

Integration Guide

Integrating Bitwarden Password Manager with EventTracker

Publication Date:

December 21, 2021

Abstract

This guide provides instructions to retrieve the **Bitwarden Password Manager** events via integration. Once the logs start coming into EventTracker, the reports, alerts, and categories can be configured.

Scope

The configuration details in this guide are consistent with EventTracker version 9.3 or above and **Bitwarden Password Manager** (Classic 2019 Enterprise Organizations, Enterprise Organizations, and Teams Organizations on-Premises and Cloud).

Audience

Administrators who are assigned the task to monitor the **Bitwarden Password Manager** events using EventTracker.

Table of Contents

| | |
|---|----|
| Table of Contents | 3 |
| 1. Overview | 4 |
| 2. Prerequisites..... | 4 |
| 3. Configuring Bitwarden Password Manager to Forward Logs to EventTracker | 4 |
| 3.1 Getting API details from Bitwarden PM console..... | 4 |
| 3.2 Integrating Bitwarden Password Manager with EventTracker..... | 5 |
| 4. EventTracker Knowledge Packs | 7 |
| 4.1 Categories..... | 7 |
| 4.2 Alerts..... | 7 |
| 4.3 Reports | 7 |
| 4.4 Dashboards..... | 9 |
| 5. Importing Bitwarden Password Manager Knowledge Pack into EventTracker..... | 15 |
| 5.1 Categories..... | 15 |
| 5.2 Alerts..... | 16 |
| 5.3 Knowledge Objects..... | 17 |
| 5.4 Reports | 18 |
| 5.5 Dashboards..... | 19 |
| 6. Verifying Bitwarden Password Manager Knowledge Pack in EventTracker | 22 |
| 6.1 Categories..... | 22 |
| 6.2 Alerts..... | 22 |
| 6.3 Knowledge Objects..... | 23 |
| 6.4 Reports | 24 |
| 6.5 Dashboards..... | 25 |
| About Netsurion | 26 |
| Contact Us..... | 26 |

1. Overview

Bitwarden is a free and open-source password management service that stores sensitive information such as website credentials in an encrypted vault. Bitwarden offers a cloud-hosted service as well as the ability to deploy the solution on-premises.

EventTracker helps to monitor events from the Bitwarden Password Manager. Its dashboard and reports will help you to monitor cipher and user events that occur within the organization.

2. Prerequisites

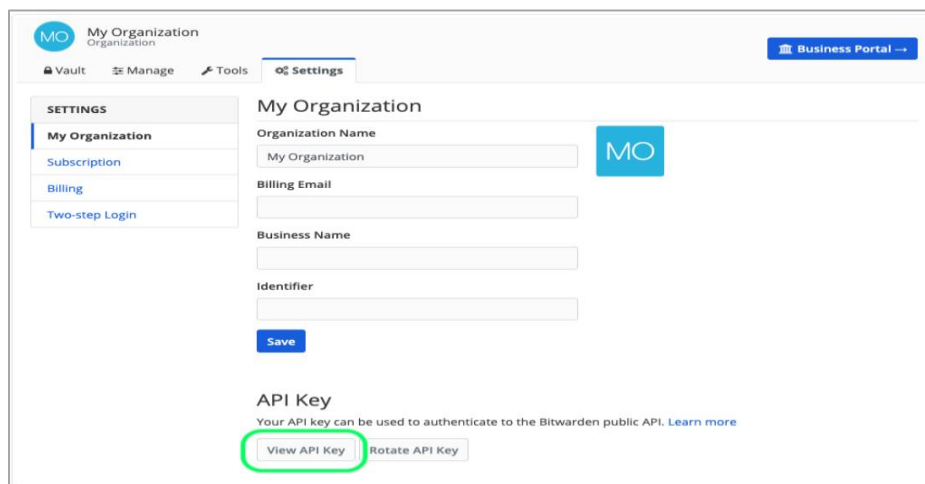
- **EventTracker v9.3 or above** should be installed.
- A user with administrator access for the Bitwarden Password Manager.
- Port should be allowed in the firewall.

3. Configuring Bitwarden Password Manager to Forward Logs to EventTracker

The Bitwarden Password Manager is combined with EventTracker by the Integrator based on the API Integration to forward logs to the EventTracker Manager.

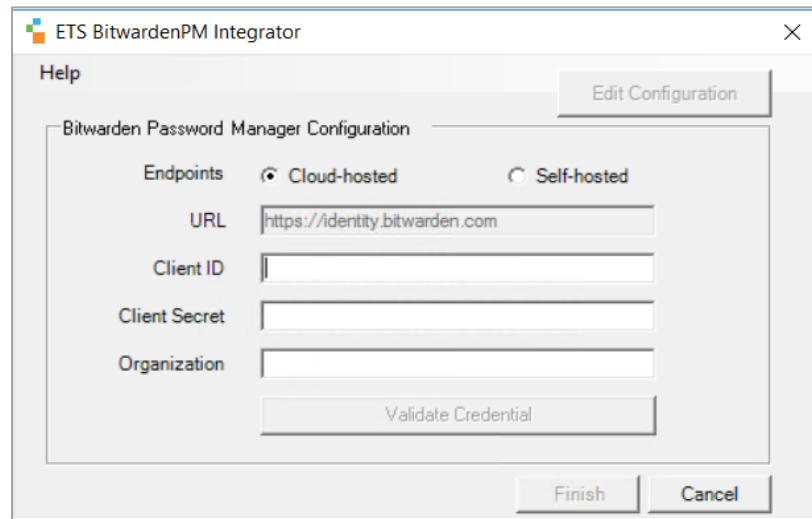
3.1 Getting API details from Bitwarden PM console

1. Login to the Bitwarden PM console.
2. Go to the **Settings** tab > **My Organization**.
3. Click the **View API Key** and copy the below details
 - client_ID
 - client_secret

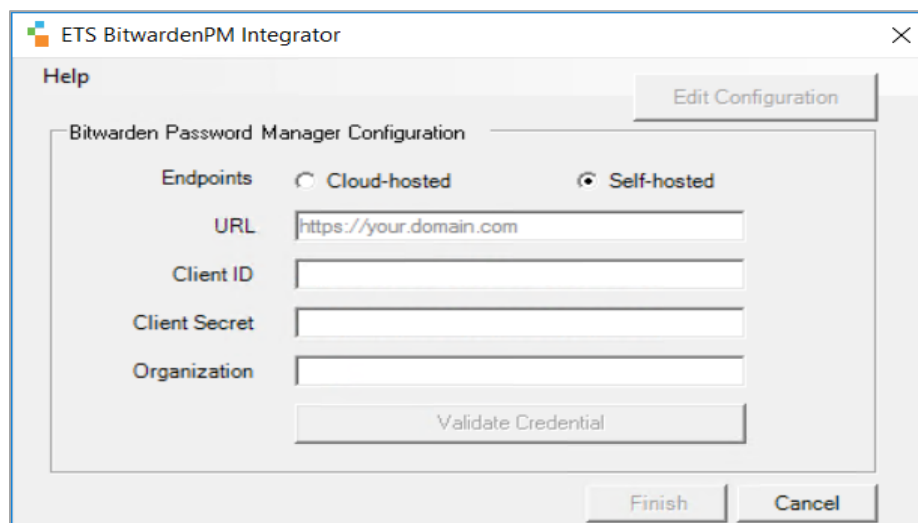


3.2 Integrating Bitwarden Password Manager with EventTracker

1. Download the Bitwarden Password Manager integrator package on the EventTracker Agent machine from the following link:
<https://www.netsurion.com/knowledge-packs/bitwarden-password-manager>
2. Run the downloaded **ETS_BitwardenPM_Integrator.exe** file.
The **ETS Bitwarden Integration** window opens.
3. To check the Integrator version, go to **Help > About**. Make sure you are using the latest version of Integrator.

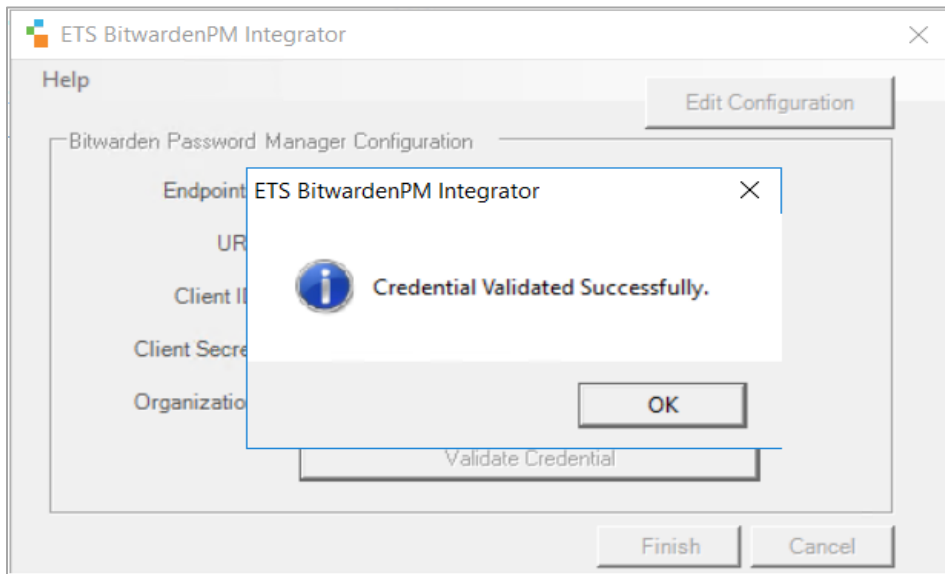


4. Select the hosted service type:
 - Cloud-hosted (**Default** selected)
 - Self-hosted (on-premises)
5. For the Self-hosted type, enter the Bitwarden PM URL (<https://your.domain.com>).

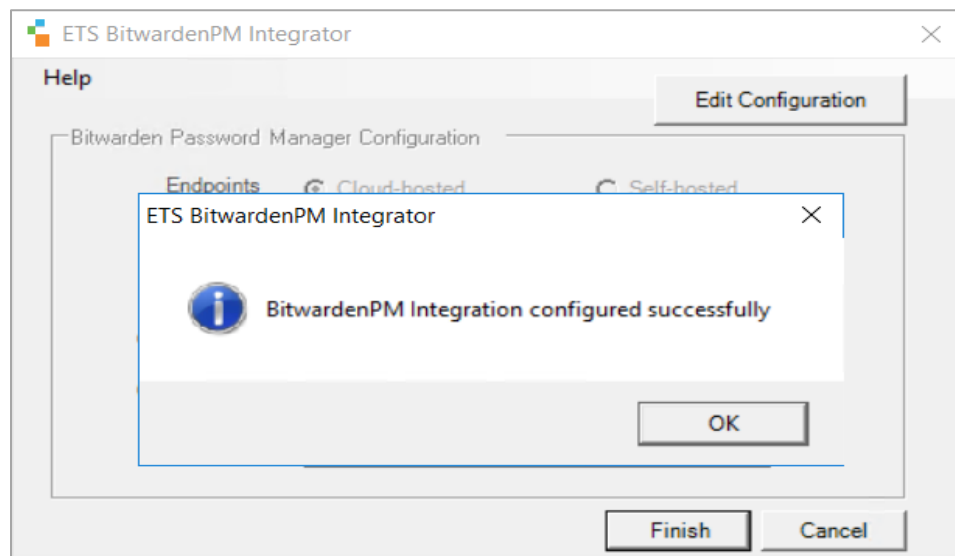


6. Provide the **Client ID**, **Client Secret** saved from the Bitwarden PM console.

7. Provide the **Organization** name displayed under the EventTracker Manager.
8. Click **Validate Credential**.
A message window will pop up stating **Credentials Validated Successfully**.
9. Click **OK**.



10. Click **Finish** to complete the integration.



4. EventTracker Knowledge Packs

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

The following Knowledge Packs (KPs) are available in EventTracker to support the Bitwarden Password Manager.

4.1 Categories

- **Bitwarden PM: Cipher Events** - This category will allow users to search events specific to the cipher-related events performed in the Bitwarden Password Manager.
- **Bitwarden PM: Group and Collection Events**- This category will allow users to search groups and collect management activities performed in the Bitwarden Password Manager.
- **Bitwarden PM: Organization Events**- This category will allow users to search the organization management activities performed in the Bitwarden Password Manager.
- **Bitwarden PM: Provider User and Organization Events**- This category will allow users to search the events related to the provider user and provider organization management performed in the Bitwarden Password Manager. Providers are administration entities in Bitwarden that allow the Managed Service Providers (MSPs) and Resellers to create and fully manage the multiple client organizations on behalf of the individual business customers.
- **Bitwarden PM: User Events**- This category will allow searching activities performed by the users to manage their Bitwarden Password Manager account.

4.2 Alerts

- **Bitwarden PM: Login Failed** - This alert will be triggered when the user login failure is detected in the Bitwarden Password Manager.
- **Bitwarden PM: MFA Disabled** - This alert will be triggered when the user disables the Two-Step Login in the Bitwarden Password Manager.
- **Bitwarden PM: Policy Updated**- This alert will be triggered when the organization policy is updated in the Bitwarden Password Manager.

4.3 Reports

- **Bitwarden PM - User Login Failure Report:** This report provides a detailed summary of the user login failure events detected. It contains a user IP address, username, user email, device type, and more.

| UserID | User | Email | Event Name | IP Address | User Type | Device Type |
|--------------------------------------|------------|-----------------------|------------------|---------------|-----------|-------------|
| 4c1681bf-2b47-4901-a598-ad8d014690a9 | Jim | jim45@contoso.edu | User_FailedLogin | 10.103.75.190 | User | iOS |
| 81d0de2b-35e9-45dd-a93c-ad94011a2f72 | Mark Robie | MarkRobie@contoso.edu | User_FailedLogin | 110.25.148.38 | Owner | Chrome |
| 81d0de2b-35e9-45dd-a93c-ad94011a2f72 | Mark Robie | MarkRobie@contoso.edu | User_FailedLogin | 110.25.151.2 | Owner | Chrome |

- **Bitwarden PM – User Login Success Report:** This report provides a detailed summary of the user login success events. It contains a user IP address, username, user email, device type, and more.

| User | UserID | Email | IP Address | User Type | Device Type |
|------------|--------------------------------------|-----------------------|---------------|-----------|------------------|
| Mark Robie | 4c1681bf-2b47-4901-a598-ad8d014690a9 | jim45@contoso.edu | 10.113.75.190 | User | Chrome Extension |
| Mark Robie | 4c1681bf-2b47-4901-a598-ad8d014690a9 | MarkRobie@Contoso.edu | 10.113.75.190 | User | iOS |
| Jim | 08b3530d-e4e2-49c4-be3c-ad920131bfa2 | jim45@contoso.edu | 110.25.150.25 | Owner | Chrome |

- **Bitwarden PM – Cipher Events Report:** This report provides a detailed summary of the Cipher events. It contains a Cipher ID, the user who triggered the event, user email, device type, event name, and more.

| UserID | Email | Event Name | IP Address | Item ID | User | Device Type | User Type |
|--------------------------------------|--------------------|-------------------------------------|---------------|--------------------------------------|------|------------------|-----------|
| 4c1681bf-2b47-4901-a598-ad8d014690a9 | jim454@contoso.edu | Cipher_ClientViewed | 114.25.151.13 | 7d4811c4-9492-4738-83ee-ad8d01483329 | Jim | Chrome Extension | User |
| 4c1681bf-2b47-4901-a598-ad8d014690a9 | jim454@contoso.edu | Cipher_ClientAutofilled | 114.25.151.13 | 7d4811c4-9492-4738-83ee-ad8d01483329 | Jim | Chrome Extension | User |
| 4c1681bf-2b47-4901-a598-ad8d014690a9 | jim454@contoso.edu | Cipher_ClientToggledPasswordVisible | 114.25.151.13 | 0647f163-c39b-459b-9e4b-adba011095c3 | Jim | Chrome Extension | User |

- **Bitwarden PM - Group and Collection Management Report:** This report provides a detailed summary of the group and collection management events. It contains an event name, group ID/collection ID, a user who triggered the event, and more.

| UserID | Collection ID | Email | Event Name | IP Address | User | Device Type | User Type |
|--------------------------------------|--------------------------------------|-------------------|--------------------|---------------|------|-------------|-----------|
| 08b3530d-e4e2-49c4-be3c-ad920131bfa2 | c98dd2ca-6648-411c-8a34-ad92013247a5 | jim45@contoso.edu | Collection_Deleted | 114.25.150.25 | Jim | Chrome | Owner |
| 08b3530d-e4e2-49c4-be3c-ad920131bfa2 | dcd9ca9e-e05d-4038-a850-ad9400ca983 | jim45@contoso.edu | Collection_Created | 114.25.150.25 | Jim | Chrome | Owner |
| 08b3530d-e4e2-49c4-be3c-ad920131bfa2 | | jim45@contoso.edu | Group_Created | 114.25.150.25 | Jim | Chrome | Owner |

- **Bitwarden PM – User Events Report:** This report provides a detailed summary of events performed by users to manage their accounts. It contains an event type, username, user email, device type, and more.

| UserID | Email | Event Name | IP Address | User | Device Type | User Type |
|--------------------------------------|-------------------|-------------------------|---------------|------|-------------|-----------|
| 08b3530d-e4e2-49c4-be3c-ad920131bfa2 | jim45@contoso.edu | User_ChangedPassword | 10.25.150.25 | Jim | Chrome | Owner |
| 08b3530d-e4e2-49c4-be3c-ad920131bfa2 | jim45@contoso.edu | User_Updated/Enabled2fa | 75.10.202.158 | Jim | Chrome | Owner |
| 08b3530d-e4e2-49c4-be3c-ad920131bfa2 | jim45@contoso.edu | User_ChangedPassword | 10.25.150.25 | Jim | Chrome | Owner |

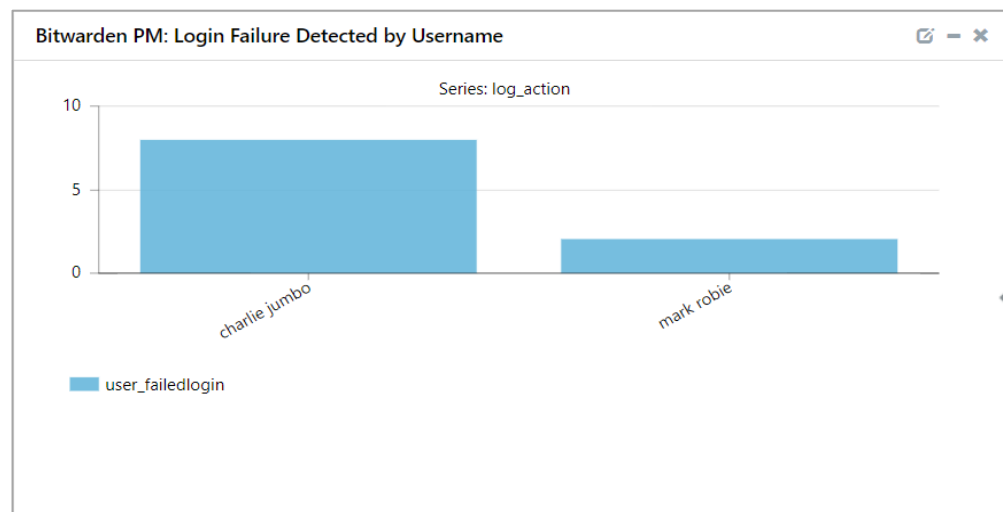
- **Bitwarden PM – Organization Events Report:** This report provides a detailed summary of the organization’s management events. It contains an event type, username, user email, device type, and more.

| UserID | Email | Event Name | IP Address | User | User Type |
|--------------------------------------|-------------------|--------------------------|--------------|------|-----------|
| 08b3530d-e4e2-49c4-be3c-ad920131bfa2 | jim45@contoso.edu | OrganizationUser_Updated | | Jim | Owner |
| 08b3530d-e4e2-49c4-be3c-ad920131bfa2 | jim45@contoso.edu | Organization_Updated | 10.25.148.38 | Jim | Owner |
| 08b3530d-e4e2-49c4-be3c-ad920131bfa2 | jim45@contoso.edu | OrganizationUser_Removed | | Jim | Owner |

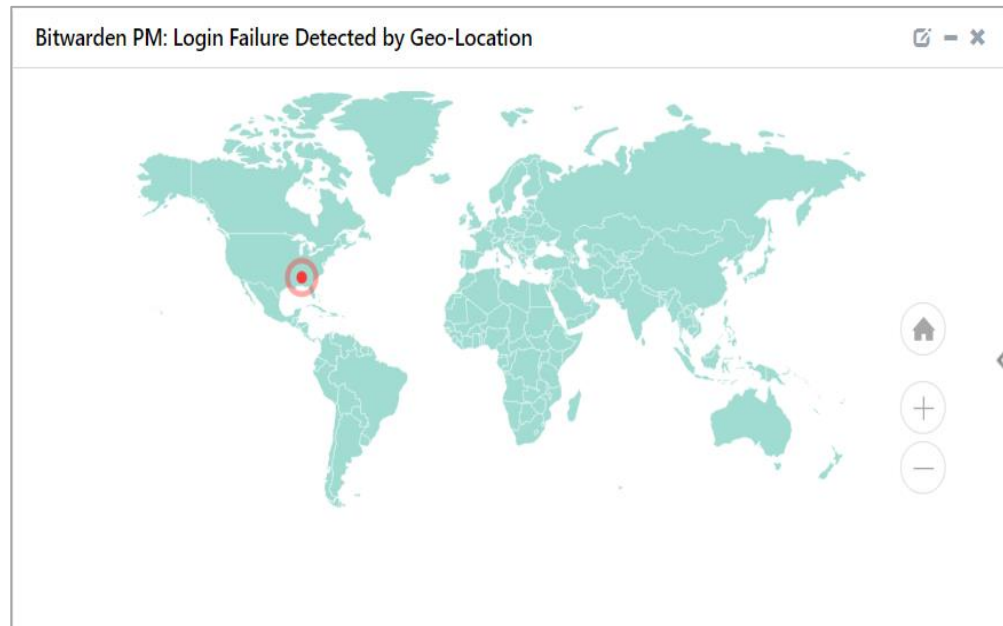
- **Bitwarden PM – Provider User and Organization Events Report:** This report provides a detailed summary of the provider users and provider organization’s management events. It contains an event type, username, user email, device type, and more.

4.4 Dashboards

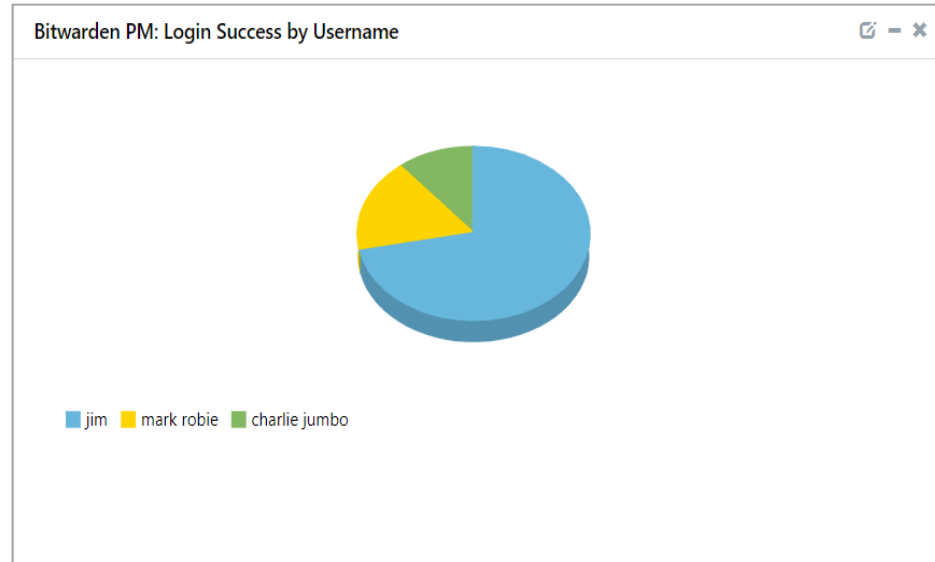
- Bitwarden PM: Login Failure Detected by the Username



- Bitwarden PM: Login Failure Detected by the Geo-Location



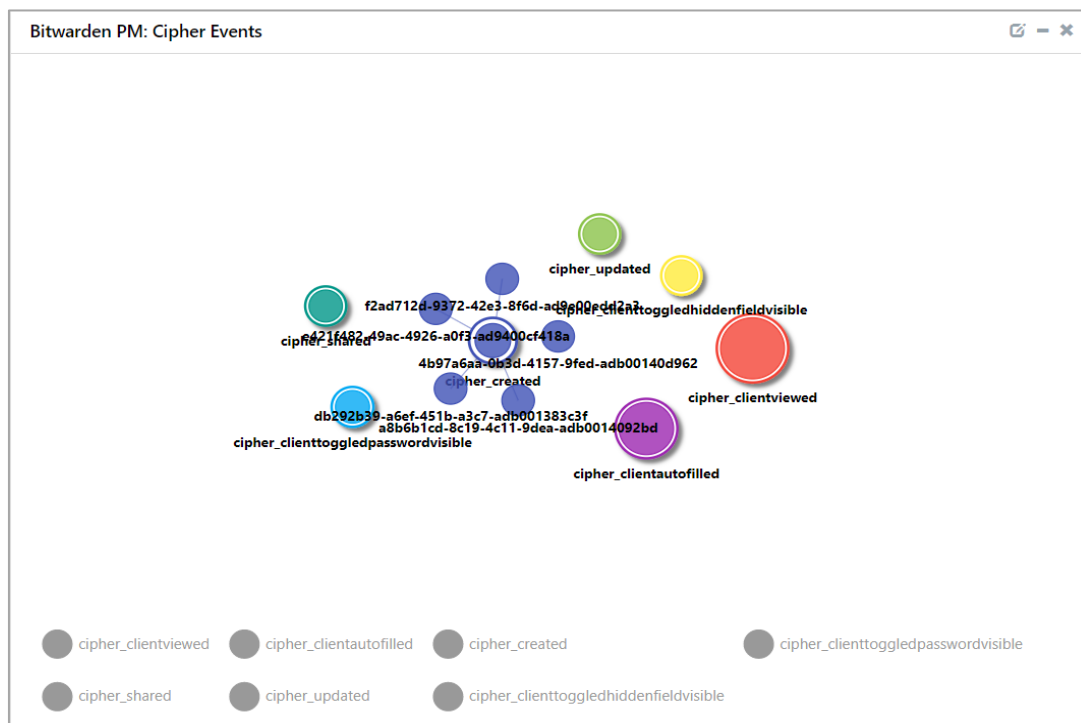
- Bitwarden PM: Login Success by the Username



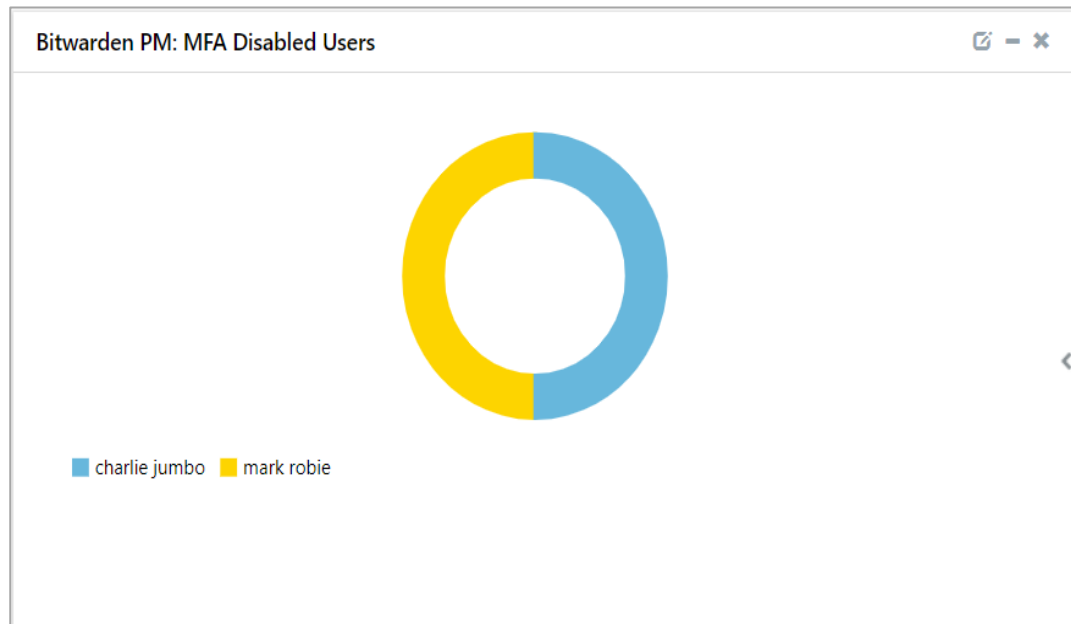
- Bitwarden PM: Login Success by Geo-Location



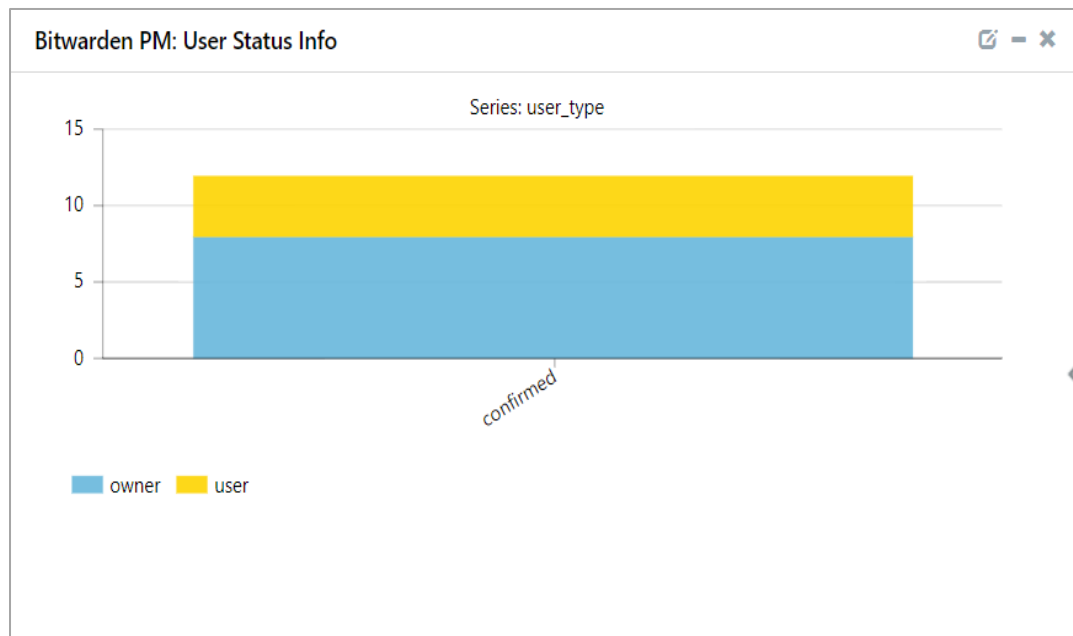
- Bitwarden PM: Cipher Events



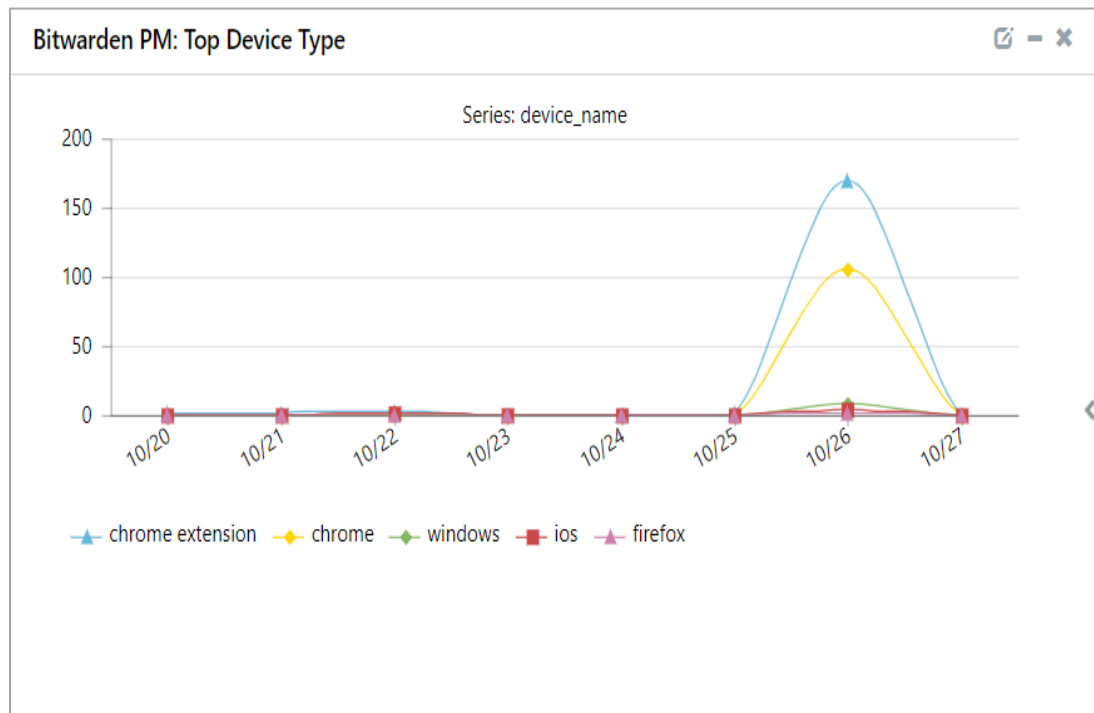
- Bitwarden PM: MFA Disabled Users



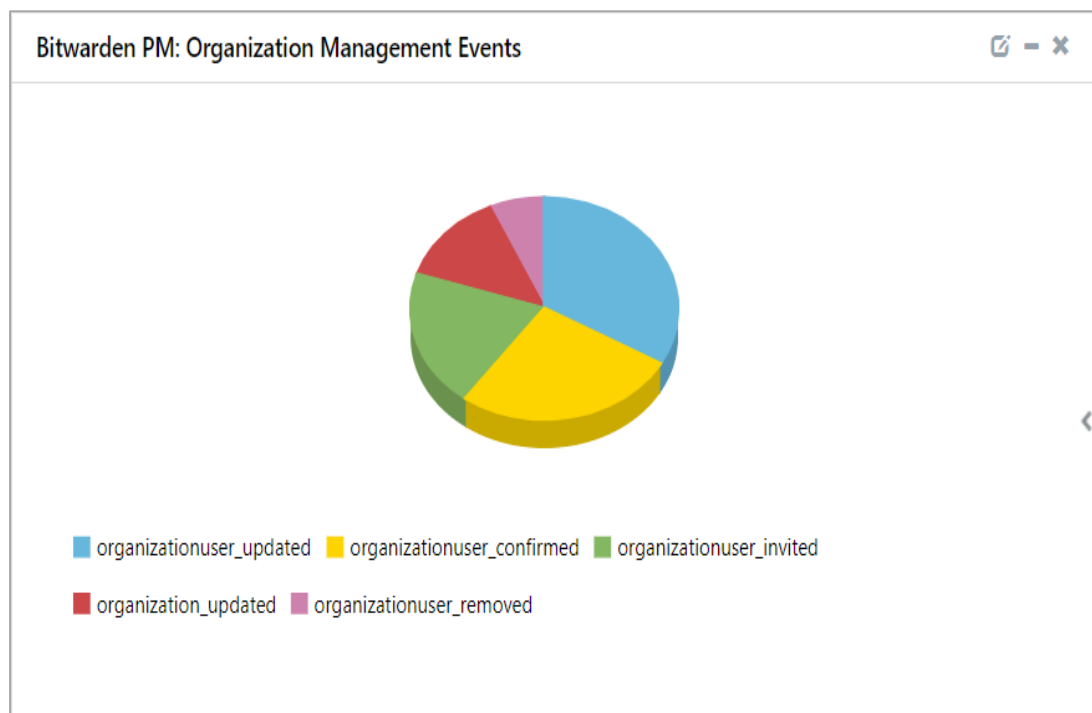
- Bitwarden PM: User Status Information



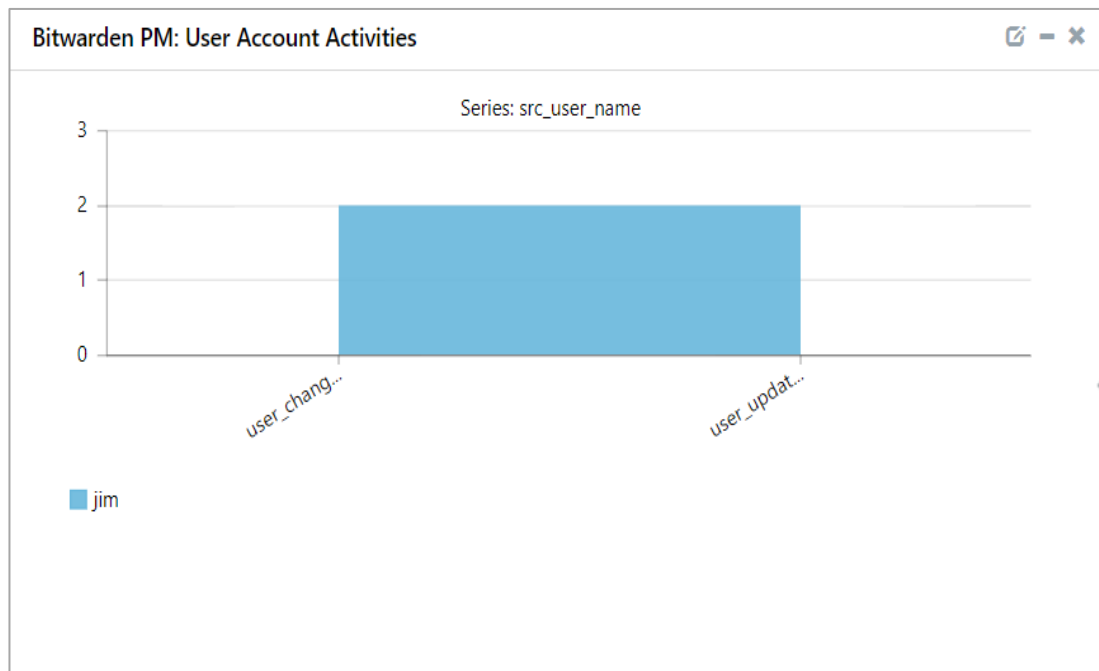
- Bitwarden PM: Top Device Type



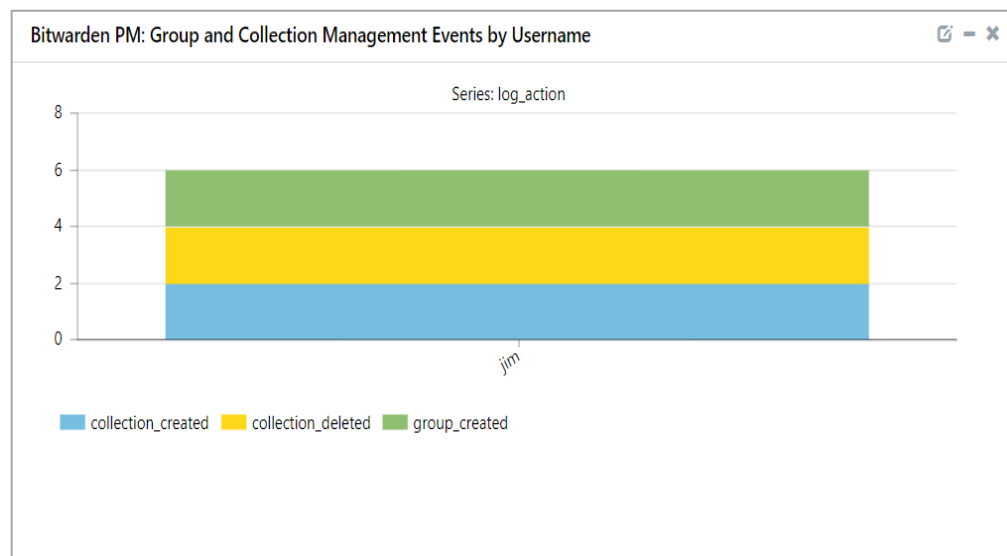
- Bitwarden PM: Organization Management Events



- Bitwarden PM: User Account Activities

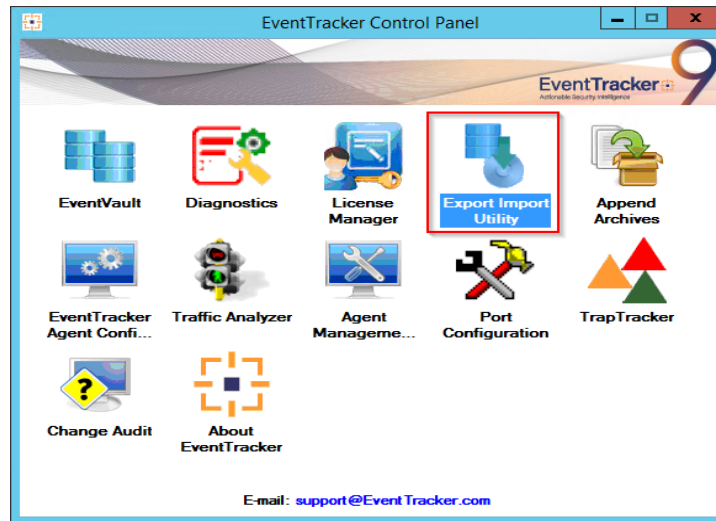


- Bitwarden PM: Group and Collection Management Events by the Username



5. Importing Bitwarden Password Manager Knowledge Pack into EventTracker

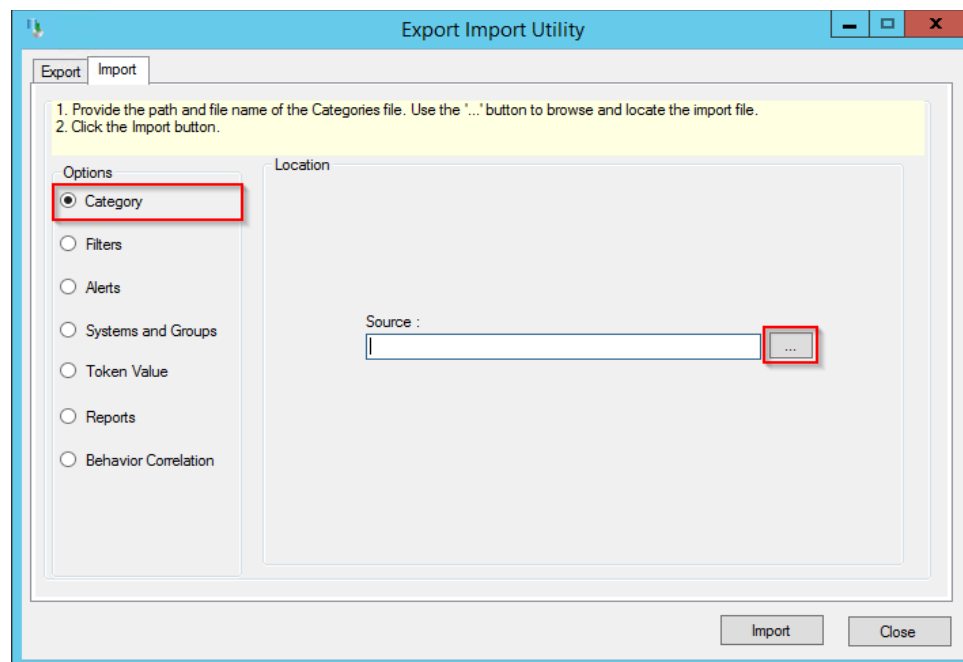
1. Launch the **EventTracker Control Panel**.
2. Double click **Export Import Utility**.



3. Click the **Import** tab.

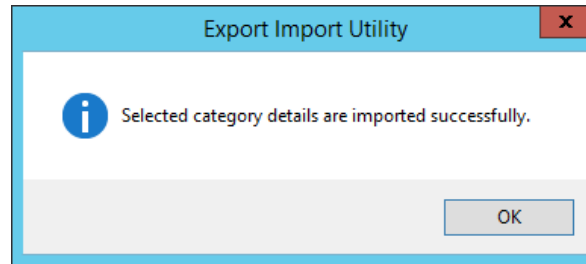
5.1 Categories

1. Click the **Category** option, and then click the Browse button.



2. Locate the **Categories_Bitwarden PM.iscat** file, and then click the **Open** button.
3. To import the categories, click the **Import** button.

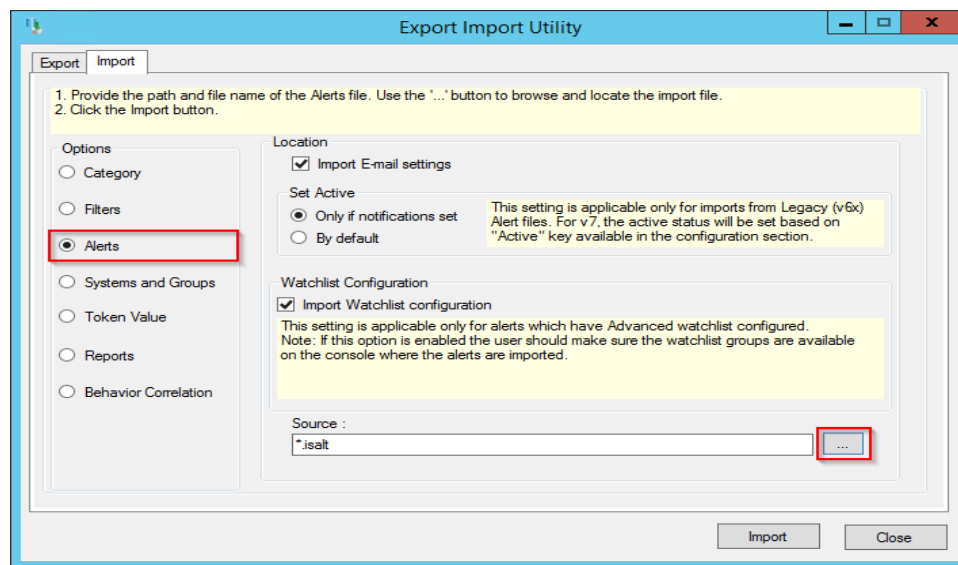
EventTracker displays a success message.



4. Click **OK**, and then click the **Close** button.

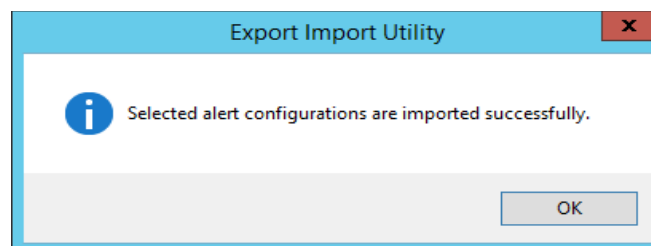
5.2 Alerts

1. Click the **Alert** option, and then click the **Browse** button.



2. Locate the **Alerts_Bitwarden PM.isalt** file, and then click the **Open** button.
3. To import the alerts, click the **Import** button.

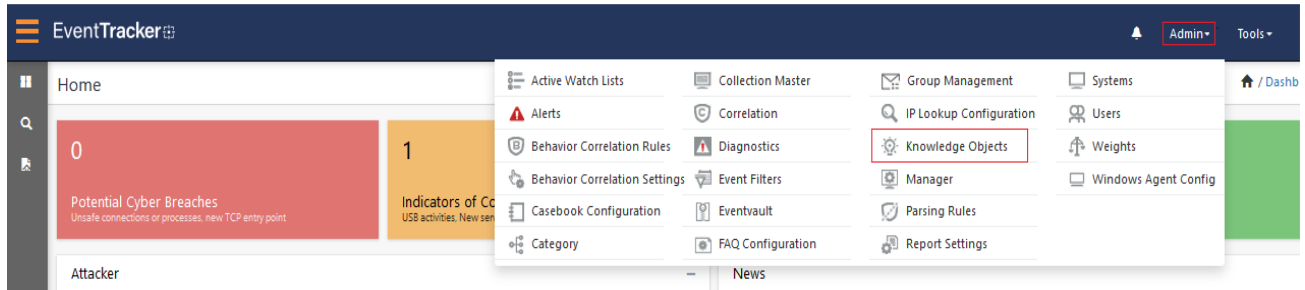
EventTracker displays a success message.



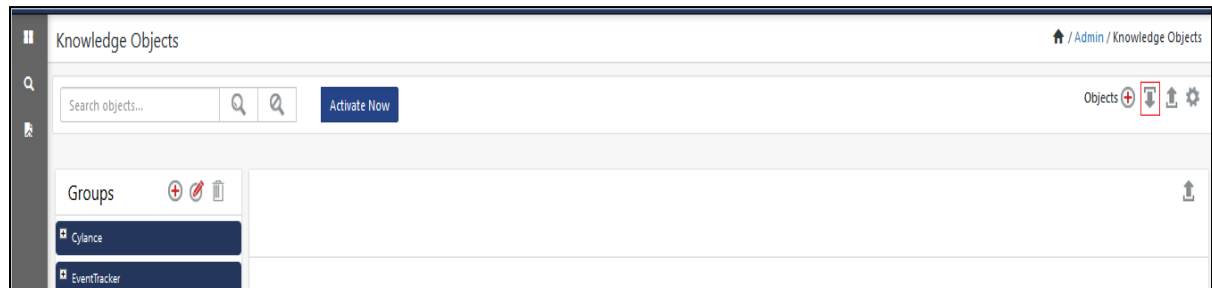
- Click the **OK** button, and then click the **Close** button.

5.3 Knowledge Objects

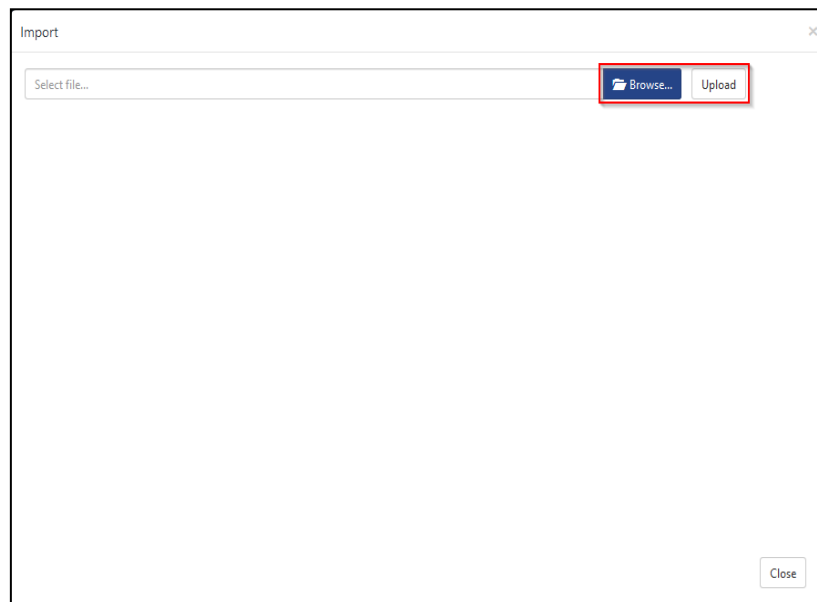
- Click the **Knowledge Objects** under the **Admin** option on the EventTracker Manager page.




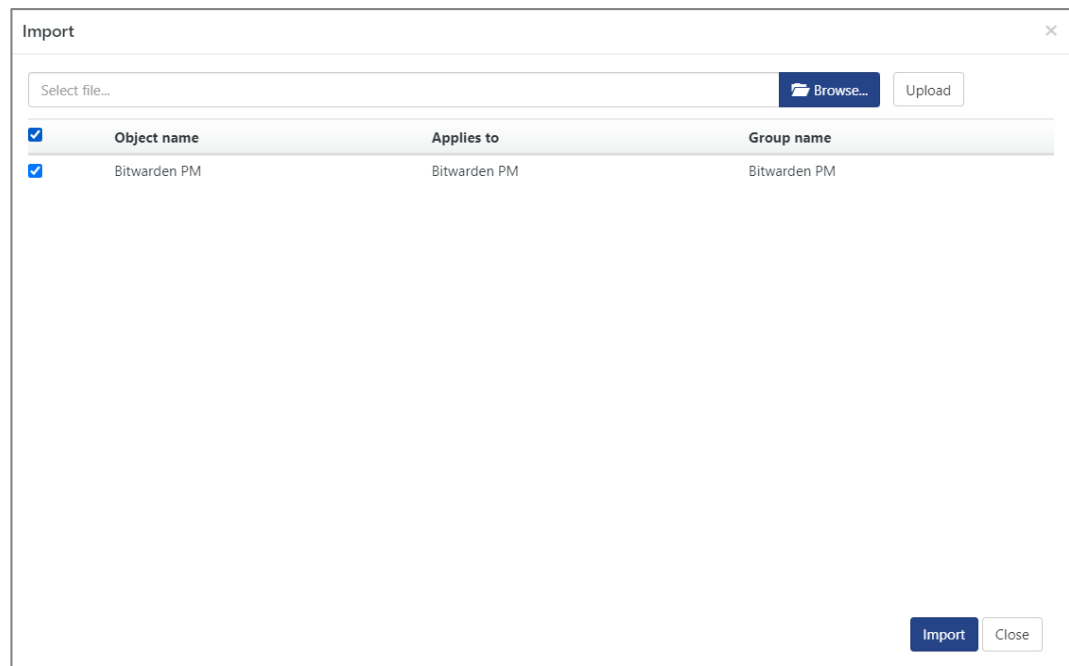
- Click the **Import** button as highlighted in the below image:



- Click the **Browse** button.



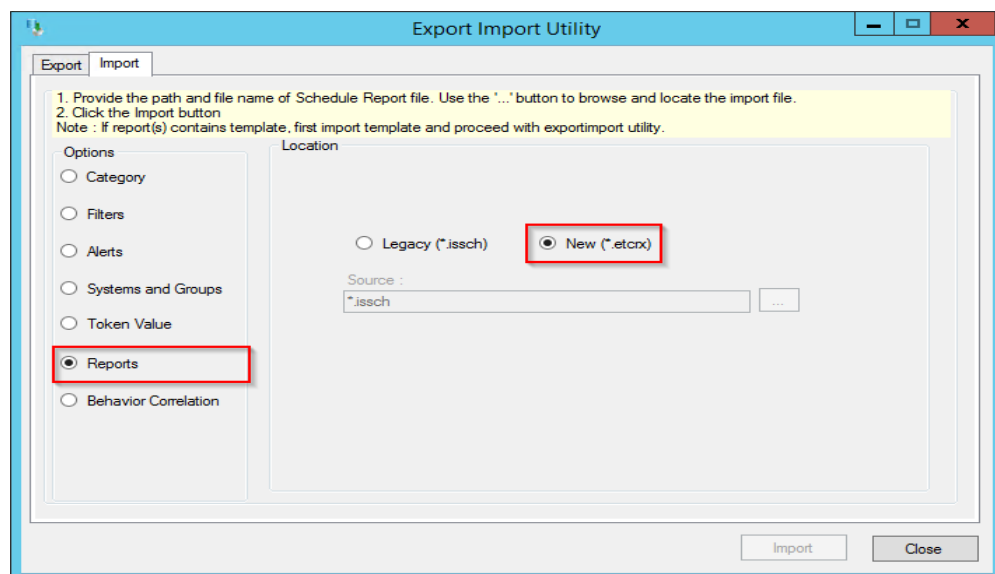
4. Locate the file named **KO_Bitwarden PM.etko**.
5. Select the check box and then click the  **Import** option.



6. Knowledge Objects (KO) are now imported successfully.

5.4 Reports

1. Click the **Reports** option and select the **New (*.etcrx)** option.



2. Locate the file named **Reports_Bitwarden PM.etcrx** and select all the check boxes.

Reports Import

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

Select file

Available reports

Title Frequency Show all

| <input checked="" type="checkbox"/> | Title | Sites | Groups | Systems | Frequency |
|--|--|-----------------|--------|---------|-----------|
| <input checked="" type="checkbox"/> EDIT | Bitwarden PM - Cipher Events Report | WIN-MCKKRLN6K0I | | | Undefined |
| <input checked="" type="checkbox"/> EDIT | Bitwarden PM - Group and Collection ... | WIN-MCKKRLN6K0I | | | Undefined |
| <input checked="" type="checkbox"/> EDIT | Bitwarden PM - Organization Events R... | WIN-MCKKRLN6K0I | | | Undefined |
| <input checked="" type="checkbox"/> EDIT | Bitwarden PM - Provider User and Org... | WIN-MCKKRLN6K0I | | | Undefined |
| <input checked="" type="checkbox"/> EDIT | Bitwarden PM - User Events Reports | WIN-MCKKRLN6K0I | | | Undefined |
| <input checked="" type="checkbox"/> EDIT | Bitwarden PM - User Login Failure Rep... | WIN-MCKKRLN6K0I | | | Undefined |
| <input checked="" type="checkbox"/> EDIT | Bitwarden PM - User Login Success R... | WIN-MCKKRLN6K0I | | | Undefined |

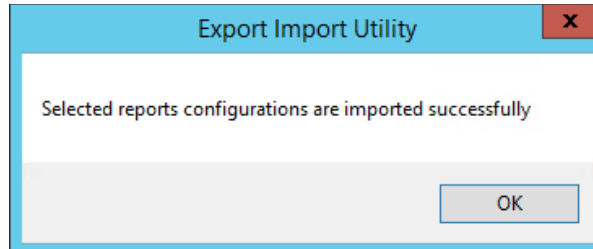
Note: Set run time option is not applicable for Defined Reports and Hourly Reports

Set run time for report(s) from AM at interval of minutes

Replace to

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

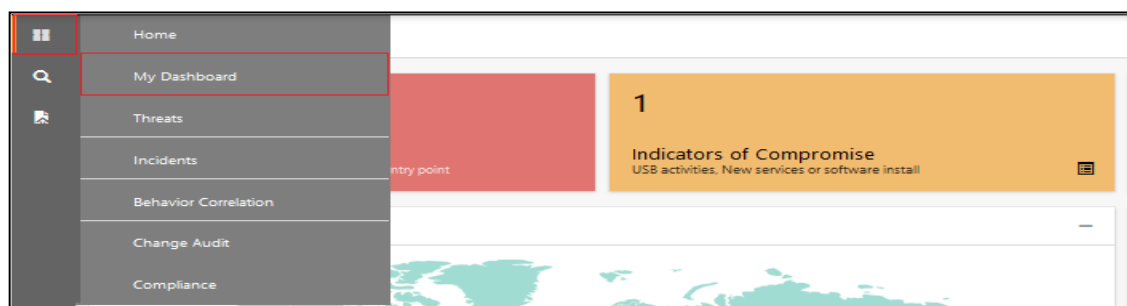
- Click the **Import**  button to import the report. EventTracker displays a success message.




5.5 Dashboards

NOTE: Below steps given are specific to EventTracker9 and later.

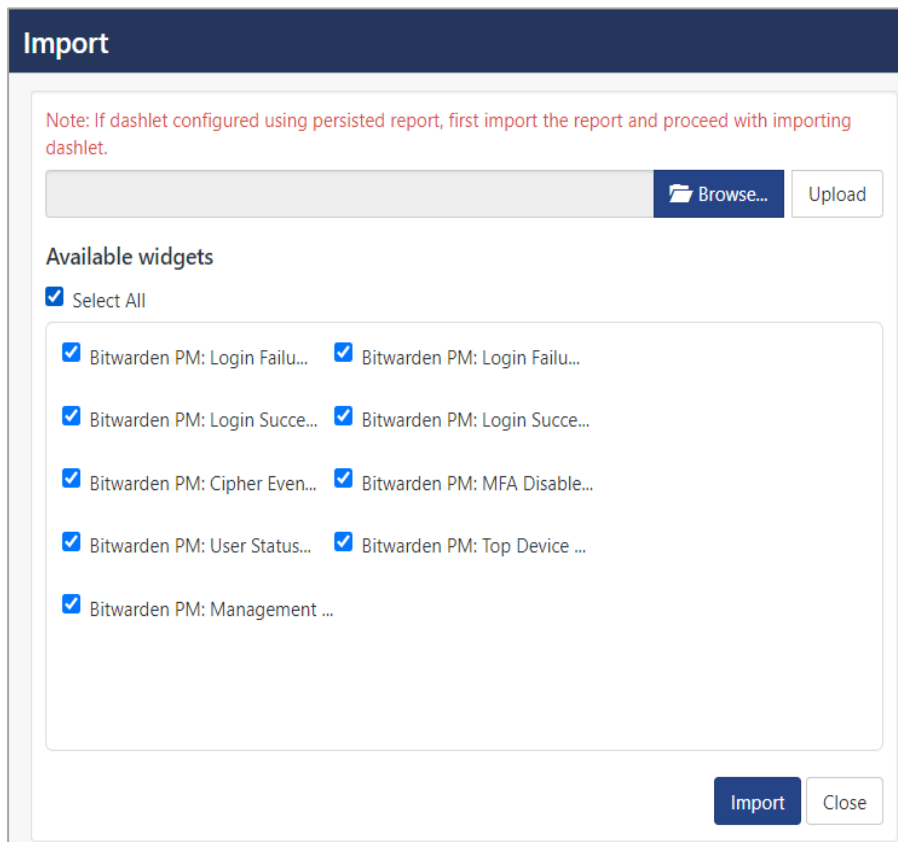
- Open the **EventTracker** in a browser and log on.



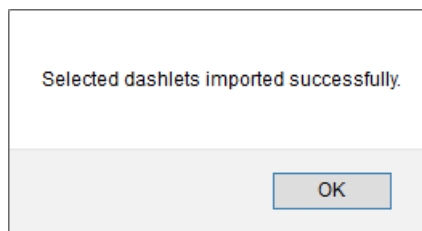
2. Navigate to the **My Dashboard** option as shown above.
3. Click the **Import**  button as shown below.




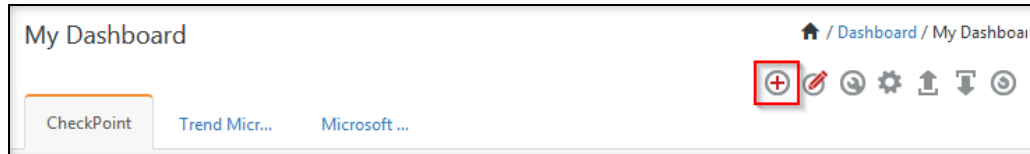
4. Import the dashboard file **Dashboards_Bitwarden PM.etwd** and select the **Select All** checkbox.
5. Click the **Import** as shown below.



Import is now completed successfully.



6. In the **My Dashboard** page select  to add the dashboard.




7. Choose the appropriate name for the **Title** and **Description**. Click **Save**.

Add Dashboard

Title

Description

8. In the **My Dashboard** page select  to add dashlets.
9. Select the imported dashlets and click **Add**.

Customize dashlets

☒ Bitwarden PM: Cipher Events

☒ Bitwarden PM: Login Failure Det...

☒ Bitwarden PM: Login Failure Det...

☒ Bitwarden PM: Login Success by...

☒ Bitwarden PM: Login Success by...

☒ Bitwarden PM: Management Ev...

☒ Bitwarden PM: MFA Disabled Us...

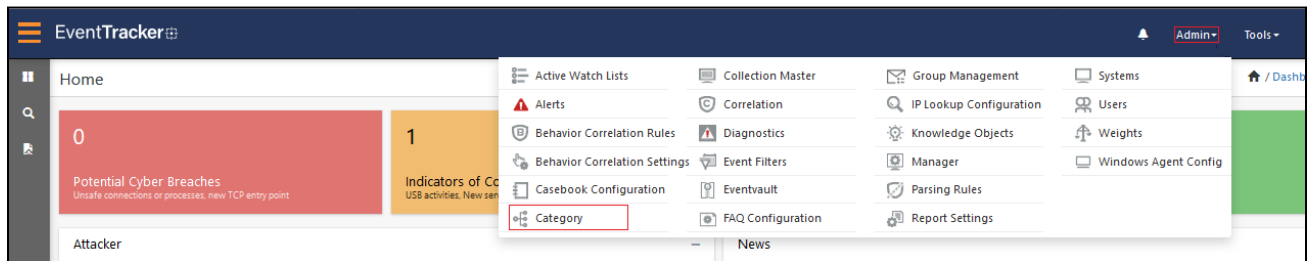
☒ Bitwarden PM: Top Device Type

☒ Bitwarden PM: User Status Info

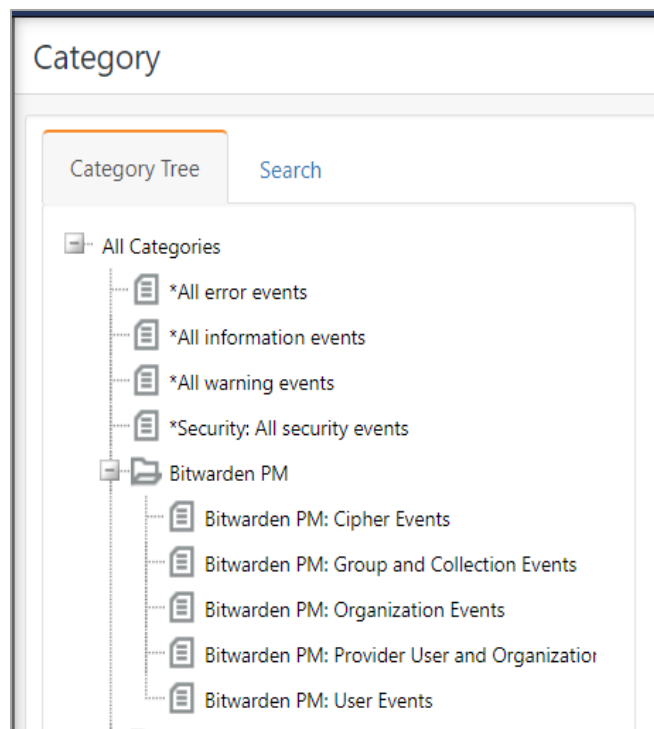
6. Verifying Bitwarden Password Manager Knowledge Pack in EventTracker

6.1 Categories

1. Log on to **EventTracker**.
2. Click the **Admin** dropdown, and then click **Category**.

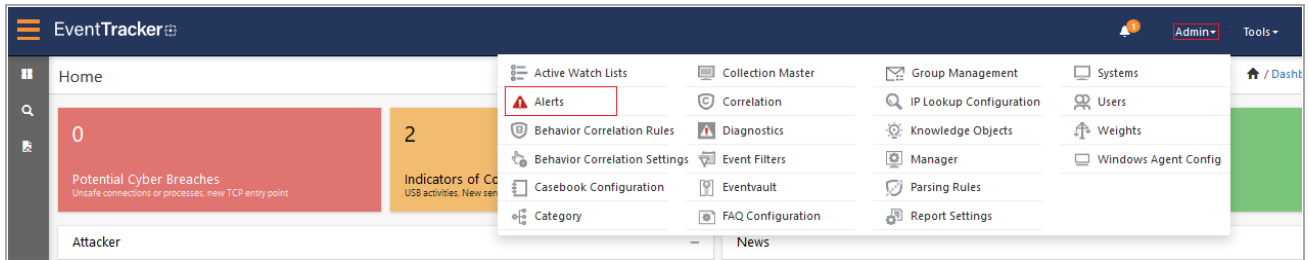


3. In the **Category Tree** to view the imported category, scroll down and expand the **Bitwarden PM** group folder to view the imported category.



6.2 Alerts

1. Log on to **EventTracker**.
2. Click the **Admin** menu, and then click **Alerts**.

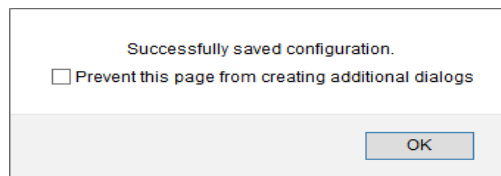


3. In the **Search** box, type **Bitwarden PM**, and then click the **Go** button.
The Alert Management page will display an imported alert.

| <input type="checkbox"/> | Alert Name ^ | Threat | Active |
|--------------------------|------------------------------|--------|--------------------------|
| <input type="checkbox"/> | Bitwarden PM: Login Failed | | <input type="checkbox"/> |
| <input type="checkbox"/> | Bitwarden PM: MFA disabled | | <input type="checkbox"/> |
| <input type="checkbox"/> | Bitwarden PM: Policy Updated | | <input type="checkbox"/> |

4. To activate the imported alert, toggle the **Active** switch.

EventTracker displays a message box.

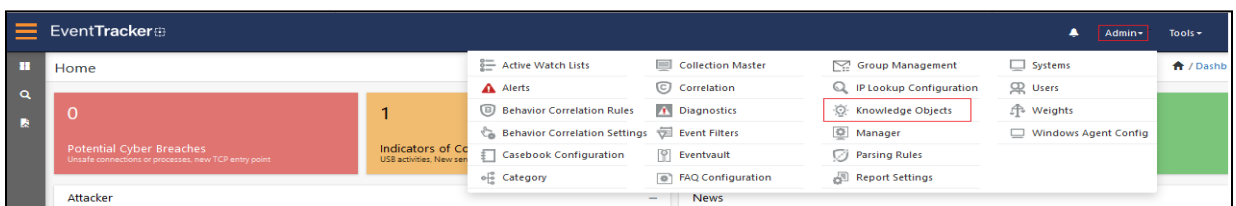


5. Click **OK**, and then click the **Activate Now** button.

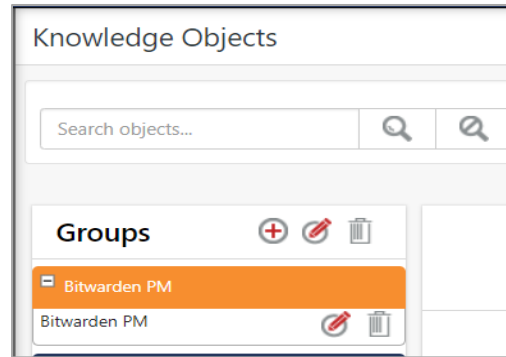
NOTE: Please specify the appropriate **system** in **alert configuration** for better performance.

6.3 Knowledge Objects

1. In the **EventTracker** web interface, click the **Admin** dropdown, and then select **Knowledge Objects**.



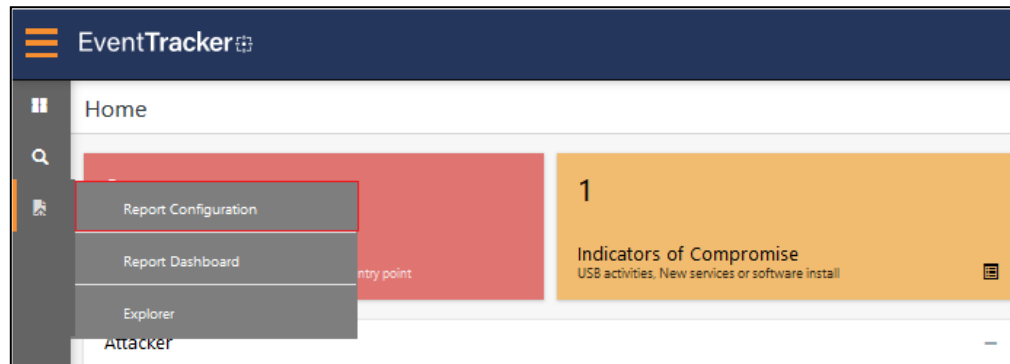
2. In the Knowledge Object tree, expand the **Bitwarden PM** folder to view the imported Knowledge Object.



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

6.4 Reports

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

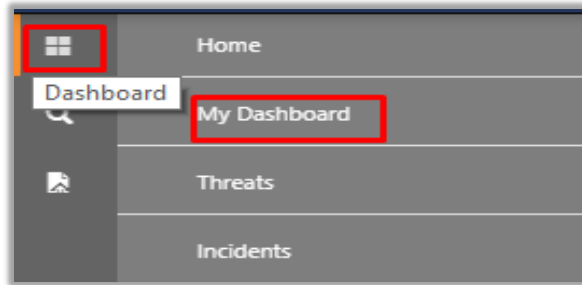



2. In the **Reports Configuration** pane, select the **Defined** option.
3. Click the **Bitwarden PM** group folder to view the imported reports.

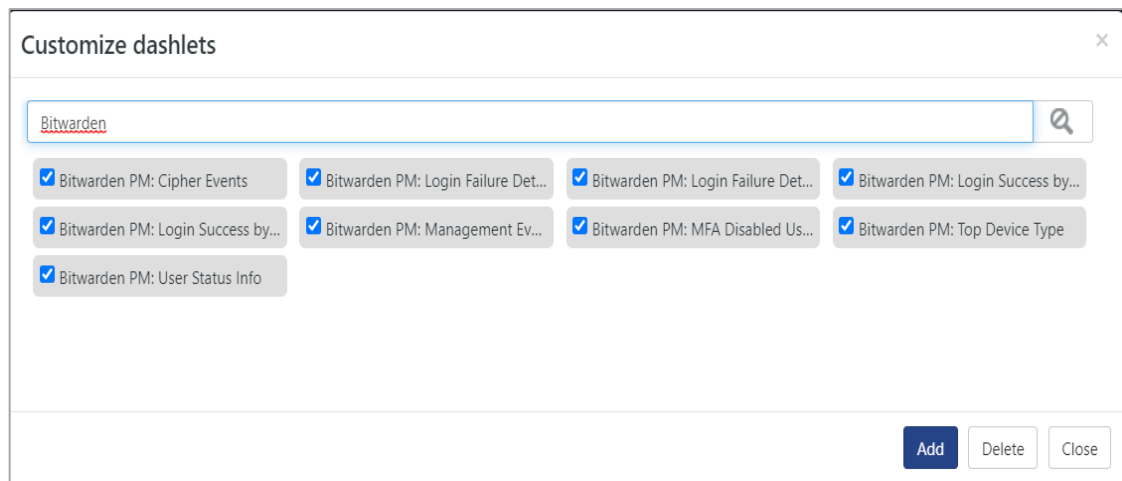


6.5 Dashboards

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



2. In the **My Dashboard** page select  to add dashlets.
3. Search **Bitwarden**, you can see the imported dashlets.



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](https://www.netsurion.com) or follow us on [Twitter](#) or [LinkedIn](#). Netsurion is #23 among [MSSP Alert's 2021 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>