# Netsurion... EventTracker

# 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.

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.

© 2019 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.	Ove	verview					
2.	2. Prerequisites						
3.	Cor 3.1	Configuring Trend Micro Worry-Free to EventTracker Environment setup					
3.2 Configuration		Configuration	. 4				
	3.3	Script usage	. 4				
	3.4	Run PowerShell script	. 7				
	3.5	Scheduling PowerShell script with task scheduler	. 7				
	3.5	.1 Configure the task with task scheduler	. 7				
4	Eve	entTracker Knowledge Pack	10				
	4.1	Flex Reports	10				
	4.2	Dashboards	12				
5	Imp	porting Trend Micro Worry-Free knowledge pack into EventTracker	14				
	5.1	Token Template	15				
	5.2	Knowledge Object	16				
	5.3	Flex Reports	17				
	5.4	Dashboard	18				
6	Ver	rifying Trend Micro Worry-Free knowledge pack in EventTracker	20				
	6.1	Token Template	20				
	6.2	Knowledge Object	21				
	6.3	Flex Reports	22				
	6.4	Dashboard	22				

Netsurion... EventTracker

# 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 <u>end\_customer.zip</u> or <u>vendor.zip</u> depending on your license and extract the files using the password "trend".
- 2. Configure logfeeder.ini file. Fill in all required information.

```
[cspi]
```

#### [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.



C:\windows\system32\cmd.exe
C:\Users\ken_chang\Downloads\vendor>python get_customer_list.py apple
Get customers start:
Keywords to be searched on company name: 'apple'
l name l customer idl
apple_1493865145657   4DCAD544-961C-42F4-B993-3E90202B4615
apple_1493873798860   60B0794E-D8D0-4DB7-9F71-FAFAE3C3D1F1
apple_1493866337629   10D35DF9-06D7-4766-AAFA-9B8D057F1E83
apple_1494202446026   38196408-7DB6-461A-8A73-51C902E44605
apple_1494144845506   27414DD2-E63D-4B89-827C-2EC1C5B5D0F0
apple_1493770450164   047961DB-9555-4159-AB91-2E6CF9278D9E
apple_1493957645464   1B5BF72A-73CC-4B05-91CA-56120B222E03
apple_1494087245937   679E26B7-A19E-4321-A369-9987D909E572
apple_1494044044793   EF402E4C-7B23-447D-9D92-CC5D755C8D82
apple_1493980895621   OCF0848E-7125-4AF1-867F-B20A403462A7
apple_1493982024117   30675DF6-804D-4183-A16A-4E8AACC3DDF4
apple_1493914445386   26CA7E53-F06F-4B90-9541-ACB263080B31
apple_1493792235695   7CA0136C-5735-45E5-AF9B-FF96D3BE8B89
Get customers list successfully.
C:\Users\ken_chang\Downloads\vendor>



- 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

C:\windows\system32\cmd.exe		×
C:\Users\ken_chang\Downloads\vendor>python_enroll_users.py_4DCAD544-961C-42F4-B993-3E90202B4615_60B0794E-D8D0 FAFAE3C3D1F1_10D35DF9-06D7-4766-AAFA-9B8D057F1E83_38196408-7DB6-461A-8A73-51C902E44605_27414DD2-E63D-4B89-8270 0F0_047961DB-9555-4159-AB91-2E6CF9278D9E_1B5BF72A-73CC-4B05-91CA-56120B222E03_679E26B7-A19E-4321-A369-9987D909 E4C-7B23-447D-9D92-CC5D755C8D82_0CF0848E-7125-4AF1-867F-B20A403462A7	4DB7-: 2-2EC10 9E572-1	9F71- C5B5D EF402
Enrolling companys start: Enrolling the following cids ['4DCAD544-961C-42F4-B993-3E90202B4615', '60B0794E-D8D0-4DB7-9F71-FAFAE3C3D1F1', 06D7-4766-AAFA-9B8D057F1E83', '38196408-7DB6-461A-8A73-51C902E44605', '27414DD2-E63D-4B89-827C-2EC1C5B5D0F0', 0555-4159-AB91-2E6CF9278D9E', '1B5EF72A-73CC-4B05-91CA-56120B222E03', '679E26B7-A19E-4321-A369-9987D909E572', 7B23-447D-9D92-CC5D755C8D82', '0CF0848E-7125-4AF1-867F-B20A403462A7'] customer id: 047961DB-9555-4159-AB91-2E6CF9278D9E . Is successful: True customer id: 27414DD2-E63D-4B89-827C-2EC1C5B5D0F0 . Is successful: False customer id: 38196408-7DB6-461A-8A73-51C902E44605 . Is successful: False customer id: 38196408-7DB6-461A-8A73-51C902E44605 . Is successful: True customer id: 4DCAD544-961C-42F4-B993-3E90202B4615 . Is successful: True customer id: 10D35DF9-06D7-4766-AAFA-9B8D057F1B83 . Is successful: True customer id: 6080794E-D8D0-4DB7-9F71-FAFAE3C3D1F1 . Is successful: True customer id: 679E26B7-A19E-4321-A369-9987D909E572 . Is successful: True customer id: 679E26B7-A19E-4321-A369-9987D909E572 . Is successful: True customer id: 1B5EF72A-73CC-4B05-91CA-56120B222E03 . Is successful: True customer id: 10CF0848E-7125-4AF1-867F-B20A403462A7 . Is successful: True customer id: 0CF0848E-7125-4AF1-867F-B20A403462A7 . Is successful: True	' 10D3. ' 0479i ' EF40:	5DF9- 61DB- 2E4C-
customer 16: Er402E4C-7625-447D-9D92-CC5D755C6D62 . Is successful: frue Enroll successfully. C:\Users\ken_chang\Downloads\vendor>_		

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.

Administrator: C:\Windows\System32\cmd.exe - python query_logs.py
D:\Program Files\Python2?\Scripts\Trend>python query_logs.py
<pre>query logs start: start download: D:\Program Files\Python27\Scripts\Irend\Logs\virus_2017_07_30_p 000.72</pre>
download is complete. start_download:==D:\Program_Files\Python27\Scripts\Irend\Logs\spyware_2017_07_30
_p000_72 download is complete. start download: D:\Program Files\Python27\Scripts\Irend\Logs\web reputation 201
7_07_30_p000.7z download is complete.
start download: D:\Program Files\Python27\Scripts\Irend\Logs\behavior_monitorin g_2017_07_30_p000.7z download is complete.
start download: D:\Program Files\Python27\Scripts\Irend\ python query_logs.py_1 _07_30_p000.7z
download is complete. start download: D:\Program Files\Python27\Scripts\Irend\Logs\outbreak_defense_2 M12 M2 3M pMMM 2z
download is complete. start_download: D:\Program Files\Python27\Scripts\Irend\Logs\url_filtering_2017
_87_30_p888.72

Figure 4



~								
🕒 🗢 🚽 🕨 Compute	er ► Local Disk (D:) ► Program Files ► Python27 ► S	cripts 🕨 Trend 🕨 Lo	gs					
Organize  Include II	n library  Share with  INew folder							
🖉 🔆 Favorites	Name	Date modified	Туре					
🧮 Desktop	application_control_2017_07_30_p000.7z	7/31/2017 5:14 PM	7Z File					
🕕 Downloads	🖬 behavior_monitoring_2017_07_30_p000.7z	7/31/2017 5:14 PM	7Z File					
🔚 Recent Places	device_control_2017_07_30_p000.7z	7/31/2017 5:14 PM	7Z File					
	network_virus_2017_07_30_p000.7z	7/31/2017 5:14 PM	7Z File					
4 📜 Libraries	🖬 outbreak_defense_2017_07_30_p000.7z	7/31/2017 5:14 PM	7Z File					
Documents	predictive_machine_learning_2017_07_30_p000.7z	7/31/2017 5:14 PM	7Z File					
🖻 🌙 Music	Bigging spyware_2017_07_30_p000.7z	7/31/2017 5:14 PM	7Z File					
🛛 🔛 Pictures	url_filtering_2017_07_30_p000.7z	7/31/2017 5:14 PM	7Z File					
🖻 📑 Videos	🖬 virus_2017_07_30_p000.7z	7/31/2017 5:14 PM	7Z File					
	web_reputation_2017_07_30_p000.7z	7/31/2017 5:14 PM	7Z File					
🗉 🖳 Computer								

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.



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".







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

🕑 Task Scheduler		- 🗆 X
File Action View Help		
🗢 🄿 🞽 🖬 👔 🖬		
Task Scheduler (Local) Task Scheduler Library	Name ^	Actions
	🕒 Adobe Acro	Task Scheduler Library
	Ali Cloud Lo	🕑 Create Basic Task
	EventTracker	🐌 Create Task
	Event Iracker	Import Task
	EventTracker	Display All Running Tasks
		Dicable All Tasks History
	General Trigg • •	Mew Folder
	Name: Ac	View 🕨
		Q Refresh
	Location: \	7 Help
1	Author Ad	
	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.

varrie.	Worry-Free 7zip extractor	
ocation:	1	
Author:	- And	
Description:	Worry-Free 7zip extractor Powershell script.	
Security opt When runn	ons ng the task, use the following user account:	
SYSTEM	Change User or Group	
Run only	when user is logged on	
O Run whe	ther user is logged on or not	
Don	ot store password. The task will only have access to local computer resources.	

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**.

New Trigger	$\times$
Begin the task: On a schedule ~	
One time       Start: 10/23/2019 ■▼ 10:41:36 AM ➡ Synchronize across time zones         ● Daily       Oweekly         ● Monthly       Recur every: 1 days	
Advanced settings       Delay task for up to (random delay):     1 hour       Repeat task every:     1 hour   for a duration of: 1 day	
Stop task if it runs longer than: 3 days	
Expire: 10/23/2020 Total:08 AM	
Enabled	
OK Cance	



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

When you creat	e a task, you must specify the action that will occur wh	en your task starts.
Action	Details	*
New	Edit Delete	



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



Settings		
Program/script:		Deeuree
Add arguments (optional):	powersh	ell.exe -executio
Start in (optional):		

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.

LogTime	Computer	Action	Device_Na me	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_e x.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	019-WFBS	Contoso	run.dll32	Device (Default)	-	C:\User\MyOffice Directory	Scheduled Scan	Storm Worm

#### TM Worry Free- Action taken on malware



#### Integrate Trend Micro Worry-Free

Figure 13

#### Sample Logs:

action	+- Arress blocked
addl info	+- run dll32
davica nama	+- 010.WEPC
uevice_nume	+- 015-W185
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="2019-09-10T19:0
	0:33-04:00" 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



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.

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://malwarel auncher.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://Uwatchf ree.torentz.co m/all+latest+ho	Randy Peter
10/21/2019 02:49:14 PM	WORRYFREE	Access to a website was blocked	Peachs- MacBook-Pro	-	Laptops	-3	High	http://Uwatchf ree.torentz.co m/all+latest+bo	Hemilton
10/21/2019 02:49:24 PM	WORRYFREE	Access to a website was blocked	Win123	Contoso	Desktops	-	Medium	http://malwarel auncher.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://Uwatchf ree.torentz.co m/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://Uwatchf ree.torentz.co m/all+latest+bo	Hemilton

#### **TM Worry Free Web reputation events**

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="Acc
	ess to a website was blocked" Device name="Peachs-MacBook-Pro" Domain="-" Generated="2019-09-10T1
	5:01:58-04:00" Group name="Laptops" IPv6 Address="-" Label="-" Received="2019-09-10T15:31:15-04:00" R
	isk Level="High" URL="http://Uwatchfree.torentz.com/all+latest+bollywood+3idiots/access+download+pat
	h" 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
<pre>src_domain_name</pre>	+
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

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

#### Figure 18

#### • TrendMicro 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

device_name	event_computer	src_domain_name	threat_name
019-WFBS	WorryFree	Contoso	Storm Worm
030-WS76	WorryFree	Contoso	Anna Kournikova
012-WFBS	WorryFree	Contoso	Wannacry
019-WFBS	WorryFree	Contoso	Storm Worm
030-WS76	WorryFree	Contoso	Anna Kournikova
012-WFBS	WorryFree	Contoso	Wannacry
019-WFBS	WorryFree	Contoso	Storm Worm
030-WS76	WorryFree	Contoso	Anna Kournikova
012-WFBS	WorryFree	Contoso	Wannacry
019-WFBS	WorryFree	Contoso	Storm Worm



# 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.





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

Parsing Rules			👚 / Admin / Parsing Rules
Parsing Rule Template			
Groups	Group : All	Search Q	CIT
Default	^		

Figure 23

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

Impo	ort		
select	ted file is: Template_TrendMicro Worry free.ettd	🗲 Browse	
	Template name	Separator	Template description
	TrendMicro Worry-Free - Action taken on malware	\n	<116>1 2019-09-10 19:00:33 10.3( 6.1.4.1.6101 Action Taken="Attemp ssful; No action taken" Device nam e name="ParalQUA_ex.dll" Genera up name="Device (Default)" IPv6 A nViewBranchDeposit\TR\TSBinfiles 00" Scan Type="Scheduled Scan" \
	TrendMicro Worry-Free - Web Reputation events	\n	<116>1 2019-09-10 15:31:15 10.3( ation@1.3.6.1.4.1.6101 Action="Ac name="Peachs-MacBook-Pro" Dor 1:58-04:00" Group name="Lantons



5. Templates are imported now successfully.







# 5.2 Knowledge Object

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

		🔎 🛛 Admin 🗸	Tools 🗸 🌔
Active Watch Lists	Event Filters	😥 Parsing Rules	♠/[
Alerts	Eventvault	Report Settings	_
Behavior Correlation Rules	FAQ Tile Configuration	Systems	
Behavior Correlation Settings	Group Management	Q Users	
Casebook Configuration	Q IP Lookup Configuration	r Weights	since the last 24 ho
● Category	·☆ Knowledge Objects	Windows Agent Config	
Diagnostics	🔯 Manager		



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"

Import		
KO_TrendMicro Worry free.etko	🗲 Browse Upload	
Figure 28		
	Netsurion Even	ltTracker

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

Import			×
Selec	t file		🖆 Browse Upload
•	Object name	Applies to	Group name
•	TM Worry Free All Events	Trend Micro AV	Trend Micro Worry Free
			Import Close

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)":

🐁 Export Import Utility	- 0	×
Export Import		
1. Provide the path and file nam 2. Click the Import button Note : If report(s) contains temp	me of Schedule Report file. Use the '' button to browse and locate the import file. plate, first import template and proceed with exportimport utility.	
Options	Location	
Category		
⊖ Filters		
◯ Alerts	O Legacy (* issch) ( New (*.etcnx)	
O Systems and Groups	Source : *issch	
O Token Value		
Reports		
O Behavior Correlation		
	Import Close	





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.

	· · ·							
🔂 Reports Im	port							>
Note : If report	(e) contains template, first import template	and proceed with report im	not process					
note : in report	(a) contains template, mat import template	and proceed with report in	poit process.					
Select file		h	Wony-Free Cor	figuration \Re	ports_TrendMicro Worry fr	ee.etcrx	Select file	
Available repor	ts		-					
litle		Frequency	Show all	•	લ લ			
	Title	Sites			Groups	Sy	stems	Frequency
	TrendMicro Wony-Free - Action taken	E						Undefined
	TrendMicro Worry-Free - Web reputati	2						Undefined
<								>
Note: Set nu	n time ontion is not applicable for Defined	Reports and Hourly Report	•					
Set run tin	ne for report(s) from	M • at interval of	i minute	es Set	Û			
Replace	to		Rep	ace A	sign systems			
					Note: Make sure that Site	(s), Group(s) and Syst	em(s) selections are v	alid. II 🛞

Figure 31

3. EventTracker displays a success message:



Figure 32

## 5.4 Dashboard

- 1. Login to EventTracker.
- 2. Navigate to **Dashboard**  $\rightarrow$  **My Dashboard**.
- 3. In "My Dashboard", click Import Button:



≡	Event <b>Tracker</b> ⊕	
	Home	
۹	My Dashboard	
2	Threats	
	Incidents	
	Behavior Correlation	
	Change Audit	
	Compliance	
	Figure 33	
	🕈 / Dashboard / My Dashboar	ď
	0 🖉 🕼 🌣 👔 🗊	i
	Import configu	uration



- 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.





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







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.

(	Customize dashlets			×	
	TM			Q	
ſ	☑ TM Worry Free - Action taken o	☑ TM Worry Free - Action taken o	TM Worry Free - All events	✓ TM Worry Free - Threats by dev	
Ì					
				Add Delete Close	

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.



Parsing Rules				
Parsing Rule Template				
Groups		Ð		Group : TM Worry Free
EventTracker	Ĩ	1	^	
ForeScout CounterAct		1		Template Name
FortiNAC		1	11	TM Worry Free - Virus/Malware Information
JIRA Service Desk	III.	1		TM Worry Free - Web Reputation
Netgear Prosafe	Ĩ	1	11	
Proofpoint	Ē	1	11	
RSA SecurID	Ē	1	15	
SalesForce	Ē	1		
SentinelOne	Ē	1		
TM Worry Free	Ĩ.	1		
Windows	Ī	1		



# 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.

Knowledge Objects					
Search objects	ଦ୍ ହ	Ad	tivate Now		
Groups	🕀 🧭 🗓	Objec	t name TM Worry Free All Events		٦
JIRA Service Desk	^	Applie	s to Trend Micro AV		
Netgear Prosafe		Rules			
■ ORACLE			Title	Log type	
		+	TM: Worry Free All Events		
+ PoliWall			Message Signature:		
■ Proofpoint			Message Exception:		
RSA SecuriD			Expressions		
			Expression type	Expression 1	
Salesforce			Regular Expression	(? <key>[a-zA-Z/\s]+)="(?<value>[^"]</value></key>	+)"
■ SentinelOne			Regular Expression	\[Log(? <log_type>[^@]+)</log_type>	
EP Cloud					
Sonicwall UTM					
Trend Micro Worry Free					
TM Worry Free All Events	Ø 🗓				
♥ untangle					

Figure 39



### 6.3 Flex Reports

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





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

	Repor	t Configuration						
٦	Sch	eduled 🔘 Queued 💿 Defined						
ż.	Report	t Groups		$\oplus$		Repo	rts configura	tion: TM Worry Free Security
	2.1.2	riex			*	•	Î 2,	
		Amazon AWS	Ē	Ø				
		ConnectWise Manage	Ű	1		0	M	litle
	B	Cybereason	۱.	Ø		-	2.2.3	TM Worry Free Web reputation events
		EventTracker	Ē	1			1	TM Worry Free Action taken on malwar
		ForeScout CounterAct	Û	1				
		ORACLE	Ĩ	1				
		SEP Cloud	Ē.	Ø				
		TM Worry Free Securi	前	(A)				



### 6.4 Dashboard

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





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



# Integrate Trend Micro Worry-Free



Figure 43

