Netsurion. | EventTracker®

Integration Guide for Nessus Vulnerability Scanner

EventTracker v9.x and later

Publication Date: January 3, 2019

Abstract

This guide provides instructions to integrate **Nessus/Tenable vulnerability scanner** with EventTracker . Once **EventTracker** is configured to collect and parse these logs, dashboard and reports can be configured to monitor **Vulnerability** in your environment.

Scope

The configurations detailed in this guide are consistent with EventTracker version 9.x or above and **Nessus/Tenable Vulnerability scanner.**

Audience

Administrators who are assigned the task to monitor **Nessus/Tenable Vulnerability scanner** 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.

Complying with all applicable copyright Nessus 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.

Table of Contents

1. Overview

Nessus/Tenable Vulnerability scanner is a tool that identifies the vulnerability available/present in our environment.

EventTracker can integrate Nessus/Tenable vulnerability scanner that helps you to monitor vulnerabilities detected by the scanner into the EventTracker console. It provides a visual representation of top vulnerabilities detected in the environment, also shows highly vulnerable system which is having a high CVE score. Alerts are triggered whenever any critical or high severity vulnerabilities are detected in the environment. EventTracker can generate vulnerability reports on a scheduled basis as well. This report provides information about the system which is highly vulnerable.

2. Prerequisites

- EventTracker manager v9.x is required.
- EventTracker knowledge packs are required.
- Integrator should be installed in ETAgent/Manager machine.

3. Integrating Nessus/Tenable VS with EventTracker

1. Contact EventTracker Support for downloading Nessus Integrator.
2. Please import the Nessus KP before proceeding in EventTracker Manager machine.
3. Once the Nessus Integrator is downloaded, please run the integrator on EventTracker Agent Machine.

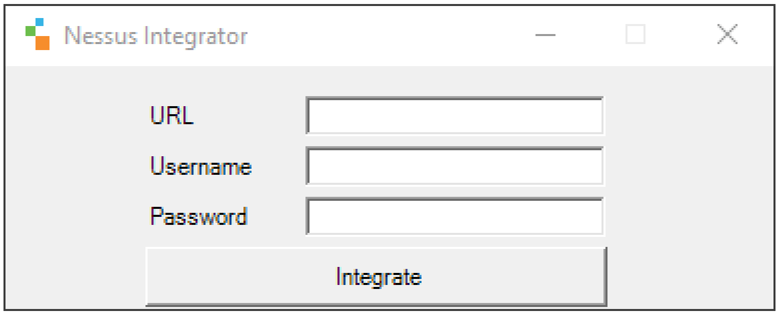
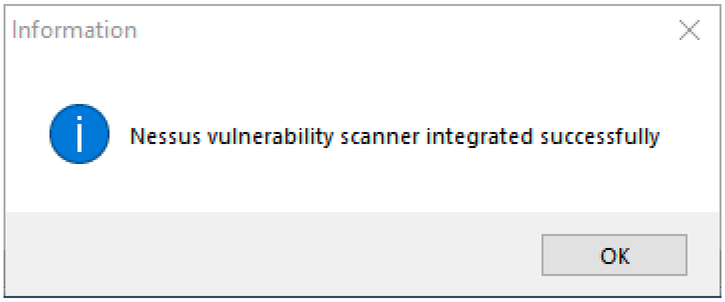


Figure 1

4. Please provide the Nessus web console URL (e.g. https://nessus.contoso.local:8834) and admin username/password.
   Note: In case of Tenable IO, please provide https://cloud.tenable.com in URL textbox.
5. Once you provide the information, click on **Integrate** button. It will validate the username/password. If it’s correct it will show the pop-up, integrated successfully message. Click on OK button to close the integration.


Information

Nessus vulnerability scanner integrated successfully

Figure 2

4. EventTracker Knowledge Packs

4.1 Saved Searches

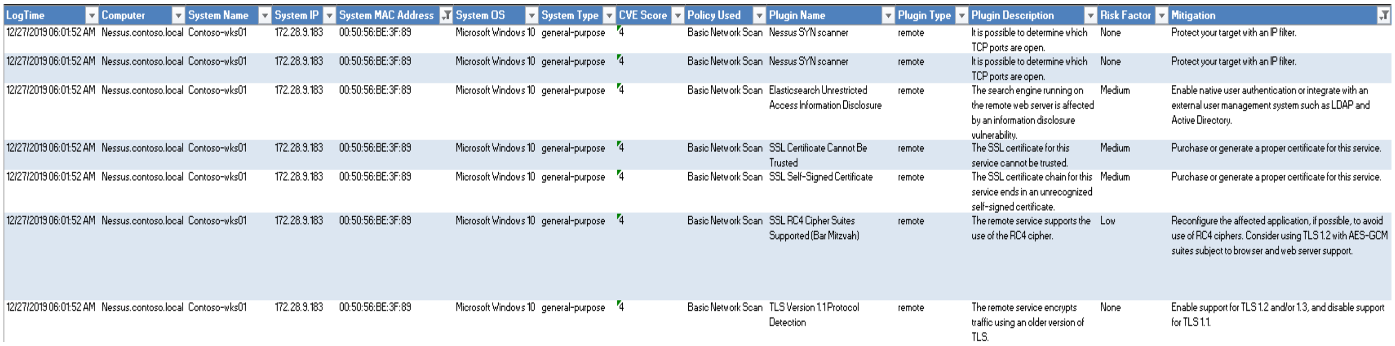
- **Nessus – Host with high CVE score:** This saved search provides information about the host which is having high CVE score.
- **Nessus – Vulnerability Detected:** This saved search provides information about the vulnerability detected on the environment.

4.2 Alerts

- **Nessus: Host with high CVE score** – This alert will generate whenever scanner detected host with CVE score between 6-10.
- **Nessus: Vulnerability with high risk –** This alert will generate whenever any vulnerability is detected with high risk.

4.3 Flex Reports

- **Nessus – Vulnerability Detected –** This report will provide information about the vulnerability detected in the environment. This report will have information about the system, CVE score, vulnerability detected on it and its risk level. It also provides information about the mitigation of vulnerability detected on the system.



LogTime	Computer	System Name	System IP	System MAC Address	System OS	System Type	CVE Score	Policy Used	Plugin Name	Plugin Type	Plugin Description	Risk Factor	Mitigation
12/27/2019 06:01:52 AM	Nessus.contoso.local	Contoso-wks01	172.28.9.183	00:50:56:BE:3F:89	Microsoft Windows 10	general-purpose	4	Basic Network Scan	Nessus SYN scanner	remote	It is possible to determine which TCP ports are open.	None	Protect your target with an IP filter.
12/27/2019 06:01:52 AM	Nessus.contoso.local	Contoso-wks01	172.28.9.183	00:50:56:BE:3F:89	Microsoft Windows 10	general-purpose	4	Basic Network Scan	Nessus SYN scanner	remote	It is possible to determine which TCP ports are open.	None	Protect your target with an IP filter.
12/27/2019 06:01:52 AM	Nessus.contoso.local	Contoso-wks01	172.28.9.183	00:50:56:BE:3F:89	Microsoft Windows 10	general-purpose	4	Basic Network Scan	Elasticsearch Unrestricted Access Information Disclosure	remote	The search engine running on the remote web server is affected by an information disclosure vulnerability.	Medium	Enable native user authentication or integrate with an external user management system such as LDAP and Active Directory.
12/27/2019 06:01:52 AM	Nessus.contoso.local	Contoso-wks01	172.28.9.183	00:50:56:BE:3F:89	Microsoft Windows 10	general-purpose	4	Basic Network Scan	SSL Certificate Cannot Be Trusted	remote	The SSL certificate for this service cannot be trusted.	Medium	Purchase or generate a proper certificate for this service.
12/27/2019 06:01:52 AM	Nessus.contoso.local	Contoso-wks01	172.28.9.183	00:50:56:BE:3F:89	Microsoft Windows 10	general-purpose	4	Basic Network Scan	SSL Self-Signed Certificate	remote	The SSL certificate chain for this service ends in an unrecognized self-signed certificate.	Medium	Purchase or generate a proper certificate for this service.
12/27/2019 06:01:52 AM	Nessus.contoso.local	Contoso-wks01	172.28.9.183	00:50:56:BE:3F:89	Microsoft Windows 10	general-purpose	4	Basic Network Scan	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	remote	The remote service supports the use of the RC4 cipher.	Low	Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.
12/27/2019 06:01:52 AM	Nessus.contoso.local	Contoso-wks01	172.28.9.183	00:50:56:BE:3F:89	Microsoft Windows 10	general-purpose	4	Basic Network Scan	TLS Version 1.1 Protocol Detection	remote	The remote service encrypts traffic using an older version of TLS.	None	Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Figure 3

4.4 Dashboards

- **Nessus – Vulnerability detected on host**

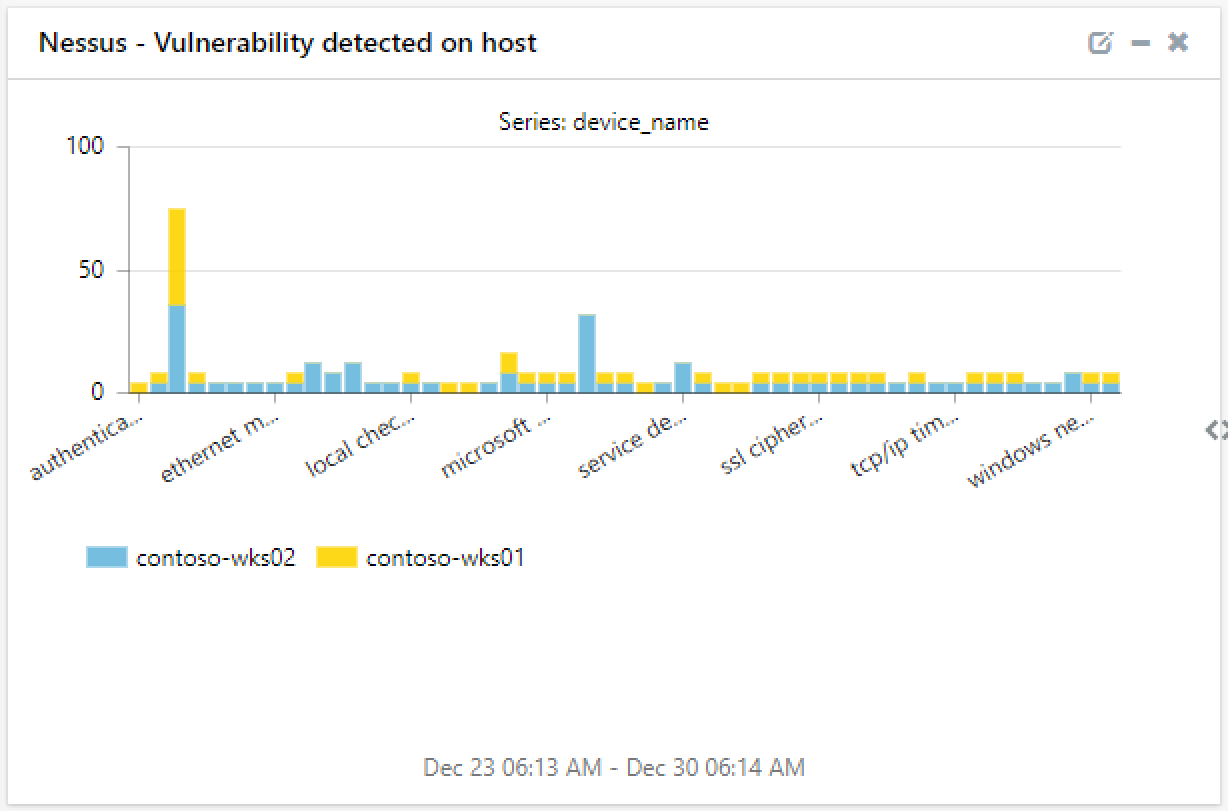


Figure 4

- **Nessus – Host with high CVE score**

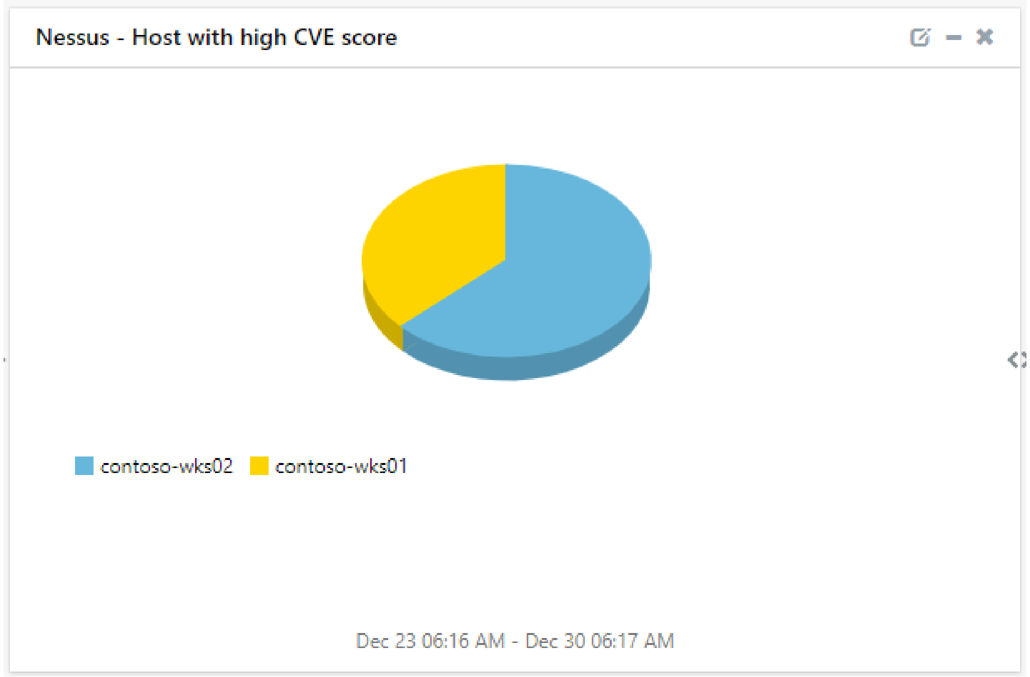

Nessus - Host with high CVE score
🟦 contoso-wks02
🟨 contoso-wks01
Dec 23 06:16 AM - Dec 30 06:17 AM

Figure 5

- **Nessus – Operating system scanned**

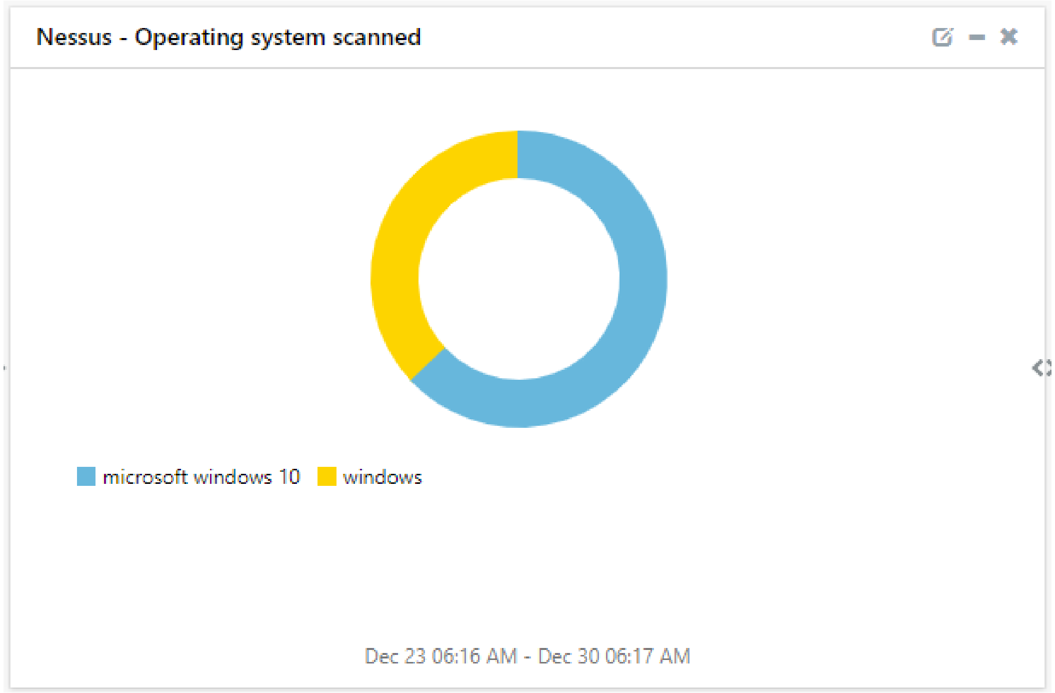

Nessus - Operating system scanned
🟦 microsoft windows 10
🟨 windows
Dec 23 06:16 AM - Dec 30 06:17 AM

Figure 6

- **Nessus – Policy used by scanner**

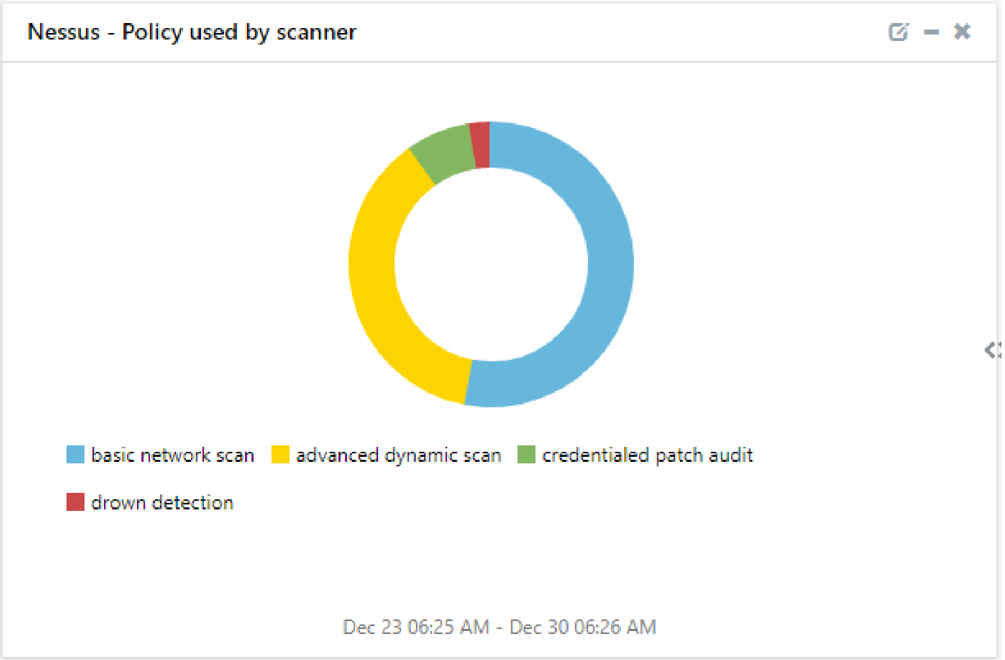


Figure 7

- **Nessus – Vulnerability detected on daily basis**
- **Nessus – Vulnerability by risk factor**

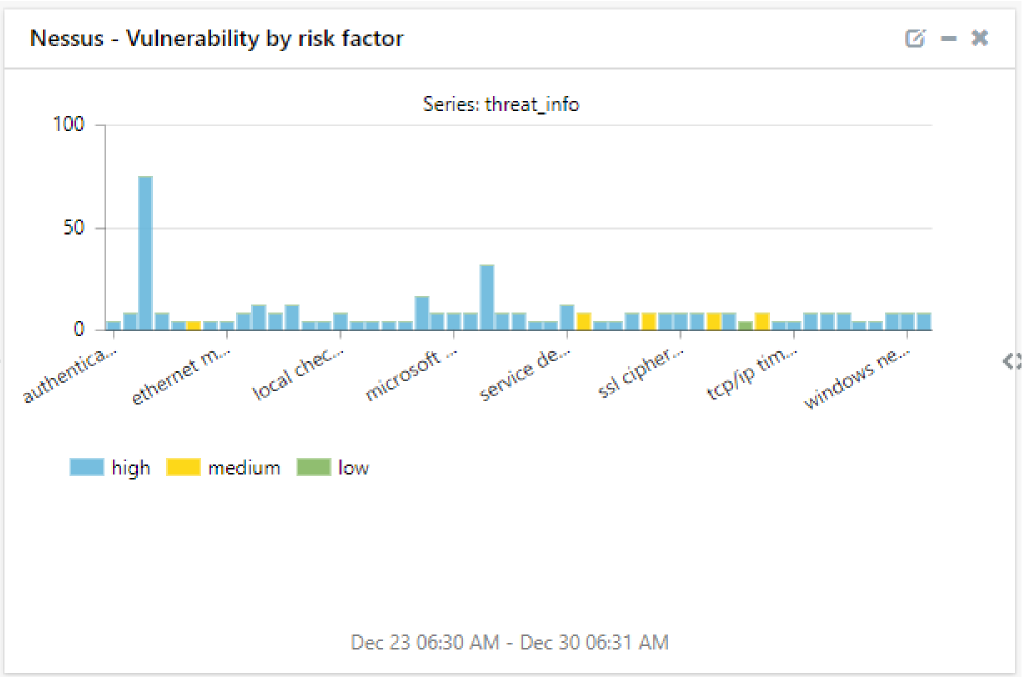


Figure 8

5. Importing knowledge pack into EventTracker

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

1. Press "⊞ + R".
2. Now, 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
- Alerts
- Flex Reports
- Knowledge Objects
- Dashboards

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

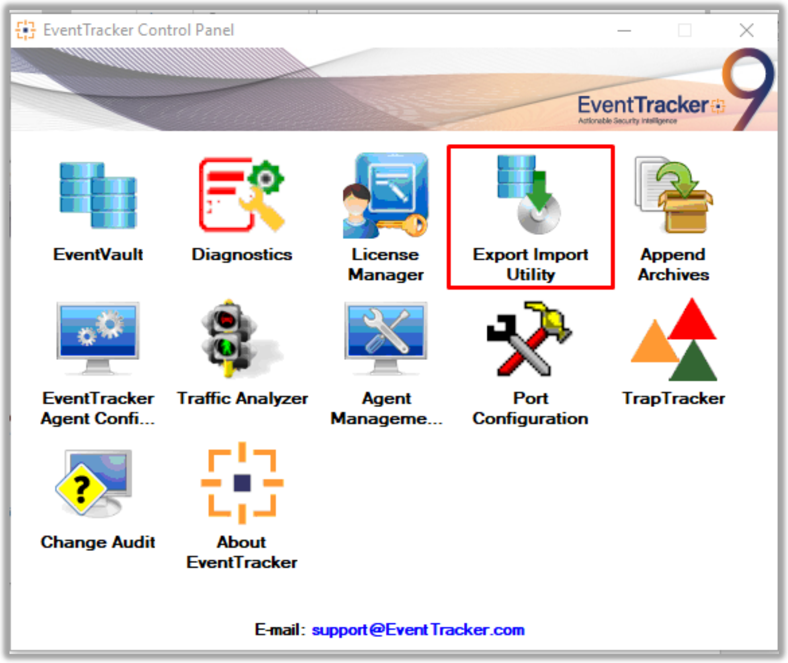
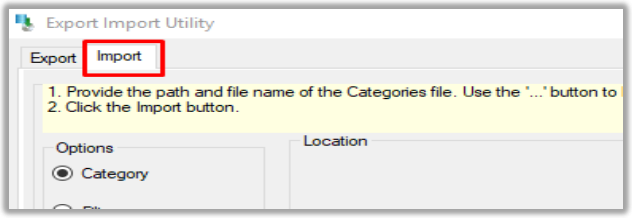


Figure 9



1. Provide the path and file name of the Categories file. Use the '...' button to
2. Click the Import button.

Figure 10

3. Click the **Import** tab.

5.1 Saved Searches

For importing saved searches, please login to **EventTracker web interface**

1. Click on **log Search** button and navigate to **Import**

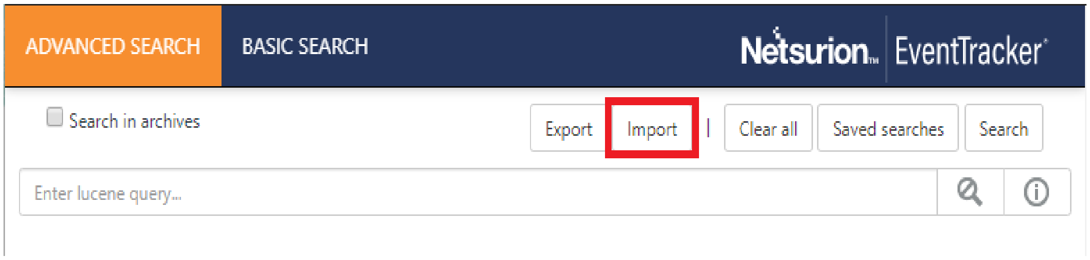


Figure 11

2. Now click on **browse** and select **Saved searches_Nessus Scanner.etss** file and click on **Upload** button.

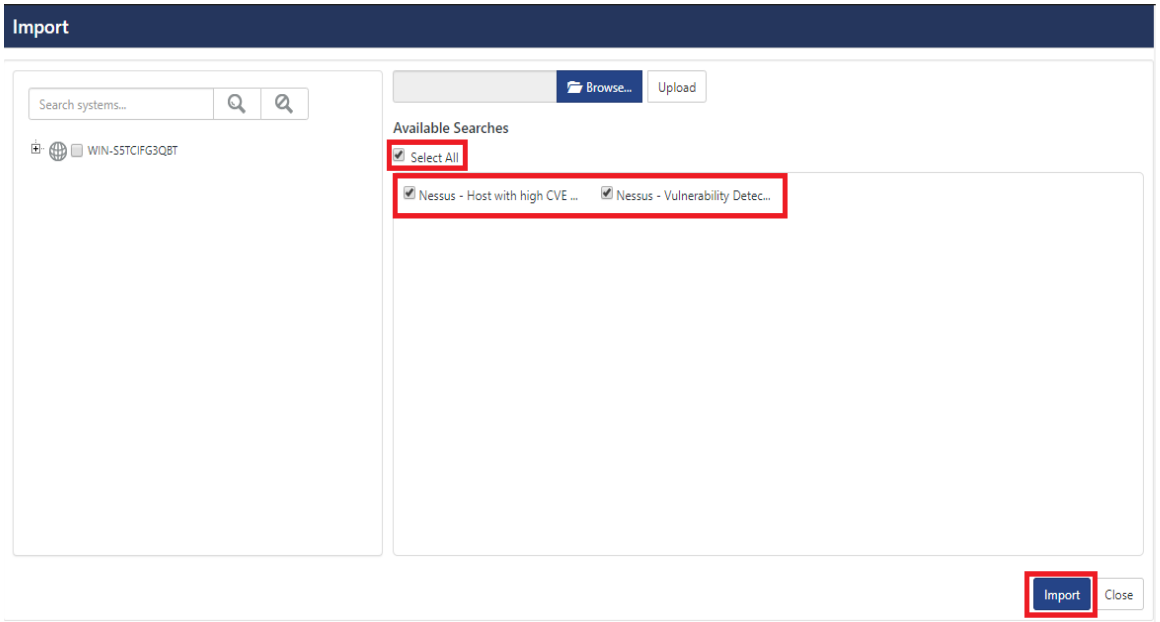
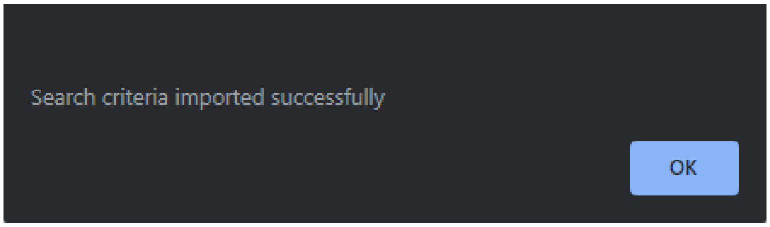


Figure 12

3. Now check **Select All** button and click on **import.**

   EventTracker display success message

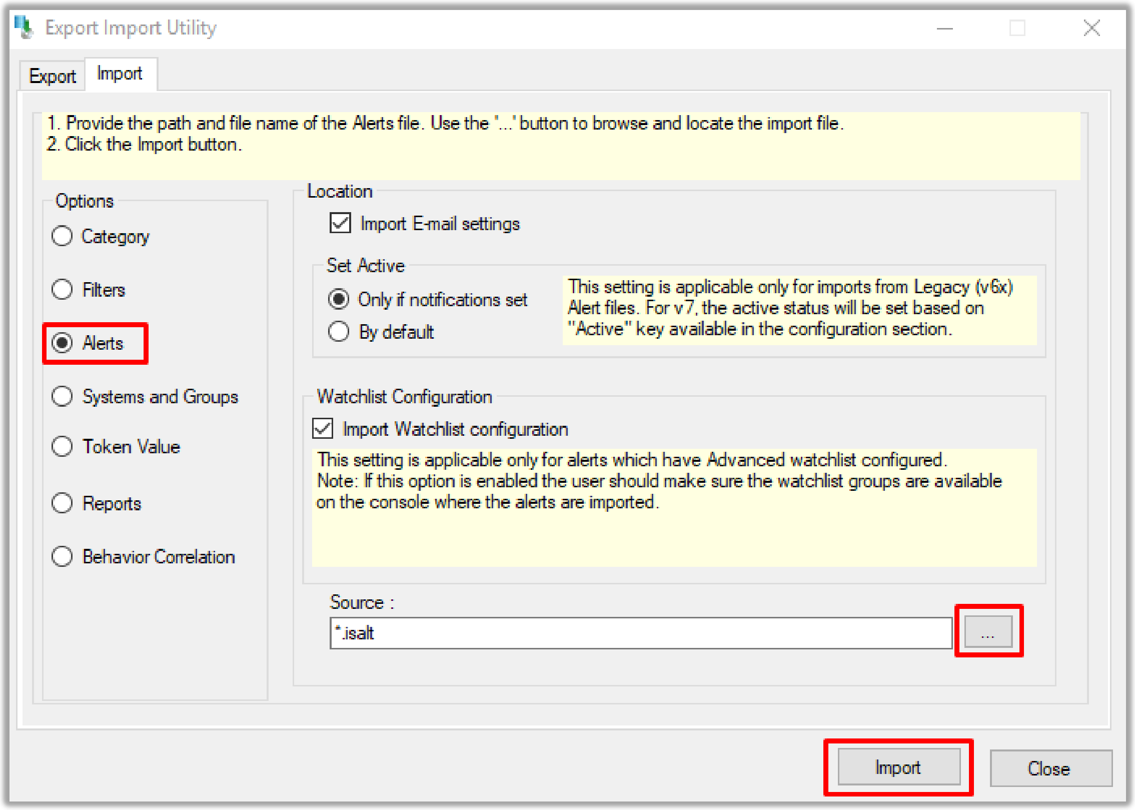


Search criteria imported successfully

Figure 13

5.2 Alerts

1. Once you have opened "**Export Import Utility**" via "**EventTracker Control Panel**", click **Alert** option, and then click the browse button. ...
2. Navigate to the knowledge pack folder and select the file with extension **".isalt**", **e.g.** "**Alerts_Nessus Scanner.isalt**" and then click on the "**Import**" button:



1. Provide the path and file name of the Alerts file. Use the '...' button to browse and locate the import file.
2. Click the Import button.

Options: ○ Category ○ Filters ● Alerts ○ Systems and Groups ○ Token Value ○ Reports ○ Behavior Correlation

Location

☑ Import E-mail settings

Set Active: ● Only if notifications set ○ By default

This setting is applicable only for imports from Legacy (v6x) Alert files. For v7, the active status will be set based on "Active" key available in the configuration section.

Watchlist Configuration

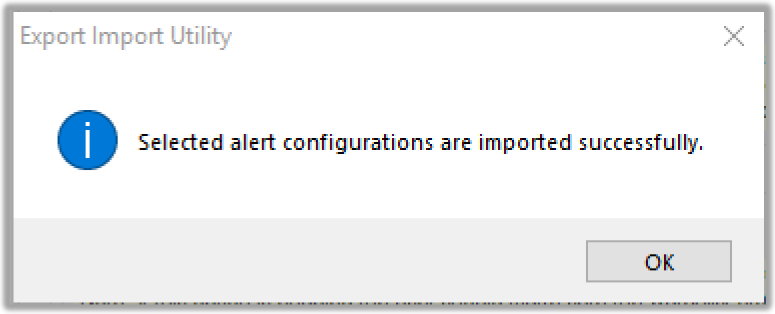
☑ Import Watchlist configuration

This setting is applicable only for alerts which have Advanced watchlist configured.
Note: If this option is enabled the user should make sure the watchlist groups are available on the console where the alerts are imported.

Source : *.isalt

Figure 14

EventTracker displays a success message:

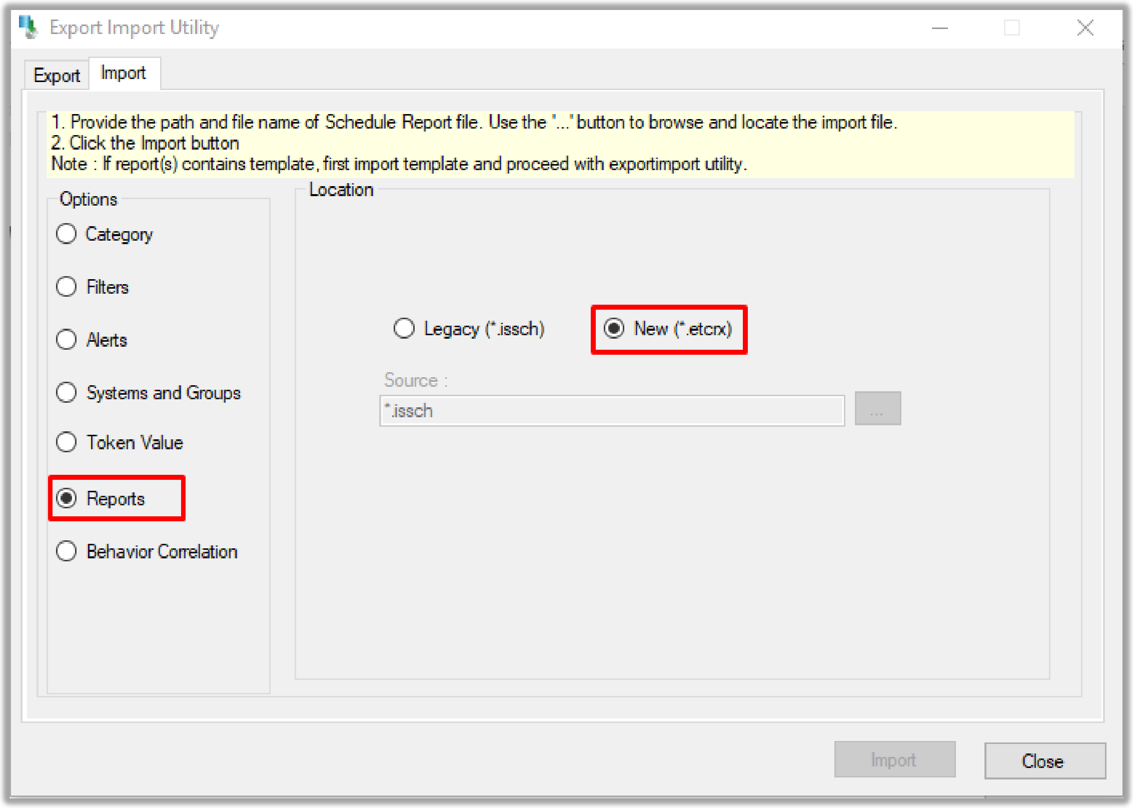


Selected alert configurations are imported successfully.

Figure 15

5.3 Flex Reports

1. In EventTracker control panel, select “**Export/ Import utility**” and select the “**Import tab**”. Then, click **Reports** option, and choose “**New (*.etcrx)**”:



1. Provide the path and file name of Schedule Report file. Use the '...' button to browse and locate the import file.
2. Click the Import button
Note : If report(s) contains template, first import template and proceed with exportimport utility.

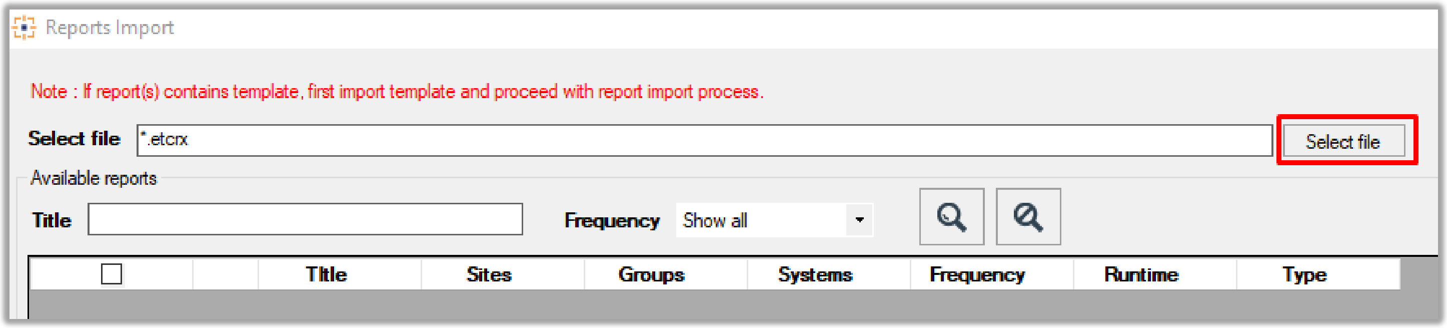
○ Category
○ Filters
○ Alerts
○ Systems and Groups
○ Token Value
● Reports
○ Behavior Correlation

○ Legacy (*.issch) ● New (*.etcrx)

Source : *.issch

Figure 16

2. Once you have selected “**New (*.etcrx)**”, a new pop-up window will appear. Click “**Select File**” button and navigate to knowledge pack folder and select file with extension **“.etcrx”, e.g. “Reports_Nessus Scanner.etcrx”.**



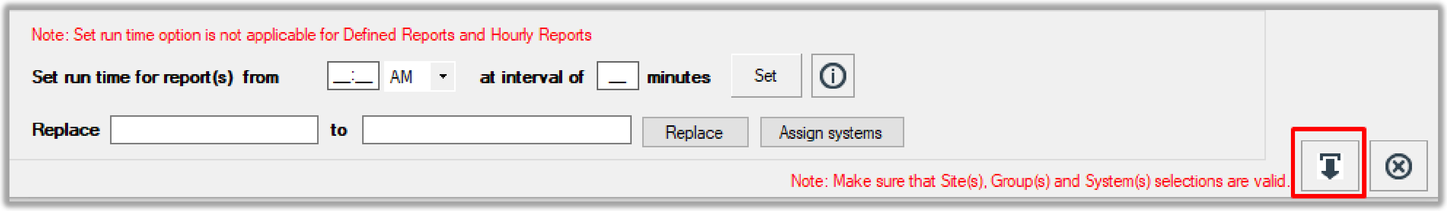
Note : If report(s) contains template, first import template and proceed with report import process.

Select file: *.etcrx

☐		Title	Sites	Groups	Systems	Frequency	Runtime	Type

Figure 17

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

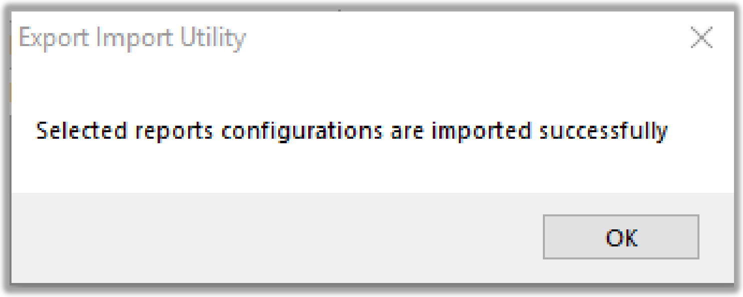


Note: Set run time option is not applicable for Defined Reports and Hourly Reports

Note: Make sure that Site(s), Group(s) and System(s) selections are valid.

Figure 18

EventTracker displays a success message:



Selected reports configurations are imported successfully

Figure 19

5.4 Knowledge Objects

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

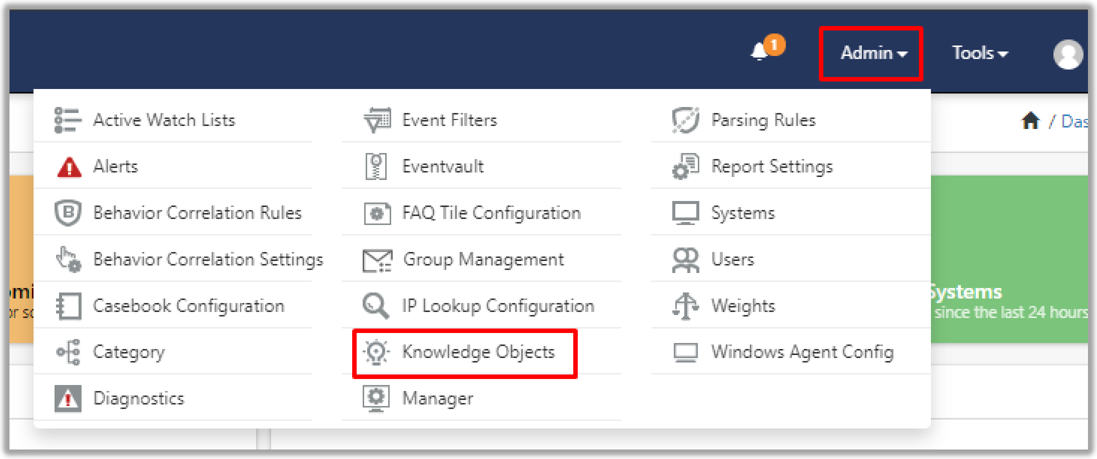


Figure 201

2. Next, click the **"import object"** icon:

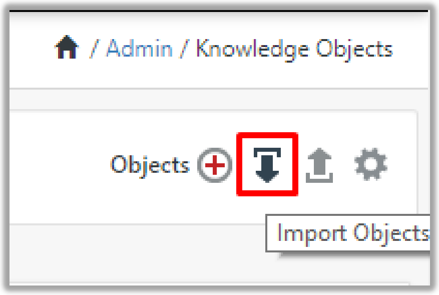


Figure 21

3. A pop-up box will appear, 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_Nessus Scanner.etko"** and then click "**Upload**" button.

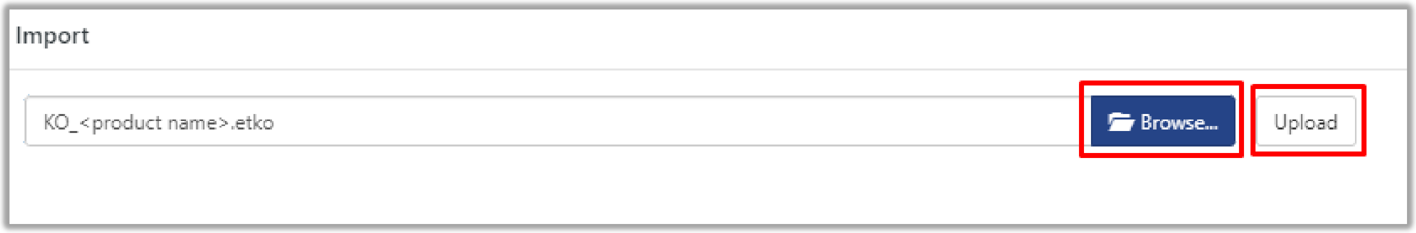


Figure 22

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

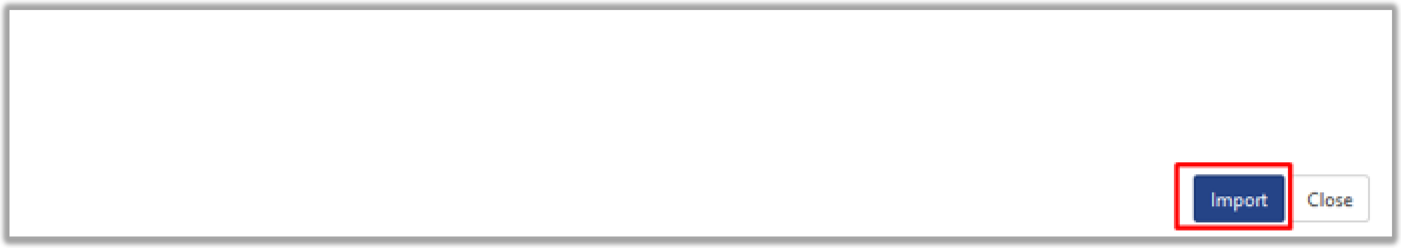


Figure 23

5.5 Dashboards

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

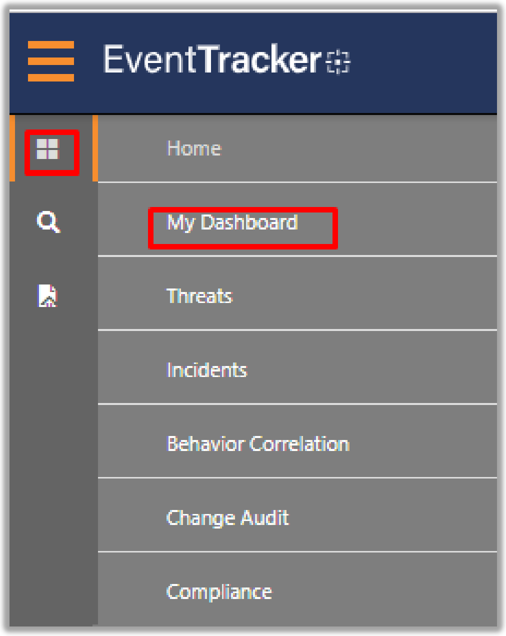


Figure 2

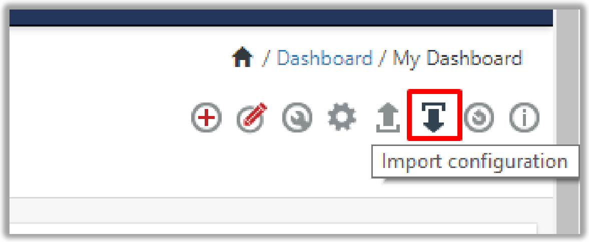
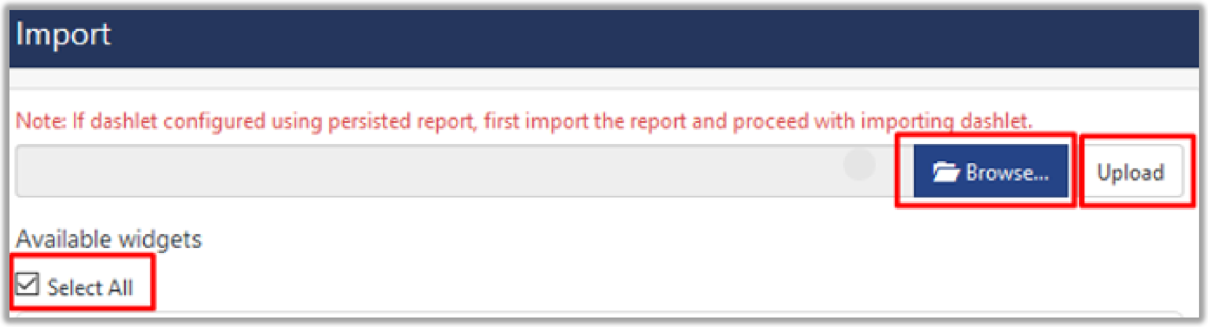


Figure 25

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_Nessus Scanner.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.



Import

Note: If dashlet configured using persisted report, first import the report and proceed with importing dashlet.

Figure 26

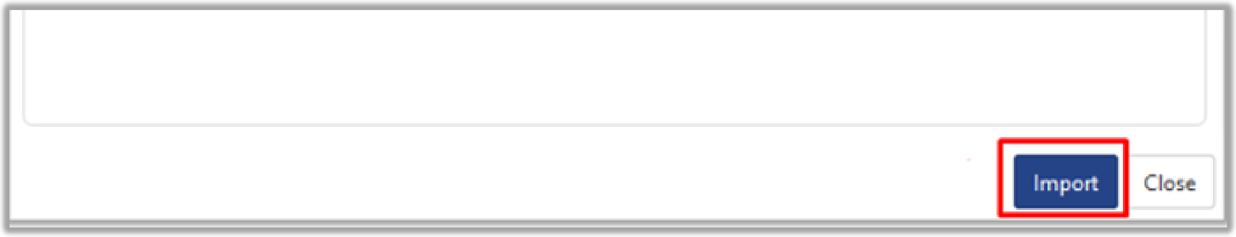
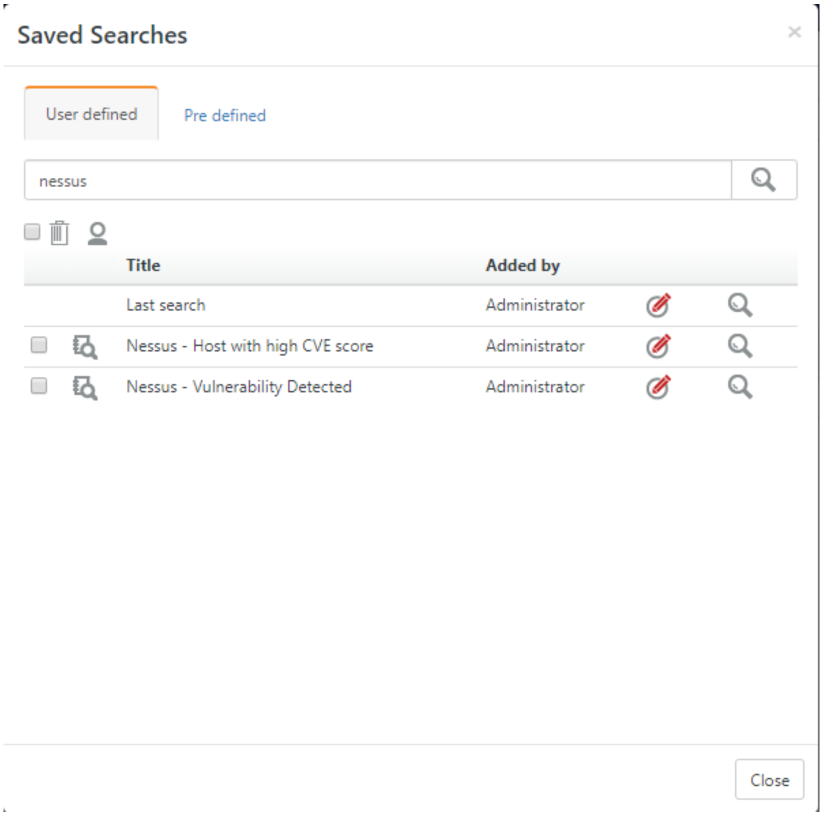


Figure 27

6. Verifying knowledge pack in EventTracker

6.1 Saved Searches

1. Login to **EventTracker manager web interface**.
2. Click **log search** button, and then click **Saved Searches**.
3. In **search bar** type Nessus and click on search button.



Saved Searches

User defined | Pre defined

nessus

		Title	Added by
		Last search	Administrator
□		Nessus - Host with high CVE score	Administrator
□		Nessus - Vulnerability Detected	Administrator

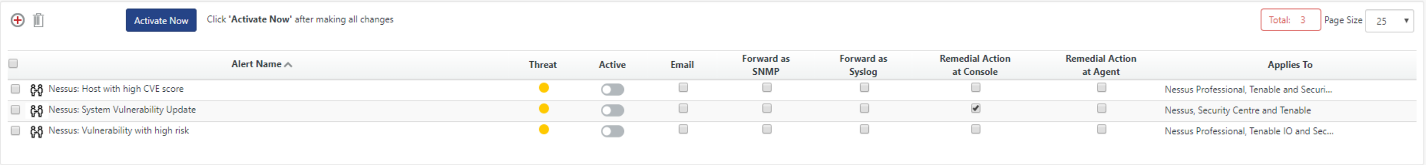
Close

Figure 28

6.2 Alerts

1. In the **EventTracker manager** web interface, click the **Admin** dropdown, and then click **Alerts.**
2. In search box enter “**<search criteria> e.g. “Nessus”** and then click the **Search** button.

   EventTracker displays an alert related to **“Nessus”:**



Activate Now Click **'Activate Now'** after making all changes

Total: 3 Page Size 25

□	Alert Name	Threat	Active	Email	Forward as SNMP	Forward as Syslog	Remedial Action at Console	Remedial Action at Agent	Applies To
□	Nessus: Host with high CVE score	●		□	□	□	□	□	Nessus Professional, Tenable and Securi...
□	Nessus: System Vulnerability Update	●		□	□	□	☑	□	Nessus, Security Centre and Tenable
□	Nessus: Vulnerability with high risk	●		□	□	□	□	□	Nessus Professional, Tenable IO and Sec...

Figure 29

6.3 Flex Reports

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

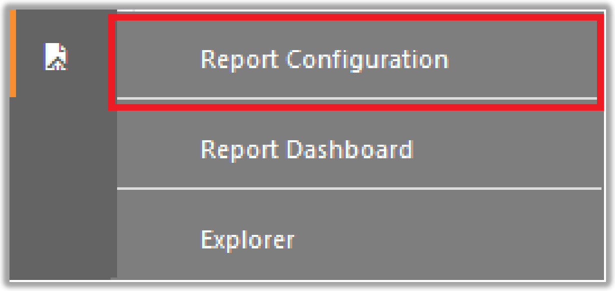
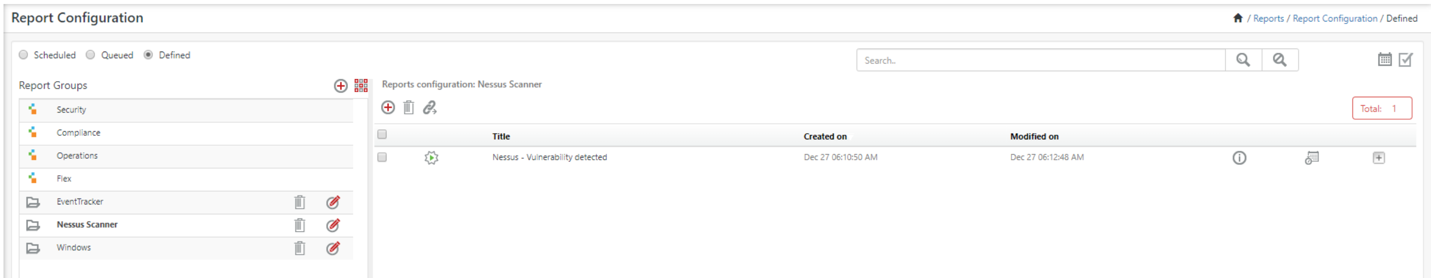


Figure 3

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



		Title	Created on	Modified on
□		Nessus - Vulnerability detected	Dec 27 06:10:50 AM	Dec 27 06:12:48 AM

Figure 4

6.4 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 "**Nessus Scanner**" group folder to view the imported Knowledge objects.

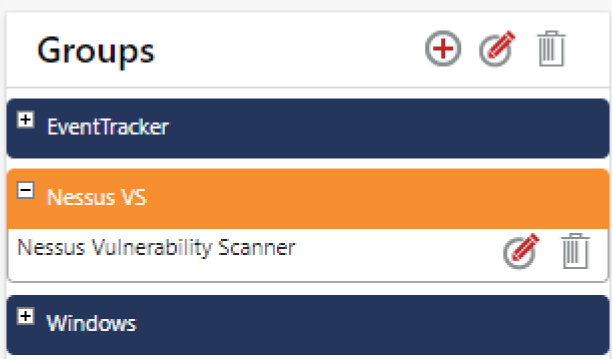


Figure 32

6.5 Dashboards

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

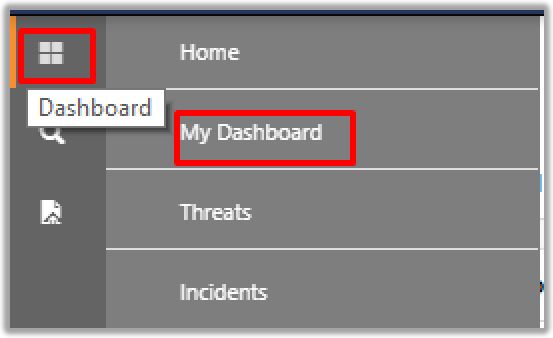
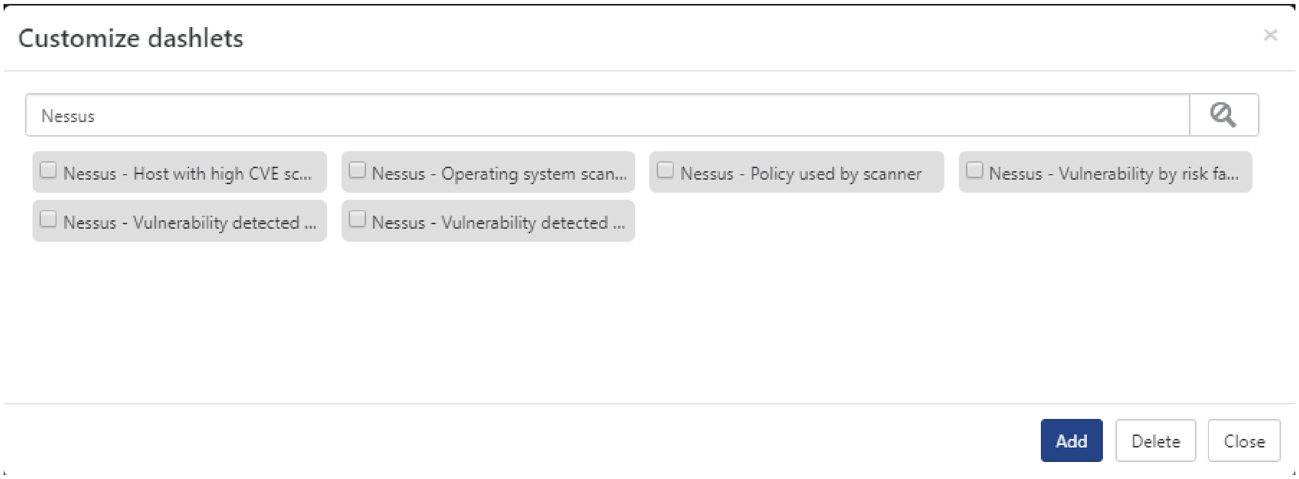


Figure 33

2. Click on dashlet configure button and search for "**Nessus**"



Customize dashlets

Nessus

☐ Nessus - Host with high CVE sc...
☐ Nessus - Operating system scan...
☐ Nessus - Policy used by scanner
☐ Nessus - Vulnerability by risk fa...
☐ Nessus - Vulnerability detected ...
☐ Nessus - Vulnerability detected ...

Figure 34