Netsurion®
Powering Secure and Agile Networks

Integration Guide

Integrating QualysGuard with EventTracker

Publication Date:

March 30, 2021

Abstract

This guide provides instructions to retrieve the information from QualysGuard. Once the information starts coming-in into EventTracker, reports, dashboards, alerts, and saved searches can be configured.

Audience

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

Table of Contents

1. Overview 4
2. Prerequisites 4
3. Integrating QualysGuard with EventTracker 4
   3.1 Getting the API URL from Cloud UI 4
   3.2 Configure QualysGuard to forward logs to EventTracker 5
4. EventTracker Knowledge Packs 6
   4.1 Report 6
5. Importing knowledge pack into EventTracker 9
   5.1 Getting Knowledge Packs 9
   5.2 Saved Searches 9
   5.3 Token Template 11
   5.4 Knowledge Objects 12
   5.5 Dashboards 13
6. Verifying knowledge pack in EventTracker 14
   6.1 Saved Searches 14
   6.2 Token Template 14
   6.3 Knowledge Objects 15
   6.4 Dashboards 15

About Netsurion 16

Contact Us 16

1. Overview

QualysGuard is the Qualys Cloud Platform. It integrates four key elements cloud agents, virtual scanners, and network analysis (passive scanning) capabilities into a single application.

It enables organizations to automatically discover every asset in their environment which includes unmanaged assets, inventory of all hardware and software, classify and tag critical assets. It continuously assesses assets for the latest vulnerabilities and prioritizes actively exploitable vulnerabilities.

On the bases of the inputs received, EventTracker provides various dashboard related to vulnerabilities and CVEs. Also, scan activity reports done in QualysGuard can be generated.

2. Prerequisites

- EventTracker v9.2 and above should be installed.
- Administrative/root access to QualysGuard Cloud UI.
- PowerShell v5 and later should be installed.

3. Integrating QualysGuard with EventTracker

3.1 Getting the API URL from Cloud UI

1. Click **Help → About**.

2. From the list of API's base URL (choose the one with API term present.)

General Information

Qualys Web Service

Application Version:	10.8.0.0-7
Online Help Version:	10.8.25-1
SCAP Module Version:	1.2

Qualys External Scanners

Security Operations Center (SOC):	103.75.173.0/24 2001:0df1:f600:4400::/64
Scanner Version:	12.3.51-1
Vulnerability Signature Version:	2.5.144-3
Scanner Services	1.1.4-11

Qualys Scanner Appliances

Security Operations Center (SOC):	- qualysguard.qg1.apps.qualys.in:443 - distribution.qg1.apps.qualys.in:443 - monitoring.qg1.apps.qualys.in:443 - orchestrator.qg1.apps.qualys.in:443 - qgadmin.qg1.apps.qualys.in:443 - scanservice1.qg1.apps.qualys.in:443 - qualysapi.qg1.apps.qualys.in:443

Qualys Cloud Agents

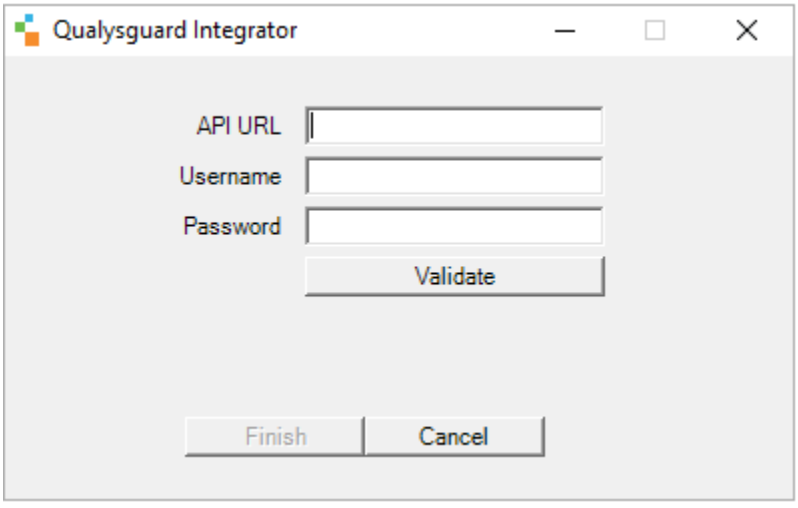
Cloud Agents Public URL:	https://qagpublic.qg1.apps.qualys.in

3. Note the API for future use.

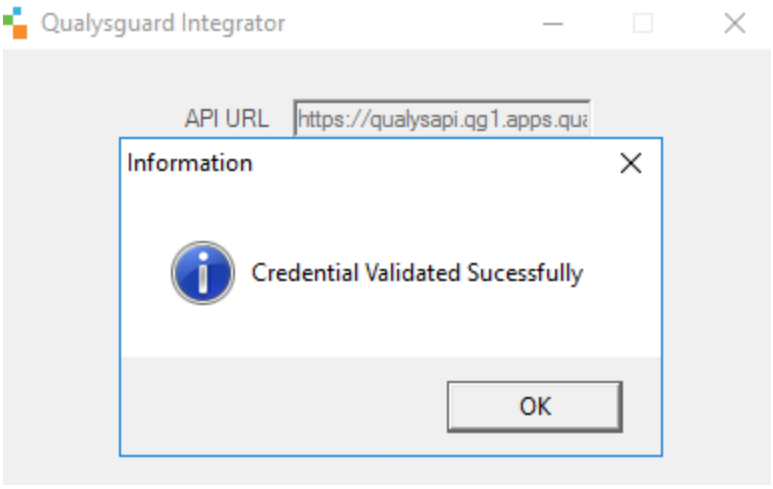
3.2 Configuring QualysGuard to forward logs to EventTracker

Note : Contact EventTracker support to get the **QualysGuardIntegrator.exe.**

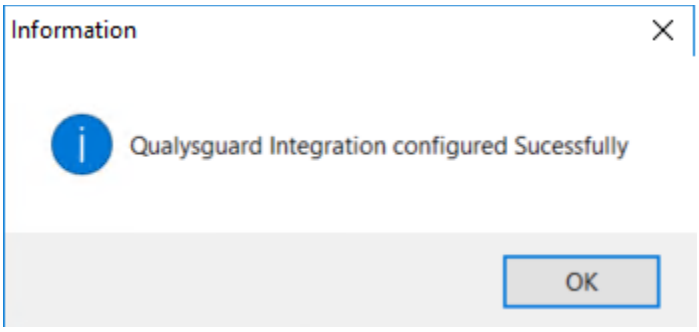
1. Run **QualysguardIntegrator.exe** as administrator in EventTracker agent machine.
2. Enter the correct username and password (Use administrative credentials).
3. Enter the noted API URL in from above.



4. Click **Validate**.



5. Once successfully verified, click on the **Finish** button to complete the integration process.
6. The following message display once successfully configured.



4. EventTracker Knowledge Packs

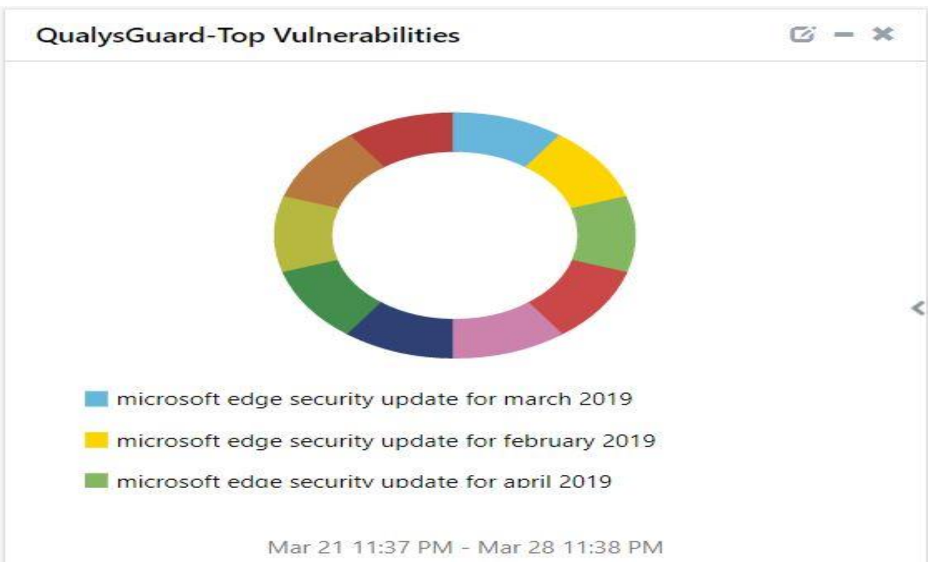
4.1 Report

- **QualysGuard: Scan Activities**: This report will provide details about the vulnerabilities which QualysGuard detects in your environment. This report will contain information about the host, which is scanned, its vulnerability details like CVE Id and vulnerability names.

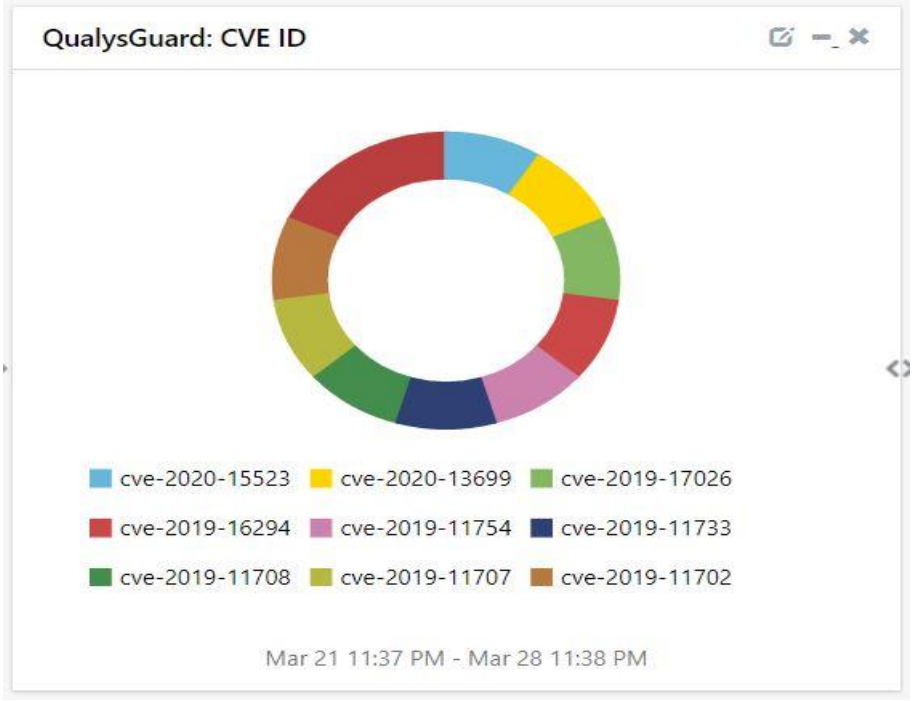
Operating System	Vulnerability In	Severity	Times Found	Type
Windows Server 2016 Datacenter 64 bit Edition Version 1607	HKLM\SOFTWARE\Wow6432Node\Microsoft\Office\14.0\Common\ProductVersion LastProduct = 14.0.7015.1000	4	66	Confirmed
Windows Server 2016 Datacenter 64 bit Edition Version 1607	HKLM\Software\Microsoft\Internet Explorer Version = 9.11.14393.0	5	66	Confirmed
Windows Server 2016 Datacenter 64 bit Edition Version 1607	HKLM\SOFTWARE\Wow6432Node\Microsoft\Office\14.0\Common\ProductVersion LastProduct = 14.0.7015.1000	4	66	Confirmed
Windows Server 2016 Datacenter 64 bit Edition Version 1607	HKLM\SOFTWARE\Wow6432Node\Microsoft\Office\14.0\Common\ProductVersion LastProduct = 14.0.7015.1000	3	66	Confirmed
Windows Server 2016 Datacenter 64 bit Edition Version 1607	HKLM\SOFTWARE\Wow6432Node\Microsoft\Office\14.0\Common\ProductVersion LastProduct = 14.0.7015.1000	4	66	Confirmed
Windows Server 2016 Datacenter 64 bit Edition Version 1607	HKLM\SOFTWARE\Wow6432Node\Microsoft\Office\14.0\Common\ProductVersion LastProduct = 14.0.7015.1000	4	66	Confirmed
Windows Server 2016 Datacenter 64 bit Edition Version 1607	HKLM\SOFTWARE\Wow6432Node\Microsoft\Office\14.0\Common\ProductVersion LastProduct = 14.0.7015.1000	4	66	Confirmed
Windows Server 2016 Datacenter 64 bit Edition Version 1607	HKLM\SOFTWARE\Wow6432Node\Microsoft\Office\14.0\Common\ProductVersion LastProduct = 14.0.7015.1000	5	66	Confirmed

Dashboards

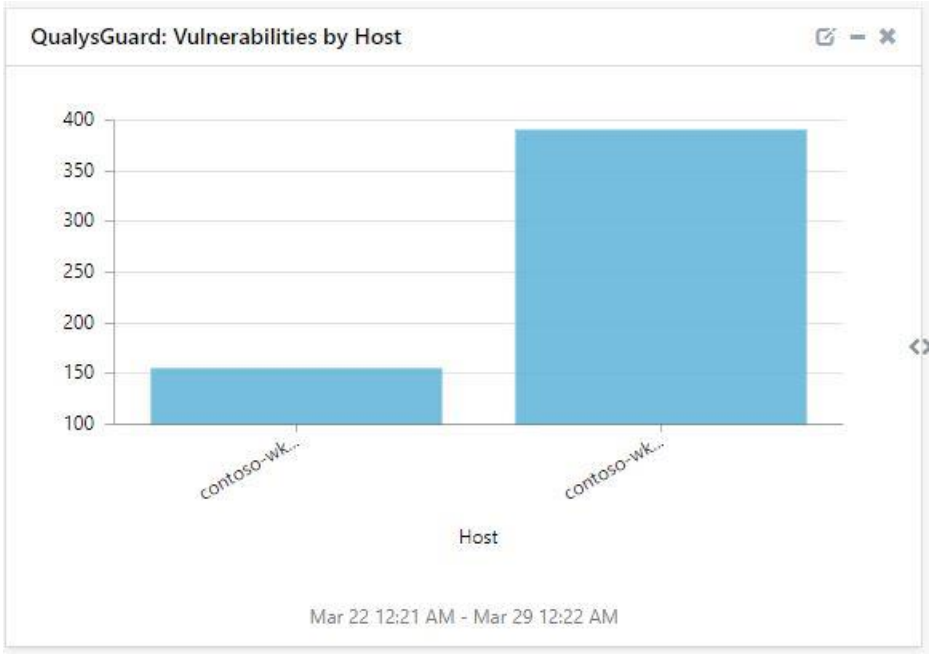
- **QualysGuard :Top Vulnerabilities**



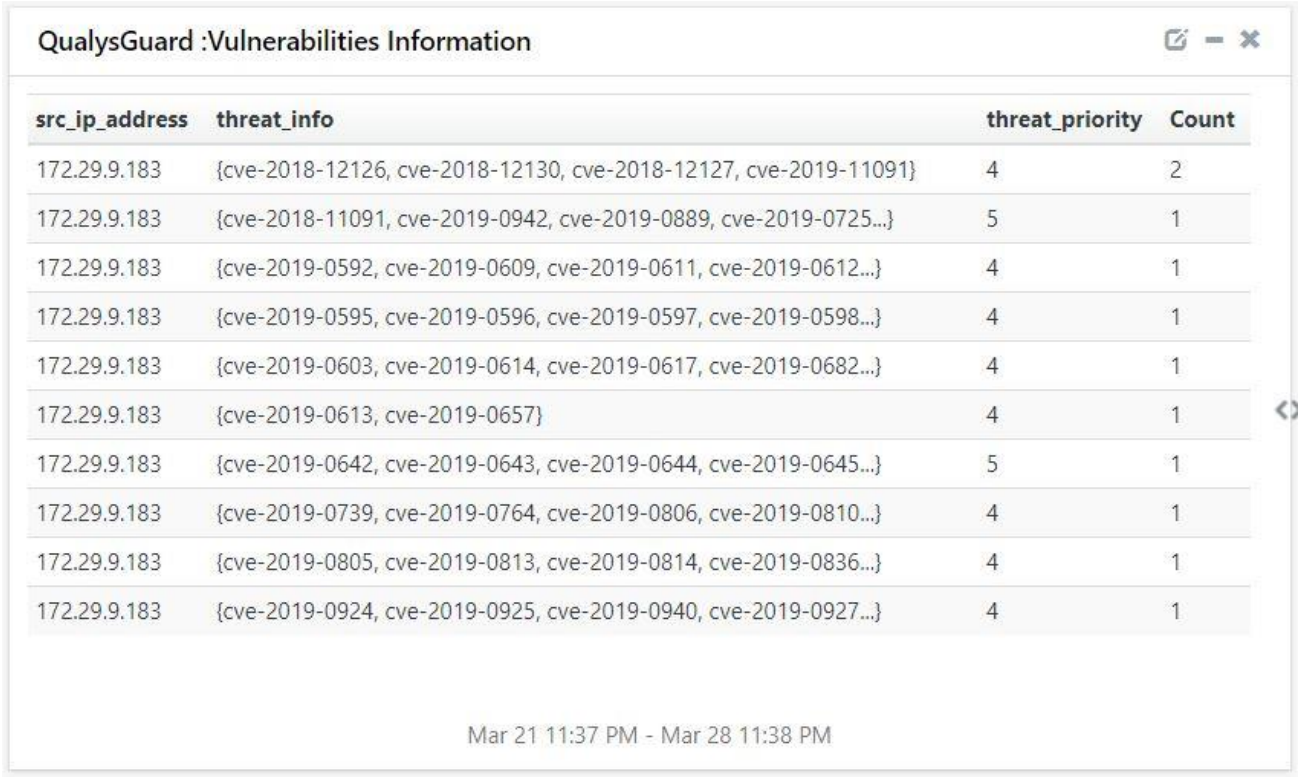
- **QualysGuard: CVE ID**



- **QualysGuard: Vulnerabilities by Host**



- **QualysGuard :Vulnerabilities Information**



QualysGuard :Vulnerabilities Information

src_ip_address	threat_info	threat_priority	Count
172.29.9.183	{cve-2018-12126, cve-2018-12130, cve-2018-12127, cve-2019-11091}	4	2
172.29.9.183	{cve-2018-11091, cve-2019-0942, cve-2019-0889, cve-2019-0725...}	5	1
172.29.9.183	{cve-2019-0592, cve-2019-0609, cve-2019-0611, cve-2019-0612...}	4	1
172.29.9.183	{cve-2019-0595, cve-2019-0596, cve-2019-0597, cve-2019-0598...}	4	1
172.29.9.183	{cve-2019-0603, cve-2019-0614, cve-2019-0617, cve-2019-0682...}	4	1
172.29.9.183	{cve-2019-0613, cve-2019-0657}	4	1
172.29.9.183	{cve-2019-0642, cve-2019-0643, cve-2019-0644, cve-2019-0645...}	5	1
172.29.9.183	{cve-2019-0739, cve-2019-0764, cve-2019-0806, cve-2019-0810...}	4	1
172.29.9.183	{cve-2019-0805, cve-2019-0813, cve-2019-0814, cve-2019-0836...}	4	1
172.29.9.183	{cve-2019-0924, cve-2019-0925, cve-2019-0940, cve-2019-0927...}	4	1

Mar 21 11:37 PM - Mar 28 11:38 PM

5. Importing knowledge pack into EventTracker

5.1 Getting Knowledge Packs

To get the knowledge packs, locate the knowledge pack folder. Follow the below steps:

1. Press "windows + R".
2. Type **%et_install_path%\Knowledge Packs** and press **Enter**.

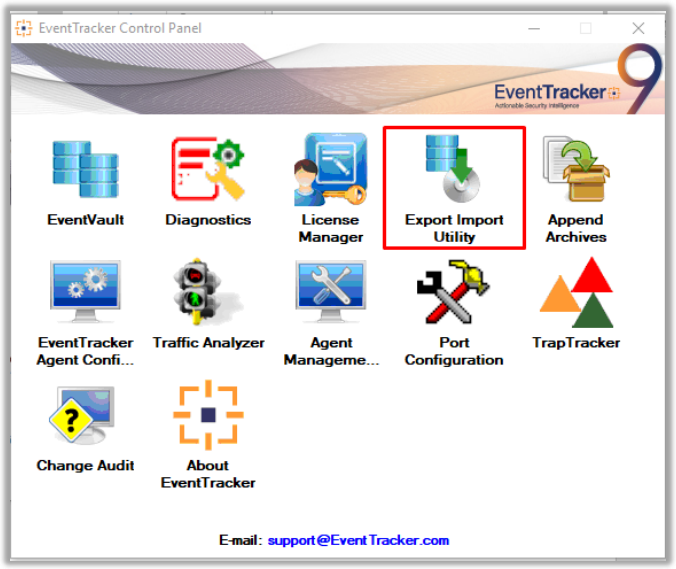
Note :– If, not able to locate the file path as mentioned above, please contact EventTracker support to get the assistance).

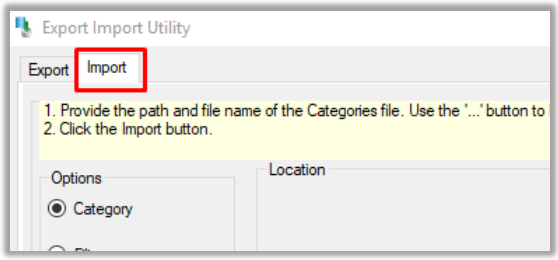
NOTE: Import knowledge pack items in the following sequence:

- Categories
- Token Template
- Knowledge Objects
- Dashboards

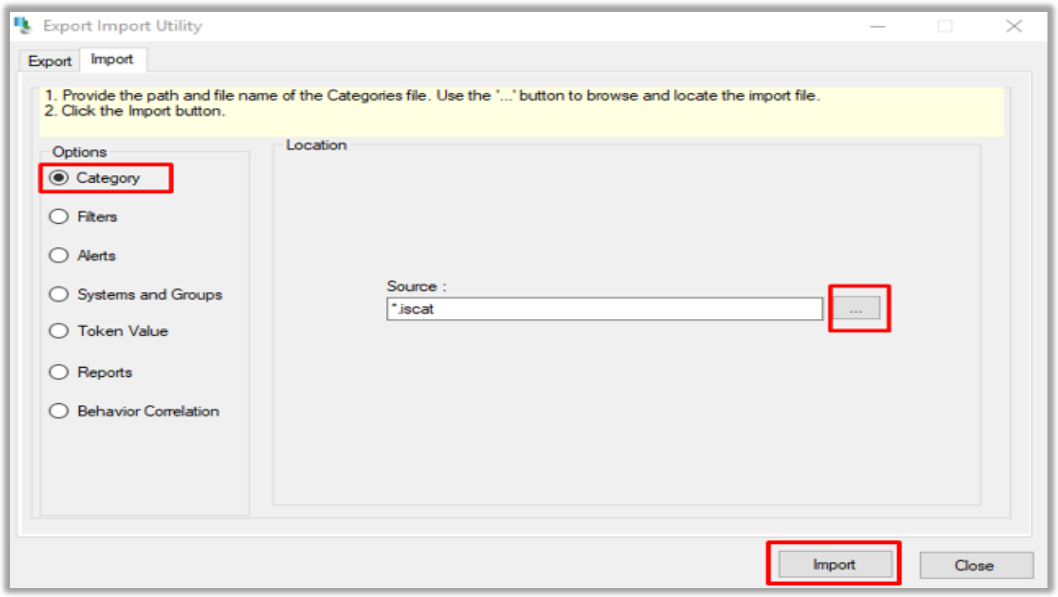
5.2 Saved Searches

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

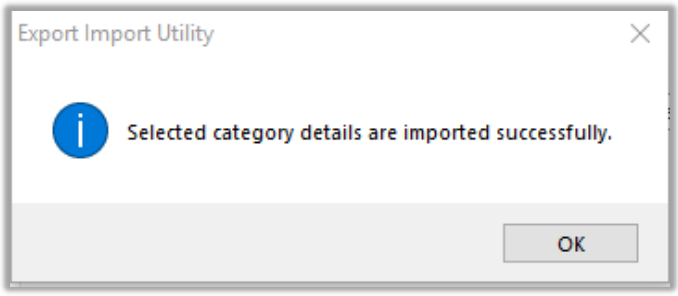




3. Click the **Import** tab.
4. Once you have opened **Export Import Utility** via **EventTracker Control Panel**, click the **Category** option, and then click the browse ... button.
5. Navigate to the knowledge pack folder and select the file with extension **".iscat", e.g., Categories_Qualysguard.iscat** and then click on the **Import** button:



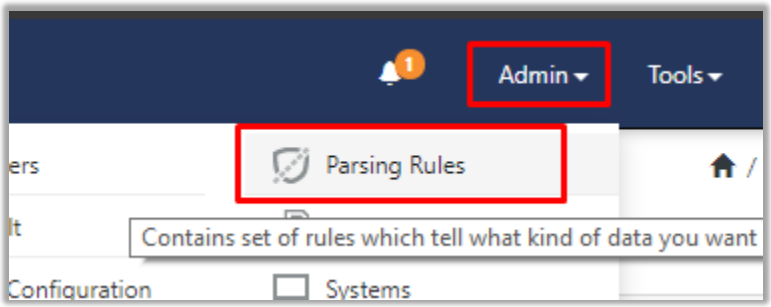
6. EventTracker displays a success message:



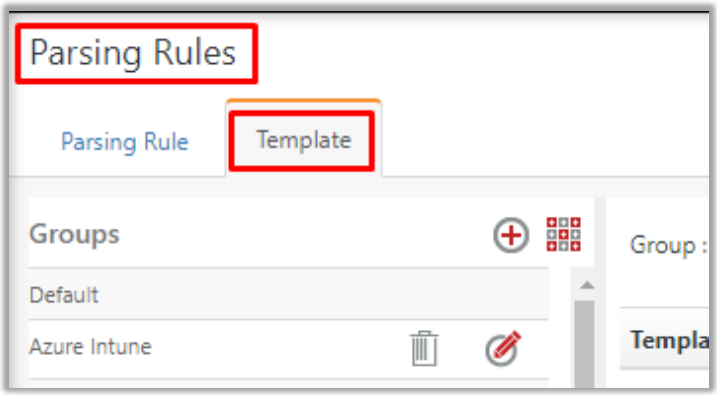
5.3 Token Template

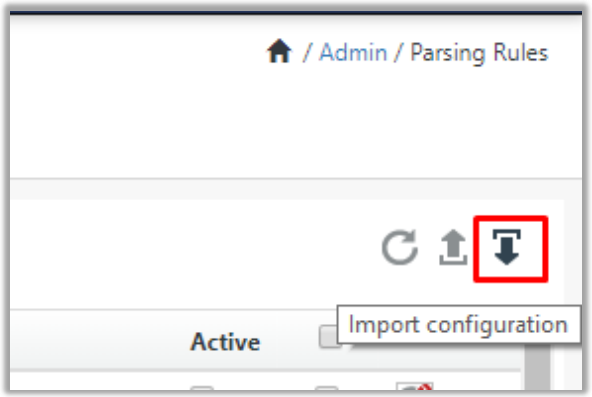
For importing **Token Template**, navigate to **EventTracker manager** web interface.

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

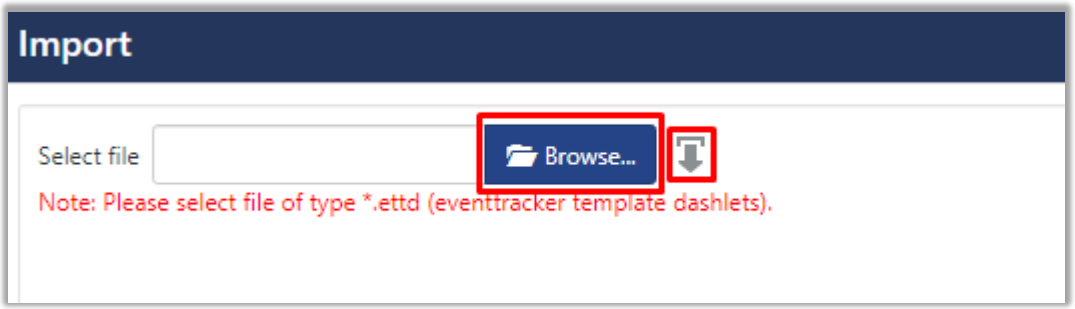


2. Click the **Template** tab and then click the **Import Configuration** button.



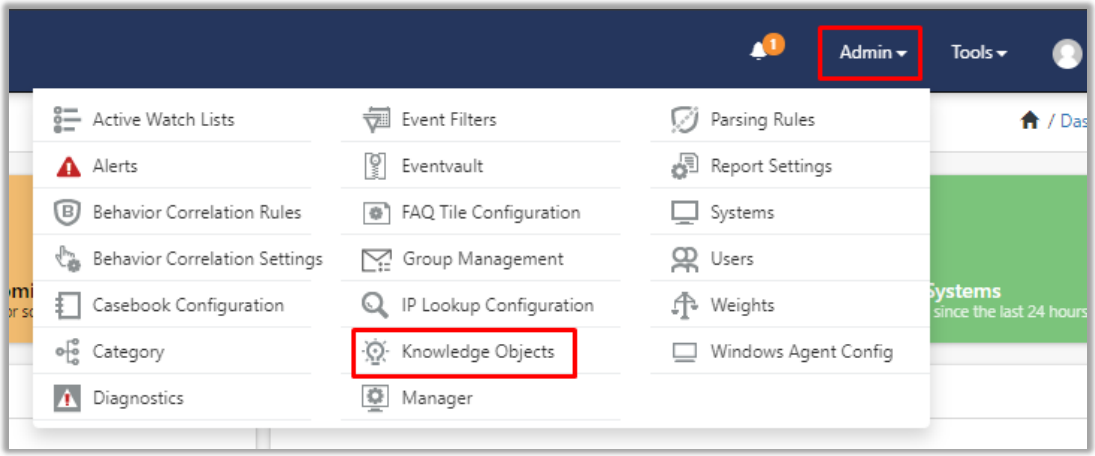


3. Click **Browse** button and navigate to the knowledge packs folder (type **%et_install_path%\Knowledge Packs** in navigation bar) where **".ettd", e.g., Templates_ Qualysguard.ettd** file is located. Wait for few seconds, as templates will be loaded. Once you see the templates, click desired template,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

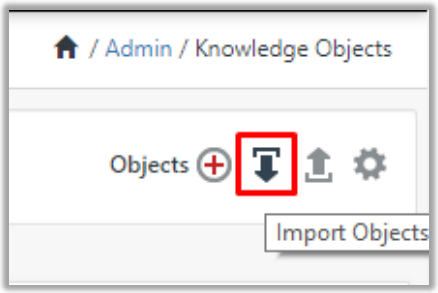


5.4 Knowledge Objects

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



2. Click the **Import object** icon:

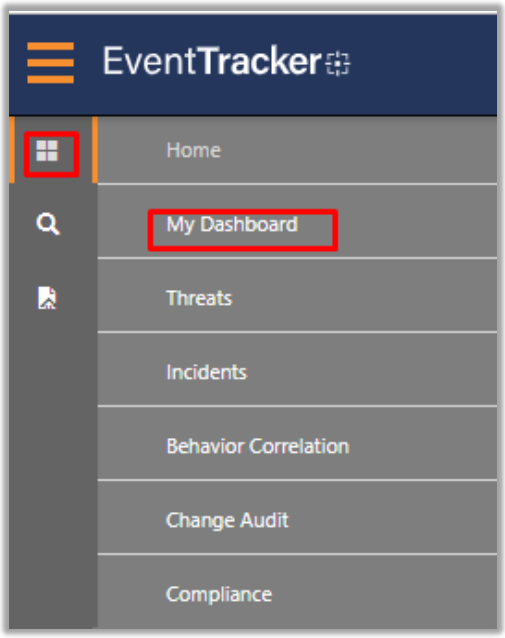


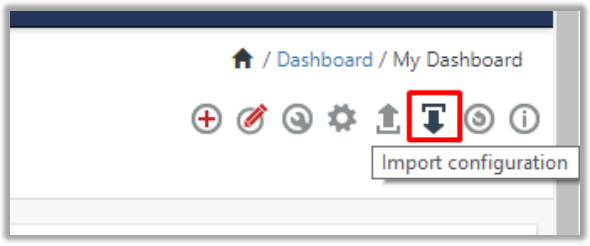
3. A pop-up box will appear, click **Browse** and navigate to knowledge packs folder (type **%et_install_path%\Knowledge Packs** in navigation bar) with the extension **".etko", e.g., KO_ Qualysguard.etko** and then click **Upload** button.

4. Wait while EventTracker populates all the relevant knowledge objects. Once the objects are displayed, select the required ones, and click on **Import** button:

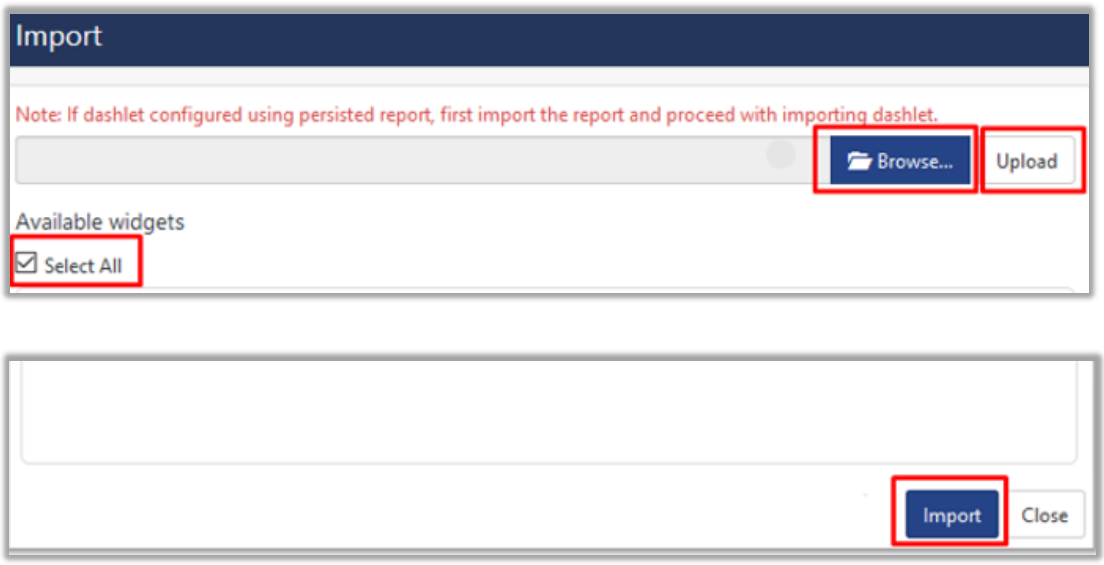
5.5 Dashboards

1. Login to **EventTracker manager web interface**.
2. Navigate to **Dashboard ->My Dashboard**.
3. In My Dashboard, Click **Import Button**:





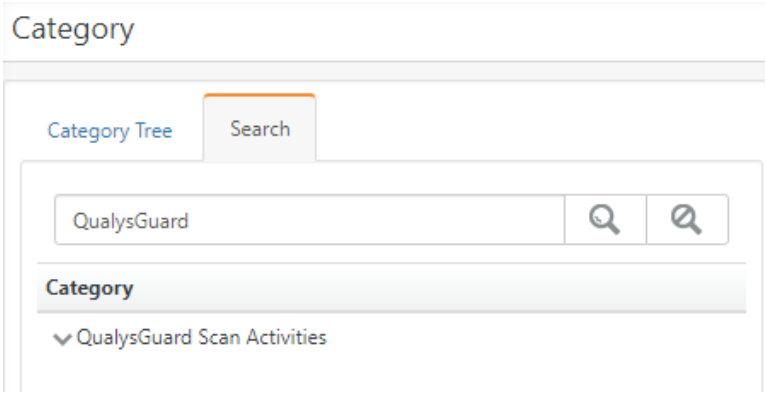
4. Select the **browse** button and navigate to knowledge pack folder (type **%et_install_path%\Knowledge Packs** in navigation bar) where "**.etwd**", **e.g., Dashboards_ Qualysguard.etwd** is saved and click on **Upload** button.
5. Wait while EventTracker populates all the available dashboards. Now, choose **Select All** and click on **Import** button.



6. Verifying knowledge pack in EventTracker

6.1 Saved Searches

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

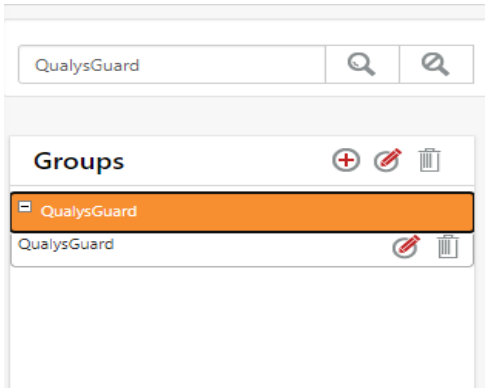


6.2 Token Template

1. In the **EventTracker** web interface, click the **Admin** dropdown, and then click **Parsing Rules.**
2. In the **Template** tab, click on the **Qualysguard** group folder to view the imported Templates.

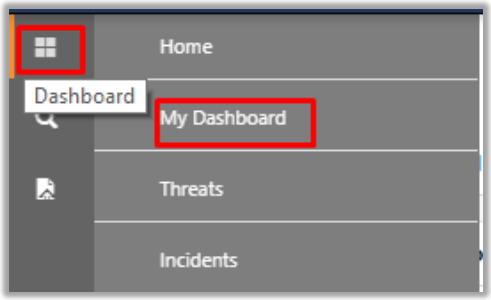
6.3 Knowledge Objects

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

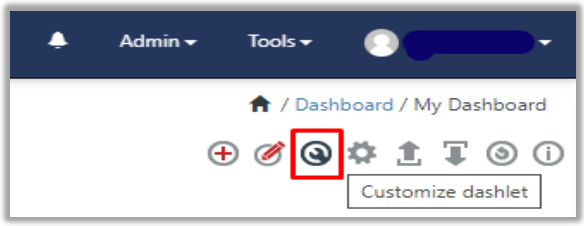


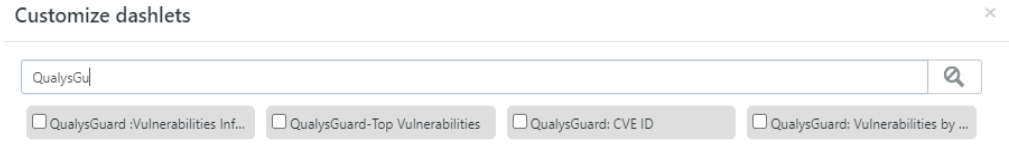
6.4 Dashboards

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



2. Select **Customize daslets** button and type **Qualysguard** 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