NG SIEM - Atlassian Confluence Integration

What are API Token Scopes?

Scopes define what actions an API token is allowed to perform in Atlassian apps such as Jira and Confluence. They enhance security by limiting permissions to only what's needed (e.g., read-only access to audit logs). Always use scoped tokens for AQUILA integrations—unscoped tokens are deprecated for most apps and may not support fine-grained access. For audit logs (events like user actions, config changes, or security incidents), use the specific scopes listed below. Broader scopes may be needed for other integrations (e.g., content indexing), but stick to these for basic monitoring to minimize risk.

Creating an API Token with Scopes

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 with scopes".
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. Select the application (Jira or Confluence). **Important:** Create separate tokens for Jira and Confluence—tokens are app-specific and cannot access both.
6. Select the scopes or permissions the token should have:
   - For Jira (audit logs): read:audit-log:jira (allows viewing audit events).
   - For Confluence (audit logs): read:audit-log:confluence (allows viewing audit events; add write:audit-log:confluence if needed for custom logging, but not required for AQUILA).
7. Click "Create".
8. 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 Jira: "Administer Jira" global permission (or Jira System Administrator).
- For Confluence: Confluence Administrator permission.

Without these, 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.

> **Additionally, ensure audit logging is enabled and set to "Full" coverage on the Atlassian side (via their admin settings) to generate events. Low activity instances may produce sparse logs.**

> **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 Jira; 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 #13
Created 23 September 2025 08:13:30 by Richmond Abella
Updated 3 December 2025 07:15:20