

Hibob

How do I link my Hibob account?

Overview

To authenticate Hibob using a Service Account, you will need to provide the following information:

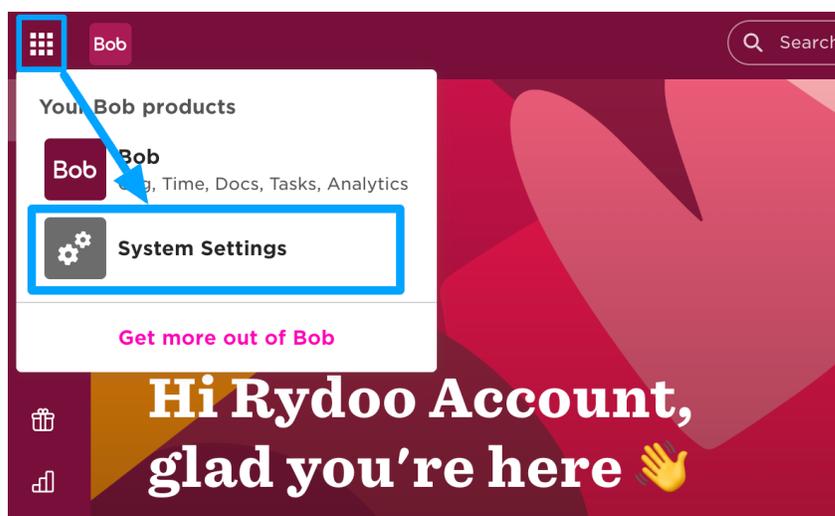
- Service Account User ID
- Service Account Token

Prerequisites

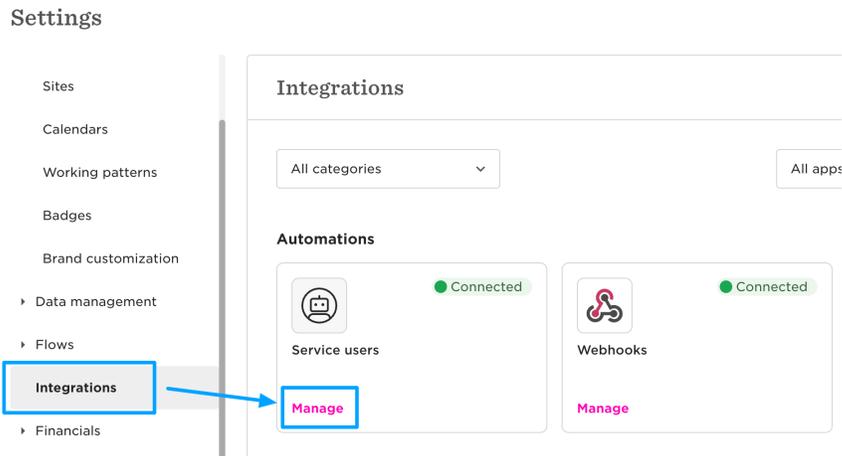
- Please ensure you fulfill all the requirements to set up the integration:
- You have Administrator permissions in your company's Hibob instance

Step 1: Create the Service User in your Hibob Account

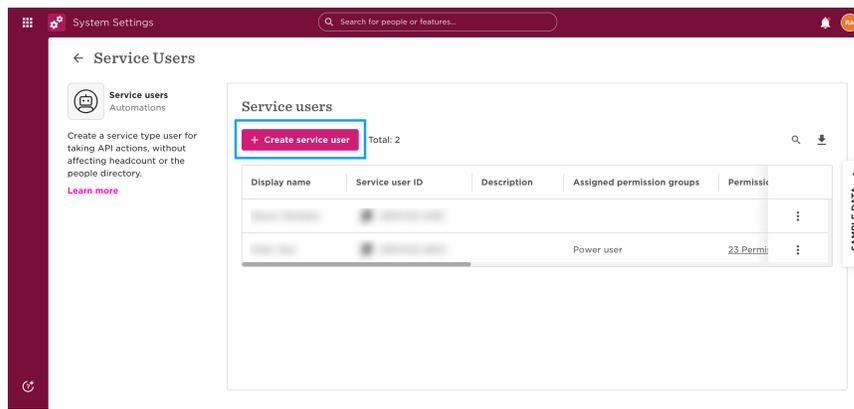
1. Navigate to your Hibob System Settings



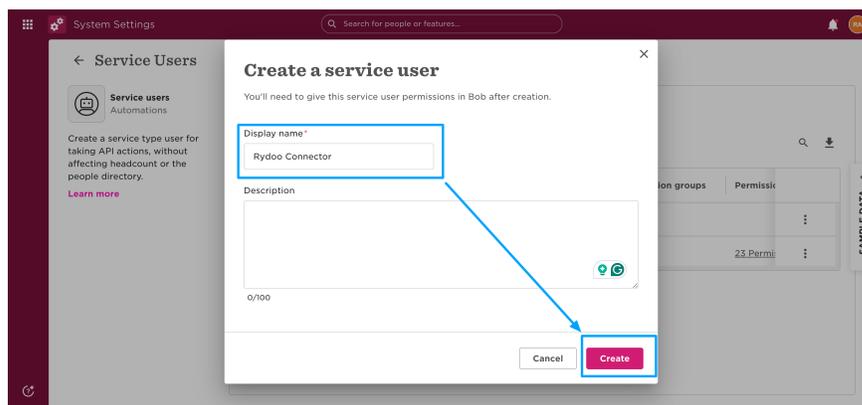
2. On the Settings screen, open **Integrations** and click **Manage** on the **Service users** tile



3. Click on **Create service user**



4. Enter **Display Name** and click **Create**



5. On the next screen, Hibob display the credentials for your new service user. Make a note of both the **ID** and the **Token**, then click on **Go to permission groups** and proceed with the next step

Service user info [Close]

Credentials

ID
SERVICE-2 [Copy]

Token
cR [Copy]

⚠ These details can give someone permanent access to your company's account. Don't share them with a third party. For security, these credentials won't be available after you close this window.

Permissions

We recommend giving this service user the permissions they need by adding them to a dedicated permission group.

[Go to permission groups]

[Done]

Step 2: Create a Permission Group

1. Click **Add permission group**, then **Service user**

System Settings [Search for people or features...]

Settings

- Company
- Data management
- Flows
- Integrations
- Financials
- Account
- Permission groups**
- Feature management
- Access
- API audit

Permission groups
Manage access to features and people's data.

[+ Create permission group] Total: 7 [Search]

Employee	User type	Type
Admins	Admin	Out of the box
Managers	Manager	Out of the box
All people – own data	Employee	Out of the box
All people – others' data	Employee	Out of the box

2. Enter any **Group name**, select your new service user under **Select service users** and click **Create**

Create service user permission group ×

Group name* Tags

Description

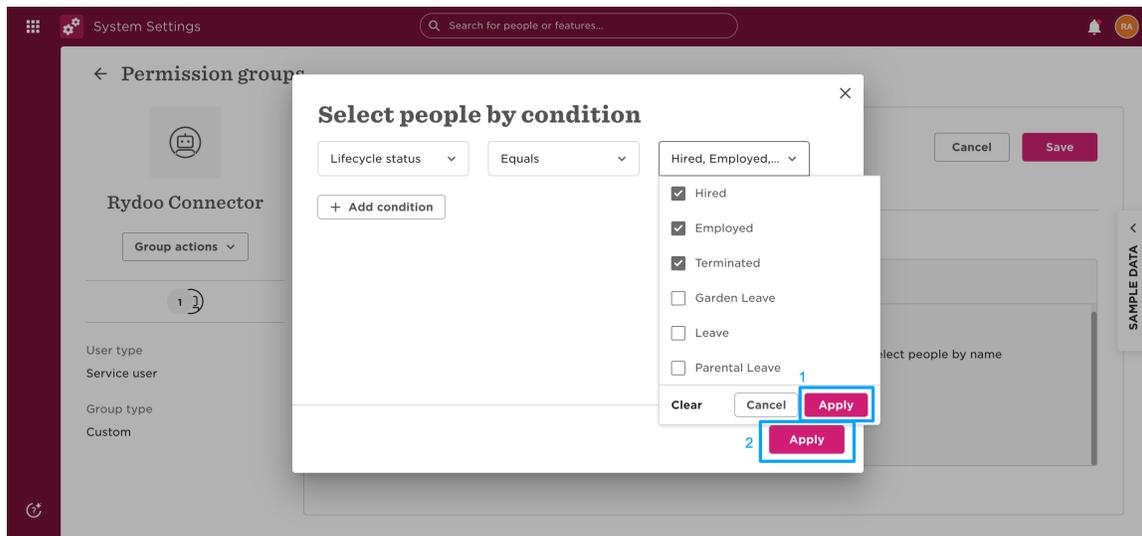
Members

Select service users*

3. When asked to confirm the changes, click **Confirm**
4. Switch to the **People's data** tab of the new Permission Group, pick "Select people by condition" under **Whose data can members access?**, then click on **Edit** to select the people the integration can access

The screenshot shows the 'System Settings' interface. On the left, there is a sidebar for 'Rydo Connector' with a 'Group actions' dropdown and a '1' icon. The main area is titled 'Permission groups' and contains a search bar for permissions, 'Cancel' and 'Save' buttons, and a 'Features' section with 'People's data' selected. Below this, there is a section for 'Access data for' with a list of features: Benefits, Docs, Import, and People. The 'Access data for' section is expanded, showing 'Whose data can members access?' with three radio button options: 'Everyone', 'Select people by condition' (which is selected), and 'Select people by name'. Below these options, there is an 'Edit' button, a count of '46' with a circular progress indicator, and the text '46 Employees'. A 'Lifecycle status equals Employed' filter is also visible. On the right side of the main area, there is a vertical 'SAMPLE DATA' button.

5. In the **Select people by condition** pop-up, select all relevant **Lifecycle Statuses**. In most scenarios this will include *Hired*, *Employed*, and *Terminated*. Click Apply twice once done:



6. Back in the **People's Data** add the following permissions:

Please note the permissions below are the required permissions for the full HRIS API. You only need to configure the permissions based on your use case.

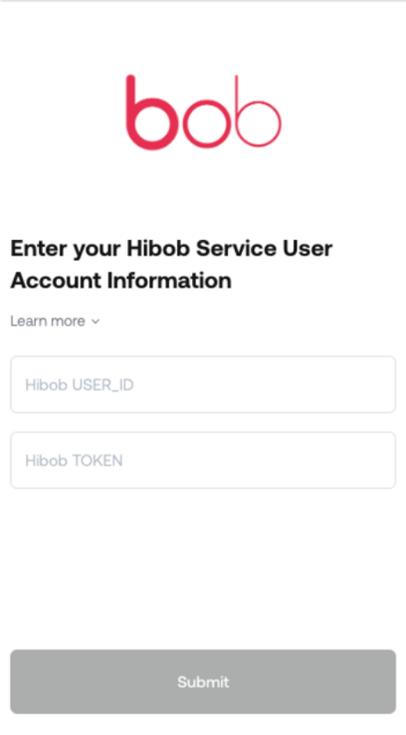
- a. **People > Basic Info**
View selected employees' Basic info sections (This is required to surface employees)
- b. **People > Employment**
View selected employees' Employment sections
View selected employees' Employment section histories
- c. **People > History**
View selected employees' profile changes history
- d. **People > Identification**
View selected employees' Identification sections
- e. **People > Lifecycle**
View selected employees' Lifecycle sections (This is needed to surface Employment Status)
View selected employees' Lifecycle section histories
- f. **People > Personal**
View selected employees' Personal sections
- g. **People > Personal contact details**
View selected employees' Personal contact details sections

- h. **People > Work**
View selected employees' Work sections
View selected employees' Work section history
- i. **People > Work contact details**
View selected employees' Work contact details sections

7. Once done adding the above permissions, finish creating the Permission Group by selecting Save

Step 3: Link your Hibob account

Copy and paste the Service Account User ID and Token created in part 1 into the linking flow



The screenshot shows a web form for linking a Hibob account. At the top is the Hibob logo in red. Below it is the heading "Enter your Hibob Service User Account Information" with a "Learn more" link and a dropdown arrow. There are two input fields: "Hibob USER_ID" and "Hibob TOKEN". At the bottom is a grey "Submit" button.

Notes

Hibob allows moving fields into categories other than those listed in the guide above. If some fields are missing after linking your Hibob account, view a sample employee in Hibob and confirm under which category (e.g. Personal, Work, About) the missing field can be found. Then add **View** permissions under **People's data** for that category as described above.

The account will be set up considering our default mapping as table below. If you wish to use different fields for mapping, provide the specific field names present in your BambooHR to your Customer Success Manager (CSM). This ensures the technical team can correctly remap the fields according to your requirements.

Hibob	Rydo
Site	Branch Name
Site	Branch ID
Division	Group Name
Division	Group ID