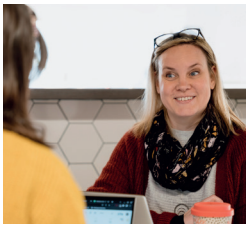
Unmanaged Users

How much control do you really have over your data?



Visit: **cts.co** Email: **hello@cts.co**

SPECIALIZATION
Work Transformation Enterprise
Google Cloud

Contents

What are unmanaged users?

Whether your business has consciously deployed Google Workspace and Google Cloud or not, it's almost guaranteed that some of your employees will be using a Google Account to get certain aspects of their jobs done. The reason? Many common services that are now considered essential require it.

For example; the Marketing department using Google Analytics or Google's marketing suite will need a Google Account to access these services. Anyone publishing on YouTube will need an account. Anyone with an Android device will have created a Google Account to get apps, updates and navigation. There may also be projects created on Google Cloud using services like virtual machines, databases and Maps Platform. In many cases your teams will, quite reasonably, use their work email as the address for their Google Account.

These accounts are technically considered by Google to be personal accounts, despite having a company email address, as they were created by the individual and not issued to them by your business.

This means you could have business data residing in personal accounts over which you have no right of access, and crucially - no control. This restricts your ability to have a consolidated view across all of your company data. Additionally, when someone leaves your organisation you will have difficulty correctly identifying their accounts and removing access, permanently.

With GDPR compliance being enforced aggressively across Europe, coupled with a risk of fines of up to 2% of a company's entire global yearly turnover, it's never been more important to protect your data.

For this reason it's vital to identify cases where "unmanaged user" accounts exist, and gain control of the situation. You can then put measures in place to prevent any further creation of unmanaged accounts.

How do you know if your organisation has unmanaged accounts?

You may not realise there are Unmanaged users operating in your business. Here are some points to help you identify where you might be running the risk.

- Does your team use Google Analytics?
- Does your team leverage Google's paid advertising services?
- Does your team publish content on YouTube?
- Do any of your employees have Android devices?
- Is Google Chrome used within the business? Keep in mind what employees may be using when working remotely or from personal devices.
- Do you have partners that share Google Drive and Workspace (G Suite) documents with you?
- Is your business profile and company details visible via Google Search?
- Do your teams use any third party applications where they sign in with Google? e.g. Dropbox, LinkedIn
- Has anyone in the organisation signed up for a Google Account for their own collaboration/ communication reasons, using a work email address?

If you've answered yes to any of the questions above, and you've not already established controls over Google Account creation, then your organisation will have unmanaged Google Accounts in use.

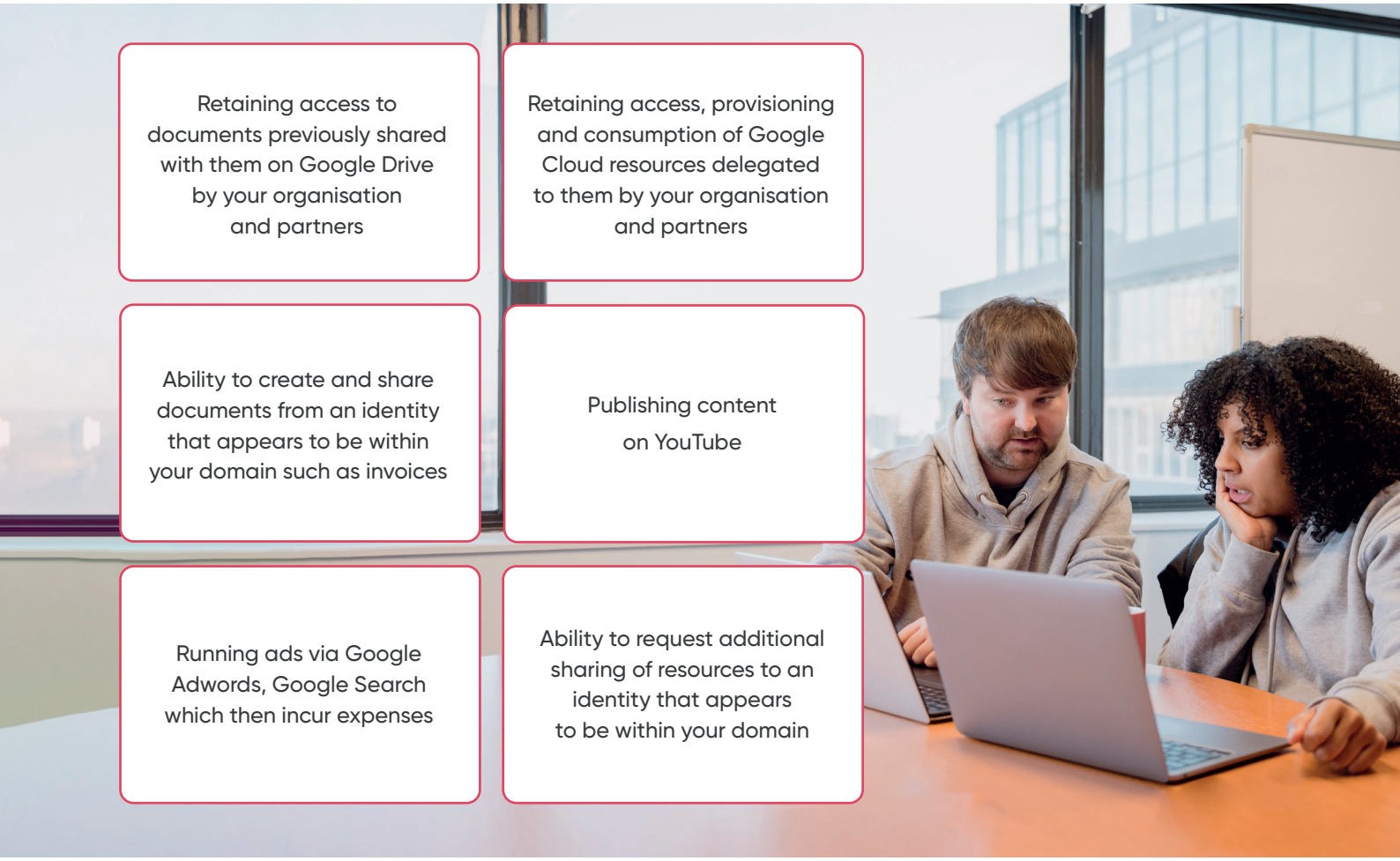
The risk to your business

If you have unmanaged users, then this can pose a number of serious security risks for your business including:

Data leakage
Lack of control over access to your data, increasing the risk of unauthorised access.

Malicious use of services
Employees who previously created personal accounts and have since left the business, are still able to act on behalf of the business using their personal Google Account.

This can include:



- Retaining access to documents previously shared with them on Google Drive by your organisation and partners
- Retaining access, provisioning and consumption of Google Cloud resources delegated to them by your organisation and partners
- Ability to create and share documents from an identity that appears to be within your domain such as invoices
- Publishing content on YouTube
- Running ads via Google Adwords, Google Search which then incur expenses
- Ability to request additional sharing of resources to an identity that appears to be within your domain

If you've answered yes to any of the questions above, and you've not already established controls over Google Account creation, then your organisation will have unmanaged Google Accounts in use.

No controls over Google verification for 3rd Parties

Use of Google verification for login to third party applications is not controlled for unmanaged accounts. In contrast, Google verification against 3rd party services can be controlled for managed accounts.

No guaranteed service levels

Google offers 99.999% uptime and technical support for Google Drive when purchased as a business account. Unmanaged users are not entitled to availability and support services.

Unmanaged accounts are not controlled by Joiners, Movers and Leavers processes

Unmanaged accounts cannot be controlled by your Joiners, Movers and Leavers processes. Managed accounts can be controlled by these processes and can also be synced with your identity provider to provide efficient and consistent integration.

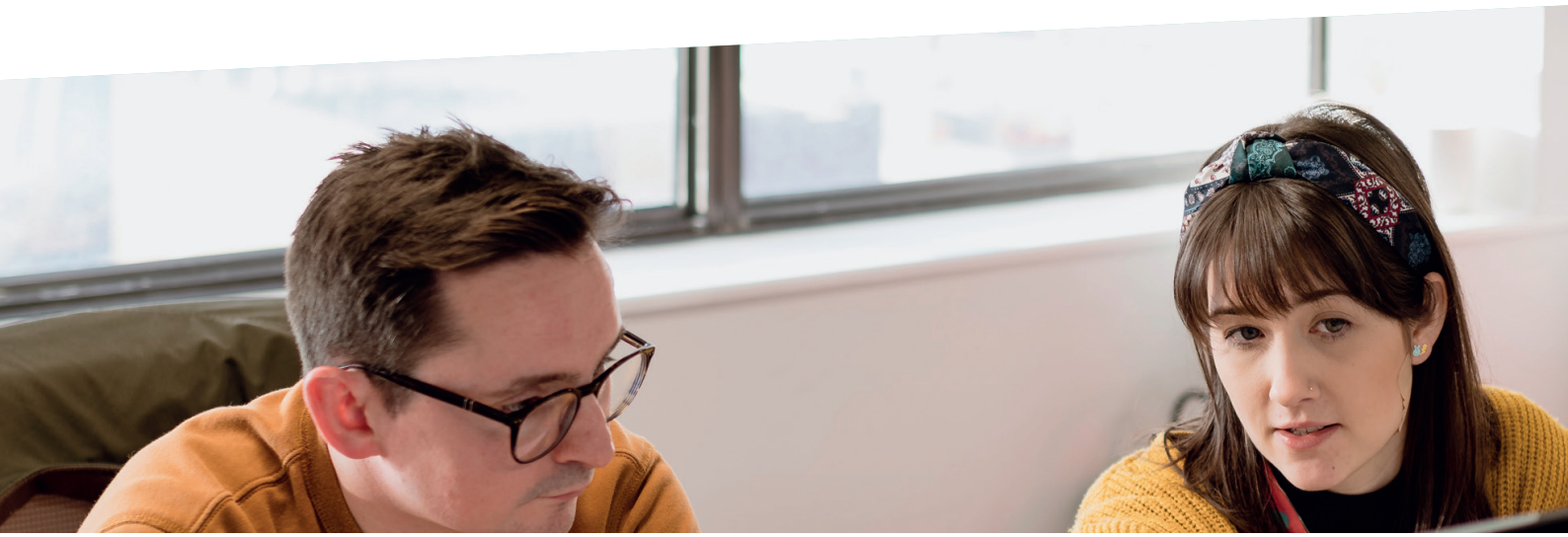
No audit log or accountability for access

Companies who have issued their employees with Workspace accounts have access to data logs for these accounts, with admins being able to control this access. Unmanaged account activity is not included in these logs. In the event that your company ever requires evidence of previous activity, or wants to govern certain behaviours such as sharing private information, this would not be possible for any of your unmanaged accounts.

Authentication and credentials policies are not enforceable

Policies for setting password complexity and expiry are not enforced for unmanaged accounts - it's up to the consumer to decide what credentials they set. Conversely, with managed accounts, businesses are able to set policies for these credentials.

If you require employees to have single sign-on (SSO) across all applications for increased security, their unmanaged account would be outside the SSO scope so they would need to use a separate password. Certain insurance policies, such as those around data protection, demand certain levels of security for end users. Therefore you're at risk of not being covered, should you have unmanaged users in your organisation.



How do you gain control of these unmanaged accounts, and prevent additional accounts from being created in the future?

The only way to gain full control of these accounts is for you or a Google Partner to set up a Google "Tenancy" for your domain and provision managed accounts (free and paid for options are available). This means you'll own, have visibility, and be in full control of your data.

Where to start

1. You'll need to get a clear view of who is using Google Accounts to complete their daily tasks. Marketing is a good place to start as this team may already be using Google Analytics, followed by cataloguing who has been issued Android devices.

2. You should also review your remote working environment, to get a sense of whether employees are using Chrome, if this isn't the primary browser used by the organisation.

3. Once you have identified the potential use cases in your business, and set up a Google Tenancy for your domain then you or a Google partner can survey the unmanaged accounts which use your organisation's email addresses. Each unmanaged account will need to be transitioned into a managed Google Account. This involves sending a notification to each unmanaged user, requiring them to confirm the move from their personal account to your organisation's managed account.

Act now, with the help of CTS, to secure your business

Whilst there is some administration required in this process, the risk far outweighs any efforts, and as a Google Partner, we can manage a large proportion of the workload for you.

The more time that passes with unmanaged accounts operating in the business, the larger the risk becomes. You'll be increasing the amount of activity running through these accounts, increasing the number of employees leaving the business with full control of this data, and increasing the likelihood for more unmanaged accounts to be created.

The good news? Now that you are aware, you can act, and work towards the highest level of security for your business.

Want to start securing your Google users?
Reach out to the award-winning Google Workspacespecialists at CTS

Get in touch

About the author

Steve Franks is a Senior Cloud Consultant at CTS, specialising in Google Workspace and began his career in the leisure industry, where he spent over 10 years implementing cloud migration projects at The Bannatyne Group. His experience includes delivering Cloud initiatives across several key industries such as retail and finance and he is now helping organisations design and deliver digital workplace transformation initiatives at CTS.

About CTS

CTS is proud to be the largest dedicated Google Cloud partner in Europe, helping customers to differentiate by adopting not just Google Cloud technology, but also their culture of innovation and sustainability. CTS works with organisations to modernise their technology stack, providing consultancy, implementation, billing and managed services for both Google Cloud Platform (GCP) and Workspace.

Google Cloud Partner
Managed Service Provider