CONSOLA DE ADMINISTRADOR > GESTIÓN DE USUARIOS >

# **Ping Identity SCIM Integration**

Ver en el centro de ayuda: https://bitwarden.com/help/ping-identity-scim-integration/

### **Ping Identity SCIM Integration**

System for cross-domain identity management (SCIM) can be used to automatically provision and de-provision members and groups in your Bitwarden organization.

### (i) Note

Las integraciones SCIM están disponibles para **organizaciones de Empresa**. Las organizaciones de Equipos, o los clientes que no utilizan un proveedor de identidad compatible con SCIM, pueden considerar el uso de Conector de Directorio como un medio alternativo de aprovisionamiento.

This article will help you configure a SCIM integration with Ping Identity. Configuration involves working simultaneously with the Bitwarden web vault and Ping Identity Administrator dashboard. As you proceed, we recommend having both readily available and completing steps in the order they are documented.

### **Enable SCIM**

(i) Note ¿Estás autoalojando Bitwarden? Si es así, complete estos pasos para habilitar SCIM para su servidor antes de continuar.

To start your SCIM integration, open the Admin Console and navigate to **Settings** → **SCIM provisioning**:

<b>D bit</b> warden	SCIM provisioning	
${\ensuremath{\boxtimes}}$ My Organization $~~ \lor$	Automatically provision users and groups with your preferred identity provider via SCIM provisioning	
Collections	Enable SCIM	
A Members	Set up your preferred identity provider by configuring the URL and SCIM API Key	
뿅 Groups		
$ arrow  ext{Reporting}  \lor$	C SCIM API key	
🗄 Billing $\checkmark$		◎ ᢗ 🗋
Settings	This API key has access to manage users within your organization. It should be kept secret.	
Organization info	Save	
Policies		
Two-step login		
Import data		
Export vault		
Domain verification		
Single sign-on		
Device approvals		
SCIM provisioning		
	Aprovisionamiento de SCIM	

Select the Enable SCIM checkbox and take note of your SCIM URL and SCIM API Key. You will need to use both values in a later step.

### **Create a SCIM app**

1. Navigate to provisioning  $\oplus$  **New Connection**.

• Getting Started	Provisioning 🕕
Overview	Administrators can manage their provisioning connections. A connection contains configuration that tells PingOne how to connect to an external resource for the purpose of provisioning user to that resource. Learn More
ル Monitoring 🗸	Rules Connections
🐣 Directory 🔹	0
Applications -	
	0 Connections by Name -
<ul> <li>Authentication •</li> </ul>	
★ Threat Protection ★	
💉 Integrations 🔶	
External IdPs	
Provisioning	

Ping Identity new Connection

2. In the Create a New Connection window, choose the Select option for Identity Store.

3. In the Identity Store, enter SCIM into the search box and select SCIM Outbound. Once this step is complete, select Next.



SCIM Connection

4. Input a Name and Description for the SCIM connection.

- 5. Next, you will be required to input the SCIM BASE URL. Copy the SCIM URL value located on the Enable SCIM page in the Bitwarden Admin Console and paste it into this field.
- 6. Using the Authentication Method dropdown menu, select OAuth 2 Bearer Token. A field will appear named Oauth Access Token, paste the SCIM API key value from the Bitwarden Admin Console into this field.

 $\times$ 





Specify the authentication configuration for the connection.

### **Configure Authentication**

SCIM BASE URL *	Users Resource		
https://vault.bitwarden.pw/scim/v2/		/Users	
SCIM version		Groups Resource	
2.0	•	/Groups	
Authentication Method			
OAuth 2 Bearer Token	•		
Oauth Access Token *			
•••••	Ø		
Auth Tura Haadar			
Auth Type Header			
Bearer	•		

Previous

Cancel

Test Connection

Next

Ping Identity SCIM connection test

7. Once setup is complete, you may select Test Connection. If successful, select Next.

8. On the **Configure Preferences** page, select desired preferences and actions.

#### (i) Note

Setting the Remove Action setting to **Disable** will result in Bitwarden users being moved to **Revoked** status rather if the user fails to meet the filter criteria set on Ping Identity. Restoring the criteria will return the user to their **previous** state.

If the Remove Action is set to Delete, the same action will deprovision the user.

9. Select Save once complete. Select the newly created Connection and enable the Connection using the toggle.



Enable Ping Identity Connection

### **Create a Rule**

Before syncing user groups and directories, a Rule is required to sync the user groups to Bitwarden SCIM.

- 1. Return to the Provisioning Screen.
- 2. Select the **Rules** tab and then  $\oplus$  **New Rule**.
- 3. Enter an app specific name for the Rule and select Create Rule.
- 4. Edit the new Rule in the Configuration tab. Select Bitwarden SCIM connection and then Save.



Ping Identity Rule

5. Select the Configuration tab and add a 2 User Filter. For more information, see the Ping Identity documentation. Select Save once complete.

Bitwarden Rule > Edit User Filter				×
User Filter				
Edit the user filter to change how users are selected for provisioning.				_
All Any of the conditions are true			(Add+	)
Attribute Email Address	•	Operator Equals	Value @my-company.com	
		0	Nelse .	
Country Code	-	Equals	US	Î

Ping Identity User Filter

6. Enable the Rule using the toggle.





2. Choose the group or groups to provision and select Save. Once saved, the directory will trigger a sync.

### Appendix

#### **Required attributes**

Both the Bitwarden and Ping Identity **SCIM Provisioner with SAML (SCIM v2 Enterprise)** applications use standard SCIM v2 attribute names. Bitwarden will use the following attributes:

#### User attributes

- active
- emails<sup>a</sup> or userName
- displayName
- externalId

<sup>a</sup> - Because SCIM allows users to have multiple email addresses expressed as an array of objects, Bitwarden will use the value of the object which contains "primary": true.

#### **Group attributes**

For each group, Bitwarden will use the following attributes:

- displayName (required)
- members<sup>a</sup>
- externalId

<sup>a</sup> - members is an array of objects, each object representing a user in that group.