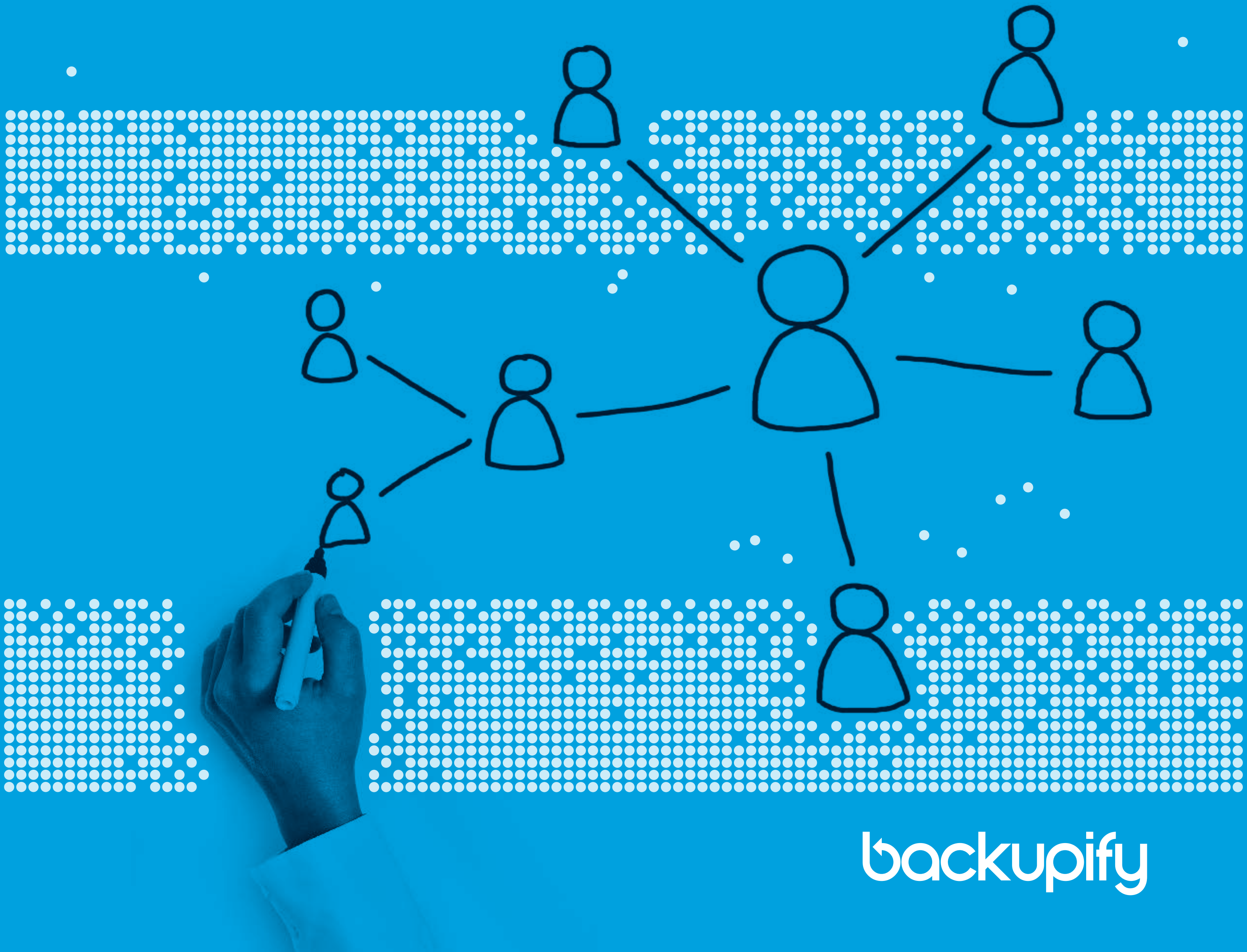
THE GUIDE TO GOOGLE APPS TRAINING

Part Five

ORGANIZATIONAL UNITS AND PERMISSIONS



backupify

Contents

Introduction

In most organizations, your role affects your level of access.

Roles vary, so access to information and tools varies. A help desk technician, a network administrator, and a CIO each need different tools. Faculty, staff, and students also may need different tools and levels of access.

And that's exactly what a Super Administrator configures in Google Apps: which groups of people have access to services, settings and administrative controls.

Google organizes user accounts into "organizational units", and provides administrative permissions with "admin roles". Administrators new to Google Apps need to know that organizational units and admin roles are unrelated to domains and groups.

This document covers the concepts you need to know to manage user accounts and administrative permissions in Google Apps.

Account access overview

Organizational units, privileges and roles

In Google Apps, two settings control a person's access: the account's assigned organizational unit and the account's privileges. The organizational unit determines which services a person may access, while the account's privileges determine which administrative settings a person may change.

Every Google Apps account belongs to one organizational unit. Initially, all accounts connect to a single organizational unit. Because of this, every account accesses the same set of apps. An Administrator creates a new organizational unit to provide access to different services for different groups. For example, a school might create "Faculty", "Staff", and "Student" organizational units, in order to provide each group access to different sets of Google Apps services.

Each person's account also receives privileges assigned by an Administrator. To simplify management, Google provides several "pre-built" collections of privileges in the form of Administrative Roles. (An Administrator also may create new roles as needed.) An Administrator may assign multiple administrative roles to an account.

In some cases, it helps to restrict an administrative role to a specific organizational unit. For example, a person might be assigned the "User Management Admin" role for the "Staff" organizational unit. The person could create or delete user accounts in the "Staff" organizational unit only; they would not be able to create or delete user accounts for "Faculty" or "Students".

This ability to configure and delegate administrative privileges for an organizational unit allows Google Apps to scale to serve the needs of a large organization.

Organizational units

Things start simply: every account and device belongs to the same organizational unit. Every person has access to the same set of apps, with the same configuration. When an Administrator adds or enables an app, access to the app is enabled for everyone. For many organizations, that's how things remain.

However, with growth comes a need to configure groups of accounts differently. Settings may differ by business need, location, or organization. You might provide part time employees different access than full time employees, groups in different locations — or divisions — might require different settings, and affiliated or subsidiary organizations with different names may be more easily managed as a distinct group.

Create a new organizational unit

To create a new organizational unit, log in to the Google Apps admin console as a Super Administrator, then select Users. Select the "Filter" menu icon to display your organizational units, then select your initial organizational unit (this is typically your organization's domain name). Choose the menu to the right of your initial organizational unit. You'll see an option to "Add sub organization". Select this to add your sub-organization.

Once created, you may select and move both user accounts and managed Chrome devices to the new organizational unit. Remember, each account — and device — may belong to just one organizational unit.

By default, a new organizational unit inherits the settings of its parent organizational unit. Changes made to the parent organizational unit will be inherited by the child organizational unit. Conversely, changes made to the child organizational unit settings do not affect accounts in the parent organizational unit.

How many organizational units?

You should create as many organizational units as necessary, but as few as possible. Create a new organizational unit only when you identify a group of users that must have different access to services, devices or settings than other users. You may create an organizational unit that includes a single account, but that should be a rare event, not standard practice.

In general, keep things as simple as possible when configuring organizational units. Don't configure one unless you must. Remember, the goal is to simplify user management, not complicate it.

Domains and organizational units

Domains are unrelated to organizational units.

Initially, this may be confusing, since Google Apps supports multiple domains within a single Google Apps enterprise account.

However, additional domains added to Google Apps may be configured either as a domain alias or as a separate domain.

With a domain alias, one account will have two addresses: one for the primary domain and one for the domain alias. In this setup, both mary@companyA.com and mary@companyB.com are associated with a single person's account.

When configured as separate domains, the accounts are separate: mary@companyA.com and mary@companyB.com represent two different accounts.

These account addresses are unrelated to the organizational unit to which each account belongs.

That said, a Super Administrator certainly may choose to create an organizational unit, then move accounts into that unit. For example, a Super Administrator might place all people at companyA into a "companyA" organizational unit, and all people at companyB into a "companyB" organizational unit. This may simplify management when you wish to provide different access to Google services for the different companies.

Just remember that all accounts are part of the same organizational unit, until a Super Administrator configures the units differently.

Learn more about multiple domains from Google's "Additional domains FAQ"

Configure services and settings

As an Administrator, you choose which organizational units may access Google Apps services (such as Gmail, Calendar, and Drive), Google Marketplace Apps, and other Google services (such as AdWords, Google Analytics, or YouTube).

For most apps and services, you choose whether the service will be "ON for everyone", "ON for some organizations", or "OFF". However, some apps are either "ON" or "OFF" for everyone. For example, Google+ is either enabled or not for everyone on your Google Apps enterprise account.

Sample configuration: Google Sites

For example, at a school, we might want to enable Faculty or Staff to use Google Sites, but not enable Google Sites for Students. To configure this, we would create three organizational units, "Faculty", "Staff", and "Students". All three would be sub organizations of the main organization. We would need to move each user's account into the correct organizational unit.

Then, we would go to Google Apps settings in the Admin console, and select Sites, then choose "ON for some organizations". Since the master setting is "ON", we could select the "Students" organization then "override" the inherited settings to turn Sites "OFF" for "Students". The service would remain available for "Faculty" and "Staff".

Learn more from Google about how to "Apply policies to different users"

New Features? New services?

Some settings apply to all users in your Google Apps enterprise account.

For example, Google frequently releases new features and sometimes adds new services. You choose how these features roll-out to your users.

New features may be configured to be enabled "as soon as Google releases them" (Rapid Release), or a week or two later ("Scheduled Release"). The latter provides people more time to understand the changes.

New services may be set for an "Automatic" or "Manual" release. The manual setting requires an Administrator to enable a new service from the Admin console for users. Automatic makes a service available when Google releases it.

Learn more from Google about the "Google Apps release process for users"

Chrome devices

Google offers Chrome device management services for an additional fee. These services allow Chrome devices, such as Chromebooks and Chromeboxes, to be enrolled and managed from your organization's Google Apps admin console.

A managed Chrome device belongs to a single organizational unit, in the same way a user account does.

Chrome management settings allow administrators to manage network settings, manage installed apps, or configure printing. These settings — and many more — can be configured for the entire organization, or for a selected organizational unit.

As with other Admin roles, Chrome device administrative roles and privileges may be configured and customized by a Super Administrator. For example, a teacher might be given the ability to manage installed apps on Chrome devices for their classroom.

Learn more from Google about how to "Manage Chrome Devices" and "Delegate administrator roles in Chrome"

Administrative privileges and roles

Each Google Apps setup needs at least one account with Super Administrator privileges. The Super Administrator has full administrative authority for everything in the Google Apps setup. Because of this, people with Super Administrator privileges should take care to secure access to this account (e.g., use a strong password and require two-step authentication for access).

Additionally, while one Super Administrator is necessary, we recommend at least two people have this level of access. At a small nonprofit organization, this might mean that one staff person and one board member have Super Administrator access. In a large organization, this level of access would typically be restricted to trusted system administrators in different locations.

Pre-built roles

Google offers several pre-built Administrative roles, each of which provides some level of access to your organization's Admin console.

Three commonly used pre-built roles include:

- **Help Desk Admin**, who can reset passwords, as well as view user profiles and the organizational unit structure.
- **Groups Admin**, who can manage all tasks for your organization's Google Groups, including the ability to create, delete and manage membership of Groups.
- **User Management Admin**, who can manage all tasks related to non-administrative users. This includes the ability to create and delete user accounts.

Two less frequently used roles are those of a **Services Admin** and **Reseller Admin**. The Service Admin can manage services and settings for Google Apps, Google Marketplace Apps, and other Google Services. A Service Admin may also manage mobile and Chrome devices. As above, a person with Service Admin privileges may be a system administrator. The Reseller Admin is used in circumstances where an organization resells Google apps. (Details of the Reseller Admin role are outside the scope of this document. If you have access to that role, you'll know what it does.)

Learn more from Google about "Pre-build administrator roles"

Assign and configure roles

Only a Super Administrator may assign administrative roles. Multiple roles may be assigned to an account. A person's account might be assigned both a Help Desk Admin and Groups Admin role, for example.

Admin roles may be restricted to a specific organizational unit. A person might be given the User Management Admin role, but only for people within their organizational unit.

Often, the pre-built roles are sufficient. But in cases where they're not, a Super Administrator may create a custom administrator role. Customizable privileges include access to many administrative settings in the Admin console, including user management, groups, the Google Apps account, reports, security, support, services, Chrome and more.

Custom administrator roles for both Reports and Support may be helpful. The Reports privilege enables a person to access account usage information, audit logs, and search email logs. This type of access may be useful for various legal or regulatory compliance purposes. The Support privilege gives a person the information needed to contact Google enterprise support.

Learn more from Google about how to "Assign administrator roles to a user"

Google Groups

A Google Group simplifies communication and information sharing among a set of people. The most common Group is an email group. (Other types of groups include a web forum, a Q&A forum, or a collaborative inbox.)

A group administrator adds or removes a member to a group with each member's email address. Notably, a group may include members outside the organization.

Each Google Group has a unique email address, which is used to share information with the group. Send an email to the group email address to convey a message to all group members. Share a document -- or calendar, or site -- to the group email address to provide access to all group members.

Learn more from Google about "Google Groups for Business"

Directory sync from legacy systems

Google Apps Directory Sync (GADS) configures Google Apps organizational units, accounts and groups based on an existing LDAP (lightweight directory access protocol) server. Most often, GADS sync Google Apps account information with an existing Microsoft Active Directory server.

GADS changes your Google Apps data based on existing LDAP server data. Data on your LDAP server will not be changed based on Google Apps data. The "sync" is a one-way sync, not a two-way sync.

Install GADS, then configure it to connect to both your legacy LDAP server and Google Apps account. Next, define how you want users, groups, shared resource calendars and shared contacts to sync from LDAP to Google Apps.

By default, GADS places users into a single organizational unit. However, you may also choose to map existing organizational unit structures from LDAP onto a corresponding organizational unit structure in Google Apps. This would preserve your organizational unit hierarchies. (You may then configure services and settings in Google Apps with these organizational units.)

You may exclude account — or entire units — from the sync. For example, you might exclude administrator accounts from syncing, to ensure administrator accounts remains unchanged in Google Apps. Or, you might add an exclusion rule to preserve an existing Google Apps account that lacks a corresponding account on the LDAP server: otherwise, the Google Apps account would be deleted during sync.

After a successful manual sync of GADS, you may configure synchronization to occur periodically. (To do this, set up a scheduled task on Windows servers, or a cron job on Linux systems.) The synchronization may be set to occur hourly or weekly, depending on your environment. If your user list changes frequently, you'll likely want a more frequent synchronization.

GADS may be most helpful for an organization during a transition to Google Apps, since it allows continued used of your legacy LDAP server to manage accounts and organizational units during a transition period.

Learn more from Google about how to "Sync user data with your LDAP server"

Structure and culture

There's no more fundamental question for a leader to answer than "who has permission to (name a task)?"

The answer to that question reveals a great deal about how a leader enables people to succeed and delegates authority.

Your organization's Google Apps configuration will work best when your settings reflect and reinforce your organization's culture. Culture? In a bunch of settings? Absolutely!

Organizational units reinforce which people may access apps and services: the settings say "these people may", while "these people may not". Administrative settings control who may modify settings. Again, the settings say "these people may", while others "may not". In most instances, there are very good reasons for the settings.

However, be very alert to settings that restrict people's ability to succeed.

When a person has a self-perceived need for an app or access, but lacks permission, workarounds ensue. In such a circumstance, people seek out "unapproved" tools to get work done.

We suggest you periodically review your organization's Google Apps configuration to make sure your settings enable people to succeed.

Conclusion

Google Apps offers a great deal of flexibility and control to a Super Administrator. As covered above, a Super Admin may:

Create **organizational units** to allow different people to access different services (and devices), with different settings;

Delegate **administrative roles** to allow different people to manage specific services, apps or devices;

Configure Google Apps to support **multiple domains** to serve distinct organizations or branding needs; and

Create and manage **Google Groups** to simplify communication and sharing among Group members.

All of these settings work well once configured. But remember that business circumstances and roles change. Review your Google Apps settings periodically to ensure that the settings meet your organization's current needs.

Take a look at our other Google Apps guides for help during your review.

- Guide to Google Apps: How to setup your domain
- Guide to Google Apps: How to secure your domain
- Guide to Google Apps: Guide to External Mail Server Setup
- Guide to Google Apps: Advanced Security & Compliance