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 four 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.

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

Step 1: Creating a Profile

Valo recommends creating a dedicated profile for the integration user. While not strictly necessary for minimizing permissions, this step is crucial for implementing a recommended security practice: restricting logins by the Valo integration user to only the IP addresses Valo utilizes.

To achieve minimized user rights, it's best to start with minimal functionalities. Therefore, create a new profile by cloning a standard profile. Choose a descriptive name for the profile, such as "Valo Integration User." The appropriate minimum profile to clone depends on the user license you've selected:

- **For Integration User:** Clone “Minimum Access - API Only Integrations”
- **For Standard:** Clone “Minimum Access - Salesforce”

After creating the new cloned profile, locate it under "Profiles" in Salesforce Setup. Then, add login IP ranges for this profile. Valo's IP addresses are:

```
34.77.65.33
35.241.240.44
35.195.129.123
```

To configure these three IP addresses as the login IP ranges, follow these steps:

1. Go to "Login IP Ranges" and click "New."
2. For each of the IP addresses listed above:
    - Enter the IP address as both the "Start IP Address" and "End IP Address."
    - Add a description, such as "Valo backend".
    - Click "Save."
    - You may receive an error message: "The list of IP Ranges do not cover your current IP address."
    - Select "Save this IP Range even though it does not cover my current IP address" and click "Save" again.

If you need to log into this Valo Integration User account for other reasons, you will need to add additional IP addresses. However, for pure Valo use, these three IP addresses are sufficient.

IMPORTANT

To ensure the login IP restriction for the Valo connected app is enforced, verify that you have installed the Valo Connected App and that the IP restriction setting is set to "Enforce IP restrictions."

Valo.ai

Step 2: Creating a Permission Set

Begin by creating a new Permission Set within Salesforce Setup. A suitable name is e.g. "Valo Connection User." When configuring the Permission Set, determine the appropriate License setting:

- **For an Integration User:** Set the License to "Salesforce API Integration."
- **For a Standard Salesforce User:** Leave the License field blank.

After creating the Permission Set, proceed to assign the necessary System Permissions:

1. Navigate to Permission Set > System Permissions
2. Click “Edit”
3. Add following permissions and then click “Save
    1. Allows users to modify Named Credentials and External Credentials
    2. API Enabled (valid only for non-integration user)
    3. Customize Application
    4. Manage Connected Apps
    5. Manage Custom Permissions
    6. Modify Metadata Through Metadata API Functions
    7. View DeveloperName
    8. View Event Log Files
    9. View Event Log Object Data (if available)
    10. View Login Forensics Events (if available)
    11. View Real-Time Event Monitoring Data (if available)
    12. View Roles and Role Hierarchy
    13. View Setup and Configuration
    14. View Threat Detection Events (if available)
    15. Assign Permission Sets
    16. Freeze Users
    17. Manage Internal Users
    18. Manage IP Addresses
    19. Manage Login Access Policies
    20. Manage Password Policies
    21. Manage Profiles and Permission Sets
    22. Manage Roles
    23. Manage Sharing
    24. Manage Users
    25. Monitor Login History
    26. Reset User Passwords and Unlock Users
    27. View All Profiles
    28. View All Users

Valo.ai

Step 3: Creating the User

Navigate to Salesforce Setup to create the new user. The user license and profile will depend on whether you are creating an Integration User or a standard Salesforce user.

Recommended Option: Create an Integration User

- **User License:** Salesforce Integration
- **Profile:** The profile you created in Step 1
- **Other Data:** No additional access is required.

Alternative Option: Create a Non-Integration User

- **User License:** Salesforce
- **Profile:** The profile you created in Step 1
- **Other Data:** No additional access is required.

Step 4: Assign permission set to the new user

After successfully creating and saving the new user, the final step is to assign the Permission Set created in Step 1.

Once the Permission Set is assigned, the user account is fully configured and ready for connecting your Salesforce Org to Valo.

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.

Valo.ai

Step 5: “Install” Valo.ai connected app

Beginning September 2025, Salesforce requires connected apps to be explicitly "installed" within an Org if the integration user does not have the "Approve Uninstalled Connected Apps" system permission. The user created in the previous steps does not possess this permission.

Action Required: A Salesforce System Administrator must install the Valo connected app after the integration user has tried to connect Valo to the Org.

Instructions for System Administrator:

1. 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" next to the Valo.ai app
5. Once the app is installed, the integration user will be able to successfully connect your Salesforce Org to Valo

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.