

Creating an Integration User with Minimal Access Rights for Valo.ai

Introduction

This document outlines the process for creating a Salesforce user account with the minimal access rights necessary for Valo.ai to connect to a Salesforce Org using a connected application.

Valo strongly suggests creating a dedicated user with an integration license for Valo.ai Salesforce integration. This section outlines the steps to create the user with minimized access rights, adhering to security best practices.

The process involves the following steps:

1. **Create a Permission Set:** Define specific permissions required for Valo.ai.
2. **Create a User:** Set up the user account with appropriate licensing and permission set assignment.
3. **Finalize User configuration:** Setup one time MFA and login credentials.
4. **Connect Valo to the Org:** Using the User created above
5. **Install Valo Connected App:** Allow the integration user to use Valo connected app
6. **Clone and Configure a Profile:** IP restriction requires a dedicated profile for the integration user

Step 1: Permission set setup

Create and Configure Valo Permission Set

1. Navigate to **Setup > Permission Sets** and Click **New**.
2. Name it (e.g., **Valo Connection User**).
3. Select **Salesforce API Integration** from the **License Setting** list
4. Click **Save**.
5. **Assign System Permissions:**
 - a. Navigate to **System Permissions** and click **Edit**.
 - b. Add or confirm the selection of **ALL** the required permissions listed below.
 - Approve Uninstalled Connected Apps
 - Customize Application
 - Manage Custom Permissions
 - Manage MFA in User Interface
 - Modify Metadata Through Metadata API Functions
 - View Developer Name
 - View Event Log Files
 - View Roles and Role Hierarchy
 - View Setup and Configuration
 - Assign Permission Sets
 - Freeze Users
 - Manage Internal Users
 - Manage IP Addresses
 - Manage Login Access Policies
 - Manage Password Policies
 - Manage Profiles and Permission Sets
 - Manage Roles
 - Manage Sharing
 - Manage Users
 - Monitor Login History
 - Reset User Passwords and Unlock Users
 - View All Profiles
 - View All Users

Save changes.

Step 2: User creation and permission assignment

Create the Valo Integration User

1. Navigate to **Setup > Users > Users**. Click **New User**.
2. **License and Profile**
 - **Create an Integration User**
 - **User License: Salesforce Integration**
 - **Profile: Use “Minimum Access - API Only Integrations”**
3. **Save** the user.

Assign Permission Set to the New User

1. Navigate to the newly created user's detail page.
2. Find the **Permission Set Assignments** section and click **Edit Assignments**.
3. Assign the **Valo Connection User** Permission Set.

Step 3: MFA setup and login credentials.

Configure login credentials Integration User

1. Ensure you have configured a strong and unique password for the user. Do this by copying the email link in an Incognito/Private browser or you will lose your current Salesforce session.
2. With the Integration User still selected, under **User Detail > Temporary Verification Code**: Select **Generate**.
3. Select 1 hour lifetime for the code. Generate it and **save it to a secure location for a later step**.

Step 4: Connect Valo to the org.

Note

When connecting Valo to your org, use a private browsing window or log out of other Salesforce accounts first.

1. Open a **Private/Incognito** browsing window.
2. Log in to the Valo user interface, use Valo's onboarding wizard or navigate to **Home > Add Org**.
3. Select your org type **Production/Sandbox**
4. When prompted by Salesforce, log in with the **Username and Password of the new integration user**. Enter the **Temporary Verification Code from Step 3** when prompted for MFA.
5. Click **"Allow"** when prompted for the OAuth scope.

Note

If you ever need to change this connected account, you can easily do so later using Valo's reauthentication feature.

Step 5: Connected App installation

Install the Valo Connected App (System Admin Required)

This step is required by Salesforce security policies.

1. **As a System Administrator**, navigate to Salesforce **Setup**.
2. Search for and select **"Connected Apps OAuth Usage"**.
3. Locate the **Valo.ai** app in the list.
4. Click **"Install"** behind the **"Load Actions"** button next to the Valo.ai app.
5. Go back to the **Valo Connection User** permission set created in Step 1. Remove the "Approve Uninstalled Connected Apps" system permission as it was only necessary for the installation process.

Step 6: Clone and configure a profile

Create & Configure the Valo Integration Profile

1. Navigate to **Setup > Profiles**.
2. **Clone** the **Profile** ([Minimum Access - API Only Integrations](#)).
3. Name the new profile (e.g., [Valo Integration User](#)).
4. Open the new profile and scroll to **Login IP Ranges**. Click **New**.
5. Add the three Valo IP addresses as both Start and End IP Address:
 - 34.77.65.33
 - 35.241.240.44
 - 35.195.129.123
 - *Note: If prompted with the "The list of IP Ranges do not cover..." error, check the box and click **Save** again.*

Assign the Secured Profile

This is the final step to enable IP restrictions and lock down the user.

1. Navigate back to the **User Detail** page for the integration user.
2. Click **Edit**.
3. Change the **Profile** from the temporary assignment to the secured profile: [Valo Integration User](#).
4. **Save** the user.

Note

Once the profile and IP restrictions are in place, you will no longer be able to log in as the integration user. This is why we assign the profile as the last step. If you ever need to do that you will need to add your IP address to the IP restrictions for the profile.