BetterCloud
Powering Cloud IT

A Comprehensive Guide for Google Apps

Onboarding, Offboarding & Everything in Between

A Training Guide for Google Apps Admins from BetterCloud

Table of Contents

1. Introduction
2. The 4 Layers of the User Lifecycle
3. Onboarding
4. Common ULM Events
    a. User's Name Changes
    b. User's Profile Changes
    c. User Changes Team
    d. User Gets Promoted
    e. User Goes On Leave/Vacation
    f. User Joins a Project
    g. User Needs to Reset Password
    h. User's Account is Compromised
5. Offboarding

Introduction

From onboarding and offboarding, to managing org unit changes and group memberships, to updating a user's contact info, user lifecycle management (ULM) is no small responsibility. That's why we created this guide: to help you navigate and manage user lifecycles at your organization.

We interviewed customers and IT experts to pinpoint common challenges, pain points, and scenarios to create this guide. It will walk you through the major changes you might need to make throughout the entire user lifecycle. You'll read about common ULM events, best practices for managing and protecting data, and procedures that can mitigate risk. These scenarios are in no way meant to be exhaustive, but they'll provide a foundational start.

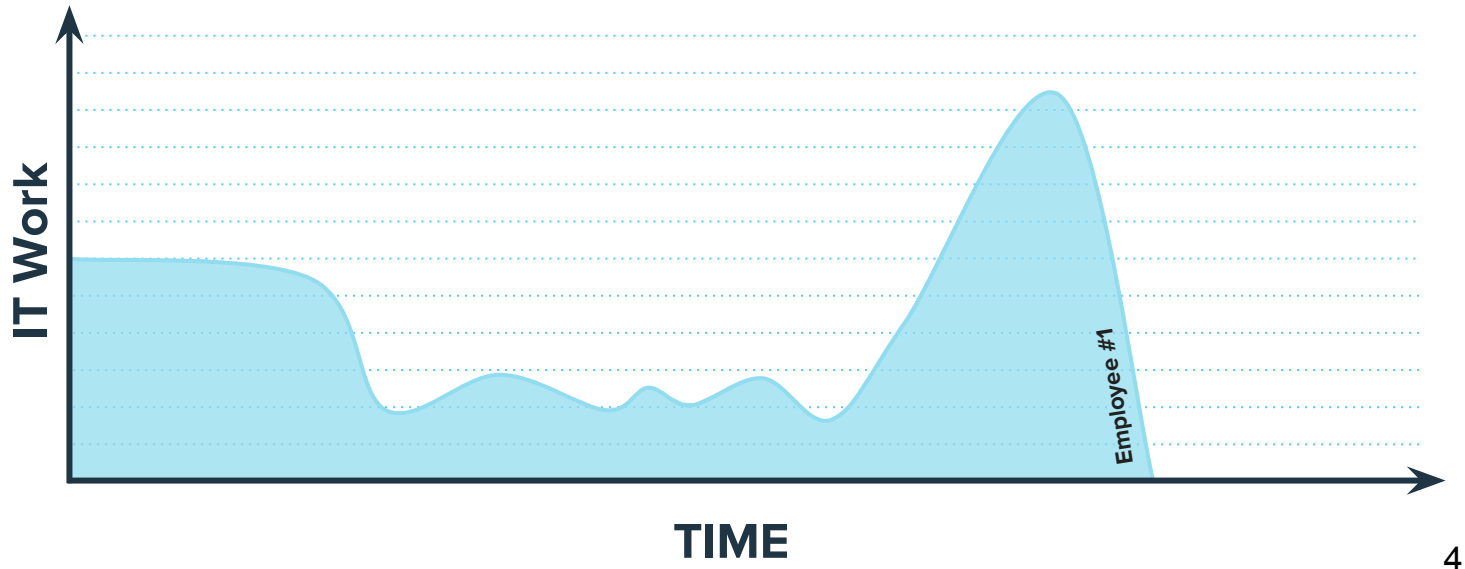
We hope you find this guide useful.

—The BetterCloud Team

Introduction

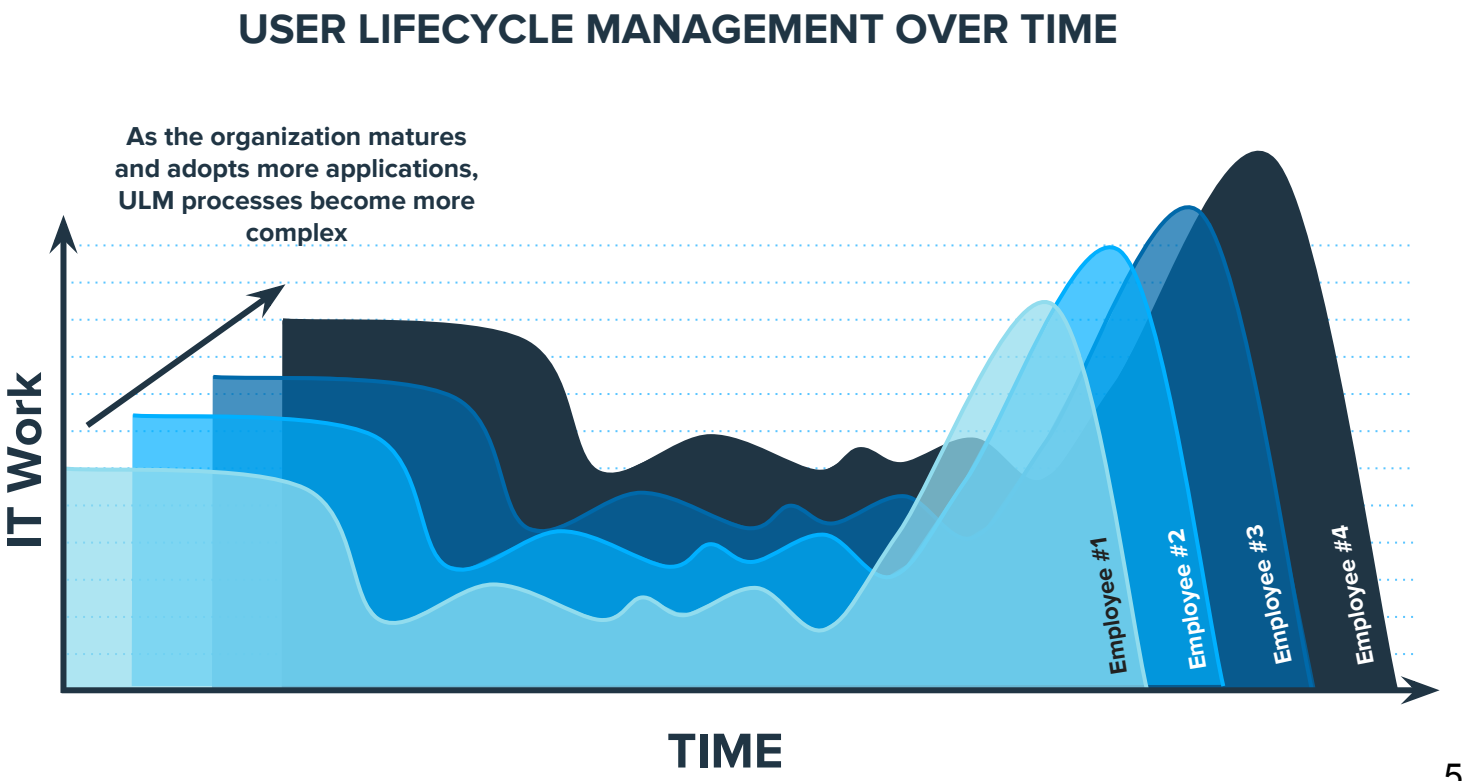
Not only must ULM processes enable employees to do their jobs effectively, but they must also keep company data secure. ULM is a complex process, and it demands different work from IT over time. It creates especially complex situations at offboarding, when a user has created significant data during their time at the company and likely has access to many critical assets and systems.

USER LIFECYCLE MANAGEMENT OVER TIME



Introduction

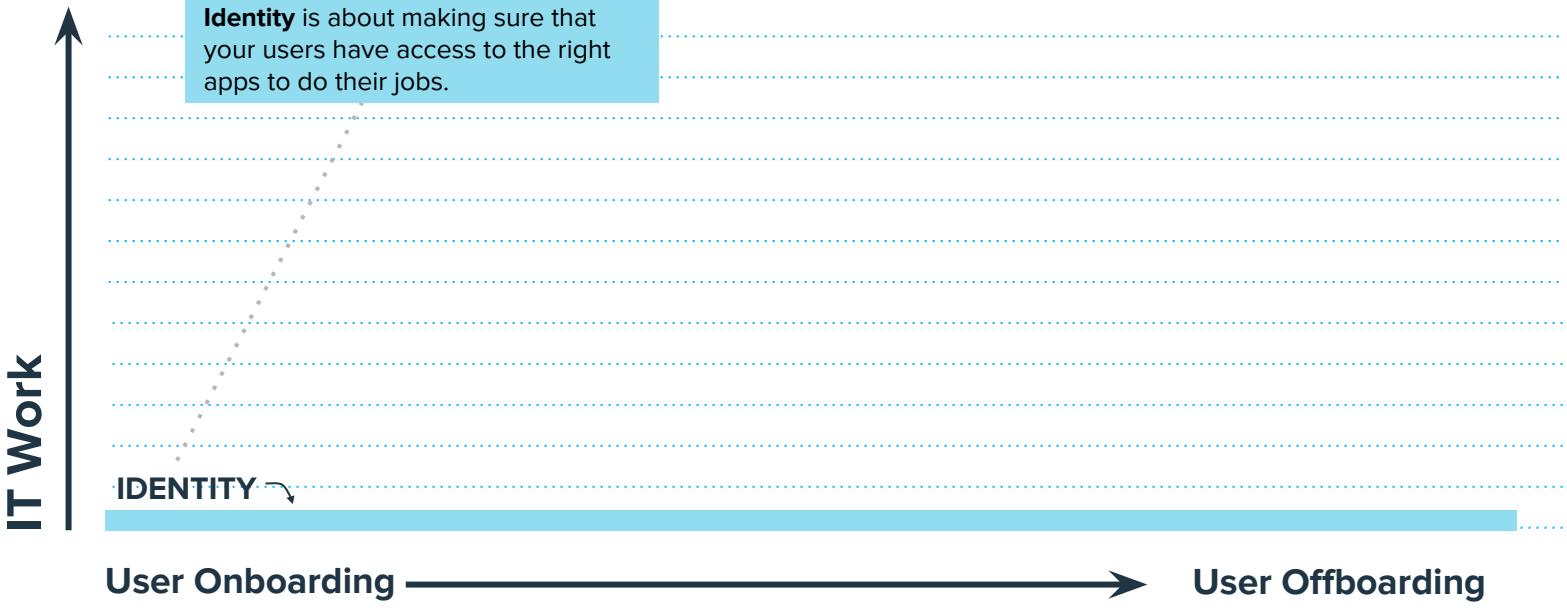
Furthermore, these ULM processes only get more complex over time as companies add in additional SaaS applications, or the organization starts using existing SaaS applications in more complex ways (e.g., Google Drive).



The 4 Layers of the User Lifecycle

We've identified four layers in the user lifecycle. Each one is critical to effective user management, and we'll be using them as a framework when we discuss ULM events. The first layer, **Identity,** is all about making sure that your users have access to the right applications to do their jobs. For example, employees typically need email and perhaps enterprise chat (e.g., Slack or Hangouts). From there you'll grant access by department (e.g., sales gets Salesforce, marketing gets Marketo). Many IT professionals stop here when they think about their ULM processes, but in reality, this is just the bare minimum. Think of it as a baseline. Identity is an incredibly important part of effective user lifecycle management–without access to the right applications, users simply can't do their jobs. Identity is also the most basic layer; it doesn't take into consideration everything that happens inside of those applications over time.

USER LIFECYCLE TIMELINE LAYERS

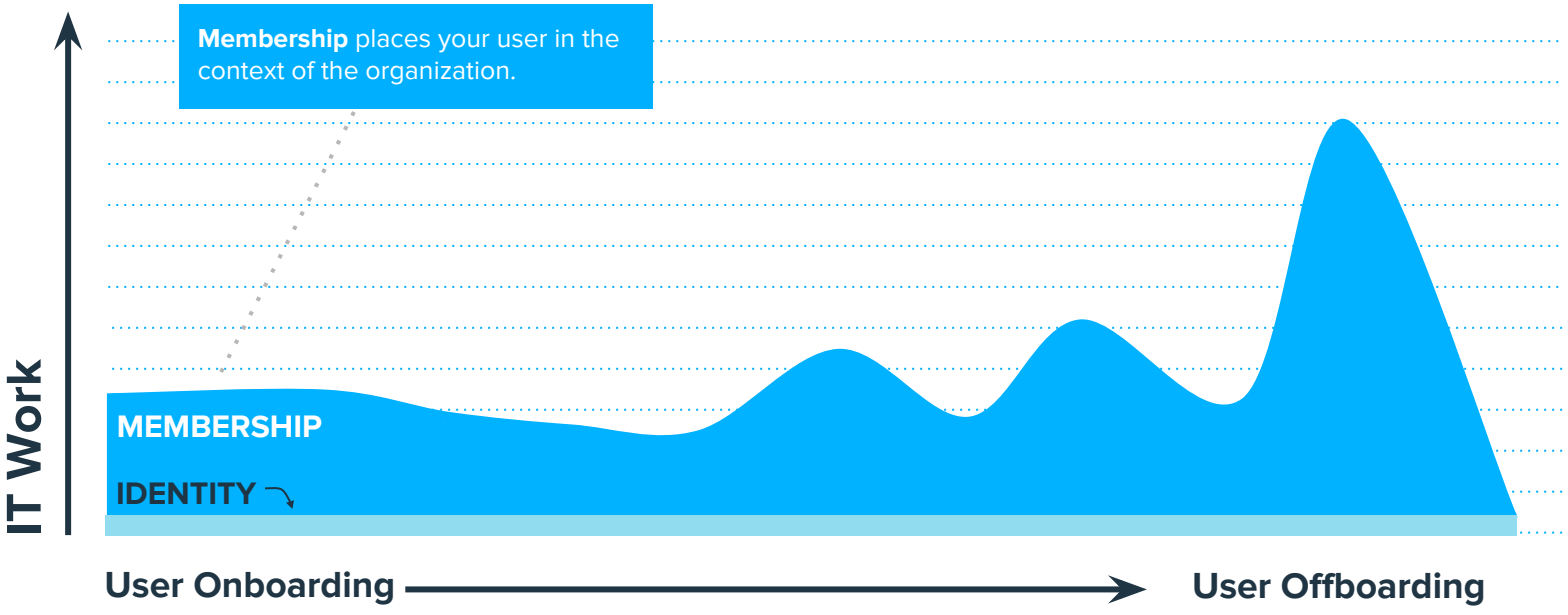


The 4 Layers of the User Lifecycle

The second layer, **Membership,** places your user in the context of the organization. It represents the OU and groups that a user belongs to. This layer ensures proper communication and sometimes even access to different systems and data. It sounds so simple, but think about it: If you place a user in the wrong OU, or don't include them in the right groups, they'll fail to receive critical information. This is a vital component to ULM, but many IT professionals don't pay enough attention to this layer.

For example, a VP of Sales for North America needs to be in the Sales OU and have access to the right apps. He needs to be in the right groups—perhaps sales@, leadership@, and northamerica@, just to name a few. His co-workers may assume that he's already in these groups, but if he's not, he'll miss out on vital emails.

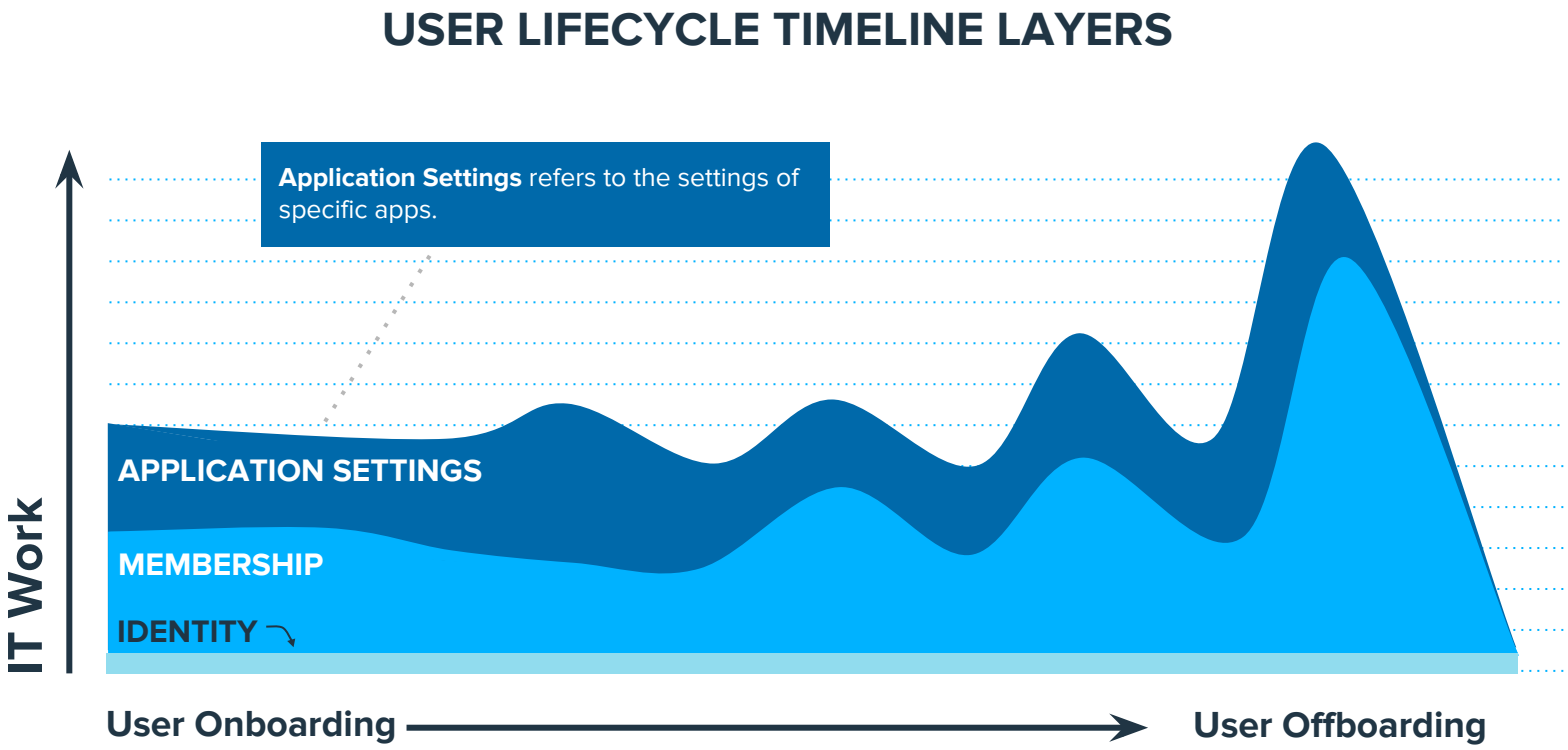
USER LIFECYCLE TIMELINE LAYERS



The 4 Layers of the User Lifecycle

Application Settings refer to the settings of specific apps like Gmail, Drive, Calendar, etc. These settings may have to be changed over time, depending on specific ULM events.

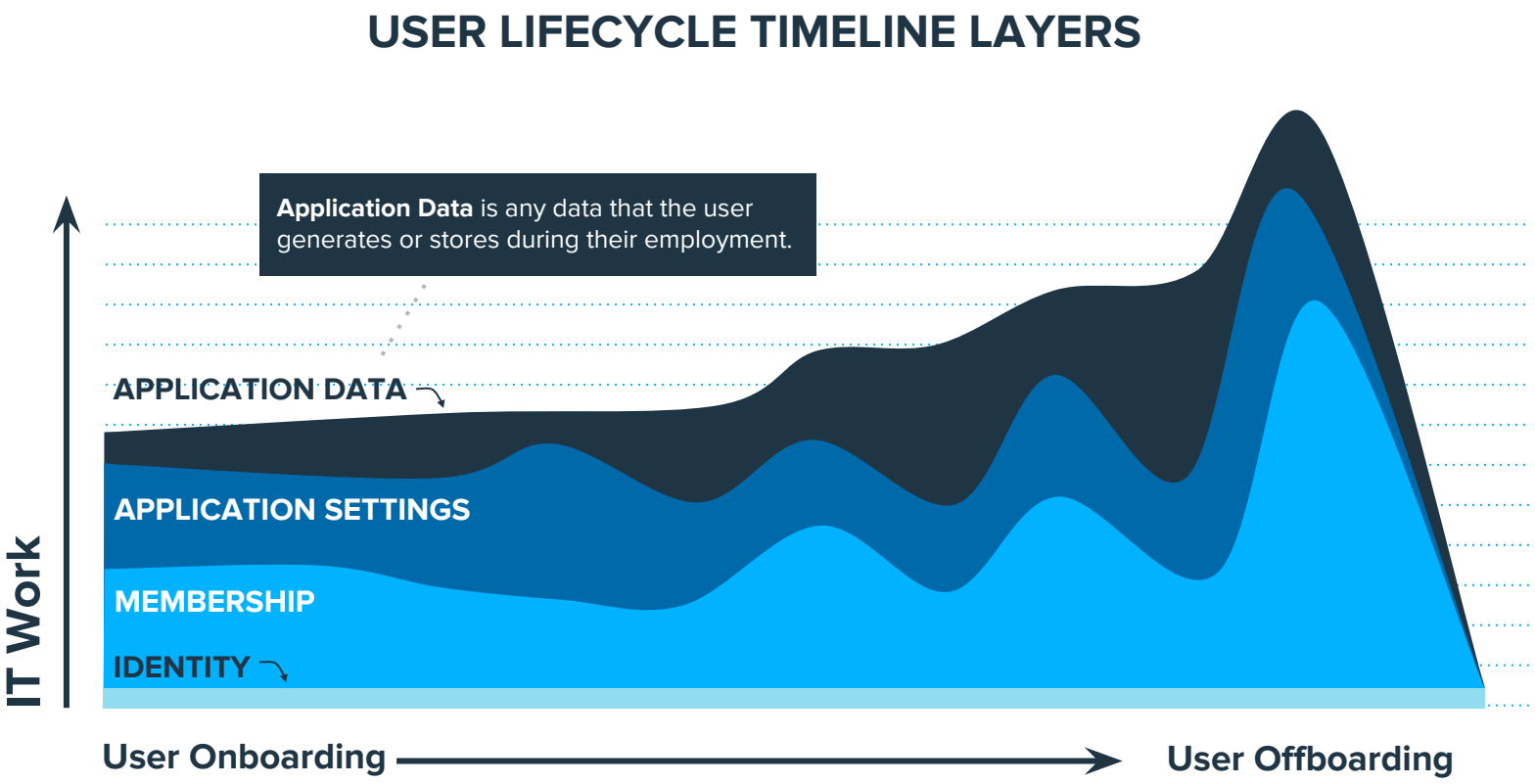
For example, if an employee goes on vacation, you may need to create an out-of-office message or delegate their inbox, which requires changes in Gmail.



The 4 Layers of the User Lifecycle

And finally, **Application Data** is pretty straightforward—it's any data that the user generates or stores. This can include data in Drive, Gmail, Calendar, Contacts, etc. Throughout any given user's tenure, he will create hundreds, if not thousands, of files, so the amount of data accumulates drastically over time. This becomes an important layer during the offboarding process; at that point, you need to decide if you want to transfer all the data, archive it, or delete it.

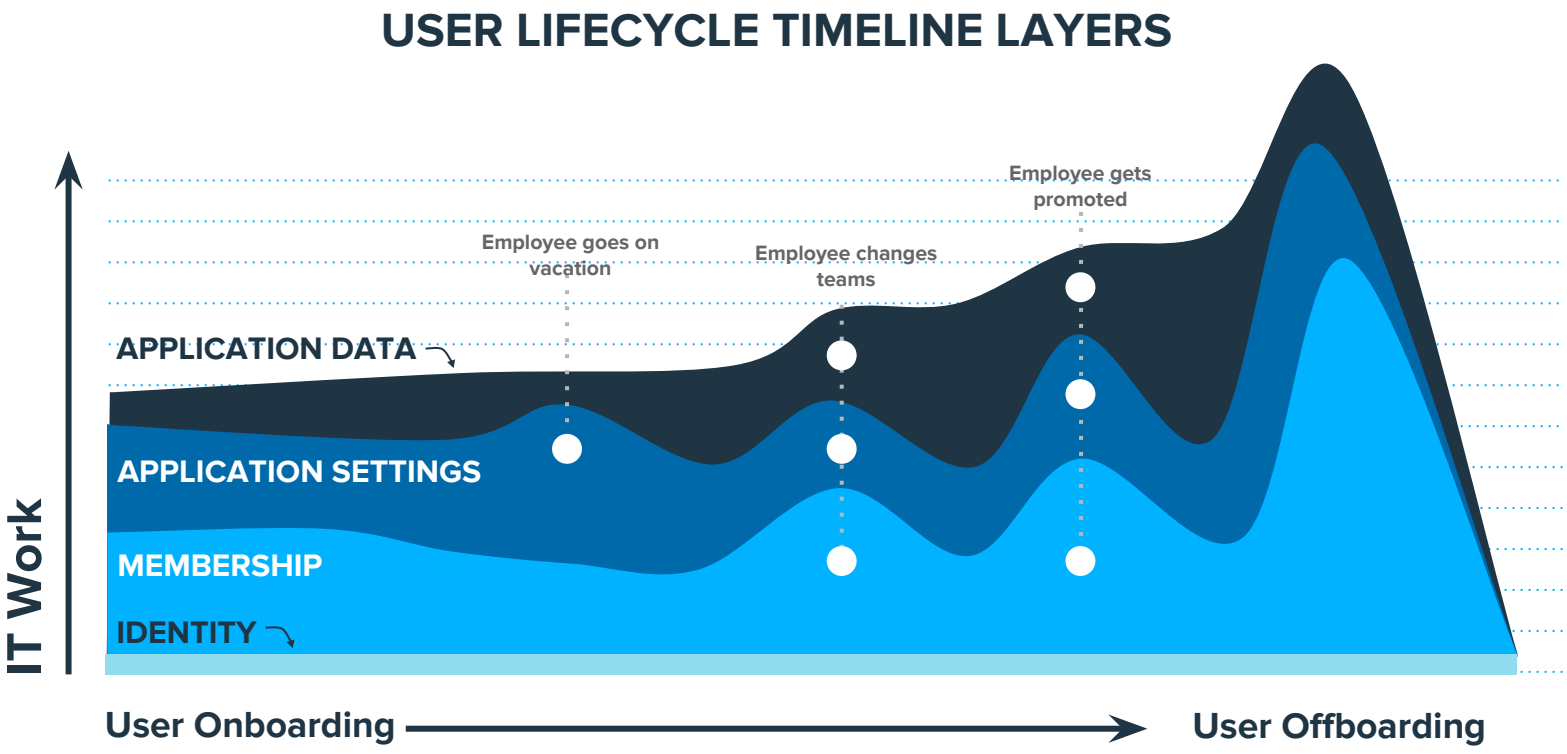
When all four layers are combined together, you can see that ULM is a multidimensional process that grows more complex over time.



The 4 Layers of the User Lifecycle

Now that we've discussed each layer individually, let's combine them and show how a few key ULM events interact with each layer. For example:

- **Employee goes on vacation:** This event primarily affects the Application Settings layer, because it only involves modifying settings (like creating an auto-responder in Gmail) in applications.
- **Employee changes teams:** This event falls into multiple layers. It touches the Membership layer (the user's groups/OU membership will change), the Application Settings layer (his email signature will change), and the Application Data layer (he will continue to generate data).
- **Employee gets promoted:** This event also falls into multiple layers. Like the example above, it affects the Membership layer (the user may be added to additional groups), the Application Settings layer (his email signature will change), and the Application Data layer (he will generate more data, given his additional responsibilities in his new role).



Onboarding

Now that we've discussed the four layers of ULM to provide some context, let's get to the first component of ULM: onboarding.

When new hires show up at the office on their first day, bright-eyed and bushy-tailed, they want to hit the ground running. But incorrect provisioning can prevent them doing their jobs effectively, resulting in loss of productivity—or even worse, improper access to sensitive data.

Here are **five critical provisioning steps** that'll keep your organization secure and set up your users for success.

1. Create a new user

To start off the provisioning process, you'll have to create a new user account and input basic information like the user's name, email address, and password.

You have a few options for adding users. You can add users individually using the Admin console (which we will show you how to do in this guide), or you can add several users at once by uploading their names in a CSV file.

Onboarding

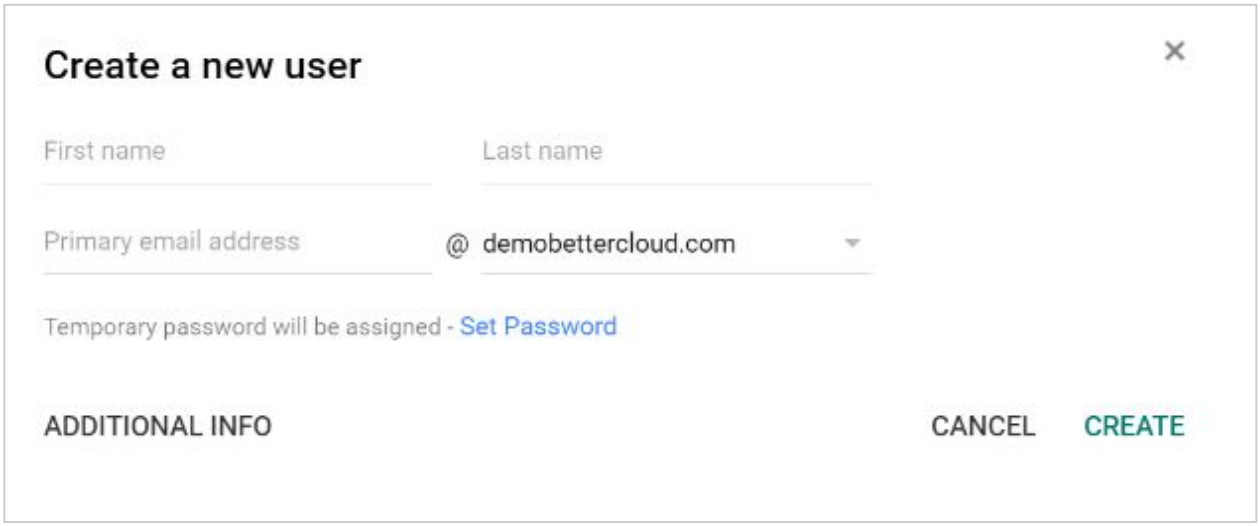
For large organizations with hundreds or thousands of users, there are additional options you can use:

- Google Apps Directory Sync (GADS) can sync user data in your existing LDAP directory with your Google account. This will sync groups, contacts, and organizations.
- The Admin SDK Directory API can provision multiple users from your existing LDAP directory (for example, Microsoft's Active Directory).
- Google Apps Migration for IBM® Notes® (if you're migrating from IBM Notes).
- A single sign-on (SSO) tool.

Here's how create new users individually in the Admin console:

- In the Admin console dashboard, go to Users > click  **to add user** > enter their **First name, last name, and email address.** If your account has multiple domains associated with it, use the dropdown menu to select the correct domain.

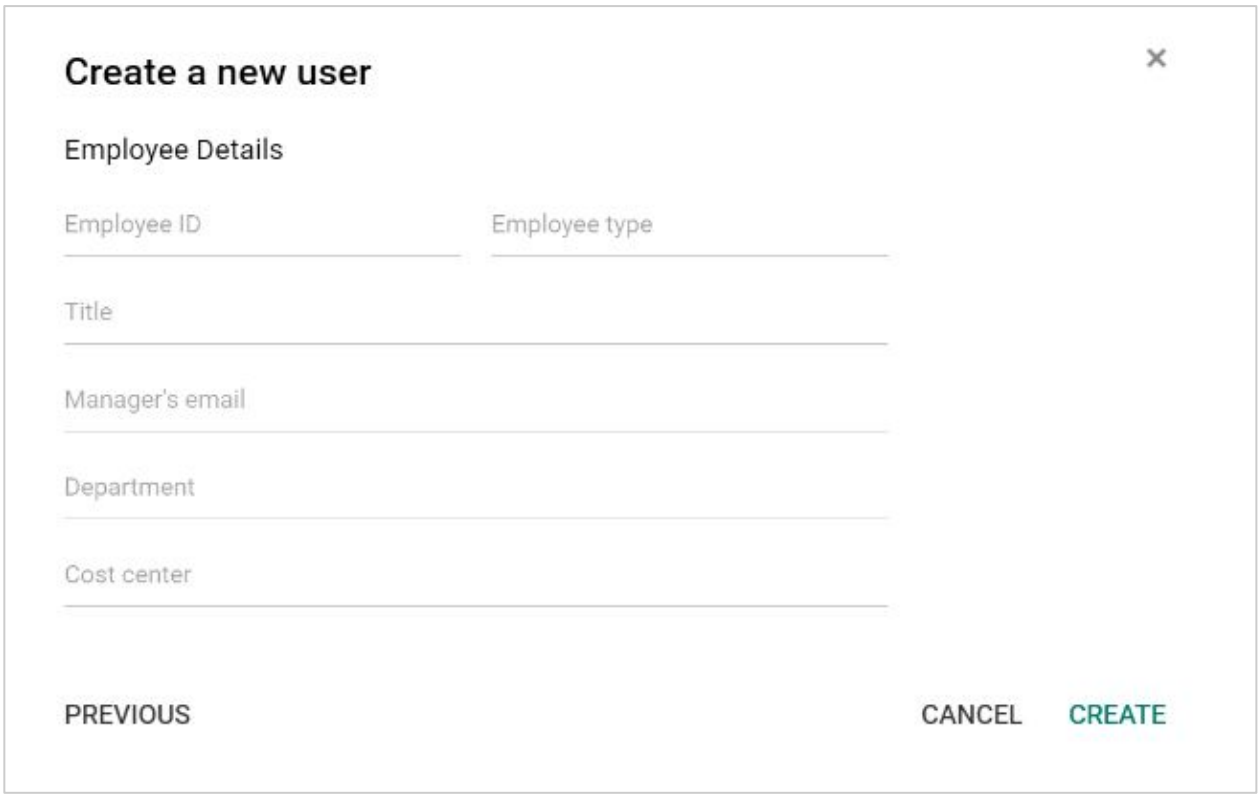
Onboarding



- The Admin console will create a temporary password with a mix of symbols, upper and lower case letters, and numbers. If you'd like to set the password yourself, you can do that as well.

- [Optional]: If you want to add additional contact information (e.g., a work address or a cell phone number) or employee details (e.g., employee ID number or cost center), click **Additional info**.

Onboarding



- Click **Create** > **Send email** or **Print** to send the account information to the new employee. (If you're emailing instructions, just remember to send it to the user's personal email address, not this new one you're creating.)
- Click **Done.**

2. Apply email signature

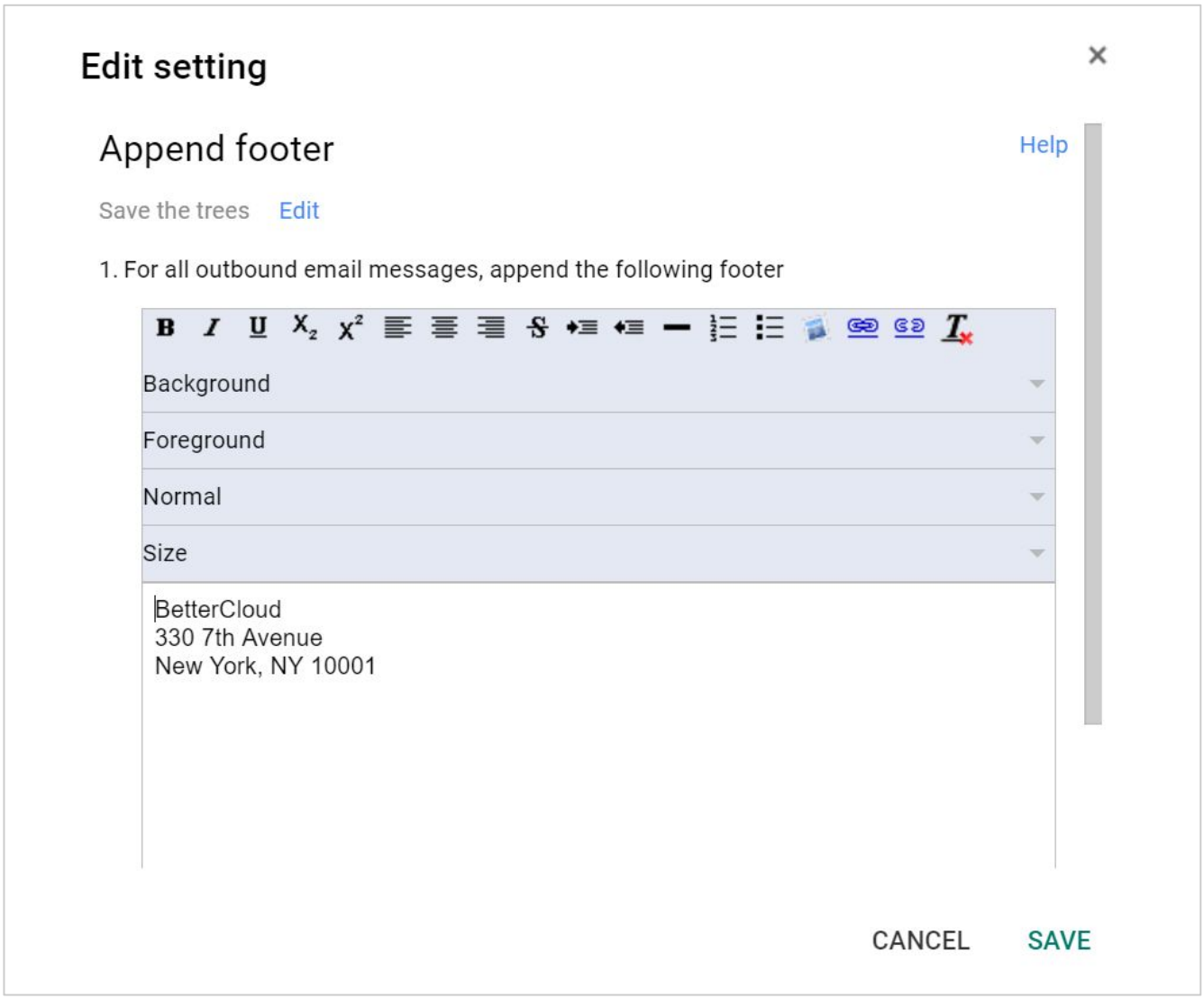
Append your organization's email signature to the user's emails. A standardized email signature helps your organization maintain brand consistency and provides a professional, visually coherent look.

For Google Apps for Education and Business users, Google recommends using the Google Email Settings API to programmatically update Gmail settings for multiple users. For Google Apps for Work customers, Google recommends using the API or the Append footer setting to add automatic signatures for all of your users. We'll outline how to use the Append footer feature below, but there are limitations to this solution. The information must be the same for everyone in the domain or in particular OUs, so if you want personal or customized information in your email signatures, you can either log into the user's account to create them, or use a third-party tool.

- In the Admin console dashboard, go to **Apps** > **Google Apps** > **Gmail** > **Advanced settings.**
- Scroll down to **Append footer.** If the status underneath says:
    - **Not configured yet** → click **Configure** to configure the setting.
    - **Locally applied** → click **Edit** to edit an existing setting or **Add another** to add a new setting.
    - **Inherited** → click **View** to view the setting or **Add another** to add a new setting.

Onboarding

- Enter in your organization's email signature using the formatting tools provided.



BetterCloud
Powering Cloud IT

Pro Tip: Create customized email signature templates in BetterCloud and apply them to individual users, groups, org units, or the entire domain. Set a signature policy to ensure signature standardization.

3. Determine org unit membership

Add the user to the appropriate organizational unit (OU) and necessary groups. A user can belong to multiple groups, but only one OU.

- In the Admin console dashboard, go to **Users** > select the user and click on their name.
- Click  to add the user to a group.
- Click  to move the user to another OU.

What's the difference between an OU and a group? OUs determine which Google services and features (e.g., Drive, Calendar, Google+, Sites, Adwords, Google Analytics, any Marketplace app) are available to a user, as well as how your IT team can act on those users through delegated access roles (e.g., the APAC IT team can only work on users in the APAC OU). Meanwhile, a user's group membership determines which emails they will receive.

Click here to learn more about OUs vs. groups.

BetterCloud
Powering Cloud IT

Pro Tip: During the provisioning process, use BetterCloud's Time Saver option to mirror the group/OU memberships of an existing user on your domain, or better yet, use Workflows to automatically add users to groups/OUs based on customizable criteria.

4. Send a welcome email

Send a welcome email to your new user's personal email address containing any vital IT information they should know on day one. At the very least, this email should include their login name, password, and instructions on how to log in for the first time. We recommend that they also be required to change their password upon first logging in. Here's some other information you might consider including:

1. How to set up 2-factor authentication
2. The best way to contact IT (e.g., ticket submission system, phone numbers for the help desk, email addresses)
3. Your acceptable use policy
4. Security tips around recognizing phishing attempts, who to report suspicious activity to, etc. You may also want to include Do's and Don'ts (e.g., don't leave your computer unlocked, don't click on suspicious links)
5. Phone instructions (e.g., their extension, how to check voicemail messages for the first time, etc.)
6. Printer instructions
7. FAQs

5. Share the right files and grant the right permissions

Making sure your new user has access to the right Drive files, folders, Sites, and Calendars is an important step in the onboarding process, so that they can get up and running quickly. Unfortunately, there is no native way in the Admin console for an admin to add collaborators to shared Drive files, folders, etc., unless all of these have already been shared with the admin team as well. Additionally, if you add a user to a group, the user will not be aware of what shared files or folders they automatically have access to; they need to have the exact link to the document or folder (unless you use third-party tools).

If managers create their own shared folders for their teams, and IT is not a collaborator on these folders and files, then the onus lies on managers to share the right files and grant new hires the right permissions. In this sense, IT loses a degree of control during the onboarding process. Employees will lose productivity if they have to wait hours or days to get access to the information they need, and IT cannot help with this aspect. Conversely, managers could put the organization at risk for compliance violations if they accidentally grant new hires *more* access than is required.

Pro Tip: Save valuable time by automating the provisioning (and deprovisioning) processes with BetterCloud Workflows. Automate away human error by automatically adding users to the right groups/OU and automatically sharing the right Drive files with a user. Create templates for users in certain departments or roles to onboard with the appropriate access and information in minutes.

Onboarding

That wraps up provisioning, but you're not quite done with onboarding yet. Many IT professionals leave out an essential step that truly helps set up users for success: an "IT welcome" meeting. For more information, read our article here: Onboarding Isn't Just Provisioning: Are You Leaving Out This Vital Step?

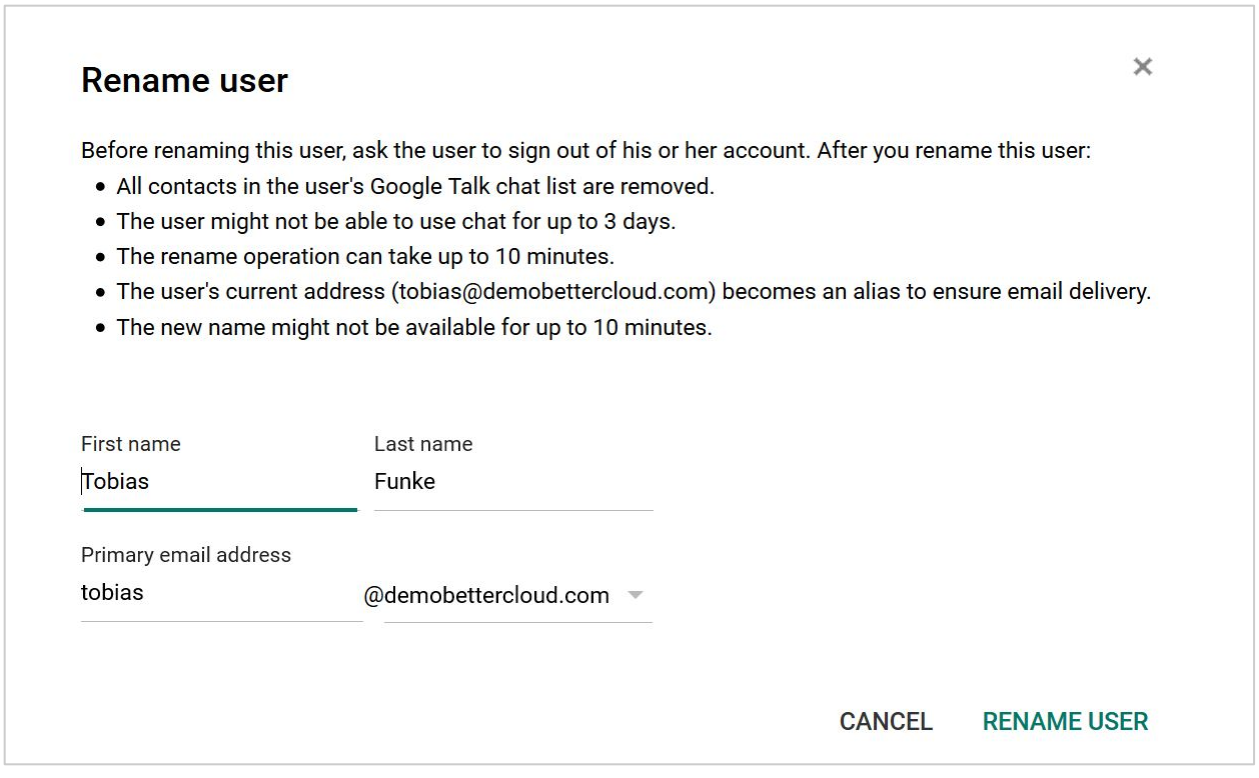
Onboarding is just the first part of ULM. Over the course of a user's employment with a company, there will be many user management tasks requested of you. Here are some common scenarios that may arise and how you can handle them.

User's Name Changes

Employees may want to change their names if they get married, divorced, or just want to be known by another name. If a user's name changes, you can change his display name, as well as his primary email address.

- In the Admin console dashboard, click on **Users** > Find the user you'd like to rename > **Click on the pencil icon** on the right side by their name.

- You can change his first name and/or last name in the fields provided. When you do this, you're changing his default display name.
- You can also change his primary email address, which changes the name he uses to sign into his Google account.



User's Name Changes

- Click **Rename user** when you're done.

Note: Changing a username can have other consequences. Read more on the impact of changing a username.

A few points to keep in mind:

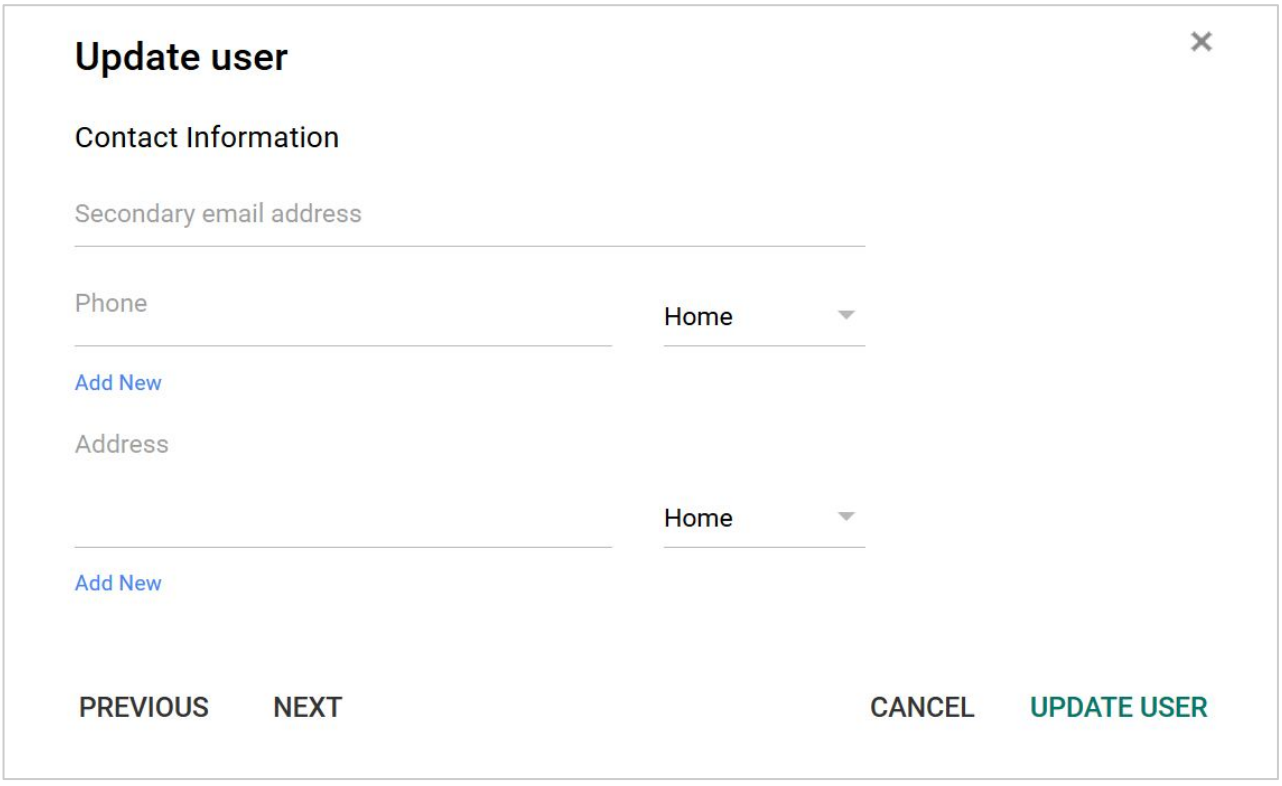
- The user's old primary address will now be an alias, in order for email to be continuously delivered. To reuse the old address, delete the email alias.
- Any emails sent to the old address will be delivered to the new one.
- The old email address will still appear in autocomplete results (because it's an alias).
- The user will retain access to any mail received under the old address.

Tip: If a user just wants another email address, consider creating an email alias instead of changing their name.

User's Profile Changes

There are a few scenarios where you may need to update a user's profile. For example, if an employee changes teams, gets promoted, changes managers, or moves offices, you'll want to update their profile information. If you want to update a user's secondary email address, phone number, address, employee ID, employee type, title, manager, department, or cost center, here's how to do it:

- In the Admin console dashboard, click on **Users** > Click on the user's name > **Account.**
- Under Basic information, click **Edit** > **Additional info.** Here, you can add or change a secondary email address, phone numbers, or addresses. If you want multiple fields, click **Add new.**
- Click **Next** if you want to add an employee ID number, title, department, and more. Then click **Update user** when you're done.



User Changes Team

Let's say one of your employees moves from the customer support team (in the New York office) to the HR team (in Atlanta). This is a weightier lifecycle task because it touches upon multiple ULM layers: Identity (he will need access to new HR apps); Membership (his groups and possibly OU will need to be updated); Application Settings (his email signature will also need to be updated); and Application Data (more data will accrue over time).

A few notable actions to take are:

- Updating the user's profile (with a new title, address, phone number, etc.)
- Moving him to a different group(s) and possibly OU
- Giving him access to any new apps required for the new role
- Revoking access to apps he no longer needs
- Updating his access to the right files, folders, Calendars, etc.
- Updating his email signature

To move a user to a different group:

- In the Admin console dashboard, click on **Users** > click on the user's name.
- Click  to add him to a group.

User Changes Team

Alternatively, you can also do this:

- In the Admin console dashboard, click on **Groups >** click on the Group you'd like to add the user to > Manage users in (Group name).
- In the Add new members box, **type the name, username, or email address** of the user you'd like to add.
- In the "**Add as"** dropdown menu, choose whether you'd like to add them as a **member or owner.**

To move a user to a different OU:

- In the Admin console dashboard, click on **Users >** click the user's name.
- Click  to move him to another OU.

Alternatively, you can also do this:

- In the Admin console dashboard, click on **Users >** click the filter icon > select the OU they are currently in.
- Find the user in the list and click on his avatar. It will turn into a checked box.
- At the top of your screen, click  to move him to another OU.

User Gets Promoted

Let's say a marketing director at your organization gets promoted to VP of marketing.

Again, this is a substantial event because it falls into multiple ULM buckets: Identity (he may need access to new apps that only execs use); Membership (he will need to be added to new groups and possibly OU); Application Settings (his email signature will also need to be updated); Application Data (he will likely generate even more data than before, since he has additional responsibilities in his new role).

Many of the necessary steps are similar to those taken when a user changes teams. However, because this ULM event involves a promotion, this means he will likely need more powerful administrative privileges.

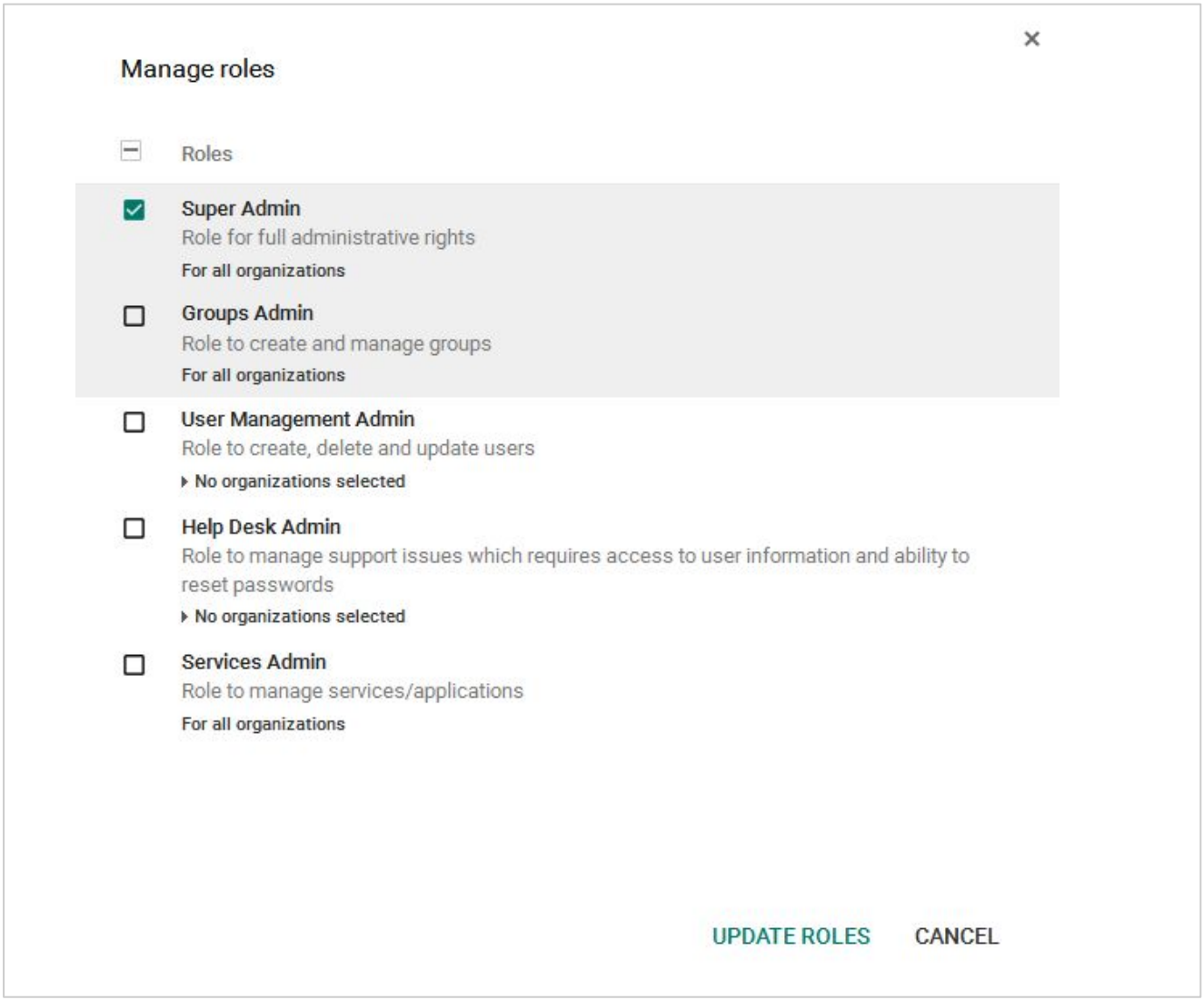
For example, you may want to make him an owner (rather than a member) of a group. Or you may want to assign an administrator role to him, so that he can perform select management tasks in the Admin console (e.g., create new groups in the Admin console, manage members of groups, or manage group access settings).

You can assign pre-built roles or custom roles.

User Gets Promoted

To assign pre-built roles:

- In the Admin console dashboard, click on **Users** > Click on the user's name > Show more > **Admin roles and privileges.**
- Click **Manage roles** > Check off the role you'd like to assign to the user.
- Click **Update roles.**



User Goes On Leave/Vacation

When a user goes on leave or vacation, it can be helpful to set up an auto-reply message on their behalf, so that people emailing them are aware that they're out of the office. However, in the Admin console, short of resetting a user's password, logging into their account, and setting up an auto-responder, there doesn't appear to be a native way to do this.

Pro Tip: Use BetterCloud to set up email autoresponders that automatically apply to a user's Gmail account. This is triggered based on customizable criteria you can set.

If a user is on leave for an extended period of time, you may also consider hiding them from the directory, have them delegate their inbox to another person who can send or reply to emails sent to them, or even suspend their account. They won't be able to log into their account while they're suspended, but their email, documents, calendars, and other data will remain saved, and their shared documents will still be accessible to others. When the user returns, you can restore their account.

Pro Tip: Use BetterCloud to easily delegate a user's inbox to another user. BetterCloud allows this action to be implemented without the confirmation of the receiving user, which is not possible in the standard Control Panel.

User Joins a Project

Sometimes, teams may need to work cross-functionally and collaborate together on a project.

If a user joins a project, the important ULM layer to keep in mind is Membership. You'll need to add him to the correct groups (or even create a new group for the project). Additionally, you'll need to make sure he has access to the right files, Calendars, folders, Sites, etc. for the duration of the project.

If the project is temporary, remember to revoke membership access after the project finishes.

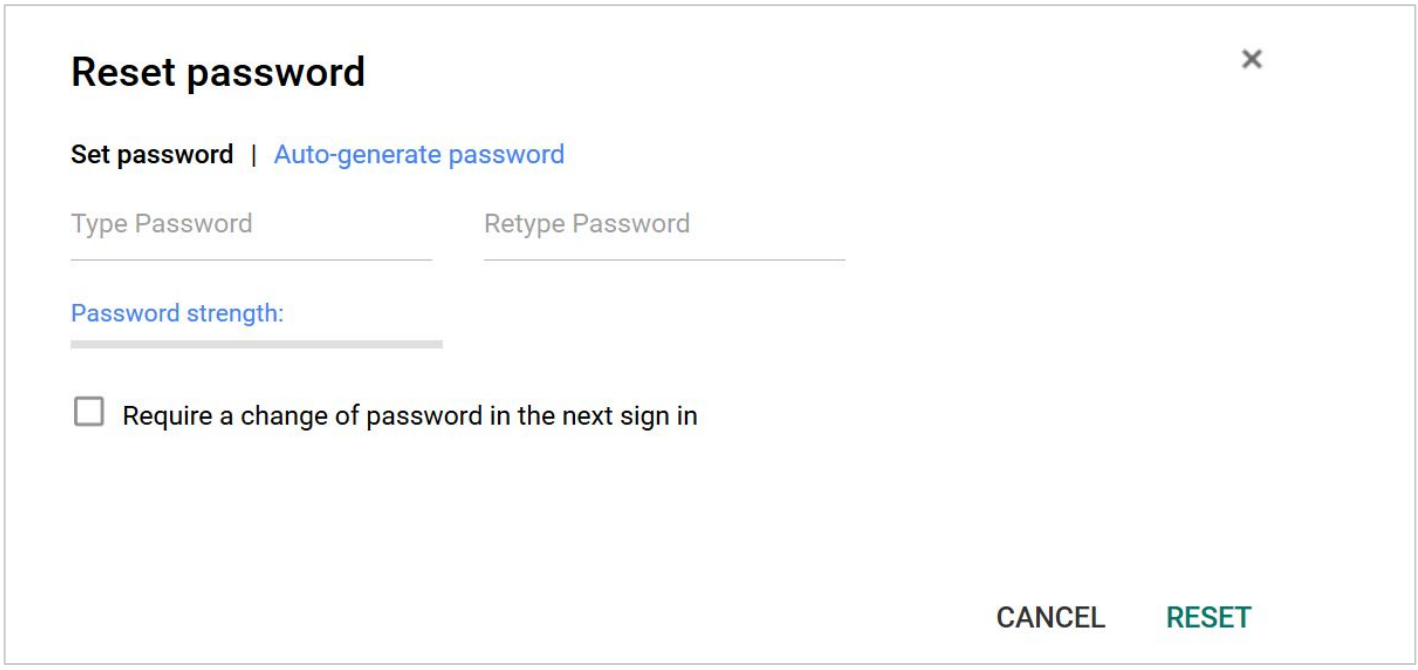
User Needs to Reset Password

It happens to the best of us: You can't seem to remember your password, no matter how hard you try.

To reset a user's password:

- In the Admin console dashboard, click on **Users** > find the user you'd like to rename > **click on the lock icon** on the right side by their name.

- Type and retype the new password. You can also click **Auto-generate password** to automatically generate a new password.
- If you want to require a change of password in the next sign in, check the box. Click **Reset** when you're done, and send the user their new password.



User's Account is Compromised

Users may misplace their company computers or fall victim to phishing scams. If a user's account is compromised, you should act immediately in order to prevent any exposure of sensitive data.

Here are a few key steps to take:

- Suspend the user's account to prevent any unauthorized access.
- Reset sign-in cookies. This will log the user out from all current HTTP sessions and require new authentication the next time a login is attempted, thereby blocking access to Google Apps.
- If you're using Google MDM, remotely wipe the device.
- Strongly consider setting up 2-factor verification, if you haven't done so already.

Offboarding

Offboarding users is the most resource-intensive component of ULM. By this point, the departing employee has created a substantial amount of files and data, and you're left with a few questions: Where does the data go? Does it need to be saved—if so, for how long? Should we suspend or delete the user?

We've distilled the offboarding process to **12 general steps,** but of course, this may vary from organization to organization, depending on individual policies and preferences. These are general best practices to follow.

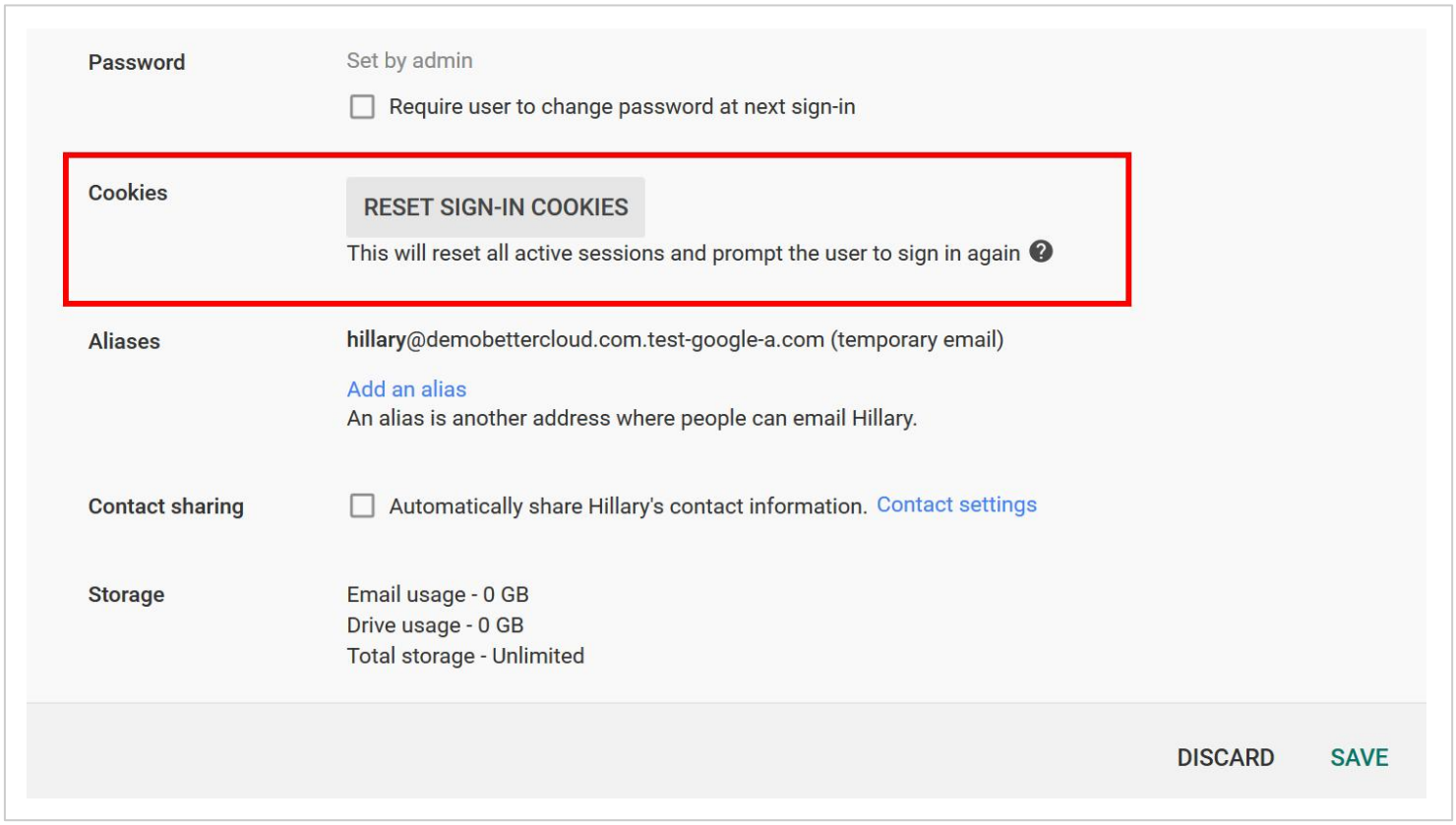
Pro Tip: Automate the deprovisioning process with BetterCloud Workflows. Customize your own workflow and automatically reset passwords, hide users from the directory, delegate inboxes, transfer files, and suspend accounts.

1. Reset password/sign-in cookies

Reset the user's password to prevent them from logging into their account. This is a crucial security step, as a disgruntled former employee could potentially tamper with files or send inappropriate emails. It's also a good idea to reset their sign-in cookies and/or require a password change on the next sign-in. This way, you'll log them out of any current sessions and also prevent further access.

To reset sign-in cookies:

- In the Admin console dashboard, click on **Users** > click on the user you want to hide > Account.
- In the **Cookies** section, click **Reset sign-in cookies** > click **Reset sign-in cookies** again to confirm.



2. Find a new owner

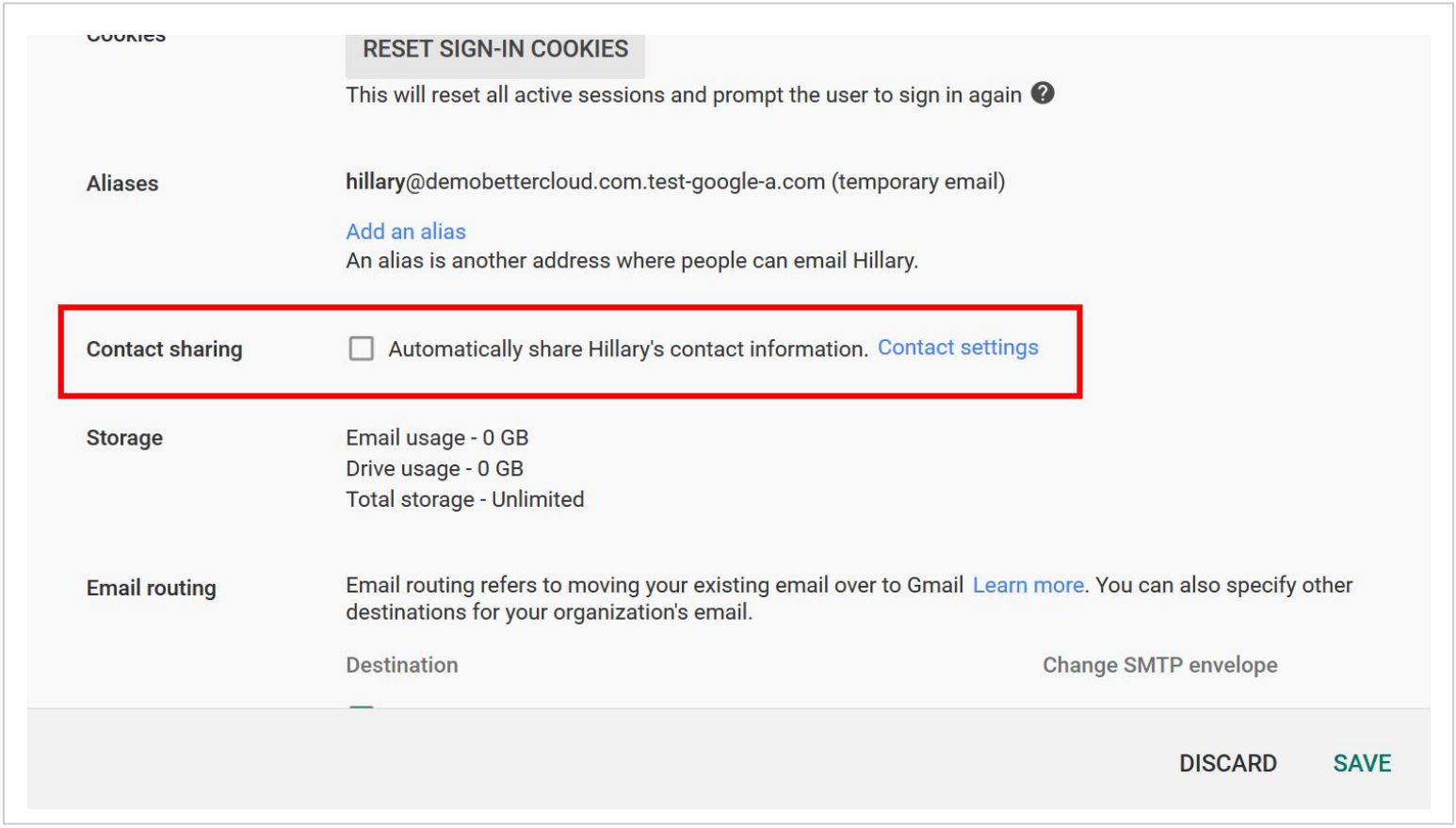
You'll need to find an account executor to become the owner of the user's digital property (e.g., documents, Calendars, groups owned). Usually this is the user's manager, a trusted supervisor, or a new account owner.

Offboarding

3. Hide user from the directory

When you hide someone from the directory, their contact information will no longer appear when employees type their email address into services like Gmail and Calendar. The user's profile also will no longer appear in Contact Manager. If you use messaging apps like Slack, hide the user in those as well.

- In the Admin console dashboard, click on **Users** > click on the user you want to hide > **Account** > **Contact Sharing.**
- Uncheck the **"Automatically share contact information"** box.
- Click **Save.**



4. Set up an autoreply email

Set up an automatic response to people who are trying to send emails to the user, and provide information on who should be contacted instead. Here's an example:

Please be advised that Dwight Schrute is no longer with Dunder Mifflin. If you have any inquiries, please direct them to Michael Scott at mscott@dundermifflin.com.

Note that not all companies may want to set up an autoresponder, so check with your HR department and/or company policy on this step.

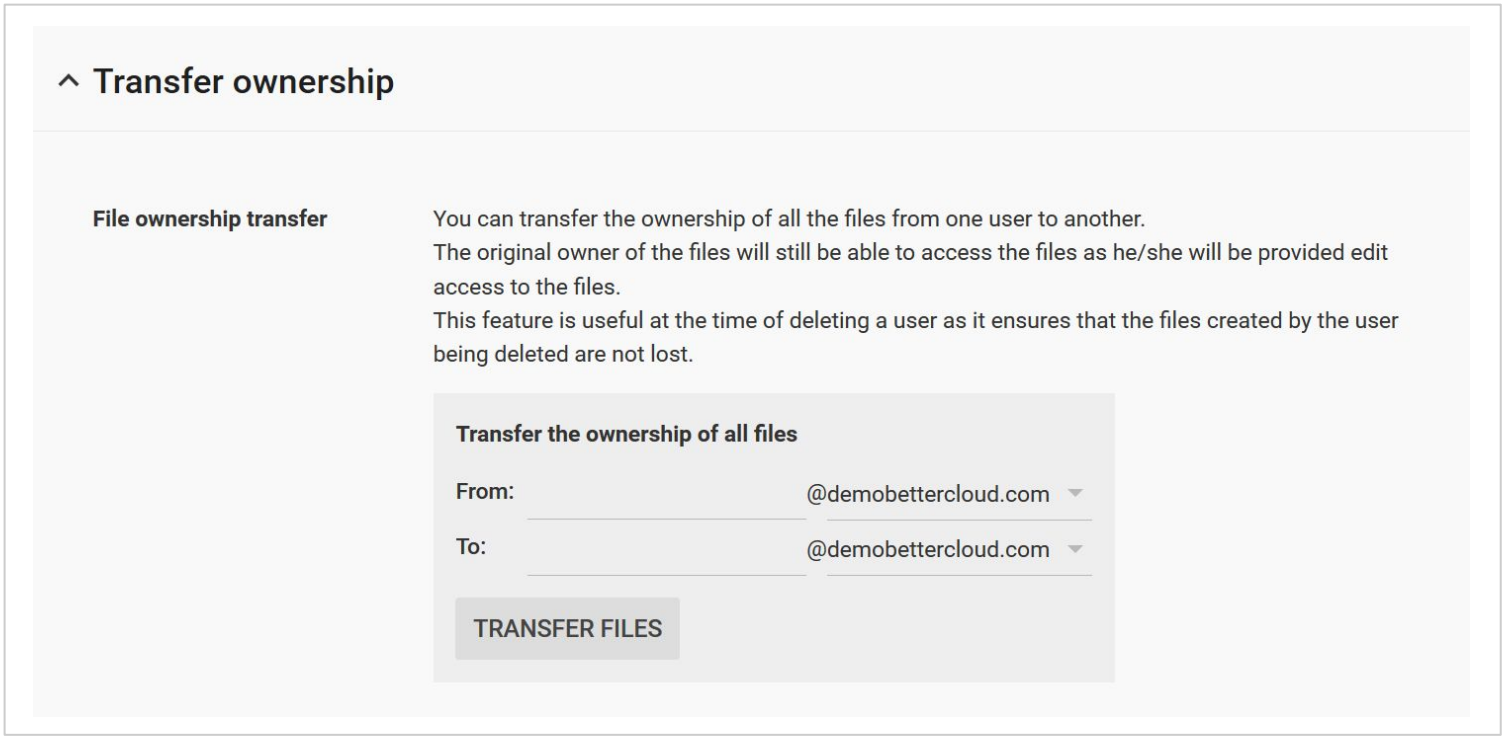
5. Delegate the user's inbox

Delegate the user's inbox to the account executor.

6. Transfer ownership of application data

Overlooking this step can mean significant data loss. Don't forget to transfer ownership of application data such as Drive files, Sites, and Calendars. Of course, if you plan on deleting these files, you can skip this step.

- In the Admin console dashboard, click on **Apps > Google Apps > Drive.**
- Click **Transfer ownership** and fill out the fields for **From** (the departing employee's username) and **To** (the new owner's username).
- Click **Transfer Files.**



A few notes on the transferral process:

- The transferred documents will be placed in a new folder that can be found in the new owner's Drive. It will be titled with the previous owner's email address.
- The admin and owners (both new and previous) will receive an email about the transfer once it finishes. It will outline any problems with the transfer, if there were any.
- It's recommended that you wait until the transfer finishes if you're planning on deleting the original owner of the files.

7. Transfer group ownership & membership

If the user owns (or is a member of) any important groups, you can transfer these assignments to someone else.

Again, some organizations may prefer not to delegate an inbox or transfer ownership of assets, so check with your HR department and/or company policy on these steps.

8. Terminate access to other software accounts

Check which software the departing employee had access to (perform an audit if needed), and terminate, suspend, or reset access to any necessary software (e.g., chat programs, password management tools, VPN, CRM tools, etc).

9. Take care of the offline stuff

Don't forget to collect items like laptops, keys/keycards, and other company property before the user leaves. Additionally, remember to revoke keycard access.

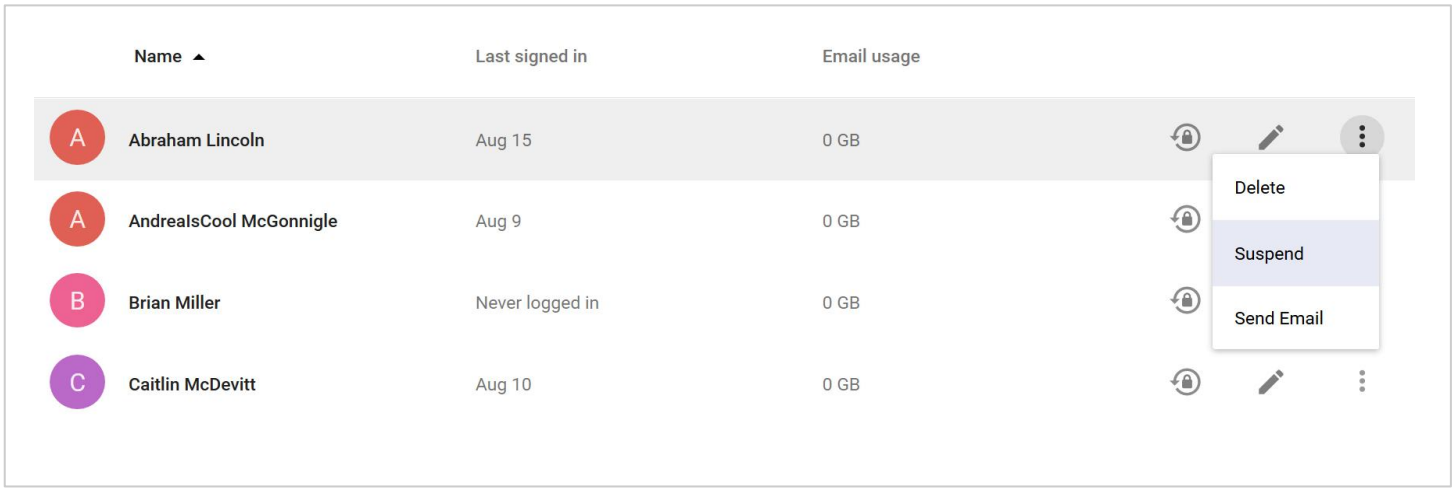
10. Archive everything

If you plan on deleting a user, creating an archive for your records can be a useful step in case you need to access anything later. If you want to have a copy of all the user's files, you can download and export the data from Google. Some companies have certain limits on how long data can be archived, so check what your IT department's data retention/lifecycle policy says.

11. Suspend the user's account

If the user's account has information that you'd like to save, you can suspend their account until you've transferred the information to another person. By suspending the account, you keep it preserved but inactive.

- In the Admin console dashboard, click on **Users >** Find the user you'd like to suspend > **Click on the three dots** on the right side by their name > **Suspend.**



- To confirm, click again.

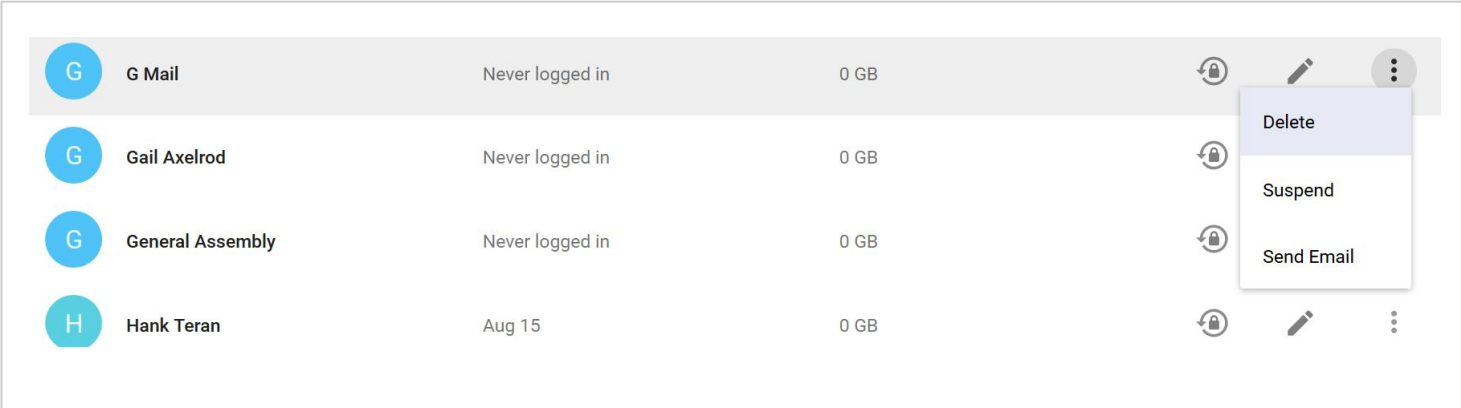
Note: License fees will still apply to suspended users if you're on the annual billing plan.

12. Delete the user or assign a VFE license

You can delete the user, or you can set a reminder to take more decisive action in the future (for example, in 30 days). If you do delete the user permanently from your domain, you will lose all of their Drive files, emails, and secondary Calendars. It will also free up a Google Apps account license to use on new users. If you want to hold on to data in Vault for inactive user accounts, look into Vault Former Employee Licenses. They'll allow administrators to search, export, and retain data in Vault.

Offboarding

- In the Admin console dashboard, click on **Users >** Find the user you'd like to delete > **Click on the three dots** on the right side by their name > **Delete.**



- Confirm that you want to delete this user.

The user's e-mail messages and primary calendar will be deleted after five days, as will his Drive files (unless they are transferred). To learn more about what happens to a deleted user's data, click here.

BetterCloud provides critical insights, automated management, and intelligent data security for cloud office platforms. By leveraging open APIs, BetterCloud securely connects with your data at its source, providing maximum control without requiring any cumbersome setup. BetterCloud is trusted by IT teams in over 50,000 organizations worldwide.

*Subscribe to **our newsletter** for daily tips, tricks, and updates!*