Valo.ai

Creating an integration user with minimal access permissions for Valo.ai use

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. By minimizing user permissions, organizations can adhere to security best practices, ensuring that Valo only has the access required to provide its full range of features.

Valo supports both Integration and standard Salesforce users. This section outlines the steps to create a user with minimized access rights, adhering to security best practices.

The process involves the following main steps:

1. **Clone and Configure a Profile:** IP restriction requires a dedicated profile to be used for the integration user
2. **Create a Permission Set:** Define specific permissions required for Valo.ai.
3. **Create a User:** Set up the user account with appropriate licensing and the cloned profile.
4. **Assign Permission Set to the User:** Grant the defined permissions to the newly created user.
5. **Connect Valo to the Org:** Using the User created above
6. **Install Valo Connected App:** Allow the integration user to use Valo connected app
7. **Assign the Profile:** This will enable the IP restriction. We assign the profile last so that connecting Valo works from your browser in the previous step.

Each step is detailed in the following sections. Please note that these configurations are expected to be completed within the Lightning UI Setup, and there may be minor differences if using the Classic UI.

Before starting with the steps, you need to decide if you will use an Integration User or a Standard Salesforce User license as it affects the steps. **Using an Integration User for connecting Valo is recommended.**

IMPORTANT

Valo recommends using an Integration User for the connection. This is a more secure option and Salesforce Orgs have a number of free Integration User licenses.

Valo.ai

Phase 1: Security & Permissions Setup (Steps 1 & 2)

Create & Configure Valo Integration Profile

1. Navigate to **Setup > Profiles**.
2. **Clone** the determined **Profile to Clone** (e.g., 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.*

Create and Configure Valo Permission Set

1. Navigate to **Setup > Permission Sets** and Click **New**.
2. Name it (e.g., Valo Connection User).
3. **License Setting (CRITICAL)**:
    a. For **Integration User**: Set License to **Salesforce API Integration**.
    b. For **Standard User**: Leave License blank.

IMPORTANT

Since Salesforce updated their uninstalled app policy the “Approve Uninstalled Connected Apps” is required for a minimized permission user to connect an application so that it becomes visible for admins. This allows the app to be installed but requires the removal of the system permission at a later step.

4. **Assign System Permissions:**
    a. Navigate to **System Permissions** and click **Edit**.
    b. **Add ALL** the required permissions listed below and **Save**.
        - Allows users to modify Named Credentials and External Credentials
        - API Enabled (valid only for non-integration user)
        - Approve Uninstalled Connected Apps
        - Customize Application
        - Manage Connected Apps
        - Manage Custom Permissions
        - Modify Metadata Through Metadata API Functions
        - View DeveloperName
        - View Event Log Files
        - View Event Log Object Data (if available)
        - View Login Forensics Events (if available)
        - View Real-Time Event Monitoring Data (if available)
        - View Roles and Role Hierarchy
        - View Setup and Configuration
        - View Threat Detection Events (if available)
        - 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

Valo.ai

Phase 2: User Creation and Initial Connection (Steps 3, 4, 5)

Create the Valo Integration User

1. Navigate to **Setup > Users > Users**. Click **New User**.
2. **License and Profile**

   Recommended Option: Create an Integration User
   - **User License:** Salesforce Integration
   - Profile: Use "Minimum Access - API Only Integrations" for now
   - **Other Data:** No additional access is required.

   Alternative Option: Create a Non-Integration User
   - **User License:** Salesforce
   - Profile: Use "Minimum Access - Salesforce" for now
   - **Other Data**: No additional access is required.

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.
4. **Known Issue Fix (If Error Occurs)**: If you receive an error about the user license not allowing permissions, follow the fix:
   - Go to User **Detail > Permission Set License Assignments > Edit Assignments**.
   - Assign the **Salesforce API Integration** license. Then return to step 4 and assign the Permission Set.

Valo.ai

Connect Valo to the Org

IMPORTANT

When using the newly created user for the Valo connection, ensure you are logged out of any other Salesforce accounts or use a private browsing window (e.g., Chrome's Incognito mode). This ensures that Salesforce prompts you for login credentials. Enter the username and password of the Valo integration user and then click "Allow" when prompted for OAuth scope.

Depending on your Salesforce security settings, the integration user may require multi-factor authentication (MFA). A temporary authentication code can be generated for the user to facilitate this.

Should you need to change the user account used for the connection in the future, Valo offers a "reconnect org" feature.

1. Open a **Private/Incognito** browsing window.
2. Log in to the Valo user interface, navigate to **Manage Orgs > Add Org**.
3. When prompted by Salesforce, log in with the **Username and Password of the new integration user.**
4. Click "**Allow**" when prompted for the OAuth scope.
    - *(Note: The connection may fail at this point if Step 6 is required by your security settings.)*

Valo.ai

Phase 3: Final Security & Activation (Steps 6 & 7)

Install the Valo Connected App (System Admin Required)

This step is required by Salesforce security policies.

1. **As a System Administrator**, navigate to **Setup**.
2. Search for and select **"Connected Apps OAuth Usage"**.
3. Locate the **Valo.ai** app in the list (it should appear after the connection attempt in Step 5).
4. Click **"Install"** next to the Valo.ai app.

> **IMPORTANT**
>
> To ensure login IP restrictions for the Valo connected app are enforced, open the app from “Manage Connected Apps” in setup and verify that the IP relaxation setting is set to "Enforce IP restrictions" (the default).

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 (from Step 3).
2. Click **Edit**.
3. Change the **Profile** from the temporary assignment to the secured profile: **Valo Integration User** (the one created in Step 1).
4. **Save** the user.
    - *Note: The integration user is now locked down to the Valo IP addresses. You will no longer be able to log in with this user unless you add your current IP address to the profile's Login IP Ranges.*

> **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.

Go back to the permission set system permission setting as in Phase 1. Remove the “Approve Uninstalled Connected Apps” system permission as it was only necessary for the installation process.

Valo.ai

Known Issues

#	Issue	Description	Fix or workaround
1	Error with Permission Set Assignment	Permissions set assignment to Integration User fails with error message “Can’t assign permission set to User. The user license doesn’t allow App Permissions’.	Assign Permission Set License “Salesforce API Integration” to User: Setup > User > Permission Set License Assignments > Edit Assignments. Then assign the permission set to the user.