NG SIEM - (Plain Scope) Atlassian Confluence Integration

What is API Token?

A secure string used to **authenticate external applications or scripts** so they can access Confluence's REST APIs without needing a user password. Its main use is to **allow programmatic access** for integrations, automation, or tools to interact with Confluence content.

Creating an API Token

Follow these steps to create a token. Note: As of March 13, 2025, tokens created before December 15, 2024, will expire between March 14 and May 12, 2026. New tokens default to 1-year expiration (adjustable from 1 to 365 days).

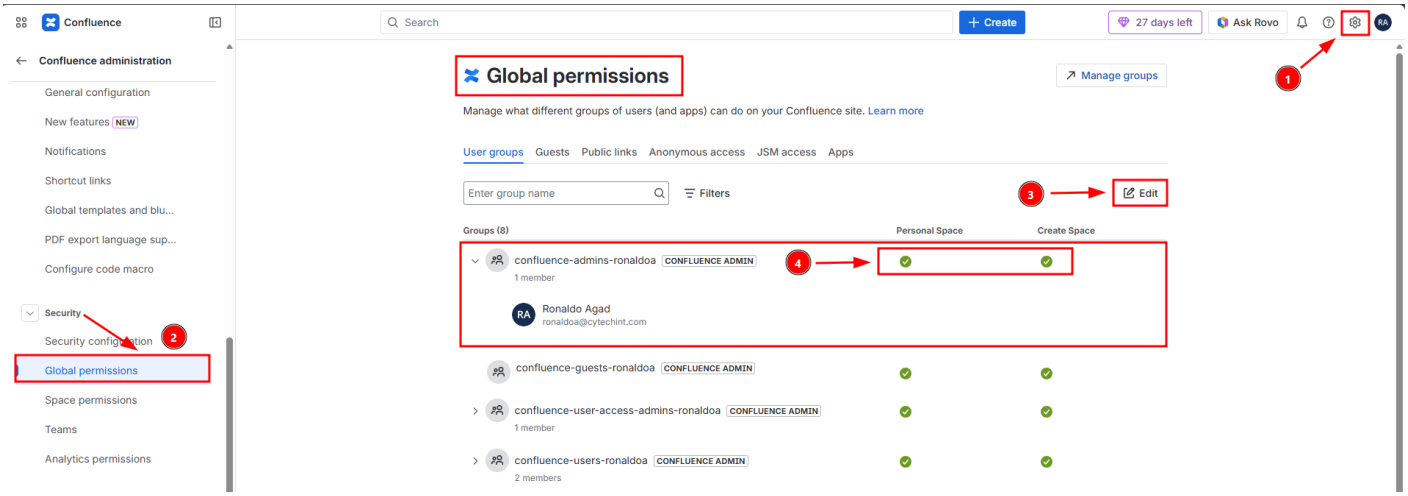
1. Log in to https://id.atlassian.com/manage-profile/security/api-tokens.
2. Select "Create API token".
3. Enter a descriptive name for the token (e.g., "AQUILA- Audit Logs Monitoring").
4. Choose an expiration date for the token (between 1 and 365 days; consider shorter for security).
5. Click "Create".
6. Copy the token and save it securely. You cannot view it again after this step. If lost, generate a new one. Share only with trusted integrations like AQUILA—revoke if compromised.

Required Atlassian-Side Permissions

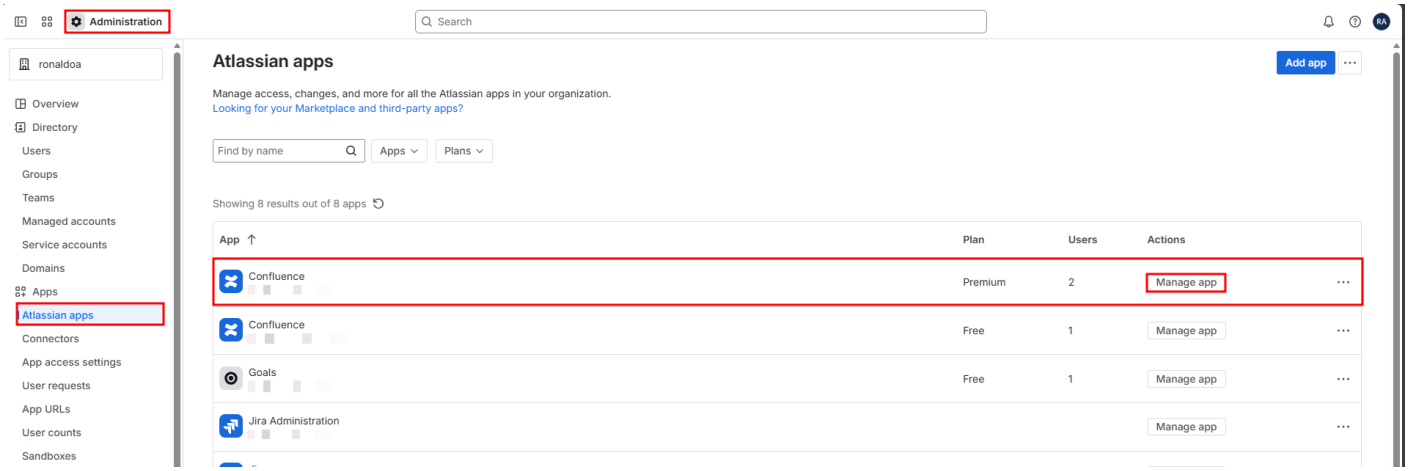
The user account tied to the email (Jira/Confluence User Identifier) must have admin-level access to fetch audit logs via API:

- For Confluence: Confluence **Global permission**.

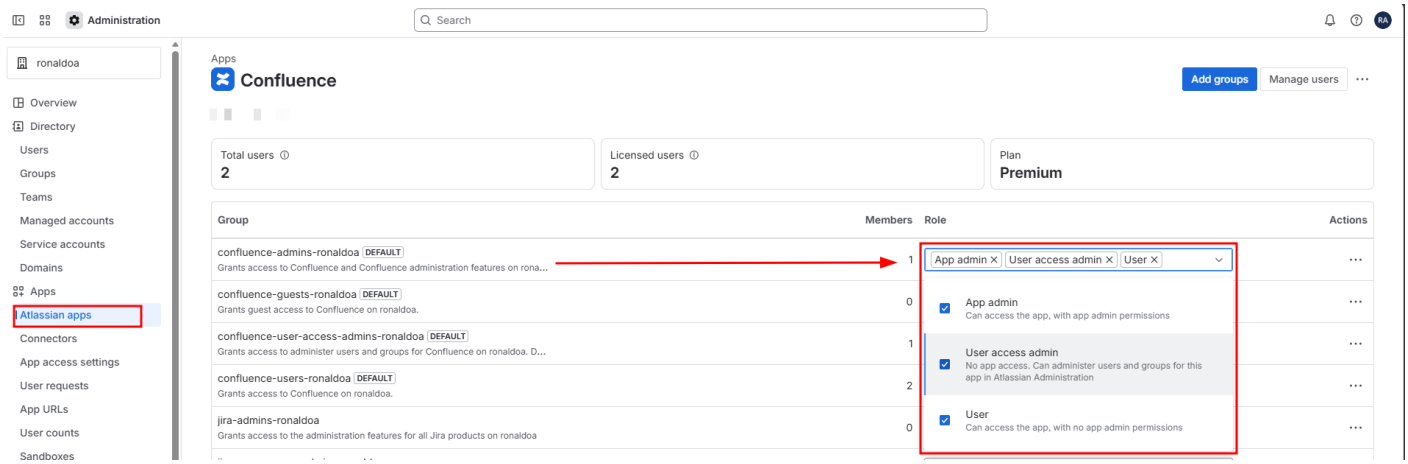
  https://your-domain.atlassian.net/wiki/admin/permissions/global?tab=internal
- The **confluence-admins-ronaldoa** both **Personal Space** and **Create Space** should be checked. Click the "Edit" to proceed.



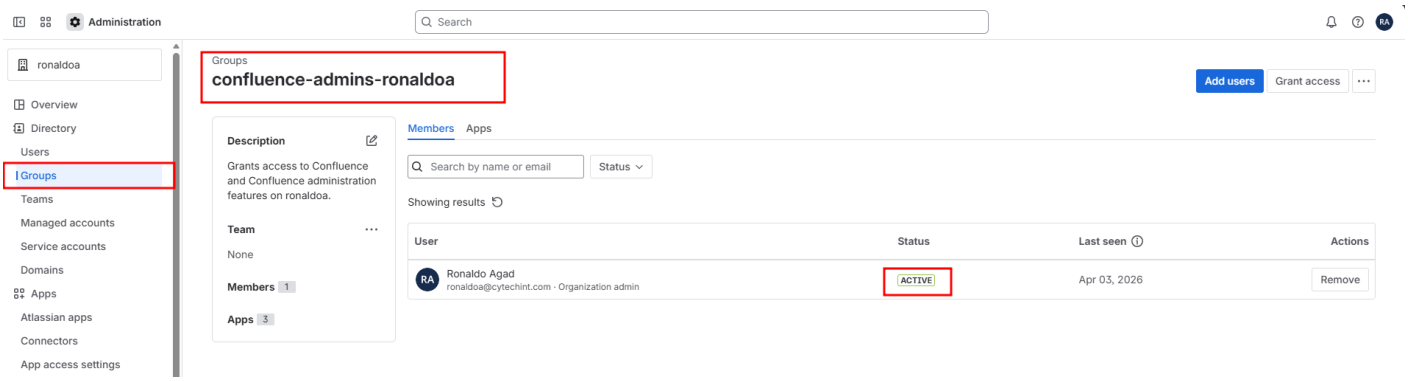
- For Confluence: Confluence **Administration** permission.
  https://admin.atlassian.com/o/8d1afe09-e60a-4bf3-87d9-c71b10e4842b/atlassian-apps
- Click "**Manage app**".



- Provide Role **App admin**, **User access admin**, **user** in **confluence-admins-ronaldoa.**



- In **Groups** under by **Directory,** make sure the **User** is active.



Without this, the API may authenticate successfully (leading to a "healthy" status in AQUILA) but return no data or errors like 403 Forbidden. If you lack access to the client side, request they verify/add these permissions via admin.atlassian.com > Global Permissions.

> **Note: If you're on a Free plan without org access, you can't enable advanced features—consider upgrading or using site-level logs in individual apps.**

Required Credentials for Integration Access (AQUILA Setup)

Use these in AQUILA > Integrations > Atlassian Jira/Confluence setup (separate integrations for each). For Atlassian Cloud, authentication uses Basic Auth (email + token).

- **API URL**: Base Atlassian API URL without paths (e.g., https://your-site.atlassian.net for Confluence; add /wiki for Confluence endpoints if needed, but AQUILA handles this).
- **User Identifier**: Your Atlassian email address (must be linked to an admin account as noted above).
- **API Token**: The scoped token created above.
- **Personal Access Token (PAT) -** : The Personal Access Token used for self-hosted instances. If set, Jira User Identifier and Jira API Token will be ignored. **(Optional)**

For self-hosted (Data Center/Server) instances, a Personal Access Token may be used instead, but Cloud setups prefer the API token.

> Please provide the following information to CyTech

- **API URL**: Base Atlassian API URL without paths (e.g., https://your-site.atlassian.net for Jira; add /wiki for Confluence endpoints if needed, but AQUILA handles this).
- **Confluence User Identifier**: Your Atlassian email address (must be linked to an admin account as noted above).
- **Confluence API Token**: The scoped token created above.

Revision #2
Created 2 April 2026 22:43:52
Updated 2 April 2026 23:36:41