

Delegating your Google Apps user management to other people

Learn to share your Google Apps power without fear, so you can confidently delegate domain management to your staff while you focus on your real job

Who wrote this guide?

The authors have worked with Google Apps in growing startup companies since 2008, and now provide software solutions to integrate Google Apps with WordPress.

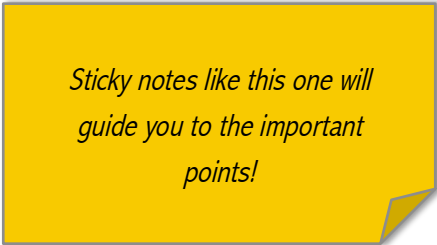
See <http://wp-glogin.com/>

Introduction

Setting up Google Apps users is easy, but can you make it even easier and also guard against potential future problems?

A simple 'employee change' checklist based on this document will mean you can delegate Google Apps management to support staff as your organization grows, without fearing that you will compromise security.

The guide is aimed at growing companies or organizations (perhaps fewer than 50 employees). You are the Google Apps admin, but you're not really a full time IT person.



*Sticky notes like this one will
guide you to the important
points!*

Contents

This guide will not cover the 'how to' of administrating Google Apps. Creating a new user or group is pretty easy, and working out new tasks can generally wait until the day you find out you need them.

Instead we'll cover a few things that a growing organization *can* always leave until tomorrow. But implementing them will mean that you can make user admin easier for yourself – or delegate to support staff without worrying (too much) that they have the keys to your whole organization.

First we need to cover a couple of features available in Google Apps, which you may not be using already, and then we put them together to help build your checklist.

- Topic summary: Organizational units
- Topic summary: Admin roles and privileges
- Delegating to support staff: checklist for new/leaving employees
- Creating a basic organizational structure with admin roles
- Avoid 'losing the keys'

If you don't initially want to cover details of the first two topics – organizational units and admin roles – just jump straight to the section on delegation for some ideas for approaching that!

Organizational Units

*Skip if you already know
this stuff!*

Organizational Units are a hierarchy that can be applied to user accounts, meaning you can control access to Google Apps features for every user within a particular group of units at once. This simply saves setting individual settings one-at-a-time.

So, for example, you may start off creating new users, and they are added to the top-level default organization. You give everyone in the organization access to GTalk. That's fine until you realize that your developers are interrupted too often with this feature enabled. So you create a new unit underneath the top-level organization called 'Developers'. You add all developer accounts to this, and then disable access to GTalk for that sub-unit.

Or you may need to create accounts for contractors, and you feel that they shouldn't have permission to share Drive documents outside the company. By contrast, full-time employees are trusted to make the judgment about which documents should be shared, so they have permissions to share documents with any Google user. So you can create a sub-unit for Contractors, changing Drive sharing settings just for those users.

There is a flexible system for inheriting these settings through the hierarchy. When you turn off GTalk for Developers, you can specify whether this will override any future changes to that setting higher up the chain.

Most small companies don't really need to treat different departments differently, and there is absolutely no need to create an organizational hierarchy that actually reflects your company's reporting lines. That's a waste of time until you have any need for different settings for different users – and when that happens, you may find that the company's reporting lines do not determine how those units need to be created anyway.

You can read Google's help topic on Organizational Units here:

https://support.google.com/a/topic/1227584?hl=en&ref_topic=2425090

Admin Roles and Privileges

Administrator privileges are rights that you can assign to a user allowing them to create or change other users' setup, or change groups and other Google services.

*Skip if you already know
this stuff!*

Most likely, whoever set up Google Apps is a Super Admin (meaning they can do anything to any user accounts). And maybe another company director was made a Super Admin as a backup. Unless you set up privileges for other staff, one of those Super Admins needs to personally create new users, manage groups, and deal with most support issues.

Other than Super Admin, there are the following default roles available:

- Groups Admin
- User Management Admin
- Help Desk Admin
- Services Admin

Groups Admin is allowed to create or edit groups and add users to them.

User Management means they can create or edit user accounts (but not change Organizational Units).

Help Desk Admin is basically a cut-down version of User Management – they can only read user details (can't create or change) and can reset passwords.

Services Admin can enable or disable specific services and change their settings – e.g. Email, Drive. This is obviously quite powerful, but at the same time, a Super Admin can immediately reverse any of these settings.

Roles are additive rather than hierarchical. Each role will bring a set of privileges to any user given that role.

You can approach roles and users either way round – you can view a list of users and assign roles, or you can look at roles and assign/unassign those roles to selected users. The first method: go to Users in your main (new style) Admin console, click on a user, then Show More at the bottom of the screen. Find “Admin roles and its privileges”.

For the second method, you can click Admin Roles in the main Admin console. It may be hidden under “More controls” at the bottom.

Just one usability note: Privileges cannot be assigned directly to users; Roles build up a set of Privileges, and then Roles can be assigned to Users. When Google displays the list of ‘resolved privileges’ that the role(s) assigned to a user will bring, all the privileges are greyed out (since you can’t change them directly). But you have to look pretty closely to understand whether the ticks are present or not!

One fear you may have about assigning Admin roles to others, such as support staff: can they delete or disable your Super Admin account? Or if not, maybe they can create a new user account that is a Super Admin, and then log in as that user and delete you...? It appears Google has thought about this, and as long as you do not make them a Super Admin, there are controls in place to ensure they cannot take ownership of the Google Apps Domain. More thoughts on doing this successfully are coming up next!

You can read Google’s help topic on Roles and Privileges here:

https://support.google.com/a/topic/2785005?hl=en&ref_topic=2661664

Delegating to Support Staff

It's very easy for the co-founders of a company, or director of an organization, to end up dealing with Google Apps user management for a long time as the company grows. Fears over handing security to others, and worries that they "won't do it right", can make it feel easier to keep full control personally.

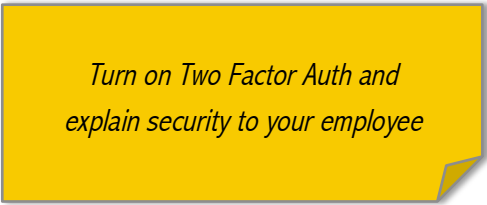
This can continue well past the point where the senior staff could have the help of existing support staff such as personal assistants or office managers.

Here are our thoughts on delegating Google Apps user management effectively.

In this section, let's assume that you have one trusted member of support staff (e.g. a Personal Assistant – PA) who you would like to manage Google Apps for everyone else in the organization (apart from two Super Admin company directors).

Increase Security

A sensible rule, if you don't already have it turned on for most users in your organization, is to insist that 2-step Authentication is turned on for all users who will become Admins – including



Turn on Two Factor Auth and explain security to your employee

yourself. Multi Factor Authentication is the security system whereby you require a code from a device such as a mobile phone as well as a password.

Enable this for your PA before granting any Admin rights, and ensure they are comfortable using it. You can insist on the use of MFA as part of your conversations designed to build up trust in the next section.

Build Trust

Before you expect your PA to take over this responsibility, it is important that everyone is happy:

- You trust your PA as a human – you don't expect them to abuse these powers deliberately, or through coercion from other staff members


- You trust your PA as a computer operator – you don't expect them to inadvertently grant unauthorized access or delete data
- Your PA needs to be comfortable with this new-found power
- Other staff will understand the new approach and be comfortable approaching the PA with support requests

Ultimately, communication is the best approach to this. You may gain some insight into your PA's understanding of security during your conversations about enabling 2-step Auth, and by seeing how easily they adopt the new security approach.

Do not be afraid to explicitly discuss all these issues around trust. Explain how severe to the on-going health of the organization it could be to lose access to Google Apps accounts.

Especially if the PA is a new member of staff, it may make sense to withhold admin rights until a significant event occurs, such as the very end of their three-month probation period – and make it very clear you are waiting for that time. That may underline the level of trust you are placing in them.

Before user management transfers to your PA, make sure you announce to the whole organization that support queries, and requests to set up accounts for new employees, should now be directed to your



Announce to everyone that Google Apps support is changing for them

PA. Explain how requests should be submitted – e.g. telephone or email, please do not bother the PA at their desk since they have other work that may take priority. Say that the PA will not be authorized to enable new services or change other settings without approval from you.

Remind all staff how important it is to keep passwords secret, to report if they may have been compromised, and to respect that the PA has clear guidelines to follow – for example, staff members must not ask the PA to give them access to another employee's account because they need information in that other employee's absence.

Finally, grant the relevant roles to the PA. For example: User Management and Groups. But do not make them a Super Admin.

Take the PA through the checklist (to be discussed in the next section) and ensure they understand how to actually perform the admin actions that may be required of them.

Checklists

Provide a checklist for your PA so they have clear guidelines for responding to support queries. In most cases, we are not suggesting that the PA actually needs to check boxes... but they do need a framework to ensure they understand how to maintain the level of security you desire.

We recommend keeping a staff directory, especially including phone numbers, so that employees can communicate with the PA, and vice versa, even if they cannot access their email.

Support checklist

How to check who they are talking to:

- Maybe direct emails about that email account are fine
- Perhaps phone calls should only be accepted from the registered phone number of the employee of that account – call back if needed
- Maybe employee's manager can call on their behalf, maybe not
- Don't go silly on these 'security checks' if your organization is small enough that the PA knows everyone anyway
- But as a minimum the PA must be sure they are talking to the account in question (don't take queries from a random Yahoo email address claiming to be an employee)

What can they do:

- Create new users? Maybe only on request from named managers
- Reset passwords
- Add/remove from groups? Maybe need a clear structure of which groups each type of employee should be allowed to join
- Change user's names? Add email aliases?
- Suspend or delete accounts? Presumably only on request from named managers
- Enable/disable particular services?
- Explicitly list actions they should not be allowed to perform
- State that things not covered should be cleared through you first
- These last two are important to give the PA confidence to refuse requests from staff members (who may technically be senior to them)

Employee change checklist

The support checklist mainly covered how to deal with ad-hoc support queries from staff. Also create a checklist to cover any Admin tasks that should be performed when certain HR events occur.

These lists can form part of wider-reaching checklists to ensure things happen outside Google Apps too. For example, you may need to enable other services such as Dropbox, or pass information on to your accountants. And you may wish to ensure that new joiners are introduced to relevant people, and given a tour of your products.

New employees

Keep a list of 'managers' who should be authorized to request new accounts to be created. List the information needed about a new employee – make a form if there is sufficient data required.

For Google Apps:

- How should email addresses be formed, especially if there are conflicts?
- Which Groups should they be added to?
- Are there any Organizational Units that should be respected?

The PA may not have billing abilities in Google Apps, in which case you will need to ensure that you have pre-paid for sufficient unused user accounts.

Departing employees

It is very important that you have a system in place for when an employee leaves. Not only must your PA understand this system but also managers must know to initiate this process in a timely manner.

The exact process may depend on why people are leaving, and managers may have different feelings about the risk posed by different employees – but that's why a checklist can be useful, to avoid this process being seen as being personal.

- Who can initiate requests for account termination – the list of managers again?
- Should accounts be suspended rather than deleted initially?
- Before suspension, should auto-responders be enabled?
- Before deletion, should the user's email be redirected to their manager?

- For employees who are terminated (rather than resigning voluntarily), should account suspension occur immediately following (or before) their termination meeting?
- Describe a process for transferring ownership of any of their Google Drive documents

Once a user account is deleted, you have five days to frantically contact Google if you really need it reactivated. They can't guarantee that all data will be intact either. So suspension can definitely be a good option, although the downside is that you continue to pay for the account.

Whether suspended or deleted, be careful with document ownership. You can see the number of docs owned by a user in their profile within the Admin console. It's sensible to go into the account and transfer ownership of all docs to someone else before it is turned off. Change the password of the account first of course.

For email forwarding, renaming the main email address of the departing employee, and then adding the real email address as an alias to their manager's email account, is the most permanent way to affect this.

Organizational Structure

In the example so far, for a relatively small organization, everyone is part of the same Organizational Unit, and only the Super Admins and PA have the ability to make changes to user accounts. Here we cover some reasons why you might want to create a more involved organizational structure.

*Just some reasons why
Organizational Units could be
useful for you...*

Keeping Senior Managers Immune

You may have a set of senior managers who should have a different level of trust to the rest of your staff. Those managers may be important enough that you don't want your PA to be able to change their accounts – that should be left to you as a Super Admin, if it ever happens.

To achieve this, set up a sub-unit for your Organization called Employees. You and your senior managers should be in the top-level Organization, and all other employees should be in the Employees sub-unit. Crucially, when you grant admin roles to your PA, you must ensure they only have rights within the Employees sub-unit.

Senior Managers Administer their own employees

Perhaps you have a senior manager covering each department in your organization: Operations, Sales, and Development; and you would like them to administer accounts for their own employees, but not be allowed to interfere with other departments.

In this case, you would create sub-units for each of those departments, granting Admin access to the manager only within their respective sub-unit.

Whether or not the manager themselves is in the sub-unit is up to you, but be careful to be consistent – if they have control of their own account, you need to think how you can make changes to their account that they cannot immediately undo.

Avoid ‘Losing The Keys’

*Small things to do that might
one day save your life!*

It may take a lot to overcome the fear of handing user management to a member of support staff.

But in practice, as long as they are not a Super Admin, they should not be able to perform many actions that are irreversible by you as a Super Admin.

Google itself is probably the biggest threat to your ownership of your domain. Ultimately, Google needs to be convinced that you are the rightful owner of your domain, and that you are paying for your Google Apps licenses.

This section describes safeguards that you may wish to implement in order to avoid the worst.

Domain Verification

Most likely, at some point you have been asked by Google to prove you own a domain name. This is where you are asked to add a DNS TXT record to your domain using whichever registrar helped you purchase your domain name – e.g. GoDaddy.

Google considers the ability to add this TXT record as the ultimate power!

Regardless of your roles and privileges, Google support will take any instructions for a Google Apps domain from anyone who can verify domain ownership in this way.

You should not be required to verify every time you want to do anything – sufficient privileges should be enough. But the domain name verification system tells you that in order to protect your Google Apps domain, you need to protect your domain itself.

DNS

Our recommendation would be to keep your DNS passwords highly secure... This is obviously important anyway, if your domain name itself is important to your business.

However, securing your Google Apps Super Admin accounts is equally important, especially if your DNS account can have its password reset through

your Google Apps email... This is a circular problem that can only really be solved by ensuring your DNS account is not tied to your company email address at all.

Avoiding Google Apps Support

We have described the importance of Google Apps support as though that is an enjoyable place to end up. Things appear to have improved over the last few years, but the product support forums are littered with people who have been shut out of their Google Apps accounts – most often for failing to pay (despite trying).

Use an independent domain registrar

It depends on the level of trust you place in Google and its own safeguards, but it could help to avoid nightmares if you do not use their own domain registration services in conjunction with Google Apps. As a last resort, even if Google refuses to acknowledge your existence, at least you could rebuild your digital presence elsewhere...

Super Admins

Google recommends that you do not add more than three Super Admins to your Google Apps account. Doing so “may limit your account recovery options”.

Billing

Keep on top of billing. There is no bigger threat than finding your credit card failed, and you ignored all warnings that your account will be suspended. There are a couple of things you can do in advance.

From your Admin console, select Billing. There should be a button labeled with a '\$' – Access billing account. Click through.

Billing settings – here you can add a backup credit or debit card. Not a bad idea in case your payment fails.

Billing profile – here you can configure a list of email address which will receive various types of billing notices, such as payment failures and impending suspension.

Make sure it's more than just you. And if you tend to ignore automated emails, add someone – anyone – who doesn't!

Another consideration is that the person who creates new user accounts may not have authorization to actually pay to have the number of accounts increased. Maybe that person should ask you to authorize another five users whenever they see that they only have one or two licenses available – be aware that you will have to pay for the unused licenses though.

Conclusion

We hope this guide has given you some ideas for sharing Google Apps management with others instead of insisting on doing everything yourself! Please let us know if it has helped you, or if you have better ideas... Get in touch via contact@wp-glogin.com

Join our mailing list

For more hints and tips like these, don't get left behind – join our mailing list at wp-glogin.com!

WordPress Plugin

Google Apps Login for WordPress is a plugin allowing users to log into blogs using Google to securely authenticate their account – no username or password is explicitly required. It eliminates the need for Google Apps domain admins to separately manage WordPress user accounts, and gives piece of mind that only authorized employees have access to the company's websites and intranet.

See <http://wp-glogin.com> for more details.

You are free to distribute this PDF exactly as published, but may not modify its contents in any way.

This guide is copyright 2013 Lesterland Ltd, company number 8553880 registered in England and Wales. Registered office: Riverdene House, 140 High Street, Cheshunt, Waltham Cross, EN8 0AW.