Obo Integration with Jira

Jira Cloud Obo connects with Jira Cloud using secure API Tokens created and managed by Jira. Users create their personal tokens in Jira using their Jira login credentials. Jira access is limited by each user's Jira account project permissions.

Jira Server The Obo Server communicates with your Jira Server using SSL encryption via published Jira API calls. User authentication and privileges are enforced by user-specific API tokens created and managed by Jira. Your Jira Server instance must allow SSL traffic from either a public IP address or a reverse proxy server that has a public IP address to enable this communication. If you have a firewall that blocks public SSL traffic to Jira Server, you will need to white-list these Obo Server IP addresses on your firewall or reverse proxy server:

- 34.218.103.31:443
- 34.209.60.123:443
- 35.163.137.106:443

If you have Jira Server 8.14.0 or higher, Obo Apps access Jira using Personal Access Tokens. This allows each Obo user to set up their own secure and private Jira integration in less than a minute - no Jira Admin required. The Personal Access Tokens are managed by Jira and enforce user-level project permissions.

If your Jira Server is pre-8.14, the Obo Server uses OAuth authentication to connect with Jira Server. A Jira user with Jira admin privileges must perform the initial Obo Jira setup, which creates the OAuth relationship between the Obo and Jira servers (takes less than 5 minutes). Subsequent Obo users set up their own secure and private Jira integration using OAuth API tokens in less than a minute. The OAuth API tokens are managed by Jira and enforce user-level project permissions.

Obo supports SAML2.0 Single Sign-On.

Obo hosts its SaaS applications in AWS and enforces a strict security framework.