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.
# Table of Contents

1. Overview .......................................................................................................................... 3
2. Prerequisites ....................................................................................................................... 3
3. Integrating Nessus/Tenable VS with EventTracker ......................................................... 3
4. EventTracker Knowledge Packs ....................................................................................... 4
   4.1 Saved Searches .............................................................................................................. 4
   4.2 Alerts .......................................................................................................................... 4
   4.3 Flex Reports ............................................................................................................... 4
   4.4 Dashboards ................................................................................................................ 5
5. Importing knowledge pack into EventTracker ................................................................. 8
   5.1 Saved Searches ........................................................................................................... 9
   5.2 Alerts ....................................................................................................................... 10
   5.3 Flex Reports ............................................................................................................. 11
   5.4 Knowledge Objects .................................................................................................. 12
   5.5 Dashboards ............................................................................................................... 14
6. Verifying knowledge pack in EventTracker .................................................................... 15
   6.1 Saved Searches ........................................................................................................... 15
   6.2 Alerts ....................................................................................................................... 16
   6.3 Flex Reports ............................................................................................................. 16
   6.4 Knowledge Objects .................................................................................................. 17
   6.5 Dashboards ............................................................................................................... 17
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.

![Nessus Integrator](image)

**Figure 1**

4. Please provide the Nessus web console URL (e.g. [https://nessus.contoso.local:8834](https://nessus.contoso.local:8834)) and admin username/password.

**Note:** In case of Tenable IO, please provide [https://cloud.tenable.com](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.
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.
4.4 Dashboards

- **Nessus – Vulnerability detected on host**

![Figure 3](image)

![Figure 4](image)
- **Nessus – Host with high CVE score**

![Nessus - Host with high CVE score](image)

Figure 5

- **Nessus – Operating system scanned**

![Nessus - Operating system scanned](image)

Figure 6
• **Nessus – Policy used by scanner**

![Nessus - Policy used by scanner](image1.png)

*Figure 7*

• **Nessus – Vulnerability detected on daily basis**

• **Nessus – Vulnerability by risk factor**

![Nessus - Vulnerability by risk factor](image2.png)

*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
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](image1)

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

   ![Figure 12](image2)
3. Now check Select All button and click on import.

EventTracker display success message

![Figure 13](image1)

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:

![Figure 14](image2)

EventTracker displays a success message:
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)”: 

![Figure 16](image)

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”.

![Figure 15](image)
3. Wait while reports are being populated in below tables. Now, select all the relevant reports and then click **Import** button.

EventTracker displays a success message:

![Success message dialog box](image)

**Figure 19**

### 5.4 Knowledge Objects

1. Click **Knowledge objects** under the **Admin** option in the EventTracker manager web interface.
2. Next, click the “import object” icon:

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.

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_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.

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.
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**”:

![Figure 29](image)

6.3 Flex 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 “**Nessus**” group folder to view the imported reports.

![Report Configuration](image1)

![Nessus Knowledge Objects](image2)

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.

![Groups](image3)

6.5 Dashboards

1. In the EventTracker web interface, Click on Home Button and select “**My Dashboard**.”
2. Click on dashlet configure button and search for “Nessus”