Netsurion®
Powering Secure and Agile Networks

Integration Guide

Integrating Tanium with EventTracker

EventTracker v9.x and above

Publication Date:

July 9, 2021

Abstract

This guide provides instructions to configure/ retrieve Tanium logs via syslog. After EventTracker is configured to collect and parse these logs, dashboard and reports can be configured to monitor Tanium management and security logs.

Scope

The configuration details in this guide are consistent with EventTracker version 9.x or above and Tanium Endpoint Security or Endpoint Management.

Audience

Administrators who are assigned the task to monitor Tanium events using EventTracker.

Table of Contents

1. Overview

Tanium is a feature-packed endpoint management and endpoint security platform designed to strengthen and optimize an organization's cybersecurity efforts. The platform allows security and IT operations team to get access to visibility and accurate information on the state of endpoints at all times to protect against modern-day disruptions and realize new levels of business resilience.

EventTracker helps to monitor events from Tanium via syslog. EventTracker reports, saved searches and dashboards will help you to analyze the activity logs, such as vulnerability management, login failed by any user, administrative activities, etc. This contains critical information, such as time of occurrence of events, user source IP, and action taken by user. Dashboards are graphical representation of events, which allows administrators to take an overview of key information found, such as total number, or percentage of audit events or operational events.

2. Prerequisites

- Admin access to Tanium platform.
- Enable subscription for Tanium Connect.
- EventTracker server IP address. (If Tanium is cloud, the public IP is required.)
- EventTracker server port. E.g. 514 or 6514.
- Enable TLS on EventTracker Manager in case of syslog "TCP" connection.

3. Configuring Tanium

Syslog configuration for both On-Prem solution and cloud (TaaS) solution is identical.

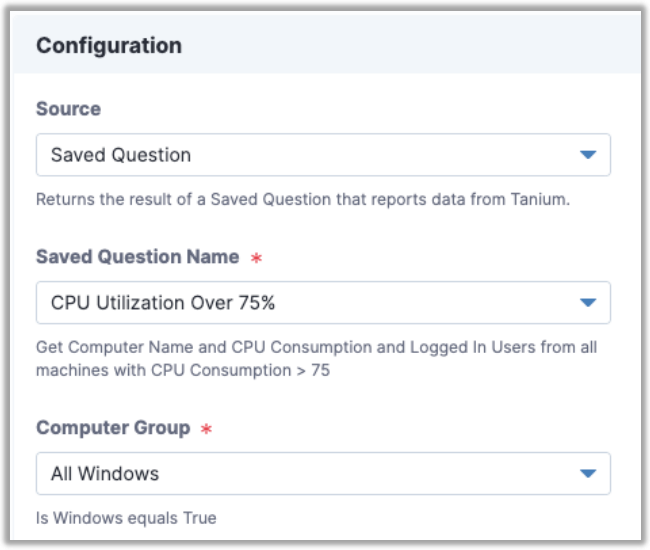
The steps provided below will help to configure Tanium via syslog to help forward logs to EventTracker servers.

1. Login to Tanium platform.
2. On the **Connect Overview** page, scroll to the **Connections** section and click **Create Connection**.
3. Enter a name and description for the connection.

3.1 Configuring the connection source.

The connection source determines what data you are sending to the destination. This data is usually the information from Tanium, such as a saved question, question log, client status, or event. The settings vary depending on which source you choose.

There are multiple connection sources that can be considered for e.g., action history, client status, event, Tanium audit source, Tanium threat response, etc.



3.2 Configuring the SIEM Destination.

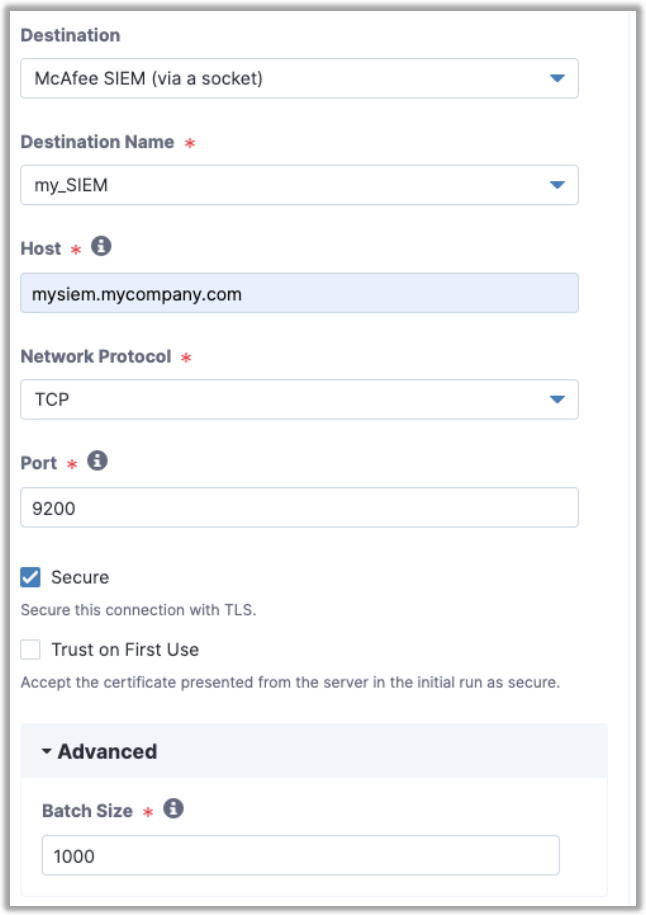
Specific details about the server to which you want to send the SIEM data.

1. For the **Destination**, select the type of SIEM that you are configuring.
2. Specify a name for the destination:
    - You can specify a unique name to save the configuration information as a new destination or select an existing SIEM destination from the list.
    - If you edit the settings for an existing destination, all connections that use that destination are affected.
    - To clone an existing destination, select the existing destination and change the name.
3. Specify how to connect with the server (TCP/UDP), and where you want the data to go, such as the SIEM host and port.
   Fill-in the below required fields:
    - **Host** – EventTracker server IP address/ hostname
    - **Network Protocol** – UDP/TCP. (Select UDP in case of On-prem)
    - **Port** – e.g., 514 or 6514. (Select 514 in case of UDP)

Note – Optionally, a self-signed certificate can be created to use in case of TCP as network protocol. You can also select **Trust** on **First Use** to accept the certificate presented from the server and trust only that certificate for future connection runs.

3.3 Saving and verifying the connection

After you enter the details for the connection, click **Save**. (To save the connection and immediately run the connection, click **Run and Save**.)



4. System Licensing

For On-Prem solution, a single system will get created by the format of <HostName~syslog> or <ComputerName~syslog>.

For Cloud-based solution, multiple system with format <IPAddress~syslog> may get created. If logs are coming in from multiple IP addresses for the same customer, the system name extraction can be done from the logs .

5. EventTracker Knowledge Pack

After the logs are received by EventTracker manager, Knowledge Packs can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker to support Tanium.

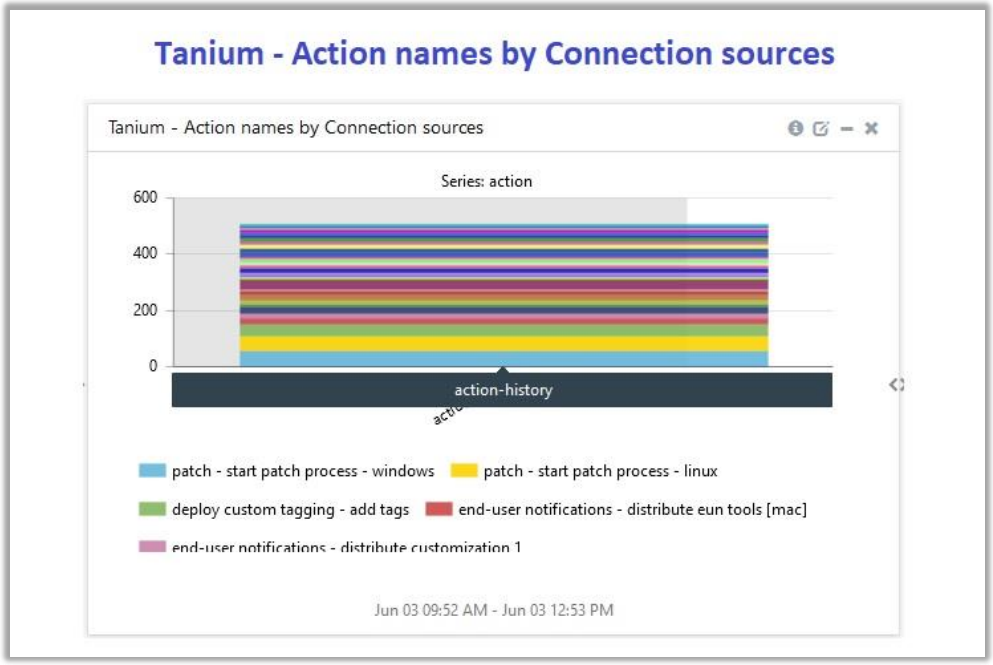
5.1 Reports

- **Tanium - Action History report** – Action history reports consists of record of all actions issued by console operators. This includes actions such as, flush DNS cache, action lock, deploy direct connect - open session – Windows, discover - execute scan for non-Windows [distributed Nmap], etc.

LogTime	Action Name	ActionID	Command	Comment	Connection Source	Status	StartTime	Insert Time	Approver	Issuer	Package Name	SourceID	Expiration	Distribute Over
06/03/2021 11:47:27 AM	Patch - Start Patch Process - Linux	85519	/bin/sh ./start-patch-process.sh	Ensures that the Tanium Patch process is running on targeted Linux endpoints	Action-History	Closed	2021-04-16T04:32:04	2021-04-16T04:32:12	taniumconsole	taniumconsole	Patch - Start Patch Process - Linux	12646	2021-04-16T04:47:04	0 minutes
06/03/2021 11:47:27 AM	Deploy Custom Tagging - Add Tags	85685	cmd.exe /c cscript.exe //E:VBScript //T:60 add-tags.vbs		Action-History	Closed	2021-04-16T09:26:23	2021-04-16T09:26:30	pumba@contoso.com	pumba@contoso.com	Custom Tagging - Add Tags	5525	2021-04-16T09:37:23	0 minutes
06/03/2021 11:47:27 AM	Comply action-500-575-xxxxxxxx	85599	cmd /c cscript invoke-report.vbs xxxxxxxx compliance joval low 0	CIS Microsoft Windows Server 2016 RTM (Release 1607) Benchmark: Level 1 - Member Server	Action-History	Closed	2021-04-16T07:12:05	2021-04-16T07:12:05	taniumconsole	taniumconsole	Comply - Run Compliance Report - Windows - xxxxxxxx	79	2021-04-16T08:05:05	3 minutes

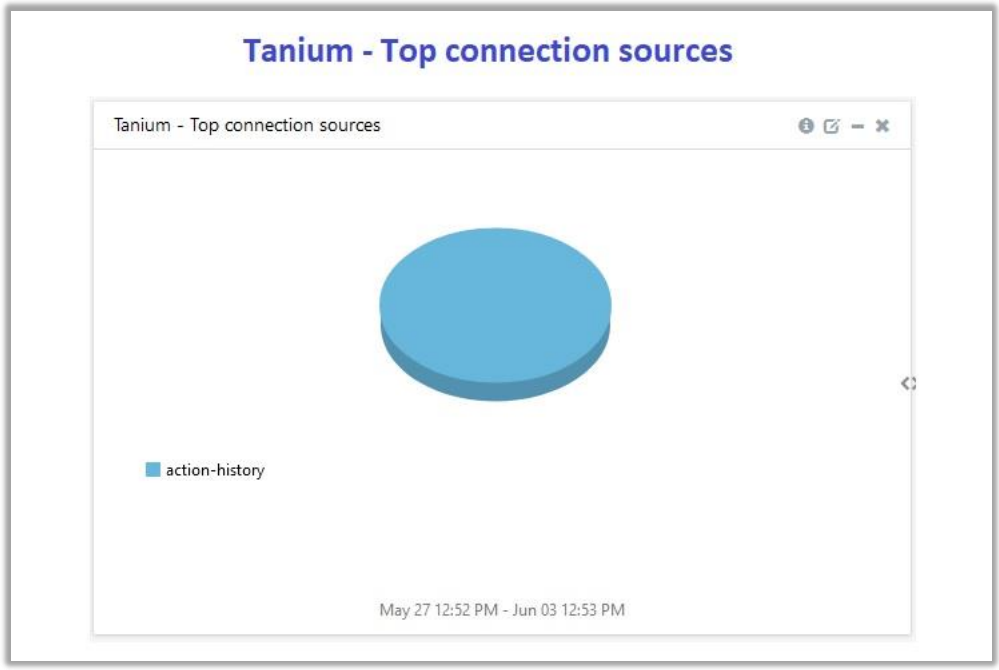
5.2 Dashboards

- **Tanium - Action names by Connection sources.**



- **Tanium - Top command executions.**

- **Tanium - Top connection sources.**

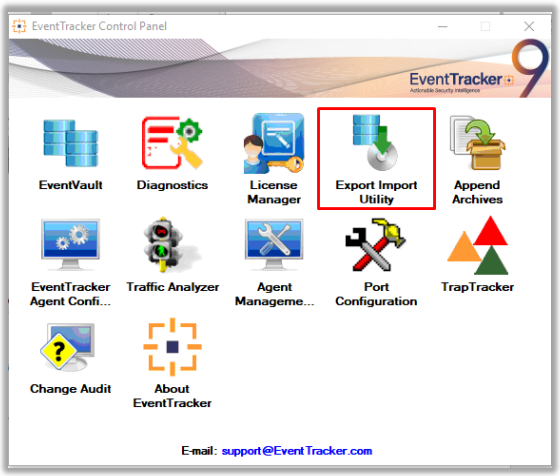


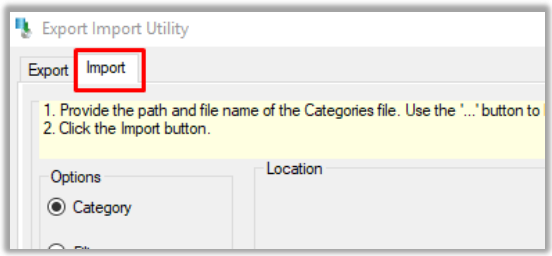
6. Importing Tanium Knowledge Pack into EventTracker

NOTE: Import knowledge pack items in the following sequence:

- Categories
- Token Template
- Knowledge Objects
- Flex Reports
- Dashboard

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

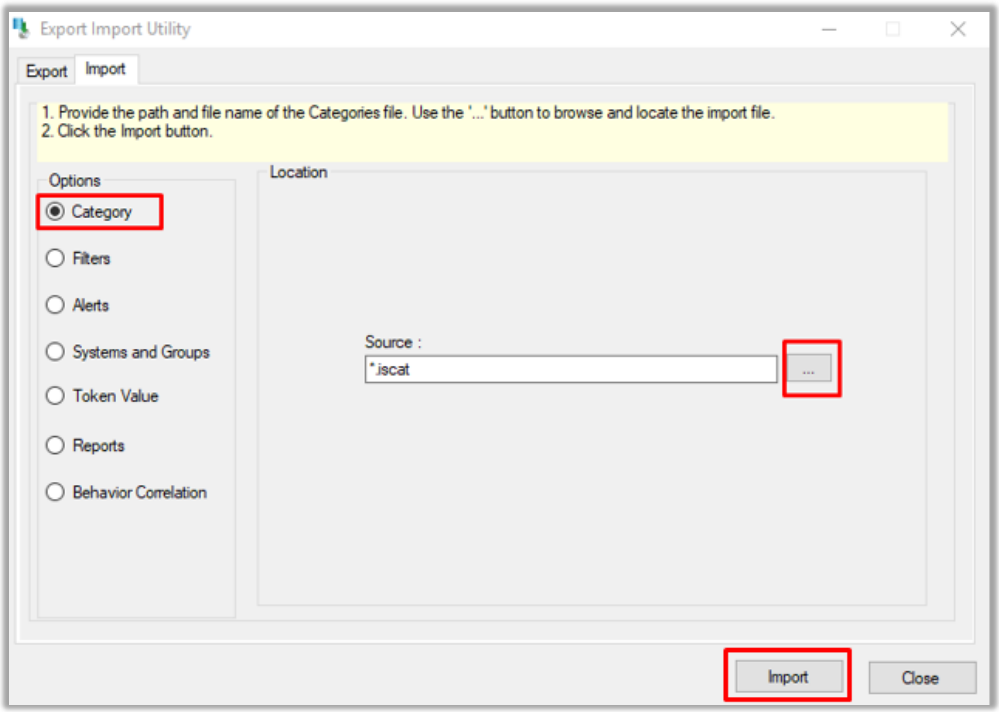




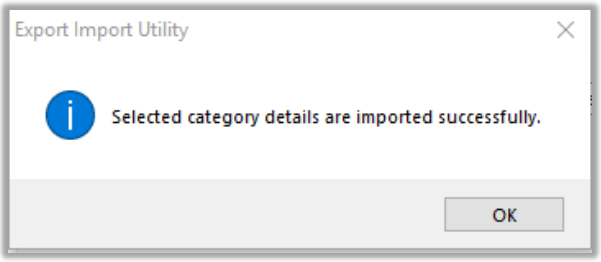
3. Click the **Import** tab.

6.1 Categories

1. After you have opened **Export Import Utility** via **EventTracker Control Panel**, click the **Category** option, and then click the browse ... .
2. Navigate to the knowledge pack folder and select the file with extension **".iscat", e.g. "Categories_Tanium.iscat"** and then click on the **Import** button.



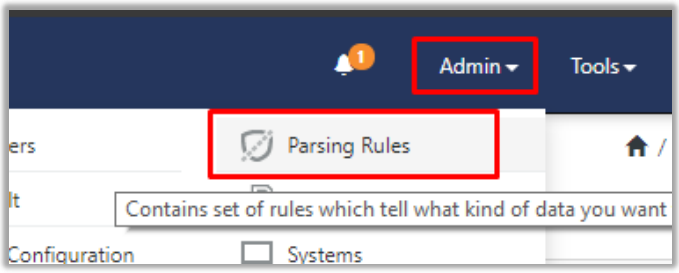
EventTracker displays a success message:



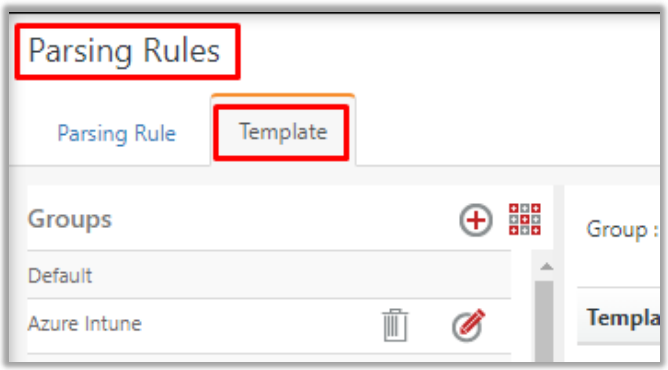
6.2 Token Template

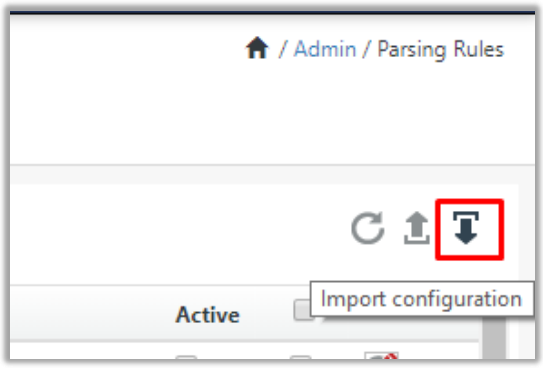
For importing **Token Template**, navigate to **EventTracker manager** web interface.

1. Click **Parsing Rules** under the **Admin** option in the EventTracker manager web interface:

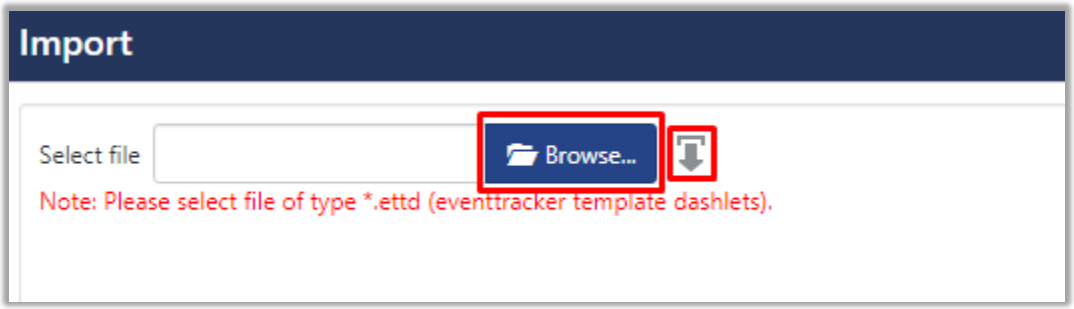


2. Click the **Template** tab and then click the **Import Configuration** button.



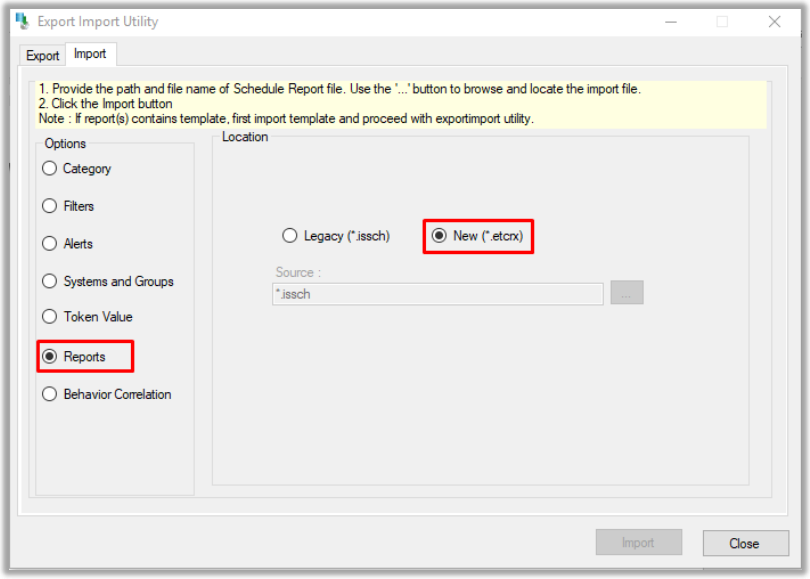


3. Click **Browse** and navigate to the knowledge packs folder (type **%et_install_path%\Knowledge Packs** in navigation bar) where "**.ettd", e.g. "Token Templates_Tanium.ettd** file is located. Wait for few seconds, as templates will be loaded. After you see the templates, click desired template, and click **Import** button:

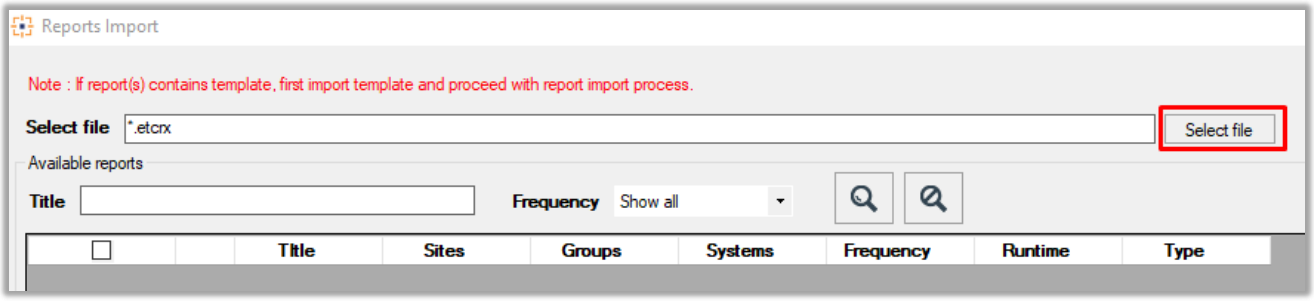


6.3 Reports

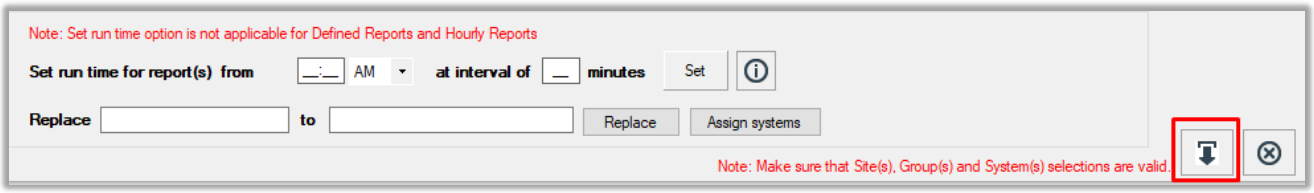
1. In EventTracker Control Panel, select **Export/ Import utility** and select the **Import tab**. Then, click **Reports** option, and Choose **New (*.etcrx)**:



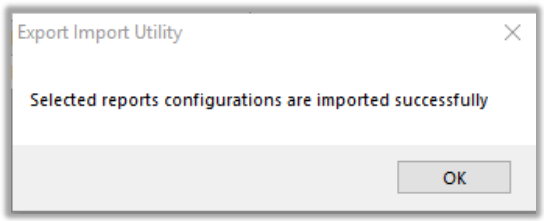
2. After you have selected **New (*.etcrx)**, a new pop-up window will appear. Click on the **Select File** button and navigate to the file path with a file having the extension "**.etcrx", e.g., Reports_ Tanium.etcrx.**



3. Wait while reports are being populated in below tables. Select all the relevant reports and then click **Import** button:

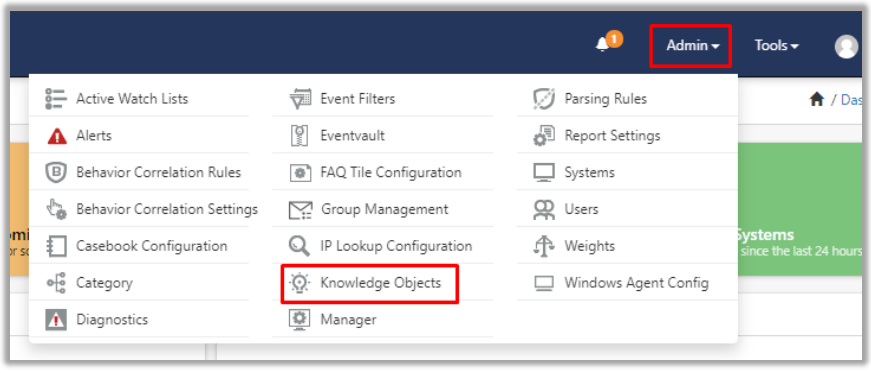


4. EventTracker displays a success message:

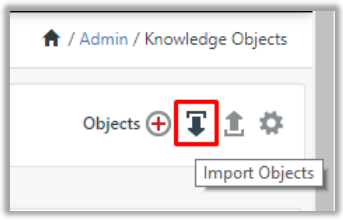


6.4 Knowledge Object

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



2. Click on the **import object** icon:

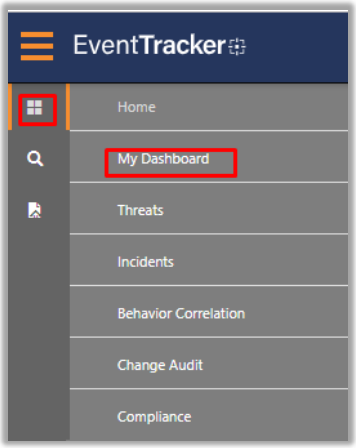


3. A pop-up box appears, click Browse in that and navigate to knowledge packs folder (type **%et_install_path%\Knowledge Packs** in navigation bar) with the extension **".etko", e.g., KO_Tanium.etko** and then click **Upload**.

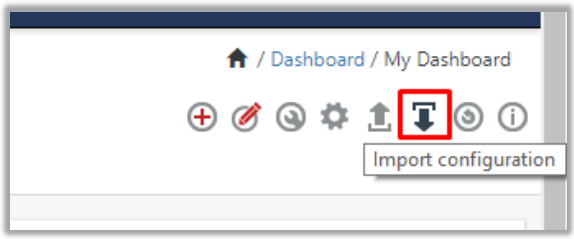
4. List of available knowledge object appears. Select the relevant files and click **Import.**

6.5 Dashboard

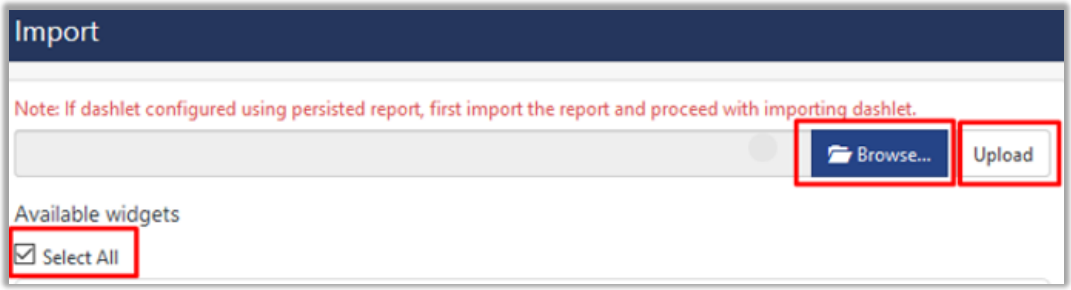
1. Login to **EventTracker**.
2. Navigate to **Dashboard** → **My Dashboard**.



3. In **My Dashboard**, Click on **Import Button**.



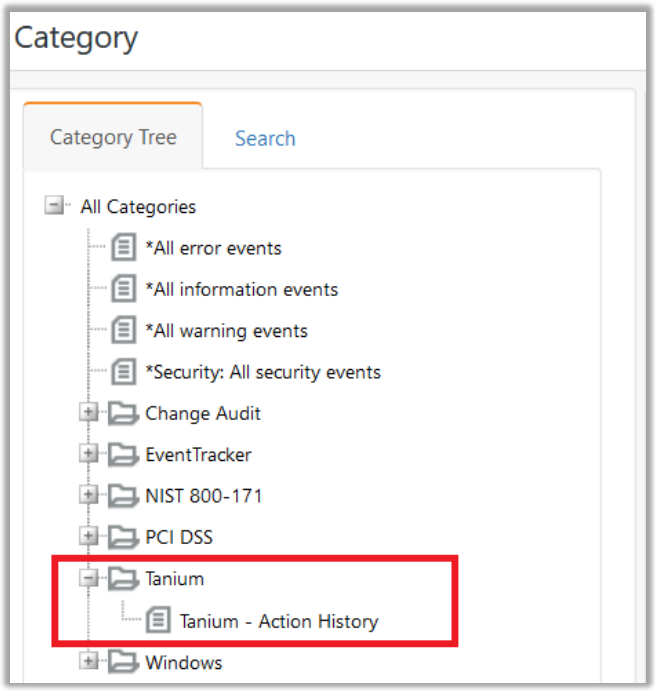
4. Select **Browse** and navigate to knowledge pack folder (type **%et_install_path%\Knowledge Packs** in navigation bar) where **.etwd**, **e.g. Dashboards_Tanium.etwd** is saved and click **Upload**.
5. Wait while EventTracker populates all the available dashboards. Choose **Select All** and click **Import.**



7. Verifying Tanium Knowledge Pack in EventTracker

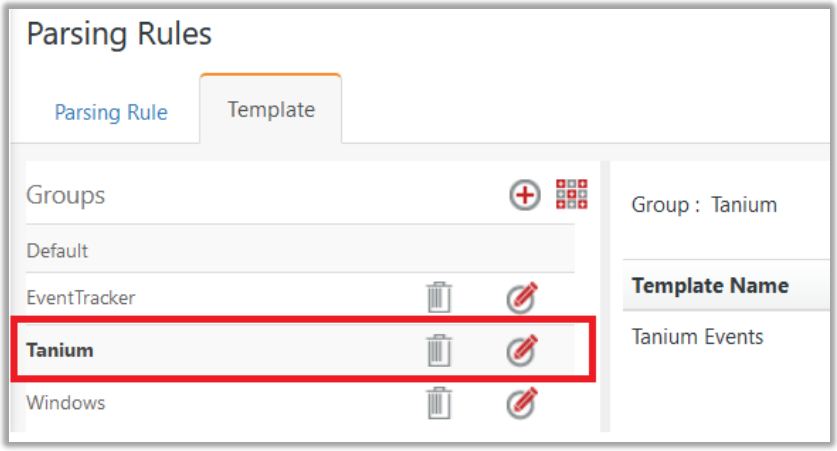
7.1 Categories

1. Login to **EventTracker**.
2. Click **Admin** dropdown, and then click **Categories**.
3. In **Category Tree** to view imported categories, scroll down and expand **Tanium** group folder to view the imported categories.



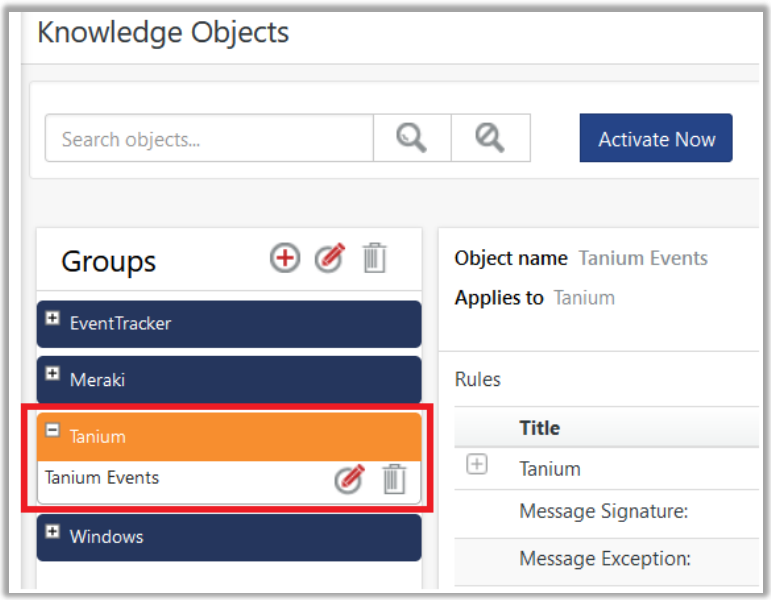
7.2 Token Value

1. In the **EventTracker** web interface, click the **Admin** dropdown, and then click **Template.**
2. In the **Template** tab, click on the **Tanium** group folder to view the imported Token Values.



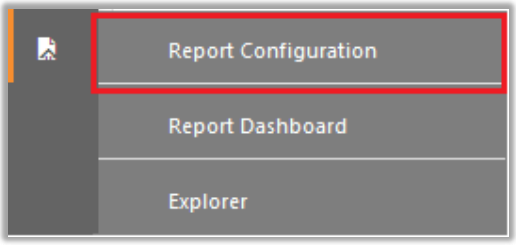
7.3 Knowledge Objects

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

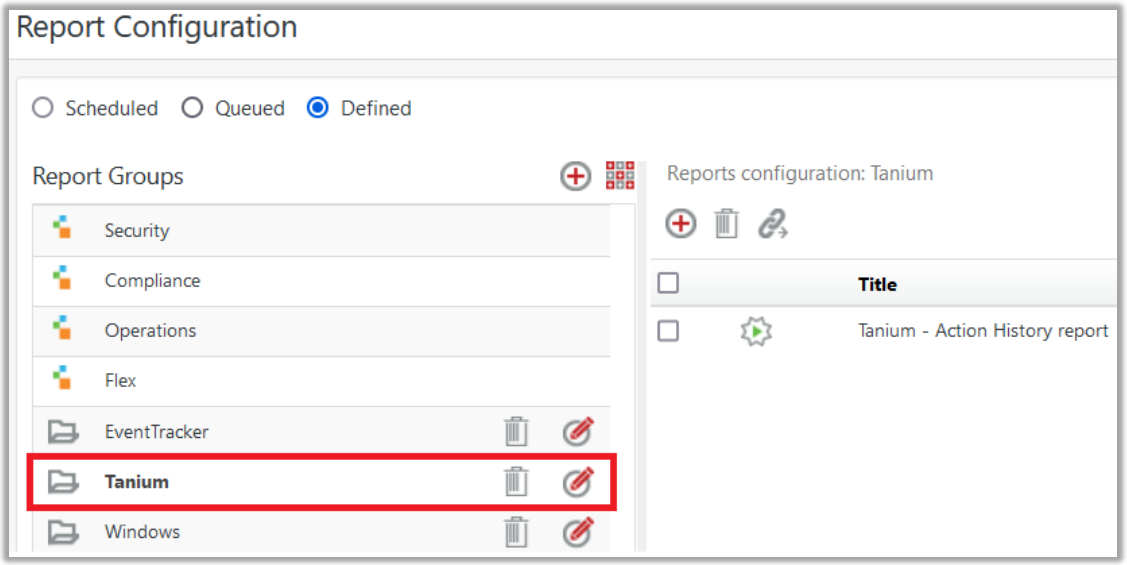


7.4 Reports

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

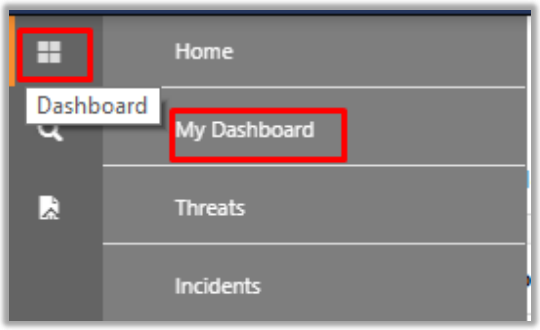


2. In **Reports Configuration** pane, select the **Defined** option.
3. Click on the **Tanium** group folder to view the imported reports.

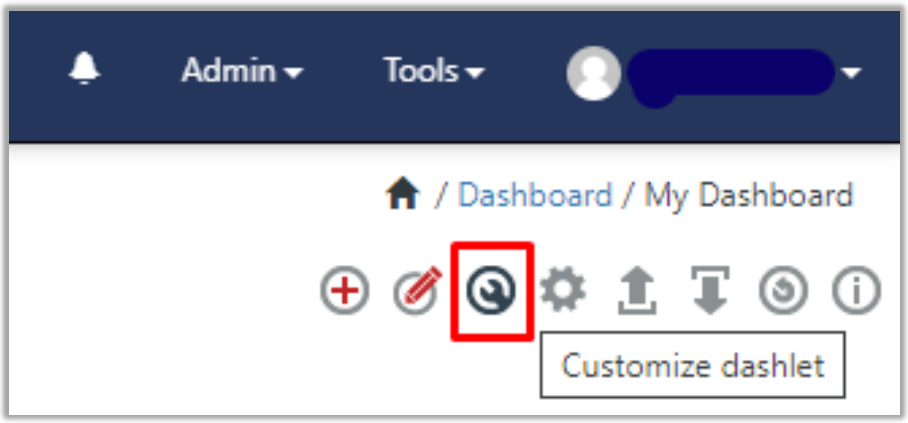


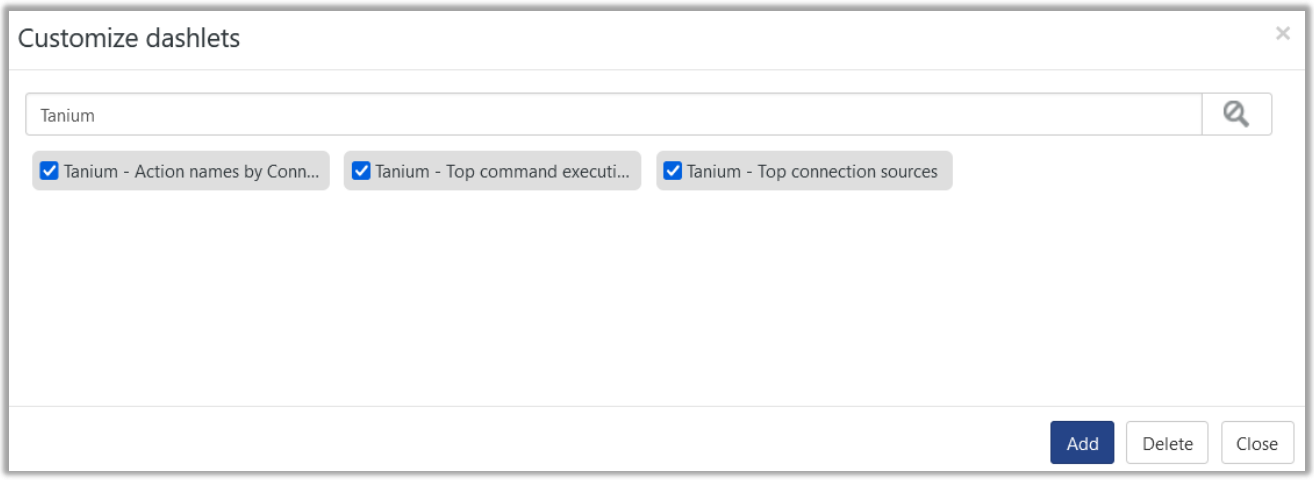
7.5 Dashboard

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



2. Select **Customize daslets** button and type **Tanium** in the search bar.





About Netsurion

Flexibility and security within the IT environment are two of the most important factors driving business today. Netsurion's cybersecurity platforms enable companies to deliver on both. Netsurion's approach of combining purpose-built technology and an ISO-certified security operations center gives customers the ultimate flexibility to adapt and grow, all while maintaining a secure environment.

Netsurion's EventTracker cyber threat protection platform provides SIEM, endpoint protection, vulnerability scanning, intrusion detection and more; all delivered as a managed or co-managed service.

Netsurion's BranchSDO delivers purpose-built technology with optional levels of managed services to multi-location businesses that optimize network security, agility, resilience, and compliance for branch locations. Whether you need technology with a guiding hand or a complete outsourcing solution, Netsurion has the model to help drive your business forward. To learn more visit netsurion.com or follow us on Twitter or LinkedIn. Netsurion is #19 among MSSP Alert's 2020 Top 250 MSSPs.

Contact Us

Corporate Headquarters

Netsurion
Trade Centre South
100 W. Cypress Creek Rd
Suite 530
Fort Lauderdale, FL 33309

Contact Numbers

EventTracker Enterprise SOC: 877-333-1433 (Option 2)

EventTracker Enterprise for MSP's SOC: 877-333-1433 (Option 3)

EventTracker Essentials SOC: 877-333-1433 (Option 4)

EventTracker Software Support: 877-333-1433 (Option 5)

https://www.netsurion.com/eventtracker-support