

Monitor Suspicious Activity

Abstract

This update will allow the user(s) to monitor and terminate suspicious activity for the EventTracker agent and helps in avoiding any unsafe connection to external IP address and internal unsafe activities.

Audience

This guide is intended for customers using EventTracker v9.0 build 18. It assumes that you have EventTracker access and understanding of networking technologies.

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.

Process to be followed after applying the update

After applying the update,

1. Go to **EventTracker Control Panel** and double click **EventTracker Agent Configuration**.
2. Click the **Suspicious Activity** tab.

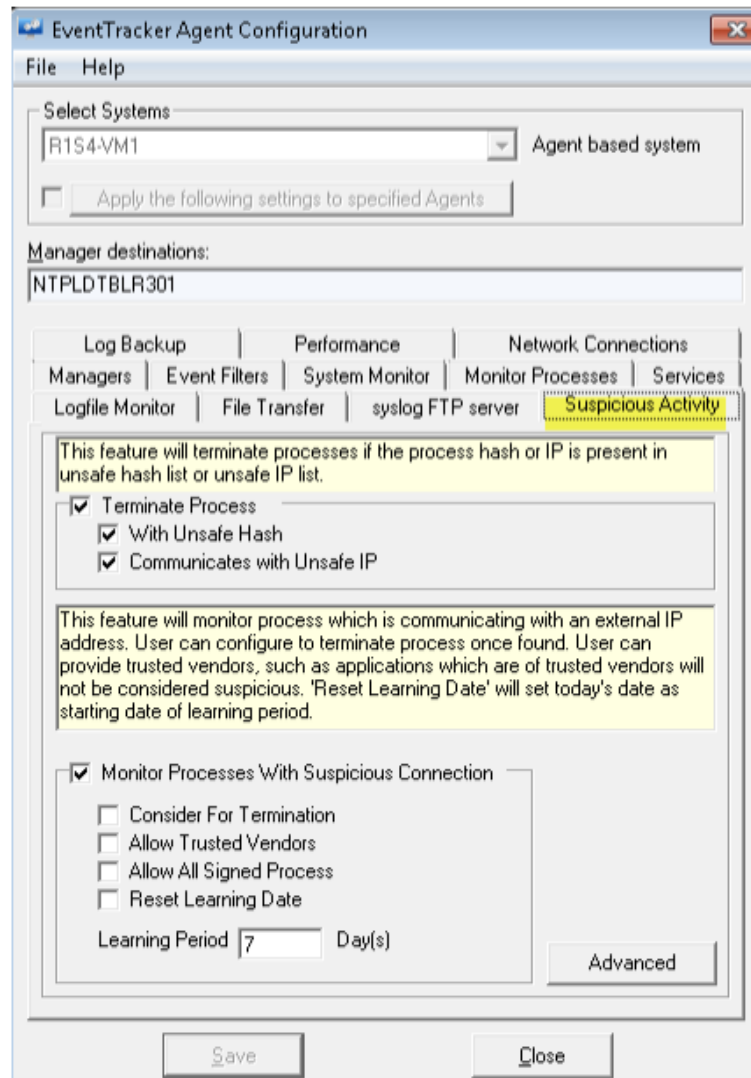


Figure 1

3. Select **Terminate process** option to block any process hash or IP present in **unsafe hash list** or the **unsafe IP list**.

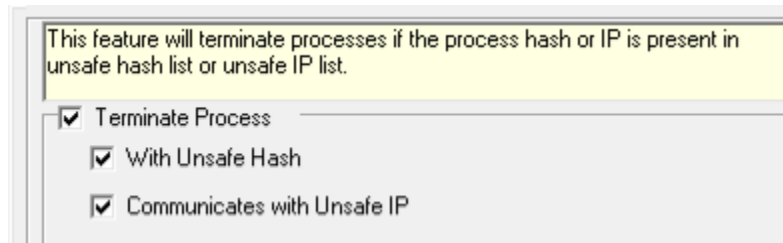


Figure 2

4. Select **Monitoring Suspicious Processes** option to monitor the process that is trying to connect to an external IP address.

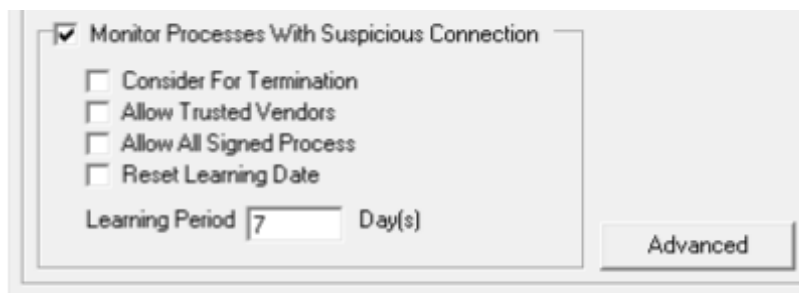


Figure 3

5. Enter number of days in the **learning period field** to configure the learning period for the agent.

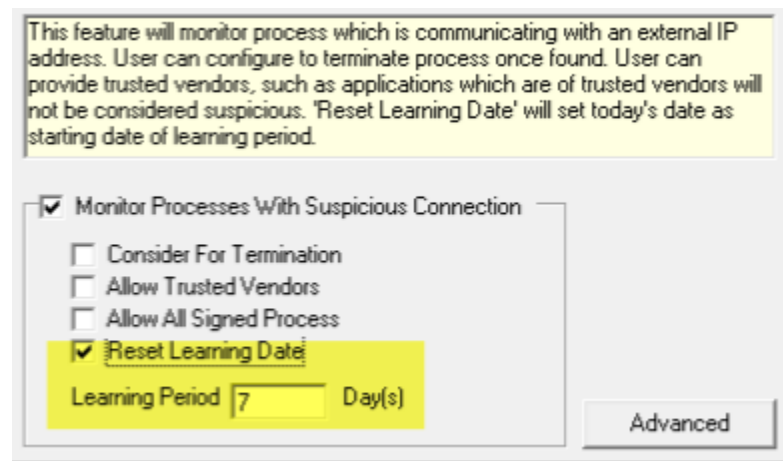


Figure 4

6. Before enabling the “**Allow Trusted Vendors**” option, create the Signer file “**VENDORSIGNERQ_DATA.safe**” and Product Name file “**VENDORPRODUCTQ_DATA.safe**” manually in the **EventTracker\Agent\Cache** path.
7. Click the **Advanced** option.
This option monitors the launching process.

NOTE: Whitelist file “**WHT_HLST.safe**” should be available in the exact path and monitor process does not have any learning period.

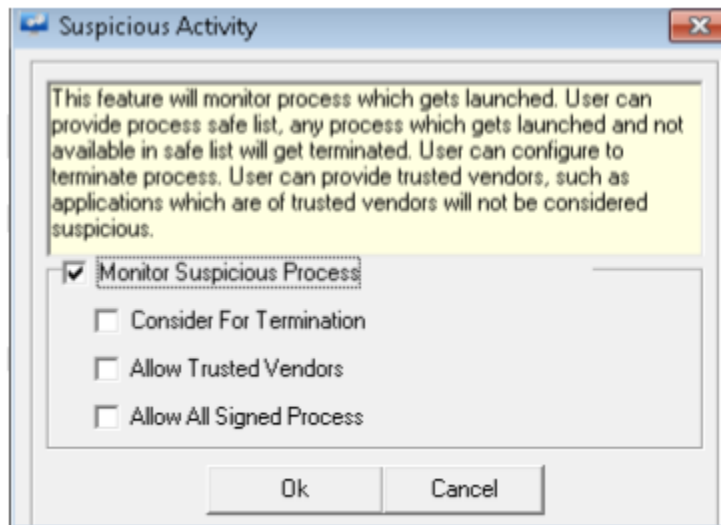


Figure 5

NOTE: If the user enables the option “**Apply Agent Configuration across Enterprise**” while changing the configuration, the **suspicious activity** option is enabled in the window as shown below:

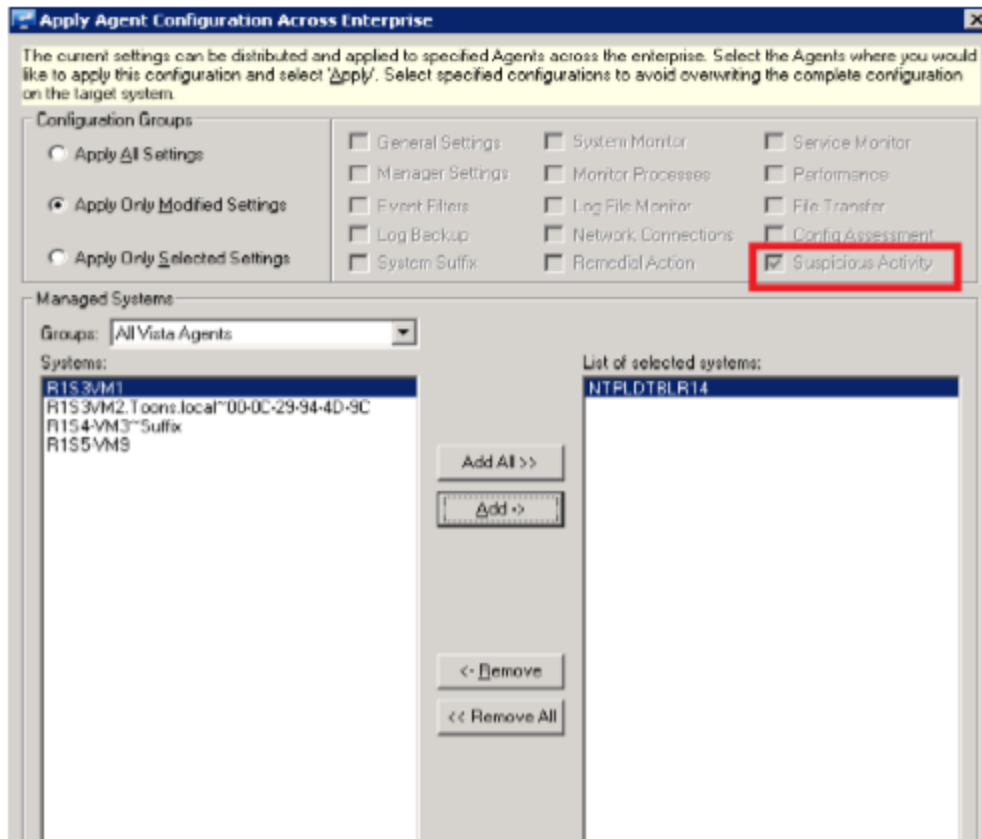


Figure 6

Creating Safelist Files

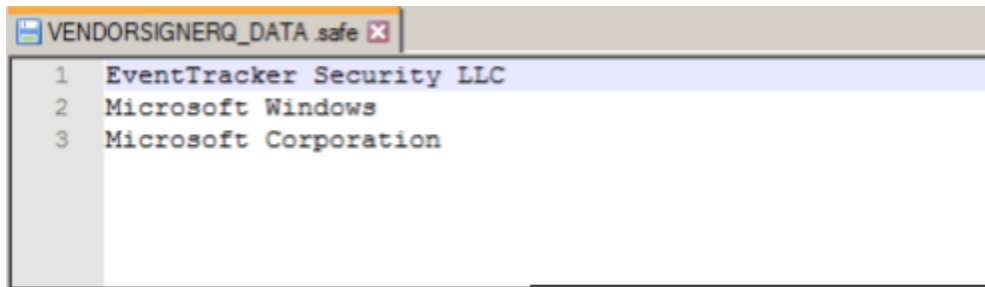
1. **FOLDERQ_DATA.safe**: Create a file using the name “**FOLDERQ_DATA.safe**” and add the folder names or the exact path. To add multiple folder/path, use the separator as “new line” or “Enter”.

Example:



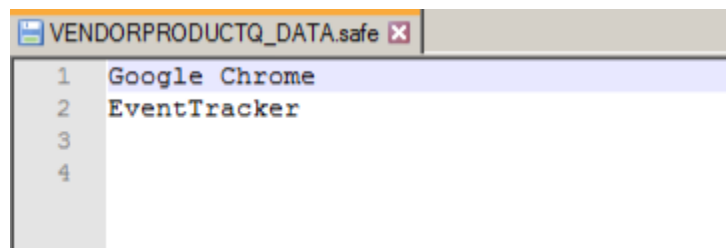
Figure 7

- VENDOR safe lists:** Create a file using the name “**VENDORSIGNERQ_DATA.safe**” and add the Vendor signer. To add multiple Vendors signer, use the separator as “new line” or “Enter”.
Create a file using the name “**VENDORPRODUCTQ_DATA.safe**” and add the Vendor name same as the signer.

Example:

```
VENDORSIGNERQ_DATA.safe
1 EventTracker Security LLC
2 Microsoft Windows
3 Microsoft Corporation
```

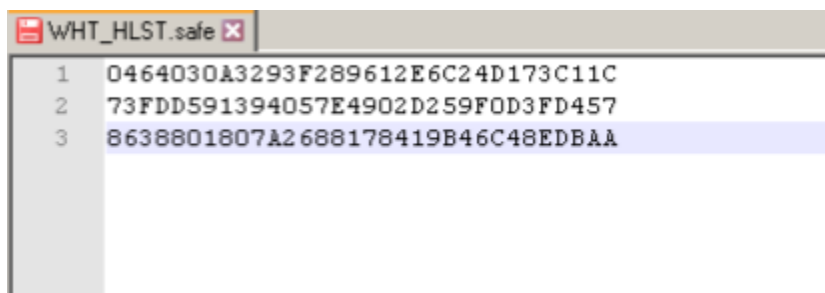
Figure 8



```
VENDORPRODUCTQ_DATA.safe
1 Google Chrome
2 EventTracker
3
4
```

Figure 9

- WHT_HLST.safe:** Create a file using the name “**WHT_HLST.safe**” and add the Hash value. To add multiple Hash value, use the separator as “new line” or “Enter”.

Example:

```
WHT_HLST.safe
1 0464030A3293F289612E6C24D173C11C
2 73FDD591394057E4902D259F0D3FD457
3 8638801807A2688178419B46C48EDBAA
```

Figure 10

4. **FOLDERQ_DATA.unsafe**: Create file using the name “**FOLDERQ_DATA.unsafe**” and add the folder names or the exact path. To add multiple folder/path, use the separator as “new line” or “Enter”.
5. **PPROCESS_DATA.safe**: Create file using the name “**PPROCESS_DATA.safe**” and add the process name or the exact path. To add multiple processes/path, use the separator as “new line” or “Enter”.

PPROCESS_DATA.safe file contains parent process detail and will allow the child process not to terminate.

6. **PPROCESS_DATA.unsafe**: Create file using the name “**PPROCESS_DATA.unsafe**” and add the process name or the exact path. To add multiple processes/path, use the separator as “new line” or “Enter”.

PPROCESS_DATA.unsafe file contains parent process detail and will terminate the child processes.

NOTE: Before adding the parent process to the **PPROCESS_DATA.safe** list and **PPROCESS_DATA.unsafe** list, parent process must be added to the **WHT_HLST.safe** file.

The above-mentioned files should be created in **EventTracker\Agent\Cache** path.

Name	Date modified	Type	Size
WHT_HLST.safe	8/30/2018 2:22 PM	SAFE File	3,525 KB
VENDORSIGNERQ_DATA.safe	8/30/2018 2:58 PM	SAFE File	1 KB
VENDORPRODUCTQ_DATA.safe	8/29/2018 12:20 PM	SAFE File	1 KB
PPROCESS_DATA.unsafe	8/28/2018 6:08 PM	UNSAFE File	1 KB
PPROCESS_DATA.safe	8/30/2018 7:09 PM	SAFE File	0 KB
PNCMHASHQ_DATA.bin	8/30/2018 2:59 PM	BIN File	1 KB
PHASHQ_DATA.bin	8/30/2018 7:07 PM	BIN File	1 KB
IPQ_DATA.bin	8/30/2018 2:25 PM	BIN File	5 KB
HASHQ_DATA.bin	8/30/2018 7:08 PM	BIN File	7 KB
FOLDERQ_DATA.unsafe	8/29/2018 12:24 PM	UNSAFE File	1 KB
FOLDERQ_DATA.safe	8/29/2018 12:23 PM	SAFE File	1 KB

Figure 11

Using the **etaDataDispatcher.exe**, files can be sent to the respective remote agents/sensors.

NOTE:

1. In Learning period, Agent/Sensor collects the system activity hashes and stores the hash details in **PNCMHASHQ_DATA.bin** file under **EventTracker\Agent\Cache**. In this duration no events are generated.
2. Once the learning period is crossed, any new activity that occurs from the Agent/Sensor end will store the hash details in **PNCMHASHQ_DATA.bin** file under **EventTracker\Agent\Cache** and will add/update the hashes to **BLK_HLST.blk** under **EventTracker\Agent**. In this duration, Event ID 3519 is generated.
3. Based on the user's safelists such as **FOLDERQ_DATA.safe** (Folder name/path), **VENDOR safe lists** (Signer/Product Name), **WHT_HLST.safe** (safe hashes), **PPROCESS_DATA.safe** (parent name/path), **PPROCESS_DATA.unsafe** (parent name/path) and **FOLDERQ_DATA.unsafe** (Folder name/path), it monitors suspicious processes and terminates.
4. If user(s) finds the terminated activity not suspicious, they can remove it from the blacklist file and add it to the Whitelist.
5. If users have enabled the **Allow Trusted Vendor** option, and if the Vendor safe list in the cache path is not created, then event id 3525 is generated, whenever the agent restarts.
6. If the user enables the **Monitor Suspicious process** and considers terminating, and there is no white list file, then if any process gets launched, event id 3524 is generated and whenever the agent gets restarted, event id 3525 is generated.