Obo Security

- Obo is an approved Atlassian Marketplace Vendor.
- Obo has completed the Atlassian Security Assessment Program.
- Obo does not require, request, or store a user's Jira login credentials.
- Obo users must have valid Jira login access to access Jira data from within Obo. Obo uses Jira-generated API tokens for Jira integration. These tokens are revocable by Jira users and admins. The tokens enforce the most-current user access permissions that are established in Jira.
- Each Obo user is allocated their own private data space. No database records are shared across users.
- Data at rest is 256-bit AES SSL encrypted.
- Data in transit is TLS 1.2 encrypted.
- Obo personnel cannot see your data unless you explicitly share logoin credentials with us.
- The Obo application is hosted in EC2 (private IP address space) behind a load balancer (public IP address).
- Obo is hosted at AWS S3. AWS is compliant with: CSA, ISO 9001, ISO 27001, ISO 27017, IS0 27018, PCI DSS Level 1, SOC 1, SOC 2, and SOC 3.
- Obo runs within a Virtual Private Cloud (VPC) behind a security group with strict firewall rules in accordance with AWS security and privacy practices.
- Obo uses the AWS EC2 infrastructure. All production data is archived during upgrades to protect against data loss.
- Obo is PCI Level 1 compliant through our integration with Stripe.