Rippling Identity & Access Management

User account provisioning, single sign-on, password management, and more — all powered by one unified, "Zero-Upkeep" directory,

RIPPLING

Table of Contents

Rippling's Identity Management Model. 4

How Rippling IDM Works. 5

How We Integrate With Your Apps & Websites. . . . . .6 - 7

How to Configure Rippling IDM . . . . . .8 - 10

Integration Methods: Partner API . . . . . 12 - 13

Integration Methods: SAML. . . . . 14 - 15

Integration Methods: RPass 16

Integration Methods: LDAP & Rippling REST API 17

Integration Methods: SSH Key Management 18

Rippling Security Overview 20

How Rippling Makes Your Org More Secure 21

Rippling High Availability Architecture 22

Rippling Identity & Access Management Overview

A (somewhat) non-technical overview of what Rippling Identity and Access Management is, and how it works.

Rippling's Identity Management Model

A rich identity model is the foundation of Rippling's Identity and Access Management system, and is the basis for managing your employees' access and security.

When you onboard an employee in Rippling, several attributes are collected from the hiring manager or the new hire themself:

- Department
- Title
- Work Location
- Manager
- Employment Type (e.g. full time or contractor)
- Usernames (such as preferred email address or Github username)
- Class Codes
- Custom Fields
- Start Date
- SSH Keys
- Multi-Factor Authentication

All of these attributes can be used to define smart rules that determine which cloud services an employee gets access to, which licenses and permissions they get access to, what groups they're included in, and so forth. For instance, you can define a rule such as "all part-time sales contractors in the New York office get Zoom Basic access" or "all full-time engineers in the Frontend department belong on the Frontend Google group." In the next sections, we'll see how smart rules can be used to configure most onboarding/offboarding actions in an automated way.

The First Unified, Zero-Upkeep Directory

The most challenging part of most identity models is ensuring that the data is kept up-to-date as employees join, leave, or change roles. If the data isn't accurate, the identity model is useless at best, and insecure at worst.

Because Rippling is the key HR onboarding and offboarding tool for our clients, new employees' information is generally entered into Rippling before any other services. Rippling then manages their employment status, such as whether the employee has accepted the offer, and whether their start date has arrived yet. So Rippling can manage the exact timeline of the onboarding and offboarding cycle. Similarly, when an employee moves to a different department, the change is done in one place in Rippling, and then Rippling can automatically create or suspend accounts based on the employee's new role.

Altogether, this ensures that Rippling's identity data will be the most accurate and the first to reflect new changes, so employees' access always stays in sync with their role.

And since Rippling provides a single source of truth across HR and IT functionality, changes in data will update both HR and IT systems immediately, without having to worry about syncing data between segregated HR and IT databases.

How Rippling Helps Your Team Securely Provision, Access & Manage Their Apps

What are apps and what do they do?
You can leverage the Rippling identity model with "apps" that connect Rippling with various cloud services, such as G Suite, Slack, Dropbox and 300+ others. Once an app is installed in Rippling, the identity model can automatically manage many aspects of the service for you. The most common functionality is to create and remove employee accounts when employees are onboarded and offboarded. But Rippling apps can manage many other aspects of the employee lifecycle:

During Onboarding:

- Create employees' accounts in cloud services, with the right permissions and group memberships according to their role in Rippling.
- Automatically record option grants for new hires in your captable software.
- Collect public ssh keys from employees that need access to your servers.
- Automatically ship pre-configured swag packs to new hires.
- Import candidates from leading applicant tracking systems.
- Initiate background checks from leading background check providers.

During Employment:

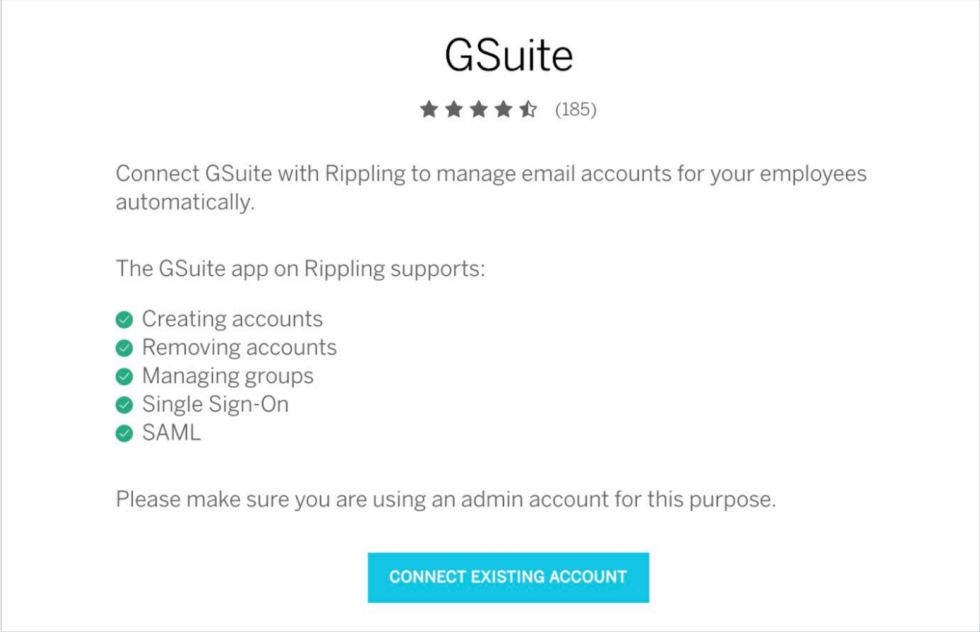
- Provide Single Sign-On (SSO) capabilities for your employees.
- Store employee passwords and credentials in a zero-knowledge vault.
- Easily reset passwords and perform account maintenance in one place.
- Authenticate SSH logins to your servers.
- Expose a virtual LDAP server with your org's employees and structure.
- Import 401k contributions from 401k services into payroll.
- Import timeclock data from Time & Attendance services into payroll.

During Offboarding:

- Suspend or disable offboarded employees' accounts. Apps can do this for all services at an exact time, which is impossible with manual offboarding.

How Does Rippling Integrate With Your Apps (Part 1)?

Rippling uses six different methods (depending on the 3rd party and their technical limitations) to integrate with all of your team's apps and websites. While all six are technically different, to the end user (e.g. your employees), it looks, feels, and acts like one, unified solution.



#1: Partner API (Application Programming Interface)
APIs allow Rippling to query and update data directly in the cloud service. This is most commonly used to create and remove employee accounts, but can also provide other functionality (such as option grants, 401k sync, syncing employee attributes between cloud services, etc.). Most modern cloud services expose APIs.

#2: SAML (Security Assertion Markup Language)
SAML allows Rippling to log employees into the cloud service with one click, and in many cases, create their accounts if they're logging in for the first time. Most modern cloud services support SAML.

#3: Password Management (via RPass, Rippling's password manager for teams)
RPass can manage your employees' credentials, allowing employees to use Single Sign-On through web-based forms, and giving you visibility and control into your organization's password security. This can be done for any web-based service. It look, feels and acts like other password management tools, like LastPass or OnePassword.

The largest and most common cloud services (such as G Suite, Dropbox, Slack, etc.) generally support both APIs for user provisioning and SAML for single sign-on. Less mature cloud services might support only one or the other. Rippling apps will always use the fullest extent of what the underlying cloud services provides.

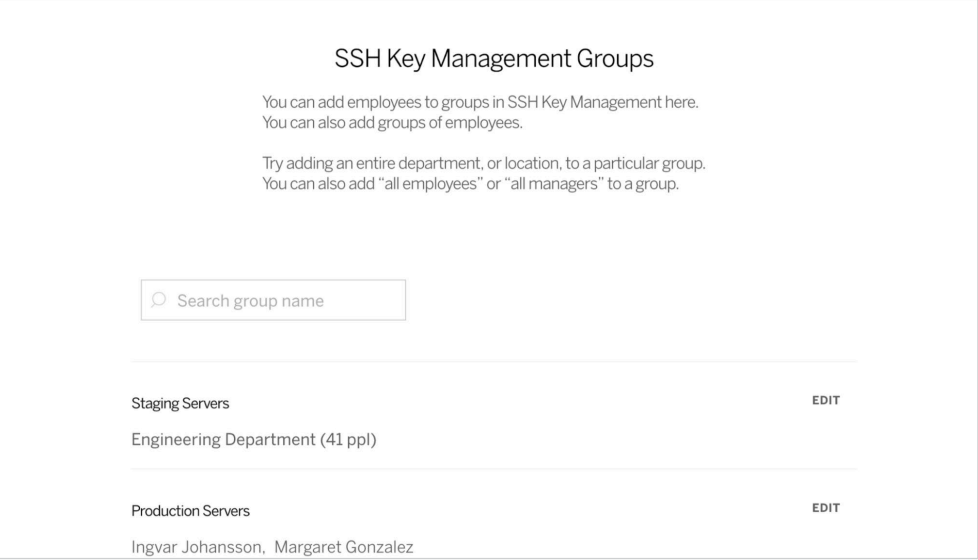
How Does Rippling Integrate With Your Apps (Part 2)?

#4: Rippling REST API
Many Rippling customers have custom in-house systems to which they need to provision and deprovision user access. For that, Rippling exposes a REST API with endpoints to read and interact with employee data, groups, payroll, and PTO. The API is developer-friendly and can be set up within minutes. For example, with the Rippling REST API, companies can sync employee list to provision accounts in internal software systems, or populate an intranet with names, photos, and contact info of new hirees.

#5: LDAP
The Virtual LDAP app in Rippling gives you access to your employee data in Rippling via the industry standard LDAP protocol, which is also used by Microsoft's Active Directory. Any service that connects to LDAP can be pointed to Rippling's LDAP service. One very common use case is for a company transitioning away from a legacy on-premise Active Directory server.

#6: SSH Key Management
Rippling's SSH Key Management feature doesn't integrate with your internal and external apps and websites — it integrates with your server infrastructure using SSH keys. Built-in, easy-to-setup SSH key management is an important part of identity management.

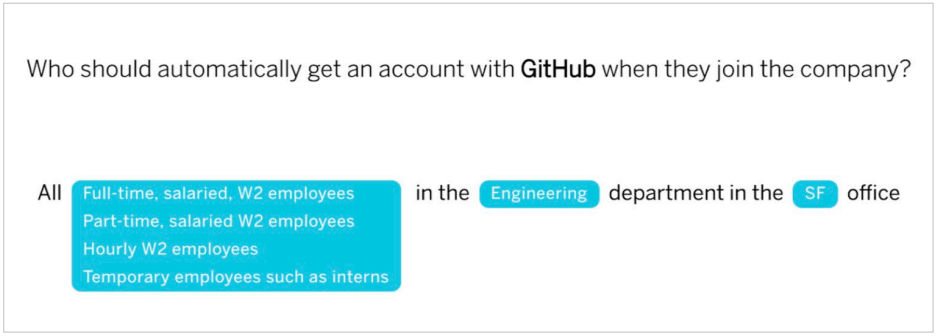
The SSH app lets you manage your developers' SSH access in the same seamless, automated way that you manage other cloud services in Rippling. When you install the SSH app, you can set up smart group rules indicating which employees should get access to which server groups. When an employee is configured to get access to at least one server group, Rippling prompts them to generate a public/private key pair and upload their public key to Rippling. **And most importantly, when an employee is offboarded, their public key entry is immediately removed from Rippling's LDAP service, so they can no longer connect to any servers**.



Configuring Rippling's IDM — Who Gets Access to What Apps, When, and Where.

Configuring Access Rules

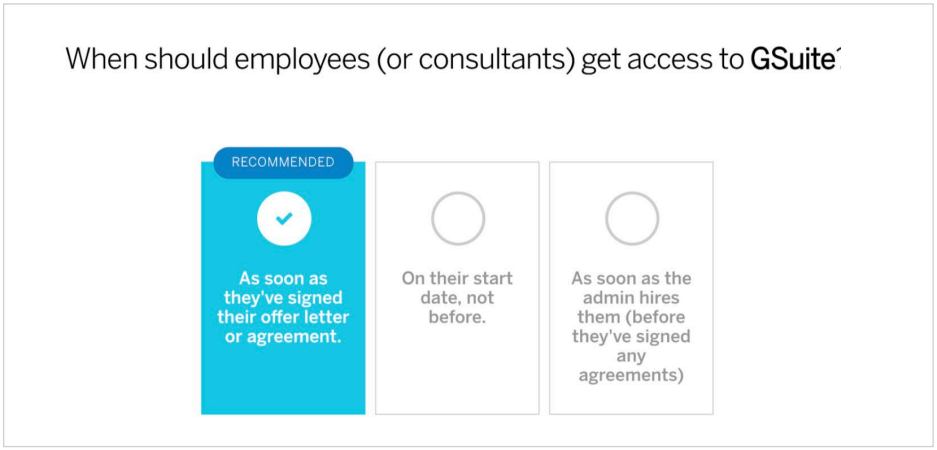
When installing an app, you configure a set of smart rules defining who should get access to the service. These rules allow granular selection and boolean logic between any of the employee attributes listed above.



When a new employee is onboarded or any of their attributes change, Rippling checks if the employee matches your configured access rules. If the matching status has changed, Rippling will take an action based on the type of app. For API apps, this generally means creating or suspending the employee's account. For SAML apps, the access rules control whether to allow Single Sign-On to the service from Rippling. For RPass apps, the access rules control whether to prompt the user to store their credential in RPass.

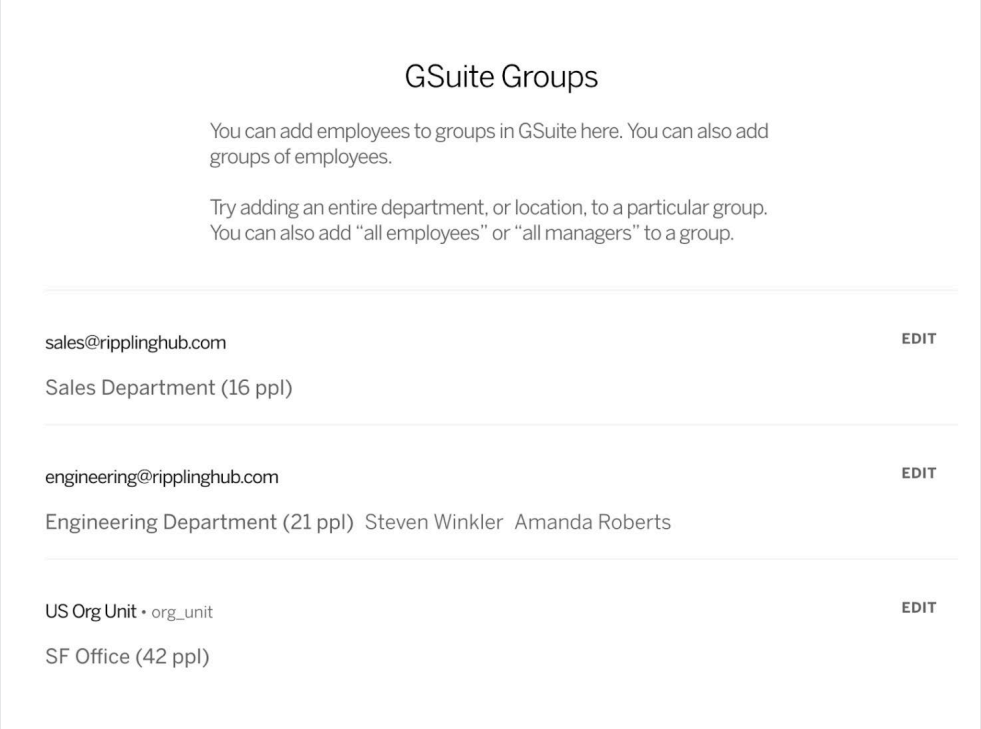
Configuring Access Time

Since Rippling's identity model manages the entire lifecycle of your employees, Rippling knows when a new hire has accepted an offer but not started employment yet. This lets you configure exactly when your employees get access to their accounts, so you can ensure they have a productive first day.



Configuring Group Rules (only applies for apps with APIs)
Many cloud services have some concept of a "group" of employees — for instance G Suite has mailing lists, Github has repos, Box has folders, and Slack has channels. These are all mapped to a unified model of "groups" in Rippling.

This concept of Rippling groups is a powerful abstraction because it lets you manage many other attributes of your employees' accounts in a simple and consistent way. You can use any of the employee attributes and smart rules to define which employees should be in which groups, and Rippling will maintain that group membership as employees join the company, change roles, and lave.



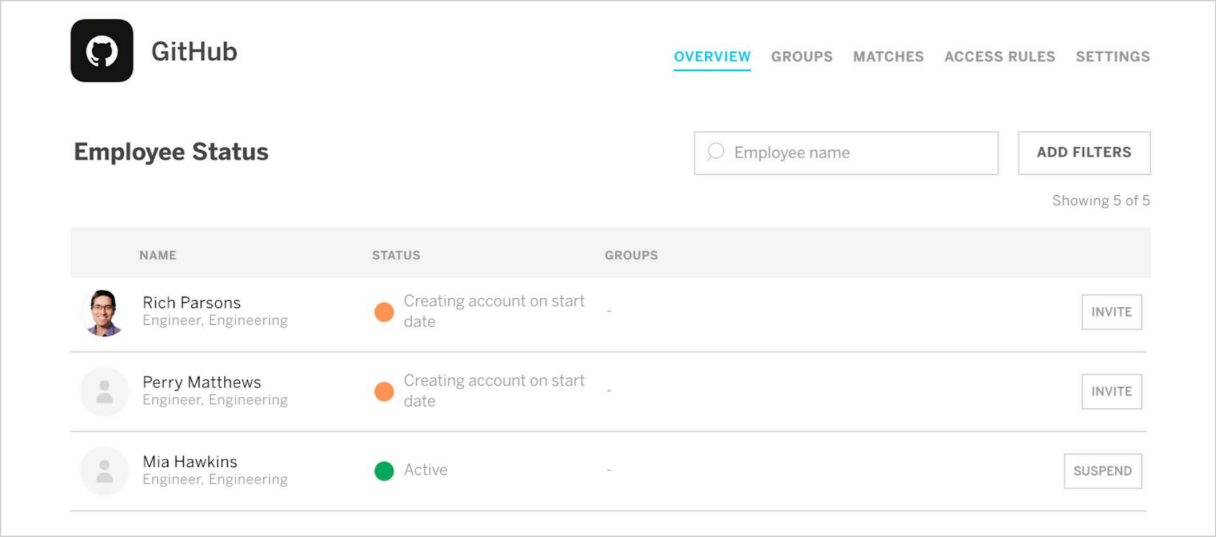
Note that Rippling generally doesn't create or delete groups in your cloud services since the meanings of those groups may be specific to that particular service. So for instance, if you have an Engineering department configured in Rippling, Rippling won't automatically create an Engineering channel in Slack. But if you have a #dev channel in Slack, you can configure Rippling to manage its membership and include everyone in the Engineering department.

Matching (only applies for apps with APIs)
When you install an app in Rippling for the first time, Rippling needs to know how the existing accounts in your cloud service correspond to your employees in Rippling. Rippling applies a set of heuristics to match accounts with employees based on the associated email address, name, or username. The person installing the app gets a chance to review the auto-selected matches and correct any mismatches.

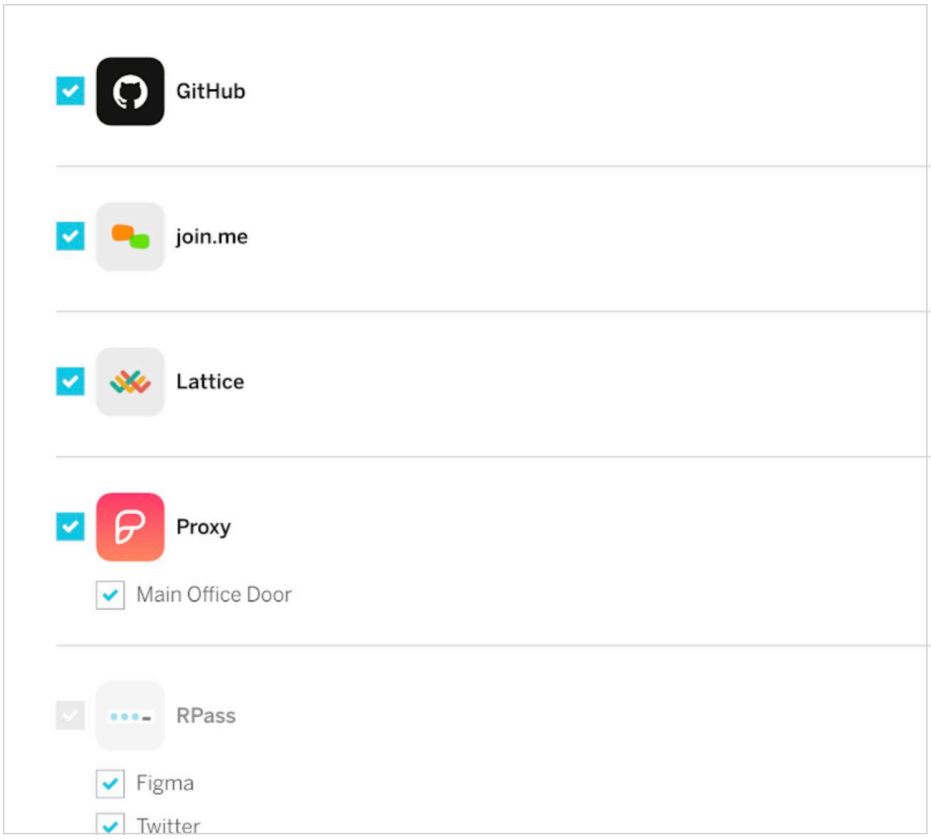
As part of the daily sync, if new accounts are detected in a cloud service Rippling will notify the corresponding app admins that they should match the accounts to employees. It's important to maintain the correct matching between accounts and employees, so that if an employee is offboarded, the correct account can be disabled.

Overriding Automatic Rules and Manually Updating Apps
In addition to configuring smart rules based on employee attributes, Rippling also allows for flexibility. This happens in one of two ways:

On each app's dashboard, the app admin can create or suspend an employee's account as a one-off, and add or remove a user from groups



In addition, when hiring a new employee, the hiring manager can choose to add or remove access to an app or group if they have permission to do so.



IN-DEPTH:

Integrating with your internal and external apps via Partner API, Rippling API, SAML, RPass, LDAP, and SSH.

IN-DEPTH:

Integrating with your internal and external apps via **Partner APIs**.

Many services offer open APIs that Rippling can connect to. This is generally the most powerful type of integration, because Rippling can read and update users, groups, and licenses, and automate many other actions as part of the employee lifecycle.

Installation
To install an API app, Rippling walks you through a couple quick steps that grant API access to the underlying cloud service. The exact type of authentication depends on the service. When possible, Rippling uses the OAuth 2.0 protocol, where you can tell the cloud service to grant limited access to Rippling with just a few clicks. OAuth 2.0 also allows for scoped access, and Rippling asks for the most minimal scope that allows managing users and groups.

Other services that don't support OAuth generally have an API key that you can copy and paste into Rippling.

Either way, the installation takes only a few seconds, and gives Rippling a durable and secure way to connect to the service.

Connecting to your cloud services is a responsibility that Rippling does not take lightly. See the Security section below for more information about how Rippling protects your API keys and OAuth tokens.

Daily Sync
Rippling uses the API to fetch a list of users and groups from the cloud service each night. This ensures that the data you see in Rippling is up-to-date, even if you or other users make changes to accounts directly in the cloud service.

You can also run a sync on-demand from the Settings page within each app.

Creating, Inviting and Deleting Users
There are two ways in which Rippling can decide that an account should be created or removed:

- When an access rule changes (for instance, or an app admin adds an account as an exception).
- When an attribute on the employee changes (for instance, when their start date occurs, or if they are moved to a different department).

When either of these occur, Rippling checks the employee's attributes against the configured access rules both before and after the change, and if the result is different, Rippling uses the API to create or remove the employee's account in the cloud service.

In most cases, Rippling does this by making a POST call to an endpoint in the service's API. The details depend on the particular API, but the POST body payload generally contains the employee's name, email address, and any other employee attributes that the service supports. Rippling checks the response of the POST call and correlates it with the results of fetching the user list from the service to be sure the account status changed successfully.

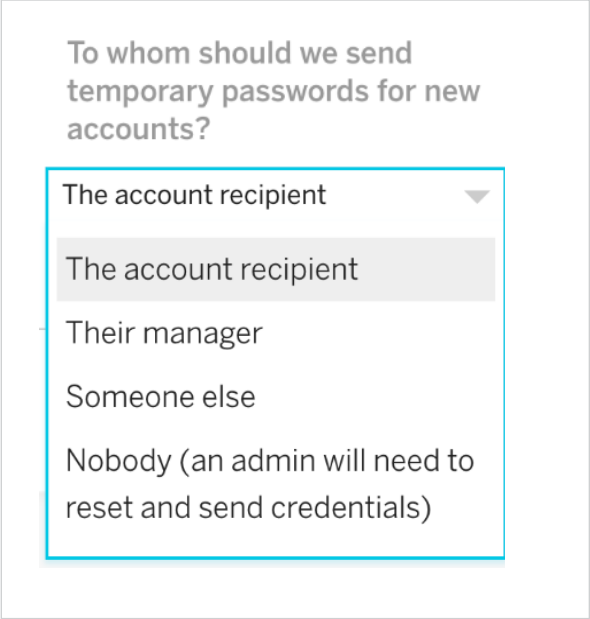
This "closed loop" process ensures that the account status you see in Rippling is an accurate representation. And if there's ever a problem detected with creating an employee account (e.g. the service requires purchasing additional licenses to provision the account), Rippling will notify the app admin via email and with a notification on their Rippling dashboard.

Some services don't expose an API endpoint to create accounts directly, but do have an API endpoint that sends invitations to the employee's email address which must be accepted before their account is created. For apps that use this invitation model, Rippling sends the invitation and then polls at least every 30 minutes to see when the user has accepted the invitation, and this status is displayed in the app dashboard in Rippling.

Setting Passwords

Many services support setting an initial temporary password in the API. If the service supports this, Rippling can set the password, and you can configure whether the temporary password should be sent directly to the new hire or to someone else.

Services that allow setting passwords generally also allow resetting passwords. An app admin can reset accounts' passwords from the app dashboard in Rippling.



Work Email Address

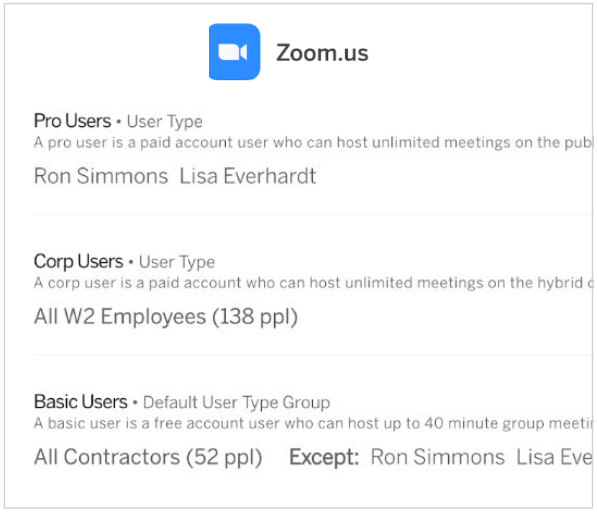
When onboarding a new hire in Rippling, the hiring manager is prompted for whether the new hire should get a work email address or not. If the hiring manager says yes, Rippling will collect the work email address of the new hire and use it to send the invitation for their accounts. Otherwise, their accounts will be created under the employee's personal email address.

GitHub Usernames

Some services like GitHub require a new user's username rather than their email address to create an account. If a new hire is configured to get access to one of these services, Rippling will prompt the new hire for their username during onboarding, and then send the invitation using that username. Admins may also enter GitHub usernames on the employee's profile page in Rippling.

Software Licenses

Many cloud services support different license types for user accounts, and it's important to create accounts with the right license type based on the role of the corresponding employee. Rippling lets you manage how licenses are assigned using smart group rules. For instance, in the video conferencing service Zoom for example, employee accounts can have either Pro, Corp, or Basic licenses, which can be managed in Rippling as groups.



This means that you can give some employees a Corporate Zoom account (like a full-time sales rep) and other employee ia Basic Zoom account (like a contractor or part-time employee).

Soft Deletion

Many services support a form of "soft deletion" for employee accounts. This may be called "suspending" or "disabling" an account, depending on the service. In general, when removing accounts, Rippling apps will perform a soft deletion if the service supports it. This allows you to suspend an employee's account immediately upon termination, and then give you or another admin time to take any remaining clean-up actions.

For instance, in G Suite, it's recommended that a G Suite admin go into the suspended account to recover any Google Drive files and set up email forwarding, then delete the account.

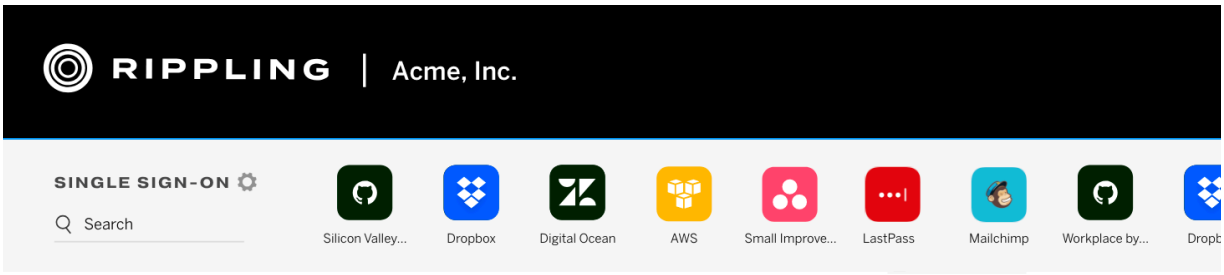
API Changes

Rippling maintains partnerships with API services so that if the underlying API is changed, Rippling is notified in advance and can update the integration accordingly. All such updates are seamless. The admins don't need to do anything to take advantage of the new API.

IN-DEPTH:

Integrating with your internal and external apps via **SAML**.

Many apps use the Security Assertion Markup Language (SAML) protocol to enable Single Sign-On (SSO) for employees. When a SAML app is installed, employees who should get access to the service will get an SSO link on their Rippling dashboard that automatically signs them into the service.



Pictured above: The Rippling Single Sign-On Bar: *Your employees can securely sign in to all of their apps and websites in just 1-click, via the Rippling SSO bar located in their dashboard.*

SAML Overview and Single Sign-On

SAML basically works by having the Identity Provider (in this case, Rippling) create an X.509 public/private key pair and transfer the public key to the Service Provider as part of installation and setup. Then when one of your employees clicks on an SSO link to the service from Rippling, Rippling causes the user's browser to make a POST request with a base64-encoded XML payload — called the SAML Assertion — to an endpoint on the service called the Assertion Consumer Service URL.

The SAML Assertion contains many fields, including an identifier for the user (generally an email address), restrictions on when the assertion expires and what it may be used for, and other metadata about the user.

It is also signed with the X.509 private certificate created by Rippling. The service reads the SAML Assertion and verifies the signature using the X.509 public certificate. If the assertion is valid, the service automatically logs the user in. From the user's point of view, it's simply one-click access to the service they need, without having to remember a password.

Since only Rippling has the X.509 private certificate and the private certificate never leaves Rippling's servers, nobody can log into the service unless they have valid access through Rippling. X.509 is the same technology underpinning TLS/SSL and HTTPS, and the SAML protocol is an open standard well-accepted by the security and IT community.

Rippling uses industry standard best practices for setting metadata in the SAML assertion that optimizes for security while maintaining end user ease-of-use.

You can view an example of the SAML assertion generated here.

Installation

When you install a SAML app, Rippling walks you through step-by-step instructions for setting up the SAML connection. The details vary based on each service, but in most cases you'll need to copy/paste a certificate or metadata file from Rippling into the external service. You may also need to copy/paste a URL or entity id from the external service back into Rippling.

SAML JIT

Many services support "just in time" (JIT) provisioning of accounts along with SAML. So when an employee clicks on the Single Sign-On link in Rippling for the first time, the service will automatically create the employee's account and log them into it.

Notifications
If a SAML app does not support API provisioning and does not support JIT, Rippling will notify the app admin when an account must be created for a new hire. This gives you a central dashboard and audit log for all account provisioning and deprovisioning, even for services that can't support automated account management.

Admin Account
Rippling lets you optionally designate one account in the cloud service as the admin account for that service. Any employees with full admin permissions in Rippling will be allowed to SSO to that admin account.

This is useful for giving your admins access to functionality that is tied to a separate service account. For instance, you might have a single G Suite admin account that has access to your G Suite Admin console, in addition to the regular non-admin SSO link for G Suite that takes users to their GMail inbox.

SP-Initiated Logins & Mandatory SSO
Many services allow you to disable traditional password-based logins for employees, thus requiring employees to use SSO. This can make your organization more secure, since employee passwords can't be hacked, and you can immediately remove an employee's access upon termination by revoking their SSO access.

Services that support such mandatory SSO will generally also support "Service Provider Initiated" logins, whereby an employee that tries to sign in on the service provider's site will be redirected to Rippling, log in on Rippling, and then be redirected back to the service provider.

Rippling apps support Service Provider Initiated logins whenever the underlying services supports them.

IN-DEPTH:

Integrating with your internal and external apps via **RPass**.

RPass (Rippling's password manager for teams) provides all the features you would expect of a modern password manager: zero-knowledge password vault, team sharing, etc. But you can also use RPass to manage accounts in cloud services in a consistent way even if they don't support API or SAML integration.

RPass Overview and Single Sign-On

You can read the RPass whitepaper for more information about the RPass security model and inner workings.

When you install an RPass app in Rippling, you configure an access rule that defines who should get access to the service, just as with an API or SAML app. Employees that should get access to the service are prompted to enter their account credentials into RPass.

Once an employee has saved their account credentials into RPass, a Single Sign-On link for the service appears in the employee's Rippling dashboard, just as a SAML-based Single Sign-On link would. Clicking the link takes the user to the service's login page and automatically signs them in with the password in the RPass vault. From the user's point of view, it feels just like more traditional Single Sign-On: one click, and they have access to the service they need.

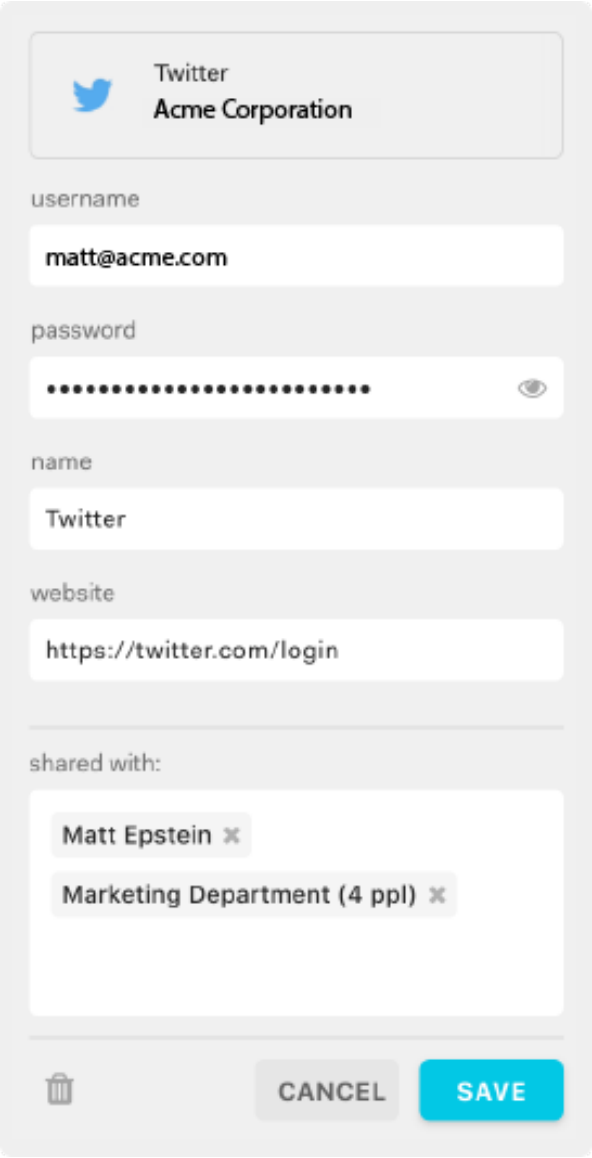
Notifications

As with some SAML apps, RPass apps can't automatically create or remove accounts in the corresponding cloud service. But by using RPass apps to track accounts, Rippling will notify app admins when accounts need to be created for new hires, and give you an audit trail of when the app admins did this.

Offboarding

When an employee with access to an RPass app is offboarded, they immediately lose access to any passwords saved in their RPass company vault. Furthermore, a notification is sent to the app admin reminding them to remove the employee's account from the underlying cloud service, with an audit trail of when the admin confirms this has been done.

RPass in action: *Here's what your employees will see when they share their password with a fellow coworker via RPass, which is available on their desktop and mobile device.*



IN-DEPTH:

Integrating with your internal and external apps via **LDAP and Rippling's REST API**

Virtual LDAP Overview

The Virtual LDAP app in Rippling gives you access to your employee data in Rippling via the industry standard LDAP protocol, which is also used by Microsoft's Active Directory. Any service that connects to LDAP can be pointed to Rippling's LDAP service.

One very common use case is for a company transitioning away from a legacy on-premise Active Directory server. Since Active Directory uses the LDAP protocol, almost any service that currently connects to your Active Directory server can easily be routed to Rippling's LDAP service instead. And unlike Active Directory, Rippling's data is automatically kept in sync when employees are onboarded and offboarded.

Rippling's Virtual LDAP app supports simple authentication (also known as simple bind). Data is organized in the usual Distinguished Name format; for instance, users are contained in ou=users,dc=yourcompany name,dc=rippling,dc=com. Rippling's Virtual LDAP is a read-only system supporting BIND and SEARCH operations.

Rippling REST API Overview

Many Rippling customers have custom in-house systems to which they need to provision and deprovision user access. For that, Rippling exposes a REST API with endpoints to read and interact with employee data, groups, payroll, and PTO. The API is developer-friendly and can be set up within minutes.

Here are some examples of what Rippling customers have done with the API:

- Sync employee list to provision accounts in internal software systems.
- Populate an intranet with names, photos, and contact info of new hirees.
- Read and manage group membership
- At a professional services company, use Rippling custom fields to store employees' proficiencies and pull that into employee assignment and scheduling software.
- At a gig economy company, push real-time commissions and bonuses into Rippling's payroll system.
- Fetch PTO requests to show who is out of office on the company's internal homepage.

For more information, please refer to our Rippling API documentation.

IN-DEPTH:

Integrating with your server infrastructure using **SSH keys.**

SSH Key Management Overview

The SSH app lets you manage your developers' SSH access in the same seamless, automated way that you manage other cloud services in Rippling.

When you install the SSH app, you can set up smart group rules indicating which employees should get access to which server groups. When an employee is configured to get access to at least one server group, Rippling prompts them to generate a public/private key pair and upload their public key to Rippling.

Rippling then walks you through setting up sssd on your servers. Sssd is an established open-source library that allows Unix accounts to be driven by a remote identity provider. When an employee uses SSH to connect to one of your servers, the sssd process looks up the employee's public key from an LDAP service provided by Rippling, then uses the public key to authenticate the login.

From your employees' point of view this process is invisible — they simply log in with private key authentication like they're used to. But from an IT and DevOps point of view the change is immense — admins no longer have to maintain SSH keys consistently across the server fleet.

And most importantly, when an employee is offboarded, their public key entry is immediately removed from Rippling's LDAP service, so they can no longer connect to any servers.

Rippling IDM Security Overview

Rippling Security Overview

At Rippling, we understand that connecting to your cloud services is a serious responsibility, and we go to great lengths to protect your data.

Protecting API Keys

- Rippling uses OAuth 2.0 whenever possible. This modern protocol allows for scoped access tokens, and time-limited access with periodic refreshes. So you're always in control of what Rippling has access to.
- Rippling requests access tokens with the minimal scopes required to manage your accounts, and nothing more.
- Your company's data is logically partitioned from any other clients, with a deeply-ingrained role-based permission system that prevents unauthorized access.
- API keys and access tokens are encrypted at rest and in transit.

Protecting SAML Certificates

- Rippling uses a different certificate for every client and every app installation, so there's no way for your certificate to be used by anyone outside your company.
- Your company's data is logically partitioned from all other clients, with a deeply-ingrained role-based permission system that prevents unauthorized access.
- SAML certificates are encrypted at rest and in transit.

Security is at the Heart of What Rippling Does

- All data is transferred using 256-bit TLS 1.2+ encryption, which is the latest cryptographically secure algorithm used by banks and governments.
- Bank-grade AES encryption protects your data at rest. We follow industry best practices for defense in depth: data is encrypted with multiple keys, keys are rotated regularly, and sensitive data uses end-to-end encryption.

A Strong Team Enables Strong Security

- We keep our team up-to-date on the latest security practices with regular security and privacy awareness training. New features go through extensive testing and peer review with a rigorous SDLC.
- Admin access requires a strong password with two-factor authentication, and separation of duties is built in to sensitive tasks.
- Security teams work around the clock to protect your data and respond to threats.

Tested and Trusted

- Rippling works with independent third-parties as well as external researchers who regularly assess our site for vulnerabilities. All data is hosted and processed in an SSAE 16 SOC2 compliant data center, with 24/7 physical security.

How Rippling Identity & Access Management Makes Your Organization More Secure

Eliminate Weak and Reused Passwords
Research by Verizon concluded that 81% of corporate data breaches are due to weak or compromised passwords. By enabling SSO for your employees -- and better yet, enabling mandatory SSO for services that support it -- you can simply eliminate the most common cause of data breaches.

Enforce MFA Across All Your Cloud Devices
Not all cloud services support Multi-Factor Authentication (MFA), which is an industry best-practice for securing accounts. But by enabling MFA for logins to Rippling, and using Rippling as the SSO Identity Provider for other services, you can effectively enable MFA for services that don't otherwise provide it.

Instantly Disable Accounts During Offboarding
Immediate removal of offboarded employees' accounts is essential to preventing malicious behavior by someone who has nothing to lose.

Centralize Logging and Account Activity Visibility
By managing account creation, deletion, and SSO in one place, you have a central dashboard for monitoring account activity throughout your entire organization. Review audit trails, identify abnormal behavior, and pass compliance audits with ease.

About Rippling's High Availability Architecture

We understand that you and your employees need access to their cloud services 24/7, with no disruption. As an identity manager, we take this responsibility very seriously, and we built the whole product around ensuring that Rippling will always be available whenever you need it.

Rippling achieves high availability through an architecture of redundancy, avoiding single points of failure, and continuous monitoring.

Rippling's API servers are clustered behind a load balancer, and distributed across multiple AWS availability zones. API servers are kept stateless to allow easy horizontal scaling.

The database leverages MongoDB, one of the most widely deployed and trusted NoSQL solutions. Data is replicated live to multiple backups that can be elevated to master within seconds. In addition to the live backups, data is dumped nightly and stored in redundant availability zones.

Server infrastructure is monitored 24/7, and Rippling's infrastructure team regularly reviews and plans future capacity to account for growth.

As a result of these efforts, Rippling has passed a SOC2 Type 1 audit that included attestation to the availability controls of Rippling's system.