# Best Practices for Managing Identities When You Move to Google Cloud

# Contents

# About this guide

| Highlights | |
|---|---|
| **Purpose** | To provide best practices and guidance to GCP, Google Workspace, and Cloud Identity customers for managing identities when they move to Google Cloud.<br><br>To provide the information an organization would need to transfer data and ownership from one Google Account to another for some of the noncore Google services, such as Google Ads, Google Analytics, or DV360. |
| **Intended audience** | Organization administrators. Staff planning Google Cloud / Google Workspace migration. |
| **Key assumptions** | That the audience has a basic understanding of identity concepts. |
| **Delivery note** | Use this guide before you provision Google Cloud identities. |
| **Related Document** | [Migrating consumer accounts to Cloud Identity or Google Workspace](#)<br>[About conflicting accounts](#)<br>[Migrating Projects into an Organization | Resource Manager Documentation](#) |

# 1. Introduction

Cloud Identity is the Google Cloud IDaaS solution. It is the same identity source that powers Google Workspace and GCP. So whether you are a Cloud Identity customer, a Google Workspace customer, or a GCP customer, this guide can be useful to you.

For simplicity, we often refer to a "Cloud Identity organization" in this guide, but the same considerations apply if you are a Google Workspace customer or a GCP customer.

To make the best use of this guide, you should know these terms:

- **Managed account:** A Google Account managed by a Cloud Identity organization.

- **Consumer account:** A Google Account whose ownership belongs to the user and which falls under consumer terms of service, for example, a Gmail.com account. Unmanaged accounts are also consumer accounts.

- **Unmanaged account:** After an organization verifies ownership of a domain in the Admin Console, a consumer Google Account with a primary email address of that same domain is now an unmanaged account. An unmanaged account is a consumer account: it is still under the consumer terms of service, but it is not managed by the organization.

- **Conflicting account:** An unmanaged Google Account becomes conflicting when a Cloud Identity organization provisions a managed account with the same email address as the primary email address of an unmanaged Google Account.

# 2. Managing identities

When you move to Google Cloud, you have the option to use managed Google accounts, inviting unmanaged Google accounts to transfer their existing accounts (the recommended approach), or to use unmanaged identities.

## 2.1 Why managed accounts?

Provisioning a managed Google Account brings several benefits. For example, you can:

- Enforce security policies on the accounts (such as password policies or 2FA enforcement)
- Easily administer all the accounts with a single pane of glass
- Audit and monitor account activities and get reporting
- Leverage SSO when using 3P IdP (for example, Okta, Ping, ADFS)
- Manage devices

## 2.2 Should you transfer existing unmanaged accounts or not?

▶ If you transfer existing Google Accounts:

- User data is preserved.
- User history and preferences are preserved.
- User access to Google services is preserved, as long as licensing permits for Google Workspace services and the Google Service is enabled by admin.
- GCP access and IAM is preserved.
- Users can keep using the same Google Account. The account is not re-created and the ownership is moved from the user to the organization, who will then be able to manage the account.

▶ If you don't transfer existing Google Accounts:

- You will not bring employee's personal data into your domain (for example, Google Payments).

  This might result in users having to handle two separate Google identities, one consumer identity and one managed identity. For example, the user might have to use a consumer account for accessing Google Ads and a managed account to access Google Drive or GCP.

# 2.3 How to provision a managed Google Account

There are several ways of provisioning identities in Cloud Identity. Here is a brief overview of the different possibilities.

| User provisioning methods | | | |
|---|---|---|---|
| **Method** | **Effort** | **Staff involved** | **Notes** |
| Manual provisioning | High | Google Workspace admin | Easiest method, but not scalable |
| CSV upload via Admin Console | Medium | Google Workspace admin | More flexibility, but not scalable |
| **Google Cloud Directory Sync** | **Medium** | **LDAP admin** | **Integrates with LDAP, scalable, requires no programming** |
| Third party tools via Directory API | Medium | LDAP admin | Scalable, may incur additional cost |
| Admin SDK Directory API | High | LDAP Admin, Development staff | Scalable, flexible, requires in-depth programming |

If your identities already live in a Microsoft Active DIrectory or an LDAP server, the best practice is to use Cloud Directory Sync to provision identities and keep Cloud Identity in sync with your Microsoft Active DIrectory or LDAP server, which will be your source of truth. For more information, see About Google Cloud Directory Sync.

If you don't use a Microsoft Active Directory or an LDAP server, the recommendation is to use Admin SDK Directory API to provision identities. If you use Azure AD, see this tutorial to sync users from Azure AD to Cloud Identity.

For more information about the Admin SDK Directory API, see Manage everything in your Google Workspace domain.

Information about which users can be transferred, and the methodology and process for doing that, follow in subsequent chapters.

# 3. What happens when users already have a Google Account

Once your organization decides to provision Google identities, one important element to consider is that your users might already have signed up to Google. They might have a Google Account with the same corporate email address that belongs to them as an employee, and they might be using that same Google Account for business services. To avoid loss of data or access, or duplication of accounts, it is crucially important to plan carefully how to handle those accounts before provisioning identities in your new Cloud Identity domain.

The following use cases illustrate the three most common scenarios.

## 3.1 Unmanaged users with no Gmail involvement

Prior to your move to Google Cloud, users could have created a Google consumer account using their corporate email address. (This can also happen after you move to Google Cloud, discussed in Section 5.5, <u>Preventing the creation of conflicting accounts when syncing users</u>.)

For example, Anna is working for drusstech.com. Her email address at work is anna@drusstech.com. drusstech.com is not a Cloud Identity customer.

In her role with the company, Anna will need to begin managing Google Analytics properties, so she signs up to Google with her company email address. Now Anna owns a Google Account with the same email address, anna@drusstech.com. This is a consumer Google Account, whose ownership belongs to Anna.

When Anna signed up for the account, she filled out the following information:

**Visibility for your organization**. This type of user is visible in the Transfer tool for unmanaged users (covered in [Section 4](#)), and they can be invited to transfer their Google Account to the organization's domain.

## 3.2 Unmanaged users who upgraded to Gmail

Users who have created a Google consumer account using their corporate email address might also have added Gmail to their Google consumer account.

For example, Mike is another drusstech.com employee who created a Google Account, just like Anna did. His email address is mike@drusstech.com. In addition to that, Mike also upgraded his Google Account to Gmail, meaning that he added a Gmail email address to his Google Account, making it mike.drusstech@gmail.com.

Mike did something like this:



**Add Gmail to your Google Account**

By completing this form, you're upgrading to Gmail, email from Google. Gmail works on any device, blocks spam and much more.

You'll be able to sign in using your new Gmail address, which will become the primary email address associated with this account. We'll send account updates, invitations and other notifications to your Gmail address.

mike@drusstech.com will become an alternative email address on this account, and you'll still be able to sign in with it.

If you prefer, you can create a new Google Account with email, and leave this one as-is.

**Name**

Mike | Smith

**Choose your Gmail address**

mike.drusstech | @gmail.com

**Mobile phone**

🇬🇧 ▾ | +44

**Your current email address**

mike@drusstech.com

Submit

Now Mike can log in to Google with either email address (mike@drusstech.com or mike.drusstech@gmail.com) to use Gmail. The two email addresses are effectively the same Google Account.

The other effect is that the Gmail email address (mike.drusstech@gmail.com) became the primary email address, while the company email address (mike@drusstech.com) became an alternative email address.

The UI showing the email addresses info looks like this:

← Email

Manage the email addresses associated with your Google Account. Learn more

Google Account email     mike.drusstech@gmail.com

The address used to identify your Google Account to you and others. You can't change this address.

Recovery email     mike@drusstech.com    ›

The address where Google can contact you if there's unusual activity in your account or if you get locked out.

Contact email     mike.drusstech@gmail.com    ›

The address where you get information about most of the Google products that you use with this account.

Alternative emails     mike@drusstech.com    ›

Other email addresses that you can use to sign in to your account. They can also be used to reach you in case you get locked out.

About me emails     **ADD ABOUT ME EMAIL**

Email addresses that you can share with others across Google products like Drive, Photos and Google+.

Note that this would be the same as Mike signing up to Gmail first with mike.drusstech@gmail.com and then adding mike@drusstech.com as an alternative email address. Note also that you can't use a Gmail email address as an alternative email address, so the inverse is not a possible scenario.

**Visibility for your organization**. This type of users is not visible in the Transfer tool for unmanaged users, and they can not be invited to transfer their Google Account to the organization's domain.

To make the user transferrable again, you can ask the user to downgrade from Gmail, deleting the Gmail service from their account.

**Downgrading from Gmail**. Before a user deletes Gmail from their account, they can use Google Takeout to download their Gmail data.

Downgrading from Gmail means that users lose all their Gmail data (unless they first preserve it with Google Takeout) and that their Gmail email address will become an alternative username without a Gmail mailbox. Users, such as Mike, who take this route will still be able to log in to their Google Account with their Gmail email address (in this case, mike.drusstech@gmail.com), but with no Gmail mailbox. The new primary email address will be an alternative email address of the user's choice, including their corporate email address, if they so choose (in this case, mike@drusstech.com).

The Google Account will still be the same Google Account, meaning that other non-Gmail data will be preserved and that access to services linked to that account will be preserved. And most importantly, the user can be invited again to transfer to the organization.

This is what the flow would look for Mike when he visits myaccount.google.com/data-and-personalization:
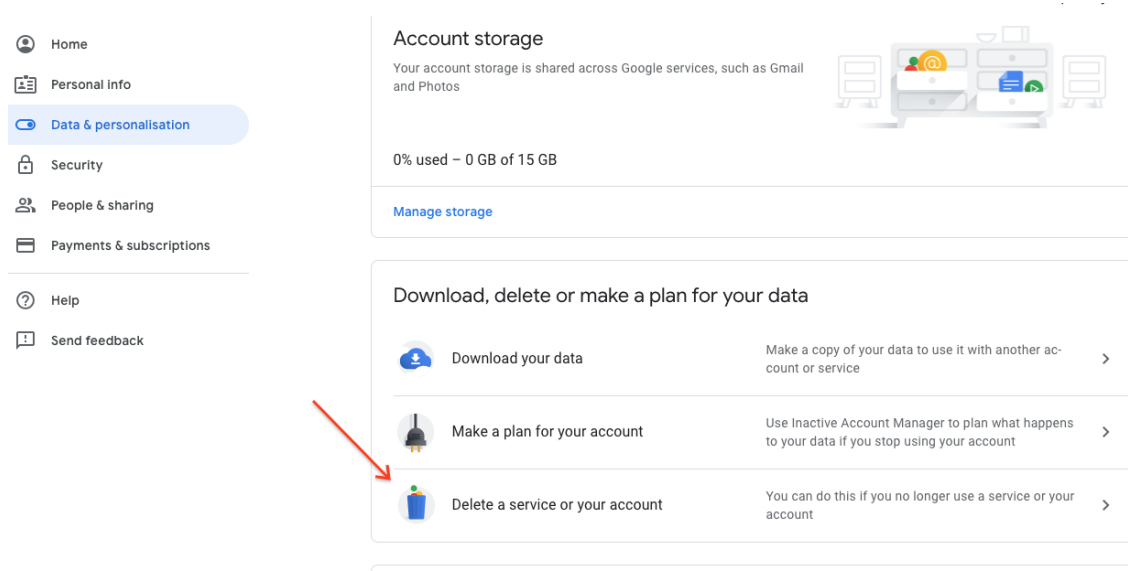
# ← Delete a service or your account

## Delete a Google service

You can delete a specific Google service from your account, such as YouTube or Gmail

**Delete a service**

## Delete your Google Account

You can permanently delete your Google Account and all your services and data, such as emails and photos

**Delete your account**

## Download your data

Create an archive of your Google data to use with another service

**Export your data**

## Make a plan for your account

Decide what happens to your data if you stop using your account

Plan for inactive account
⊖ Off

**Set up a plan**

← Delete a Google service

A Google Account offers many services. Some of these services can be deleted from your account individually.

Consider downloading your data before deleting a service.

DOWNLOAD DATA

Or choose a service below:

M   Gmail                                                                🗑

---

← Delete a Google service

A Google Account offers many services. Some of these services can be deleted from your account individually.

**How you'll sign in to Google**                                          ✕

To continue using your other Google services with this account – like Google Play, Docs or Calendar – you'll need an address to sign in with. It can't be a Gmail address. Select an alternative email address or enter a new email address.

mike@drusstech.com   ▾

CANCEL        NEXT

## Delete a Google service

### Please read this carefully. It's not the usual yada yada. ✕

Before you delete Gmail from your Google Account, remember that you'll no longer be able to send, receive or access email from your **mike.drusstech@gmail.com** account.

You also could lose access to services outside of Google where you use mike.drusstech@gmail.com. For example, if you use this email address as a recovery email for your bank account, you may have difficulty resetting your bank password. If you proceed, you'll need to update your email address everywhere you use it outside of Google.

When you delete Gmail, your mailbox will be closed, all of its contents will be permanently deleted and you'll lose access to your email address within 2 business days.

You will be able to use **mike@drusstech.com** to sign in to your Google Account after you delete Gmail.

### All of your 2 conversations will be deleted.

☑ Yes, I want to delete mike.drusstech@gmail.com permanently from my Google Account.

CANCEL     DELETE GMAIL

Within two business days, Gmail data will be deleted and the chosen alternative email address will become the new primary email address.

In this example, the new primary email address for Mike will again be mike@drusstech.com. The old Gmail address, mike.drusstech@gmail.com, will still be an alternative username, which means that Mike can log in to his account using this address, but he cannot send or receive emails or use Gmail with that address.

← **Email**

Manage the email addresses associated with your Google Account. Learn more

| | | |
|---|---|---|
| Google Account email | mike@drusstech.com | > |
| | The address used to identify your Google Account to you and others. | |

| | | |
|---|---|---|
| Recovery email | mike@drusstech.com | |
| | Your Google Account email (mike@drusstech.com) is used as your recovery email. | |
| | The address where Google can contact you if there's unusual activity in your account or if you get locked out. | |

| | | |
|---|---|---|
| Contact email | mike@drusstech.com | > |
| | The address where you get information about most of the Google products that you use with this account. | |

| | |
|---|---|
| Alternative emails | **ADD ALTERNATIVE EMAIL** |
| | Other email addresses that you can use to sign in to your account. They can also be used to reach you in case you get locked out. |

| | |
|---|---|
| Alternative usernames | mike.drusstech |
| | Usernames that you can use to sign in to your Google Account. You can't add or remove them. |

Gmail email addresses cannot be reused or changed. The Gmail email address will stay associated with the Google Account, and the user will have the possibility to re-upgrade to Gmail (with brand new mailbox after the data is deleted) with the same email address, until the user becomes a managed account.

**Note**: The user will preserve the Gmail alternative username even after the transfer. This means that the managed user could still log in to the managed account with a Gmail email address. This is purely to prevent recycling of Gmail email addresses and the account is fully managed with no possibility by the managed user to add or recover a personal Gmail mailbox.

## 3.3 Consumer Gmail users

Users could also have created a Google Account without using a company email address.

For example, at drusstech.com, Maria created a Google Account for business needs, but she did not use her company email address. She only owns a Google Account with a Gmail address, maria.drusstech@gmail.com

**Visibility for your organization**: This type of users is not visible in the Transfer tool, and they can not be invited to transfer their Google Account to the organization's domain.

# 4 Finding and inviting users to transfer

It is possible to find and manage users with an existing Google Account by using the Transfer Tool for unmanaged users or using APIs.

## 4.1 Using Transfer Tool for unmanaged users

After you have added a domain in your Google Workspace instance and you have successfully verified the ownership, you can view unmanaged users in your Admin Console via the Transfer tool for unmanaged users.

It can take up to 24 hours for new users to be displayed in the tool. The same consideration applies for newly created unmanaged users of your domain.

The Transfer tool shows all the unmanaged users related to the domains you have verified. In other words, it shows every consumer Google Account whose domain in the email address matches exactly with one of the domains (primary and secondary) that you have verified. For more information, see Verify your domain for Google Workspace.



With the Transfer tool, it is possible to send requests to users to invite them to transfer their Google Account to the domain.

The Transfer Tool allows also to download the list of unmanaged users and bulk update unmanaged users, sending user invitations to all your unmanaged users or a large batch for example.

It is also possible to track the status of the request and filter the users by status:

- Not sent (unmanaged users who haven't received an invite)
- Request sent (unmanaged users who received an invite and took no action)
- Declined (unmanaged users who received an invite and declined it)
- Accepted (former unmanaged users who accepted the invite, now managed users)

**Google** Cloud

## 4.2 Using User Invitations API

It is also possible to use User Invitations API (in beta) to list unmanaged users and manage user invitations programmatically.

The available methods are:

- isInvitableUser -> Determine whether a user is unmanaged (invitable)
- get -> Get the status of an invitation
- cancel -> Cancel an invitation
- send -> Send an invitation
- list -> List unmanaged users with invitation status

Note: GAM also supports the User Invitation API.

## 4.3 Best practices for planning user invitations

If you are planning to send user invitations, it is important to also send a separate communication to those users, so they know what to expect and why they are required to accept the invitation. Building tailored communications for users will increase the acceptance rate of the invitations.

It is recommended to use Transfer Tool for Unmanaged users if:

- You have only a few users to transfer or
- You would like to pick and choose which users to transfer or
- You want to do one-off bulk invite or few batches of invitations or
- You only want to monitor invitation status or
- You want a no-code solution

It is recommended to use User Invitations API instead if:

- You want to regularly send batch invitations or
- You want a programmatic solution or
- You want to integrate invites with your own solution / application

Note that it is possible to resend an invitation to users whose request in status Not sent, Request sent, or Declined.
The invitation has no expiration date and cannot be recalled back by the admin.

Note also that unmanaged users can be invited only if:

- The primary user email address is in one of the verified domains (primary or secondary). Domain aliases are excluded.

- The user email address does not contain [special characters](#) not supported by Google Cloud. The user can rename the email address removing the special characters in order to become transferable.

# 4.4 The user transfer request

When you send a transfer request, the user receives an invitation via email.

For example, this is the email anna@drusstech.com would receive, localized in the language Anna has chosen as primary language for her Google Account:

to Google Cloud. This can occur at any time until we finish deleting content from consumer Google+, even though this data may be visible to you in your Google Cloud account. Data you create in your Google Cloud account shouldn't be affected. However, if you post media to your Google Cloud account that was uploaded to consumer Google+, it might be deleted unless it's backed up to Google Photos. Before transferring your account, you can save your Google+ data.

- As you may lose access to some Google services after the transfer, we recommend using Google Takeout to export any important data before accepting the transfer request.

**Is this a personal account?**

If this account is for personal use, you can decline this request. If you do so, you'll be required to rename this account later when your admin creates a new Google Cloud account for you.

**Transfer account**

Visit our help center to learn more about transferring your account.

The user has the option to accept or decline the account transfer request.

# Complete your account transfer

You're about to transfer the account **anna@drusstech.com** to your organisation's Google Cloud account. You'll be able to collaborate with your colleagues in the enterprise versions of Google's products and services, and your Google Cloud admin will manage your account.

Here are some things to be aware of before transferring your account

**G** **Google apps and services**

- You might have access to the enterprise versions of Google apps and other services like Google Cloud Platform – depending on what your organisation allows and what Google Cloud products they've purchased.

- Some Google services that you're using might not be available after you transfer your account.

- The consumer version of Google+ was shut down, effective 2 April 2019. Google+ data created in your consumer account might be deleted after you join Google Cloud. Before joining, you can save your Google+ data. Learn more about what happens to your Google+ data.

**Account access**

Your Google Cloud admin will be able to access your account information and any data you store in this account. You can have a separate Google Account for personal use and switch between accounts.

**Data export**

Before you join, you can use Google Takeaway to save any data in your Google Account that you don't want to be managed and any data that you want to keep from unavailable services.

**Terms and policies**

You'll need to follow your organisation's privacy policy, if one exists, when using your account; your organisation's G Suite agreement when using core services if they have purchased G Suite and the Google Terms of Service, the Google Privacy Policy and service-specific terms when using additional services.

By clicking **Next**, you agree to the Google Terms of Service and the Google Privacy Policy.

NEXT        DECLINE TRANSFER

Google Cloud

# Your Google Account has been transferred

You're ready! You're ready to start collaborating with the enterprise versions of Google products and services.



If Anna transfers the account, her account is now fully managed by her organization.

| Users | Showing users from all organisational units | Add new user | Bulk upload users | Download users | More ▼ |
|---|---|---|---|---|---|

| | Name ↑ | Email | Status | Last sign-in | Email usage | ⚙ |
|---|---|---|---|---|---|---|
| ☐ | Anna Rossi | anna@drusstech.com | Active (created 1 day ago) | 11 minutes ago | 0 GB | |

## 4.5 What happens to the user's data and account if the transfer request is accepted

If the user accepts the request to transfer their account, the organization will be able to manage the account just like any other account in the Cloud Identity domain. The only exceptions are sites and secondary calendars created by the user before the transfer. They cannot be administered by your organization's managed Google Account.

All user data is preserved, meaning that history, bookmarks, and preferences are retained.

Existing email aliases are also preserved.

**IMPORTANT**: Access to Google Services is retained if the service is turned on in the Cloud Identity domain. Appropriate licensing might also be required.

For example:

- If Google Analytics is ON for the Organization Unit Anna belongs to, Anna can continue to manage Google Analytics properties as before. Her access and all her settings are retained.

- Before the transfer, Anna used Google Calendar. After the transfer, if Google Calendar is turned OFF for the Organization Unit Anna belongs to, Anna cannot use Google Calendar anymore.

- Before the transfer, Anna used Google Sites as part of the consumer offering. After the transfer, if Anna has only a Cloud Identity license, she will not be able to use Google Sites anymore. Her sites are not deleted, and they will be accessible again once the organization assigns the appropriate license to Anna.

  Note: With a Cloud Identity license, Anna can still use Google Drive and the editors. See the Cloud Identity Services Summary.

## 4.6 What happens to the user's data and account if the transfer request is declined

If the user permanently ignores or declines the transfer request, then the only option for the organization is to provision a new managed account, which triggers a conflict.

A user who has a pending request or who has declined the request, can be re-invited by the organization with the Transfer tool. In that case, the user will receive a new email invitation. The previous link is not invalidated, which means that the user can accept any received invitation.

# 5 How conflicting accounts happen and what to do about them

When the organization provisions a user with the same email address of an unmanaged user, there's a conflict.
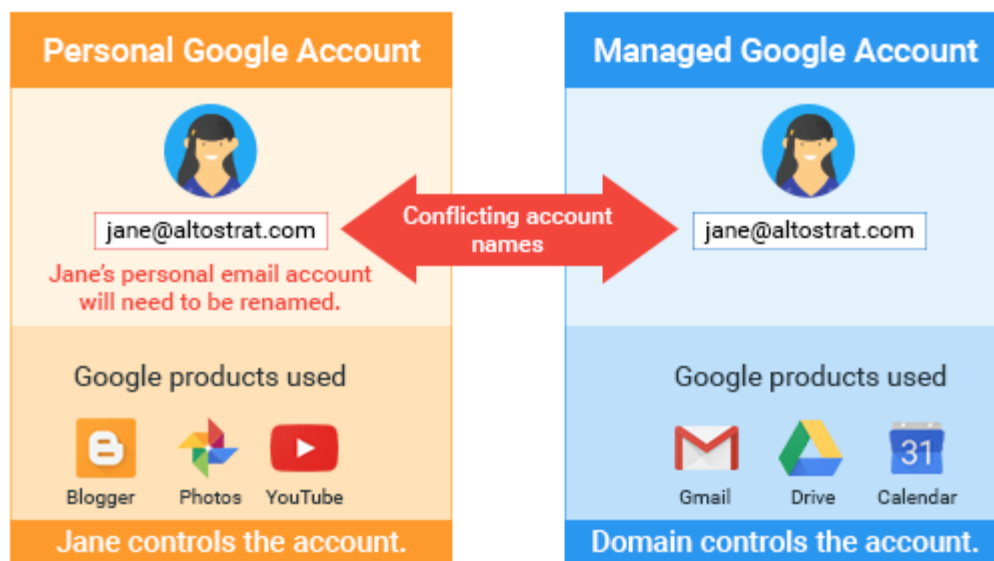


If the organization is adding user manually and individually via the UI, the admin will be warned of the potential conflict and presented the option either to email a transfer request to the user or to go ahead and provision the new user in the domain, creating the conflict.

**User already exists**

Someone is using anna@drusstech.com as an
unmanaged(individual) account. Learn more

⦿ Email existing user a transfer request (recommended)
The existing user can decide whether to transfer their account
to the drusstech.com organisation or continue using it as an
unmanaged (individual) account. If the user accepts the
transfer request, their account and data will be managed by
drusstech.com.

◯ Create new user anna@drusstech.com
You can use anna@drusstech.com for your user. The existing
user will be renamed to
anna%drusstech.com@gtempaccount.com email.

CANCEL    **CONTINUE**

**IMPORTANT**: The warning will be displayed only if:

- You are using the Admin Console UI.

- You are logged in as a Super Admin

  No warning is provided using any method that leverages the Admin SDK Directory API.
  For information on how this applies when syncing users, see Preventing the creation of
  conflicting accounts when syncing users.

- The email address specified in the UI matches exactly, including upper- and lowercase,
  with the unmanaged email address.

  For example, if the unmanaged user's email address is Jack@drusstech.com and the
  admin is attempting to add a user to the domain via UI using jack@drusstech.com, a
  conflict will be generated and no warning will be displayed. For this reason, it is highly
  recommended to use the Transfer tool for unmanaged users.

Regardless of any uppercase specified in the UI, the managed user's email address will only
have lowercase.

# 5.1 What happens when a conflict is generated

A conflict happens when there is an existing unmanaged Google Account and the organization provisions a managed Google Account with the same email address of the unmanaged user. This is what happened, for example, when Sara signed up to Google using her corporate email address sara@drusstech.com.



Now her organization is not inviting Sara to transfer her account (as outlined in Sections 4.1, Finding and inviting users to transfer, and following) and is creating a managed Google Account for her with an email address sara@drusstech.com.

Your newest user can now start using G Suite

## Sara Rossi

sara@drusstech.com

Password

● ● ● ● ● ● ● ●  👁

Click to copy password

DONE                    MORE ACTIONS ▼

The moment that the managed account is created, the consumer Google Account that used to be sara@drusstech.com is renamed to sara%drusstech.com@gtempaccount.com.

**Important**: Sara now has two separate accounts associated with Google. It is not possible to merge them or to roll this action back. For information on transferring ownership of some Google services from one account to another, see Section 7, [Migrating existing GCP projects into an organization](#).

Sara can log in using:

- sara%drusstech.com@gtempaccount.com: This will lead straight to her consumer Google Account.

- sara@drusstech.com: Sara will be presented with a screen inviting her to choose whether she wants to continue with her consumer Google Account (sara%drusstech.com@gtempaccount.com) or the managed Google Account.

**Google** Cloud

# Google

There are two existing Google Accounts for
sara@drusstech.com. Which account do you want to use?

| | **Organisational G Suite Account**<br>Business account owned by<br>drusstech.com | › |
| --- | --- | --- |
| | **Individual Google Account**<br>An account that you created through the<br>normal sign-up process | › |

Learn more

**Best practice**: While the user can continue to log in to her personal Google Account using the same email address of the Cloud Identity / Google Workspace account (or directly with user%domain@gtempaccount.com), Google recommends resolving the conflict as soon as possible.

## 5.2 Resolving a conflict by renaming the account

Every time Sara logs in to the consumer Google Account (sara%drusstech.com@gtempaccount.com), she is invited to solve the conflict.

Options for solving the conflict are:

- Rename the personal account with a new Gmail address.
- Rename the consumer account with a non-Google email address that the user already owns.

**Google** Accounts

**Your account has changed**

The sara@drusstech.com address is no longer available because an organisation has reserved this drusstech.com address. Why does this matter now?

Don't worry. **Your data is safe.** To use it, you need to create a new account with a different email address. Your password and security settings will remain the same.

⊞ Account details

What kind of account would you like?

○ An account with Gmail and a new Gmail address
Select this option if you want to add Gmail to this account. Unfortunately, we cannot move your data to an account with an existing Gmail address.

○ An account that uses a non-Google email address that you already own. e.g. myname@yahoo.com
Select this option if you want Google products, but not Gmail.

[ Continue ] [ Do this later ]   **Not sure what to do?**

For more information, see this Help Center article.

# 5.3 Rolling back a conflict and making a user transferrable again

If you have provisioned a user by mistake, thus generating a conflict, you have the option to "roll back" the action.

For example, in the Admin Console you have created sara@drusstech.com, which because it conflicts with the same email address used as primary email address for a consumer Google Account, now been renamed to sara%drusstech.com@gtempaccount.com.

To roll back a mistakenly created account:

1. Delete the mistakenly created account (in this example, sara@drusstech.com0 from your Cloud Identity domain or rename it to a different email address.

   If you choose to rename it, make sure to delete the automatically generated email alias. In this example, sara@drusstech.com would automatically be generated as an email alias for the account. Make sure to remove it.

   **IMPORTANT**: This means that any shared items or any access granted to the deleted or renamed account will stay linked with that account. To prevent any unintended sharing, carefully examine the implications of deleting or renaming the account.

2. Ask the user to choose **An account that uses a non-Google email address that you already own** when asked to rename the account and to specify the address you are rolling back (in this example, sara@drusstech.com) as the new primary email address.

3. The user will receive a verification email at that email address with a link to verify the change.

4. After approximately 24 hours, an account with that email address (in this example, sara@drusstech.com) will show up again in the Transfer tool and can be invited to transfer. Or if you attempt to create the user in the UI, you should be prompted to the transfer invitation, as long as the email address matches in a case-sensitive way and you are logged in as a Super Admin, as described in Section 5.1, [What happens when a conflict is generated](#).

## 5.4 Avoiding the creation of unmanaged accounts after verifying a domain in Cloud Identity

Conflicting accounts can still happen going forward, even if your organization is now on Cloud Identity and you have successfully verified the domains you own.

To prevent users signing up to Google consumer services with corporate email addresses that belong to your organization, you can take one of two actions:

- **The recommended approach.** Provision your entire population in Cloud Identity. In this way, a user's attempt to create a Google Account with the company email address will fail because a Google Account with that email address already exists. This strategy offers the best protection and it is the recommended approach.

- **An alternate approach.** Set up a filter in your email provider to capture the Google verification email that is sent after a user signs up to Google and monitor those verification emails.

  As a filter, for example, you could look at the envelope sender and match *@idverification.bounces.google.com, holding the matching incoming emails for an internal review process. Note that:

  1. This solution is not guaranteed by Google, as the envelope sender of the email verification is not guaranteed to remain the same.
  2. If you are using Google as your Identity Provider, that filter with the envelope sender might also interfere with password reset requests.

# 5.5 Preventing the creation of conflicting accounts when syncing users

If you enable the one-way sync from an LDAP server and Cloud Identity, it is possible that, as a result of synchronization, the sync tool provisions users in Cloud Identity causing a conflict (see Section 5, [How conflicting accounts happen and what to do about them](#)). There is no warning about the potential conflict.

To prevent that from happening, exclude the unmanaged users from the sync. The subsections that follow address Cloud Directory Sync and Azure AD auto-provisioning, but the same logic can be applied to other environments.

## 5.5.1 Preventing conflicting accounts when using Google Cloud Directory Sync

[Google Cloud Directory Sync](#) is a tool used for one-way synchronization of data from a Microsoft Active DIrectory or LDAP server and Cloud Identity.

As a result of the synchronization, Cloud Directory Sync can provision users in Cloud Identity causing a conflict to happen (see Section 5, [How conflicting accounts happen and what to do about them](#)). There is no warning about the potential conflict.

To avoid the creation of conflicting accounts, the recommendation is to identify the unmanaged users that can be transferred and then either:

- Wait until they have all transferred

or —

1. Put them in a specific AD group, for example *Unmanaged*.

2. Create your LDAP user search rules in Cloud Directory Sync so that they exclude members of that specific group from the sync.

3. Once users accept the invite, remove them from the *Unmanaged* AD group, allowing them to start syncing.

   Note that if you've excluded them from the LDAP side of the sync, and they are added to Google Cloud, Cloud Directory Sync would try to delete them (as it treats the LDAP as the source of truth). Make sure you remove them from the AD group after they joined your Google domain, but before you run the next Cloud Directory Sync sync. For the next Cloud Directory Sync sync, run it with the `-f` command-line argument to clear the cache, because data on the Google side has changed.

If using one of these approaches, you should make sure the unique identifier specified in Cloud Directory Sync is the email address of the user, instead of the objectGUID, as otherwise this might result in sync failure.

## 5.5.2 Preventing conflicting accounts when using Azure AD auto-provisioning

If you are using Azure AD and you are configuring it to automatically provision users to Cloud Identity, you can use scoping filters to exclude users from the sync.

For example, you could:

- Tag unmanaged users with a specific custom attribute, for example, `extensionAttribute1 = Unmanaged`
- Create a scoping filter using that custom attribute
- Select **Sync only assigned users and groups**

## 5.5.3 Preventing conflicting accounts when using a custom solution for provisioning

If you are using an in-house custom solution to provision Google accounts using Google Workspace Admin SDK Directory APIs, it is highly recommended to leverage User Invitations API to check first if an unmanaged user exists before provisioning it.

If the user exists you can leverage the same set of User Invitations APIs to invite the user to transfer, if that is in line with your chosen strategy.

# 6. Transfering data and ownership from one Google Account to another

Sometimes, you will want to simply transfer data and ownership from one Google Account to another.

There are three common scenarios when you might want to do this:

- If you have generated a conflicting account and you can't roll it back
- If your corporate email address is an alternative email address of a Gmail primary email address and you want to transfer ownership from that Google Account to a managed Google Account
- If you simply want to transfer ownership of specific Google Service from one Google Account to another

## 6.1 Transferring your Google Analytics account (UI)

If you have Manage Users permission, you can manage account users (add/delete users, assign any permissions) in Google Analytics. If you do not have this permission, you will need to find someone in the organization with it.

To add the new managed user and grant it the rights from your original account, the user with Manage Users permission can follow the directions in Add, edit, and delete users and user groups.

In Google Analytics, there are also tools to create users in bulk using a Google Sheet in the user interface. In addition, the Google Analytics Management API has methods to manage account user links, which allows programmatic management of users when authenticated with a user with Manage Users permission.

## 6.2 Transferring your Google Ads account (UI)

If you have Admin permission, you can give account access, change access levels, and cancel invitations from other users in Google Ads. If you do not have this access level, you will need to find someone in the organization with it.

To add the new managed user and grant it the rights from your original account, the user with Admin permission can follow the directions in Manage access to your Google Ads account. If you are using a manager Account, follow the directions in Manage users and access levels for your manager account.

## 6.3 Transferring your DV360 account (UI)

If you have read and write access to an entire partner (that is, you are a partner-level user), you can add and edit users in DV360. If you only have read-only or reporting-only access or have read and write access to an advertiser, you will need to find someone in the organization with read and write access to an entire partner.

To add the new managed user and grant it the rights from your original account, the user with read and write access to an entire partner can follow the directions in Manage users in Display & Video 360.

## 6.4 Transferring your SA360 account (UI)

If you have agency manager access, you can add and edit users in SA360. If you only have advertiser manager, user or viewer access, you will need to find someone in the organization with agency manager access.

To add the new managed user and grant it the rights from your original account, the user with agency manager access can follow the directions in Add, edit, or remove users in Search Ads 360.

## 6.5 Transferring your Campaign Manager account (UI)

If your user profile has full access to user profiles, you can add and edit user profiles in Campaign Manager. If your user profile does not have full access to user profiles, you will need to find someone in the organization with this access. Typically look for the Advanced Agency Admin default profile.

To add the new managed user and grant it the rights from your original account, the user with full access to user profiles can follow the directions in Manage user access. Alternatively, this user can add the new account to the same user roles. For Campaign Manager, there are methods in the AccountUserProfiles part of CM API for managing users programmatically.

One note: In Campaign Manager, if you have an account that was originally a Gmail account with a secondary email for the unmanaged user and if the CM user profile was created originally by inviting the unmanage email address, then there is a case where you can transfer the account. After the unmanaged account is added to the domain, the unmanaged email will be removed from the gmail account and the CM profile will still be accessible only by the gmail account. If in Campaign Manager an admin disables and re-enables the user profile, the access will move from the Gmail account to the newly created managed user (as Campaign Manager will refresh the association between the originally invited email and the Google Account). This behavior applies only in Campaign Manager.

## 6.6 Transferring your YouTube channel ([UI](#))

If you have an individual YouTube channel associated with your Google Account, to transfer access you will have to move the channel to a brand account and then transfer the ownership of the brand account to the new user. If you own brand accounts, each one will need to be transferred.

If you have an individual Google Account channel, first follow the instructions in [Move your YouTube channel to another account](#). Be careful with the source and destination (and how you are logged into the window) before you execute the transfer. The destination brand account will lose any existing channel (the channel will be deleted). Each brand account can only be associated with a single channel (although a user account can have access to multiple brand accounts).

Once the channel is transferred to a brand account, follow the directions in [Change who manages your Brand Account](#) to give access to the new user. You can also remove access from the original user once the new user has access to the brand account. Repeat for each channel or brand account in your profile.

## 6.7 Transferring your Data Studio account ([UI](#))

Every Google Account has access to Data Studio. To transfer ownership of a dashboard to the new account, follow the instructions in [How to share reports and data sources](#).

After the new account has edit rights to both the dashboard and the data source, navigate to **Share settings > Invite people > Advanced** in the dashboard and change the new account access to **Is Owner**. There can only be one owner of the dashboard. Saving this with a new owner will transfer the ownership of the dashboard, and the old account will only be an editor.

This process will need to be repeated for each dashboard.

# 7. Migrating existing GCP projects into an organization

Once you create a Google Workspace or Cloud Identity domain, a GCP organization resource will also be created. The name of the GCP organization matches the primary domain of the Google Workspace or Cloud Identity domain.

If you have existing GCP projects and you want to move them into the new organization you created, see [this guide](). You must be an owner or an editor of the project and a project creator in the organization to be able to move the projects.