datto

EBOOK

5 ESSENTIALS TO A SUCCESSFUL GOOGLE APPS ADMINISTRATION

Expert Google Admins on the Biggest Problems to Avoid in Managing Google Apps Domains

Table of Contents

INTRODUCTION: HINDSIGHT IS 20-20

Believe it or not, Google Apps turns 10 years old in 2016. Today, there are seasoned Google Apps administrators with years of experience under their belts. These admins have amassed a wealth of knowledge on running Google Apps for Work domains over long periods of time—and they’ve identified significant problems that only become apparent to an admin once Google Apps hsd been in operation for years.

We consulted a quintet of these Google Apps experts—who have worked for multiple companies in multiple industries—to find out which future Google Apps headaches you can avoid with a little careful planning in the present. With the help of their advice, we’ve outlined five areas of concern you can address when setting up your own Google Apps domain, so small problems today don’t become major issues tomorrow.

GETTING SECURITY RIGHT THE FIRST TIME

To no one's surprise, security is easy to get wrong when configuring your Google Apps domain. Even when you follow a reputable security guide, enable two-factor authentication, require SSL at all times, and encrypt your Gmail messages, there's still plenty of work to be done. A lot of that security work isn't obvious, and may require using Google Apps in ways that wouldn't occur to many administrators.

Build a Better Super Admin

Sean Satterlee, Senior Information Security Architect at Findly, is a reformed hacker, and his advice for Google Apps security boils down to this: "Hold tight your Google Super Admin."

The primary administrator or "Super Admin" of your Google Apps domain has broad-ranging powers over every service and user on that domain. If a hacker compromises the Super Admin, they can lock out all the other administrators, suspend or delete all the other users, and steal or destroy all the data on your domain. That's why Satterlee tries not to use the Super Admin whenever possible.

"Don't use the basic Super Admin. Like UNIX, don't log in as root. Build an everyday use account," says Satterlee. This account can be a standard user with administrator permissions that isn't listed as the Super Admin with Google. If you don't remember creating a Super Admin, you probably are one. The first user created when setting up a Google Apps domain is, by default, the primary administrator. Once you're done configuring your domain, create an everyday account for your use and keep the primary admin account on lockdown.

Bear in mind that the Super Admin gets information from Google that no other account on the domain will automatically receive, but Satterlee has a simple solution for that. "Just forward all the superuser alerts to the everyday account." A few smartly composed Gmail filters in the Super Admin's inbox will forward all the relevant alerts to one or more non-super administrators.

In certain cases, the Super Admin's privileges are needed for a specific domain configuration task. When that happens, you can log in as the Super Admin, do the work, and then log out. But under no circumstances should the Super Admin for your Google Apps domain be receiving personal messages to Gmail, opening shared documents, or accepting Google Calendar invitations. Satterlee has personal experience as to why.

The first user created when setting up a Google Apps domain is, by default, the primary administrator. Once you're done configuring your domain, create an everyday account for your use and keep the primary admin account on lockdown.

“I was helping a company, and they were using Google Apps. They had no security set up at all. No two-factor, nothing. They were sharing a load of emails, and their password manager had [the] Heartbleed [security bug]. I used this to get access to the shared Gmail accounts, which gave me access to their Google Apps admin account. That gave me everything.”

Employing a Google Apps Super Admin account for everyday correspondence makes it a target for these kinds of attacks. **Don’t use it!** Give your admin a “mortal” account instead.

Set Up Data Loss Prevention the Smart Way

One of the most promising recent security innovations in Google Apps for Work is Gmail’s Data Loss Prevention (DLP) feature, which scans outgoing mail for sensitive data and stops it from leaving your domain if it violates certain policy algorithms. Think of it as a reverse spam filter; instead of keeping unwanted messages from entering your inbox, DLP makes sure that Gmail doesn’t expose any information that shouldn’t be shared outside your company.

Data Loss Prevention comes with a number of built-in content detectors for identifying common terms like credit card or social security numbers, but DLP also allows administrators to set up a number of custom filters. When one of these custom filters detects an outgoing email message that contains information that may violate your information-sharing policy, your domain administrator can be alerted.

This, in effect, means your Google Apps domain administrator can spy on outgoing Gmail messages, which sets up a “who watches the watchmen” security scenario. Google Apps administrators should not be allowed to configure DLP without oversight, as Satterlee explains.

“When you do DLP, you really need to make sure your Google Apps admin is an InfoSec person.” If the administrator doesn’t understand the implications of the outgoing content detectors, they could fail to filter the right content, or abuse the privileges DLP offers.

“If, for example, you put in a filter for [expletive], your admin will get an email every time an executive chews out a subordinate, which could expose confidential data. An unethical admin could also put in filters for terms like ‘layoff’ or ‘IPO’ and use it to get sensitive info from executives.”

Data Loss Prevention is, in many ways, an internal Google Alert for specific Gmail content. Make sure that when you configure DLP you consider the implications of every content detector and who will receive the alerts they will generate.

> I was helping a company, and they were using Google Apps. They had no security set up at all. No two-factor, nothing. They were sharing a load of emails, and their password manager had [the] Heartbleed [security bug]. I used this to get access to the shared Gmail accounts, which gave me access to their Google Apps admin account. That gave me everything.

Avoid “Privilege Creep”

Colin McCarthy, North American Associate IT Director for Essence, has administered Google Apps domains personally and professionally since 2010. His concerns about Google Apps begin with Google Drive.

“One of my complaints about Google with their Drive management policies is it’s far too open. As soon as you create and share a document, the default setting is for that person to be able to add other accounts without the document owner knowing. Default permissions should be the lowest access level, *View,* and not the highest, *Can Edit*. I really wish Google would update these policies. Certain sharing settings are an individual per-user, per-document setting and not something we as Admins can enforce. This can create a problem if you have a user that’s leaving, there’s nothing to stop them from adding their personal Gmail to a load of documents, and keep the ability to view or share your confidential data outside your company. Employing 3rd party DLP software can alert you of these instances.”

Jon Stotter, IT Manager at DialogTech, agrees. “[Users] don’t have a good understanding of security, especially on Google Drive. Things like, what you’re supposed to and not supposed to share to people outside the company. How much exposure this gives to the company. Making stuff available or unavailable to their peers.”

McCarthy’s preferred solution, beyond the usual tweaking of Google Drive sharing options, is to remove as much personal ownership of key documents as possible. “Instead of everybody owning documents in a department, we would have created a system account, and then created a directory structure in that account, and gotten people to copy their documents [to the system account]. A system administrator would have periodically taken ownership of those documents.”

Under McCarthy’s scheme, the system admin would have final ownership authority—and thus control of sharing—for all critical documents in a department, organizational unit or even a full domain. If an employee leaves, the documents remain with the admin account. There are additional benefits to centralized admin document ownership. “When we use a tool like Datto Backupify,” McCarthy notes, “we could more easily do restores and keep all the sharing right.”

Data Loss Prevention is, in many ways, an internal Google Alert for specific Gmail content. Make sure that when you configure DLP you consider the implications of every content detector and who will receive the alerts they will generate.

ESTABLISH A LICENSE POLICY

Part of the appeal of cloud-based tools like Google Apps is simplified user license management. Since Google Apps is priced on a per-user, per-month basis, the days of overbuying blocks of software licenses to get a price break are over. The counterpoint to the fluidity of Google Apps licenses is that it's easy to let your license count get out of control, and every additional or unnecessary user comes with a very specific price attached.

Without the discipline of a finite license number to keep costs in line, administrators need to establish a firm Google Apps license policy. Thus, when you're tasked with creating another Google Apps user account, you'll have a set of guidelines to help you properly approve or deny the request.

When Does a Non-Person Get a Mailbox

One of the more common assumptions about Google Apps is that there is a near one-to-one relationship between the number of employees at your organization, and the number of Google Apps licenses you'll need. **Matt Hrono**, the former Google Apps Administrator Supreme at America's Test Kitchen, has personal experience to the contrary.

"We're using mailboxes for various other things than people. Every employee has their own email address. Some departments have shared mailboxes. Every time we create a hiring requisition, we use a mailbox for that requisition. Some people will have two to three mailboxes themselves."

> Instead of everybody owning documents in a department, we would have created a system account, and then created a directory structure in that account, and then gotten people to copy their documents [to the system account]. A system administrator would have periodically taken ownership of those documents.

Why not just use a Gmail alias, or a Google Group, instead of paying for an entirely separate mailbox? "With the shared mailboxes, they want a single source of truth, rather than a list, which just sends a copy. With [Google Groups], more than one person could respond to the same message." There's a legitimate use case for shared Gmail inboxes, but it's also an easy privilege to abuse.

Google Apps administrators need to lay out an explicit policy for what users qualify for their own Google Apps account and mailbox, and which department's budget will bear the additional license costs. Without these safeguards, you could end up with dozens or even hundreds of extra user accounts doing jobs that could just as easily—as far more cheaply—be performed by other Google Apps features.

How and When Do You Purge Old Licenses

There are issues beyond cost when it comes to excess Google Apps licenses. In any organization, users eventually leave, special projects end, and open requisitions are either filled or cancelled. Something must be done with the data in the resulting unneeded Google Apps accounts.

“The biggest [problem with Google Apps] I’ve noticed is ‘license creep,’” says Hrono. “We have a fixed number of licenses [in our budget], and we keep bumping into the cap. It seems like every week we’re cleaning old ones out.”

McCarthy has the same issue. “One big challenge at the moment is license management. Making sure your license count doesn’t spiral out of control, depending on the turnover and the size of the company, can be a challenge.”

Anthony Miglioranzi, Senior IT Administrator for General Assembly, is in the same boat. “We have a lot of active accounts that are for people that aren’t here anymore. Right now we’re paying for accounts we don’t need.”

License creep is also something Satterlee constantly warns his clients about. “When someone departs, do you have any processes in place? How do you keep from having 18 different aliases for their manager?”

The solution, according to McCarthy, is “efficiently deprovisioning ‘leaver’ accounts. Make sure you have workflow with your support staff when someone leaves. [That entails] making sure documents are transferred to a line manager, keeping a backup copy of the email. Making sure calendar entries are deleted, data is transferred. Now, with cloud-based systems, it’s relevant for not just Google Apps, but Microsoft 365 and Adobe Creative Cloud, and so on.”

Miglioranzi has a similar set of deprovisioning criteria. “Before we delete [user accounts] we need to make sure that we save the data, and then move it to the appropriate manager or team member that’s taking over for the termed employee.”

This concern comes up so often that Datto Backupify devoted an entire eBook to safely deprovisioning Google Apps users. This guide covers the complete *process* of deprovisioning, but not the *policies* around it. That’s a distinction that many Google Apps administrators overlook. Hrono explains. “The pain point for us is managing content ownership in Google Docs, Sheets, Slides, or whatever when someone leaves. We do use pretty extensively the bulk ownership transfer tool, but a lot of times when people leave the company, they have personal information that they don’t want others to have, or things only their manager should have, or only [Human Resources] should have. So that bulk transfer isn’t practical.”

> When we use a tool like Datto Backupify,” McCarthy notes, “we could more easily do restores and keep all the sharing right.

> We're using mailboxes for various other things than people. Every employee has their own email address. Some departments have shared mailboxes. Every time we create a hiring requisition, we use a mailbox for that requisition. Some people will have two to three mailboxes themselves.

Miglioranzi has similar concerns. "I wish HR had locked down best practices [about] how long an account stays active before it gets deleted. Who's automatically receiving the Google Drive documents an employee left behind when their account is reset?"

In ideal circumstances, the departing employee is the best expert on who should receive their Google Apps data. Hrono has adapted that concept for his deprovisioning policy. "A few weeks before someone leaves, we sit down with that someone and show them how to transfer individual items to others."

Hrono's policy also accounts for employees who aren't always around to cooperate. "If we have someone who is let go or leaves without notice, we'll generally do a bulk transfer to their direct manager, and they deal with it however they want to deal with it."

Google Apps administrators should download this checklist for deprovisioning unneeded user accounts, and create a set of criteria for identifying user accounts that need to be deprovisioned. And these standards need to be in place sooner, rather than later. Otherwise, you risk encountering the same issue that Hrono, McCarthy, Miglioranzi, Satterlee and nearly every Google Apps admin we've ever spoken to is dealing with—a bunch of old Google Apps accounts they don't need, but are still paying for, and that contain data that may have no obvious home in someone else's Google Apps account.

ACT LIKE A BIG COMPANY BEFORE YOU ARE ONE

A number of organizations adopt Google Apps because it's priced attractively for small companies that don't have the staff or resources to deploy more traditional enterprise-scale solutions. However, most successful organizations grow over time, and an absence of mature Google Apps best practices in the early days of your domain can create exponentially more work when the number of users you're supporting increases.

Create Org Units Now, Not Later

When McCarthy took over his first professional Google Apps domain, the company had been using the solution for over a year—without a full-time admin at the helm. That meant McCarthy had a lot of cleaning up to do, particularly as applies to Google Apps organizational units. (There's an ebook for setting org units up, too.)

"The biggest challenge was management and organization. At that point, everybody was put in a root organizational unit. You'd have to scroll through multiple pages to check last log-in dates and see if anyone had left. So I instigated an OU policy, so I could work out who was in what department, and it was a more manageable list of users."

Miglioranzi is just starting the process at his company, and his predicament underscores the need for adequate org. unit planning in the early days of your domain. "We don't have any organizational units set. I need to go back and build them so I can really get a bird's-eye view of all the departments in our company. I need to sit down and see how we're going to set this up so it makes sense. So when other people are added to Google Apps, they're already added to all the Google Groups."

Most companies have plans for growth. They budget for new employees, new equipment, new facilities and new customers. Google Apps administrators should be tuned into those growth plans, so their Google Apps domains can have the org. units they need in place before your user roster becomes too big to handle.

Get the Tools to Manage a Mass of Users

Setting up Google Apps for theoretical user growth is one thing; having the tools to handle large numbers of Google Apps accounts is another. The Google Apps Admin Panel is built with the expectation that you'll be managing a small group of users, and making very few changes at a given time. As your business grows, this can become cumbersome.

Miglioranzi sums the issue up well: "I think automation is the biggest [Google Apps problem] I'm running into. Manually administering is tough."

McCarthy cites a specific example of Google's automation breakdowns at scale. "The problem was the inability to multitask in the Google Apps Admin Panel. If a new user was in 10 email groups, you'd have to add them 10 times to 10 groups. Even in this day, six years later, there's no way to add a single user to multiple groups in the Google Apps Admin Panel. You still have to add a single user to multiple groups."

Satterlee is blunter in his assessment of the differences between Google Apps and other user-management systems. "When you set up a Microsoft Active Directory, it's been built with expectation that you're stupid, so there's a lot of help for you. Google Apps gives you free range, but it doesn't give you warnings that 'you might not want to do this.' It might open doors you don't want open."

Hrono praises Google Apps for its ability to let other tools do the bulk user management work, at which the Google Apps Admin panel isn't so great. "I have nothing but good things to say about Google Apps Active Directory Sync. It saves so much time and works so well, that on a good day I never have to go into the Google Apps Admin Panels. I can do it all from Active Directory and it just syncs up to Google."

Google Apps administrators need to lay out an explicit policy for what users qualify for their own Google Apps account and mailbox, and which department's budget will bear the additional license costs. Without these safeguards, you could end up with dozens or even hundreds of extra user accounts doing jobs that could just as easily—as far more cheaply—be performed by other Google Apps features.

I have nothing but good things to say about Google Apps Active Directory Sync. It saves so much time and works so well, that on a good day I never have to go into the Google Apps Admin Panels. I can do it all from Active Directory and it just syncs up to Google.

"We just rolled out Google Apps Password Sync. As soon as someone changes their [Active Directory] password or their password expires, it instantly syncs with Google. That's crucial. Instead of waiting 10-15 minutes before [a local password change] works with email, it works instantly, and that's been very, very helpful."

Beyond Active Directory, BetterCloud for Google Apps earned mentions from nearly all of our experts as an enhancement to the Google Apps admin panel.

Regardless of which tools you use, it's best to have the necessary software in place before your Google Apps roster gets too large to competently manage.

DOCUMENT BEST PRACTICES BEFORE YOU NEED THEM

Software tools are only as good as the policies that govern their use (and how rigorous you are at adhering to those policies). Google Apps wraps a number of office productivity functions into a single solution suite, which means several of your IT policies need to be updated when you adopt Google Apps.

Set Up Naming Conventions and Folder Structures

McCarthy loves Google Drive, he just wishes his company had been a bit stricter about organizing it when they first moved to Google Apps. "We have a lot of files that [live inside a set folder] structure, a very tree-like hierarchy on our internal file servers. [Our instance of] Google Drive didn't really use that at first, and now it's hard to build that. It would have been easier to think and plan that earlier on. As our business has grown, the first ten people know where a document is, but now they have to give everyone else the link because people don't really know where important documents live. It's knowledge management that's our biggest struggling point."

Many organizations don't put such planning into folder structures and knowledge management, as they assume the built-in search functions of Google Apps make browsing hierarchy a moot point. Not so, says McCarthy. "We would have also instigated a naming convention for Google Docs, just to make searching easier."

Miglioranzi takes this advice a step further, applying naming conventions outside Google Drive, too. "Calendars, Groups, Drive files; there should have been rules about how they're formatted. For example, if we have a Seattle market, you're teaching at Seattle, the group should be *teach_seattle*. That's how the formatting should be enforced so it's intuitive [when you search for it]." Without naming conventions, users can spend extra time guessing at what a file might have been named, and still never locate it.

Best practices around both file names and file locations mean that no user need ever ask for a file; they'll be able to find it on their own. For a naming convention policy to be most effective, it must be established during Google Apps setup, and enforced from there on out.

What Does Onboarding Look Like

We've talked about the problems that arise when you don't have a policy and process for deprovisioning a Google Apps user, but failing to have provisioning checklists can be just as problematic.

Miglioranzi has this simple warning: "We need to make it easier from an IT perspective when we onboard."

Stotter's new-hire checklist looks something like this:

1. Create a network password
2. Designate a computer for the new user
3. Designate a phone for the new user
4. Create a Google Apps account
5. Add the new Google Apps account to the appropriate Google Groups
6. Install Google Drive on designated computer
7. Add the user to other cloud applications, like ZenDesk or CrashPlan

You'll note there are several spots in this very reasonable checklist where policies and guidelines should be spelled out. In Step 1, what is the required password strength for all users? In Step 7, which applications does a new employee need? In Step 5, what Groups does a new employee need to belong to, and what processes govern that determination? In Stotter's experience, Group management is where onboarding most often falters.

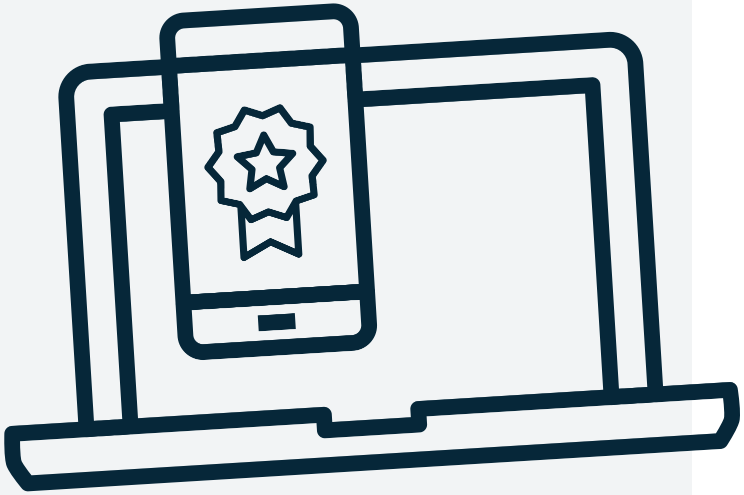
"That's a challenge, managing groups. Our sales team changes often; people move teams left and right. The managers don't bother to notify me they're moving teams, and it messes things up."

The only Groups Stotter knows to add users to are "an all-staff group (for all employees), and an all-female group, Women of DialogTech, that has its own email list."

A firm process for onboarding will prevent an untold number of help requests in the future.

> **"**
> **Calendars, Groups, Drive files; there should have been rules about how they're formatted. For example, if we have a Seattle market, you're teaching at Seattle, the group should be teach_seattle. That's how the formatting should be enforced so it's intuitive [when you search for it].**

Just because you adopt Google Apps doesn't mean that the solutions Google replaces will ever entirely go away. Be sure to keep the knowledge and tools necessary to maintain your legacy technology (or, at the least, major examples of non-SaaS technology like Microsoft Office) on hand. You never know when you'll need them.



Be Ready for Exceptions to the Rules

No matter what policies or processes you install, there are always edge cases and exceptions you must be prepared to handle. For example, when you adopt Google Apps, you may officially "retire" desktop mail clients, but that doesn't mean you no longer have to support these applications.

Stotter explains, "You have senior VPs that join the company, and they're stuck with their old habits. Users that insist on using external tools like Outlook or Mac Mail. You have this whole business to go through synchronizing them. As good as the tools are, it's still a pain."

In fact, the ability to tolerate exceptions to device and platform policies may be why your organization adopts Google Apps in the first place. That was the case when Hrono was at America's Test Kitchen. "We went to Google Apps because we're a hybrid PC/Mac environment, which is challenging. Managing an Exchange and Outlook profile in a hybrid environment isn't quite so easy as it is with Google. We went with Google to make it simple."

Just because you adopt Google Apps doesn't mean that the solutions Google replaces will ever entirely go away. Be sure to keep the knowledge and tools necessary to maintain your legacy technology (or, at the least, major examples of non-SaaS technology like Microsoft Office) on hand. You never know when you'll need them.

NEVER STOP TRAINING

Stotter articulated a sentiment that was common to every Google Apps administrator we spoke to: "I tell [users how to get the most from Google Apps] in new-hire orientation, but I don't know how much they retain." Training isn't a one-time activity. You can prevent many problems—and boost the productivity of your users—by regularly retraining everyone. Below, we outline some key areas to focus on in your training efforts.

Someone Is Always a Novice (Even the Veterans)

No matter what you as a Google Apps administrator think is an obvious aspect or function of Google Apps, your users may well have no idea that feature is available in Google Apps. Our administrators had plenty of examples.

Miglioranzi: "People get really excited when you show them the Apps icon, believe it or not. Show them that there are other apps. It blows some people's minds. I know that's not a trick, but it always gets people going."

Stotter: “I wish [my users] knew efficient use of Google Calendar. They just don’t know, and they either come to me or they just don’t use it to make their own lives much easier. Google Calendar has some nifty tricks like booking rooms and finding free time, and many of them don’t bother to find that out.”

Hrono: “Some people will get a little confused by sharing settings and the options available to them [in Google Drive]. We don’t have issues with over-sharing as much as under-sharing, where someone intends to share something a certain way and does it wrong, and doesn’t end up sharing it at all. A little bit of training and hand-holding may be required. That’s our main training issue.”

Train, train, and retrain some more. The efforts you spend in educating your users will save you tenfold support requests.

Phishing is a People Problem, Not a Tech Problem

Phishing is a social engineering tactic, wherein a fake webpage is mocked up to look like a real one in the hopes that an unwitting user will log into the phishing page, thereby divulging a username and password. It is among the most significant security risks that users are not trained to deal with.

Miglioranzi takes precautions because of it. “We had a lot of phishing emails going around, which is why we’re doing two-step verification.”

Satterlee goes even further, especially when it comes to multi-factor authentication on his prize administrator accounts. “I do three-step MFA. When you go log in, use a Yubikey, an authenticator, and password.”

That’s a technical remedy, but Satterlee concedes it can’t really solve the problem. “Not training people on phishing campaigns. Wow, that’s a big one. People will click on anything. If you make it look remotely like a Google Drive, they’ll click on it.”

No matter how good your security software, if you don’t warn your users to look for phishing attacks, they will inevitably give a hacker the credentials necessary to bypass all your safeguards. Phishing is a people problem, not a technology problem, so train your users accordingly.

No matter how good your security software, if you don’t warn your users to look for phishing attacks, they will inevitably give a hacker the credentials necessary to bypass all your safeguards. Phishing is a people problem, not a technology problem, so train your users accordingly.

Your Users Can Be Assets Instead of Liabilities

All the tasks and best practices we've laid out in this expert guide can make the job of a Google Apps administrator seem endless. If you're not careful, your user base can start to seem like a problem to be solved, rather than the group of colleagues you're paid to support. Ironically, the single greatest asset that admins fail to use to lighten their own workload is their own users.

McCarthy learned to bring users into the fold long ago. "People are more likely to listen to their coworkers than the corporate overlords dictating what they use."

"Before we did the migrations, I would find which one of those [people] I was moving was a fan of Google Apps or Gmail or Google Drive, and I would employ them and work with them to advocate [Google Apps to coworkers]. 'Yes, you won't have Outlook anymore, but you'll be gaining all this flexibility and this ability to collaborate more easily with your colleagues.' It's being honest, there are things you'll miss, but there are add-in tools to Gmail that will let you do similar functionality."

Before we did the migrations, I would find which one of those [people] I was moving was a fan of Google Apps or Gmail or Google Drive, and I would employ them and work with them to advocate [Google Apps to coworkers]. 'Yes, you won't have Outlook anymore, but you'll be gaining all this flexibility and this ability to collaborate more easily with your colleagues.' It's being honest, there are things you'll miss, but there are add-in tools to Gmail that will let you do similar functionality.

The technique proved very effective both during and after the adoption of Google Apps. "When we did our migrations, we experienced very, very little resistance. And it was usually from the more mature members of staff. Once we gave a little more training—showing them all the data was still there, just the interface is different—they were fine. My advice is to get end-user buy-in and give a lot of training."

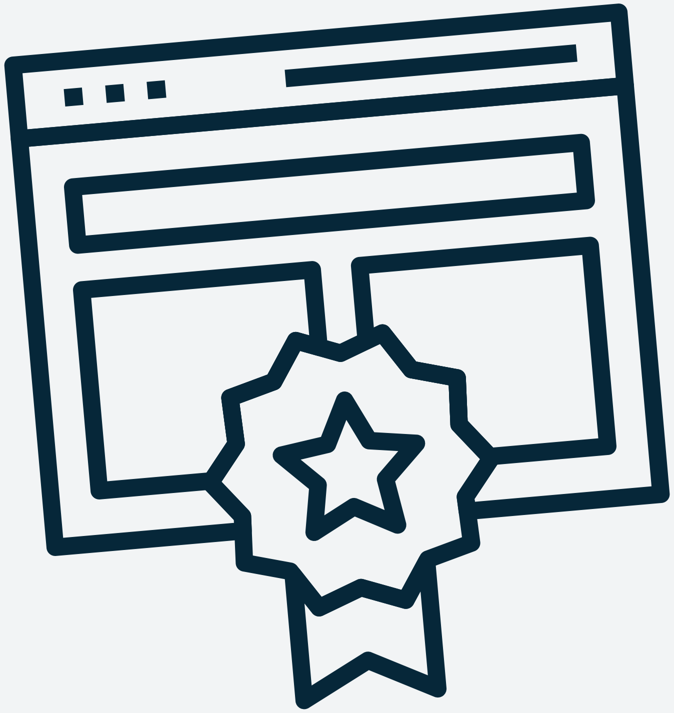
As an IT administrator, your job is to make sure your users have the tools to be successful in their daily tasks. Never forget, your users can be one of the most effective tools in getting the IT admin's job done, too.

CONCLUSION: AN OUNCE OF PREVENTION IS WORTH A POUND OF CURE

Google Apps is an incredibly robust office productivity solution, one which offers its administrators a surprising level of control over security, accessibility, and functionality. The choices you, as the administrator, make in the early days of a Google Apps deployment can prevent problems from arising in the future.

If you properly plan your security, establish a license policy, document your best practices, plan for growth, and resolve to constantly train your users, you can avoid many of the most common problems that plague Google Apps domains over time.

And, as always, have a good backup plan.



MEET THE EXPERTS

Matt Hrono
Systems Administrator
at Cimpress

Colin McCarthy,
Associate IT Director,
North America
at Essence

Anthony Miglioranzi,
IT Support Specialist
at General Assembly

Sean Satterlee
Senior Security Architect
at Findly

Jon Stotter
IT Manager
at DialogTech