LiveSafe®

SCIM Integration

Managing user profiles across systems is easier than ever with LiveSafe's SCIM (System for Cross-Domain Identity Management) connector. You can automatically share user data from your internal systems to keep your LiveSafe user data in sync.

Broader alerting reach

Simpler user management

Increased system security

Why Use SCIM with LiveSafe?

The value of your LiveSafe implementation grows each time a member of your community interacts with the system. That's why we offer flexible user management options like SCIM to simplify application installation, streamline profile management, and facilitate authentication.

One System of Record

If you already have a central directory of user information – your Human Resources Management System (HRMS), Enterprise Resources Planning (ERP), or your IT directory system – the SCIM interface allows you to push the relevant information directly to LiveSafe. Automatically populate names, email addresses and phone numbers you're already using. When information in your primary system changes, it is automatically updated in LiveSafe too.

LiveSafeMobile.com ☎ (571) 312-4645 @LiveSafe /LiveSafePlatform

Reach More Users

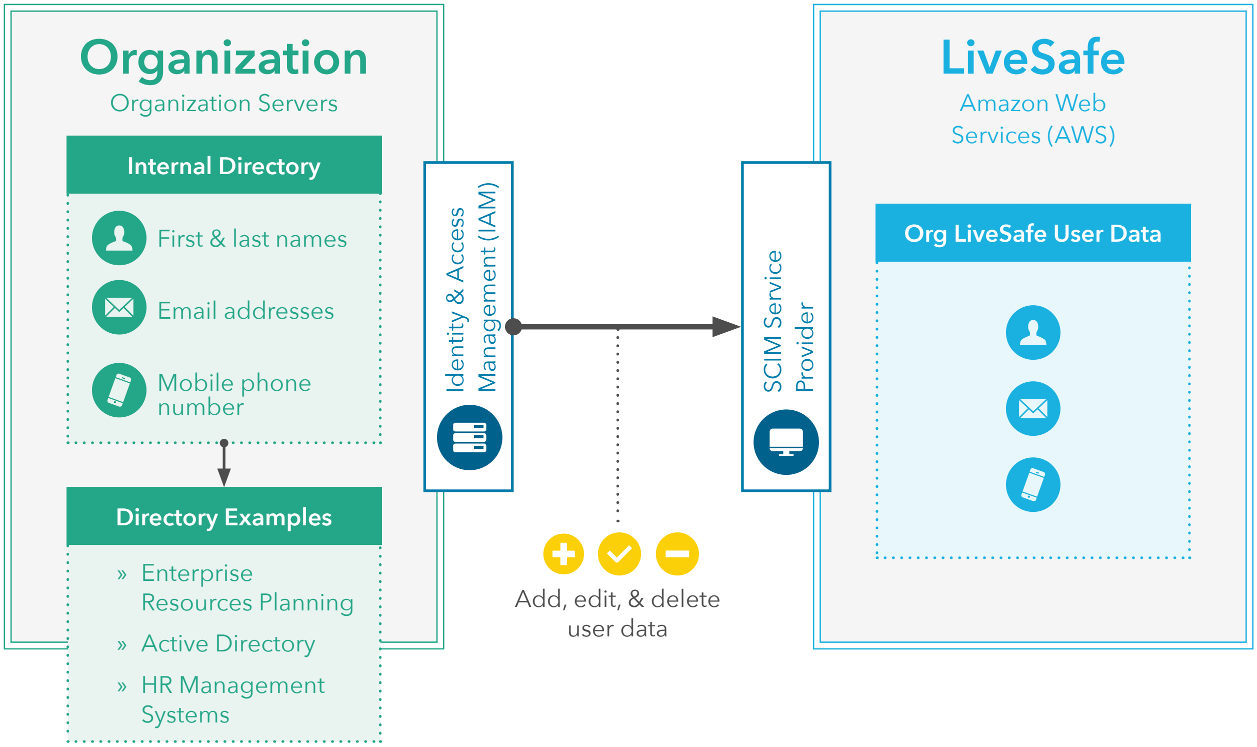
Pre-populating user data from your internal systems ensures more ways to reach your people in an emergency. While most of the profile fields in LiveSafe are optional, the SCIM connector requires at least one email address or mobile phone number for each record. This allows you to reach users via broadcast email or text messages even if they have not yet downloaded the app. If an email address or phone number changes, the system will automatically pass the update to LiveSafe so you always have the latest contact information.

When users do download the LiveSafe app or you push it to devices automatically via a mobile device management system, the pre-populated data makes user onboarding faster and easier. LiveSafe administrators can see all the users in the dashboard.

User Authentication and Security

When an employee leaves or a student graduates, automatic SCIM updates remove the user from your user list. This blocks unauthorized users from authentication and prevents them from accessing your organization's LiveSafe platform. The user will still have access to any other organizations in LiveSafe that they have subscribed to, but your organization's instance of LiveSafe will be removed from their profile.

We recommend that SCIM users implement higher level account verification options to add increased levels of security for employee interactions. Choose single sign on or email verification to ensure that every user is properly identified and authorized to access system resources.



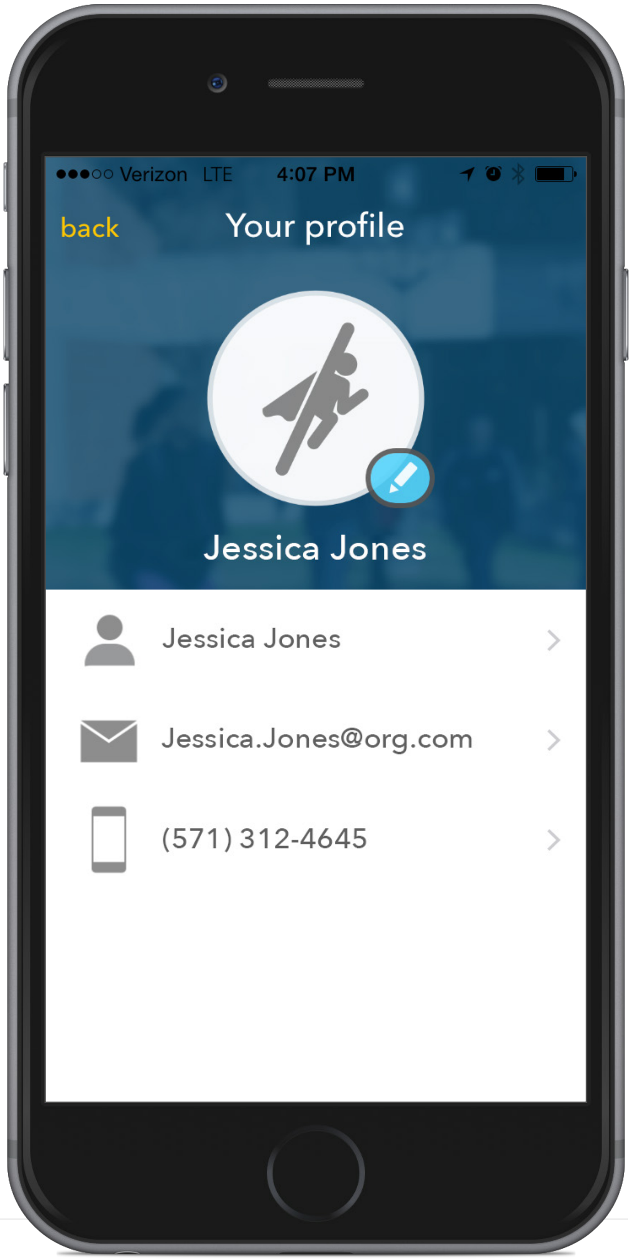
How SCIM Works with LiveSafe?

LiveSafe works with several leading Identity and Access Management (IAM) solutions for out-of-the-box SCIM integrations. Simply tell us which IAM you use and we will provide a URL endpoint and credentials to sync your directory via the SCIM interface. If your organization uses another IAM, you will need to implement SCIM with your existing Identity and Access Management system to enable user data integration with LiveSafe. Our success team will provide the necessary documentation and a developer's sandbox to help you get started.

Once the connector is in place, we recommend that you update your data once a day. However, you can architect the frequency per your organization's individual requirements.

Supported IAMs

- » Azure AD
- » Ping Identity
- » Okta
- » One Login
- » CA Identity Manager
- » IBM Security Directory



Jessica Jones

Jessica Jones

Jessica.Jones@org.com

(571) 312-4645

Ready to Learn More About How SCIM can Work for Your Organization?

Contact your LiveSafe representative or contact@livesafemobile.com to learn more about SCIM integration and next steps.