Netsurion™ | EventTracker

How to- Configure Windows Defender to forward logs to EventTracker

EventTracker v9.x and above

Publication Date: August 5, 2019

Abstract

This guide provides instructions to retrieve Windows Defender event logs and integrate it with EventTracker. Once EventTracker is configured to collect and parse these logs, dashboard and reports can be configured to monitor Windows Defender.

Audience

The configurations detailed in this guide are consistent with EventTracker version v9.x or above and Windows Defender for Windows 10 and Windows Server 2016.

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

Overview

EventTracker collects the event logs delivered from Windows Defender and filters them out to get some critical event types for creating reports, dashboard, and alerts. Among the event types, we are considering: Malware detected, Suspicious behavior detected, Windows defender configuration changes, Action taken on threats, Engine updates, Antivirus real-time protection disabled, Scan failed, etc.

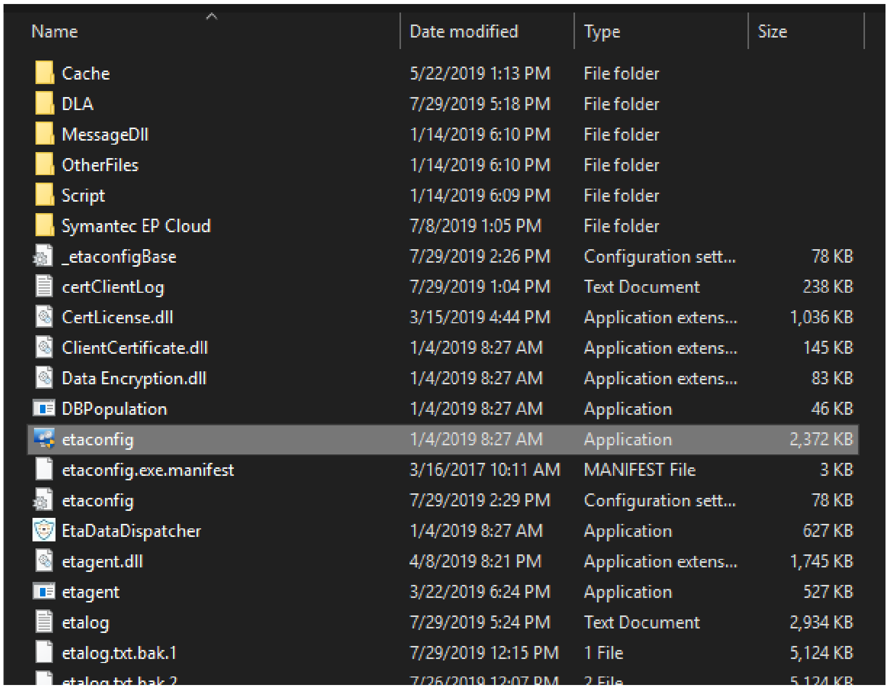
Prerequisites

- EventTracker agent must be installed in a host system/server.
- **ET91U19-031.exe** update must be installed before configuring this KP-item, in EventTracker manager.

Configuring Windows Defender to forward the log to EventTracker

Configuring Eventtracker Event Filter

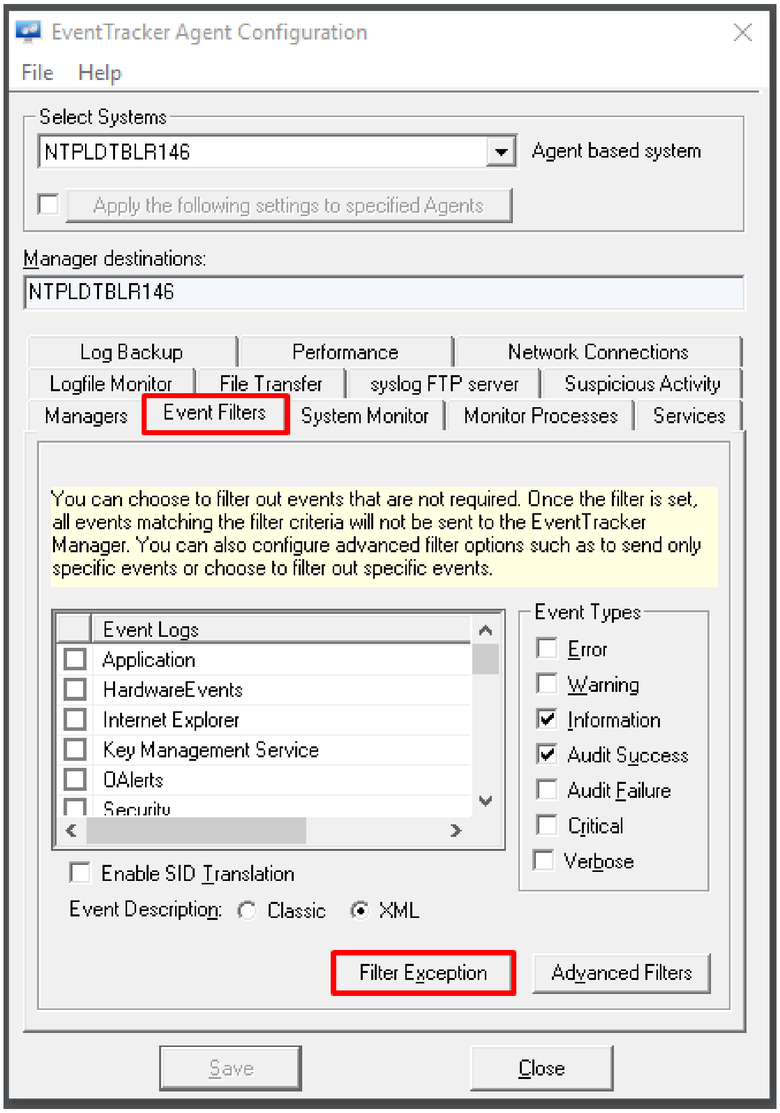
1. Follow the file path of EventTracker Agent configuration –
   C:\Program Files (x86)\Prism Microsystems\EventTracker\Agent
2. Double click on "**etaconfig**" application to launch "**Eventtracker Agent Configuration".**



Name	Date modified	Type	Size
Cache	5/22/2019 1:13 PM	File folder	
DLA	7/29/2019 5:18 PM	File folder	
MessageDll	1/14/2019 6:10 PM	File folder	
OtherFiles	1/14/2019 6:10 PM	File folder	
Script	1/14/2019 6:09 PM	File folder	
Symantec EP Cloud	7/8/2019 1:05 PM	File folder	
_etaconfigBase	7/29/2019 2:26 PM	Configuration sett...	78 KB
certClientLog	7/29/2019 1:04 PM	Text Document	238 KB
CertLicense.dll	3/15/2019 4:44 PM	Application extens...	1,036 KB
ClientCertificate.dll	1/4/2019 8:27 AM	Application extens...	145 KB
Data Encryption.dll	1/4/2019 8:27 AM	Application extens...	83 KB
DBPopulation	1/4/2019 8:27 AM	Application	46 KB
etaconfig	1/4/2019 8:27 AM	Application	2,372 KB
etaconfig.exe.manifest	3/16/2017 10:11 AM	MANIFEST File	3 KB
etaconfig	7/29/2019 2:29 PM	Configuration sett...	78 KB
EtaDataDispatcher	1/4/2019 8:27 AM	Application	627 KB
etagent.dll	4/8/2019 8:21 PM	Application extens...	1,745 KB
etagent	3/22/2019 6:24 PM	Application	527 KB
etalog	7/29/2019 5:24 PM	Text Document	2,934 KB
etalog.txt.bak.1	7/29/2019 12:15 PM	1 File	5,124 KB
etalog.txt.bak.2	7/26/2019 12:07 PM	2 File	5,124 KB

Figure 1

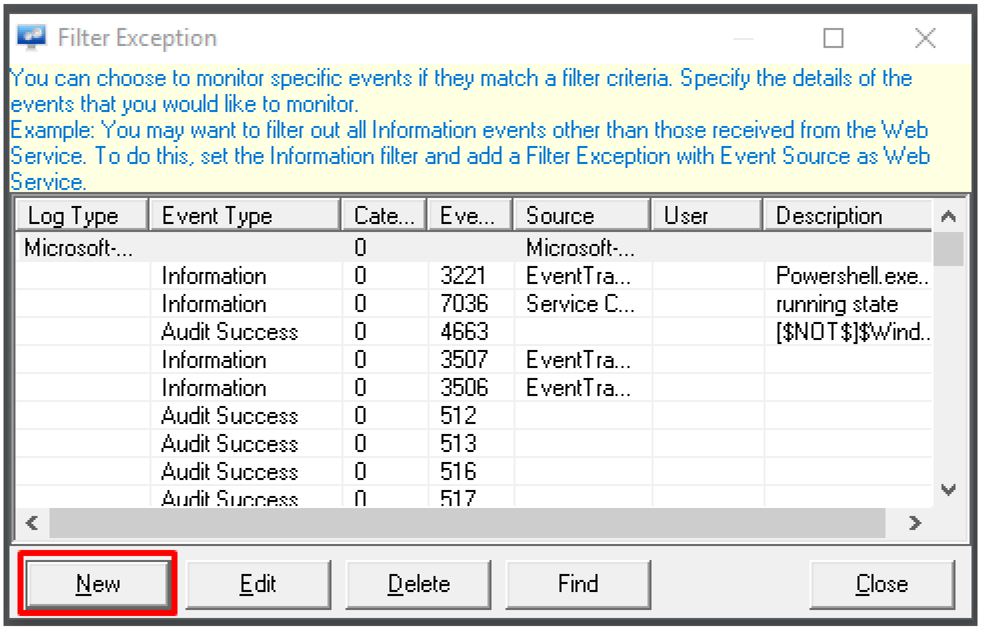
3. Navigate to **Event Filters>Filter Exception.**



You can choose to filter out events that are not required. Once the filter is set, all events matching the filter criteria will not be sent to the EventTracker Manager. You can also configure advanced filter options such as to send only specific events or choose to filter out specific events.

Figure 2

4. Click **New** and compose **Event Details**.

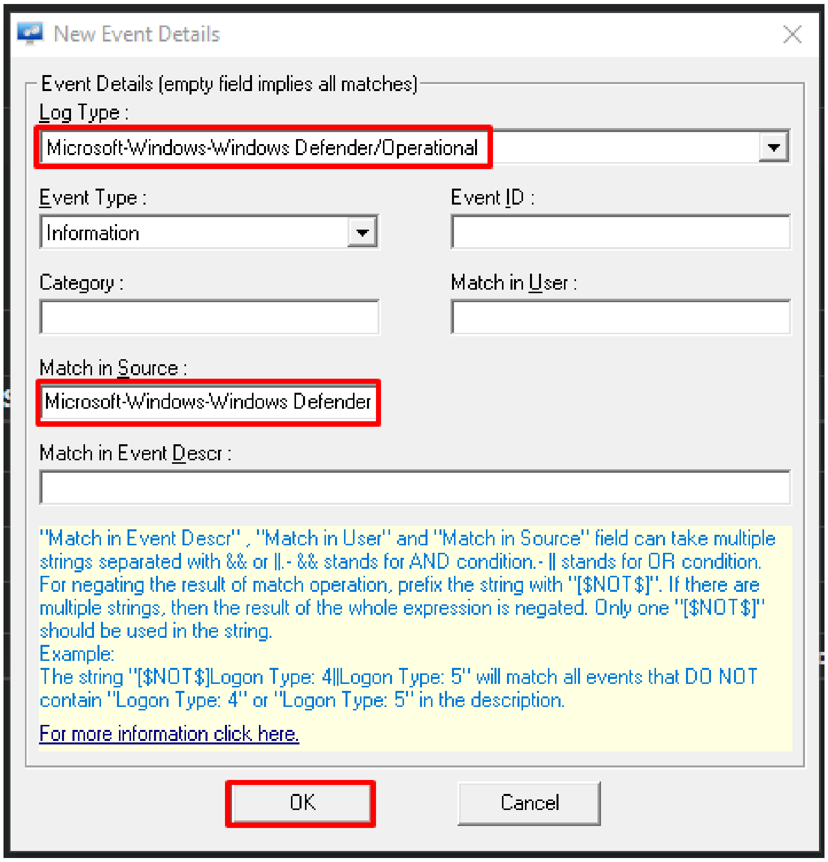


You can choose to monitor specific events if they match a filter criteria. Specify the details of the events that you would like to monitor.
Example: You may want to filter out all Information events other than those received from the Web Service. To do this, set the Information filter and add a Filter Exception with Event Source as Web Service.

Log Type	Event Type	Cate...	Eve...	Source	User	Description
Microsoft-...		0		Microsoft-...		
	Information	0	3221	EventTra...		Powershell.exe..
	Information	0	7036	Service C...		running state
	Audit Success	0	4663			[NOT]$Wind..
	Information	0	3507	EventTra...		
	Information	0	3506	EventTra...		
	Audit Success	0	512			
	Audit Success	0	513			
	Audit Success	0	516			
	Audit Success	0	517			

Figure 3

5. Select **Log Type Microsoft-Windows-Windows Defender/Operational,** match it in source **Microsoft-Windows-Windows Defender** and click on **OK**.



Event Details (empty field implies all matches)

Log Type : Microsoft-Windows-Windows Defender/Operational

Event Type : Information

Event ID :

Category :

Match in User :

Match in Source : Microsoft-Windows-Windows Defender

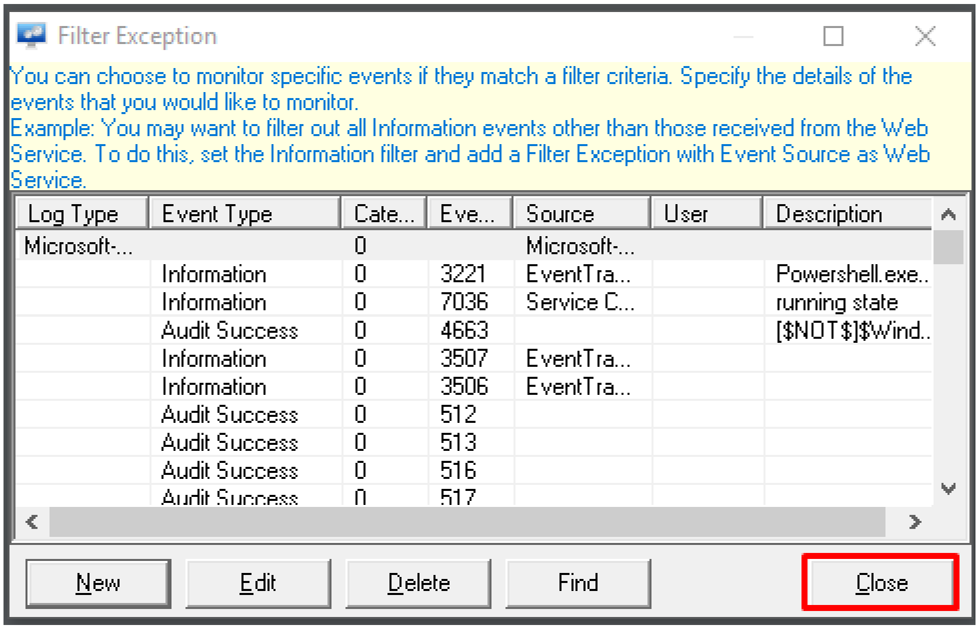
Match in Event Descr :

"Match in Event Descr" , "Match in User" and "Match in Source" field can take multiple strings separated with && or ||.- && stands for AND condition.- || stands for OR condition.
For negating the result of match operation, prefix the string with "[NOT]". If there are multiple strings, then the result of the whole expression is negated. Only one "[NOT]" should be used in the string.
Example:
The string "[NOT]Logon Type: 4||Logon Type: 5" will match all events that DO NOT contain "Logon Type: 4" or "Logon Type: 5" in the description.

For more information click here.

Figure 4

6. Click **Close** and save to apply the changes.



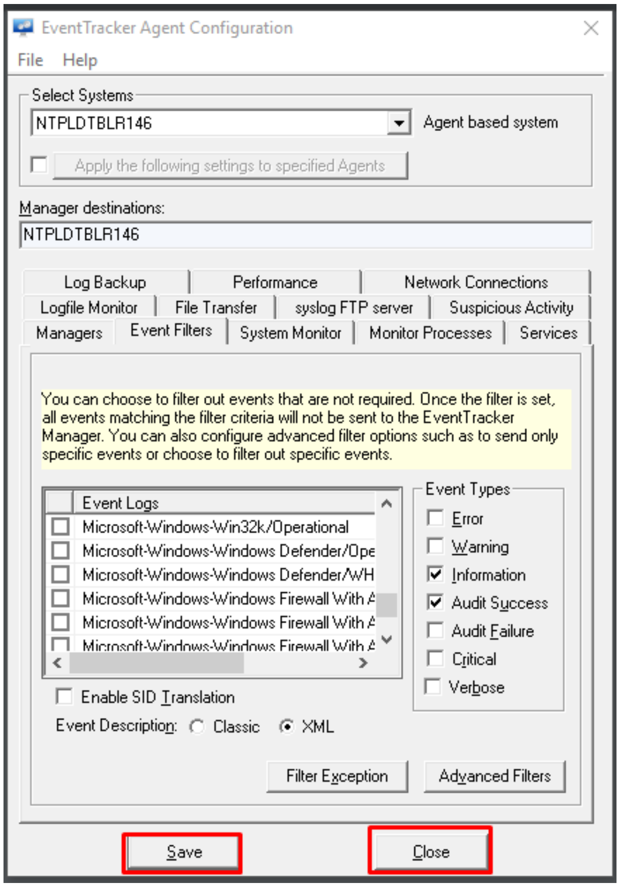
Filter Exception

You can choose to monitor specific events if they match a filter criteria. Specify the details of the events that you would like to monitor.
Example: You may want to filter out all Information events other than those received from the Web Service. To do this, set the Information filter and add a Filter Exception with Event Source as Web Service.

Log Type	Event Type	Cate...	Eve...	Source	User	Description
Microsoft-...		0		Microsoft-...		
	Information	0	3221	EventTra...		Powershell.exe..
	Information	0	7036	Service C...		running state
	Audit Success	0	4663			[NOT]$Wind..
	Information	0	3507	EventTra...		
	Information	0	3506	EventTra...		
	Audit Success	0	512			
	Audit Success	0	513			
	Audit Success	0	516			
	Audit Success	0	517			

Figure 5

7. Click **Save** and close **Eventtracker Agent configuration**.



EventTracker Agent Configuration

Select Systems

NTPLDTBLR146 Agent based system

□ Apply the following settings to specified Agents

Manager destinations:

NTPLDTBLR146

You can choose to filter out events that are not required. Once the filter is set, all events matching the filter criteria will not be sent to the EventTracker Manager. You can also configure advanced filter options such as to send only specific events or choose to filter out specific events.

Event Logs
- □ Microsoft-Windows-Win32k/Operational
- □ Microsoft-Windows-Windows Defender/Ope
- □ Microsoft-Windows-Windows Defender/WH
- □ Microsoft-Windows-Windows Firewall With A
- □ Microsoft-Windows-Windows Firewall With A
- □ Microsoft-Windows-Windows Firewall With A

Event Types
- □ Error
- □ Warning
- ☑ Information
- ☑ Audit Success
- □ Audit Failure
- □ Critical
- □ Verbose

□ Enable SID Translation

Event Description: ○ Classic ● XML

Figure 6