

Architecting Your Ideal Admin Environment:

How to Configure Google Workspace for
Better Security & Collaboration

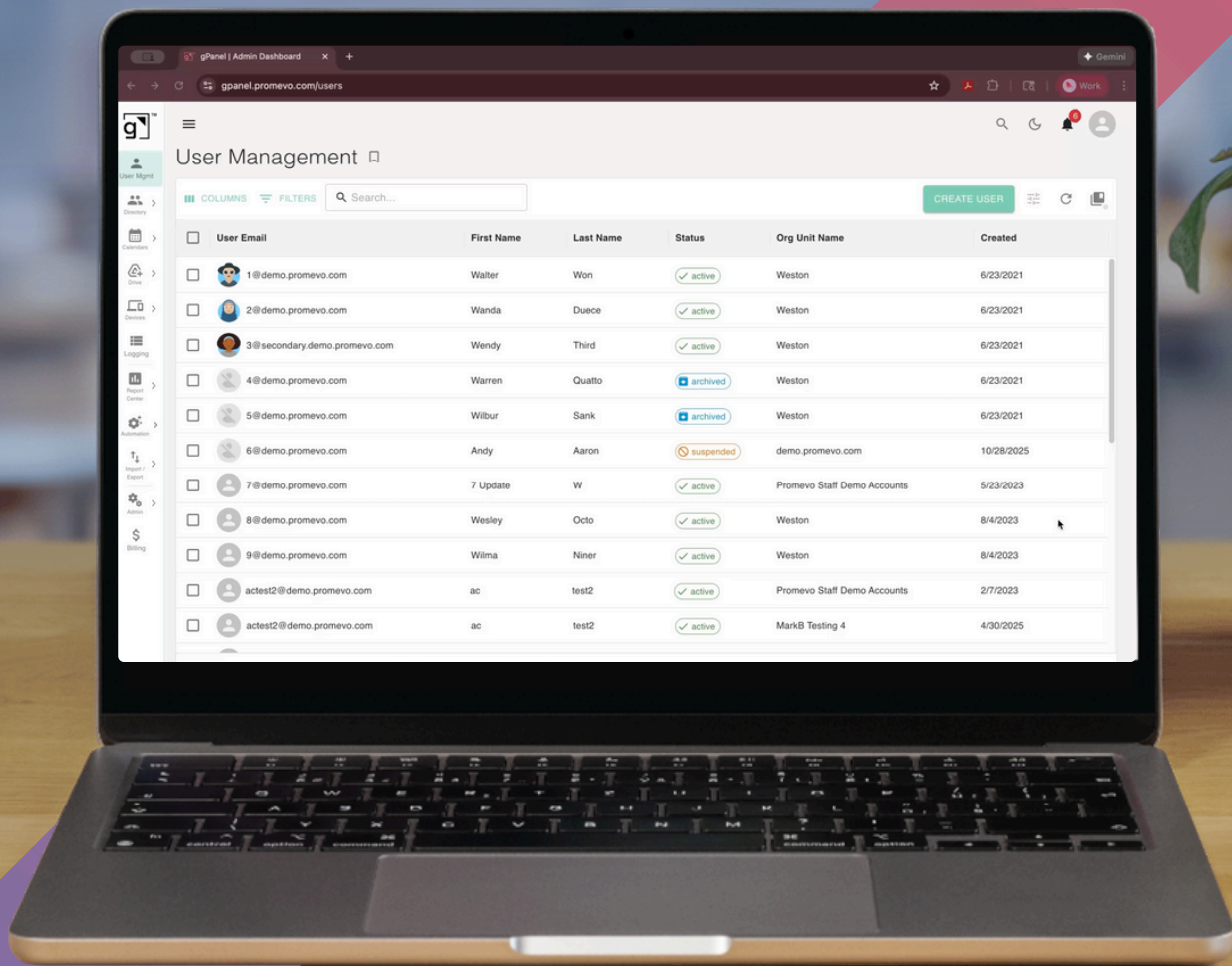




Table of Contents

3	Introduction
4	Foundations of a Secure & Productive Admin Environment
7	Roles & Responsibilities in Workspace Administration
11	File Access & Permissions Architecture
19	Security Settings & Guardrails
24	Onboarding, Offboarding & Lifecycle Management
28	Reporting, Auditing & Compliance
31	How gPanel Optimizes Your Admin Environment

Introduction

Whether your organization is new to Google Workspace, or you simply realize it's time to create a better system for using the tool effectively, the best time to develop a strong Google Workspace strategy is now.

A key prerequisite for making sure you get the most out of Workspace is understanding all the features available that aid in collaboration, security, and productivity. That's where this guide comes in. We'll cover many of the most important features and best practices for configuring your Google Workspace so it works well for both your employees and the larger organization.



Chapter 1:

Foundations of a Secure & Productive Admin Environment

Building a strong Google Workspace configuration for your organization starts with a strong foundation. Most businesses will want to prioritize two main aspects of Workspace: security and productivity. To establish the right processes and guidelines for Workspace in your organization, these are some of the most fundamental principles and structural elements to keep in mind.

Core Principles

You don't want to approach Google Workspace based on what you need today. You want to configure your Workspace to account for all your potential future needs as well. Some principles to guide you are:

- **Least Privilege:** Least privilege is a security concept that ensures people only have the level of access to sensitive information needed to do their job.
- **Scalability:** Policies that make sense for an organization of 5,000 may not suffice when it grows to 25,000. You want the structures and strategies you put in place now to be scalable enough to seamlessly grow with your business over time.
- **Visibility:** Admins can only control what they can see. Being able to track data on vital metrics like user behavior, storage capacity, shadow IT use, external shares, and more is crucial to ensuring you use Workspace responsibly and effectively.
- **Auditability:** Compliance is key in the modern business environment. Administrators need a way to generate audit logs and identify potential security and compliance issues as soon as they occur.



Workspace Structure Basics

Google provides organizational tools that help you strategically structure your Workspace in the way that works best for your employees. That includes:

- **Organizational Units (OUs):** You can create OUs based on departments, teams, or domains in order to apply standardized security and access policies across the unit.
- **Groups:** Google Groups let admins easily manage permissions for shared resources like Drive files, calendars, and Google Meet sessions. You can use groups to create mailing lists and set access for internal tools without manually adjusting settings for every user.
- **Shared Drives:** Shared Drives are a useful collaboration tool. You can control access permissions at the Drive level, to ensure all relevant users have access to the files and folders they need at once.



Chapter 2:

Roles & Responsibilities in Workspace Administration

When thinking through your security strategy for Google Workspace, start with clarifying the main roles in your organization that should have administrative access. Then consider what level of access they need to effectively carry out their responsibilities.

Common Types of Roles

While administrative access can take many forms in Google Workspace, we can divide [Workspace administrators](#) into two main categories:

- **Super Admins:** Super Admins are your top-level administrators who have access to all the Google Workspace features, can set up access permissions for everybody else in your organization, and have the ability to manage every aspect of your company's account.
- **Delegated Admins:** Delegated admins are given administrative access by Super Admins, but with limits determined based on the delegated admin's role. A Super Admin decides which features a delegated admin needs access to in order to do their job, and sets them up accordingly.

Google Workspace offers [prebuilt admin](#) roles you can use when applicable, as well as giving Super Admins the option to customize admin roles based on the details of an employee's job.

Organizations will need to decide what level of access each role in the organization should have. The particulars will depend on how your business is set up, and how different job responsibilities are defined. In practice, a few of the main job titles that can benefit from some level of admin access include:

- **Helpdesk & Admin Assistants:** Helpdesk and admin assistants likely need enough administrative access to manage issues like resetting passwords, provisioning devices, and changing service settings and permissions. You want them to be able to handle basic IT issues without having to bother busy IT managers.
- **Security & Compliance Officers:** Security and compliance officers should be able to manage security settings for both individual accounts and groups, access audit logs to track possible security and compliance issues, and have the power to review and approve or deny requests for sensitive actions.
- **Departmental IT Leads:** Departmental IT leads will need to be able to manage onboarding and offboarding functions for new and departing employees, should be capable of setting permissions for groups and organizational units, and may need the ability to provision new devices and wipe or block devices and accounts for inactive users.

Use Role-Based Access Control (RBAC)

Once you've determined all the roles in your organization that need some level of administrative access, the next step is to clarify exactly how much access they need.

Role-based access control means defining what level of access employees need based on their job title or place in the organizational hierarchy. Using RBAC, you can set up administrative permissions for each role, rather than doing it for every single employee — making the process much more efficient.

If an employee moves to a new role within the company, their access level will automatically change based on what's needed in their new job. Meanwhile whoever takes over their old job will automatically gain the access levels needed for that position.

In day-to-day practice, often employees end up with a higher level of permissions than their job requires because it's easier. When high-level administrators are busy, letting employees help themselves can (temporarily, at least) seem like a better option than having to continually take action for them. But that opens the door to more risk.

The challenge of role-based access control (RBAC) is to find the just-right balance between the level of access they need to do their job effectively and efficiently, and to provide no permissions beyond that.

That may require taking the time to clearly define the responsibilities of each position within Google Workspace to start. Or if responsibilities in your organization are already clear, sit down with employees to better understand what their days look like, which Workspace tasks they regularly perform, and whether there are any access bottlenecks causing them problems now.

Use that information to set up designated admin accounts that match the needs of each role. By using role-based access, you only have to do this for particular roles and job titles once at a time, rather than doing it for every single user. But that doesn't necessarily mean it's a one and done process. Do periodically revisit and review the permissions of each administrator position to confirm that they still match the role's needs.

Common Mistakes to Avoid

By taking a thoughtful, strategic approach to administrator roles early on, you can avoid some of the common mistakes organizations make. Some of the main issues we see companies dealing with when it comes to administrative access are:

Giving Too Much Access:

If you care about security, you don't want anyone to have Drive access beyond what they need to do their job. This issue is common because it's easier to provide employees with more access than they need than it is to create a process for approvals and changes. Plus, it's all too easy to forget to reduce access levels when a person's role in the company changes, or to disable their account when they stop working with the company.

But allowing employees more access than they need creates more vulnerabilities for your organization and its data. And when former employees maintain their access due to administrative oversight, it's both a security issue and can cost your organization wasted money. Developing a process to clearly define role-based access levels and stick with them over time is crucial.

No Separation of Duties:

While you want to be careful not to have too many Super Admins — the more people with absolute access, the more risk opportunities there are — you also want to be cautious about not putting too much power in one person's hands. If you only have one Super Admin, if something happens to the employee or their account is compromised, you won't have good options for managing the situation. Make sure you have back-up options for every administrative and security responsibility, so you're not caught unprepared if something happens to your main administrator.



Chapter 3:

File Access & Permissions Architecture



File Access & Permissions Architecture

We're all familiar with the frustration of sitting down to review a file, only to see the dreaded "You Need Access" screen. Encounter it enough times, and you can understand why some employees overcorrect by defaulting to the most generous access option when setting permissions for a file or folder. But that's a choice that can have real consequences for the security of your business.

[Recent Metomic research](#) found that over 40% of files stored on Google Drive included sensitive information like employee contracts and passwords. Do you know what the number is at your organization? And more importantly, do you know who has access to those files?

If sensitive files make it into the wrong hands, the consequences can be big. You could face:

- **Data Leaks:** Data breaches are far too common, and extremely costly for brands. [IBM](#) puts the average cost at \$4.88 million. If your Drive files are vulnerable, you're not only putting yourself at risk of facing high costs. You could also make your employees and customers targets for identity theft.
- **Regulatory & Compliance Issues:** Even if you manage to dodge a data breach, you could find yourself on the wrong side of government regulations. Violating data protection laws like GDPR (General Data Protection Regulation) can lead to big fines or other legal consequences.
- **Reputation Damage:** If lax file security on your end leads to exposing employee and customer data, you'll lose the consumer trust you've worked to build. Your brand reputation will suffer, which could lead to diminished profits as well.

Those are fates you want to avoid. Developing clear standards around [Google Drive file access and permissions](#) can help.

Apply Principle of Least Privilege to Files

The principle of least privilege is straightforward: users should only have the level of access necessary to perform their job functions.

That sounds simple in theory, but can be hard to maintain in practice. Busy workers will often default to choosing the easiest option. When it comes to setting file access permissions, "easy" means making it available to everyone with one click — rather than clarifying the specific people who need access.

Getting employees to practice the principle of least access can be an uphill battle, but there are a few steps you can take to improve your odds:

Create, Distribute, & Enforce a Clear Policy

The first is making sure all employees clearly understand the principle of least privilege. They can't follow a rule they don't know about.

Create a short, clear policy that defines how employees should handle access permissions. Make sure the policy is clearly communicated to every employee — and not just during onboarding training or via a one-time email. Consider sending periodic reminders or storing the policy somewhere that employees will regularly see it.

And make sure managers understand to hold their employees to it. Any time they see folders and files being shared beyond the people who need access, they should address the issue with the employee.

Strategically Use Groups & Shared Drives

Managing permissions for every, single file can be tedious. Luckily, within Google Workspace, it's not necessary. You can set up access permissions at a higher level, using Groups to grant access to the relevant contacts for all files within a Shared Drive or folder.

That ensures everyone in the department or group gets access to the files they need in one fell swoop, rather than having to go file-by-file to set up those permissions. And each time a new file or folder is added, it will automatically grant access to the right people.

Apply Principle of Least Privilege to Files (cont.)

Audit Permissions Periodically

Admins can use audit logs to review who has access to which files. Set up a regular practice of reviewing those logs, to identify potential issues before they become problems. For files and folders that contain sensitive information especially, aim for frequent audits.

Automate Permissions Wherever Possible

When people are busy dealing with all the main responsibilities of their jobs, managing Google Drive access and permissions is the kind of thing that falls through the cracks. That's where automation can really make a difference.

You can automate permission updates based on factors like a change in job title, department, or employment status. When someone leaves, no one should have to go in and remove their access to every file and folder manually. Automation can handle the process more thoroughly, while reducing the time and work involved at the same time.



Organizing Drives & Folders

How you organize your Google Drives and folders impacts both security and usability. Good Drive organization can simplify the administrative work of handling permissions for files that contain sensitive data, while also making it easier for employees to find the information they need faster. A couple key considerations to keep in mind when organizing your Drives and folders are:

File Naming Conventions

Have you ever tried to pull up an old file, only to realize you can't remember what it was called or where it was saved? If the file went through a long revision process, you may face the extra challenge of trying to determine which of the files with similar names was the final one.

While Google Workspace's search features can often help you cut through all the noise and get to the specific file you need, establishing clear file naming conventions and encouraging all employees to use them consistently can work even better. File naming conventions usually include important information in the file name in a standardized way.

That could include:

- Content name
- Project name
- Client name
- Date created or most recently modified
- Type of modification

Naming conventions help you group relevant files together so employees can more efficiently find what they're looking for. They help you clarify which version of a file is the best and most recent. And they improve security by helping you avoid sharing the wrong file externally (e.g. If the client name is right there in the file name, you probably won't accidentally send the file to the wrong client).

Shared Drives vs My Drives

Managing permissions file-by-file is impractical in most organizations, which is why using Shared Drives and folders strategically is so valuable. Shared Drives can be useful for collaboration. You can set it so a specific group of people has access to the Shared Drive, simplifying access issues for all the files and folders within it.

But the dark side of Shared Drives is that they can introduce security risks. You want to place limits on when and how Shared Drives are used, to help you maintain security for all the files within them. Administrators have the option to prevent other users from creating Shared Drives in the Drive and Docs settings, and block managers from overriding those security settings.

Organizing Drives & Folders (cont.)

That can help security staff maintain control over how often they're being used, but you probably don't want to ban them outright. There are use cases where Shared Drives come in handy. Some points to keep in mind when considering whether a Shared Drive or individual My Drive is the best choice:

- **Long-Term File Access:** One of the big benefits of Shared Drives is that files are owned by the team rather than the individual. When an employee leaves, you don't risk losing access. You can ensure the company maintains important files and data in the midst of employee turnover.
- **Ease of Collaboration:** Shared Drives make it easy to provide access to files and folders to all relevant employees with minimal effort. For projects where multiple people need to work together, they can help you avoid that frustrating "You Need Access" screen that slows productivity down.
- **Centralized Data Storage:** A Shared Drive keeps all the files and data it contains in one centralized location, making it easier for employees to find the files they need and for administrators to manage it all.
- **Security Concerns:** If your Shared Drive settings are too lax, it can open up vulnerabilities letting outside users gain access to files that contain sensitive information.
- **Administrative Oversight:** Administrators have more control over a Shared Drive than an employee's individual drive. They can monitor, audit, and manage the files and folders, and control permissions and access.

There's a place for both options, you just want to be thoughtful in deciding when to use each.



Managing External Sharing

Caution about file sharing within your organization is important, but files shared outside your organization can pose an even bigger risk. Metomic's research found that 34.2% of Google Drive files are shared externally.

There's probably a good reason for some of those files to be shared with people outside your organization. When you work with contractors, agencies, and other third parties, some filesharing is inevitable. But chances are, some portion of the files currently shared externally shouldn't be.

There are two main ways to minimize external file sharing — and they're pretty similar to how you handle internal sharing permissions:

- **Employee Education:** Provide training about data security best practices and clear guidelines on when it's acceptable to share a file or folder externally. Include this information in the policy we discussed, make it part of new employee training, and send reminders to employees periodically.
- **Administrative Oversight:** Conduct regular audits to identify files and folders shared externally, confirm whether they should be restricted, and remove external access from users when needed.

You'll want to use both strategies to minimize risk, and you should treat both as an ongoing project. Even if you can get all external access issues cleaned up today, you'll inevitably face new ones in a few months if you don't stay on top of it.



Monitoring Shadow IT

Sometimes employees get frustrated with the limitations of the sanctioned technology products and turn to alternative options. While that may make their workload feel easier, it introduces new security risks for the organization.

This is called "shadow IT." It refers to any technology products or services that are implemented without the IT team's approval. And according to IBM, shadow data was involved in around a third of recent data breaches. That's a good reason to nip any shadow IT sources in the bud.

Shadow IT can be tricky to identify, because the whole point is employees do it outside the purview of the IT team. But employees often don't realize they're doing anything wrong, so sometimes you'll learn it's happening because they start opening support tickets for unsanctioned software.

When that happens, some gentle education can help bring them back into the fold and nudge them toward the approved tech products.

The best way to address shadow IT isn't reactively. It's proactively making the approved systems easy to use. Often when employees turn to shadow options, it's because something in the current system isn't working for them.

Creating a feedback loop, so that employees know you're open to their input and willing to implement their suggestions, can keep them from feeling like they need to go outside of the established tech systems.

That and, of course, employee education (a theme in this section). Employees need clear guidance into why the company chose the tech products you did, and why going outside of the sanctioned products is a problem. Make clear the risks involved, and encourage employees to come to you with their concerns so you can address them directly.

Chapter 4:

Security Settings & Guardrails

Human error is often the weak link in keeping business data and accounts safe. That's why Google Workspace provides a number of security settings to help you enforce better practices for protecting your company's sensitive data and user accounts.

But to take advantage of Workspace's security tools, you have to understand what they are and how to use them. This chapter will serve as a good primer to get started.

Account Security

Every user account added to your company's Google Workspace is a potential entry point for bad actors. But you can't practically reduce the number of accounts — your employees all need Workspace access to do their jobs. Instead of reducing exposure via the quantity of accounts, your best bet is to use the security tools available to minimize the risk of each account. In particular, you can:

Set Up Two-factor or Multi-factor Authentication (2FA/MFA) Enforcement

Multi-factor authentication adds an extra layer of security for your Google Workspace accounts. Workspace gives you the option to enforce MFA on all accounts, helping you significantly minimize weak links.

You can choose whether to allow "trusted devices," to reduce how often employees have to use MFA, which can hurt productivity (and cause annoyance) if it's required for every sign-in. But requiring MFA on new devices can help you nip suspicious access attempts in the bud.

Enforce Password Best Practices

If left to their own devices, a surprising number of people default to the easiest possible password. A Nordpass study found the most popular corporate password is 123456. Yikes.

While enabling MFA can reduce some of the danger of weak passwords, you're better off having two forms of security in play when it comes to account access. Within Google Workspace, administrators can configure settings that require all employees to create long, strong passwords (e.g. minimum 12 characters, must include a number and special character). You can also require employees to periodically change their password, and disable the option to reuse the same password within a set period of time.

Configure Session Length

Google automatically signs users out after two weeks, but you can choose to set custom session lengths for accounts. By periodically forcing a new login, you reduce the likelihood of an unauthorized person accessing your company's data on a device that's been used by an employee.

For users with access to sensitive data, custom session lengths can be as short as one hour. But you want to be thoughtful about balancing employee convenience with security — forcing a new login every hour makes it harder for them to do their job. Try to find the happy medium that ensures higher security without sacrificing user experience.

Suspicious Login Monitoring:

You can set up admin email alerts to let you know immediately about any suspicious login attempts, like an account signing in from an unusual location. You can also set up additional steps for users to take if their log-in activity looks suspicious, such as requiring additional verification by phone or email.

Data Security

With how common and costly data breaches are, data security has to be a top concern at every organization. And if fear of a data breach wasn't enough of a reason to institute strong [data security practices](#), legal regulations often require it.

Google Workspace provides a few valuable features to help you reduce the risk of your data falling into the wrong hands:

DLP (Data Loss Prevention)

You can set up DLP rules that trigger a scan of files before they're shared externally. If the scan finds sensitive data, the user will be forbidden from sharing the file without taking additional steps, giving your admins a chance to review the situation and confirm whether the sharing is legitimate.

Context-Aware Access

Administrators can also set limitations on account access based on contextual attributes like user identity, location, device security status, and IP address. Proactively blocking sign-ins from a suspicious looking location or device — or at least adding extra barriers to access — can help you keep hackers or other bad actors from gaining access to sensitive data. Context-aware access controls are granular enough to let you prevent access from any devices that weren't issued by the company, as well as any that lack proper encryption.

Trusted Domains

We've established that there are scenarios when external sharing is necessary, but it always requires extra caution. Google Workspace lets you establish trusted domains and define sharing settings for each one. You can restrict sharing options for all other external users, but simplify sharing with the specific organizations outside of your business that are on your trusted list. This can be useful for when you work with third parties that need access to sensitive data, like an HR or accounting firm.

Device Security

With the growth of remote work, employees working from multiple devices has become a norm. Employees now use an [average of 2.5 devices](#) for work. And 36% use both work-issued and personal devices to get work done.

That may be good for productivity, but it makes [device management](#) a more complicated and essential aspect of Google Workspace security. Google Workspace provides a few options for improving device security you can take advantage of:

- **ChromeOS Management:** If your company issues ChromeOS devices like Chromebooks, you can manage security settings for them within the Admin console. You can install apps and extensions, connect the devices to your VPN and WiFi networks, and enforce a range of corporate policies about their usage. That includes allowing or blocking certain apps and websites, enforcing privacy policies, and managing Chrome auto-updates.
- **Endpoint Verification:** Google offers Endpoint Management features for administrators that give you a centralized way to configure security settings and set up necessary apps across your employee devices. In the management console, you can monitor and enforce security policies on each device. And when needed, you can wipe devices remotely to reduce risk in the event of loss or theft.
- **MDM (Mobile Device Manager):** Google allows administrators to practice unified mobile device management within the Google Admin Console. It works not only with ChromeOS mobile devices, but also Android and iOS, so you gain a comprehensive tool for deploying necessary apps, securing sensitive data, and enforcing device policies across a diverse fleet of mobile devices.



Shadow IT Prevention

We already covered some of the dangers of shadow IT, but one of the most insidious ways it can creep up on you is when employees connect to third-party apps with their Workspace accounts.

You've probably noticed when researching a new app how often you get the option to sign into it using your Google account. That's OAuth — a feature of Google Workspace Identity Management. It lets users connect their Workspace account to a third-party app without sharing their password. But if users aren't careful, they could end up granting the app access to sensitive data from within their Workspace account without realizing it.

Administrators have two ways to address this:

- **Block Risky Apps:** The default setting in Google Workspace is to let users download any app they choose. You can change that setting by setting up a blocklist of apps that you've identified come with risks, along with a whitelist of curated apps you trust. Employees may be annoyed when they see an app they want is blocked, but if you can direct them to a comparable option on the whitelist, they can gain the functionality they need without putting your organization at risk.
- **Monitor OAuth Usage:** OAuth lets employees connect compatible apps to their Workspace account, which gives you insight into what apps they're using. When an employee tries to access a service the IT team hasn't approved, you can get in touch to point them toward a better alternative. That helps keep your data safer, while helping employees find the tools they need to do their jobs efficiently.



Chapter 5:

Onboarding, Offboarding & Lifecycle Management

The day-to-day work of managing Google Workspace securely is important. But some of the moments when the administrative side of using Workspace matters most are when you're dealing with big changes: when new hires come on board, when former employees leave, and when current workers move roles within the organization.

Handling each of these employee lifecycle moments quickly and effectively is key to keeping your business Workspace secure and ensuring employees can do their jobs without unnecessary delay.

Why Lifecycle Management is Critical

[Google Workspace lifecycle management](#) often involves work that can feel tedious for IT and administrative staff, but getting it right is crucial for a few main reasons:

Ensure Appropriate Access Levels for All Employees

Employees can't do their jobs without access to the right accounts and files, but too much access creates security vulnerabilities. A good process for managing each stage of lifecycle management can help you efficiently stay on top of access issues.

Avoid Orphaned Accounts

When people leave the organization, you don't want their accounts to outlive their tenure there. If an account still has access to sensitive data past the point when a person is using it, it becomes a prime target for hackers. Reducing (or better, eliminating) the number of orphaned accounts linked to your organization's Google Workspace helps you reduce risk exposure.

Prevent License Waste

You only want to pay for products you use. If your team is slow to decommission unused accounts when employees leave, you'll be stuck paying for them in the interim. That's wasted money that could be put to much better use in your business.

Enable Efficiency

The longer employees spend waiting for access to the accounts and files they need to do their job, the more it hurts overall productivity. When your IT team can handle onboarding, offboarding, and mid-lifecycle changes quickly and seamlessly, it boosts efficiency throughout the organization.



Onboarding Best Practices

Have you ever shown up to a new job, ready to dive right into work, only to spend the first few days sitting around waiting for all your accounts and training materials to be ready? Every day a new employee spends waiting rather than working costs your organization money (and the employee their patience). But you don't want to rush the work of onboarding to the point where errors are made.

Effective onboarding processes often involve using automation to cut down on both the amount of time your administrative team has to spend, as well as the number of errors likely to occur. Google Workspace includes a few features to help get new hires set up right:

Role-Based Templates

You can create templates for specific roles in the Admin Console that contain all the standard settings, license, security policies and access permissions that an employee in that role will need. Each time you set up a new user account, you can use the template appropriate to their role to speed up the process, while minimizing your odds of forgetting to include something they need.

Automated Group Assignments

Another way to simplify the setup process is to use Google Groups. When you set up certain permissions at the group level, all you have to do is add new hires to the appropriate groups to ensure they can access all the team drives, folders, and files covered under the group settings.

Drive Access

You can also set up templated folders and files in their Drive that include all the onboarding materials they need. Create an "Onboarding" folder for each type of role that includes training materials, access information, contact lists, the employee handbook, and any other information they need. Load it to their Drive, and they'll have easy access to all the basic information they need to get started on day one.

Offboarding Best Practices

A solid onboarding process is crucial for getting employees started right, but a good offboarding process protects your company's security exposure. Managing offboarding correctly includes:

Timely Account Suspension

If a disgruntled former employee maintains access to all their files and folders after leaving the company, they could potentially cause big problems for your organization. Automating your offboarding process can help the IT team stay on top of account suspensions, so you address security gaps before they have the chance to become a problem.

Data Transfer

An employee's departure brings the risk of data loss. You don't want to lose access to all the files they owned, especially any that include important information the rest of the team needs to do their jobs properly. Data transfer should be a standard part of the offboarding process to ensure the company keeps access to all necessary documents, and the right employee is able to seamlessly step in to manage them. Google offers a Drive Transfer tool that lets admins change ownership of files in bulk, either to another single user in the company or a Shared Drive that makes the documents accessible to everyone in a group or department.

License Reclamation

Another important reason to deactivate old accounts quickly is license costs. You don't want to pay for licenses you're not using. Instead, you can re-assign the old employee's license to their replacement and make sure you're only spending as much money as you need to.



Chapter 6:

Reporting, Auditing & Compliance

Administrators need a way to see what's happening in the larger organization. And the bigger your business is, the harder it becomes to stay on top of what everyone is doing.

The reports Google Workspace produces are a powerful way to identify trends in how employees are using Workspace, spot potential security issues before they become a problem, and make sure the organization stays compliant with all relevant laws and regulations.

Why Reporting Matters

The reporting features in Google Workspace aren't just nice to have, they're essential. In particular, reports help you achieve:

Visibility

Workspace reports help you track user behavior that impacts security like how many users have MFA set up, are using secure passwords, and any external apps they've installed. You can also get a snapshot of usage trends like Drive logins, mobile device usage, and who's viewing, editing, and sharing files.

Compliance Evidence

Compliance is no longer just for regulated industries. All businesses need to be aware of data regulations and the steps you need to take to stay on the right side of the law. Workspace's reporting features help you meet compliance requirements by tracking information about user activities, app usage, and security incidents.

You can set up alerts to know right away when an employee tries to share sensitive data like SSNs (social security numbers) externally, track the permissions and settings and access logs for files and folders, and monitor when employees use shadow apps that lack your stringent security requirements.

All that helps your security and compliance officers stay in the know about any compliance issues that should be addressed.

Proactive Monitoring

In addition to helping reduce security risks, monitoring employee activity can help you understand usage trends in order to optimize resource allocation. It helps you identify gaps in employee training on how to use the products, and identify opportunities for support resources that improve productivity and collaboration.

The more you know, the more you can take action to improve how your organization is using and benefiting from Google Workspace.

Key Reports Every Admin Should Run

There are a lot of different reports you can run in Google Workspace — and that includes pre-built reports Workspace assumes businesses will want, along with the option to create custom reports based on your organization's priorities. Amongst the many valuable reports, a few are especially essential to any organization concerned about security:

External File Shares

You can capture detailed data on how many of your organization's files, folders, and Drives have been shared externally. This is useful both for identifying specific shares that present security risks and need to be locked down, but also for getting a snapshot of what the sharing habits are for employees in your organization. If you notice people being especially lax about how often they share files externally, it may be a sign that it's time for a training refresher or to enlist managers to help with enforcement.

Dormant Accounts

You can use reports to view user account status across the organization, to confirm if all current accounts are active. If there are dormant accounts that failed to be deactivated after an employee left the business, or because someone's out on sabbatical, you can spot them and suspend the account or delete it, as the case requires.

App Usage & OAuth Activity

You can run reports to see how many external app installations employees have made, along with which apps they're using. This is important for spotting shadow IT issues that may pose a risk to your organization's data security and compliance.

License Utilization

Finally, you can keep track of the number of licenses purchased, assigned, and used within your company. If there are unused licenses that you're paying for, recognizing that saves you money.

Chapter 7:

How gPanel Optimizes Your Admin Environment

It's clear from all the previous chapters that you can do a lot from within Google Workspace. The tool has native features that aid in keeping your employees productive and your [business data secure](#). But as good as Google Workspace is (and it is very good), there are [certain features and functions](#) within it that can be enhanced by using the [Google Workspace management tool, gPanel](#).

After working alongside IT administrators using Google Workspace for years, [Promevo](#) saw an opportunity to develop [features](#) that make managing the tool easier and more secure. As such, the product was designed with your needs top of mind.

In practice, that means gPanel offers the following benefits.

Greater Ease of Use

While Google Workspace offers a lot of functionality, some features are hard to use efficiently. With gPanel, you get:

A Single, Centralized Interface

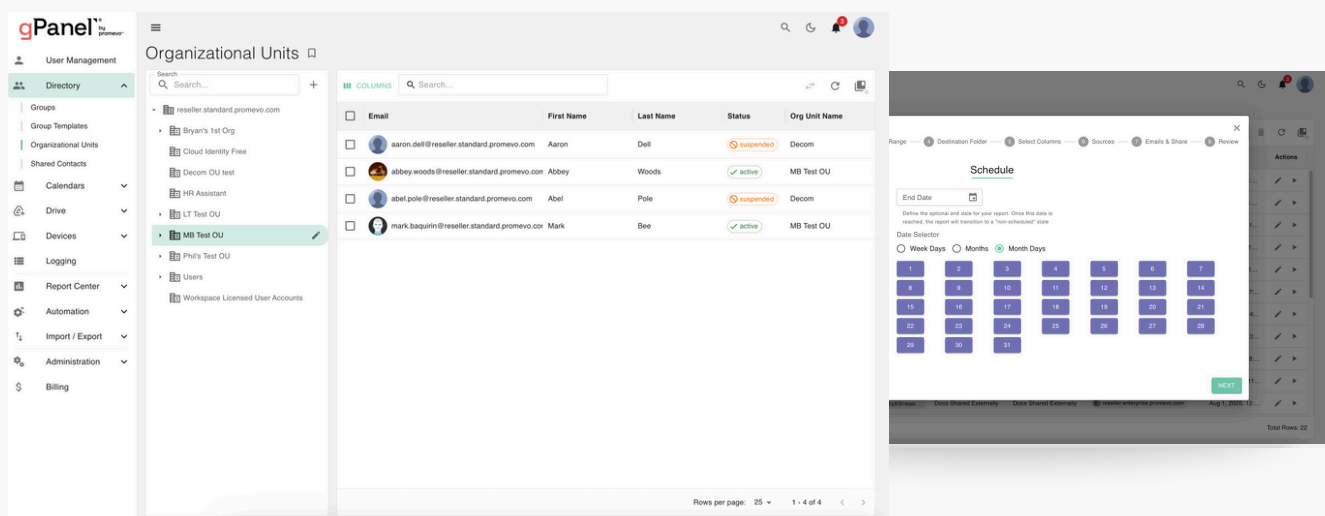
You can manage all your users, groups, data, and security settings in one centralized, intuitive interface. No more switching between multiple Google Admin console menus to handle basic tasks.

More Automation Options

gPanel lets you automate the creation and management of user accounts, batch-create users, set up automated workflows, and automate your offboarding process. Enterprise users can set up custom workflow automations using the Rules Engine and API, which also lets you connect your Workspace to your HRIS (human resources information system), ERP (enterprise resource planning), and CRM (customer relationship management) systems for more unified data.

More Powerful Search

The time employees spend digging for the file or report they need is time they're not spending on more important work tasks. gPanel offers more powerful search functions to make finding the right file, user, folder — whatever you need — faster.



More Control

gPanel also goes beyond the features available in Google Workspace when it comes to the amount of control admins have over their environment and workflows. In particular, gPanel's features enable:

More Granular Permissions

You can assign more specific access controls for each user and role, allowing you to meet more complex security and workflow needs. You can also make bulk changes to OUs, groups, and individuals to manage permissions more efficiently. And setting up delegated admin capabilities lets you offer the precise amount of access each admin needs, without increasing vulnerabilities by providing too much.

More Advanced Reporting

Generate detailed logs for compliance audits, as well as reports on user activity trends, storage usage, collaboration patterns, and security issues. Comprehensive reports help you better identify trends, cut down on external shares for security, maintain compliance, and make data-driven decisions.

More Powerful Device Management

gPanel gives you the means to remotely access essential details about your organization's mobile and ChromeOS devices, such as status, last sync, last location, and external apps installed. You also have the power to remotely wipe employee devices in the case of theft or loss.

The screenshot displays the gPanel Role Manager interface. On the left is a sidebar with navigation options: User Management, Directory, Calendars, Drive, Devices, Logging, Report Center, Automation, Import / Export, and Administration (highlighted). The main area is titled 'Role Manager' and contains a table of roles. The table has columns for Created Date, Role Name, Role Type, Is Default, Description, and Actions. Two roles are listed: 'Admin' and 'User'. A modal window is open on the right, titled 'Basic Info', showing options for report type and name, and checkboxes for 'Manual Run', 'Set Schedule', and 'Run Without Saving'.

Created Date	Role Name	Role Type	Is Default	Description	Actions
N/A	Admin	Admin	✓	This is the Admin Role. It has access to the entire application. It cannot be deleted.	
N/A	User	User	✓	This is the User Role. Any user not explicitly assigned a role will have this role. It cannot be ...	
7/15/2025, 10:56:44 AM	asdkjaskdktjdsaf	Admin	✗		
7/9/2025, 3:16:18 PM	asdfasdfsaf	Admin	✗		
6/6/2025, 12:22:15 PM	asdfasdfsaf	Admin	✗		
7/18/2025, 1:48:54 PM	asdkjaskdktjdsaf	Admin	✗		
7/18/2025, 11:45:55 AM	asdfasdfsafasdfsaf	Admin	✗		
6/11/2025, 1:19:08 PM	Calendar Role	Admin	✗		
5/14/2025, 12:44:52 PM	Change Log Demo	Admin	✗	Every action requires a change log	
1/10/2024, 3:31:09 PM	custom role 1	Admin	✗		
3/11/2025, 12:21:36 PM	gPanel Contact List	Admin	✗		
7/8/2025, 1:15:49 PM	highschool 1	Admin	✗		

What Customers Are Saying



"[In the Admin console], you can only search for drives and files by name. You can't search by the URL, you can't search by the file ID — anything like that. You can only search by the file name...Whereas with gPanel, there are a bunch of available search fields. So it makes the process [of finding files] a lot faster and a lot less frustrating."

- Liz Mitchell, Google Workspace Communications & Training Lead at [Trimble](#)



"The reporting provided through gPanel Report Center allows for quick review of many aspects of SiLo's Google environment. These reports surface data that, without gPanel, you could only access through a manual audit of the Google Admin console."

-Adam Eagle,
Business Operations Manager at [SiLo](#)



"With a small IT team, Promevo [and gPanel] allowed us to securely share Google administration across multiple IT staff members. We are able to resolve user account issues more quickly while managing tight access controls to the Google domain."

- Scott Krajewski,
Associate Vice President for IT at [Augsburg University](#)



Go Further with gPanel

Google Workspace is a powerful suite of business tools to help your organization run more efficiently, enable collaboration, and maintain security. But it has its limitations.

Using Workspace in tandem with gPanel gives you more control over your workspace, better options for security and compliance, and equips employees with features that can boost efficiency. See what gPanel can do for you with a [personalized demo](#).

