Integration Guide

# Integrate LastPass with the Netsurion Open XDR platform

**Publication Date:**

January 18, 2023

## Abstract

This guide provides instructions to configure the Data Source Integration in the Netsurion Open XDR platform to receive the logs from LastPass. The Data Source Integration contains alerts, reports, dashboards, and knowledge objects.

**Note:**

The screen/ figure references are only for illustration purpose and may not match the installed product UI.

## Scope

The configuration details in this guide are consistent with the Netsurion Open XDR platform version 9.3 or later and LastPass.

## Audience

This guide is for the administrators responsible for configuring the Data Source Integration in the Netsurion Open XDR platform.

## Product Terminology

The following are the terms used throughout this guide:

- The term “Netsurion’s Open XDR platform” or “the Netsurion Open XDR platform” refers to EventTracker.
- The term “Data Source Integrations” refers to Knowledge Packs.

# Table of Contents

# 1 Overview

LastPass is a password manager that stores encrypted passwords online. It provides features to keep the critical information safe and secure so you can access it whenever and wherever required. It saves all the passwords, addresses, credit cards, and more in the secure vault.

The Netsurion Open XDR platform facilitates monitoring events retrieved from LastPass. Its dashboard, category, alerts, and reports benefit in detecting any suspicious activities like Master password changed, reverted, and failed activities, MFA disabled activities, and more.

# 2 Prerequisite

- Configure LastPass to forward logs to the Netsurion Open XDR platform.

> **Note**
>
> Refer to How-To guide to configure LastPass to forward logs to the Netsurion Open XDR platform.

# 3 The Netsurion Open XDR platform Data Source Integration (DSI)

After the logs are received by the Netsurion Open XDR Manager, configure the Data Source Integration into Netsurion Open XDR platform.

The following Data Source Integration are available in the Netsurion Open XDR platform.

## 3.1 Category

**LastPass – User activities:** This category of the saved search allows to parse all events.

**LastPass – Password usage activity by user**: This category of the saved search allows to parse the events that are specific to the password copy activities.

## 3.2 Alerts

**LastPass: Multiple login failures detected:** This alert is triggered whenever multiple login failure activity is detected.

**LastPass: Password or provisioning hash manipulated:** This alert is triggered whenever a user modifies, reverts, and fails to update the appropriate password or resets the provisioning hash value.

**LastPass: Multifactor authentication disabled:** This alert is triggered whenever a user disables the authentication.

**LastPass: User history purged:** This alert is triggered whenever the users clear the activity history in their LastPass vault.

## 3.3 Reports

**LastPass – User activities:** This report captures all the activities performed by the users.

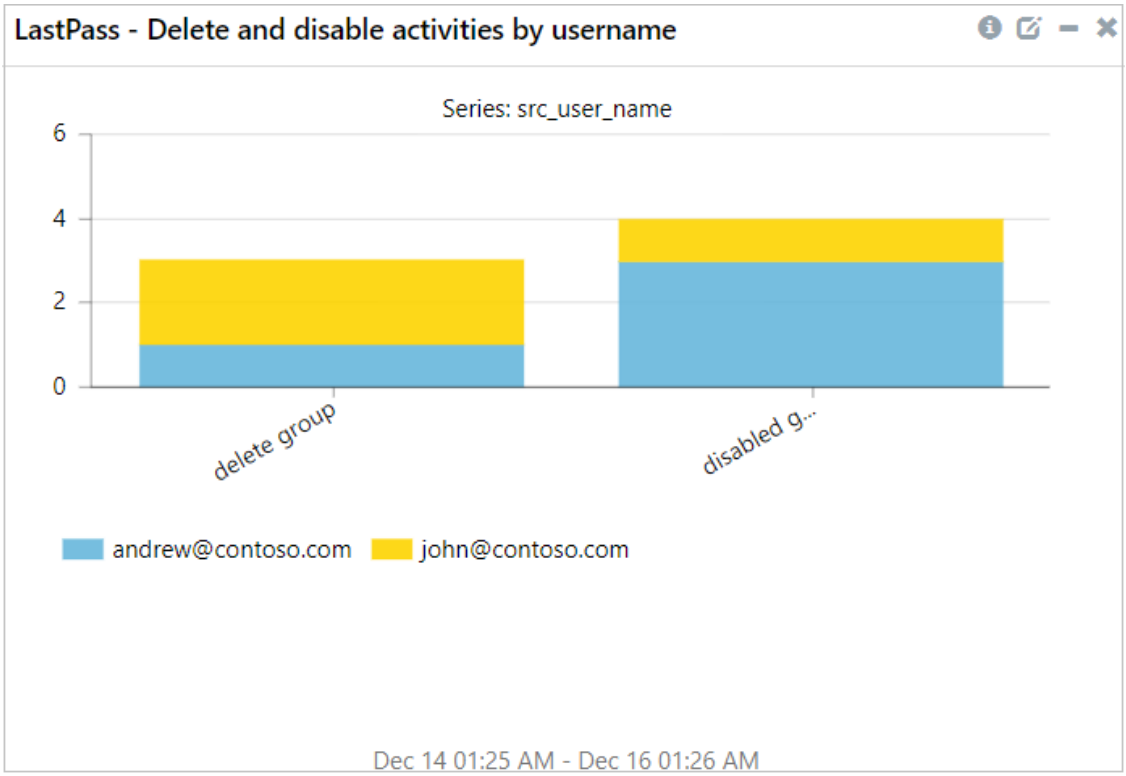
| Computer | Source IP Address | User Name | Action | LogInfo |
|---|---|---|---|---|
| ETTBLRGUI-3\LASTPASS | 24.215.16.02 | andrew@contoso.com | Deleting User | "LastPass via Website" |
| ETTBLRGUI-3\LASTPASS | 64.215.10.09 | adam@contoso.com | Deleted shared folder | myfreshworks.com |
| ETTBLRGUI-3\LASTPASS | 54.15.16.65 | nadia@contoso.com | Failed login attempt | "LastPass via Website" |
| ETTBLRGUI-3\LASTPASS | 54.15.16.65 | nadia@contoso.com | Change Password Failed | "LastPass via Website" |
| ETTBLRGUI-3\LASTPASS | 54.15.16.65 | adam@contoso.com | Disabled google authenticator | "LastPass via Website" |
| ETTBLRGUI-3\LASTPASS | 54.15.16.65 | nadia@contoso.com | Disable SAML Map Entry | "LastPass via Website" |
| ETTBLRGUI-3\LASTPASS | 54.15.16.65 | nadia@contoso.com | Failed login attempt | "LastPass via Website" |

**LastPass – Password usage activity by user**: This report captures all the user's password usage activities.

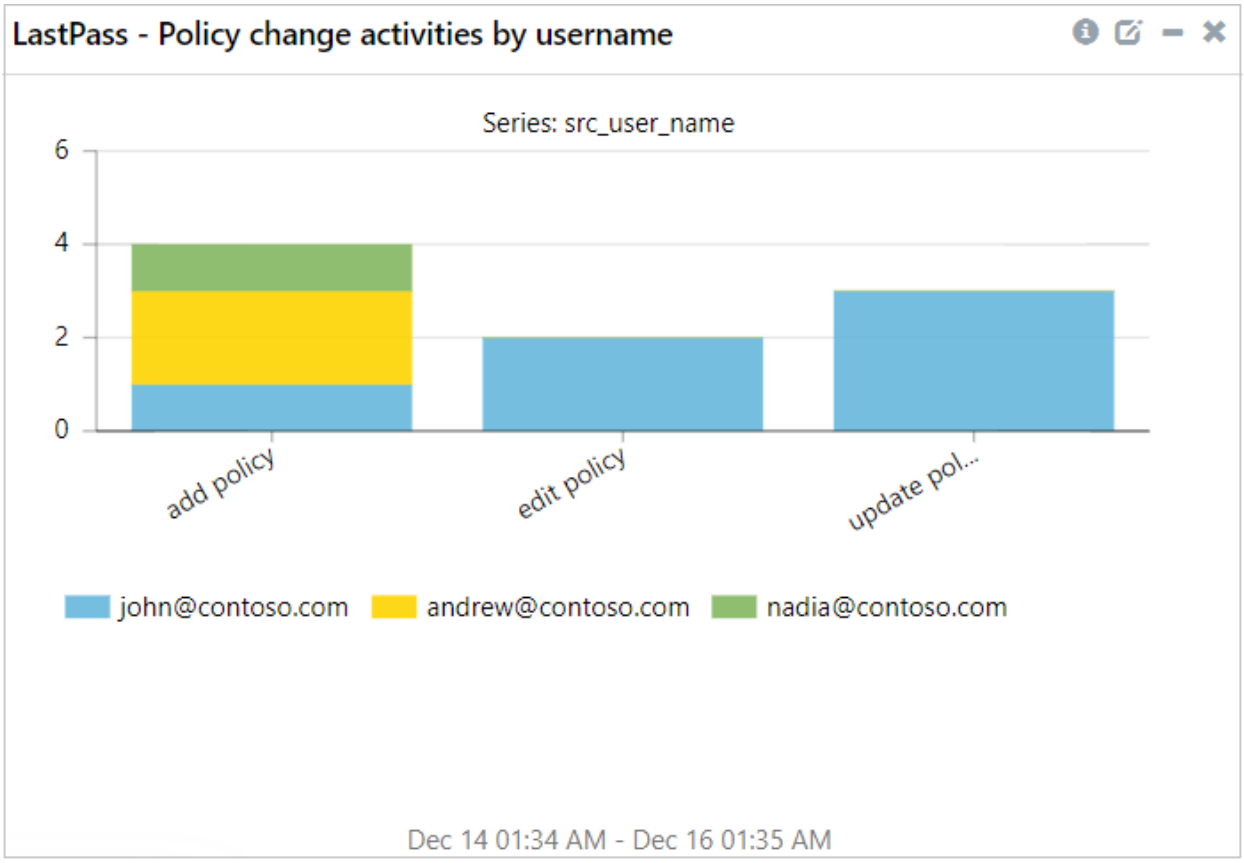
| LogTime | Computer | Source IP Address | User Name | Action | LogInfo |
|---|---|---|---|---|---|
| 12-07-2022 11:01:45 PM | ETTBLRGUI-3\LASTPASS | 10.215.16.26 | nadia@contoso.com | Log in | myfreshworks.com |
| 12-07-2022 11:01:53 PM | ETTBLRGUI-3\LASTPASS | 172.45.16.32 | john@contoso.com | Log in | myfreshworks.com |
| 12-07-2022 11:02:22 PM | ETTBLRGUI-3\LASTPASS | 10.215.16.02 | john@contoso.com | Log in | google.com |
| 12-07-2022 11:02:37 PM | ETTBLRGUI-3\LASTPASS | 198.88.17.35 | andrew@contoso.com | Log in | google.com |
| 12-07-2022 11:02:54 PM | ETTBLRGUI-3\LASTPASS | 10.36.18.54 | andrew@contoso.com | Log in | myfreshworks.com |
| 12-07-2022 11:03:08 PM | ETTBLRGUI-3\LASTPASS | 10.215.12.65 | andrew@contoso.com | Log in | amazon.com |

## 3.4 Dashboard

**LastPass – Delete and disable activities by username:** This dashlet displays all the deleted and disabled activities by username.



**LastPass – Policy change activities by username:** This dashlet displays all the user's policy change activities like add, edit, and update.

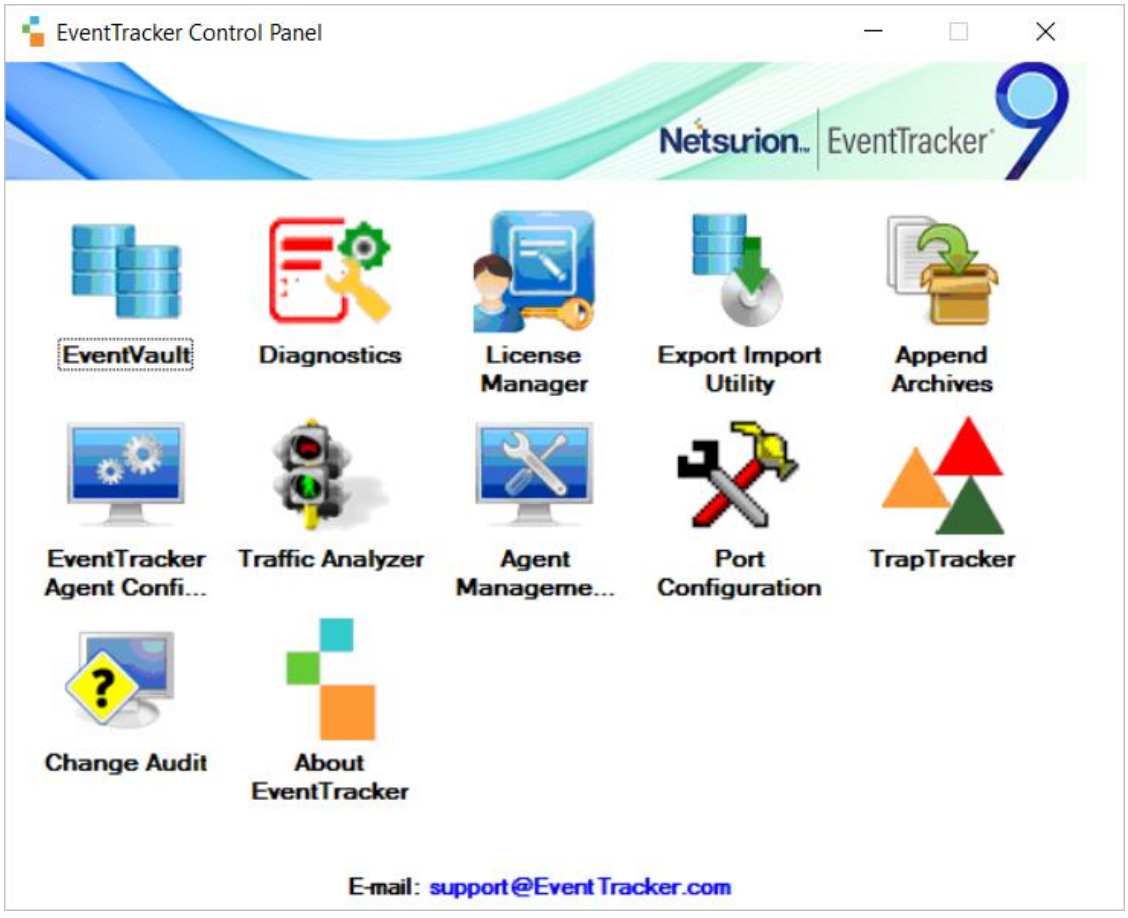


# 4 Importing Data Source Integration into the Netsurion Open XDR platform

Import the Data Source Integration items in the following sequence.

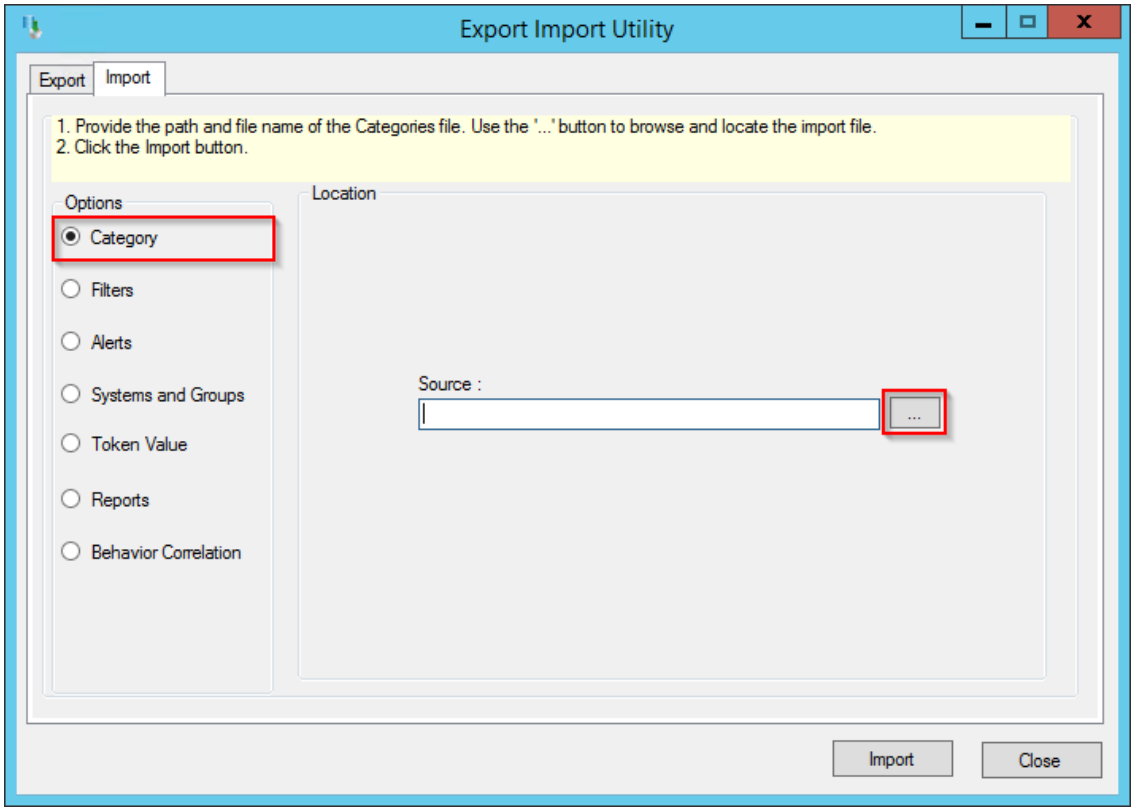
- Categories
- Alerts
- Reports
- Knowledge Objects
- Dashboard

1. Launch the Netsurion Open XDR platform **Control Panel**.
2. Double click **Export-Import Utility** and click the **Import** tab.

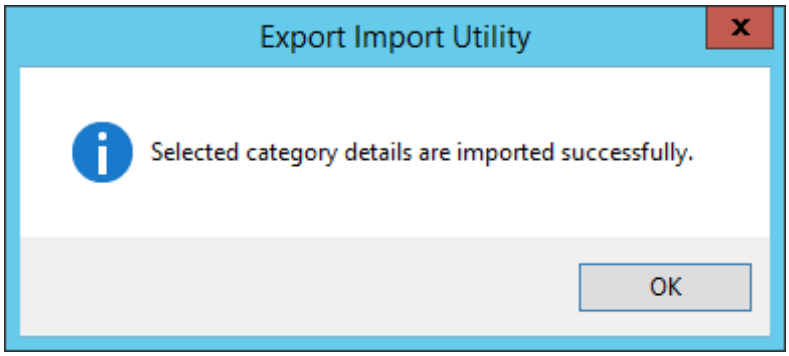


## 4.1 Category

1. In the **Import** tab, click **Category**, and then click the **Browse** button to locate the file.



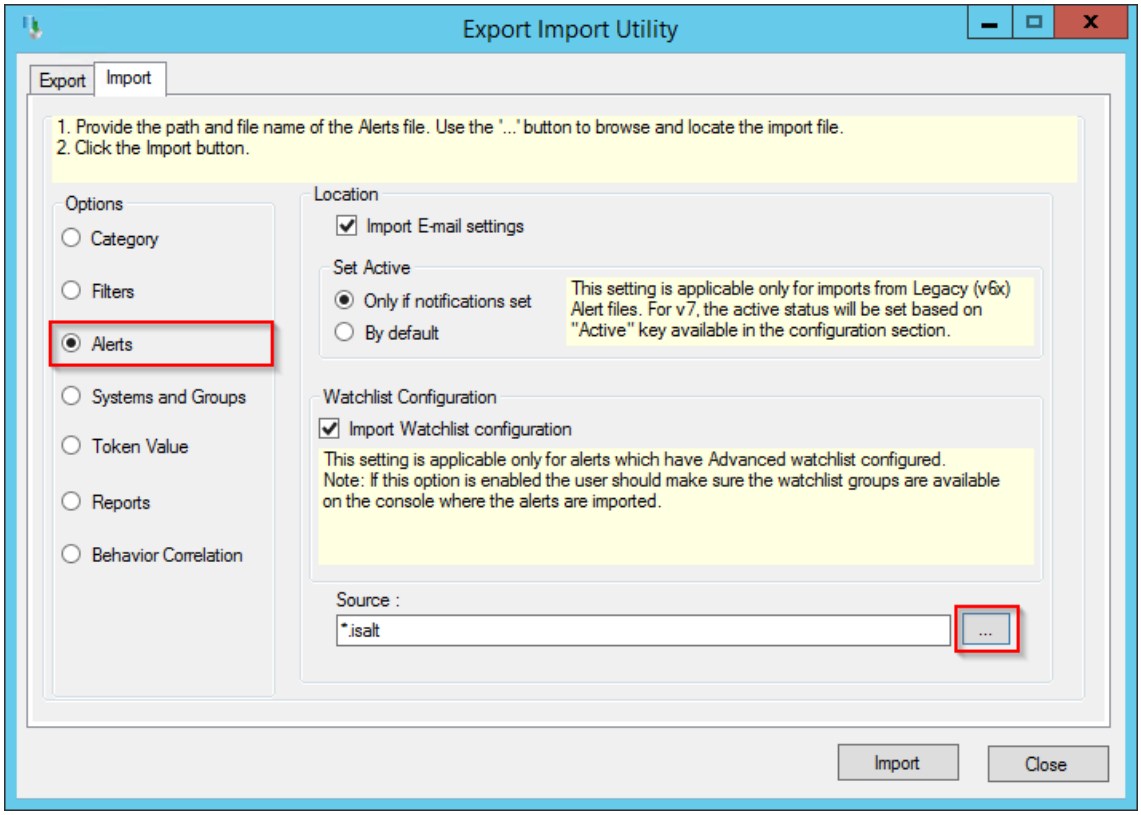

2. In the **Browse** window, locate the **Category_LastPass.iscat** file and click **Open**.
3. To import the categories, click **Import**.
4. The Netsurion Open XDR platform displays a success message on successfully importing the selected file in **Category**.



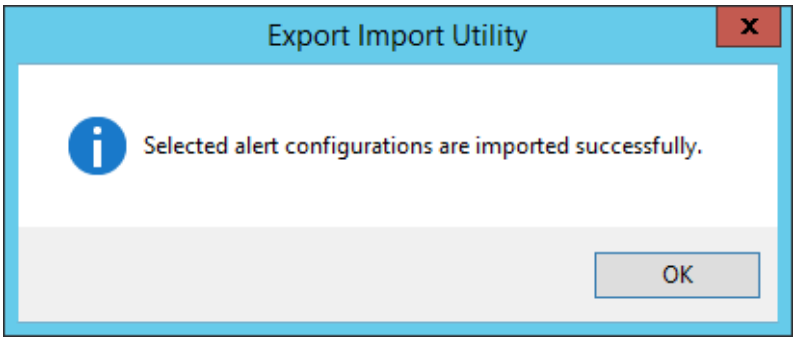

5. Click **OK** or the **Close** button to complete the process.

## 4.2 Alerts

1. In the **Import** tab, click **Alerts**, and then click the **Browse** ... button to locate the file.



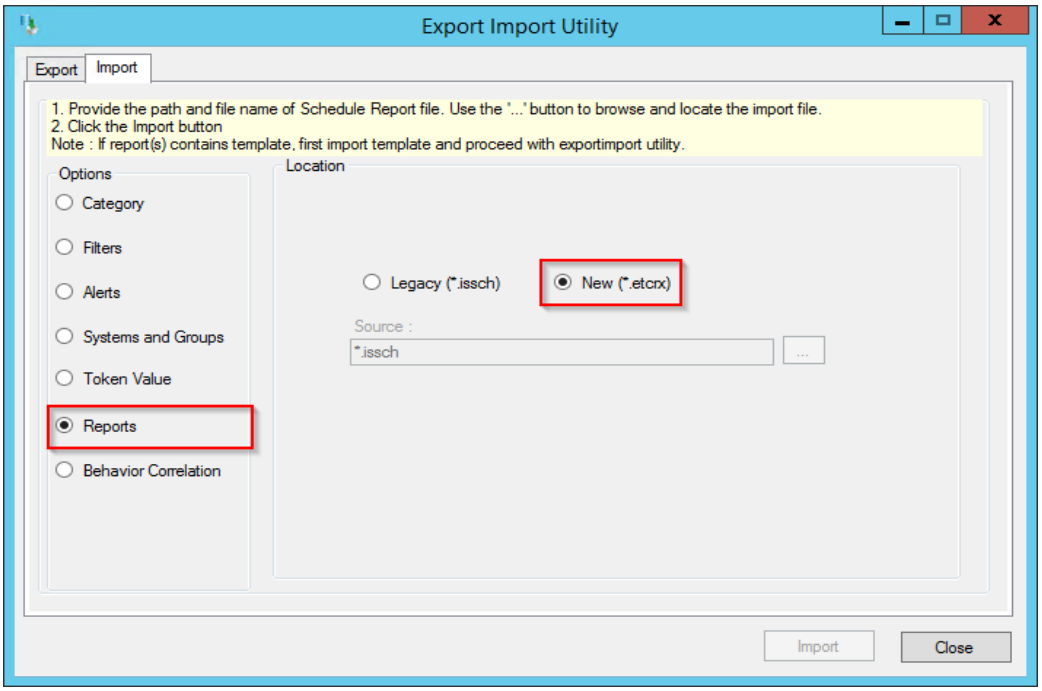

2. In the **Browse** window, locate the **Alerts_ LastPass.isalt** file, and then click **Open**.
3. To import the alerts, click **Import**.
4. The Netsurion Open XDR platform displays a success message on successfully importing the selected file in **Alerts**.



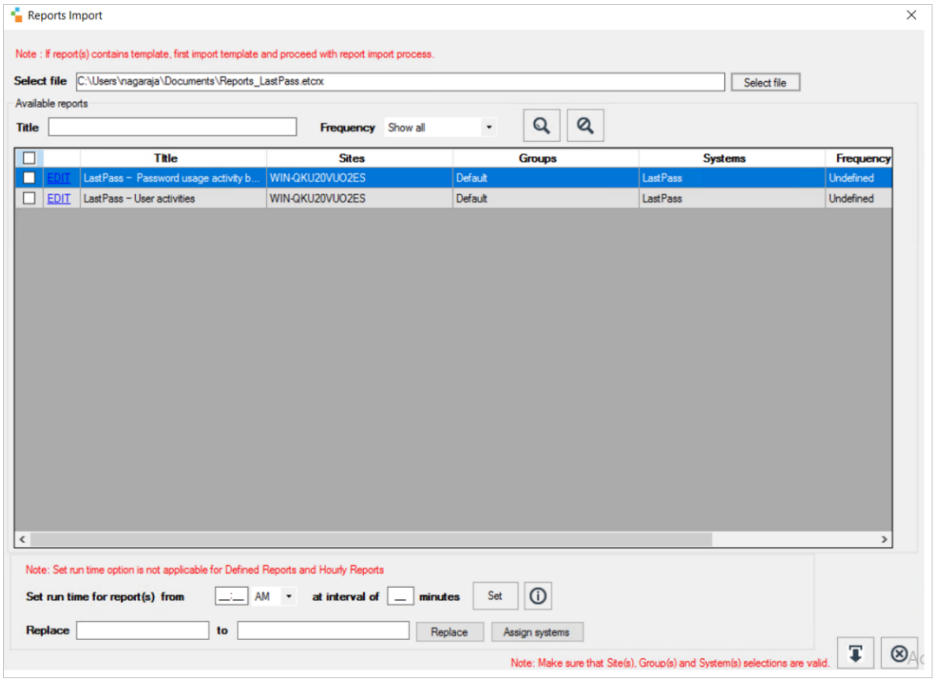

5. Click **OK** or the **Close** button to complete the process.

## 4.3 Reports

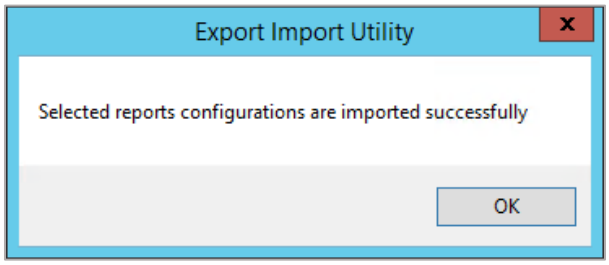
1. In the **Import** tab, click **Reports** and then click **New (*.etcrx)**.




2. In the **Reports Import** window, click **Select file** to locate **Reports_ LastPass.etcrx** file.
3. Select the check box of all the files and click the **Import** button to import the selected files



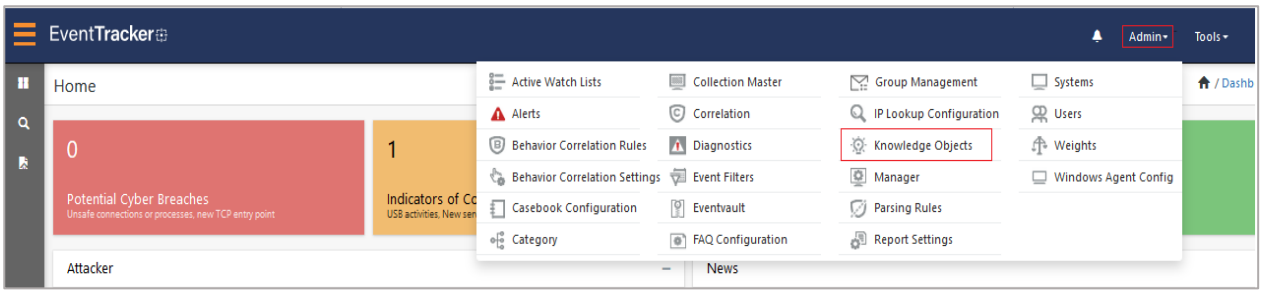
4. The Netsurion Open XDR platform displays a success message on successful importing of the selected file in **Reports**.



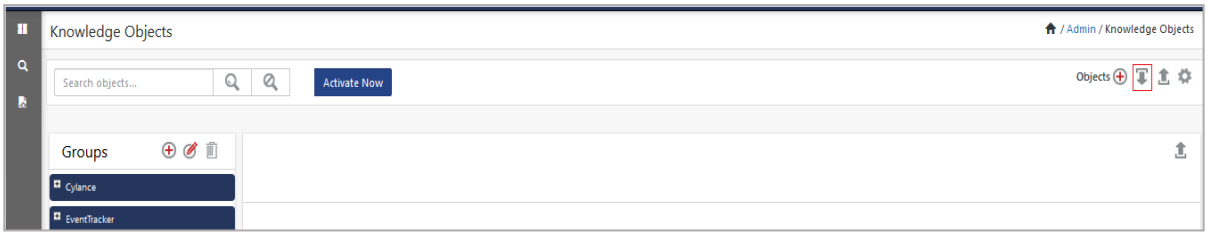

5. Click **OK** or the **Close** button to complete the process.

## 4.4 Knowledge Objects (KO)

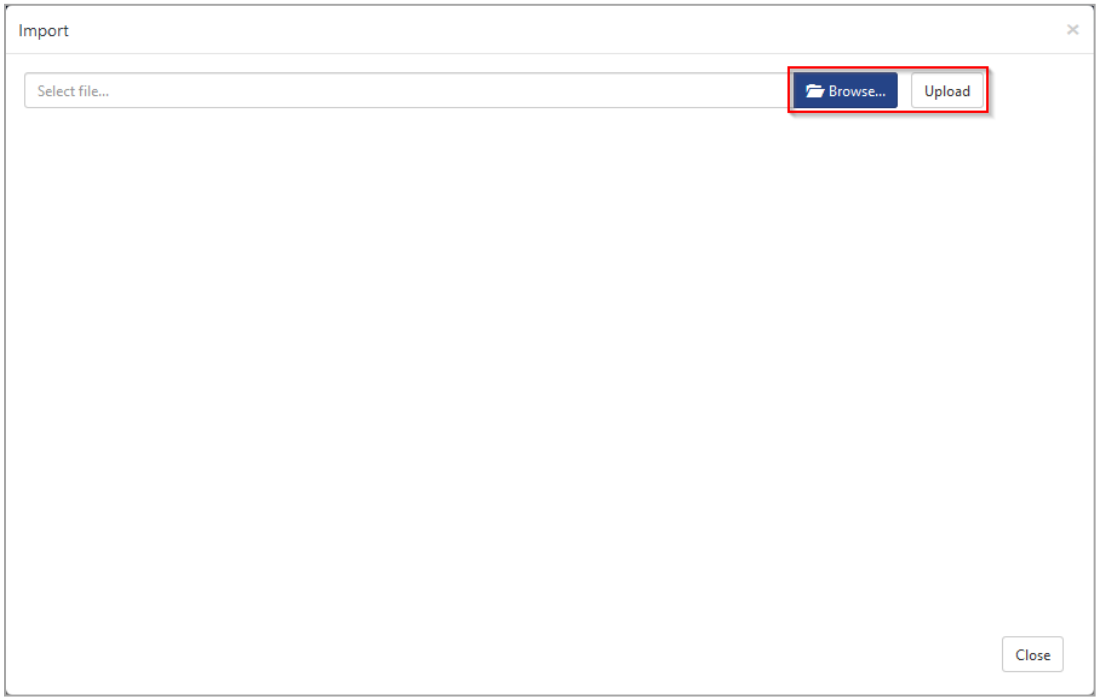
1. In the **Netsurion Open XDR platform** console, hover over the **Admin** menu and click **Knowledge Objects.**



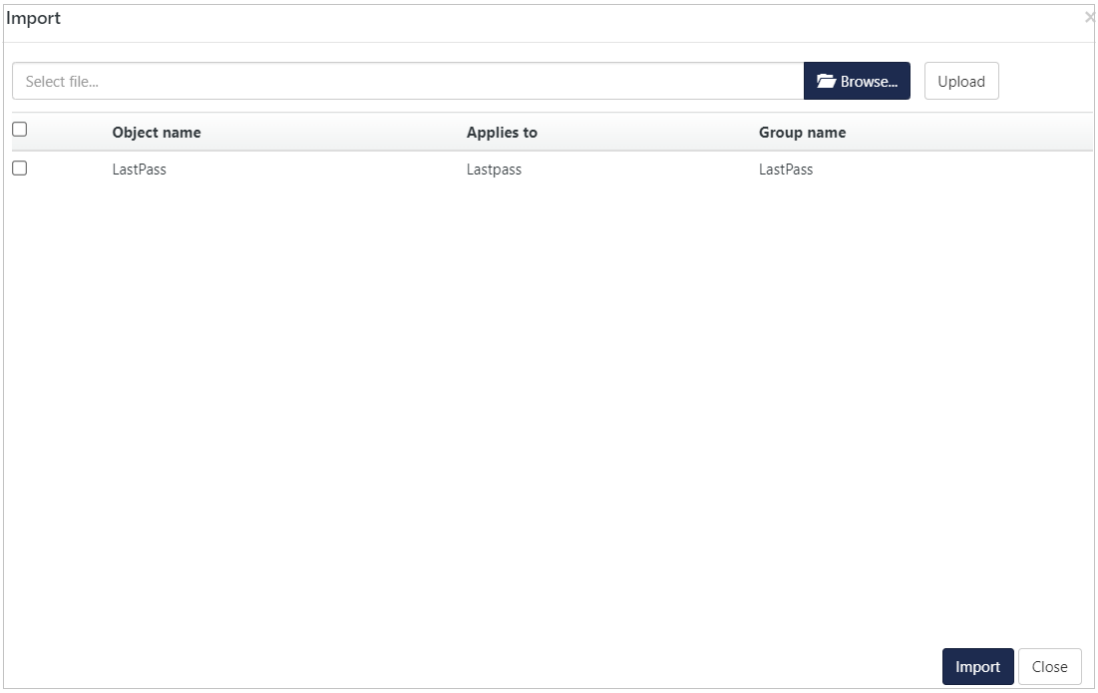

2. In the **Knowledge Objects** interface, click the **Import** button to import the KO files.



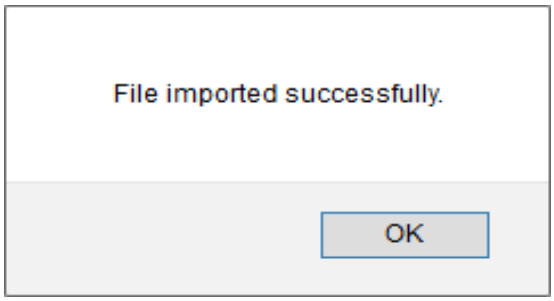
3. In the **Import** window, click **Browse** and locate the **KO_LastPass.etko** file.




4. Select the check box next to the browsed KO file and then click the **Import** button.



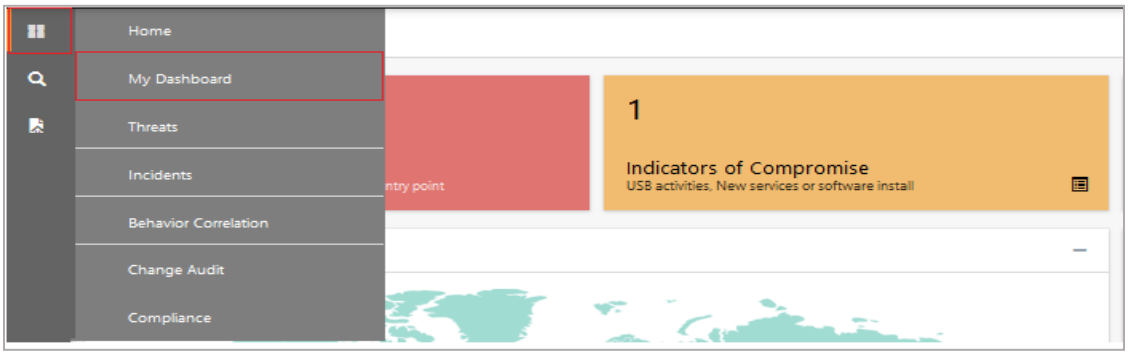
5. The Netsurion Open XDR platform displays a successful message on successfully importing the selected file in **Knowledge Objects**.




6. Click **OK** or the **Close** button to complete the process.

## 4.5 Dashboard

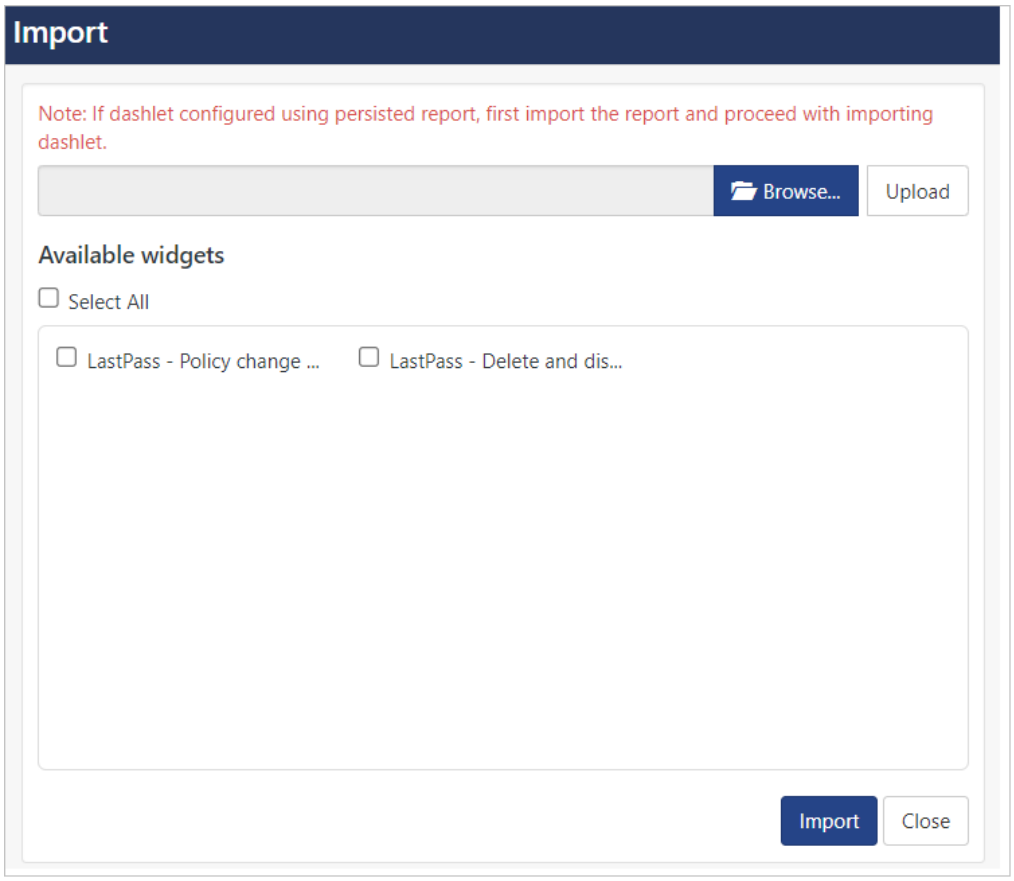
1. Log in to The **Netsurion Open XDR platform** web interface and go to **Dashboard** > **My Dashboard**.



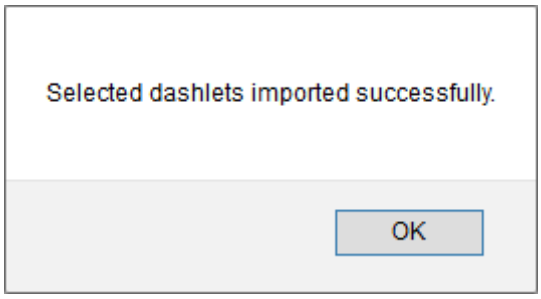

2. In the **My Dashboard** interface, click the **Import** button to import the dashlet files.


3. In the **Import** window, click **Browse** to locate the **Dashboard_LastPass.etwd** file and then click **Upload.**

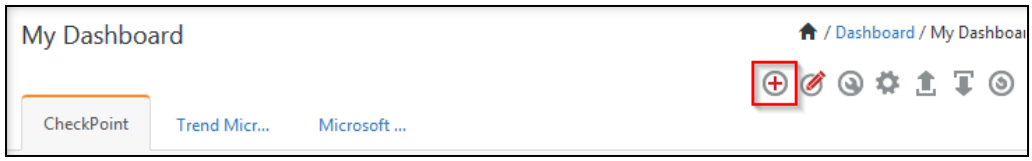
4. Select the **Select All** checkbox to select all the dashlet files and click **Import** to import the selected dashlet files.



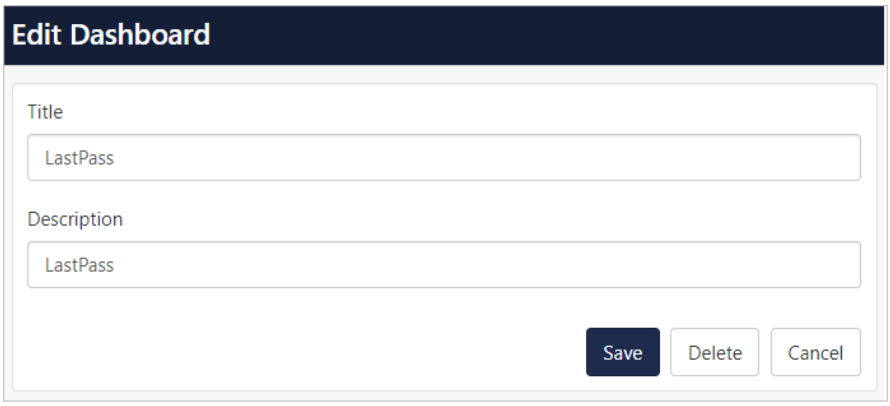

5. The Netsurion Open XDR platform displays the success message on successful import of the dashlet files.



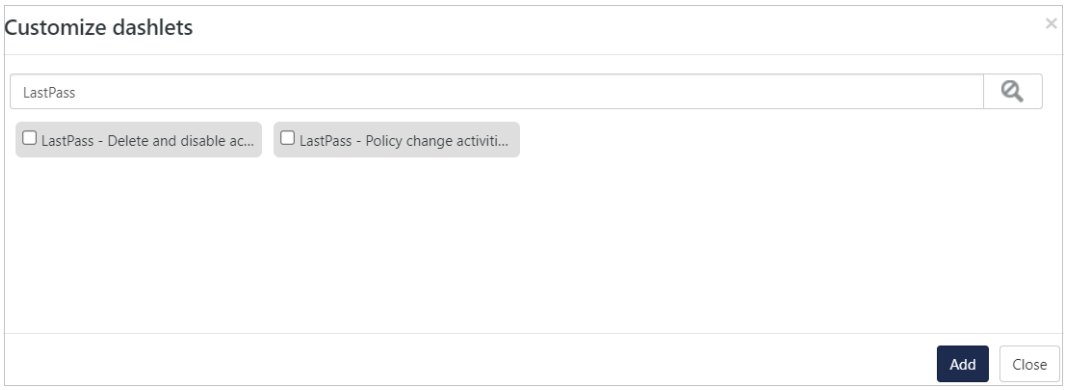

6. Then, in the **My Dashboard** interface click the **Add** ⊕ button to add dashboard.



7. In the **Add Dashboard** interface, specify the **Title** and **Description** and click **Save**.



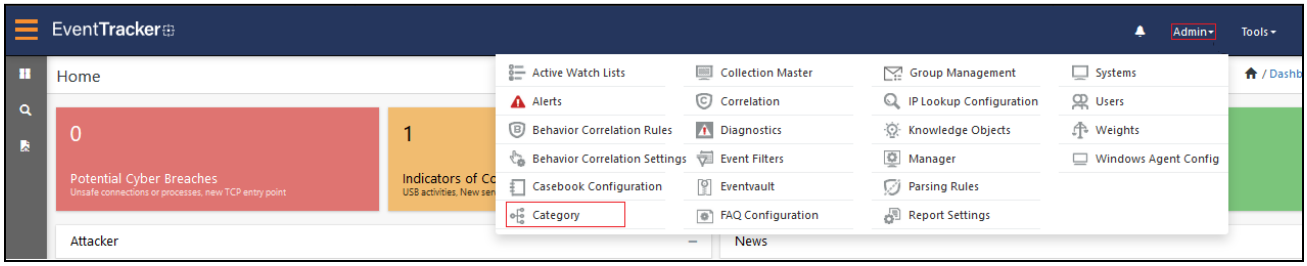

8. From the newly created dashboard interface (for example, **LastPass**), click the **Configuration** button to add the LastPass dashlets.
9. Search and select the newly imported dashlets and click **Add**.



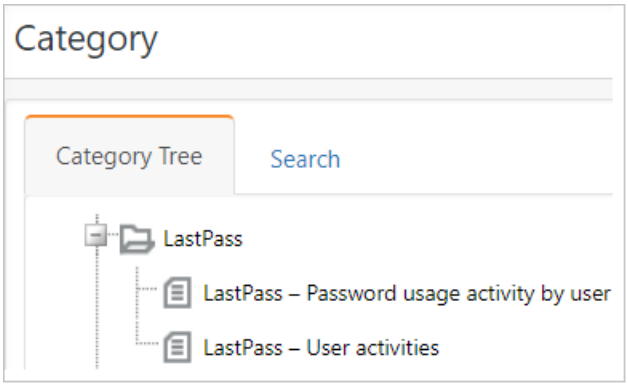
# 5 Verifying Data Source Integration in the Netsurion Open XDR platform

## 5.1 Category

1. In the **Netsurion Open XDR platform** web interface, hover over the **Admin** menu and click **Category**.

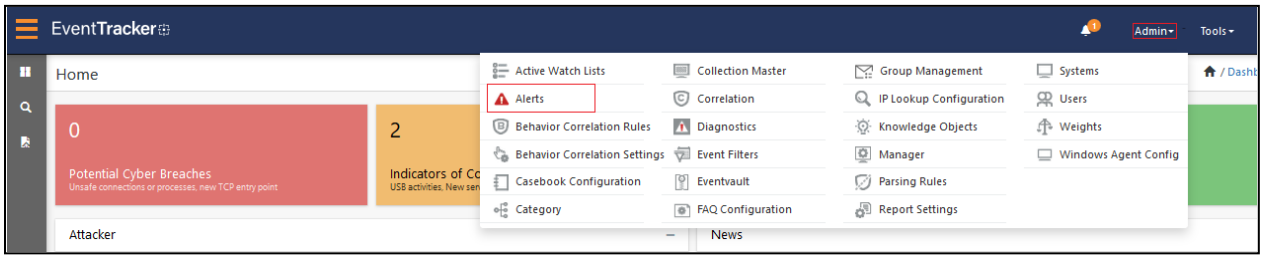



2. In the **Category** interface, under the **Category Tree** tab, click the **LastPass** group folder to expand and see the imported categories.



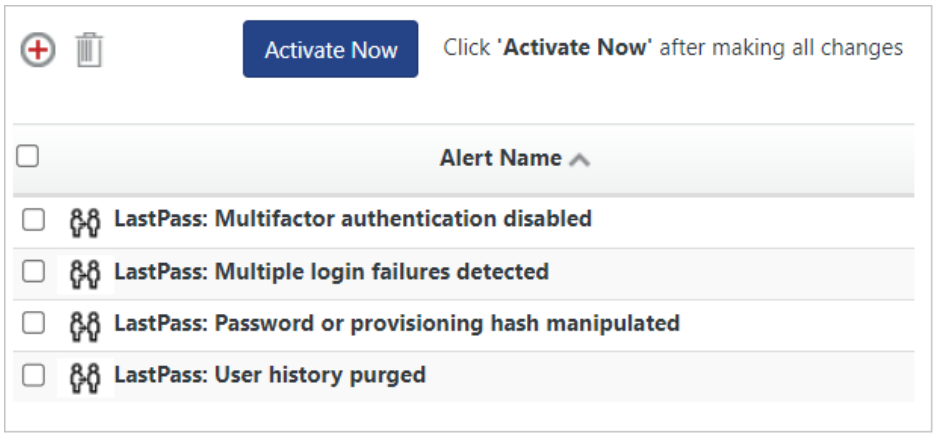

## 5.2 Alerts

1. In the **Netsurion Open XDR platform** web interface, hover over the **Admin** menu and click **Alerts**.

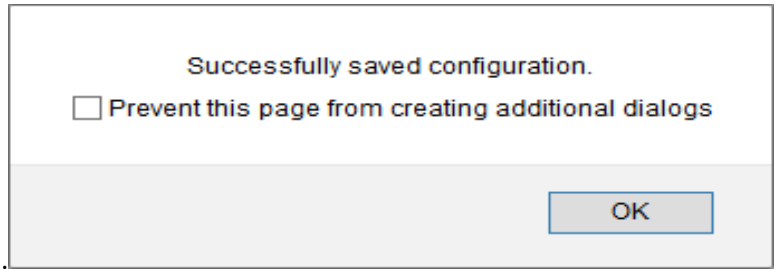



2. In the **Alerts** interface, type **LastPass** in the **Search** field and click the **Search** button.

3. The **Alerts** interface will display all the imported **LastPass** alerts.




4. To activate the imported alert, toggle the **Active** button, which is available next to the respective alert name.
5. The Netsurion Open XDR platform displays a success message on successfully configuring the alerts.




6. Click **OK** and click **Activate now** to activate the alerts after making the required changes.

**Note**

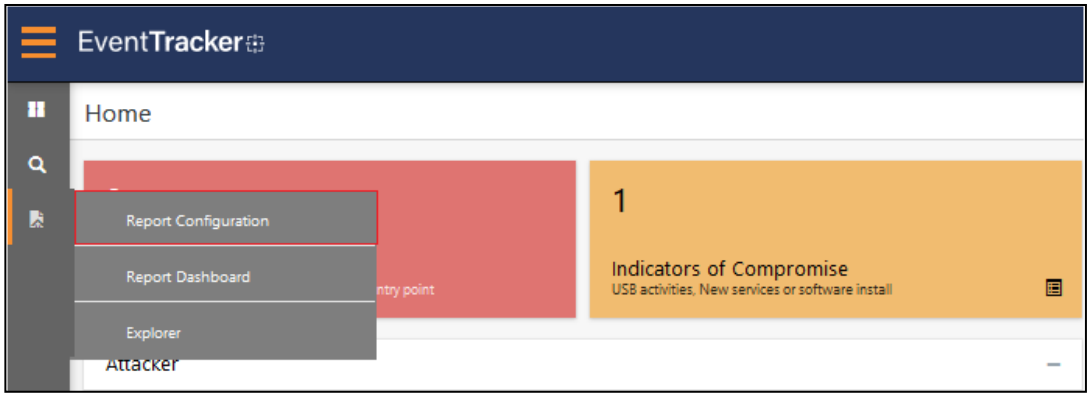
You can modify the required alert separately, and select the respective alert name check box, and then click **Activate Now** to save the alert modifications.

**Note**

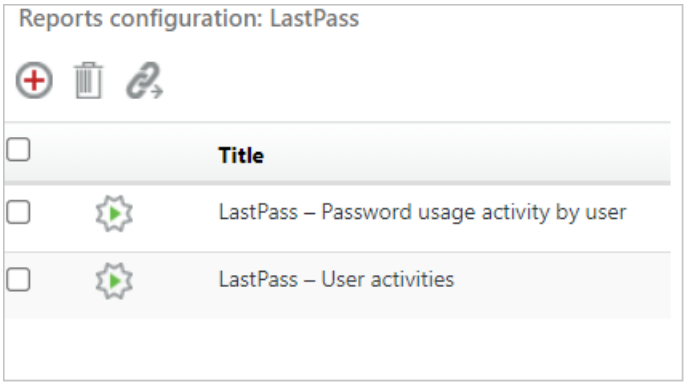
In the **Alert Configuration** interface, specify the appropriate **System** for better performance.

## 5.3 Reports

1. In the **Netsurion Open XDR platform** web interface, click the **Reports** menu, and then click **Report Configuration**.

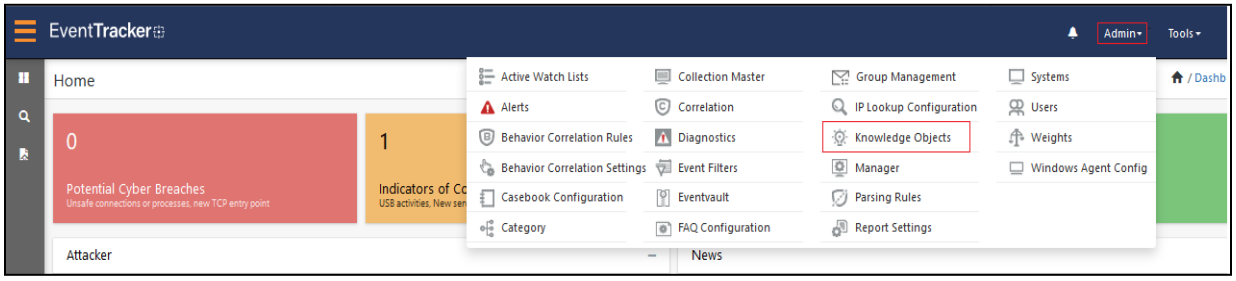



1. In the **Reports Configuration** interface, select the **Defined** option.
2. In the search field, type **LastPass** and click **Search** to search for the LastPass files.
3. The Netsurion Open XDR platform displays the reports for LastPass

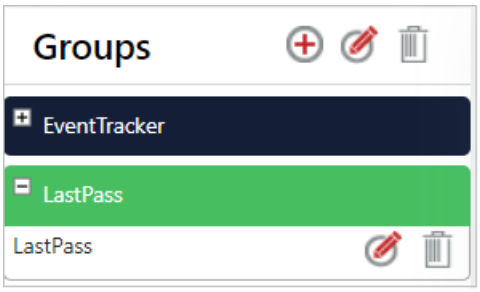



## 5.4 Knowledge Objects (KO)

1. In the **Netsurion Open XDR platform** web interface, hover over the **Admin** menu and click **Knowledge Objects.**



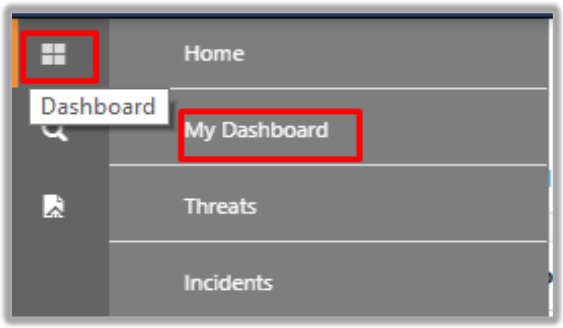

2. In the **Knowledge Object** interface, under **Groups** tree, click the **LastPass** group to expand and view the imported Knowledge objects.



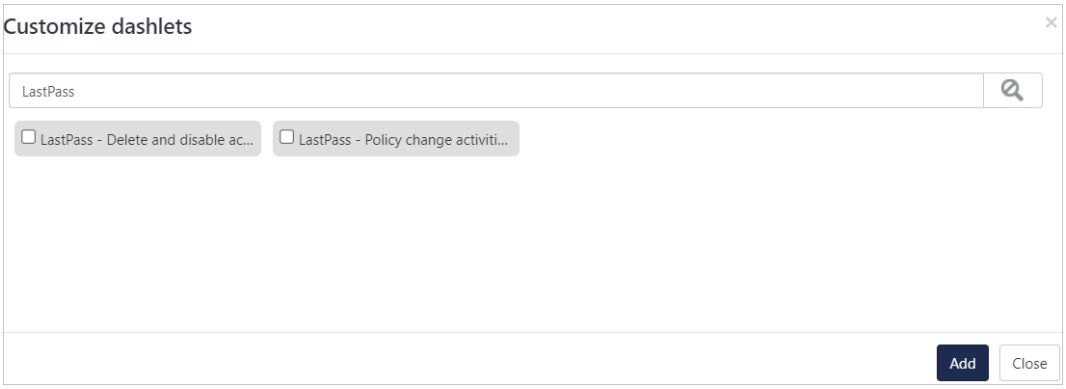

3. Click **Activate Now** to apply the imported Knowledge Objects.

## 5.5 Dashboard

1. In the **Netsurion Open XDR platform** web interface, go to **Home** > **My Dashboard**, and click the **Customize dashlets** button.




2. In the **Customize dashlets** interface, search for **LastPass** in the search field.
3. The following LastPass dashlet files will get displayed.



## About Netsurion

Netsurion® delivers an adaptive managed security solution that integrates our XDR platform with your existing security investments and technology stack, easily scaling to fit your business needs. Netsurion's managed offering includes our 24x7 SOC that operates as your trusted cybersecurity partner, working closely with your IT team to strengthen your cybersecurity posture. Our solution delivers Managed Threat Protection so you can confidently focus on your core business.

Headquartered in Ft. Lauderdale, FL with a global team of security analysts and engineers, Netsurion is a leader in Managed Detection and Response (MDR) and a Top 25 Global MSSP. Learn more at netsurion.com.

## Contact Us

### Corporate Headquarters

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

**Contact Numbers**

| | | |
|---|---|---|
| Direct Enterprise | SOC@Netsurion.com | 1 (877) 333-1433 Option 1, Option 1 |
| MSP Enterprise | SOC-MSP@Netsurion.com | 1 (877) 333-1433 Option 1, Option 2 |
| Essentials | Essentials-Support@Netsurion.com | 1 (877) 333-1433 Option 1, Option 3 |
| Self-Serve | EventTracker-Support@Netsurion.com | 1 (877) 333-1433 Option 1, Option 4 |

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