D bit warden Help Center Article

ADMIN CONSOLE > RAPPORTERING >

Rapid7 SIEM

View in the help center: 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.

(i) 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.

III RAPID

insight Connect



DISCOVER











Global Artifacts

Orchestrators

Plugins & Tools

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.

0	Bitwarden Bitwarden is an integrated open source	2.0.0	rapid7	0	bitwarden api acces	s control more
	Cb Response Cb Response is the most complete endpoint	3.1.7	rapid7	0	carbon black response	+ Create Connection
	1 to 10 of 30 e	ntries Prev	1 2 3		n nage: # Go	III Remove

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:

Password Manager	All vaults			New V	BW
🗇 Vaults			N	0	
🖉 Send			Name	Owner	:
\ll Tools \sim	Q Search vau	ASIV	Company Credit Card Visa, *4242	My Organiz	:
₩ Reports	✓ All vaults		Personal Login		
🕸 Settings 🛛 🗸 🗸	A My Vault	0 6	myusername	Me	:
	 Teams Org : + New organization 		Secure Note	Me	:
	 ✓ All items ☆ Favorites ۞ Login □ Card □ Identity □ Secure note 		Shared Login sharedusername	My Organiz	i
 Password Manager Secrets Manager Admin Console Toggle Width 	 Folders No folder Collections Default colle Default colle Trash 				

Product switcher

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.

器 Groups		
₩ Reporting	Save	API Key ×
🗟 Billing 🗸 🗸	_	
Settings		Your API key can be used to authenticate to the Bitwarden public API.
Organization info	Анксу	∆ Warning
Policies	Your API key car	Your API key has full access to the organization. It should be kept secret.
Two-step login	View API key	OAuth 2.0 Client Credentials
Import data		client_id: organization.
Export vault	Collectio	client_secret:
Domain verification	Manage the coll	scope:
Single sign-on	Owners and	api.organization grant_type:
Device approvals	Limit collect	client_credentials
SCIM provisioning	Limit collect	
	Save	Close

Organization api info

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.

(i) Note

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

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.





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 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 \pm 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 with to monitor. For this example, we will be selecting **List Events**. Select **Continue** once you have made your selection.

	Select an Action $\qquad \qquad \qquad$					
	Sear	ch Actions Q				
	0	Create a Member Create a new member object by inviting a user to the				
-	0	Delete a Member Permanently delete a member from the organization	_			
-	0	List All Collections Return a list of your organization's collections. Collec	_			
	0	List All Groups Return a list of your organization's groups. Group obj				
	0	List All Members Return a list of your organization's members. Membe				
	\bigcirc	List Events Return a filtered list of your organization's event logs]			
	0	Re-invite a Member Re-send the invitation email to an organization memb				
	0	Retrieve a Member Retrieve the details of an existing member of the org				
	< Previ	Retrieve a Member's Group Ids				
		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.

(i) 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:

Säker och pålitlig lösenordshanterare med öppen källkod för företag

nnut	Output	Log	Information	
nput	output	LUg	monnation	
🔻 Obj	ect (2)			⊥ Download 🛛 Copy
\$:	success : true	9		
▼ e	/ents [16]			
►	0 (6)			
►	1 (6)			
•	2 (6)			
	actingUse	rld :		
	date : 202	4-		
	device :			
	ipAddress	: 🔳 📕	-	
	object : ev	vent		
	type : 100	0		
•	3 (6)			
	actingUse	erld :		
	date : 202	4-		
	device :			
	ipAddress		-	
	abject : ov	ent		
	object . ev			

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:

Mat McC	Cabe Aug 20, 2024	2	0	Alerting & Notifications Cloud Security Endpoint Detection & Response Identity & Access Management 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.

Säker och pålitlig lösenordshanterare med öppen källkod för företag

insigh	ntConnect	
\bigcirc	HOME	< Jobs
Q	DISCOVER	Date Range: All ∨ Workflow: All ∨ Assignee: All ∨ Tags: All ∨
Ŕ	QUICK ACTIONS	Running Decision Required Finished A Failed
لى ا	WORKFLOWS	
٦	JOBS	Bitwarden
Φ	SETTINGS ~	Aug 29, 2024 11:03:50 AM Assignee: Unassigned Alerting & Notifications Cloud Security Finished Endpoint Detection & Response (Identity & Access Management more
?	HELP & LEARNING	
		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