Shine and Security

Shine and Security

Shine users entrust us with keeping track of the everyday actions they take to help them better themselves, their community and our planet. Putting our users first is critical to what we do, including how we protect their data. Following industry standards on top of our own security practices keep their information safe.

Our app is playful and encourages sharing, but we take keeping this information secure very seriously.

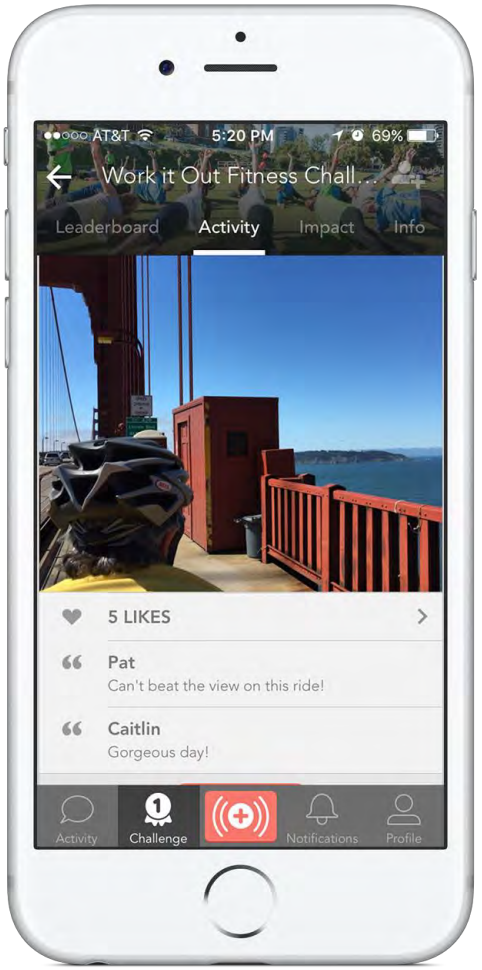
What follows is an overview of our app and some of our processes.

shine

What is the Purpose of Our App

With Shine by JouleBug, compete in challenges with fellow co-workers to improve your body, your community, and your planet. Earn points and build camaraderie by completing simple real-life actions as you and your co-workers work towards common goals.

Shine is full of simple Actions aimed at making the world a little better. When you do the actions in real-life, you record them in the app. Show you care and share how you're making a difference. Be inspired by others' activities in the Feed. Compete in short Challenges to raise the bar and strengthen your community. Track your impact with your career stats as your Trophy Case fills up. Be well, have fun, and make a positive impact with Shine!



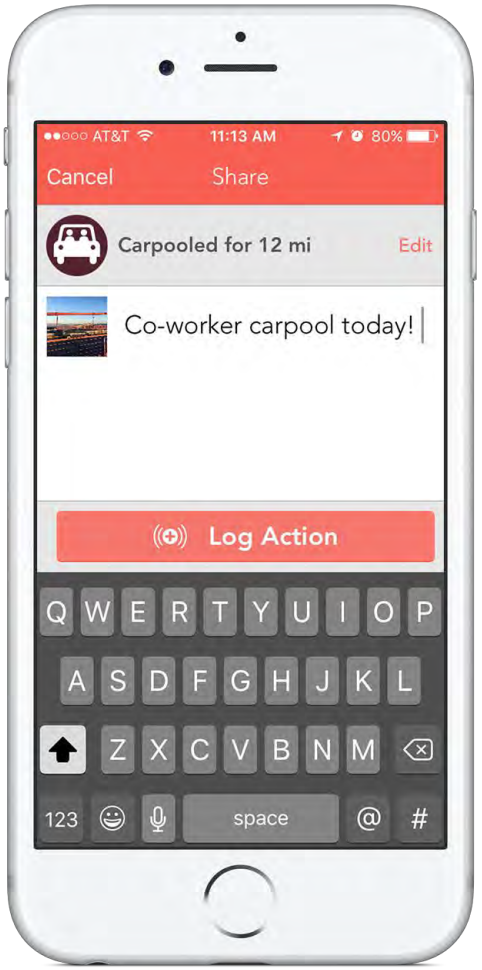
shine

Security Overview

Shine transmits data over public networks using strong encryption. This includes data transmitted between Shine clients and the Shine service. Shine supports the latest recommended secure cipher suites to encrypt all traffic in transit, including use of TLS 1.2 protocols, AES256 encryption, and SHA2 signatures, as supported by the clients.

Sensitive Data (tokens & passwords) at rest in Shine's production network is encrypted. Currently, images are stored on S3 and are not encrypted.

Each Shine customer's data is hosted in Shine's shared infrastructure and segregated logically by the Shine application. Shine uses a combination of storage technologies to ensure customer data is protected from hardware failures.



shine

Security Overview cont.

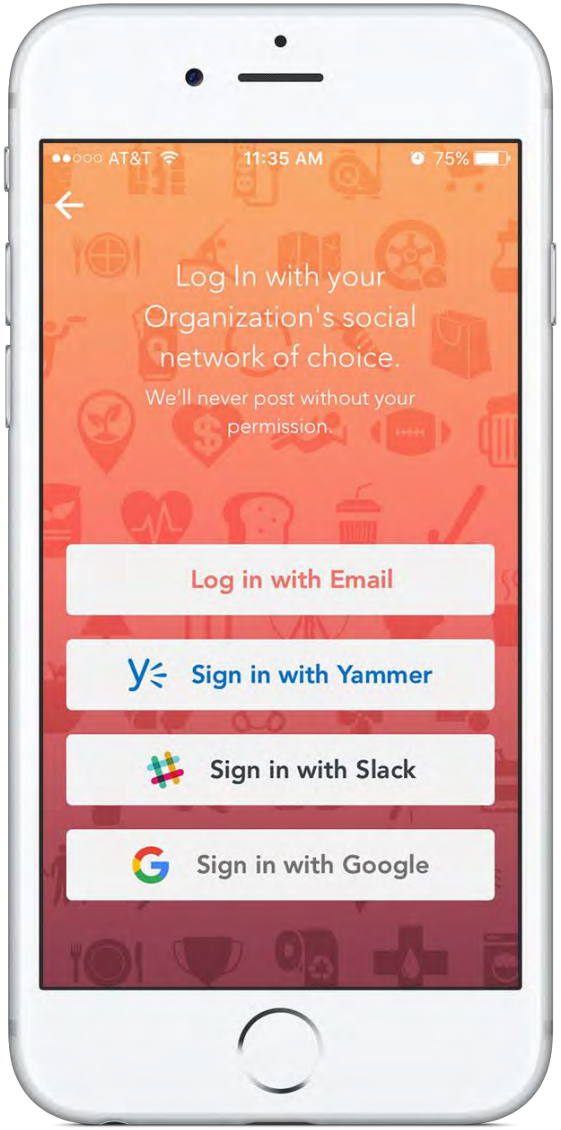
The Shine service is hosted in data centers maintained by Amazon. Amazon offers state-of-the-art physical protection for the servers and related infrastructure that comprise the operating environment for the Shine service. They are responsible for restricting physical access to Shine's systems to authorized personnel.

Shine uses Amazon Virtual Private Cloud (Amazon VPC) to control security groups and firewall rules and AWS Identity and Access Management (IAM) to control user credentials and roles.

We use Amazon Cloudwatch for monitoring logs related to Amazon EC2 instances, and Amazon Route 53 for DNS management.

shine

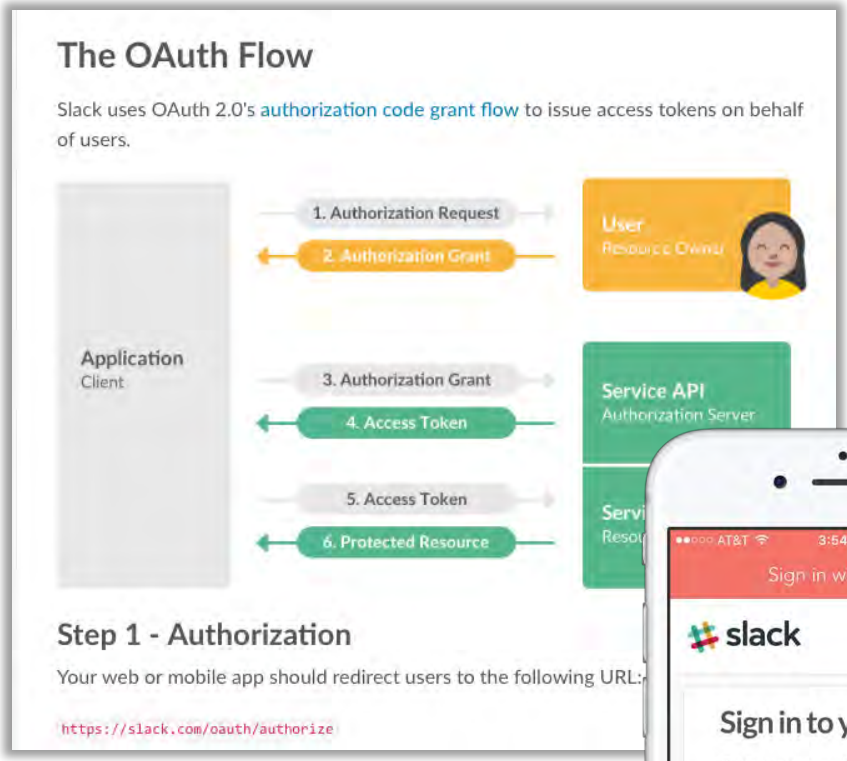
Authentication



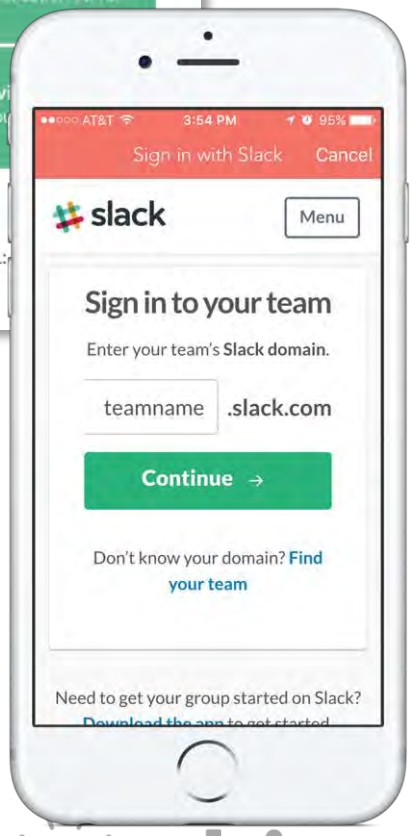
Shine utilizes Slack's API | OAuth 2.0

1. User Signs in with Slack
2. Slack provides an access token for user
3. Shine verifies token validity with Slack
4. Shine issues a Shine access token to the user to make authenticated API calls via Shine App
5. Shine token can be revoked by an admin and has an expiration time

Note: Shine does not store user's email or password



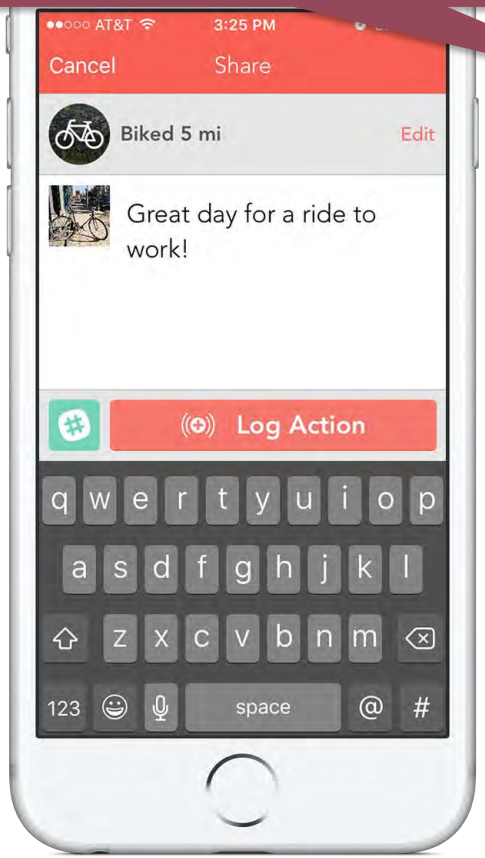
https://api.slack.com/docs/oauth

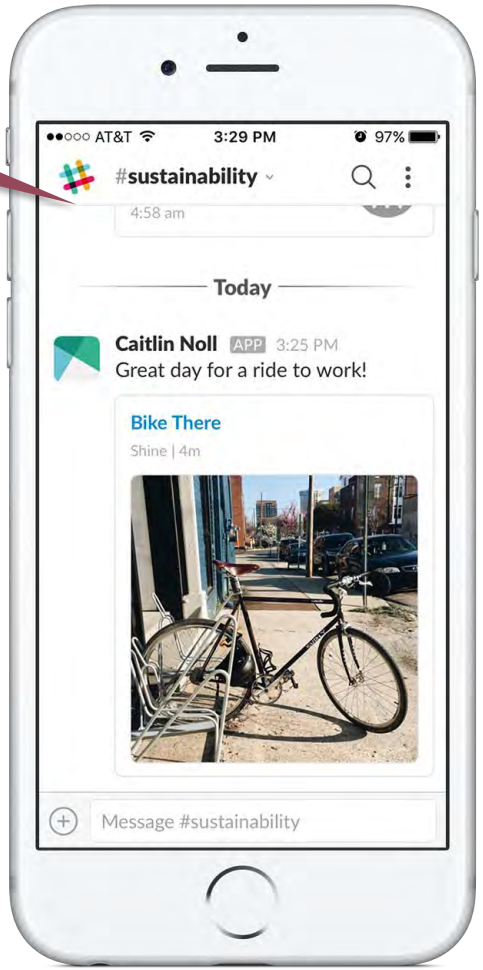


shine

Slack Data Utilization

Users have the option to share a Shine post to a designated Slack Channel





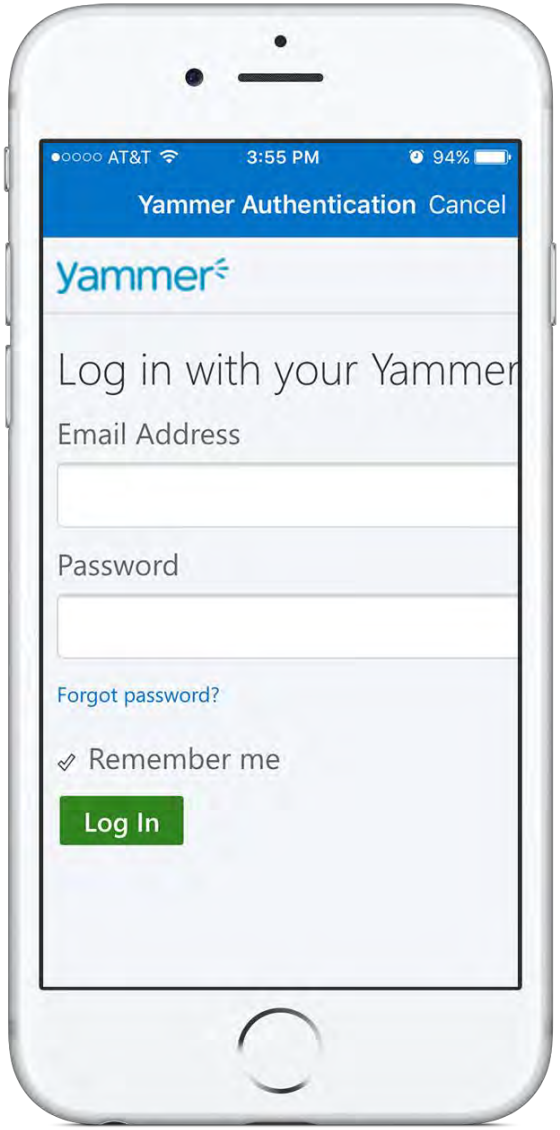
Shine will use the User's Slack Name and Profile Pic

shine

Shine utilizes Yammer's API | OAuth 2.0

1. User Signs in with Yammer
2. Yammer provides an access token for user
3. Shine verifies token validity with Yammer
4. Shine issues a Shine access token to the user to make authenticated API calls via Shine App
5. Shine token can be revoked by an admin and has an expiration time

Note: Shine does not store user's email or password

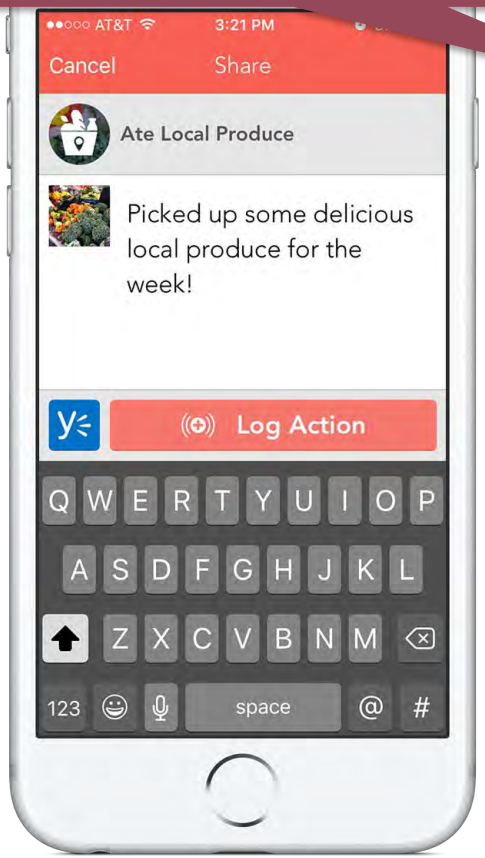


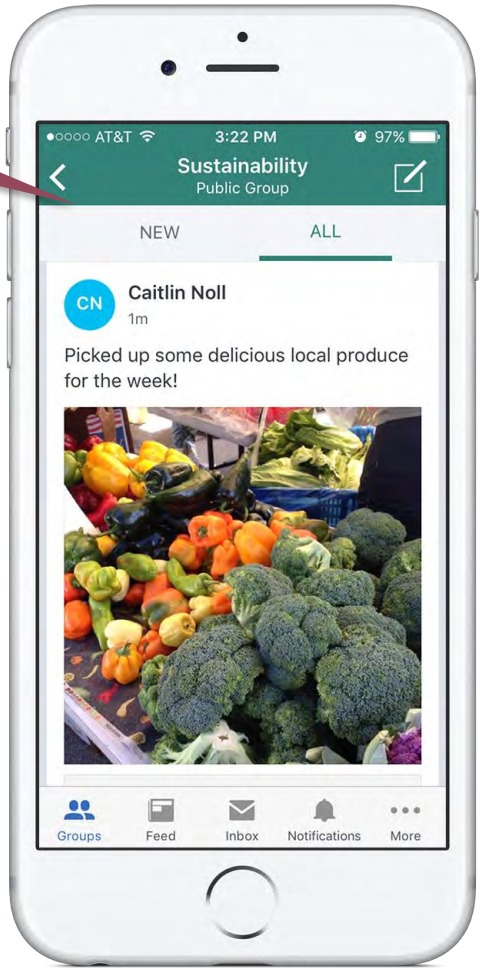
https://developer.yammer.com/docs/oauth-2

shine

Yammer Data Utilization

Users have the option to share a Shine post in a designated Yammer Group





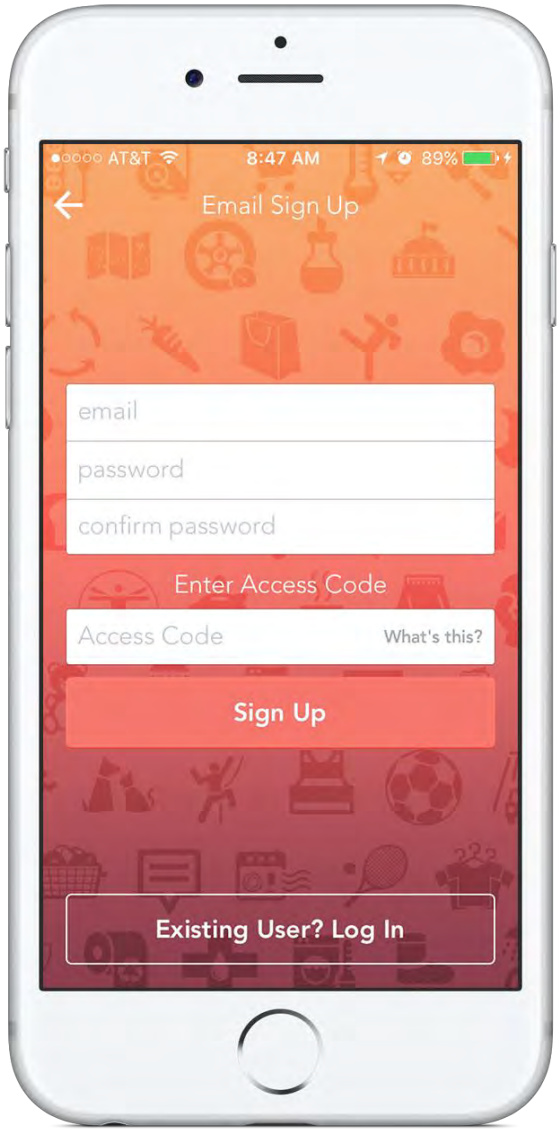
Shine will use the User's Yammer Name and Profile Pic

shine

Shine Internal Authentication

1. User enters their User Name and Password
2. User enters an Access Code unique to their Organization
3. Shine verifies Access Code
4. Shine issues a Shine access token to the user to make authenticated API calls via Shine App
5. Shine token can be revoked by an admin and has an expiration time

Note: Shine BCrypts Password



shine