ADMIN CONSOLE > RAPPORTERING >

Splunk SIEM

View in the help center: https://bitwarden.com/help/splunk-siem/

Splunk SIEM

Splunk Enterprise is a security information and event management (SIEM) platform that can be used with Bitwarden organizations. Organizations can monitor event activity with the Bitwarden Event Logs app on their Splunk dashboard.

Setup

Create a Splunk account

Installing the Bitwarden app on Splunk requires a Splunk Enterprise account. Bitwarden event monitoring is available on:

- Splunk Enterprise
- Spunk Cloud Classic
- Splunk Cloud Victoria

Install Splunk

For on-premise Splunk users, the next step is to install Splunk Enterprise. Follow the Splunk documentation to complete an install of the Splunk Enterprise software.

(i) Note

Splunk Enterprise versions 8.X are no longer supported. Currently Bitwarden is supported on versions 9.0, 9,1, and 9.2.

Create an index

Before connecting your Bitwarden organization to your Splunk Dashboard, create an index that will maintain Bitwarden data.

1. Open the Settings menu located on the top navigation bar and select Indexes.

2. Once you are on the indexes screen, select New Index. A window will appear for you to create a new index for your Bitwarden app.

⇒Splunk Cloud

Index name			
Index Data Type	🗄 Events	Ø	Metrics
	The type of data to store (event-based or metrics).		
Max raw data size			MB 🕶
	Maximum aggregated size of raw data (uncompressed) c	ontained in index. Set t llowed.	his to 0 for unlimited. Max ra
Searchable retention			
Searchable retention (days)	Number of days the data is searchable		

New Index

⇒Splunk Enterprise

New Index			×
General Settings			
Index Name	bitwarden_events		
	Set index name (e.g., INDEX_NAME). Search using inde	ex=INDEX_NAME.	
Index Data Type	Events 🔗 Metrics		
	The type of data to store (event-based or metrics).		
Home Path	optional		
rionie rau	Hot/warm db path. Leave blank for default (\$SPLUNK_I	DB/INDEX_NAME/db).	
Cold Path	optional		
	Cold db path. Leave blank for default (\$SPLUNK_DB/IN	IDEX_NAME/colddb).	
Thawed Path	optional		
mandarian	Thawed/resurrected db path. Leave blank for default (\$	SPLUNK_DB/INDEX_NA	ME/thaweddb).
Data Integrity Check	Enable	[Disable
	Enable this if you want Splunk to compute hashes on e	very slice of your data fo	r the purpose of data integrity.
Max Size of Entire Index	500		GB ▼
Maximum target size of entire index.			
Max Size of	auto		GB 🔻
Hot/Warm/Cold Bucket	Maximum target size of buckets. Enter 'auto_high_volu	me' for high-volume inde	exes.
Frozen Path	optional		
	Frozen bucket archive path. Set this if you want Splunk to automatically archive frozen buckets.		
Арр	Search & Reporting 🔻		
Storage Optimization			
Tsidx Retention Policy	Enable Reduction	Disabl	e Reduction
	Warning: Do not enable reduction without understandin reduced buckets. Learn More 🖸	ng the full implications. It	is extremely difficult to rebuild
Reduce tsidx files older	s older Days		Days 🔻
than	Age is determined by the latest event in a bucket.		
			Save

New Index Enterprise

3. In the **Index Name** field, enter **bitwarden_events**.

- 4. Apply your required values for Max raw data size and Searchable retention.
- 5. When you are finished, select **Save**.

Install the Splunk Bitwarden app

After your Bitwarden index has been created, navigate to your Splunk dashboard.

1. Open the **Apps** drop down menu and select **Find More Apps**.

Apps Sea	arch & Reporting							
Soor	oud Monitoring Console	> ;	ello, Splunk Clo	oud Admin				
Seal	lunk Secure Gateway	0	ick links Dashboard	Recently viewed	Created by you	Shared with you		
> Un	iversal Forwarder	\$						
Up	ograde Readiness App							
(Арр) Ма	anage Apps		mmon tasks					
Fin	nd More Apps		Add data	iety of common sources.	Search Turn da	1 your data ta into doing with Splunk search.		Visualize your data Create dashboards that wor
Univer	ersal Forwarder							
E⊘ Upgra	ade Readiness App		Add team memb	ers nbers to Splunk platform.	Config Login of	ure mobile devices r manage mobile devices using Splunk		
Fi	ind more apps 🖸				Secure	Gateway.		
		Le	earning and resources					
			Learn more with Deploy, manage, ar with comprehensive	Splunk Docs ⊘ nd use Splunk software e guidance.	Get he Actiona Custom	elp from Splunk experts 2 ble guidance on the Splunk Lantern er Success Center.	SB(+	Extend your capabilities Browse thousands of apps of
			<u>کومج</u> Join the Splunk (Learn, get inspired,	Community [2] and share knowledge.	See ho Browse	ow others use Splunk [견 real customer stories.		Training and Certificatio Become a certified Splunk N

Splunk apps dashboard

2. Select Browse more apps.

3. Search Bitwarden Event Logs in the app catalogue. Select Install for the Bitwarden Event Logs app.



Bitwarden event logs app

4. In order to complete the installation, you will need to enter your Splunk account. Your Splunk account may not be the same credentials used to access your Splunk portal.

Login and Install



Enter your Splunk.com username and password to download the app.

Username

Password

Forgot your password?

The app, and any related dependency that will be installed, may be provided by Splunk and/or a third party and your right to use these app(s) is in accordance with the applicable license(s) provided by Splunk and/or the third-party licensor. Splunk is not responsible for any third-party app (developed by you or a third party) and does not provide any warranty or support. Installation of a third-party app can introduce security risks. By clicking "Agree" below, you acknowledge and accept such risks. If you have any questions, complaints or claims with respect to an app, please contact the applicable licensor directly whose contact information can be found on the Splunkbase download page.

Bitwarden Event Logs is governed by the following license: 3rd_party_eula

I have read the terms and conditons of the license(s) and agree to be bound by them. I also agree to Splunk's Website Terms of Use.



Login and install Bitwarden app on Splunk

5. After you have entered your information, select Agree and Install.

(i) Note

Following the Bitwarden Event Logs app download, you may be required to restart Splunk.

Connect your Bitwarden organization

Once the Bitwarden Event Logs app has been installed in your Splunk Enterprise instance, you can connect your Bitwarden organization using your Bitwarden API key.

1. Go to the dashboard home and select the **Bitwarden Event Logs** app:

splunk:>cloud Apps * Messe	ges • Settings • Activity • Find Q	🥥 💄 Splunk Cloud Admin 👻 😗 Suppe	ort& Servi
Apps Ø Monage	Hello, Splunk Cloud Admin		
Search apps by name Q	Quick links Dashboard Recently viewed Created by you Shared with	th you	
Search & Reporting			
Bitwarden Event Logs	Common tasks		
Cloud Monitoring Console	Add data	Visualize your data	
Discover Splunk Observability Cloud	Add data from a variety of common sources. Turn data into doing a	with Splunk search. Create dashboards that work for your data.	
Splunk Secure Gateway	Sa Add team members	devices	
Universal Forwarder	Add your team members to Splunk platform. Login or manage not Secure Gateway.	bile devices using Splunk	
Upgrade Readiness App			
Find more apps 12	Learning and resources		
	Learn more with Splunk Docs 12 Deploy, manage, and use Splunk software with comprehensive guidance.	Iunk experts 12 Extend your capabilities 12 en the Splunk Lantern Browse thousands of apps on Splunkbase.	

Bitwarden on Splunk dashboard

2. Next, on the App configuration page, select **Continue to app setup page**. This is where you will add your Bitwarden organization's information.

Search	Dashboards 🔻	Setup
Setup		
Enter the	e information bel	ow to complete setup.
Your API	key can be found i	n the Bitwarden organization admin console.
Client Id		
Client Se	cret	
Choose a	Splunk index for t	he Bitwarden event logs.
Index		
main		\sim
Self-host	ed Bitwarden serve	ers may need to reconfigure their installation's URL.
Server U	RL.	
https://b	itwarden.com	
Choose t	he earliest Bitward	en event date to retrieve (Default is 1 year).
Start date	nded to be set only of (optional)	n first time setup. Make sure you have no other Bitwarden events to avoid duplications.
mm/dd	ууууу	
Submit		

Setup Bitwarden menu

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

Password Manager	All vaults		New 💛 🇱 BW
🗇 Vaults	FILTERS		Owner
🖉 Send			owner :
\ll Tools \sim	Q Search vau	Company Credit Card Visa, *4242	My Organiz
æ Reports	 ✓ All vaults 	Porconal Login	
🕸 Settings 🛛 🗸 🗸	 ∠ My vault ∅ My Organiz : 	myusername	Me
	giii Teams Org : + New organization	Secure Note	Me
	 ✓ All items ☆ Favorites ④ Login □ Card □ Identity □ Secure note 	Shared Login sharedusername	My Organiz
Password Manager Socrete Manager	 ✓ Folders ➡ No folder ✓ Collections 		
Admin Console	Default colle		
🗄 Toggle Width			
		Product switcher	

4. 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.



Organization api info

5. Copy and paste the client_id and client_secret values into their respective locations on the Splunk setup page.

Complete the following additional fields as well:

Field	Value
Index	Select the index that was created previously in the guide: bitwarden_events .
Server URL	For self-hosted Bitwarden users, input your self-hosted URL. For cloud-hosted organizations, use the URL https://vault.bitwarden.com or https://vault.bitwarden.eu.
Start date (optional)	Set a start date for data monitoring. When not set, the default date will be set to 1 year. This is a one time configuration, once set, this setting cannot be changed.

(i) Note

Your organization API key information is sensitive data. Do not share these values in nonsecure locations.



Once done, select Submit.

Understanding Search Macro

The **bitwarden_event_logs_index** search macro will be created following the initial Bitwarden Event Logs install. To access the macro and adjust settings:

- 1. Open the Settings on to top navigation bar. Then, select Advanced Search.
- 2. Select Search Macros to open the list of search macros.

Search macro permissions

Next, setup which user roles will have permission to use the macro:

- 1. View macros by selecting **Settings** → **Advanced Search** → **Search macros**.
- 2. Select Permissions on bitwarden_events_logs_index. Edit the following permissions and select Save once complete:

Object should appear in

This app only (bitwarden_event_logs)

All apps (system)

Permissions

Roles	Read	Write
Everyone	~	
apps		
can_delete		
list_users_roles		
power		
sc_admin		\checkmark
tokens_auth		
user		

Cancel

Save

Search Macro Permissions

Field	Description
Object should appear in	In order to use the macro in event searching, select This app only . The macro will not apply if Keep private is selected.
Permissions	Select the desired permissions for user roles with Read and Write access.

(i) Note

Only one search macro will be functional on the app at a given time.

Understanding the dashboards

The Dashboard will provide several options for monitoring and visualizing Bitwarden organizational data. The three primary categories of data monitoring include:

- Bitwarden authentication events
- Bitwarden vault item events
- Bitwarden organization events

The data displayed on the dashboards will provide information and visualization for a broad variety of searches. More complex queries can be completed by selecting the **Search** tab at the top of the dashboard.

(i) Note

Search results will only populate data relevant to a specific event type that occurred. Attributes that are not in-scope for a specific event type will be displayed as **null** in the search results. For example, **collectionId=null** will be present when the event type is a user logging in.

Timeframe

While searching from the Search page or Dashboards, searches can be designated to a specific timeframe.

Säker och pålitlig lösenordshanterare med öppen källkod för företag

splunk>cloud Apps Messages Settings Activity Q. Find	🧭 👤 Splunk Cloud Admin 👻 😯 Support & Services 🔻
Search Dashboards ▼ Setup	
Search	
sourcetype="bitwarden:events" type=*	Last 24 hours 🔻 ຊ
No Event Sampling -	standard_perf (search default) ▼
> Search History (?)	
How to Search	Analyze Your Data with Table Views
If you are not familiar with the search features, or want to learn more, or see your available data, see one of the following resources.	Table Views It you prepare data without using SPL. First, use a point- and-click interface to select data. Then, clean and transform it for analysis in Analytics Workspace, Search, or Pivot! Create Table View
Documentation 2 Tutorial 2	Learn more 🗷 about Table Views, or view and manage your Table Views with the Datasets listing page.

Splunk timeframe search

(i) Note

For on-premises users, the following timeframes are supported for Bitwarden event logs searches:

- Month to date
- Year to date
- Previous week
- Previous business week
- Previous month
- Previous year
- Last 30 days
- All time

Query parameters

Set up specific searches by including search queries. Spunk utilizes its search processing language (SPL) method for searching. See Splunk's documentation for additional details on searches.

Search structure:

Bash search | commands1 arguments1 | commands2 arguments2 | ...

An example of a standard search result object:

Splunk search result object

The fields shown in the standard search object can be included in any specific search. This includes all of the following values:

Bitwarden Fields

Value	Description
actingUserEm ail	The email of the user performing the action.
actingUserId	Unique id of user performing action.
actingUserNa me	Name of the user performing an action.
collectionId	Organization collection id.
device	Numerical number to identify the device that the action was performed on.
deviceName	Numerical id of device. Exact mapping can be located here.

Value	Description
groupId	Organization group id.
groupName	Organization group name.
hash	Splunk computed data hash. Learn more about Splunk's data integrity here.
ipAddress	The ip address that performed the event.
itemId	Vault item (cipher, secure note, etc) of the organization vault.
memberEmail	Email of the organization member that the action was directed towards.
memberId	Unique id of the organization member that the action was directed towards.
memberName	Name of organization member that action was directed towards.
policyId	Organization policy update. See organization events here.
type	The event type code that represents the organization event that occurred. See a complete list of event codes with descriptions here.
typeName	Type numerical id. See mappings here.

Spunk default fields

The following Splunk default fields will appear in queries. More information on the Splunk's default fields can be located in the Splunk documentation.

Fields:

- source
- sourcetype
- date
 - date_hour date_mday date_minute date_month date_second date_wday date_year date_zone
- index
- linecount
- punct
- splunk_server
- timestamp

(i) Note

Attributes that are not relevant to the event type will be reported as null.

Search all:



Filter results by a specific field

In the following example, the search is looking for actingUserName with a * wildcard which will display all results with actingUserNa me.



The **AND operator** is implied in Splunk searches. The following query will search for results containing a specific type AND actingUser Name.

Bash

sourcetype="bitwarden:events" type=1000 actingUserName="John Doe"

Include multiple commands by separating with |. The following will show results with the top value being ipAddress.

Bash
<pre>sourcetype="bitwarden:events" type=1115 actingUserName="John Doe" top ipAddress</pre>

Additional resources

Set user roles

Manage users roles to allow individuals to perform specific tasks. To edit user roles:

- 1. Open the **Settings** menu on the top navigation bar.
- 2. Select **Users** from the bottom right corner of the menu.

3. From the users screen, locate the user that you wish to edit permissions for and select **Edit**.

Edit User		×
Fuli name	optional	
Email address	optional	
Old password	Old password	
Set password	New password	
Confirm password	Confirm new password	
	Password must contain at least 7 8 characters	
Time zone [†]	– Default System Timezone – 🔻	
Default app 7	launcher (Home) *	
Assign roles ⁷	Available Item(s) add all > Selected Item(s) admin can_delete power splunk-system-role	< remove all
Require password change on next login		
I acknowledge that users assigned to roles with the fsh_manage capability can send search results data outside the compli- ant environment.		
	Cano	sel Save

Splunk edit user permissions

From this screen, details for the user can be filled out. Permission such as admin, power, and can_delete can be individually assigned here as well.

Delete data

Delete Bitwarden search data by clearing the index with SSH access. Data may need to be cleared in instances such as changing the organization being monitored.

- 1. Access the Splunk directory and stop Splunk processes.
- 2. Clear the **bitwarden_events** index with **-index** flag. For example:



3. Restart Splunk processes.



Troubleshooting

• Splunk Enterprise users, the app will log to: /opt/splunk/var/log/splunk/bitwarden_event_logs.log

If you are experiencing any errors, or the Bitwarden app is not functioning correctly, users can check the log file for errors or see Spunk's documentation.