

CONSOLA DE ADMINISTRADOR > INFORMANDO

Splunk SIEM

Ver en el centro de ayuda:
<https://bitwarden.com/help/splunk-siem/>

Splunk SIEM

Splunk Enterprise es una plataforma de gestión de información de seguridad y gestión de eventos (SIEM) que se puede utilizar con organizaciones de Bitwarden. Las organizaciones pueden monitorear la actividad de [eventos](#) con la aplicación [Bitwarden Event Logs](#) en su tablero de Splunk.

Configuración

Crea una cuenta de Splunk

La instalación de la aplicación Bitwarden en Splunk requiere una cuenta de Splunk Empresa o Plataforma Cloud de Splunk. El monitoreo de eventos de Bitwarden está disponible en:

- Splunk Cloud Classic
- Splunk Cloud Victoria
- Splunk Empresa

Instala Splunk

Para los usuarios de Splunk en las instalaciones, el siguiente paso es instalar Splunk Empresa. Sigue la [documentación de Splunk](#) para completar una instalación del software de la Empresa Splunk.

Note

Las versiones 8.X de Splunk Empresa ya no están soportadas. Actualmente Bitwarden es compatible con las versiones 9.0, 9.1 y 9.2.

Crear un índice

Antes de conectar tu organización Bitwarden a tu Dashboard de Splunk, crea un índice que mantendrá los Datos de Bitwarden.

1. Abra el menú de **Ajustes** ubicado en la barra de navegación superior y seleccione **Índices**.
2. Una vez que estés en la pantalla de índices, selecciona **Nuevo Índice**. Aparecerá una ventana para que puedas crear un nuevo índice para tu aplicación Bitwarden.

⇒ Splunk Cloud

New Index ✕

Index name

Index Data Type 📄 Events 📊 Metrics
The type of data to store (event-based or metrics).

Max raw data size MB ▾
Maximum aggregated size of raw data (uncompressed) contained in index. Set this to 0 for unlimited. Max raw data size values less than 100MB, other than 0, are not allowed.

Searchable retention (days)
Number of days the data is searchable

Cancel Save

Nuevo Índice

New Index ✕

General Settings

Index Name
Set index name (e.g., INDEX_NAME). Search using index=INDEX_NAME.

Index Data Type 📄 Events 📊 Metrics
The type of data to store (event-based or metrics).

Home Path
Hot/warm db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/db).

Cold Path
Cold db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/coldb).

Thawed Path
Thawed/resurrected db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/thawedb).

Data Integrity Check Enable Disable
Enable this if you want Splunk to compute hashes on every slice of your data for the purpose of data integrity.

Max Size of Entire Index GB ▾
Maximum target size of entire index.

Max Size of Hot/Warm/Cold Bucket GB ▾
Maximum target size of buckets. Enter 'auto_high_volume' for high-volume indexes.

Frozen Path
Frozen bucket archive path. Set this if you want Splunk to automatically archive frozen buckets.

App Search & Reporting ▾

Storage Optimization

Tsidx Retention Policy Enable Reduction Disable Reduction
Warning: Do not enable reduction without understanding the full implications. It is extremely difficult to rebuild reduced buckets. [Learn More](#) [🔗](#)

Reduce tsidx files older than Days ▾
Age is determined by the latest event in a bucket.

Save Cancel

Nueva Empresa Índice

3. En el campo **Nombre del Índice**, ingrese `bitwarden_events`.

Note

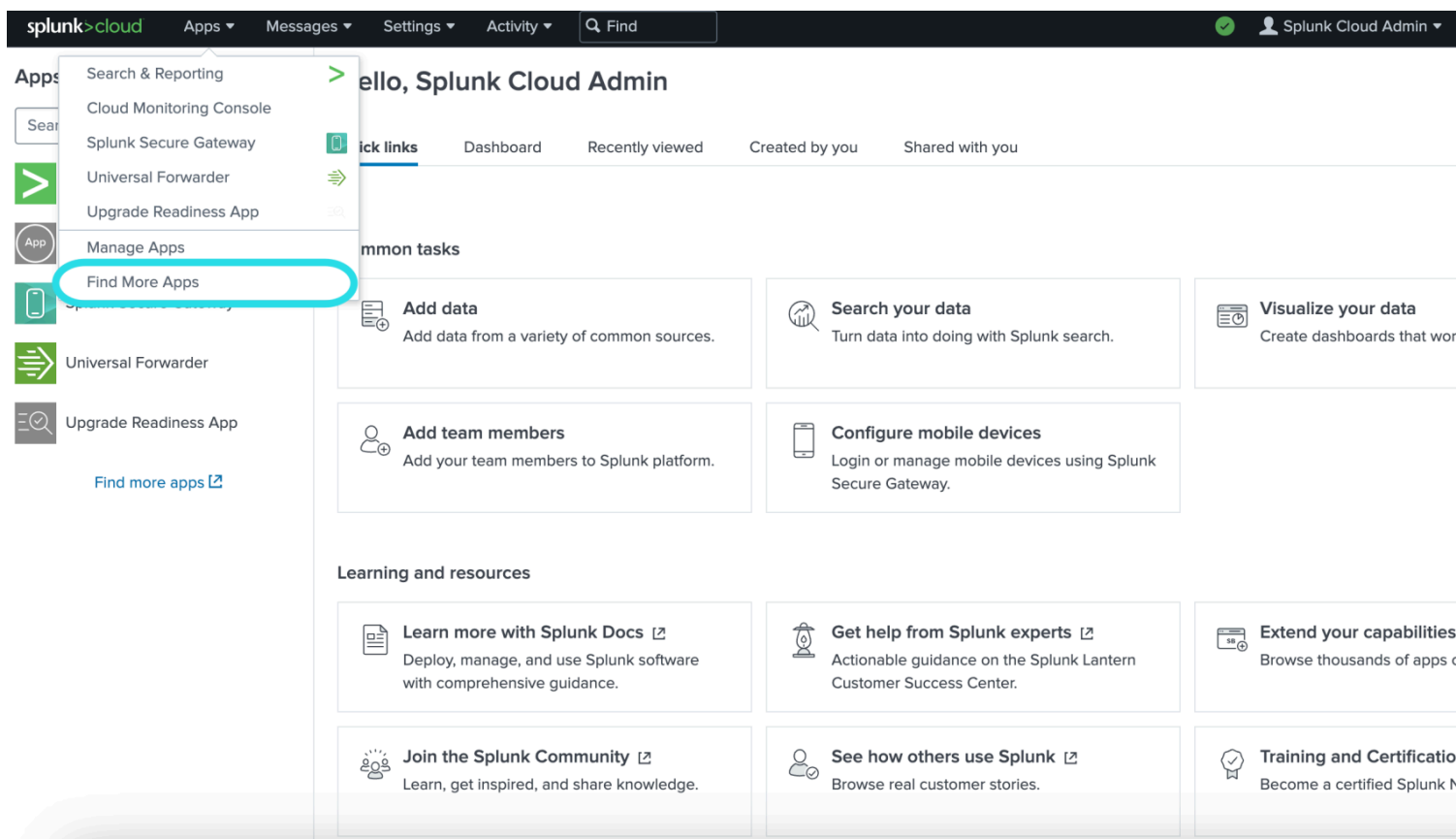
El único campo requerido para la creación del índice es **Nombre del Índice**. Los campos restantes se pueden ajustar según sea necesario.

4. Cuando hayas terminado, selecciona **Guardar**.

Instala la aplicación Bitwarden de Splunk

Después de que se haya creado tu índice de Bitwarden, navega a tu panel de control de Splunk.

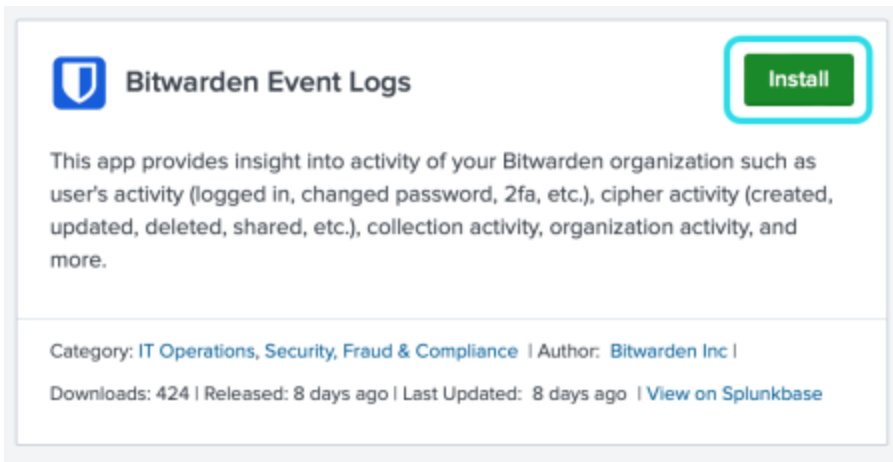
1. Abre el menú desplegable de **Aplicaciones** y selecciona **Buscar Más Aplicaciones**.



Tablero de aplicaciones de Splunk

2. Seleccione **Explorar más aplicaciones** ubicado en la parte superior derecha de la pantalla.

3. Buscar **Bitwarden Event Logs** en el catálogo de la aplicación. Seleccione **Instalar** para la aplicación **Bitwarden Event Logs**.



The screenshot shows the app listing for 'Bitwarden Event Logs' on Splunkbase. It features the Bitwarden logo, an 'Install' button, a description of the app's functionality, and metadata such as category, author, and download statistics.

Bitwarden Event Logs Install

This app 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.

Category: [IT Operations, Security, Fraud & Compliance](#) | Author: [Bitwarden Inc](#) |

Downloads: 424 | Released: 8 days ago | Last Updated: 8 days ago | [View on Splunkbase](#)

Aplicación de registros de eventos de Bitwarden

4. Para completar la instalación, necesitará ingresar a su cuenta de [Splunk](#) . Tu cuenta de Splunk puede que no sea la misma que las credenciales utilizadas para acceder a tu portal de Splunk.

Login and Install ✕

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

[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](#).

Inicie sesión e instale la aplicación Bitwarden en Splunk.

5. Después de haber ingresado su información, seleccione **Aceptar e Instalar**.

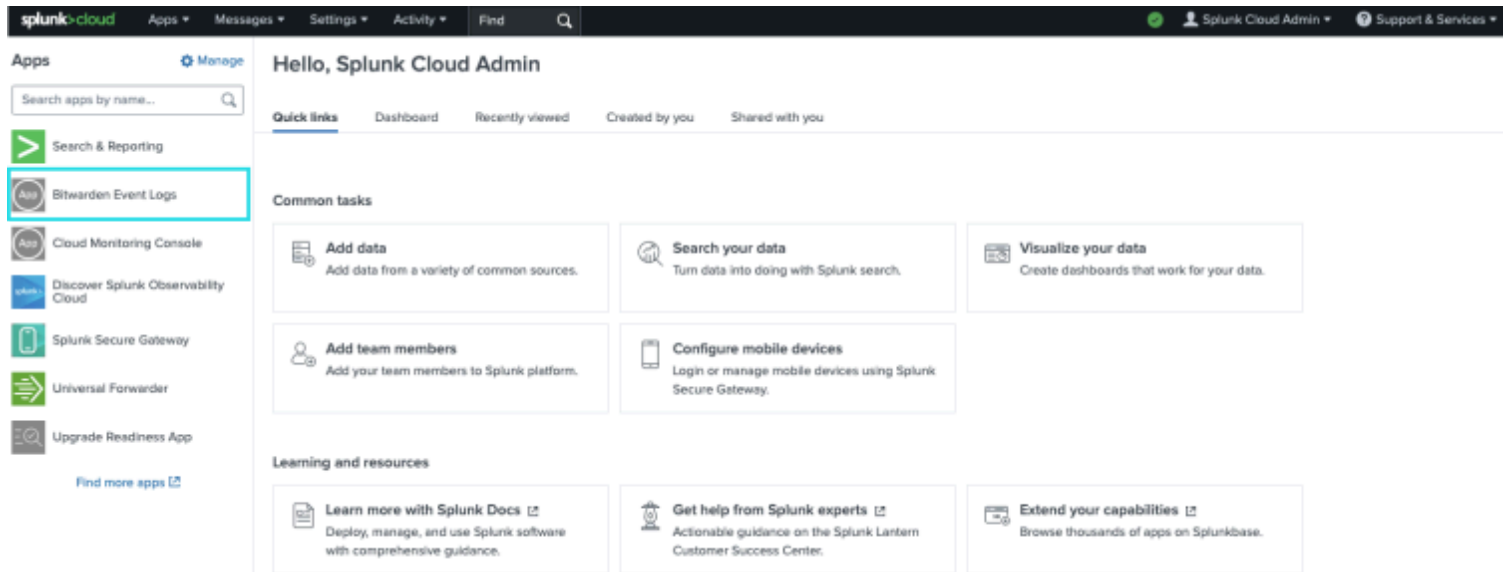
Note

Después de descargar la aplicación Bitwarden Event Logs, es posible que debas reiniciar Splunk.

Conecta tu organización Bitwarden

Una vez que la aplicación Bitwarden Event Logs ha sido instalada en su instancia de Splunk Empresa, puede conectar su organización Bitwarden usando su clave de Bitwarden [API](#).

1. Ve al inicio del panel de control y selecciona la aplicación **Bitwarden Event Logs**:



Bitwarden en el tablero de Splunk

2. A continuación, en la página de configuración de la aplicación, seleccione **Continuar a la página de configuración de la aplicación**. Este es el lugar donde agregarás la información de tu organización Bitwarden.

Search Dashboards ▾ **Setup**

Setup

Enter the information below to complete setup.

Your API key can be found in the Bitwarden organization admin console.

Client Id

Client Secret

Choose a Splunk index for the Bitwarden event logs.


Index

Self-hosted Bitwarden servers may need to reconfigure their installation's URL.

Server URL

Choose the earliest Bitwarden event date to retrieve (Default is 1 year).

This is intended to be set only on first time setup. Make sure you have no other Bitwarden events to avoid duplications.

Start date (optional)
 

Configura el menú de Bitwarden

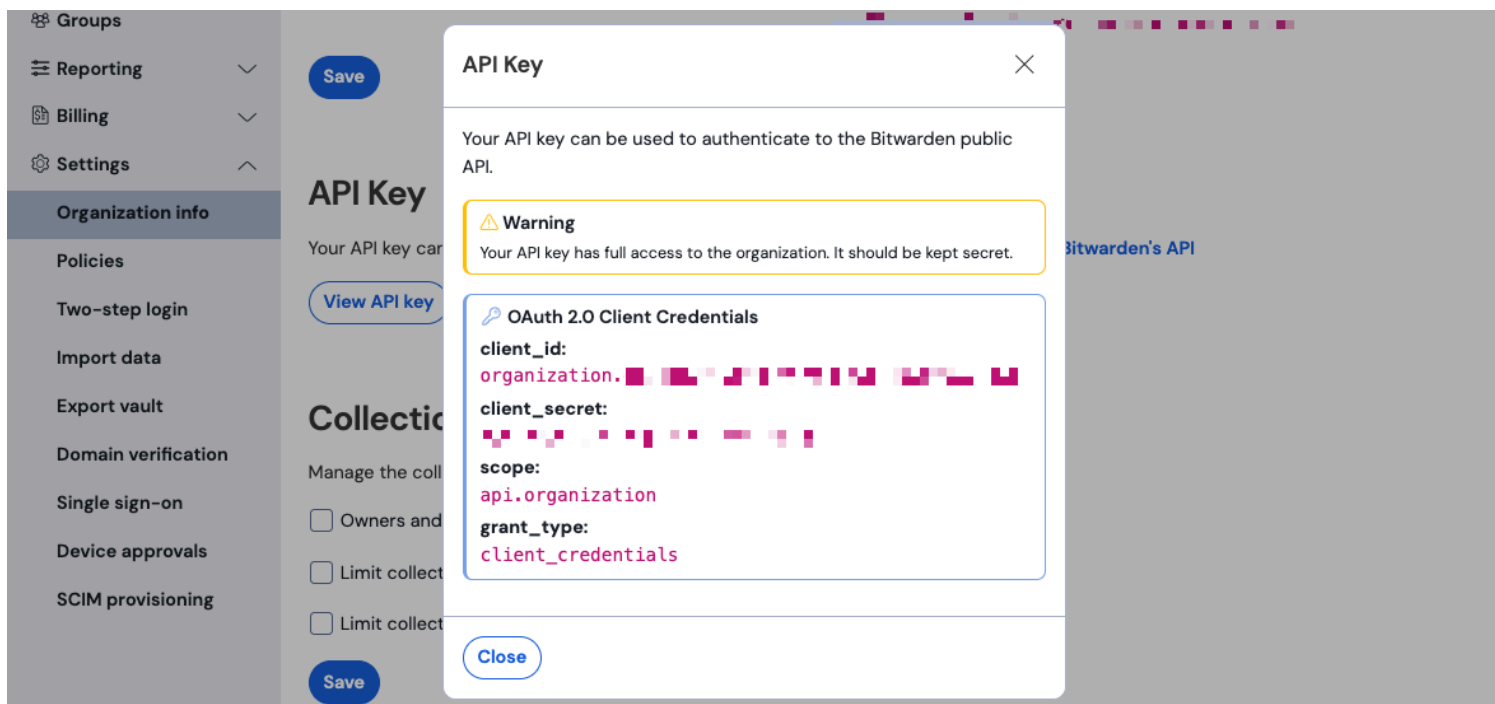
- Mantén esta pantalla abierta, en otra pestaña, inicia sesión en la aplicación web de Bitwarden y abre la Consola de Administrador utilizando el conmutador de producto :

The screenshot displays the Bitwarden web interface. On the left is a dark blue sidebar with navigation items: Password Manager, Vaults, Send, Tools, Reports, and Settings. The main content area is titled 'All vaults' and features a 'FILTERS' panel on the left and a list of vaults on the right. The 'FILTERS' panel includes a search bar and categories like 'All vaults', 'All items', 'Folders', 'Collections', and 'Trash'. A red box highlights the 'Password Manager' option in the sidebar, and a red arrow points to the 'Default collection' option in the filters menu. The vaults list has columns for 'Name' and 'Owner'.

<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...	⋮

Selector de producto

4. Navegue a la pantalla de **Ajustes** → **Información de la organización** de su organización y seleccione el botón **Ver clave API**. Se le pedirá que vuelva a ingresar su contraseña maestra para acceder a la información de su clave API.



Información de API de la organización

5. Copia y pega los valores de `client_id` y `client_secret` en sus respectivas ubicaciones en la página de configuración de Splunk.

Complete los siguientes campos adicionales también:

Campo	Valor
Índice	Seleccione el índice que se creó anteriormente en la guía: <code>bitwarden_events</code> .
Server URL	Para los usuarios de Bitwarden autoalojado, ingrese su URL autoalojada. Para las organizaciones alojadas en la nube, use la URL <code>https://bitwarden.com</code> .
Fecha de inicio (opcional)	Establezca una fecha de inicio para la monitorización de datos. Cuando no se establece, la fecha predeterminada se ajustará a 1 año. Esta es una configuración única, una vez establecida, este ajuste no puede ser cambiado.

Warning

La clave API de su organización permite el acceso completo a su organización. Mantén tu clave de API en privado. Si cree que su clave API ha sido comprometida, seleccione **Ajustes > Información de la organización > Botón Rotar clave API** en esta pantalla. Las implementaciones activas de su clave API actual necesitarán ser reconfiguradas con la nueva clave antes de usarla.

Una vez hecho, seleccione **Enviar**.

Entendiendo Buscar Macro

La macro de búsqueda `bitwarden_event_logs_index` se creará después de la instalación inicial de los registros de eventos de Bitwarden. Para acceder a la macro y ajustar los ajustes:

1. Abre los **Ajustes** en la barra de navegación superior. Luego, selecciona **Búsqueda Avanzada**.
2. Seleccione **Buscar Macros** para abrir la lista de macros de búsqueda.

Buscar permisos de macro

A continuación, configure qué roles de usuario tendrán permiso para usar la macro:

1. Ver macros seleccionando **Ajustes** → **Búsqueda Avanzada** → **Buscar macros**.
2. Seleccione **Permisos** en `bitwarden_events_logs_index`. Edita los siguientes permisos y selecciona Guardar una vez completado:

⇒**Splunk Cloud**

Object should appear in

This app only (bitwarden_event_logs)

All apps (system)

Permissions

Roles	Read	Write
Everyone	<input checked="" type="checkbox"/>	<input type="checkbox"/>
apps	<input type="checkbox"/>	<input type="checkbox"/>
can_delete	<input type="checkbox"/>	<input type="checkbox"/>
list_users_roles	<input type="checkbox"/>	<input type="checkbox"/>
power	<input type="checkbox"/>	<input type="checkbox"/>
sc_admin	<input type="checkbox"/>	<input checked="" type="checkbox"/>
tokens_auth	<input type="checkbox"/>	<input type="checkbox"/>
user	<input type="checkbox"/>	<input type="checkbox"/>

Cancel **Save**

Buscar Permisos de Macro

⇒ Splunk Empresa

Object should appear in

- This app only (bitwarden_event_logs_beta)
- All apps (system)

Permissions

Roles	Read	Write
Everyone	<input checked="" type="checkbox"/>	<input type="checkbox"/>
admin	<input type="checkbox"/>	<input checked="" type="checkbox"/>
can_delete	<input type="checkbox"/>	<input type="checkbox"/>
power	<input type="checkbox"/>	<input type="checkbox"/>
splunk-system-role	<input type="checkbox"/>	<input type="checkbox"/>
user	<input type="checkbox"/>	<input type="checkbox"/>

Cancel

Save

Buscar Macro Permisos Empresa

Campo

El objeto debería aparecer en

Descripción

Para usar la macro en la búsqueda de eventos, selecciona **Solo esta aplicación**. La macro no se aplicará si se selecciona **Mantener privado**.

Permisos

Seleccione los permisos deseados para los roles de usuario con acceso de **Lectura y Escribir**.

Note

Solo una macro de búsqueda estará funcional en la aplicación en un momento dado.

Entendiendo los tableros de control

El Tablero proporcionará varias opciones para monitorear y visualizar los datos organizativos de Bitwarden. Las tres categorías principales de monitoreo de datos incluyen:

- Eventos de autenticación de Bitwarden
- Eventos de elementos de la caja fuerte de Bitwarden

- Eventos de la organización Bitwarden

Los datos mostrados en los tableros proporcionarán información y visualización para una amplia variedad de búsquedas. Las consultas más complejas se pueden completar seleccionando la pestaña **Buscar** en la parte superior del tablero.

Plazo de tiempo

Mientras se busca desde la página de **Buscar** o los **Tableros**, las búsquedas pueden ser designadas a un marco de tiempo específico.

The screenshot shows the Splunk Search interface. At the top, there is a navigation bar with 'splunk>cloud', 'Apps', 'Messages', 'Settings', 'Activity', and a search bar containing 'Find'. Below this, there are tabs for 'Search', 'Dashboards', and 'Setup'. The main search area contains the query 'sourcetype="bitwarden:events" type=*' and a time range filter set to 'Last 24 hours'. Below the search bar, there are options for 'No Event Sampling' and 'standard_perf (search default)'. A 'Search History' link is also visible. On the right side, there is a section titled 'Analyze Your Data with Table Views' with a 'Create Table View' button. Below this, there is a 'How to Search' section with links to 'Documentation' and 'Tutorial'.

Búsqueda de intervalo de tiempo en Splunk

Note

Para los usuarios locales, los siguientes plazos son compatibles para buscar en los registros de eventos de Bitwarden:

- Mes hasta la fecha
- Año hasta la fecha
- Semana pasada
- Semana laboral anterior
- Mes anterior
- Año anterior
- Últimos 30 días
- Todo el tiempo

Parámetros de consulta

Configura búsquedas específicas incluyendo consultas de buscar. Splunk utiliza su método de lenguaje de procesamiento de búsqueda (SPL) para buscar. Vea la [documentación de Splunk](#) para obtener detalles adicionales sobre las búsquedas.

Estructura de búsqueda:

Bash

```
search | commands1 arguments1 | commands2 arguments2 | ...
```

Un ejemplo de un objeto estándar de resultado de búsqueda:

```
Time      Event
-----
4/19/23   { [-]
2:03:29.265 PM  actingUserEmail:
                actingUserId:
                actingUserName:
                date:
                device:
                hash:
                ipAddress:
                type:
```

Objeto de resultado de búsqueda de Splunk

Los campos mostrados en el objeto de búsqueda estándar pueden incluirse en cualquier búsqueda específica. Esto incluye todos los siguientes valores:

Valor	Resultado de ejemplo
correo electrónico del usuario	El correo electrónico del usuario que realiza la acción.
idUsuarioActuando	Identificación única del usuario que realiza la acción.
nombreDeUsuarioActuante	Nombre del usuario que realiza una acción.
fecha	Fecha del evento mostrada en el formato AAAA-MM-DD HH:MM:SS .
dispositivo	Número numérico para identificar el dispositivo en el que se realizó la acción.

Valor	Resultado de ejemplo
hash	Splunk calculó el hash de datos. Aprende más sobre la integridad de los datos de Splunk aquí .
dirección IP	La dirección IP que realizó el evento.
correo electrónico del miembro	Correo electrónico del miembro de la organización al que se dirigió la acción.
id de miembro	Identificación única del miembro de la organización hacia el que se dirigió la acción.
nombre de miembro	Nombre del miembro de la organización al que se dirigió la acción.
tipo	El código de tipo de evento que representa el evento de la organización que ocurrió. Vea una lista completa de códigos de eventos con descripciones aquí .

Buscar todo:*Bash*

```
sourcetype="bitwarden:events" type=*
```

Filtrar resultados por un campo específico

En el siguiente ejemplo, la búsqueda está buscando `actingUserName` con un comodín `*` que mostrará todos los resultados con `actingUserName`.

Bash

```
sourcetype="bitwarden:events" actingUserName=*
```

El operador **AND** está implícito en las búsquedas de Splunk. La siguiente consulta buscará resultados que contengan un `tipo` específico Y `nombreDeUsuarioActuante`.

Bash

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

Incluye múltiples comandos separándolos con `|`. Lo siguiente mostrará resultados con el valor superior siendo `ipAddress`.

Bash

```
sourcetype="bitwarden:events" type=1115 actingUserName="John Doe" | top ipAddress
```

Recursos adicionales

Establecer roles de usuario

Gestionar los roles de los usuarios para permitir a las personas realizar tareas específicas. Para editar roles de usuario:

1. Abra el menú de **Ajustes** en la barra de navegación superior.
2. Seleccione **Usuarios** desde la esquina inferior derecha del menú.
3. Desde la pantalla de usuarios, localice al usuario para el que desea editar los permisos y seleccione **Editar**.

Splunk editar permisos de usuario

Desde esta pantalla, se pueden completar los detalles para el usuario. El permiso como **administrador**, **poder**, y **puede_eliminar** también se pueden asignar individualmente aquí.

Eliminar datos

Eliminar los datos de búsqueda de Bitwarden limpiando el índice con acceso SSH. Los datos pueden necesitar ser borrados en casos como cambiar la organización que se está monitoreando.

1. Acceda al directorio de Splunk y **detenga** los procesos de Splunk.
2. Limpia el índice **bitwarden_events** con la bandera **-index**. Por ejemplo:

Plain Text

```
splunk clean eventdata -index bitwarden_events
```

3. Reinicia los procesos de Splunk.

Solución de problemas

- Usuarios de Splunk Empresa, la aplicación registrará en: `/opt/splunk/var/log/splunk/bitwarden_event_logs.log`

Si está experimentando algún error, o la aplicación Bitwarden no está funcionando correctamente, los usuarios pueden verificar el archivo de registro para buscar errores o ver [la documentación de Spunk](#).