bitwarden | Article du Centre d'Aide

CONSOLE ADMIN › COMPTE RENDU

Microsoft Sentinel SIEM

Afficher dans le centre d'aide:
https://bitwarden.com/help/microsoft-sentinel-siem/

Microsoft Sentinel SIEM

Microsoft Sentinel is a security information and event management (SIEM) platform that can be used to monitor Bitwarden organizations. Organizations can monitor event activity with the Bitwarden Event Logs app on Microsoft Sentinel.

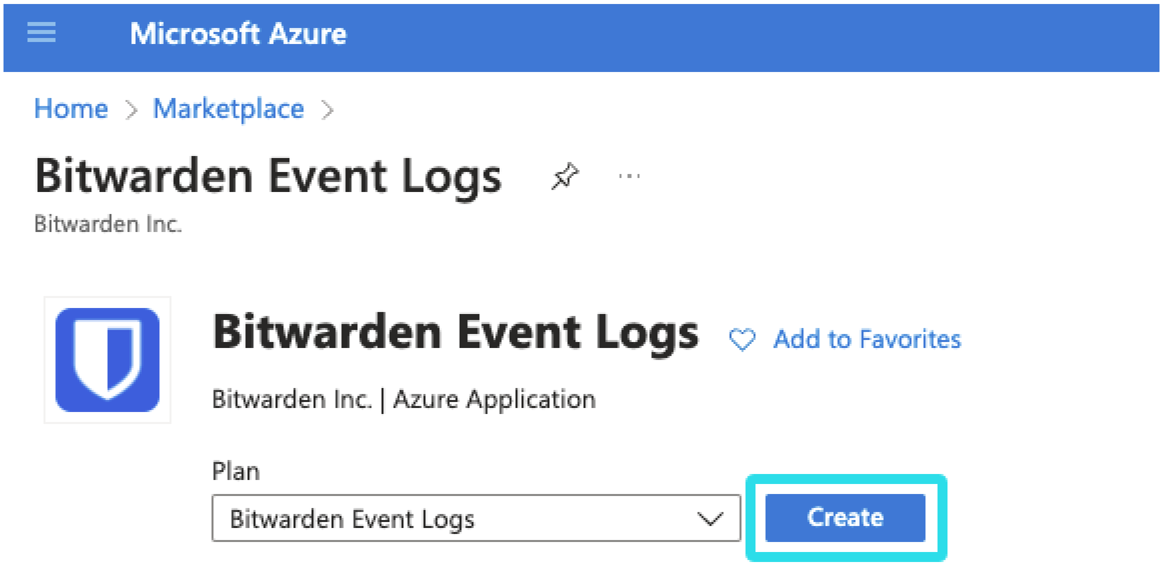
Setup

To setup the Bitwarden integration, an active Azure account with access to a Microsoft Sentinel Workspace is required. Additionally, a Bitwarden API key, which can only be retrieved by organization owners.

Install the Bitwarden app to your Microsoft Sentinel dashboard

The Bitwarden Event Logs application can be located in the Microsoft Azure Marketplace. To add the new application to your Workspace:

1. Choose the Bitwarden Event Logs plan from the dropdown menu and select **Create**.



Bitwarden Event Logs marketplace app

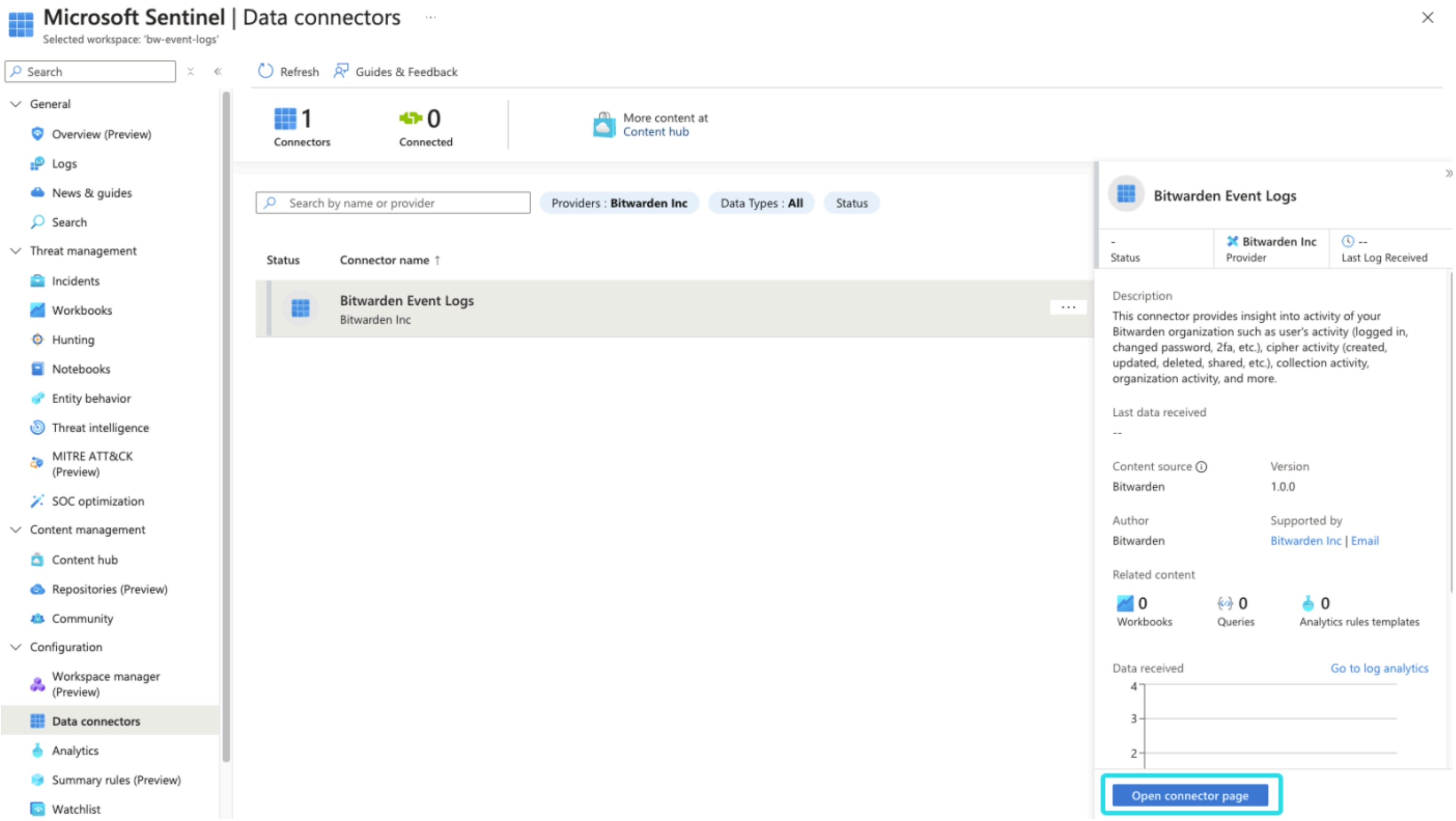
2. Complete the required fields and select the Workspace that will be monitoring Bitwarden organization data.

3. Once complete, select **Review + create**.

Connect your Bitwarden Organization

Once the Bitwarden Event Logs app has been added to your Microsoft Sentinel Workspace, you can connect your Bitwarden organization using your Bitwarden API key.

1. Return to the **Data connectors** screen and select the Bitwarden Event Logs app. Select **Open connector page**. If the Bitwarden Event Logs app is not visible, you may be required to select ⟳ **Refresh.**



Status	Provider	Last Log Received
-	Bitwarden Inc	--

Description

This connector provides insight into activity of your Bitwarden organization such as user's activity (logged in, changed password, 2fa, etc.), cipher activity (created, updated, deleted, shared, etc.), collection activity, organization activity, and more.

Last data received

--

Content source	Version
Bitwarden	1.0.0

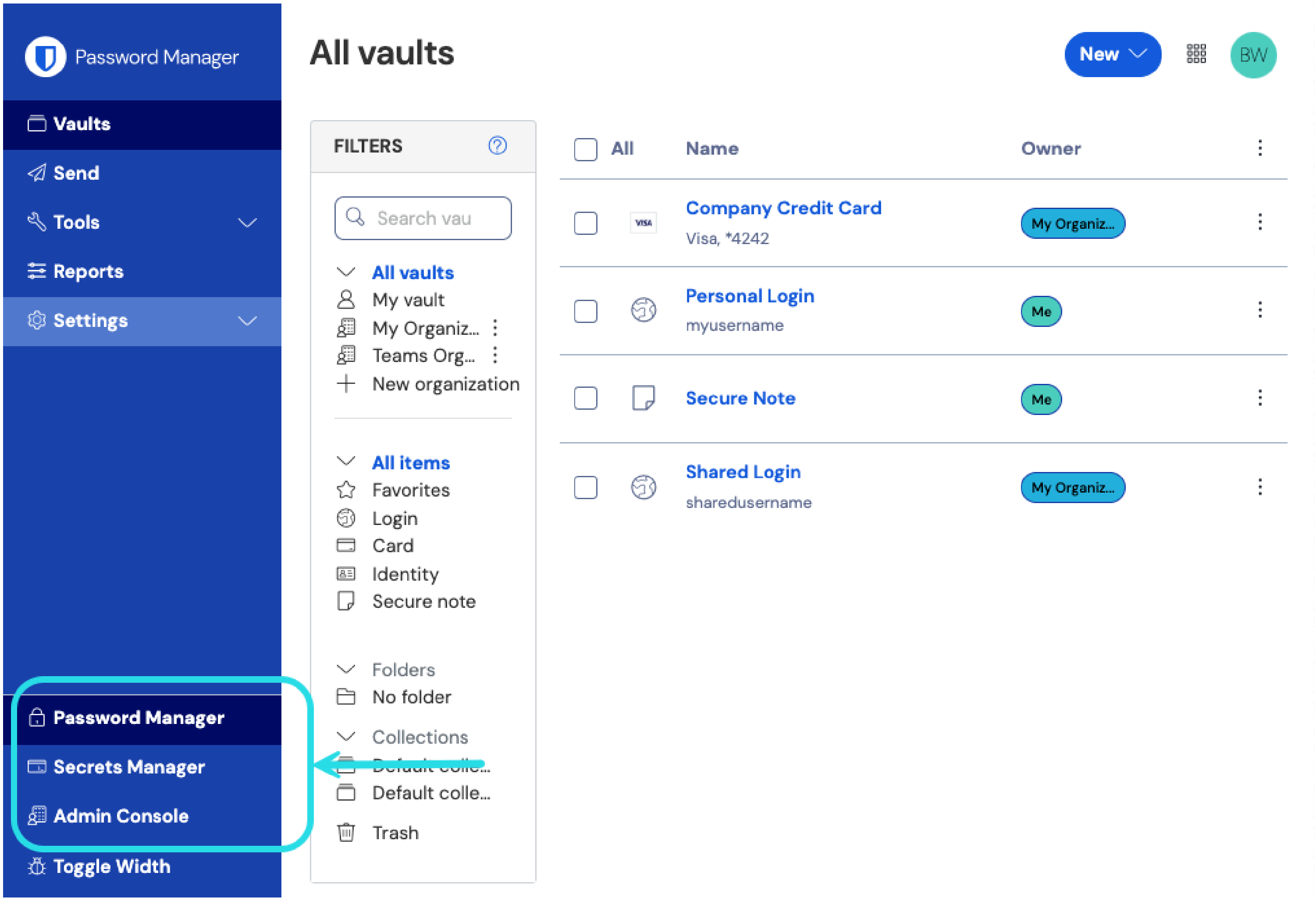
Author	Supported by
Bitwarden	Bitwarden Inc | Email

Related content

Workbooks	Queries	Analytics rules templates
0	0	0

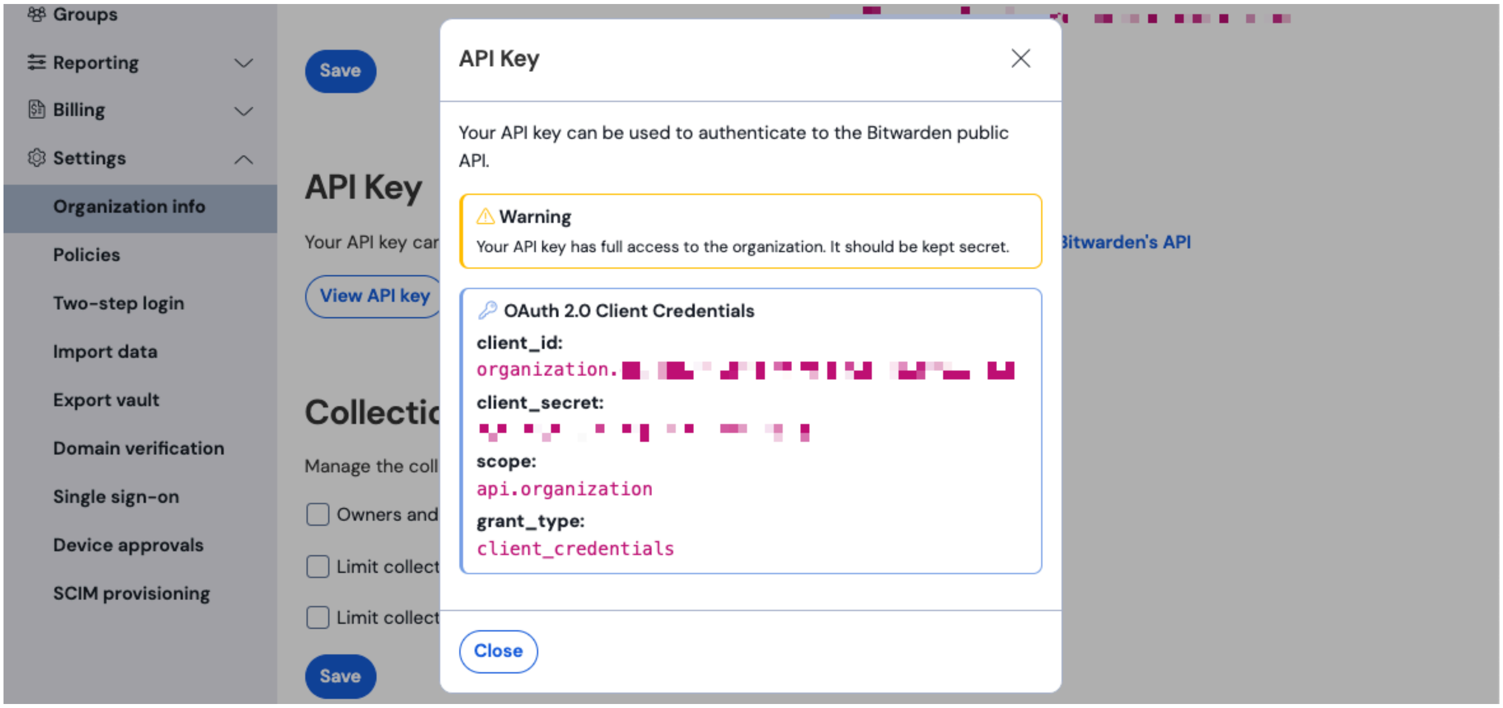
Microsoft Sentinel Bitwarden Event Logs app

2. Keep this screen open, on another tab, log in to the Bitwarden web app and open the Admin Console using the product switcher:



commutateur-de-produit

3. Navigate to your organization's **Settings** → **Organization info** screen and select the **View API key** button. You will be asked to re-enter your master password in order to access your API key information.



[redacted]

API Key

Your API key can be used to authenticate to the Bitwarden public API.

⚠ Warning
Your API key has full access to the organization. It should be kept secret.

OAuth 2.0 Client Credentials

client_id:
organization.[redacted]
client_secret:
[redacted]
scope:
api.organization
grant_type:
client_credentials

Informations sur l'API de l'organisation

4. Return to the Microsoft Sentinel tab. On the **Configuration** page, complete the following fields:

Field	Value
Bitwarden Identity URL	For Bitwarden cloud users, the default URL will be `https://identity.bitwarden.com` or `https://identity.bitwarden.eu`. For self-hosted Bitwarden users, input your self-hosted URL. For example, `https://<self-hosted-url>/identity`. Be sure that the URL does not include any trailing forward slashes at the end of the URL "`/`".
Bitwarden API URL	For Bitwarden cloud users, the default URL will be `https://api.bitwarden.com` or `https://api.bitwarden.eu`. For self-hosted Bitwarden users, input your self-hosted URL. For example, `https://<self-hosted-url>/api`. Be sure that the URL does not include any trailing forward slashes at the end of the URL "`/`".
Client ID	Input the value for `client_id` from the Bitwarden organization API key window.
Client Secret	Input the value for `client_secret` from the Bitwarden organization API key window.

Select **Connect** once the required fields have been completed.

ⓘ **Note**

Les informations de votre clé API de l'organisation sont des données sensibles. Ne partagez pas ces valeurs dans des endroits non sécurisés.

Start monitoring event logs

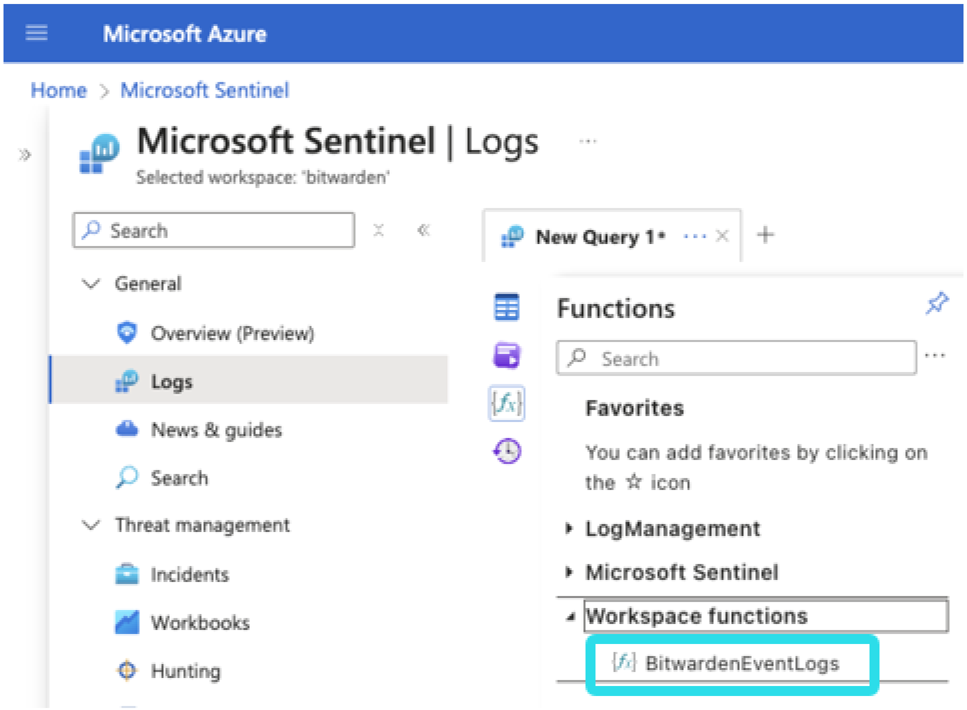
ⓘ **Note**

Historic event data is not available for the Bitwarden Event Logs app on Microsoft Sentinel at this time. Additionally, it may take up to 1 hour for the first events to appear in Microsoft Sentinel.

Bitwarden organization event logs can be viewed in Microsoft Sentinel using the `BitwardenEventLogs` query function.

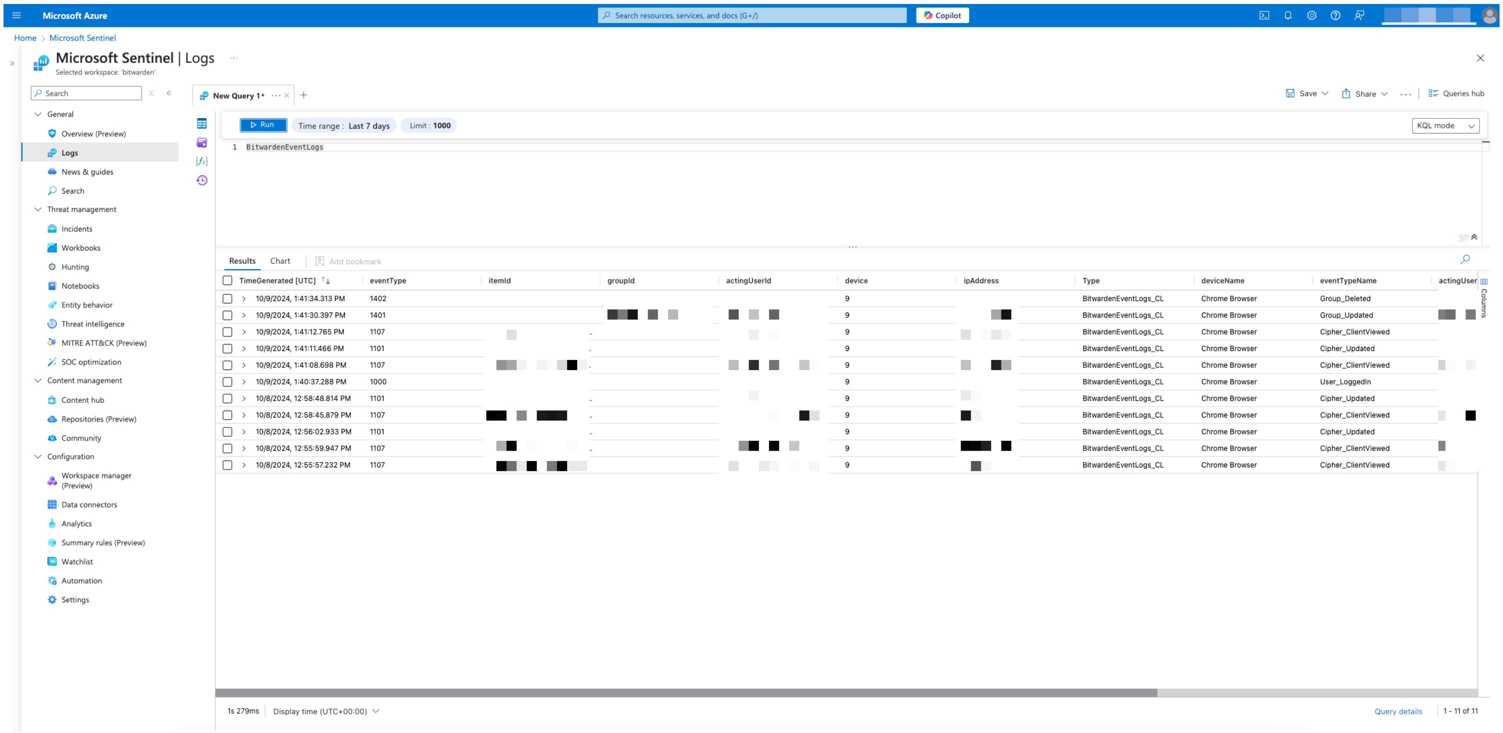
1. From Microsoft Sentinel, select **Logs**. A New Query tab will be created. On the left hand navigation, select **Functions** → **Workspace functions** → **BitwardenEventLogs**.

2. Before running the query, you may select time frame and add specific parameters to the query. To being the query, select **Run**.



Microsoft Sentinel query

Queries can be saved for future use.



```
BitwardenEventLogs
```

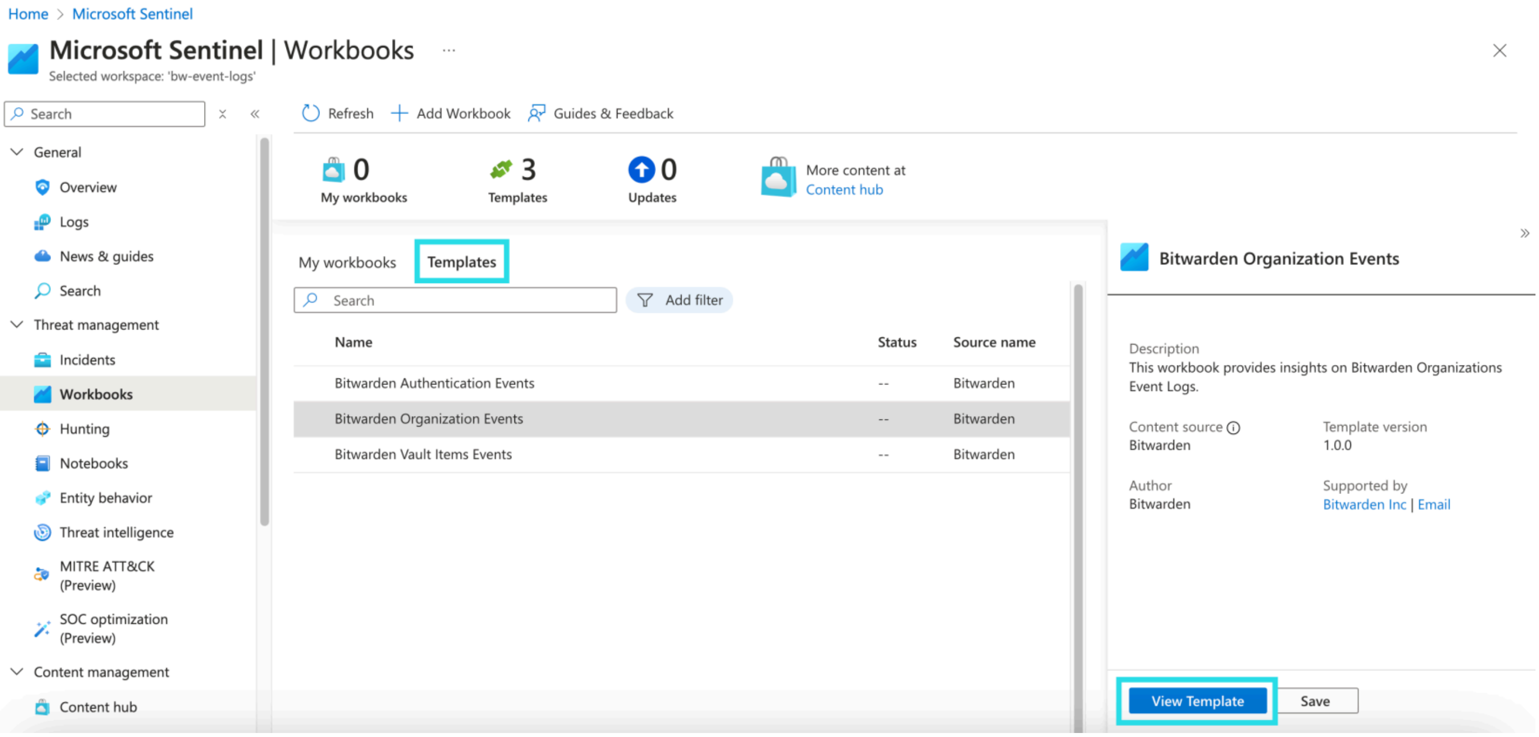
TimeGenerated [UTC]	eventType	itemId	groupId	actingUserId	device	ipAddress	Type	deviceName	eventTypeName	actingUser
10/9/2024, 1:41:34.313 PM	1402				9		BitwardenEventLogs_CL	Chrome Browser	Group_Deleted	
10/9/2024, 1:41:30.397 PM	1401		[redacted]	[redacted]	9	[redacted]	BitwardenEventLogs_CL	Chrome Browser	Group_Updated	[redacted]
10/9/2024, 1:41:12.765 PM	1107	[redacted]		[redacted]	9	[redacted]	BitwardenEventLogs_CL	Chrome Browser	Cipher_ClientViewed	
10/9/2024, 1:41:11.466 PM	1101	[redacted]			9		BitwardenEventLogs_CL	Chrome Browser	Cipher_Updated	
10/9/2024, 1:41:08.698 PM	1107	[redacted]		[redacted]	9	[redacted]	BitwardenEventLogs_CL	Chrome Browser	Cipher_ClientViewed	[redacted]
10/9/2024, 1:40:37.288 PM	1000				9		BitwardenEventLogs_CL	Chrome Browser	User_LoggedIn	
10/8/2024, 12:58:48.814 PM	1101	[redacted]		[redacted]	9	[redacted]	BitwardenEventLogs_CL	Chrome Browser	Cipher_Updated	
10/8/2024, 12:58:45.879 PM	1107	[redacted]		[redacted]	9	[redacted]	BitwardenEventLogs_CL	Chrome Browser	Cipher_ClientViewed	[redacted]
10/8/2024, 12:56:02.933 PM	1101	[redacted]			9		BitwardenEventLogs_CL	Chrome Browser	Cipher_Updated	
10/8/2024, 12:55:59.947 PM	1107	[redacted]		[redacted]	9	[redacted]	BitwardenEventLogs_CL	Chrome Browser	Cipher_ClientViewed	[redacted]
10/8/2024, 12:55:57.232 PM	1107	[redacted]		[redacted]	9	[redacted]	BitwardenEventLogs_CL	Chrome Browser	Cipher_ClientViewed	[redacted]

Microsoft Sentinel query result

Monitor using Workbooks

Workbooks can be used to review event logs and visualize data. Additionally, templates are included in the Bitwarden Event Logs Workbook for a pre-configured overview of available data.

To access Workbooks, select **Workbooks** from the navigation and then **Templates**.



Name	Status	Source name
Bitwarden Authentication Events	--	Bitwarden
Bitwarden Organization Events	--	Bitwarden
Bitwarden Vault Items Events	--	Bitwarden

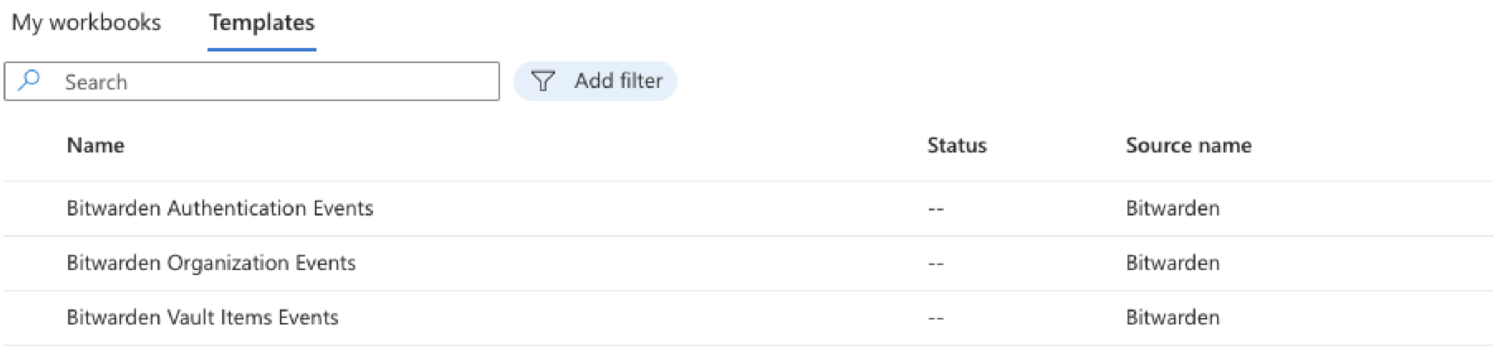
Bitwarden Organization Events

Description
This workbook provides insights on Bitwarden Organizations Event Logs.

Content source Bitwarden	Template version 1.0.0
Author Bitwarden	Supported by Bitwarden Inc | Email

Workbook templates

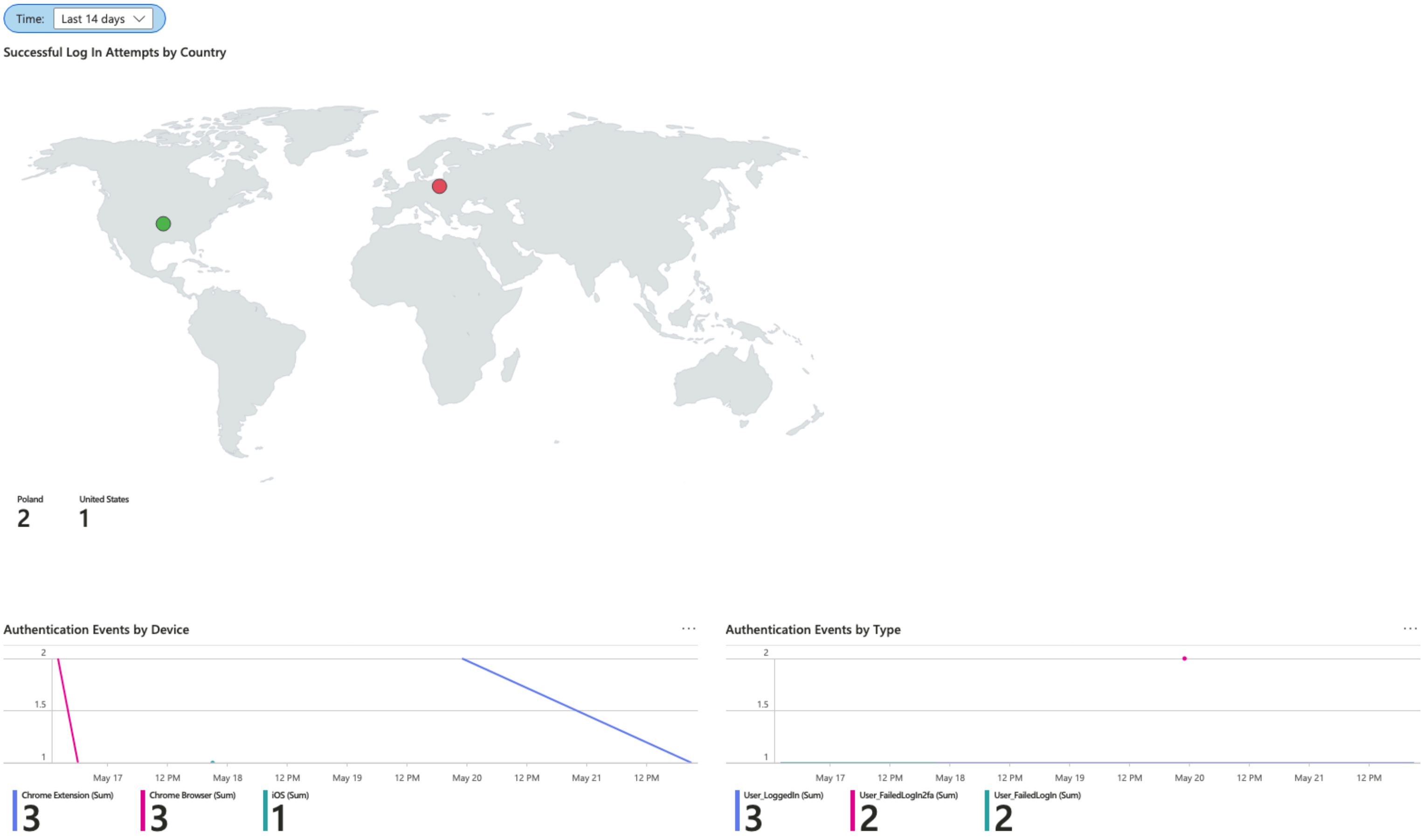
The Bitwarden Event Logs app will have three templates included by default. Select one of the templates and choose **View Template** to begin monitoring data.



Name	Status	Source name
Bitwarden Authentication Events	--	Bitwarden
Bitwarden Organization Events	--	Bitwarden
Bitwarden Vault Items Events	--	Bitwarden

Included templates

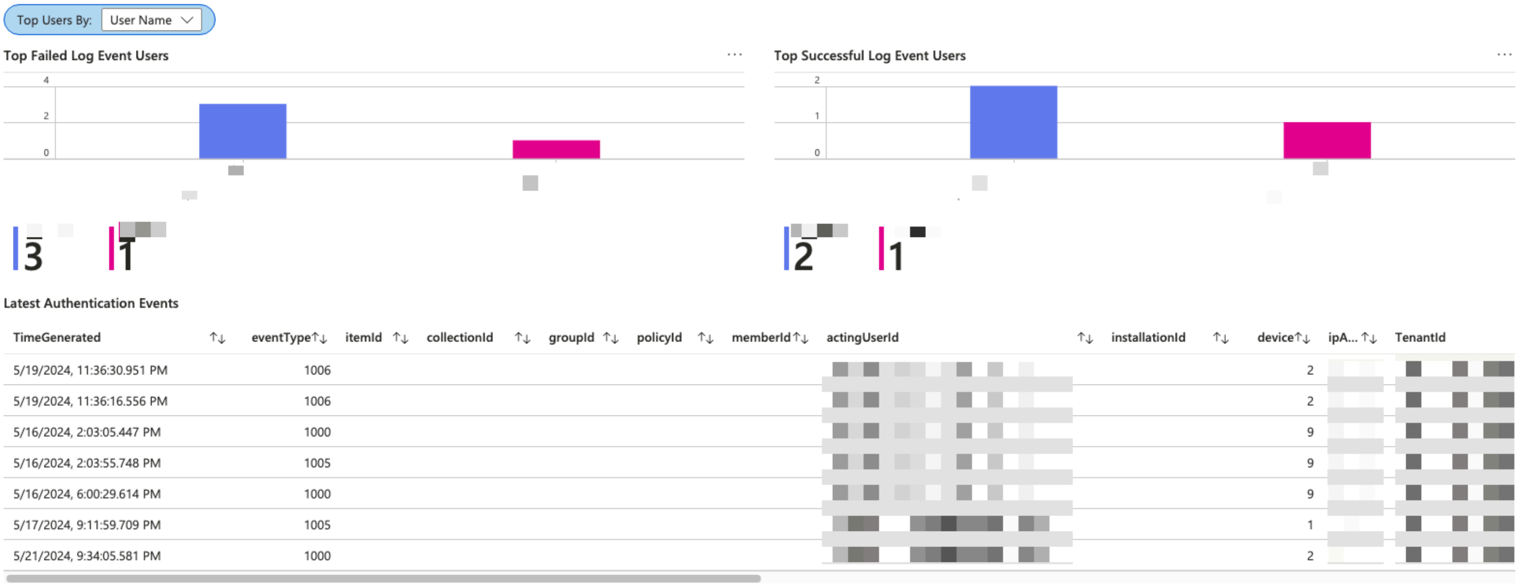
The dashboards include visualized data:



Time: Last 14 days

Microsoft Sentinel dashboard view

Continue scrolling the overview page for additional event log data:



Top Users By: User Name

Latest Authentication Events

TimeGenerated	eventType	itemId	collectionId	groupId	policyId	memberId	actingUserId	installationId	device	ipA...	TenantId
5/19/2024, 11:36:30.951 PM	1006						[redacted]		2	[redacted]	[redacted]
5/19/2024, 11:36:16.556 PM	1006						[redacted]		2	[redacted]	[redacted]
5/16/2024, 2:03:05.447 PM	1000						[redacted]		9	[redacted]	[redacted]
5/16/2024, 2:03:55.748 PM	1005						[redacted]		9	[redacted]	[redacted]
5/16/2024, 6:00:29.614 PM	1000						[redacted]		9	[redacted]	[redacted]
5/17/2024, 9:11:59.709 PM	1005						[redacted]		1	[redacted]	[redacted]
5/21/2024, 9:34:05.581 PM	1000						[redacted]		2	[redacted]	[redacted]

Bitwarden even log view