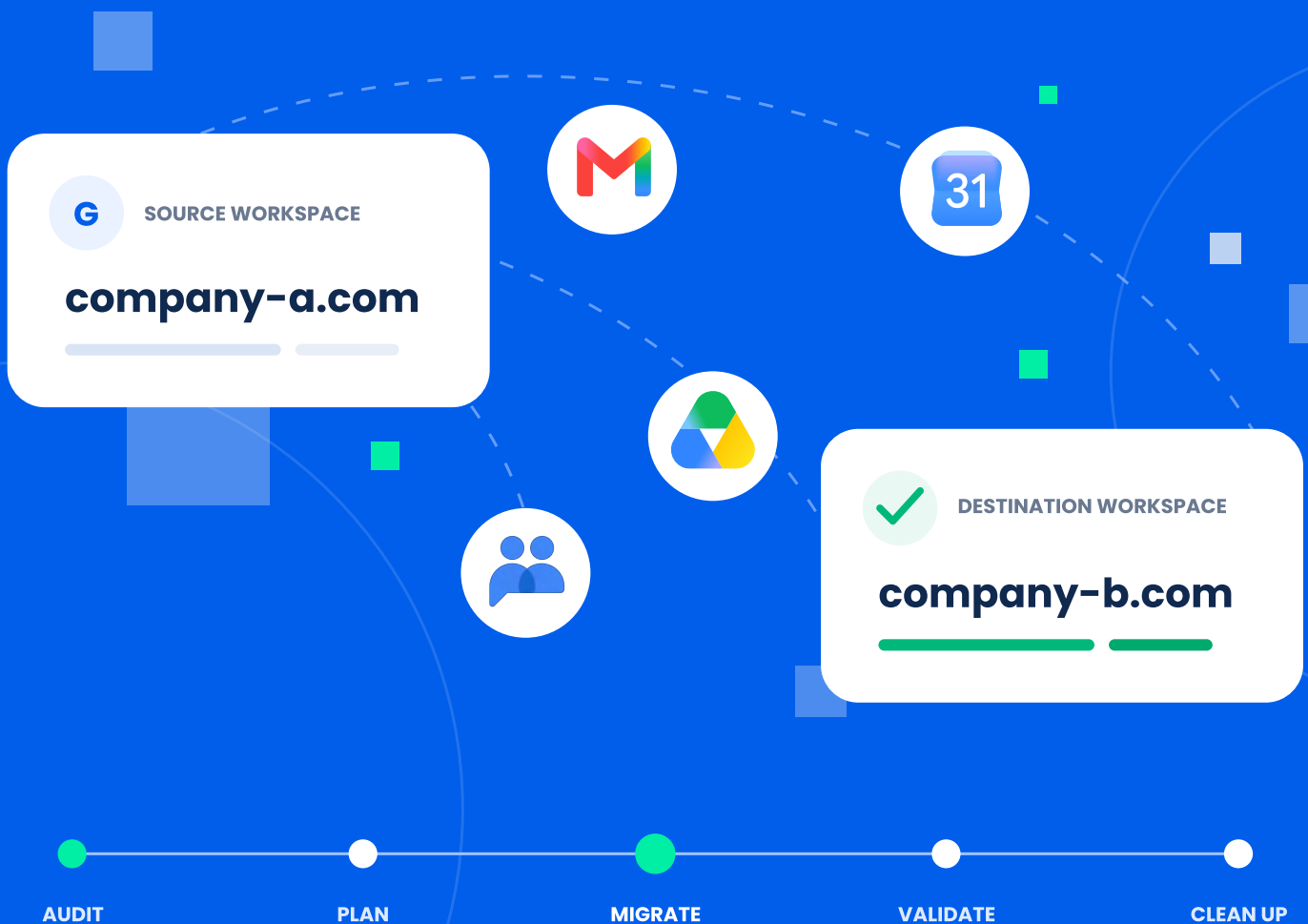


Google Workspace Domain Migration Guide

How to move users, files and data safely

A practical guide for Google Workspace administrators



The Migration at a Glance

Five stages. One controlled move.



A successful Google Workspace migration depends on more than transferring data between two environments.

Before anything moves, you need to know what exists in the source domain, who owns it, who can access it, what should move, and what the destination should look like when the migration is complete.

Files can be missed. Permissions can change. External access can remain in place. Shared Drives can be overlooked. Old accounts can retain access after users have moved.

This guide walks Google Workspace administrators through the domain-to-domain migration process, from auditing the source environment and planning the move to validating the destination and cleaning up what remains.

Google Workspace Domain Migration Checklist

Use this checklist as a starting point for your migration plan.

01

Before migration

Know the environment

- ☐ Define the source and destination Google Workspace environments
- ☐ Inventory users, groups, Gmail, My Drive, Shared Drives, calendars, and other required data
- ☐ Identify file owners and orphaned content
- ☐ Review external and public sharing
- ☐ Identify inactive and legacy accounts
- ☐ Review large files and unnecessary data
- ☐ Identify sensitive or regulated information
- ☐ Map source users to destination users
- ☐ Decide how ownership and permissions should work after migration
- ☐ Define the migration sequence and rollback plan

02

During migration

Control the move

- ☐ Create and configure destination accounts
- ☐ Migrate users and data in controlled phases
- ☐ Track migration errors and failed items
- ☐ Check ownership and permissions
- ☐ Test access with a pilot group before wider rollout
- ☐ Communicate changes to affected users

Google Workspace Domain Migration Checklist

Use this checklist as a starting point for your migration plan.

03

After migration

Prove it worked

- ☐ Compare source and destination users
- ☐ Compare file counts and ownership
- ☐ Review Shared Drive membership
- ☐ Test file, Gmail, and Calendar access
- ☐ Review external sharing
- ☐ Remove temporary or unnecessary access
- ☐ Archive, suspend, or remove legacy accounts as appropriate
- ☐ Confirm important data has not been left behind
- ☐ Repeat access and security reviews after 30 and 90 days

1. When Do You Need a Google Workspace Domain-to-Domain Migration?

A domain-to-domain migration means moving users and organizational data from one Google Workspace environment to another. That is different from changing a user's organizational unit or adding a second domain to an existing environment.

Common scenarios include:

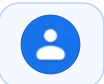
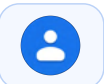
- **Mergers and acquisitions.** Moving an acquired company's users and data into the parent organization's Workspace environment.
- **Divestitures.** Separating users and data when a business unit becomes an independent organization.
- **Re-brands.** Moving to a new company identity or domain. A full migration is not always necessary, depending on the scope.
- **Domain consolidation.** Combining separate Workspace environments into one.
- **Organizational restructuring.** Moving regional offices, subsidiaries, or business units into another Workspace environment.

The scenario defines what success looks like. An acquisition may require historical data and existing access to be preserved. A consolidation project may be an opportunity to remove unnecessary accounts, files, and external access.

Define what needs to exist in the destination environment before choosing a migration method.

2. What Needs to Be Migrated?

A Google Workspace environment holds more than user accounts.

Workspace data	What to account for
 Gmail	Messages, attachments, labels, filters, delegation and forwarding settings
 My Drive	Files, folders, ownership, sharing and folder structure
 Shared Drives	Files, folder structure, members, roles and permissions
 Calendar	Events, calendars, resources and sharing
 Contacts	Personal and shared contact data
 Users	Accounts, organizational units, licenses and attributes
 Groups	Groups, memberships, settings and group-based access
 Permissions	Internal users, external users, groups, public sharing and link sharing

You may also need to account for Google Sites, Forms, Chat, Meet recordings, third-party app connections, and data subject to retention requirements.

For each service, identify the data, access, and dependencies that need to continue working after migration.



TIP

Audit both content and access. It's not just about what you move, but who can access it after the move.

3. Audit Your Google Workspace Environment Before You Migrate

Before anything moves, build an accurate picture of the source environment. A migration can affect more than data. User identities, organizational structure, groups, ownership, and access relationships may all need to be recreated or mapped in the destination.

Your pre-migration audit should cover:

Organizational structure

Document your organizational units and how users are distributed across them. Identify which OUs need to exist in the destination and where the structure may need to change.

Active, suspended, and inactive users

Identify active accounts, suspended users, and accounts that are no longer regularly used. Decide which users need to migrate, which data must be retained, and which accounts can be archived or handled separately.

Groups and memberships

Inventory Google Groups, their members, owners, settings, and any access granted through group membership. Groups used for file access need particular attention because changes to group identities or membership can affect permissions after migration.

File ownership

Identify who owns files in My Drive and determine who should own them in the destination. Pay particular attention to content owned by users who are suspended, inactive, or leaving the organization.

Shared Drives

Inventory Shared Drives, their members, roles, content, and access levels. Map how each Shared Drive should be structured and accessed in the destination.

3. Audit Your Google Workspace Environment Before You Migrate

Files shared into your domain

Identify files owned outside your organization that users currently access. Because your organization does not own this content, it needs to be considered separately from internally owned files during migration planning.

Files shared outside your domain

Review content your users have shared with external users or domains. Determine which collaborators still require access and which permissions can be removed before migration.

Public and link-shared content

Identify files with broad sharing settings. A migration is a good point to review whether that level of access should be recreated in the destination.

Orphaned or poorly organized content

Look for files without a clear owner, location, or business purpose. Content outside expected folder structures can be easier to overlook when migration scope is defined.

Data volume and storage

Understand how much data you are moving across users, My Drive, and Shared Drives. Large files, duplicate content, and obsolete data can add unnecessary migration volume.

Sensitive information

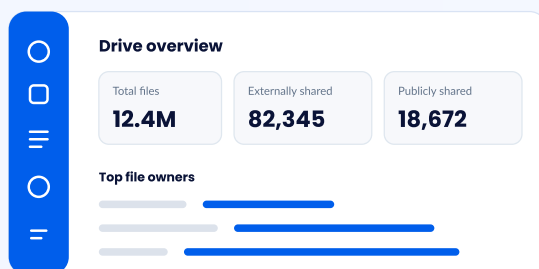
Identify where regulated, confidential, or business-sensitive information is stored and who currently has access. Use those findings when defining ownership and permissions in the destination.

3. Audit Your Google Workspace Environment Before You Migrate



Audit before you move

GAT+ gives Google Workspace administrators domain-wide visibility into Drive ownership, sharing, activity, and storage before migration begins.



REFER TO THESE HOW-TO ARTICLES

- [Audit Google Drive](#)
- [GAT+ Drive Audit Figures Explained](#)
- [Apply a Search Filter in Google Drive Audit](#)
- [Find and Delete Large Files in Google Drive](#)
- [Identify Shared-in Drive Files from External Users](#)
- [Find Publicly Shared Google Drive Files](#)
- [Conduct a User Clean-Up Assessment Before Deletion](#)

4. Build Your Google Workspace Migration Plan

Once you know what exists, decide what should happen to it.

- **Source and destination environments:** Confirm which Workspace environments are involved and that the required services and administrative access are available on the destination side.
- **User mapping:** Map each source identity that needs to move to its destination identity. For example: **alex@company-a.com → alex@company-b.com**
This becomes important when files, calendars, groups, or permissions depend on individual users.
- **Ownership:** Decide who should own migrated content. Active employees may have an obvious destination account. Departed users, shared business data, and content owned by service accounts need a designated owner.
- **Groups:** Map existing groups and decide which memberships still make sense in the new environment. Group membership can provide access to large amounts of Workspace data.
- **Permissions:** Decide whether existing access should be preserved, mapped to new identities, restricted, or removed. Do not assume every permission in the source domain belongs in the destination.
- **Migration sequence:** For larger environments, split the migration into phases based on department, location, organizational unit, priority, or data type. Start with a pilot group so mapping and access problems can be identified before wider roll-out.

4. Build Your Google Workspace Migration Plan

- **User communication:** Tell users what is changing, when, and what they may need to do afterward, including re-authenticating applications or checking access to shared resources.
- **Rollback and escalation:** Define what happens if a migration phase fails. Who decides whether to stop? What remains available in the source environment? How will failed items be handled?

Make these decisions before migration day.



Plan users and groups before migration

Use these resources to map users, manage accounts, and review Google Groups before the move.

RELATED RESOURCES

- [User Management Overview](#)
- [Bulk Add, Update or Remove Google User Accounts](#)
- [Google Groups Management with GAT Flow](#)

5. Choose How You Will Migrate the Data

Google provides tools for migrating supported data into Google Workspace. Available methods and capabilities depend on the source environment and the data being migrated.

Check Google's current migration documentation for your specific source, destination, and data types before choosing an approach. For larger projects, test the migration with a representative group before moving the wider organization.

Third-party migration platforms

Dedicated migration platforms can be useful for complex migrations, large user populations, or data coming from multiple source platforms.

Evaluate them on more than transfer speed. Check support for the Workspace services you use, ownership and permission handling, Shared Drives, failed-item reporting, migration validation, and recovery options.

Targeted ownership and data transfers

Not every migration requires a full-environment migration platform.

For smaller projects or specific Drive datasets, ownership changes or targeted transfers may be enough.



Administrative work around migration

GAT Flow can support administrative tasks around a migration, including bulk user changes, email migration between accounts, and ownership-related workflows.

RELATED RESOURCES

-  [How to Migrate Bulk Emails in Google Workspace](#) 
-  [Transfer Ownership of 'My Drive' Folder](#) 
-  [How to Transfer Ownership of Google Drive Files](#) 

For enterprise migrations, different tools may handle different parts of the project. Document which system or process is responsible for each data type before migration begins.

6. What Happens to File Ownership, Permissions and Sharing?

Moving a file does not mean the right people can access it afterward.

Permissions can depend on individual users, groups, domains, Shared Drive membership, and external identities. When those identities change, access can change with them.

Watch for:

- Internal permissions pointing to identities that no longer exist in the destination
- Group-based access that needs new group mappings
- External collaborators losing access unintentionally
- Unnecessary external permissions being recreated
- Files shared into the source domain but owned by external accounts, including personal Gmail accounts
- Shared Drive memberships and roles requiring review
- Ownership changing unexpectedly during transfer

Do not overlook externally owned files

Some business files your users work with may not belong to your Workspace domain at all. They may have been shared by a customer, partner, contractor, former employee, or even from a user's personal Gmail account.

Identify these files before migration and decide whether users only need continued access or whether business-critical content should be copied into an organization-owned location. If the source Workspace account is later removed, access to externally owned files may otherwise be lost.

When copying externally owned content, review the resulting ownership and permissions rather than assuming the new copy will retain the same access model.

Treat permissions as their own migration work stream, not something to check only after the data arrives.

6. What Happens to File Ownership, Permissions and Sharing?

For each major dataset, decide whether access should be:



Preserved:

The same user or group still needs the same access.



Mapped:

The user or group has a new identity in the destination.



Restricted:

Existing access is broader than required.



Removed:

The original user or collaborator no longer needs access.

This prevents outdated access from being carried into the destination simply because it existed in the source.



Managing ownership and permissions with GAT

For sensitive ownership and permission changes, GAT Unlock adds a second-person approval step before the change goes through, providing a record of who authorized the action.

RELATED RESOURCES

-  [Ownership Change Explained in Google Drive](#) 
-  [Change Ownership of Google Drive Folder and Its Content](#) 
-  [Transfer Ownership and Grant Read-Only Access](#) 
-  [Replace the Current Sharing Permissions on Your Google Drive Files](#) 
-  [Members and Guests of Shared Drives Explained](#) 

7. Run the Migration in Controlled Phases

For larger organizations, start with a pilot group rather than moving every user and dataset at once.

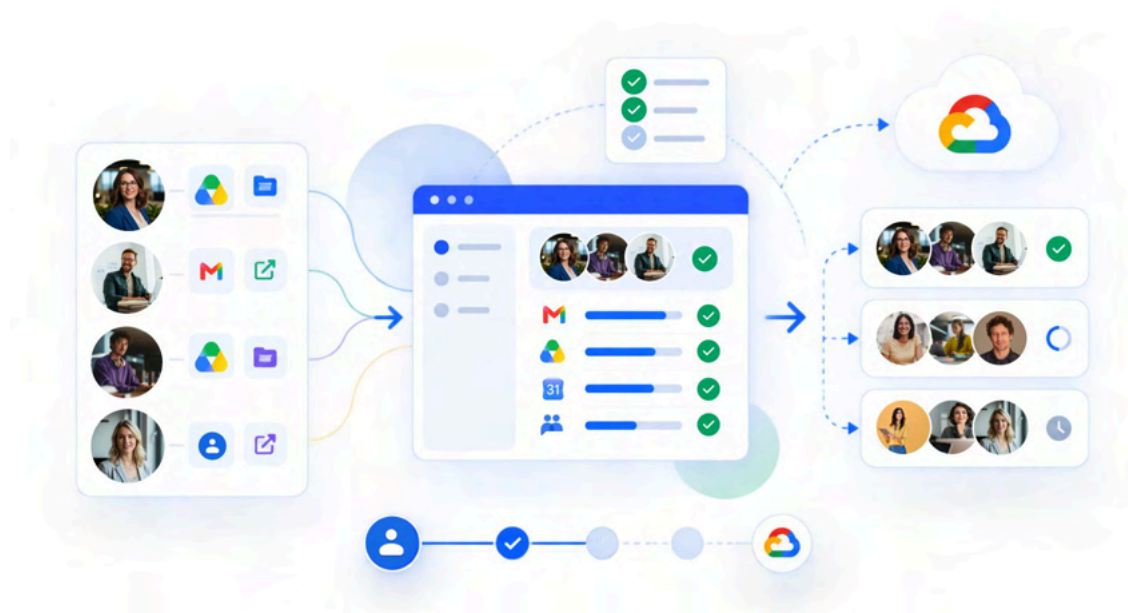
Choose users who represent different parts of the environment. Include users with large Drive accounts, Shared Drive access, external collaborators, group memberships, and different Workspace usage patterns.

Use the pilot to check:

- Did the expected data arrive?
- Can users access it?
- Is ownership correct?
- Did sharing behave as expected?
- Were migration errors recorded and resolved?

Use the results to adjust the process before moving larger groups.

Before final cutover, check for files, emails, or other data created or changed since the initial migration. Include those changes in the final migration phase so recent work is not left behind.



8. Validate the Migration

A migration tool reporting "complete" does not mean the migration succeeded. The destination needs to match what you planned. Compare it against the source directly.

- **Users:** Confirm every expected user exists in the destination with the correct status, organizational unit, licenses, and required attributes.
- **Files:** Compare file counts by user and Shared Drive where possible. Investigate unexpected differences rather than assuming they are normal migration behavior.
- **Ownership:** Check that files are owned by the intended destination accounts, especially content associated with departed users, service accounts, or ownership changes.
- **Permissions:** Compare internal, group, and external sharing against the migration plan. Check whether the resulting access is appropriate, not simply whether a permission transferred.
- **Shared Drives.** Confirm expected Shared Drives exist, files are present, members have the correct roles, and external membership still makes sense.
- **Accessibility:** Test from the user's side. Can users open and edit their files? Access the Shared Drives they need? Find historical Gmail messages? Open Calendar events? Access shared resources?

Migration reports tell you what the migration system processed. **User testing tells you whether people can work.**

RELATED RESOURCES

-  [Show Event Activity on Files, Folders or Shared Drives Across Google Drive](#) 
-  [View Any Action Taken in Google Drive by a Specific User](#) 
-  [GAT+ Drive Audit Figures Explained](#) 

9. Post-Migration Security and Cleanup

The source environment still needs attention after users and data have moved.

- **Remove temporary access:** Administrators, migration accounts, and other users may have received elevated access during the project. Remove privileges that are no longer required.
- **Review external sharing again:** Check the destination for external users, public files, and link sharing. Confirm that the resulting access matches what was planned.
- **Deal with legacy accounts:** Decide whether source accounts should be suspended, archived, retained, or deleted according to your organization's retention requirements. Do not leave accounts active without a defined reason.
- **Check the source environment:** Run a final audit for active or recently modified files, external shares, data that was not migrated, active legacy accounts, and remaining business or application dependencies.

Do not decommission the source until you know what remains and why.

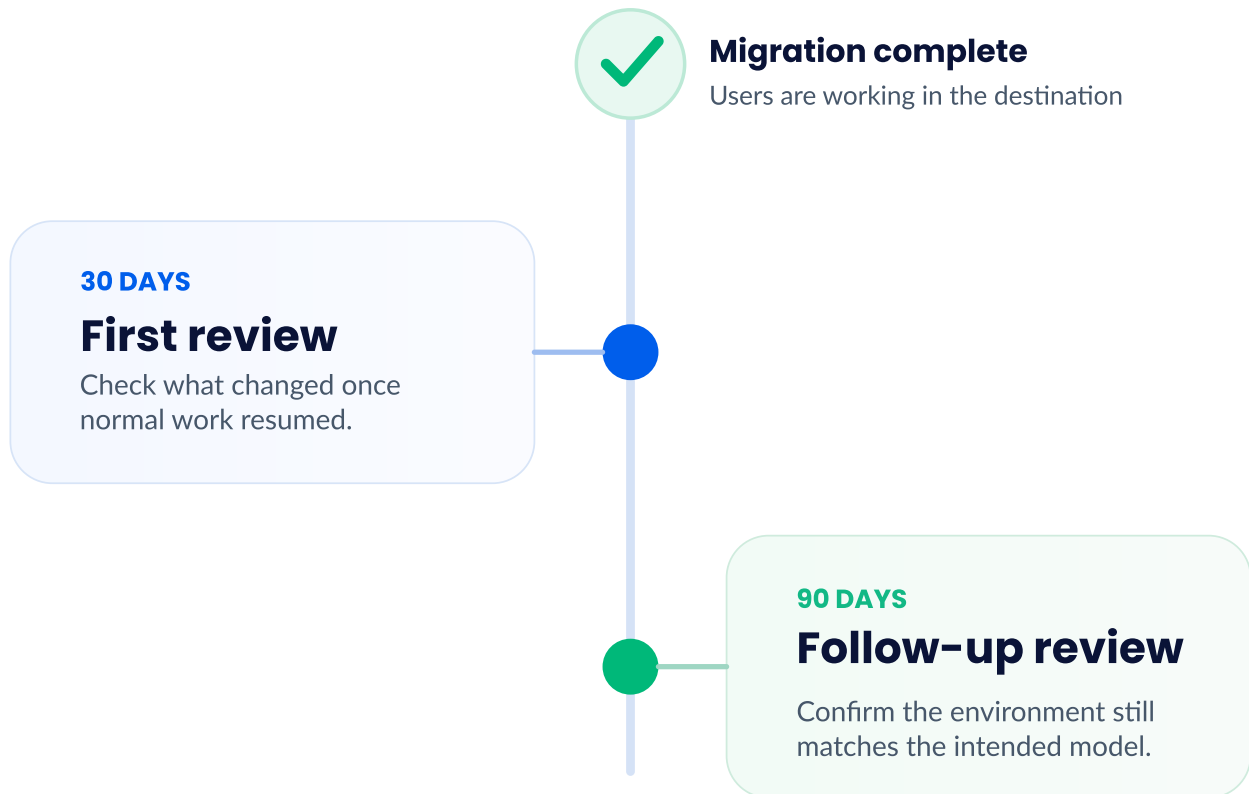
RELATED RESOURCES

- | | | |
|---|--|---|
|  | Globally Remove External Collaborator Access in Google Drive |  |
|  | Remove Public and Public-with-Link Permissions from Google Drive Files |  |
|  | Bulk Archive or Unarchive Google Workspace Users |  |
|  | Deleting Suspended Accounts from Google Workspace |  |
|  | Scheduled Automatic Removal of Workspace Users |  |
|  | Conducting a User Clean-Up Assessment Before Deletion |  |

10. Review the Environment Again After 30 and 90 Days

Some problems only appear once people return to normal work.

KEEP VALIDATING AFTER CUTOVER



What to review



External sharing

New access outside the domain



Legacy accounts

Unused accounts still active



Shared Drive access

Membership or role changes



Unexpected ownership

Files owned by the wrong accounts



Orphaned content

Files without clear ownership



Access problems

Issues users are still reporting



The Goal

Confirm that ownership and access still match the model defined during migration.

Frequently Asked Questions

Quick answers to common admin questions before, during and after migration.

01

How do I migrate from one Google Workspace domain to another?

Inventory the source environment, map users and data to the destination, choose a migration method, migrate in controlled phases, validate the destination against the source, then clean up the legacy environment.

02

Can you transfer Google Workspace data between domains?

Yes. Google provides native migration tooling, and organizations also use third-party migration platforms or targeted transfer methods depending on scope and complexity.

03

What should I audit before a Google Workspace migration?

At minimum: users, file ownership, Shared Drives, external and public sharing, permissions, groups, inactive accounts, large files and sensitive information. Know what exists before deciding what moves.

04

What happens to Google Drive permissions during a domain migration?

Permissions need mapping because users, groups and domains often have different identities in the destination. Some tools migrate certain permissions automatically and others do not. Verify your tool's behavior, then validate permissions after migration rather than assuming they carried over correctly.

05

Can Shared Drives be migrated between Google Workspace domains?

Yes, with the right tooling. Shared Drives require mapping and configuration, and permission handling can vary by tool and current platform behavior. Inventory Shared Drives, members and access levels before migration, then validate them again afterward.

06

How do I know if a Google Workspace migration was successful?

Compare the destination against the source: users, files, ownership, Shared Drives, permissions, external sharing and actual accessibility. Success means the right data is present and users have the intended access.

07

Should you clean up Google Workspace before or after migration?

Both. Clean up before migration to reduce unnecessary data, accounts and permissions, then review again afterward.

Go further with



Get more visibility, control and security
across your Google Workspace.

EXPLORE GAT LABS →



RESOURCES

Admin guides and
how-to's



LIVE TRAINING

Practical sessions
for admins

