fulcrum

Visit our website:
fulcrumapp.com

Security & Infrastructure

Fulcrum is a cloud-based data collection and storage platform designed to simplify the process of creating customized data collection apps for conducting field surveys and mobile, digital form development. As a cloud solution, the Fulcrum platform runs on the Amazon Web Services (AWS) infrastructure, including Elastic Compute Cloud (EC2), Simple Storage Service (S3), and Virtual Private Cloud (VPC). By harnessing the AWS infrastructure, Fulcrum offers higher-availability, redundant high-capacity storage, and added reliability over self-hosted software solutions.

Overview

- The Fulcrum server is cloud-based, and adheres to the policies of the Amazon Web Services standard agreement. For more information see aws.amazon.com/security.
- All traffic to the Fulcrum server and API is forced to use 256-bit secure SSL.
- Fulcrum is a Ruby on Rails web application.
- Fulcrum's mobile apps for iOS and Android are completely native, built using Objective-C and Java, respectively.
- All server requests are handled by an nginx web server.
- All persistent data is stored on a PostgreSQL database server, with PostGIS extensions for geospatial functions.
- All user accounts in Fulcrum require strong passwords for authentication to the system.
- Attachment data and maps uploaded to Fulcrum are stored on S3, a distributed, high-availability storage engine that grows along with your Fulcrum content.
- Your data always remains private, and is not shared between accounts on the system, and all data within your account belongs to you.
- All content stored on S3 has access control policies and permissions associated with it, locking down all content making it accessible only to your user account. As with the database, all associated files on S3 are stored redundantly across datacenter locations to mitigate data loss and increase availability and uptime.
- Authentication to the API is accomplished via unique tokens associated with each account which can be reset at any time. This same API is used by our iOS and Android mobile applications.
- Authentication uses standard challenge/response, with SHA1 password hashes stored in the PostgreSQL database.