

ADMINISTRATOR KONSOLE > BERICHTE

Microsoft Sentinel SIEM

Ansicht im Hilfezentrum:

<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.

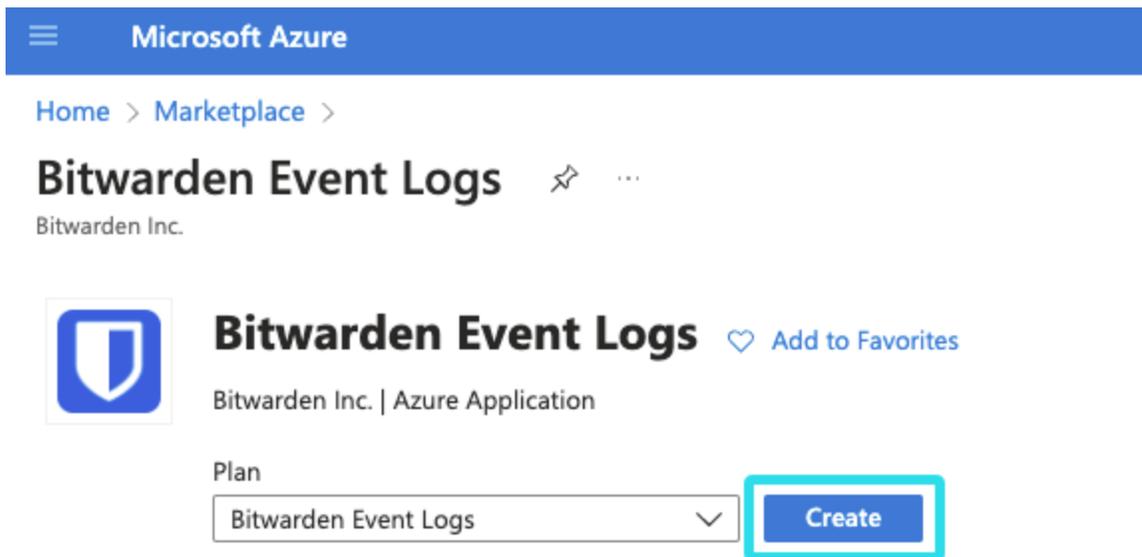
Setup

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**.

The screenshot shows the Microsoft Sentinel 'Data connectors' page. On the left is a navigation sidebar with categories like General, Threat management, Content management, and Configuration. The main area displays '1 Connectors' and '0 Connected'. A search bar and filters for 'Providers: Bitwarden Inc' and 'Data Types: All' are visible. A table lists the 'Bitwarden Event Logs' connector. A right-hand pane provides details for this connector, including a description, last data received status, content source (Bitwarden), version (1.0.0), author (Bitwarden), and supported by (Bitwarden Inc | Email). It also shows related content counts for Workbooks, Queries, and Analytics rules templates. A 'Data received' chart is partially visible at the bottom of the details pane. A blue box highlights the 'Open connector page' button at the bottom of the details pane.

Microsoft Sentinel Bitwarden Event Logs app

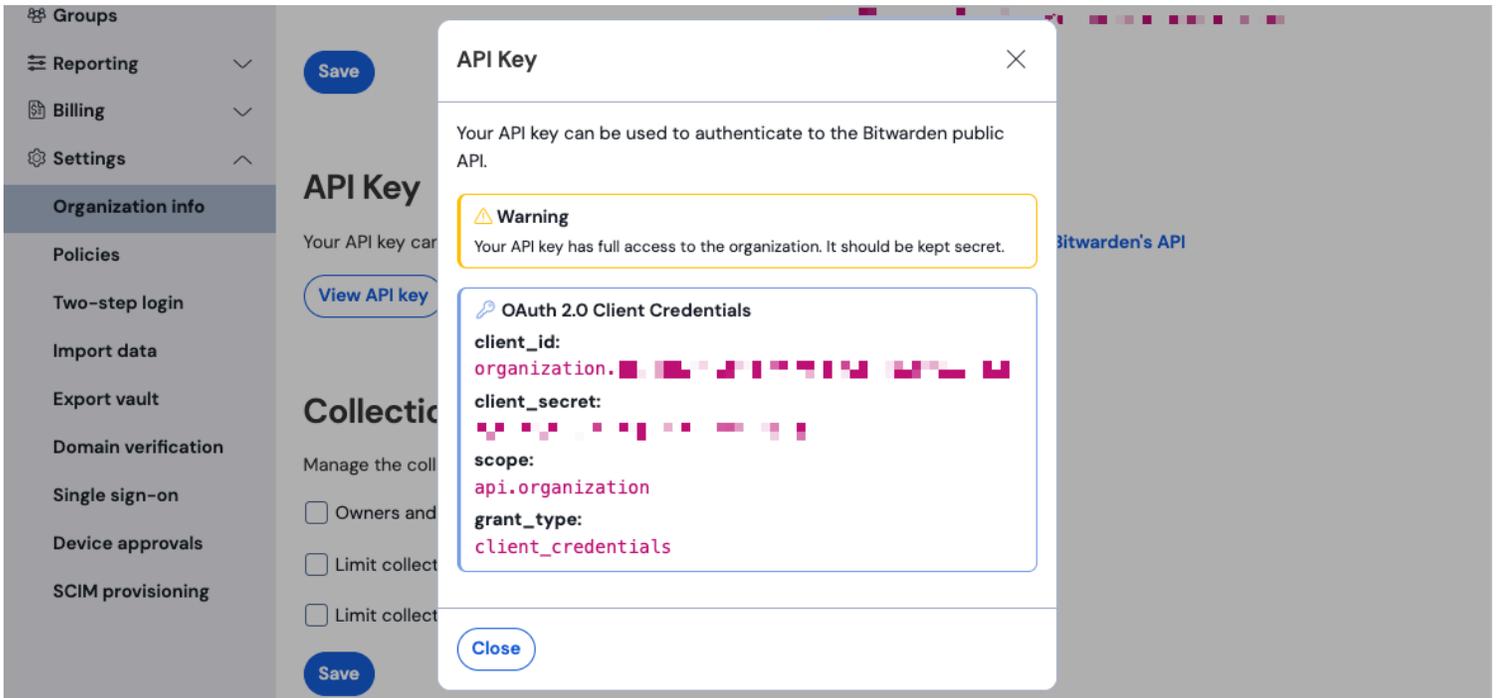
2. Keep this screen open, on another tab, log in to the Bitwarden web app and open the Admin Console using the product switcher:

The screenshot displays the Bitwarden web interface. On the left is a dark blue sidebar with navigation options: Password Manager, Vaults, Send, Tools, Reports, and Settings. The main content area is titled 'All vaults' and features a 'FILTERS' panel on the left with a search bar and a list of categories: All vaults, All items, Folders, Collections, and Trash. A red circle highlights the 'Password Manager' option in the sidebar, with a red arrow pointing to the 'All items' section in the filters panel. The main vault list contains the following entries:

| <input type="checkbox"/> | All | Name | Owner | |
|--------------------------|-----|---|---------------|---|
| <input type="checkbox"/> | | Company Credit Card Visa, *4242 | My Organiz... | ⋮ |
| <input type="checkbox"/> | | Personal Login myusername | Me | ⋮ |
| <input type="checkbox"/> | | Secure Note | Me | ⋮ |
| <input type="checkbox"/> | | Shared Login sharedusername | My Organiz... | ⋮ |

Produktwechsler

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.



Organisation API Informationen

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

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

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

Note

Die API-Schlüsselinformationen Ihrer Organisation sind sensible Daten. Teilen Sie diese Werte nicht an unsicheren Orten.

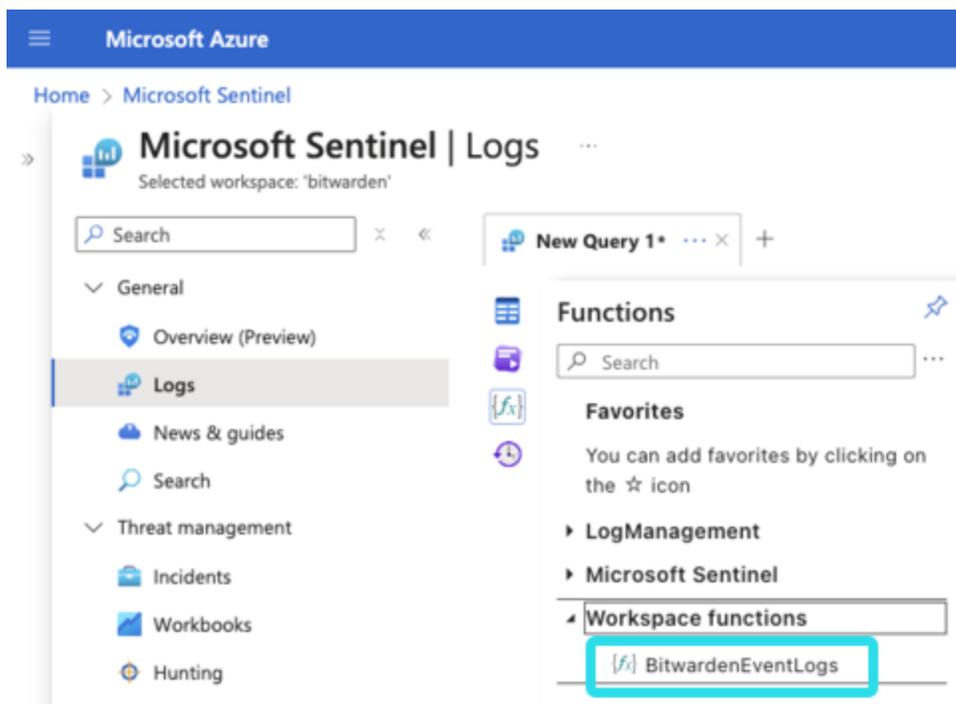
Start monitoring event logs

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 begin the query, select **Run**.



Microsoft Sentinel query

Queries can be saved for future use.

| 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 | | | | 9 | | BitwardenEventLogs_CL | Chrome Browser | Group_Updated | |
| > 10/9/2024, 1:41:12.765 PM | 1107 | | | | 9 | | BitwardenEventLogs_CL | Chrome Browser | Cipher_ClientViewed | |
| > 10/9/2024, 1:41:11.466 PM | 1101 | | | | 9 | | BitwardenEventLogs_CL | Chrome Browser | Cipher_Updated | |
| > 10/9/2024, 1:40:37.686 PM | 1107 | | | | 9 | | BitwardenEventLogs_CL | Chrome Browser | Cipher_ClientViewed | |
| > 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 | | | | 9 | | BitwardenEventLogs_CL | Chrome Browser | Cipher_Updated | |
| > 10/8/2024, 12:58:45.879 PM | 1107 | | | | 9 | | BitwardenEventLogs_CL | Chrome Browser | Cipher_ClientViewed | |
| > 10/8/2024, 12:56:02.933 PM | 1101 | | | | 9 | | BitwardenEventLogs_CL | Chrome Browser | Cipher_Updated | |
| > 10/8/2024, 12:55:59.847 PM | 1107 | | | | 9 | | BitwardenEventLogs_CL | Chrome Browser | Cipher_ClientViewed | |
| > 10/8/2024, 12:55:57.232 PM | 1107 | | | | 9 | | BitwardenEventLogs_CL | Chrome Browser | Cipher_ClientViewed | |

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**.

Home > Microsoft Sentinel

Microsoft Sentinel | Workbooks
Selected workspace: 'bw-event-logs'

Refresh + Add Workbook Guides & Feedback

0 My workbooks 3 Templates 0 Updates More content at Content hub

My workbooks **Templates**

Search Add filter

| 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

View Template Save

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.

My workbooks **Templates**

Search Add filter

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

Included templates

The dashboards include visualized data:

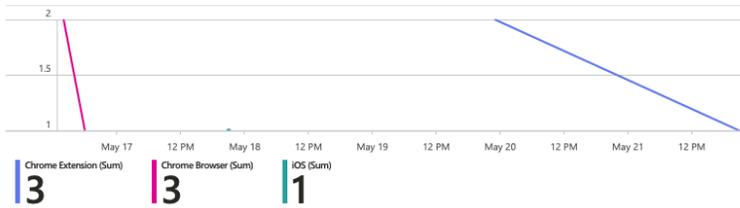
Time: Last 14 days

Successful Log In Attempts by Country

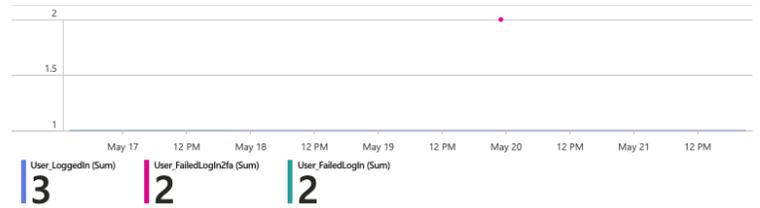


Poland 2 United States 1

Authentication Events by Device



Authentication Events by Type



Microsoft Sentinel dashboard view

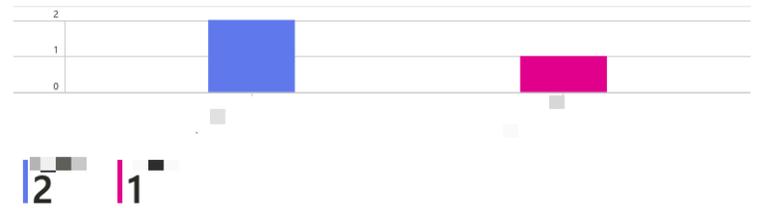
Continue scrolling the overview page for additional event log data:

Top Users By: User Name

Top Failed Log Event Users



Top Successful Log Event Users



Latest Authentication Events

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

Bitwarden even log view