How to - Configure Trend Micro Worry-Free to forward logs to EventTracker

EventTracker v9.0 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.

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.

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_learning,network_virus,dlp
storage_path = ./logs/
```

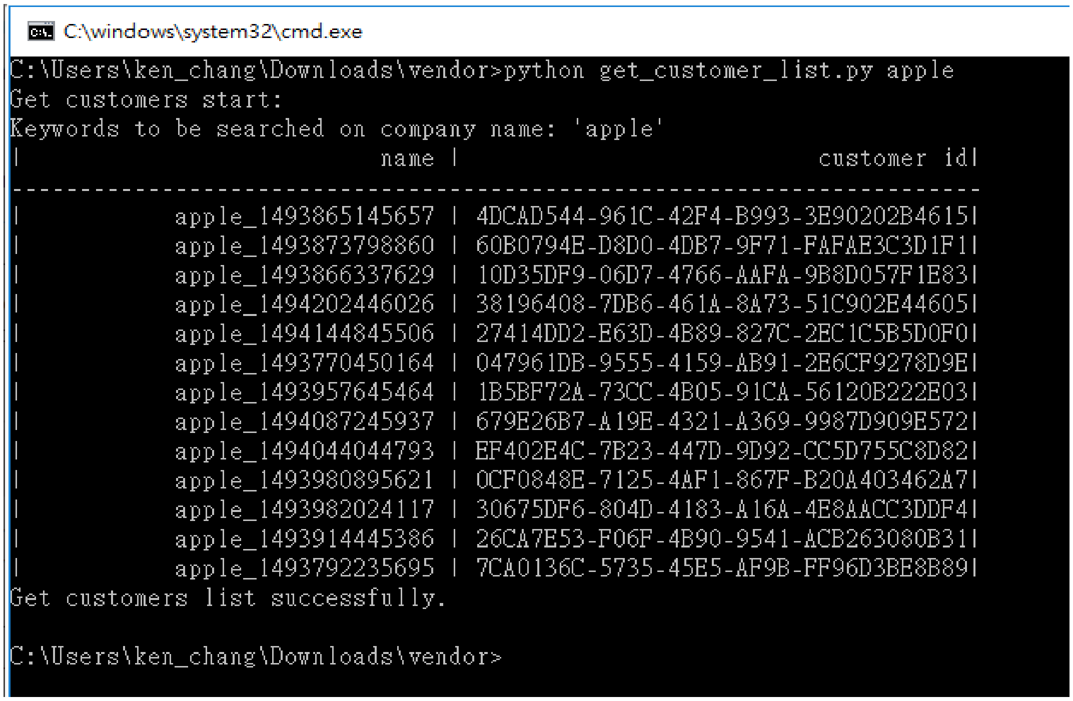
- **ACCESS_TOKEN** is one of the CSPI key pair provided by the Product Manager.
- **SECRET_KEY** is one of the CSPI key pair provided by the Product Manager.
- **SERVER_HOSTNAME** is the CSPI FQDN (no need to change).
- **SERVER_PORT** should be 443 (no need to change).
- **public_file_path** is the 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.



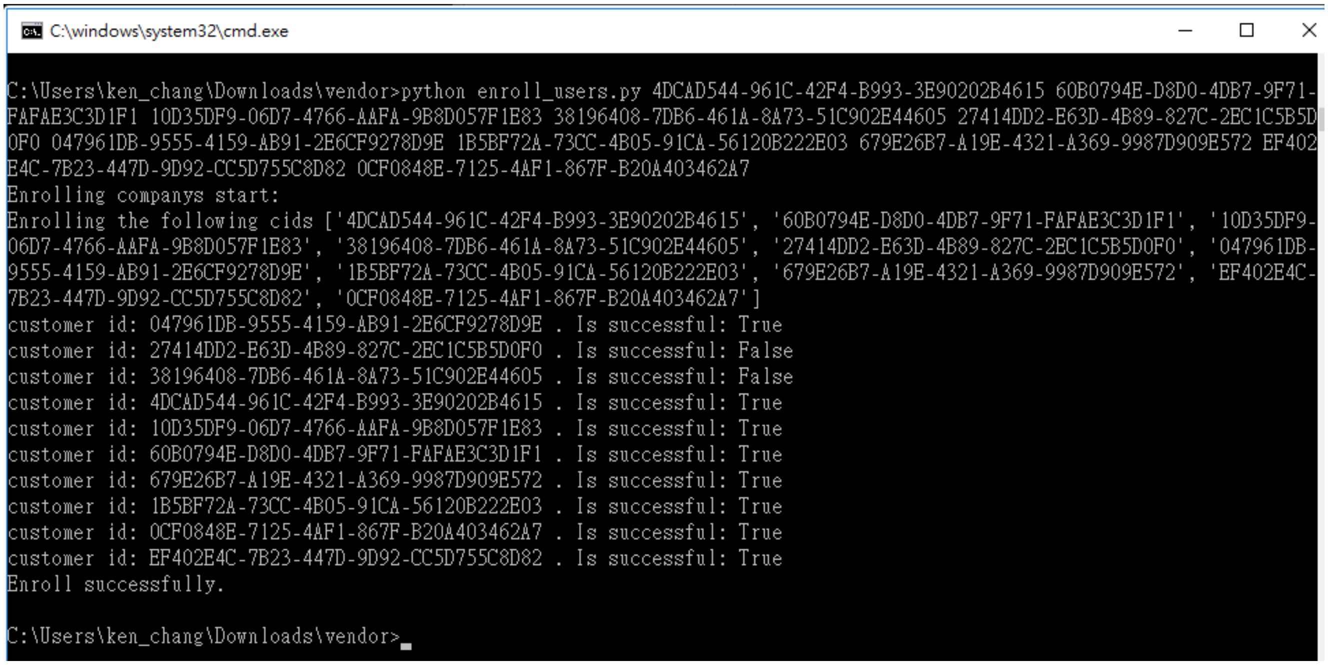
```
C:\Users\ken_chang\Downloads\vendor>python get_customer_list.py apple
Get customers start:
Keywords to be searched on company name: 'apple'
|                     name |                        customer id|
-----------------------------------------------------------------
|          apple_1493865145657 | 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 | 0CF0848E-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>
```

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



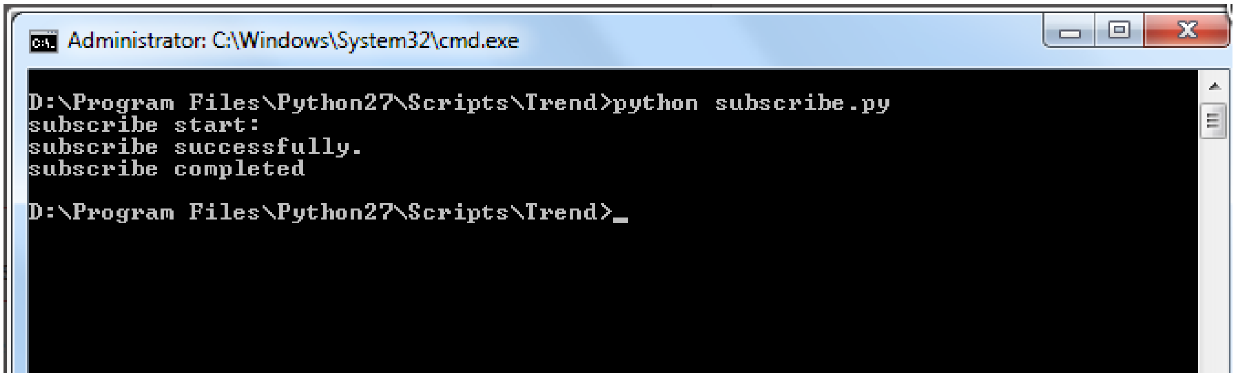
```
C:\Users\ken_chang\Downloads\vendor>python enroll_users.py 4DCAD544-961C-42F4-B993-3E90202B4615 60B0794E-D8D0-4DB7-9F71-
FAFAE3C3D1F1 10D35DF9-06D7-4766-AAFA-9B8D057F1E83 38196408-7DB6-461A-8A73-51C902E44605 27414DD2-E63D-4B89-827C-2EC1C5B5D
0F0 047961DB-9555-4159-AB91-2E6CF9278D9E 1B5BF72A-73CC-4B05-91CA-56120B222E03 679E26B7-A19E-4321-A369-9987D909E572 EF402
E4C-7B23-447D-9D92-CC5D755C8D82 0CF0848E-7125-4AF1-867F-B20A403462A7
Enrolling companys start:
Enrolling the following cids ['4DCAD544-961C-42F4-B993-3E90202B4615', '60B0794E-D8D0-4DB7-9F71-FAFAE3C3D1F1', '10D35DF9-
06D7-4766-AAFA-9B8D057F1E83', '38196408-7DB6-461A-8A73-51C902E44605', '27414DD2-E63D-4B89-827C-2EC1C5B5D0F0', '047961DB-
9555-4159-AB91-2E6CF9278D9E', '1B5BF72A-73CC-4B05-91CA-56120B222E03', '679E26B7-A19E-4321-A369-9987D909E572', 'EF402E4C-
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: 4DCAD544-961C-42F4-B993-3E90202B4615 . Is successful: True
customer id: 10D35DF9-06D7-4766-AAFA-9B8D057F1E83 . Is successful: True
customer id: 60B0794E-D8D0-4DB7-9F71-FAFAE3C3D1F1 . Is successful: True
customer id: 679E26B7-A19E-4321-A369-9987D909E572 . Is successful: True
customer id: 1B5BF72A-73CC-4B05-91CA-56120B222E03 . Is successful: True
customer id: 0CF0848E-7125-4AF1-867F-B20A403462A7 . Is successful: True
customer id: EF402E4C-7B23-447D-9D92-CC5D755C8D82 . Is successful: True
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



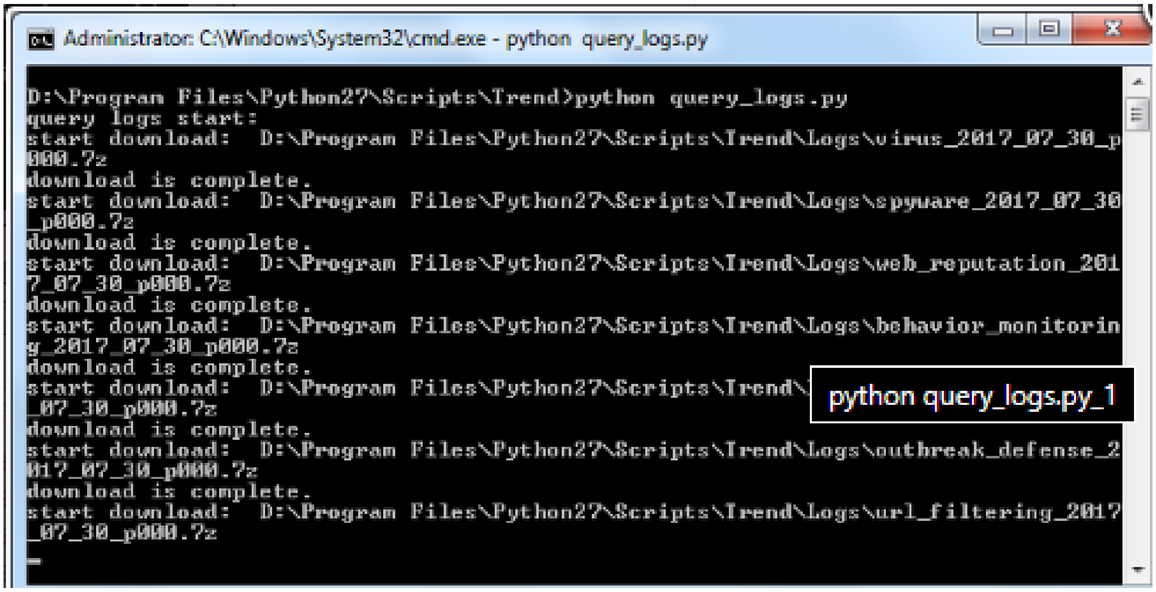
```
D:\Program Files\Python27\Scripts\Trend>python subscribe.py
subscribe start:
subscribe successfully.
subscribe completed

D:\Program Files\Python27\Scripts\Trend>_
```

Figure 3

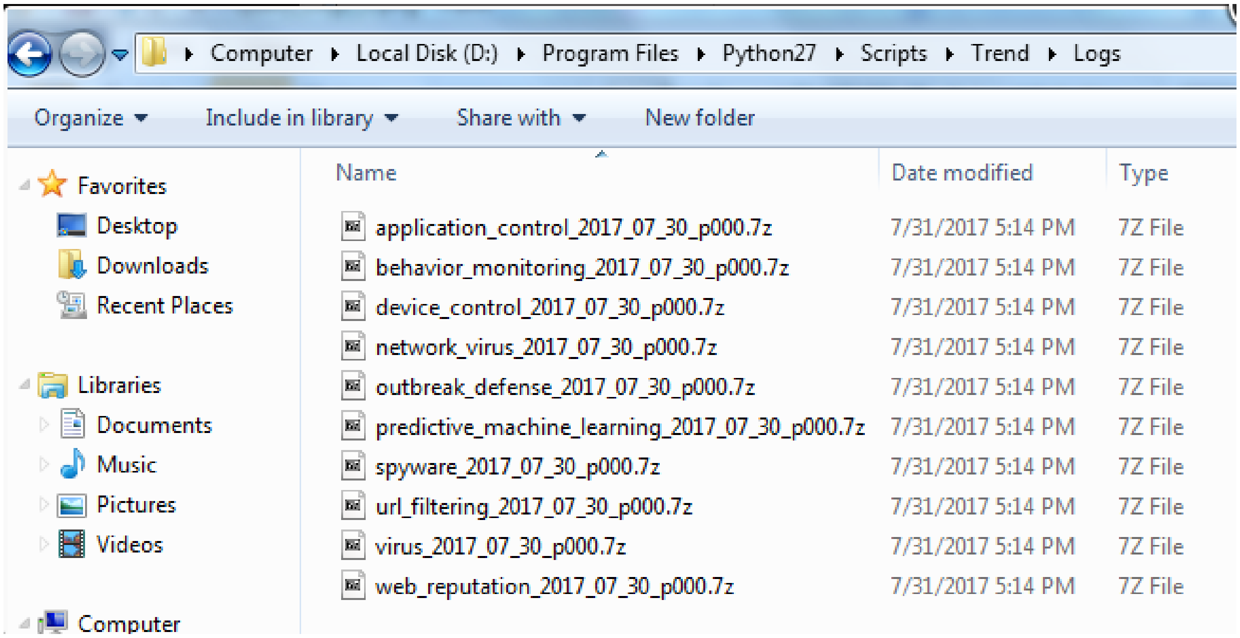
4. Query and download the log archive. Open Windows Command Prompt and run the following command:

   # 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
python query_logs.py_1

```
D:\Program Files\Python27\Scripts\Trend>python query_logs.py
query logs start:
start download:  D:\Program Files\Python27\Scripts\Trend\Logs\virus_2017_07_30_p
000.7z
download is complete.
start download:  D:\Program Files\Python27\Scripts\Trend\Logs\spyware_2017_07_30
_p000.7z
download is complete.
start download:  D:\Program Files\Python27\Scripts\Trend\Logs\web_reputation_201
7_07_30_p000.7z
download is complete.
start download:  D:\Program Files\Python27\Scripts\Trend\Logs\behavior_monitorin
g_2017_07_30_p000.7z
download is complete.
start download:  D:\Program Files\Python27\Scripts\Trend\
_07_30_p000.7z
download is complete.
start download:  D:\Program Files\Python27\Scripts\Trend\Logs\outbreak_defense_2
017_07_30_p000.7z
download is complete.
start download:  D:\Program Files\Python27\Scripts\Trend\Logs\url_filtering_2017
_07_30_p000.7z
_
```

Figure 4



Name	Date modified	Type
application_control_2017_07_30_p000.7z	7/31/2017 5:14 PM	7Z File
behavior_monitoring_2017_07_30_p000.7z	7/31/2017 5:14 PM	7Z File
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
outbreak_defense_2017_07_30_p000.7z	7/31/2017 5:14 PM	7Z File
predictive_machine_learning_2017_07_30_p000.7z	7/31/2017 5:14 PM	7Z File
spyware_2017_07_30_p000.7z	7/31/2017 5:14 PM	7Z File
url_filtering_2017_07_30_p000.7z	7/31/2017 5:14 PM	7Z File
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

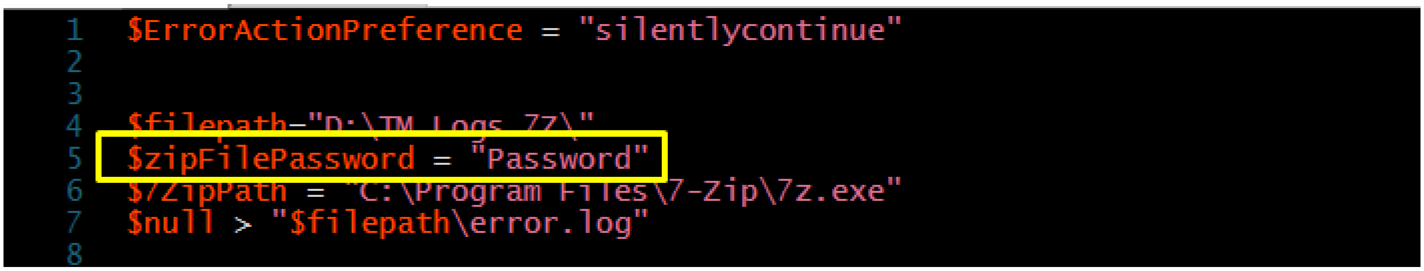
Figure 5

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.



```
$ErrorActionPreference = "silentlycontinue"


$filepath="D:\TM Logs 7Z\"
$zipFilePassword = "Password"
$7ZipPath = "C:\Program Files\7-Zip\7z.exe"
$null > "$filepath\error.log"

```

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**".

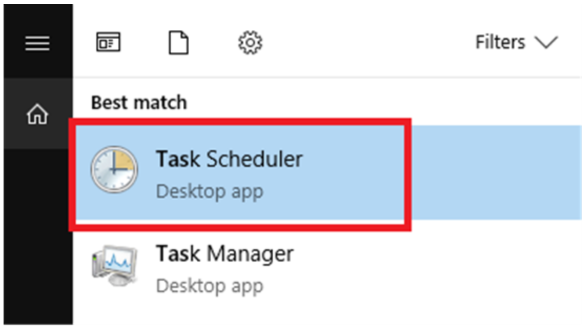


Figure 7

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

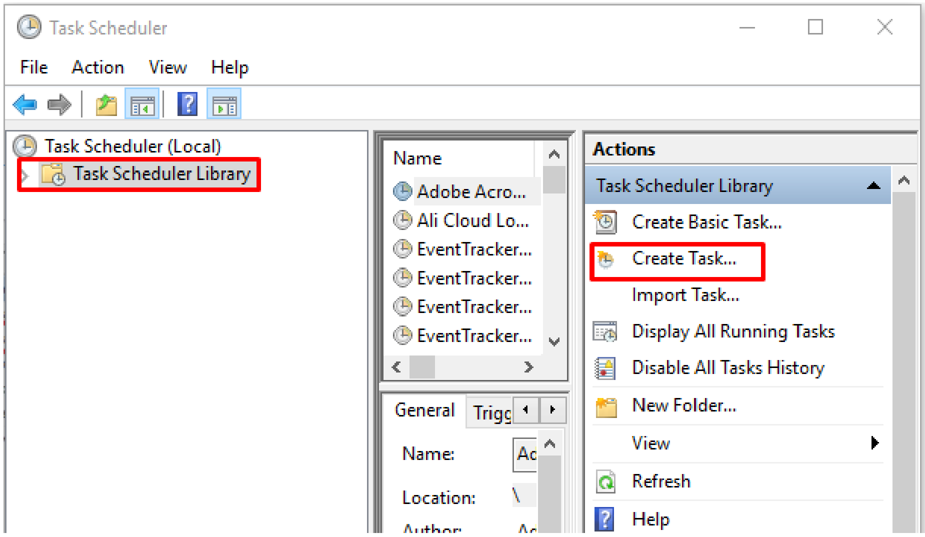
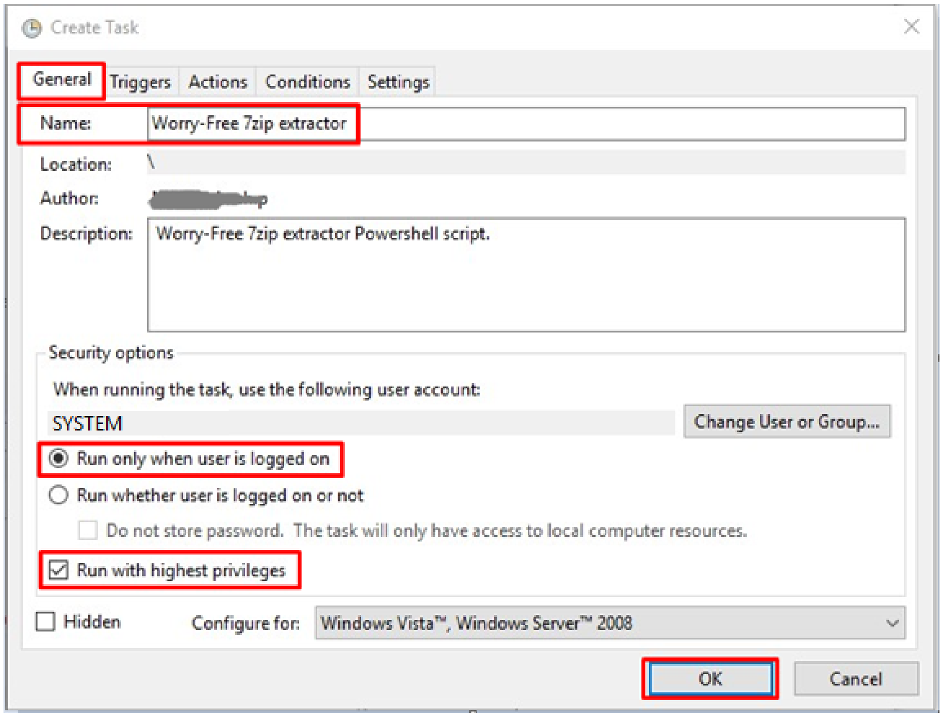


Figure 8

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.



Create Task

Name: Worry-Free 7zip extractor

Location: \

Author: [redacted]

Description: Worry-Free 7zip extractor Powershell script.

Security options

When running the task, use the following user account:

SYSTEM

● Run only when user is logged on

○ Run whether user is logged on or not

□ Do not store password. The task will only have access to local computer resources.

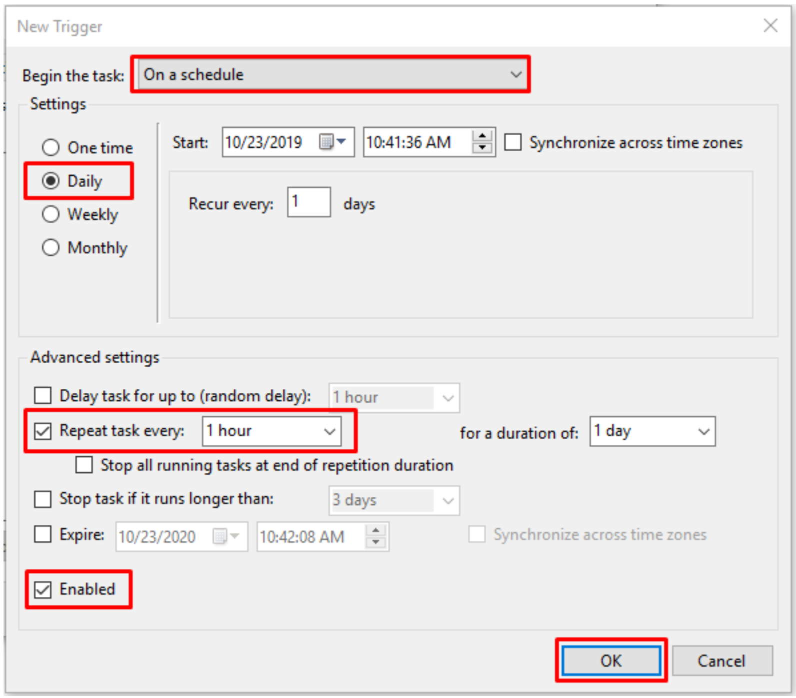
☑ Run with highest privileges

□ Hidden

Configure for: Windows Vista™, Windows Server™ 2008

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

Begin the task: On a schedule

Settings

○ One time
● Daily
○ Weekly
○ Monthly

Start: 10/23/2019 10:41:36 AM □ Synchronize across time zones

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 all running tasks at end of repetition duration

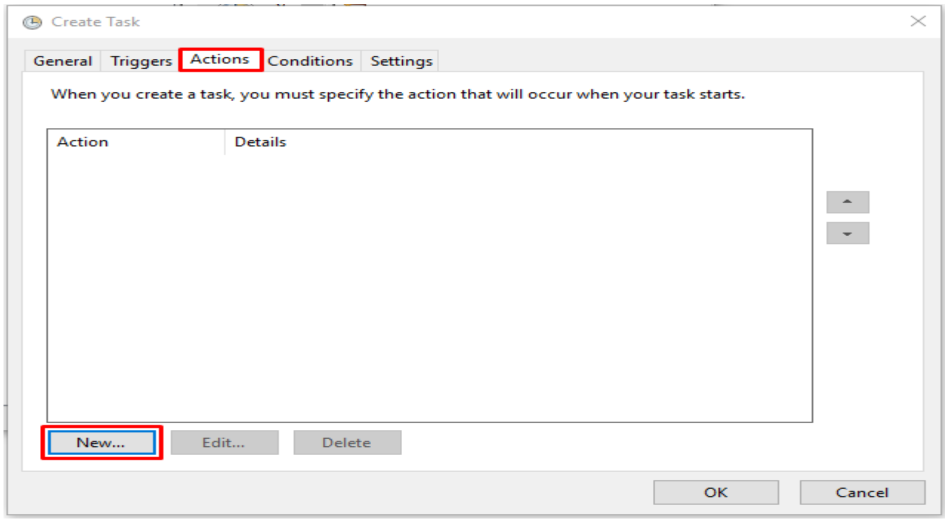
□ Stop task if it runs longer than: 3 days

□ Expire: 10/23/2020 10:42:08 AM □ Synchronize across time zones

☑ Enabled

Figure 10

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



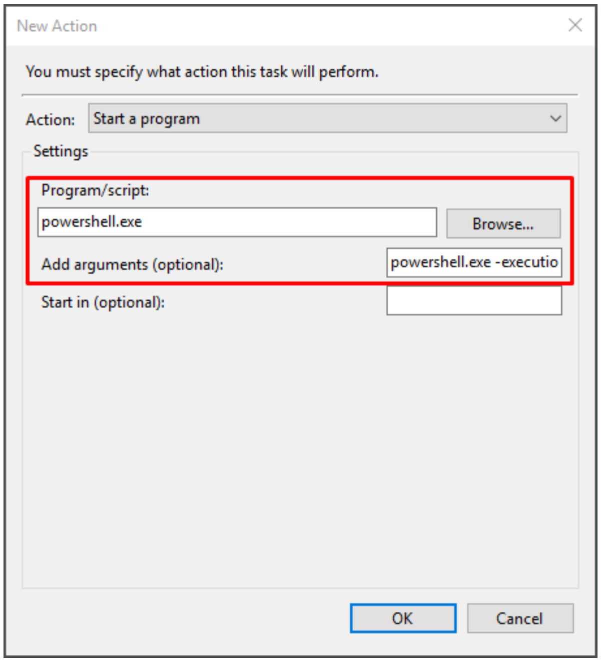
When you create a task, you must specify the action that will occur when your task starts.

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



You must specify what action this task will perform.

Action: Start a program

Program/script: powershell.exe

Add arguments (optional): powershell.exe -executio

Start in (optional):

Figure 12

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