Jira Integration

Roy OS Integration Guide | **READ + WRITE**

Overview

The Roy OS Jira integration turns meeting action items into tracked Jira issues automatically. During meetings, the agent also reads existing issues to provide project context and check for duplicates before creating new tickets.

What Roy Can Do in Jira

Capability	Description
Create issues	Turns meeting action items into Jira issues with title, description, assignee, priority, and labels.
Update issues	Updates issue status or adds comments when action items are discussed in follow-up meetings.
Search issues	Checks for existing issues before creating duplicates. Surfaces open items during meeting prep.
Read project metadata	Reads project keys and names to route new issues to the correct project.

> **What Roy cannot do:** Delete issues, modify project configuration, access organization-wide data, manage users, customize workflows, or perform any admin operations.

Required Permissions

OAuth Scope	Why It's Needed
`read:jira-work`	Search existing issues and read project metadata for context and duplicate detection
`write:jira-work`	Create new issues and update existing issues from meeting action items

Setup Guide

Prerequisites

You'll need Atlassian admin access to your organization's Jira Cloud instance and access to your Azure Key Vault.

1 **Create an OAuth App**

Go to developer.atlassian.com → **Create** → **OAuth 2.0 (3LO)**. Name it "Roy OS" and set the callback URL provided by Roy AI during onboarding.

2 **Configure Scopes**

Under **Permissions**, add **Jira API** scopes: `read:jira-work` and `write:jira-work`. Do not add admin or user management scopes.

3 **Store Credentials in Key Vault**

Copy the **Client ID** and **Client Secret** from your Atlassian app and add them to your Azure Key Vault:

Secret Name	Value
`jira-client-id`	OAuth Client ID
`jira-client-secret`	OAuth Client Secret

4 **Designate Permitted Projects**

Your Jira admin defines which projects Roy OS can access. The agent cannot exceed project boundaries set by your Atlassian permissions.

5 **User Consent**

Each user completes the OAuth consent flow on first use. This grants Roy OS delegated access to create issues on their behalf within the permitted projects.

6 **Verify Connectivity**

Roy AI runs a smoke test: OAuth flow, token exchange, and a test API call to search and create a test issue in a designated project.

Managing Access

Action	How
Restrict project access	Jira admin adjusts project permissions for the OAuth app. Immediate effect.
Revoke a user	

	User revokes consent in their Atlassian account settings. Only their delegated access is removed.
Revoke all access	Delete the OAuth app in Atlassian Developer Console. All tokens invalidated immediately.
Rotate credentials	Regenerate client secret in Atlassian console. Update the Key Vault secret.

FAQ

Can Roy access all projects in my Jira instance?

No. Roy can only access projects that your Jira admin has explicitly permitted. The OAuth app's project access is controlled by your Atlassian permissions model.

Can Roy delete issues?

No. Roy has no DELETE capability. It can only create and update issues.

What does a Roy-created Jira issue look like?

Issues are created with a title and description extracted from the meeting action item, along with assignee, priority, and labels if identified during the meeting. The description includes a reference back to the meeting where the action item was captured.

Can I control which meetings create Jira issues?

Yes. Issue creation is triggered by the agent's action item extraction. Team members can review and approve action items before they are pushed to Jira.

> **Audit trail:** Every Jira API call is logged (issue key, action type, timestamp, success/failure) and available in your Azure Log Analytics workspace.