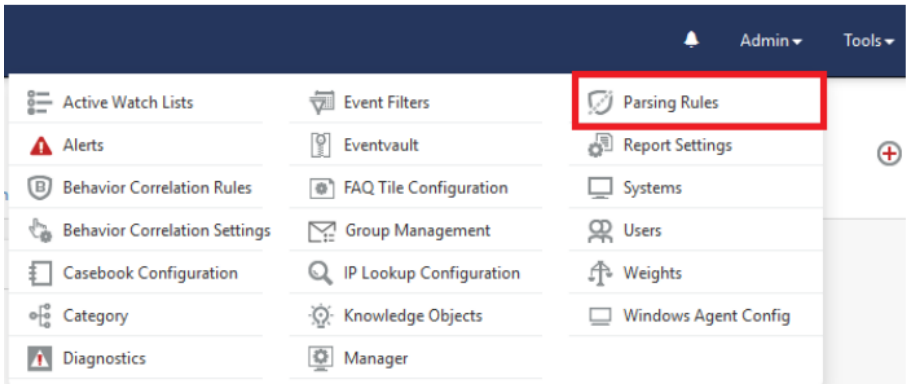

Figure 22

3. Click on **Template** and click import configuration Symbol.

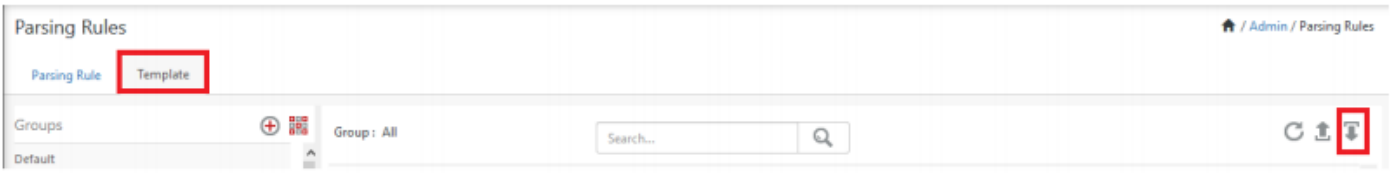

Figure 23

4. Locate the "**.ettd**" file and click on import.

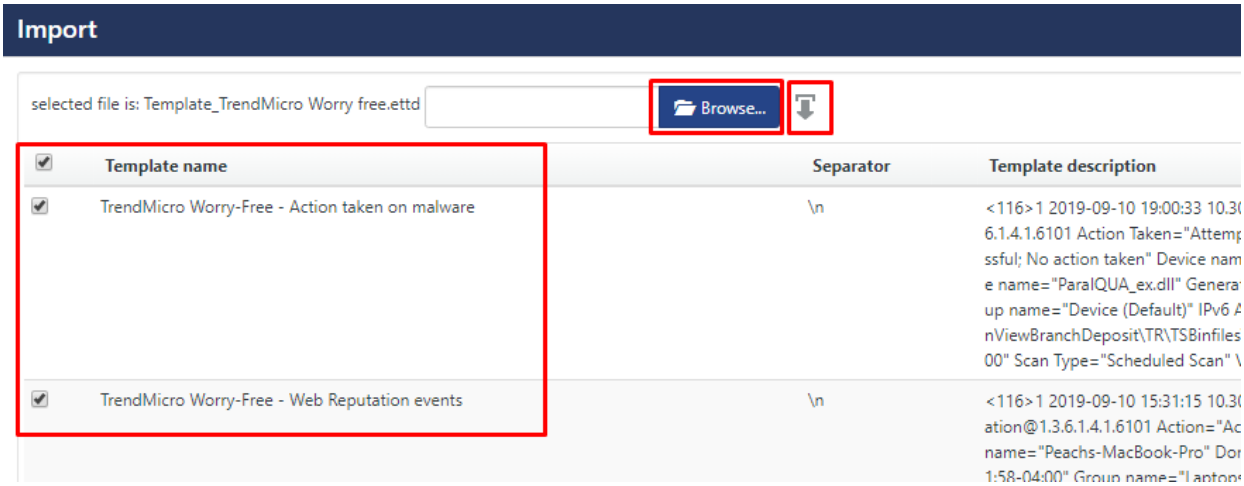

Figure 24

5. Templates are imported now successfully.

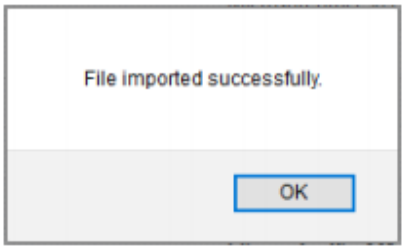

Figure 25

5.2 Knowledge Object

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

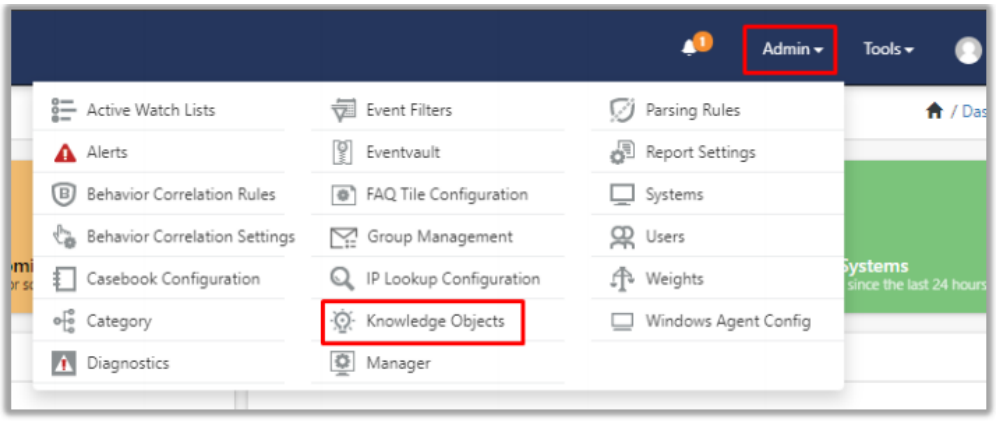

Figure 26

2. Next, click on the "**import object**" icon:

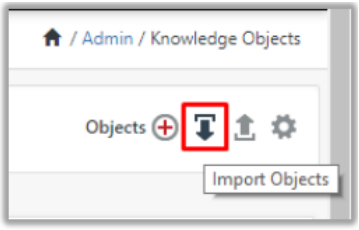

Figure 27

3. A pop-up box will appear, click "**Browse**" in that and navigate to the file path with extension "**.etko**" button"

Figure 28

4. A list of available knowledge object will appear. Select the relevant files and click on "**Import**" button:

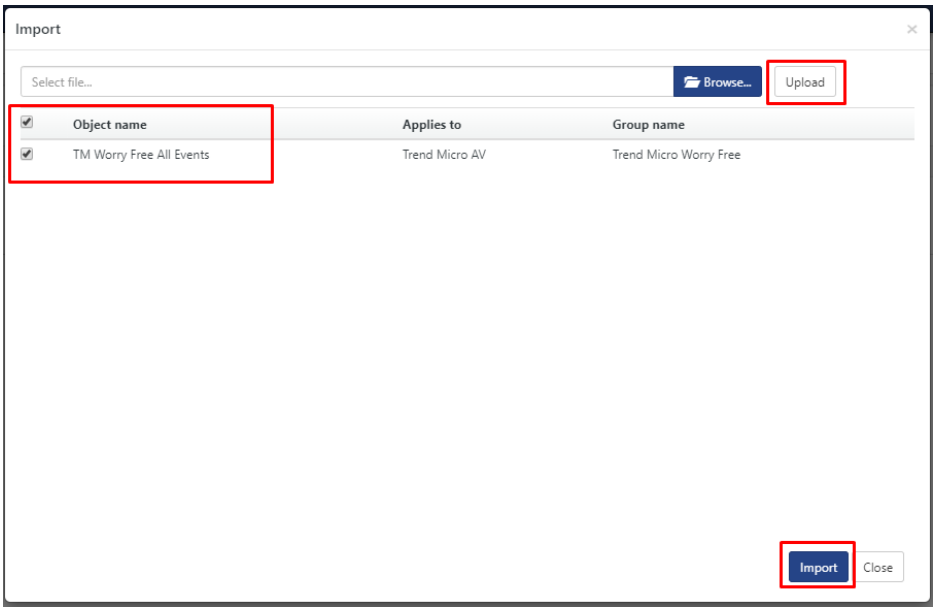

Figure 29

5.3 Flex Reports

1. In the EventTracker control panel, select "**Export/ Import utility**" and select the "**Import tab**". Then, click **Reports** option, and choose "**New (*.etcrx)**":

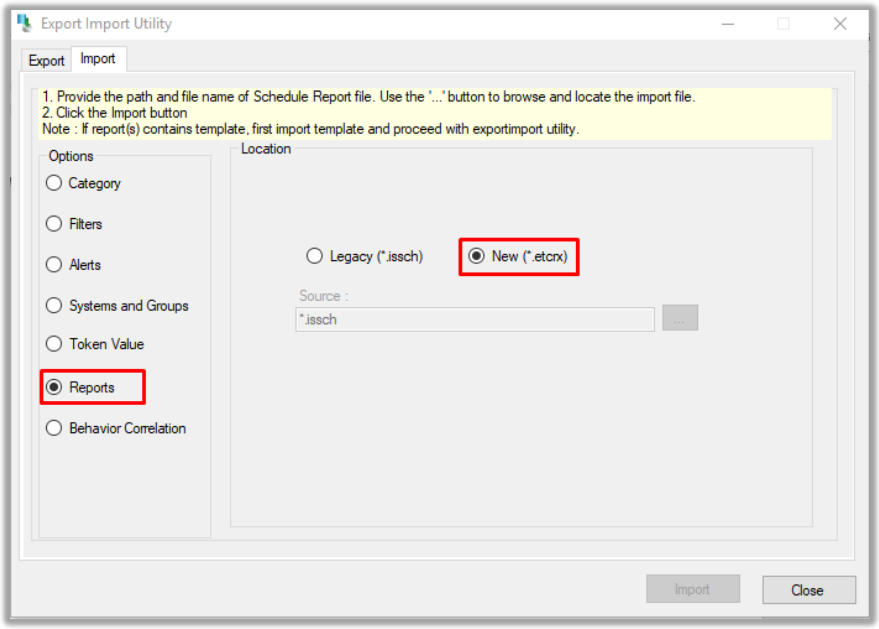

Figure 30

2. Once you have selected "**New (*.etcrx)**", a new pop-up window will appear. Click the "**Select File**" button and navigate to the file path with a file having the extension **".etcrx".** Select all the relevant files and then click **Import** button.

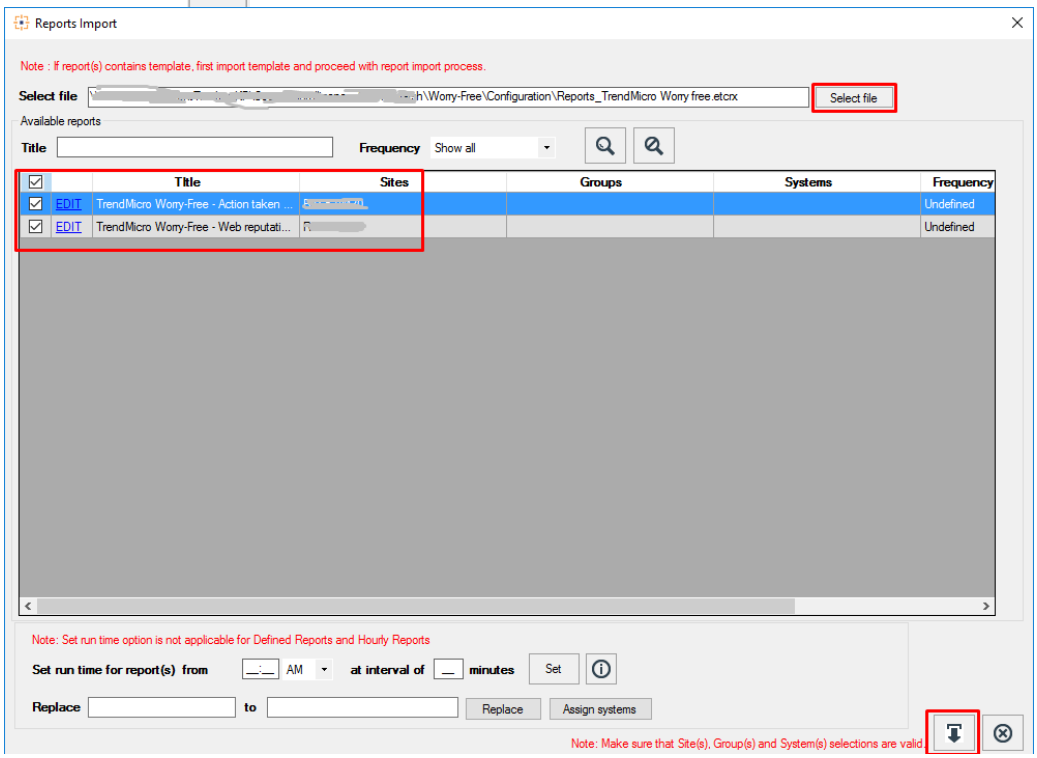

Figure 31

3. EventTracker displays a success message:

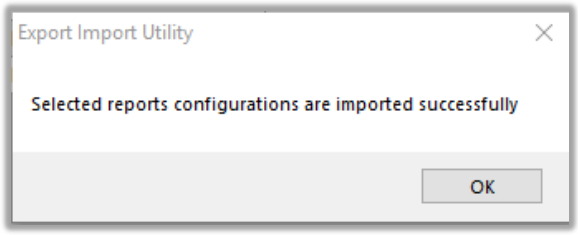

Figure 32

5.4 Dashboard

1. Login to **EventTracker**.
2. Navigate to **Dashboard → My Dashboard**.
3. In "My Dashboard", click **Import Button**:

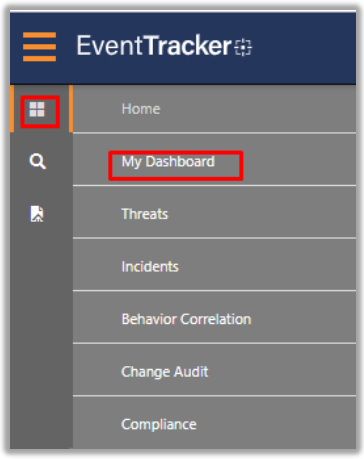

Figure 33

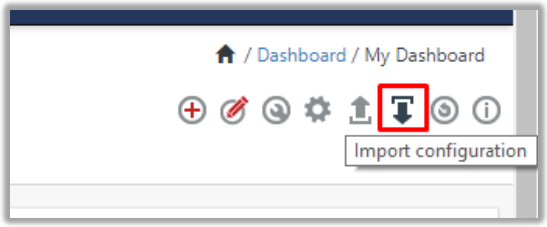

Figure 34

4. Select the **Browse** button and navigate to the file path where the dashboard file is saved and click on the "**Upload**" button.
5. Once completed, choose "**Select All**" and click on **"Import"** Button.

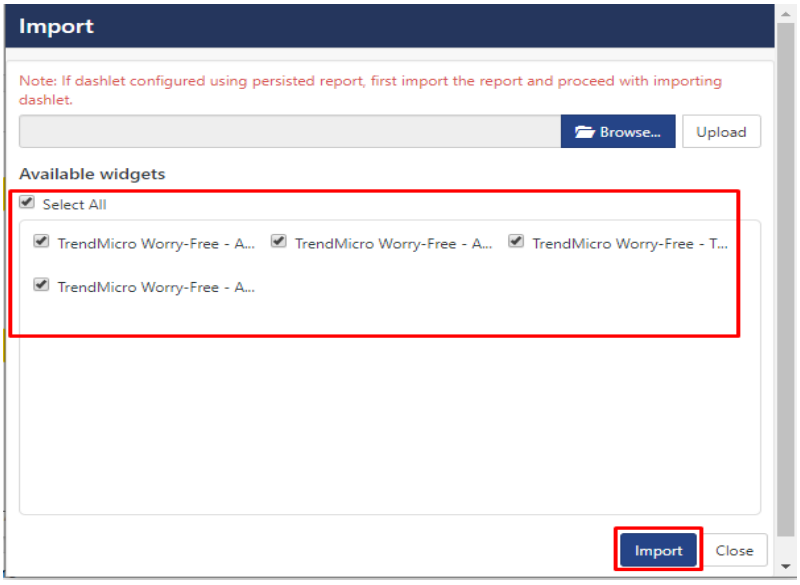

Figure 35

6. Next, click "**Customize dashlet**" button as shown below:

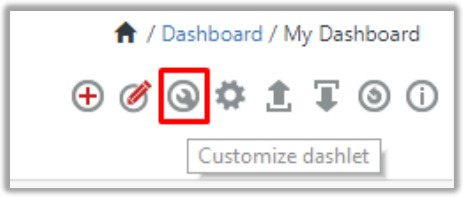

Figure 36

7. Now, put a text on the **Search bar: "TM Worry Free"** and then select the Trend Micro Worry-Free dashlets and then click the **"Add"** button.

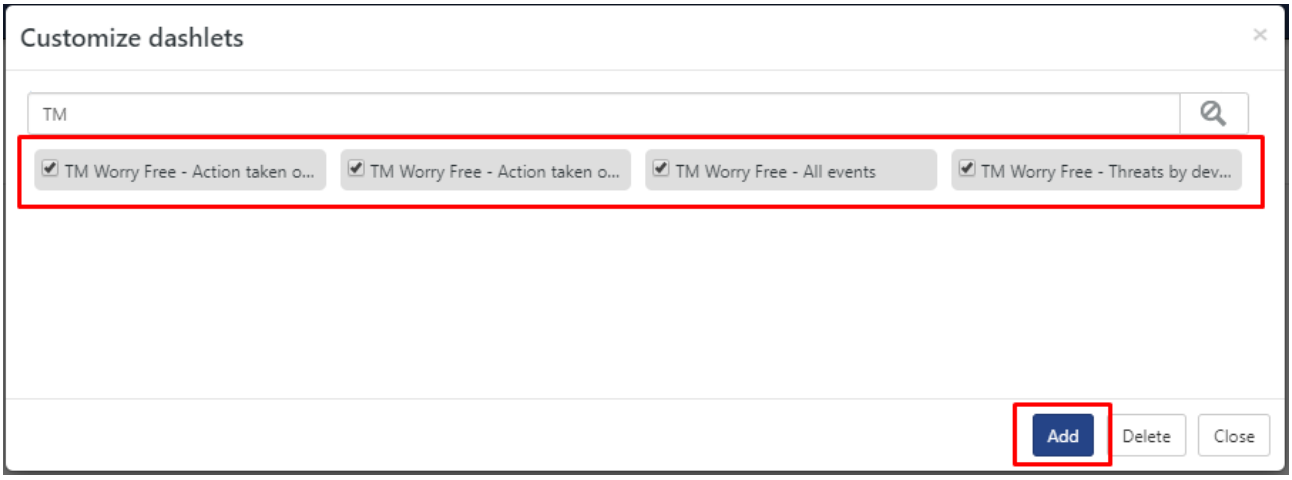

Figure 37

6 Verifying Trend Micro Worry-Free knowledge pack in EventTracker

6.1 Token Template

1. In the **EventTracker** web interface, click the **Admin** dropdown, and then click **Parsing Rules.**
2. In the **Parsing Rule** tab select **Template**, click on the **"Trend Micro Worry-Free"** group folder to view the imported templates.

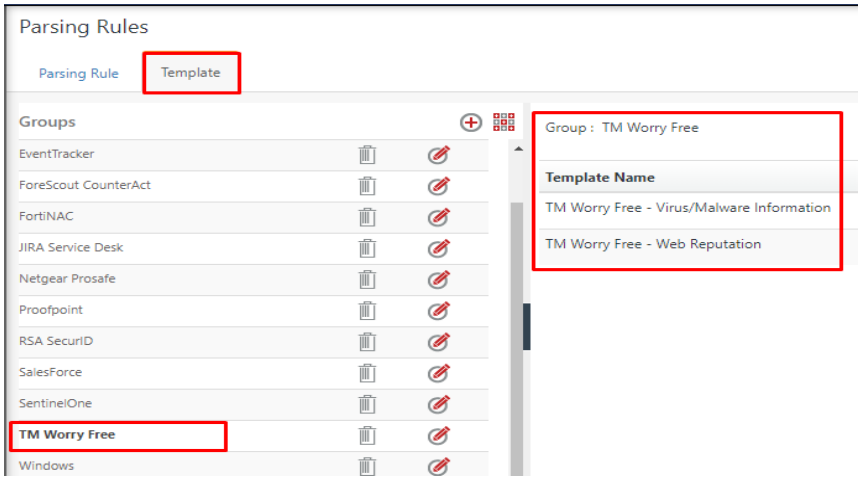

Figure 38

6.2 Knowledge Object

1. In the **EventTracker** web interface, click the **Admin** dropdown, and then click **Knowledge Objects**.
2. In the **Knowledge Object** tree, expand the "**Trend Micro Worry Free**" group folder to view the imported Knowledge objects.

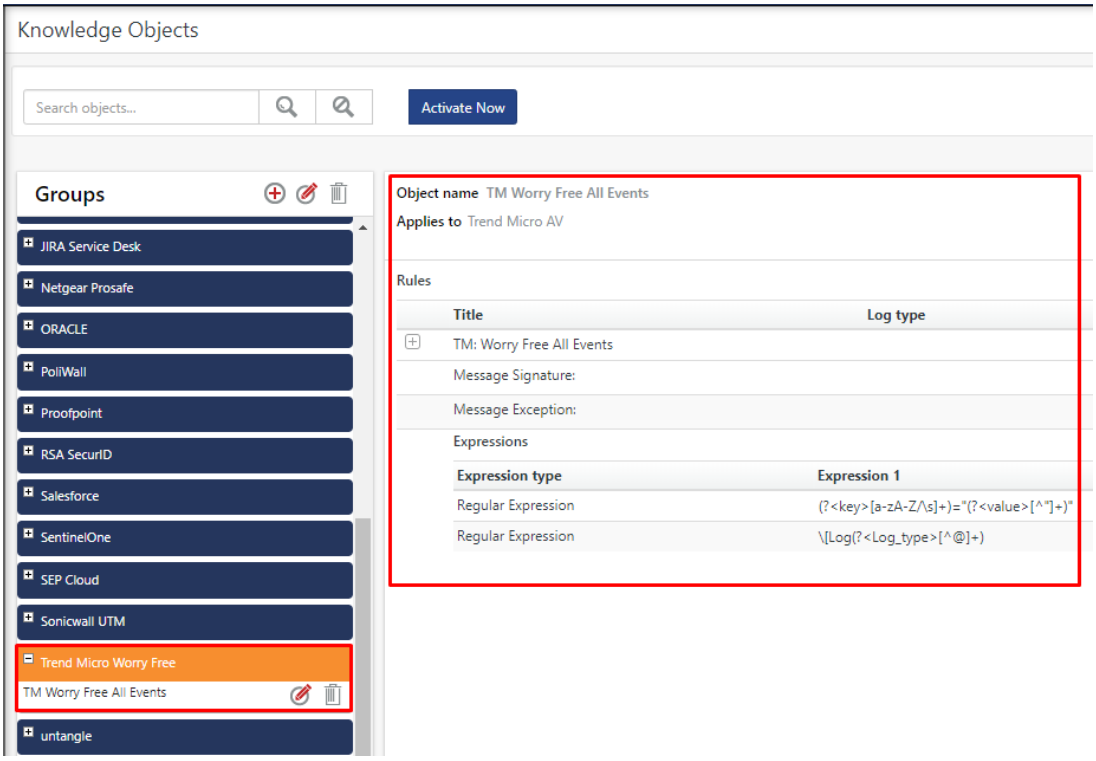

Figure 39

6.3 Flex Reports

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

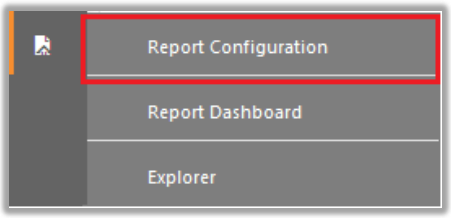

Figure 40

2. In **Reports Configuration** pane, select the **Defined** option.
3. Click on the **Trend Micro Worry-Free** group folder to view the imported reports.

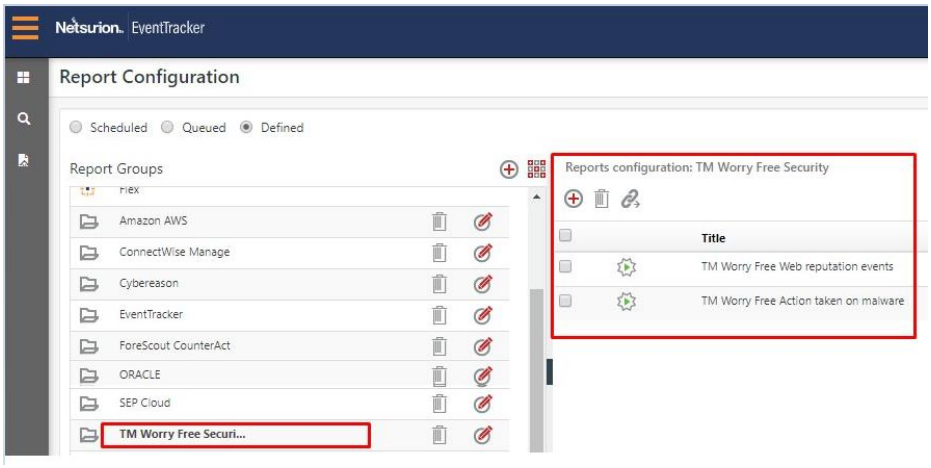

Figure 41

6.4 Dashboard

1. In the EventTracker web interface, Click on Home Button and select "**My Dashboard**".

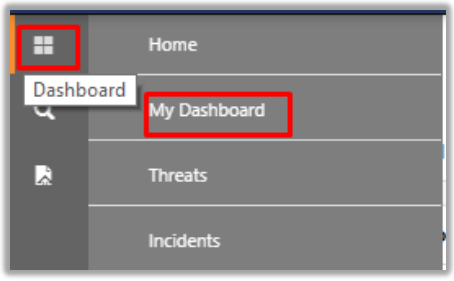

Figure 42

2. In the "**Trend Micro Worry-Free**" dashboard you should be now able to see something like this.

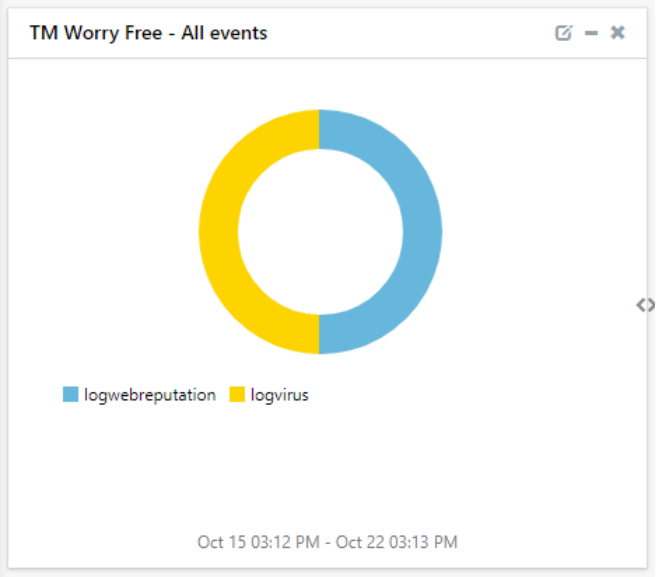
TM Worry Free - All events
logwebreputation
logvirus
Oct 15 03:12 PM - Oct 22 03:13 PM

Figure 43