

管理者コンソール > レポート

Rapid7 SIEM

ヘルプセンターで表示:

<https://bitwarden.com/help/rapid7-siem/>

Rapid7 SIEM

Rapid7 is a security platform offering several ways to analyze vulnerabilities and threat data, such as security information and event management (SIEM). With the Rapid7 Bitwarden integration, developed by the team at Rapid7, organizations can monitor Bitwarden organization and [event](#) activity with the Bitwarden app on Rapid7's InsightConnect software.

Note

The Bitwarden plugin on InsightConnect is available for cloud and Insight Orchestrator users. This guide will demonstrate the cloud setup. For more information on Insight Orchestrator, see the Rapid7 documentation [here](#).

Setup

Create Rapid7 account

To start, you will need an account with Rapid7 with access to InsightConnect. Create an account on the [Rapid7](#) website.

Download the Bitwarden plugin

1. Access the InsightConnect dashboard.
2. On the navigation menu, select **SETTINGS** → **Plugins & Tools**.



RAPID7

insightConnect



HOME



DISCOVER



QUICK ACTIONS



WORKFLOWS



JOB



SETTINGS



Global Artifacts

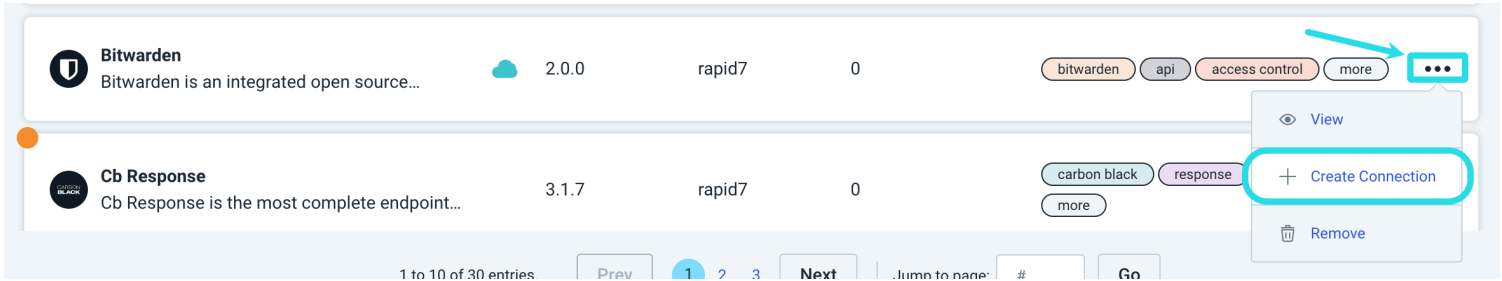
Orchestrators

Plugins & Tools

Triggers

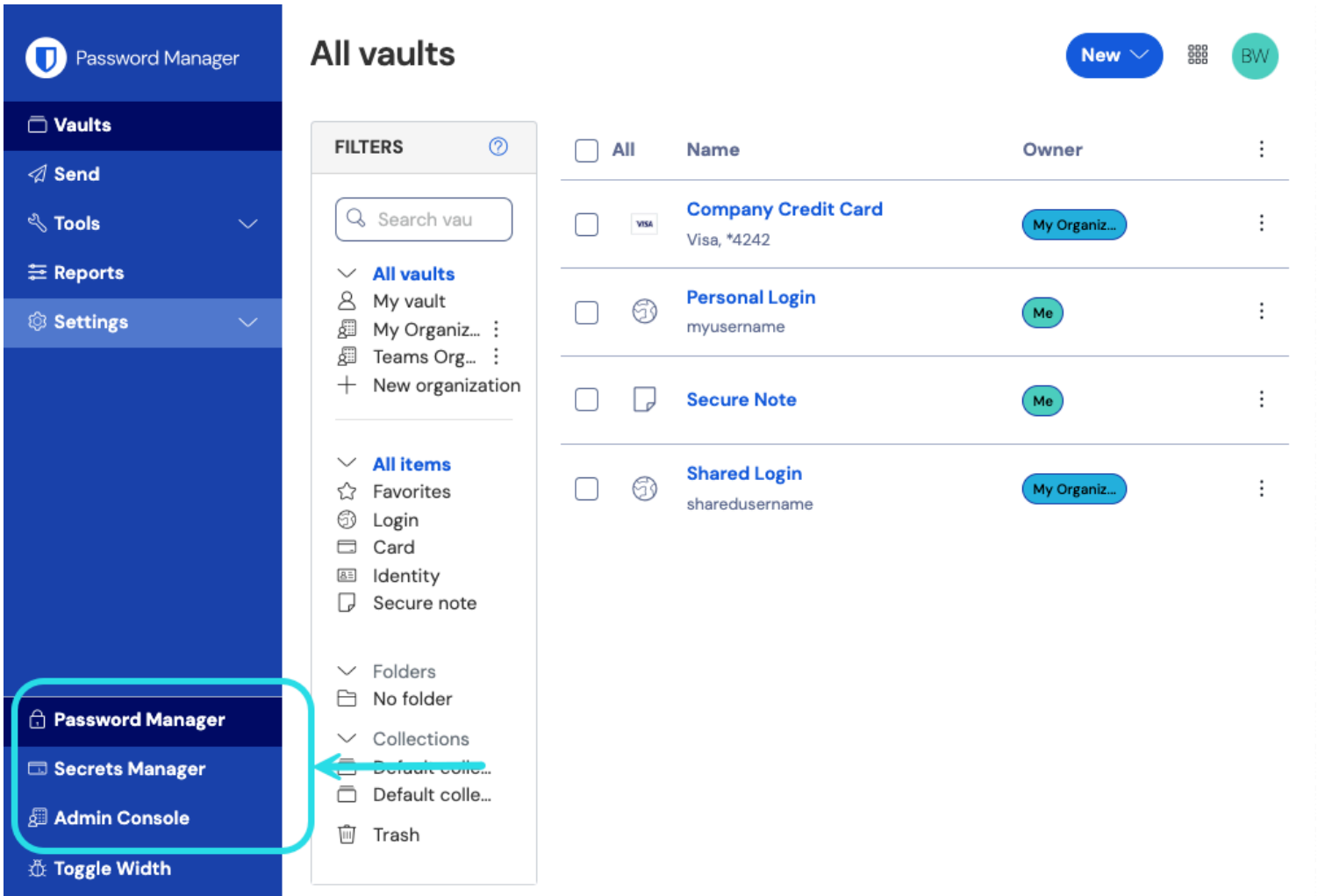
Rapid7 Plugins

3. Search **Bitwarden** in the Extension catalogue and install the plugin.
4. Return to your Extension library and select the Bitwarden plugin, then **+ Create Connection**. Keep the connection window open, information from the Bitwarden web vault is required to complete the next step.



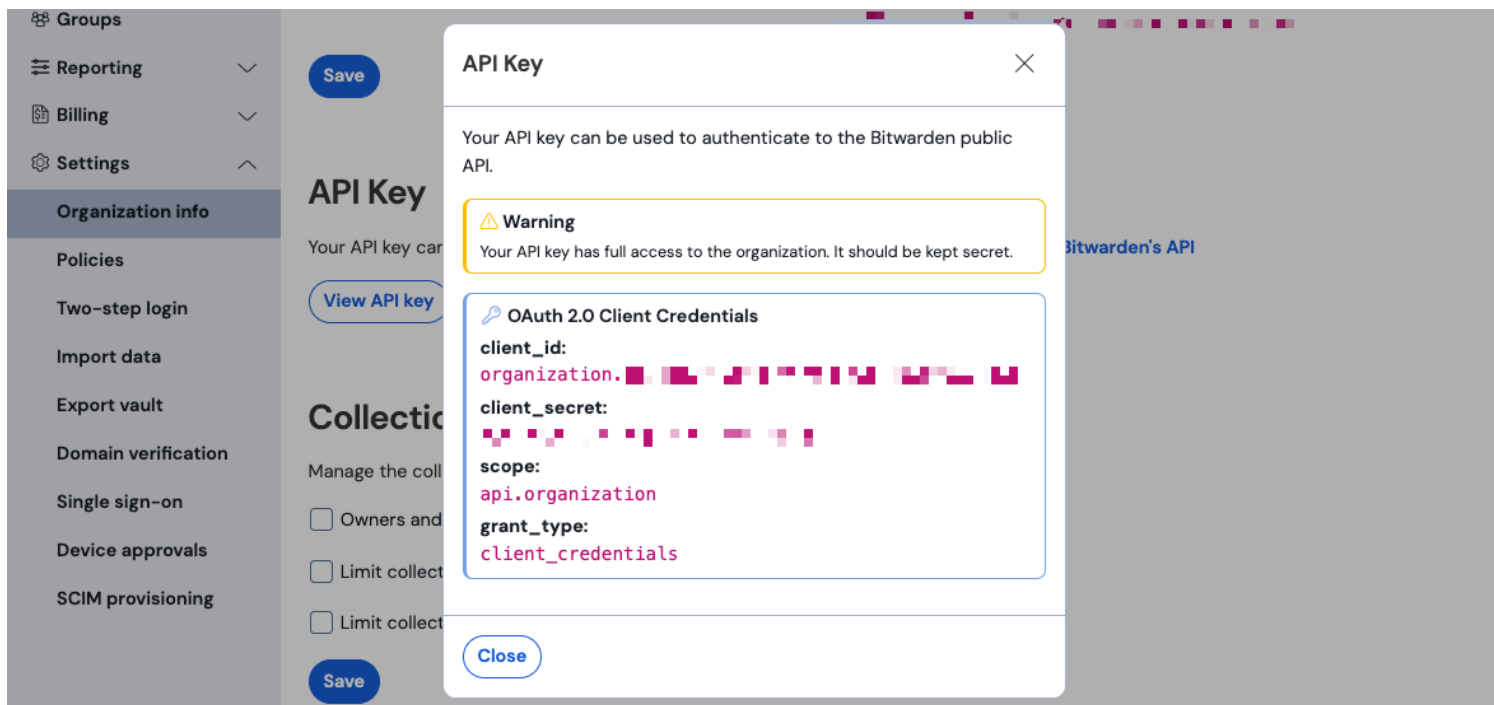
Bitwarden New Connection

5. In a new tab or window, access your Bitwarden organization's **Client ID** and **Client Secret**. Log in to the Bitwarden web app and open the Admin Console using the product switcher:



製品-スイッチャー

6. 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.



組織API情報

7. Copy the `client_id` and `client_secret` values. Return to the Create a Cloud Connection window:

1. Paste the `client_id` value into the **Client ID** field.
2. Paste the `client_secret` value into the **Client Secret** field. In order to access this field, select **Add Credential** from the **Select Credential** dropdown menu. Paste the `client_secret` value in the **Secret Key** field. Complete any additional Name and Description values you wish to include in the connection.

8. Once you have input the values, select **Save & Test Connection**. Rapid7 will run a connection test and indicate if the setup was successful.

Note

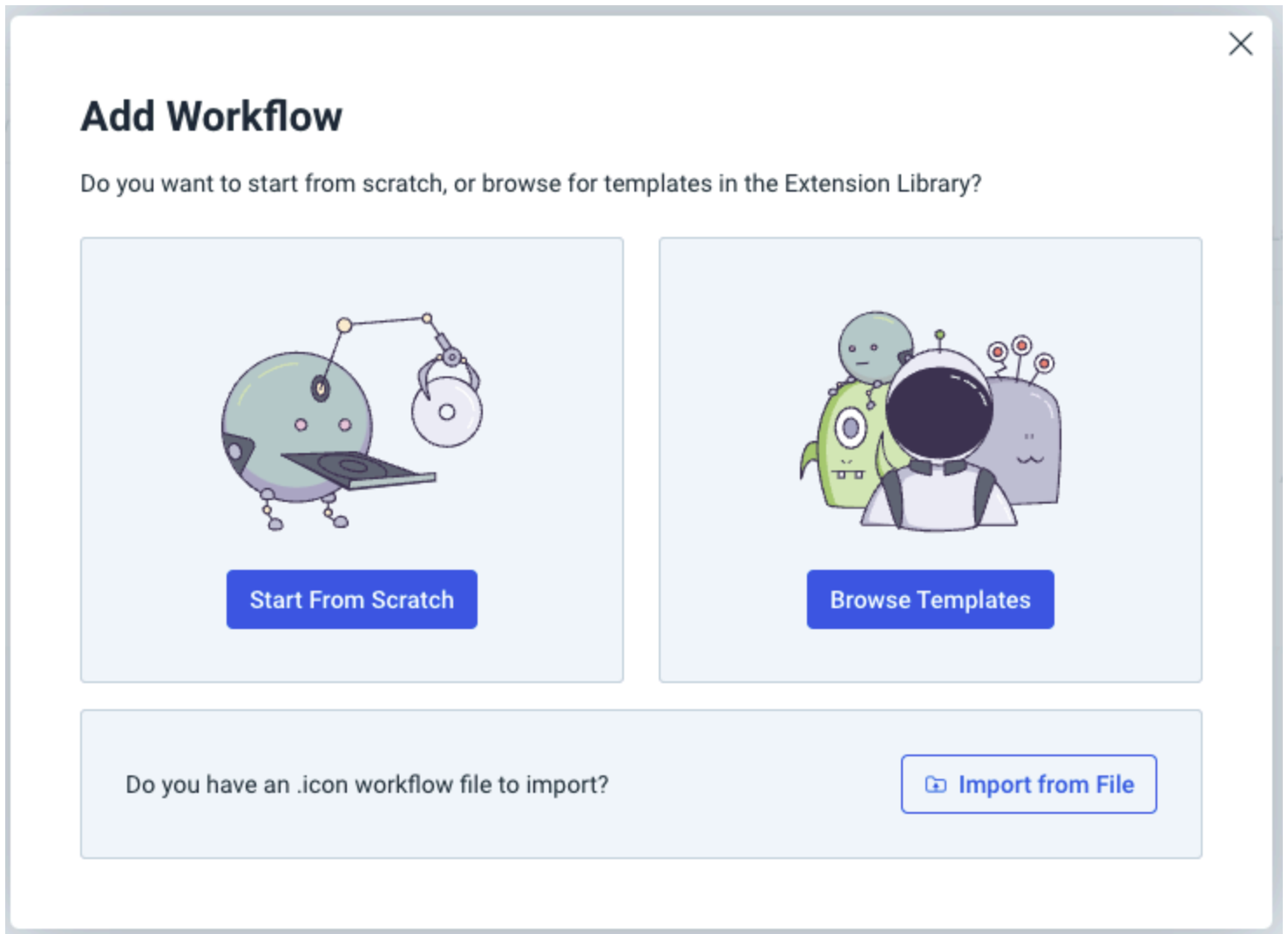
あなたの組織のAPIキー情報は、機密データです。これらの値を非セキュアな場所で共有しないでください。

Create a workflow

To begin monitoring data with Rapid7, create an InsightConnect workflow. This guide will demonstrate creating a cloud workflow and then testing the workflow.

1. On the main navigation, select **WORKFLOWS**.
2. In the right corner of the screen, select **Add Workflow** to begin.

3. A window will appear showing different options for creating a workflow. For this example, select **Start From Scratch**. Advanced users may choose to browse existing templates.



Add Workflow

4. On the Create New Workflow window, complete the following required fields:

1. **Workflow Name:** Create a name for the Workflow such as **Bitwarden Logs**.
2. **Time Savings:** Time that this Workflow will save.
3. **Optional:** Include Summary and Tags for the Workflow as desired.

5. Select **Create** once you have finished.

Create workflow trigger

1. Click on the new trigger in the workflow editor. In the Select a Trigger window, select the trigger you would like to use to initiate your workflow, such as **API Trigger**. Complete the following required fields:

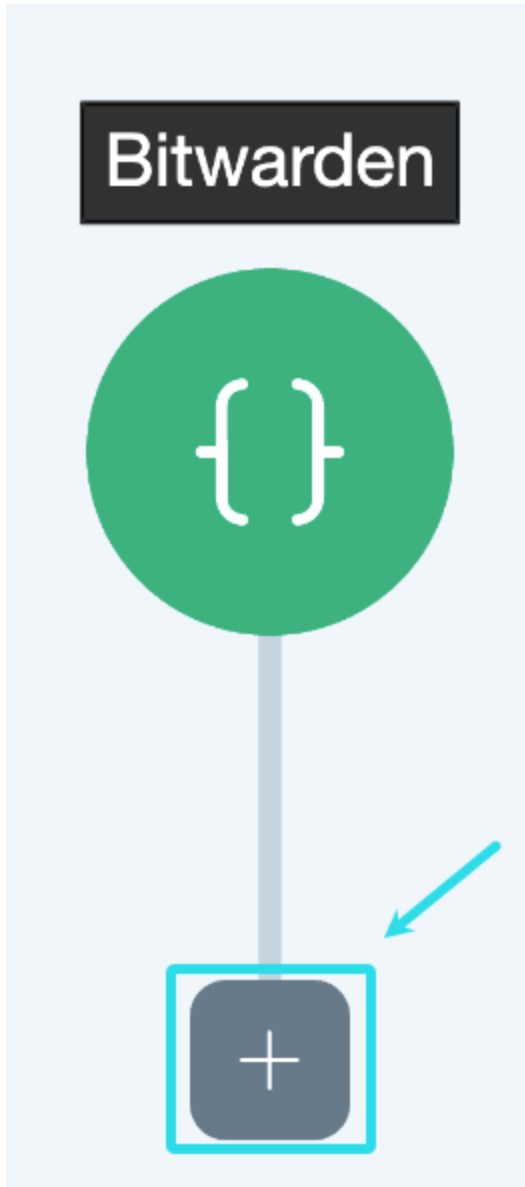
1. **Name:** Provide a name for the new trigger.

2. **Variable:** Choose variable such as **Event**.
3. **Data Type:** Select **String**.
4. **Optional:** Enter a Trigger Description to keep notes about the use of the trigger.

2. Select **Close** once you have completed the setup.

Add a workflow step

1. On the workflow editor, select the  plus icon to add a new step.



Add Step

2. Select **+** **Action** to add a new action. Select **Bitwarden** from the plugins list.


3. On the Select an Action screen, choose the action you wish to monitor. For this example, we will be selecting **List Events**. Select **Continue** once you have made your selection.

Select an Action ✕

Search Actions 🔍

- Create a Member**
Create a new member object by inviting a user to the ...
- Delete a Member**
Permanently delete a member from the organization. ...
- List All Collections**
Return a list of your organization's collections. Collec...
- List All Groups**
Return a list of your organization's groups. Group obj...
- List All Members**
Return a list of your organization's members. Membe...
- List Events**
Return a filtered list of your organization's event logs....
- Re-invite a Member**
Re-send the invitation email to an organization memb...
- Retrieve a Member**
Retrieve the details of an existing member of the org...
- Retrieve a Member's Group Ids**

[< Previous](#) [Continue >](#)



List Events Action

4. Choose the **Cloud** option for running. On the connection drop down, choose the Bitwarden connection we established previously in the guide. Select **Continue** once complete.
5. On the Configure Details screen, complete the optional fields as required by your setup, such as **Start Date**.
6. Select **Save Step** once you have customized the step details.

 **Note**

Rapid7 allows several actions to be created and chained together. You may repeat this step with additional Bitwarden actions to report more information. See a complete list of Bitwarden integration actions [here](#).

Test workflow

1. Return to the Workflow Editor and select **Test** to try out the workflow. The Test Workflow window will appear. Select **Test Workflow** at the bottom of the window to run the process.
2. This may take a moment. Once complete, a Job Details window will appear with results of the workflow:

The screenshot shows the 'Events' page in Bitwarden. At the top, there are tabs for 'Input', 'Output', 'Log', and 'Information', with 'Output' selected. Below the tabs, there is a '▼ Object (2)' section with a 'Download' and 'Copy' button. The object contains a '\$success: true' field and an 'events [16]' array. The first three events are expanded, showing details like 'actingUserId', 'date', 'device', 'ipAddress', 'object', and 'type'. The first event has a type of 1000, the second has a type of 1602, and the third has a type of 1602. The fourth event is partially visible with a type of 7.

Rapid7 Event Output

Enable workflow

1. To enable the workflow, select **WORKFLOWS** from the primary navigation.
2. Activate the workflow by using the toggle option:

The screenshot shows the Bitwarden workflow management interface. On the left, there is a toggle switch for 'Bitwarden' which is currently turned on, highlighted with a red box and a red arrow. To the right, there is a table with columns for 'Name', 'Created By', 'Created At', 'Status', and 'Count'. The table shows one workflow named 'Bitwarden' created by 'Mat McCabe' on 'Aug 20, 2024' with a status of 'On' and a count of '2'. On the far right, there is a vertical list of workflow categories: 'Alerting & Notifications', 'Cloud Security', 'Endpoint Detection & Response', 'Identity & Access Management', and 'Vulnerability Management'.

Enable Workflow

3. Once active, reports will be generated based on the trigger settings established on your workflow. View these reports by selecting **JOBS** on the navigation.

insightConnect

- HOME
- DISCOVER
- QUICK ACTIONS
- WORKFLOWS
- JOB** JOBS
- SETTINGS
- HELP & LEARNING

Jobs

Date Range: All | Workflow: All | Assignee: All | Tags: All

Running | Decision Required | Finished | Failed

Bitwarden
Aug 29, 2024 11:03:50 AM | Assignee: Unassigned

Alerting & Notifications | Cloud Security | Finished

Endpoint Detection & Response

Identity & Access Management | more

[View](#)

Bitwarden
Aug 29, 2024 11:00:43 AM | Assignee: Unassigned

Alerting & Notifications | Cloud Security | Finished

Endpoint Detection & Response

Identity & Access Management | more

View Rapid7 Jobs