Small business Google Chromebook and ChromeOS security guide

cyber.gov.au

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre

chromebook

This publication was developed by the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) with technical input from Chrome Engineering.

Table of contents

Introduction

ChromeOS is a Linux-based operating system that Google has built using the open-source ChromiumOS project. It is best known as the operating system used by Chromebooks, but can also be installed on Personal Computers (PCs) and Macs (in the form of ChromeOS Flex).

ChromeOS has a unique design that mitigates a range of cyber threats, with many of its cyber security measures working out-of-the-box with little or no configuration required. This makes ChromeOS relatively easy to secure for small businesses and enterprises with limited cyber security expertise or resources.

This guidance summarises some notable characteristics of ChromeOS' approach to cyber security and outlines how small businesses and enterprises can establish a secure information technology (IT) environment using ChromeOS.

Is this guidance right for you?

This guidance is a good starting point for small businesses and enterprises that use ChromeOS or ChromeOS Flex (it is not designed for devices running ChromeOS Kiosk). The guidance is not prescriptive or exhaustive. It offers one example of how ChromeOS can be securely configured. All small businesses and enterprises should implement cyber security measures that are proportionate to their risk profile and risk appetite.

This guidance is designed to be accessible to small businesses and enterprises with limited cyber security expertise or resources. Anyone who is comfortable using an online administration (admin) portal should be able to implement the guidance in two to three hours. The guidance does not need to be implemented all at once, it is presented in sections that can be implemented independently. Start by implementing the 'setup steps,' then implement the 'critical step', then finish with the 'next steps'. Google's Workspace administrator learning path provides a helpful series of short courses for administrators that are interested in further training.

Small businesses and enterprises should undertake their own assessments to determine which operating systems best meet their needs. ChromeOS is well suited for small businesses and enterprises that need a platform simply to browse the web and access web-based applications. Desktop applications are not the primary focus of ChromeOS, however, ChromeOS can run many Android and Linux apps as well as virtualisation software. Note, not all desktop applications can run on ChromeOS. If your small business or enterprise relies on any desktop applications, consider testing them on ChromeOS before you commit to incorporating ChromeOS into your IT environment.

ChromeOS and cyber security

Application control

ChromeOS makes it relatively easy for small businesses and enterprises to control which apps and browser extensions are allowed on their devices. Applying ChromeOS' application control features, via the Google Admin console, reduces the risk that users may accidentally install a malicious app or browser extension.

Automatic updates

Updates are one of the most effective ways to keep devices secure. ChromeOS updates automatically by default, as do any apps installed on ChromeOS devices from the Google Play store. (Note that the Google Play store is not available on ChromeOS Flex).

Cloud-first

In every operating system, there are aspects of security that the vendor is responsible for and aspects that the customer is responsible for. In comparison to other operating systems, ChromeOS places a smaller burden on the customer and a greater burden on the vendor. An important reason for this is that ChromeOS is largely a cloud-based operating system. This means that a significant proportion of the data, apps and settings are cloud based, where they are protected by Google (and any other cloud vendors that are used).

Read-only root file system

The root file system contains the files and directories that are critical for system operation. Since these files and directories are read-only on ChromeOS, they are protected from being altered or infected with malware.

Restrictions on executables

In general, ChromeOS does not allow users to execute files they have downloaded to their devices. This measure removes a common avenue for malware infections that is present in other operating systems. However, small businesses and enterprises can choose to enable the ChromeOS Linux development environment which allows users to execute files, but only in a contained development environment.

Sandboxes

Sandboxes are heavily restricted environments that are designed to isolate certain processes from the rest of a device in case something goes wrong. ChromeOS uses sandboxes extensively, for example, apps from the Google Play store all run in their own sandboxes, as do the ChromeOS Linux development environment and websites accessed through the Chrome web browser. This means that if a user visits a malicious website, or installs a malicious app, there are cyber security measures in place to stop the problem from spreading. While these are important, they do have their limits, for example, they would not necessarily stop an app from misusing legitimately granted privileges.

Verified Boot

ChromeOS detects if devices have been tampered with at boot via a feature known as 'Verified Boot'. Verified Boot works by checking that the firmware, kernel, operating system and Chrome web browser exactly match the image approved by Google. If any evidence of tampering is detected, devices reboot with a backup image. Verified boot does not apply to ChromeOS Flex or Chromebooks that have been placed in developer mode.

Threats to ChromeOS

ChromeOS has been designed to protect against many common cyber threats, however, it is certainly not immune to compromise. Some threats that are applicable to small business ChromeOS users include:

- compromise of Google account credentials
- phishing and other social engineering attacks
- malicious websites, browser extensions and Google Play Store apps.

Resourcing considerations

Protecting your small business or enterprise from cyber security incidents will require an investment of time, money and expertise. This investment should be a priority as investing in preventative measures is typically far less expensive than responding to a cyber security incident. As such, securing your ChromeOS devices will require a resourcing commitment from your staff or IT managed service provider.

How this guidance relates to the Essential Eight

This guidance applies the principles of the Essential Eight to ChromeOS, however, it should not be considered an Essential Eight implementation guide.

The Essential Eight has been designed to protect organisations' internet-connected information technology. The Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) advises against attempting to apply the Essential Eight directly to ChromeOS and instead recommends implementing guidance that is designed for this operating system, such as this guidance.

ChromeOS has a different design to Microsoft Windows. As a result, certain Essential Eight mitigations are less relevant to ChromeOS, or require a different approach to implement. For example, the 'restrict Microsoft Office macros' mitigation strategy does not apply to ChromeOS because Microsoft Office macros do not run in Microsoft Office for the web.

Implementing guidance that is designed for ChromeOS ensures that your small business or enterprise is protected against the cyber threats that are most relevant to ChromeOS and takes advantage of the security features that are unique to this operating system.

Before you begin

Create a Google Workspace account for your small business or enterprise, if you have not already done so. As part of the Google Workspace setup process, Google will guide you through the steps to verify a domain your small business or enterprise owns, or register a new domain.

Follow Google's steps to enrol all your devices. Many of the policies you configure in this guidance will only apply to enrolled devices.

Many of Google's security features are enabled by default. This guidance assumes that any setting not addressed is left in its default configuration. Before you change any default settings that are not addressed in this guidance, consider if doing so will have any security implications.

Securing ChromeOS

Set up steps

- Set up organisational units
- Set up admin and standard user accounts

Critical step

- Configure multi-factor authentication settings

Next steps

- Configure password settings
- Configure user and web browser settings
- Configure device settings
- Configure app settings
- Configure backups

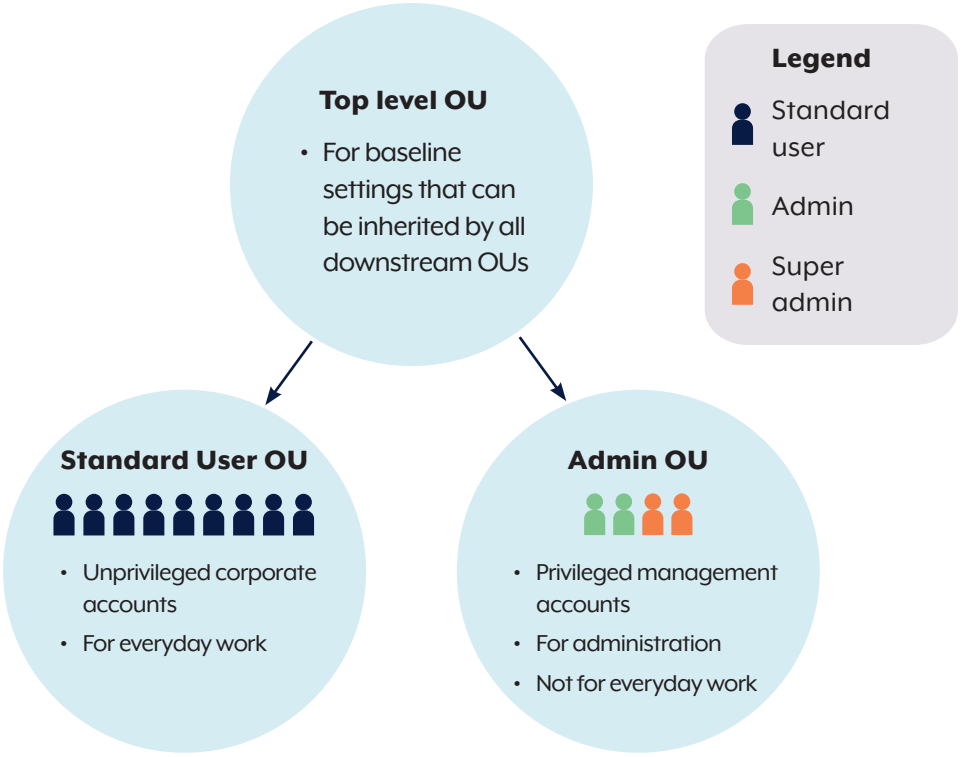
Set up organisational units

Organisational units (OU) allow you to apply different settings to groups of users or devices to ensure they only have the apps, data and privileges they need to do their job. If you are familiar with Microsoft Entra, you can consider Google organisational units as similar to Entra groups. Google has published guidance on how organisational units work and how you can set them up.

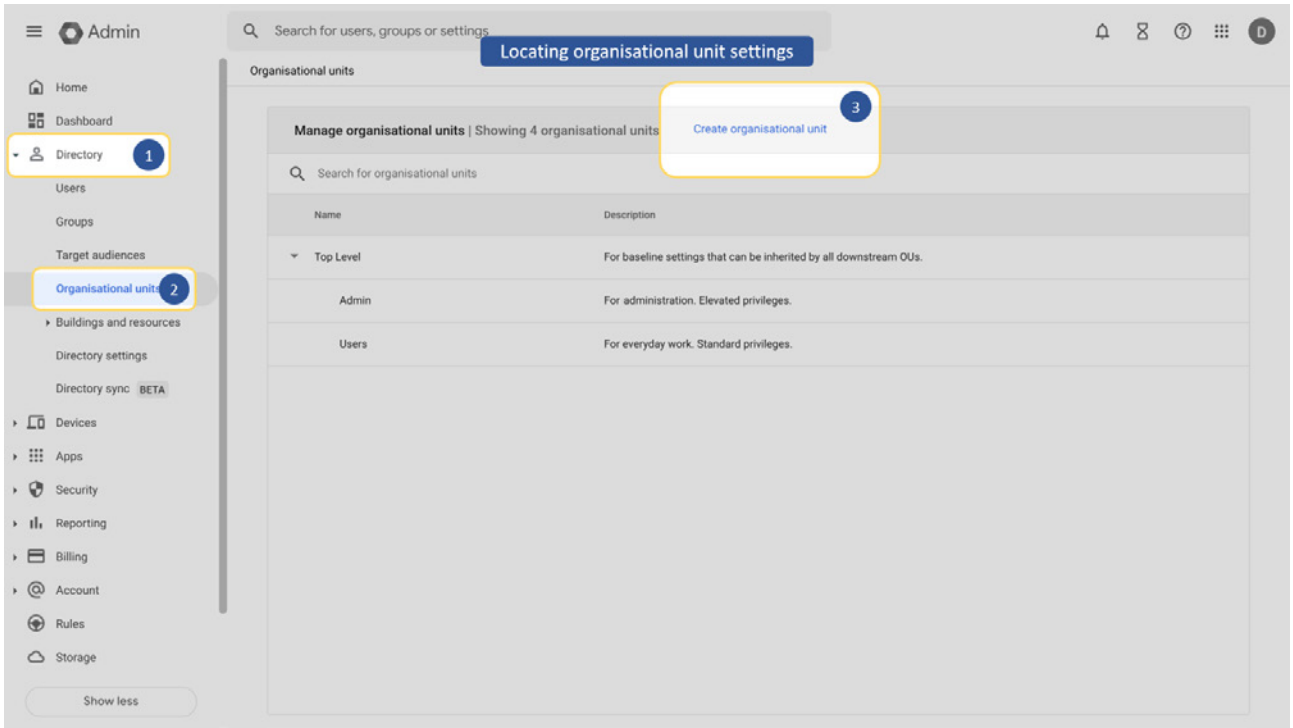
Organisational units are set up in a hierarchy with parent-child relationships. Settings that are not configured in a child organisational unit are inherited from the parent. Settings that are configured in a child organisational unit override the parent.

Your top-level organisational unit should have fewer privileges. Special privileges should be reserved for child organisational units so that they can be targeted at users that need them.

This guidance uses a simple organisational unit structure which includes a top-level organisational unit and two child organisational units, one for standard users and one for admins (as shown below). While this guidance uses an example organisation unit structure, you should establish a hierarchy of organisational units that best meets your own needs. For example, if your small business or enterprise has high contractor turnover, you may want to mitigate this risk by creating a contractor organisational unit with more restricted privileges. Alternatively, if your business has a team of developers you may want to create an organisational unit that grants them access to developer tools and apps.



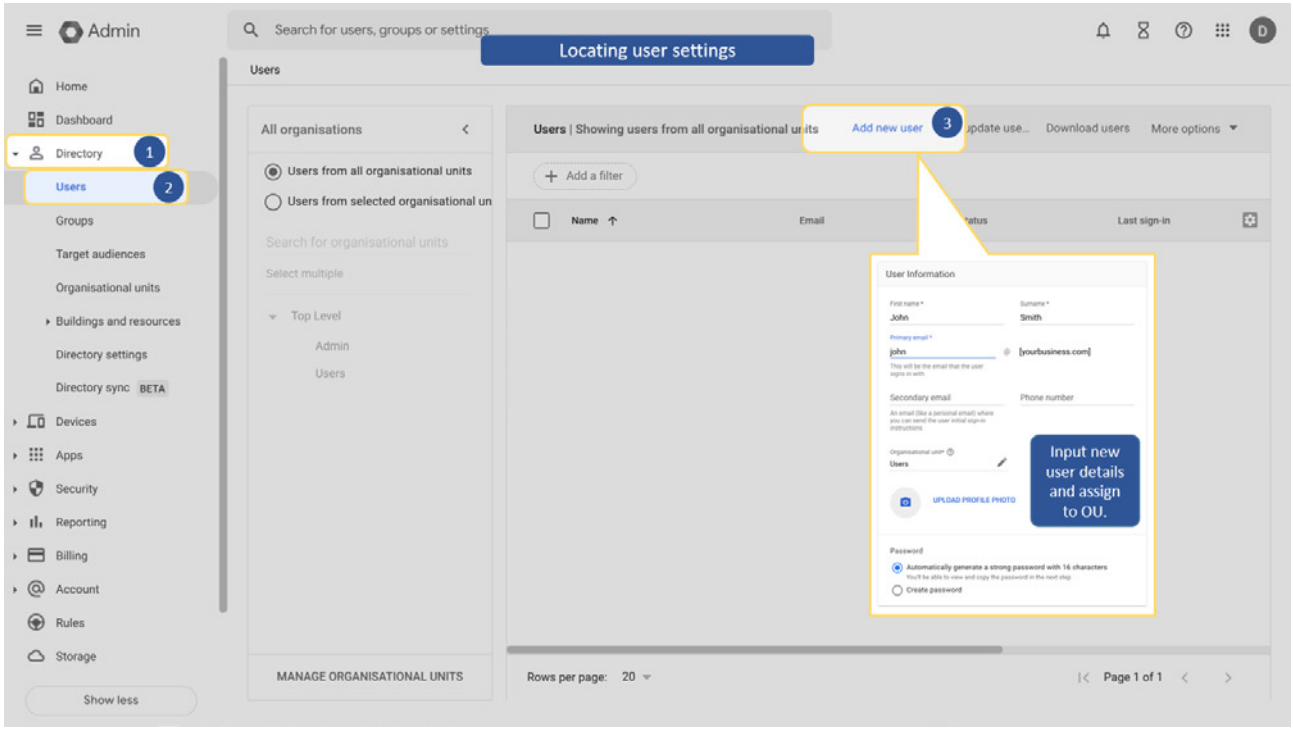
Organisational units are set up in the Google admin console as shown below.



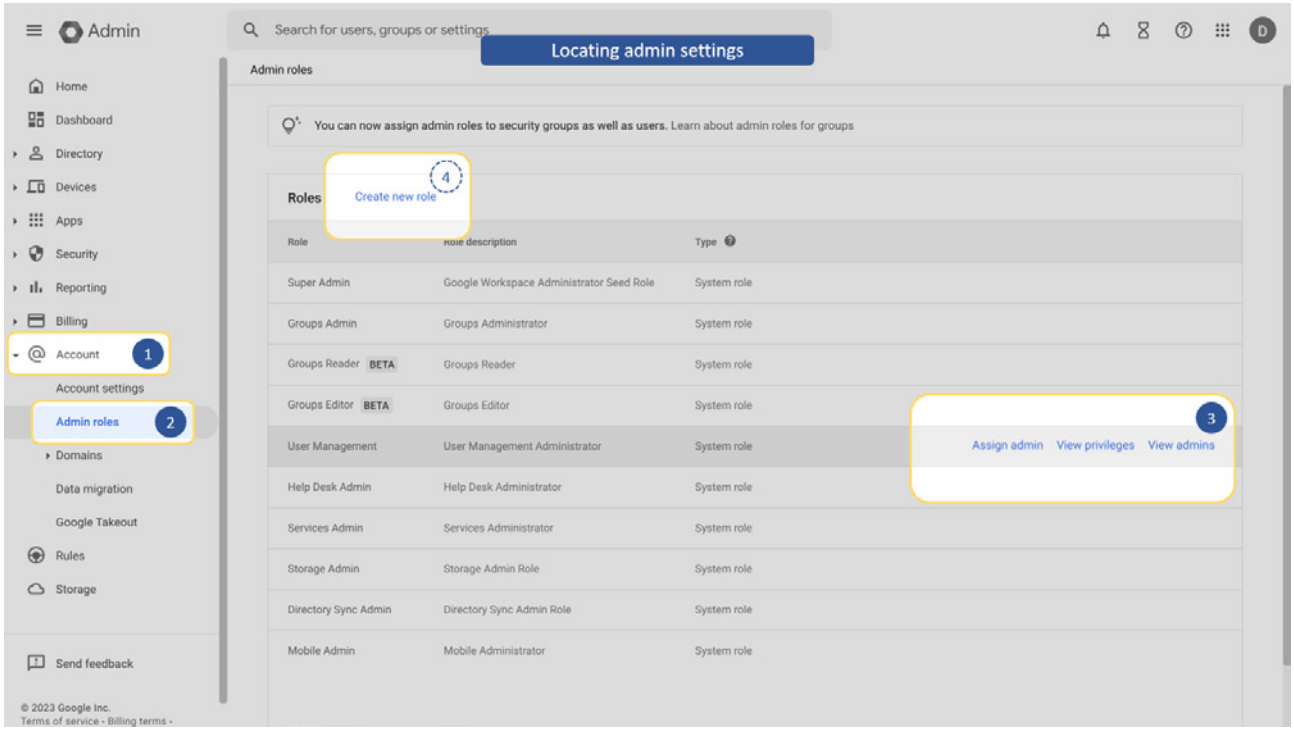
Set up admin and standard user accounts

The following guidance outlines how to set up admin and standard user accounts to provide users with only the privileges they need to do their job.

Users are created and managed in the Google admin console as shown below.



Admin roles are viewed, created and assigned to users in the Google admin console as shown below.



The basic steps to create user accounts and assign admin roles are:

1. Log in to the Google admin console with a user account that has super administrator privileges.
2. Create user accounts as required. Remember to allocate new user accounts to their appropriate organisational unit on the 'add new user' page.
3. Assign admin roles to user accounts as required (if Google's pre-defined admin roles do not meet your needs you can create new admin roles).

Google account management best practices for small businesses and enterprises

Standard user accounts

A standard user account is a user account that does not have an admin role allocated to it. All users should have a standard user account for day-to-day work. This includes admins, who should switch to their standard user account whenever they undertake work that does not require admin privileges. Working from standard user accounts, where possible, is an effective way to reduce the chance that admin privileges are misused or admin accounts are compromised.

Admin accounts

Some users will require an admin account, in addition to their standard user account. Admin accounts are required for tasks such as creating new user accounts and resetting passwords. Admin accounts are created by assigning admin roles to a user account in the Google admin console.

The following are best practices to follow when managing admin accounts. Many of these principles will be applied in subsequent sections of this guidance:

- User accounts should only be allocated an admin role if they need it.
- User accounts that require admin privileges should be allocated the minimum privileges needed to do their job.
- Admins should switch to a standard user account for any work that does not require admin privileges.
- Admin accounts should be protected with phishing-resistant multi-factor authentication, for example, a security key.
- Admin accounts should not be shared among users. Providing admins with their own admin accounts allows you to grant and revoke privileges with more precision. It also removes the need to share passwords, makes it easier to close accounts that are no longer needed and assists with auditing admin actions.
- Admins should only log in to the Google admin console from managed devices to ensure that they are protected by the security mitigations applied in subsequent sections of this guidance.
- At least two super admin accounts should be created, one to do exclusively tasks that require super admin privileges and the other as a 'break glass account', in case you lose access to the main super admin account.
- Recovery options should be configured and backup codes saved for all admin accounts.

Break glass accounts

It is good practice to set up at least one of your super admin accounts as a break glass account. Break glass accounts are for use in emergencies. They allow you to access the Google admin console if something goes wrong with your normal super admin account. The following are best practice principles for managing break glass accounts. Many of these practices will be applied in subsequent sections of this guidance:

- Assign break glass accounts super admin privileges. In the event of an emergency, you may need extensive privileges to apply a fix.
- Exempt break glass accounts from any access controls that could prevent you from using the account in an emergency, for example, Google's Context-Aware Access controls.
- Protect break glass accounts with phishing-resistant multi-factor authentication, for example, a security key. Security keys are phishing resistant and less susceptible to outages that may prevent you from accessing the account in an emergency.
- The credentials for break glass accounts should be stored in a secure location. For example, in a secure cabinet in your office. These credentials should only be accessible to a limited number of trusted users.

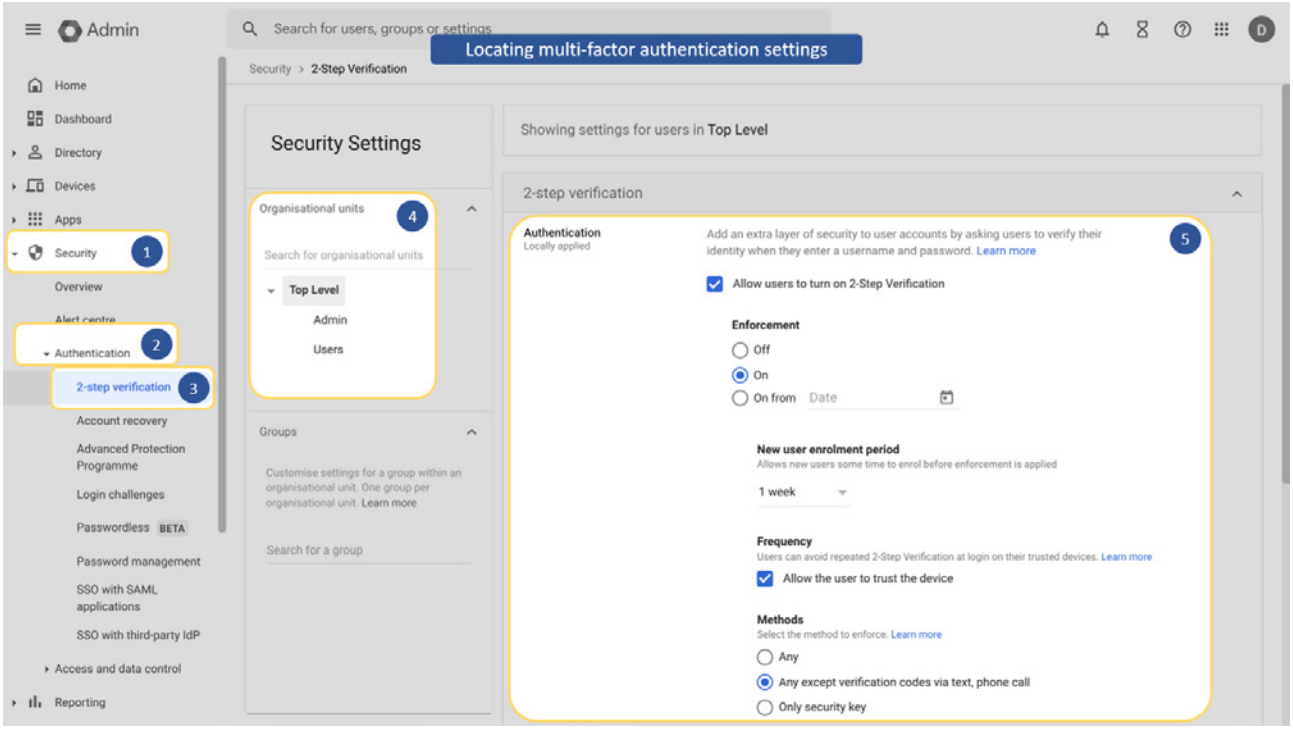
CASE STUDY – BREAK GLASS ACCOUNTS

Employees at John's pet grooming store use Chromebooks and Google Workspace to access their emails, manage their customer bookings and do their accounting. John asked his employee Amanda to be in charge of their Google Workspace super admin account as Amanda was good with computers.

After a few years, Amanda moved interstate and left John's business. Unfortunately, Amanda forgot to set up a super admin account for a different employee before she left. After Amanda left, John tried to create a super admin account for Amanda's replacement but realised that no one at work had sufficient privileges to do so.

Fortunately, John remembered he had set up a break glass account with credentials securely stored in his office cabinet. John logged in to his break glass account, allocated super admin privileges to a new employee and closed Amanda's old super admin account.

Configure multi-factor authentication settings

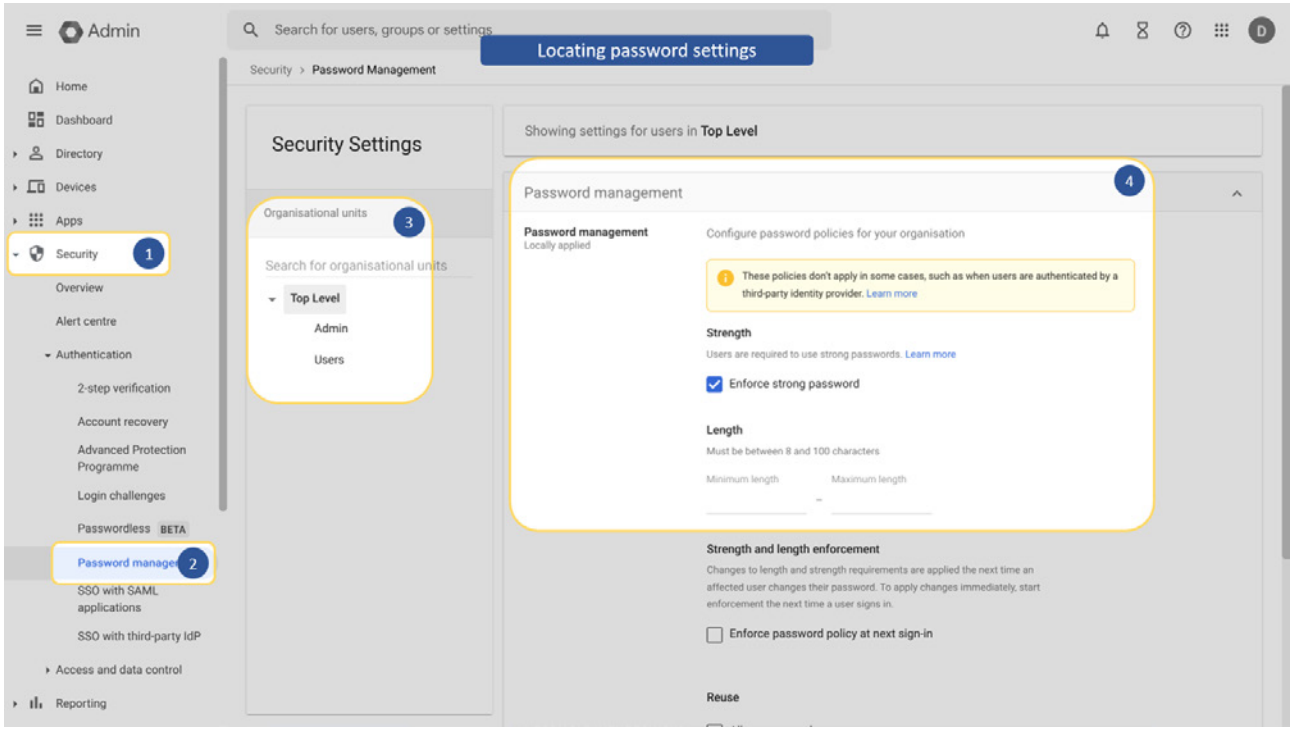


Multi-factor authentication is an essential measure to protect your user accounts. ChromeOS multi-factor authentication settings are configured in the Google admin console as shown above. The following table outlines recommended multi-factor authentication configurations for different organisational units. Note that Google refers to multi-factor authentication as '2-step verification'.

Category	Setting	Organisational Unit to configure	Configuration	Comments
2-step verification	Authentication	Apply this setting to: **Top level OU**	**Allow users to turn on 2-step Verification** ☑ Ticked **Enforcement** On **New user enrolment period** 1 week **Frequency - Allow the user to trust the device** ☐ Unticked **Methods** Any except verification codes via text, phone call	Require multi-factor authentication for all admins and standard users. Consider using alternatives to verification codes via text and phone call as these are less secure secondary authentication factors.

Category	Setting	Organisational Unit to configure	Configuration	Comments
		Admin OU	**Allow users to turn on 2-step Verification** ☑ Ticked **Enforcement** On [*Important:* before enforcing this setting, ensure admin accounts have set up security keys for authentication] **New user enrolment period** None **Frequency - Allow the user to trust the device** ☐ Unticked **Methods** Only security key	Configure admin and break glass accounts to require security keys to authenticate. Security keys are phishing-resistant which makes them an effective way to add extra protection to admin and break glass accounts.

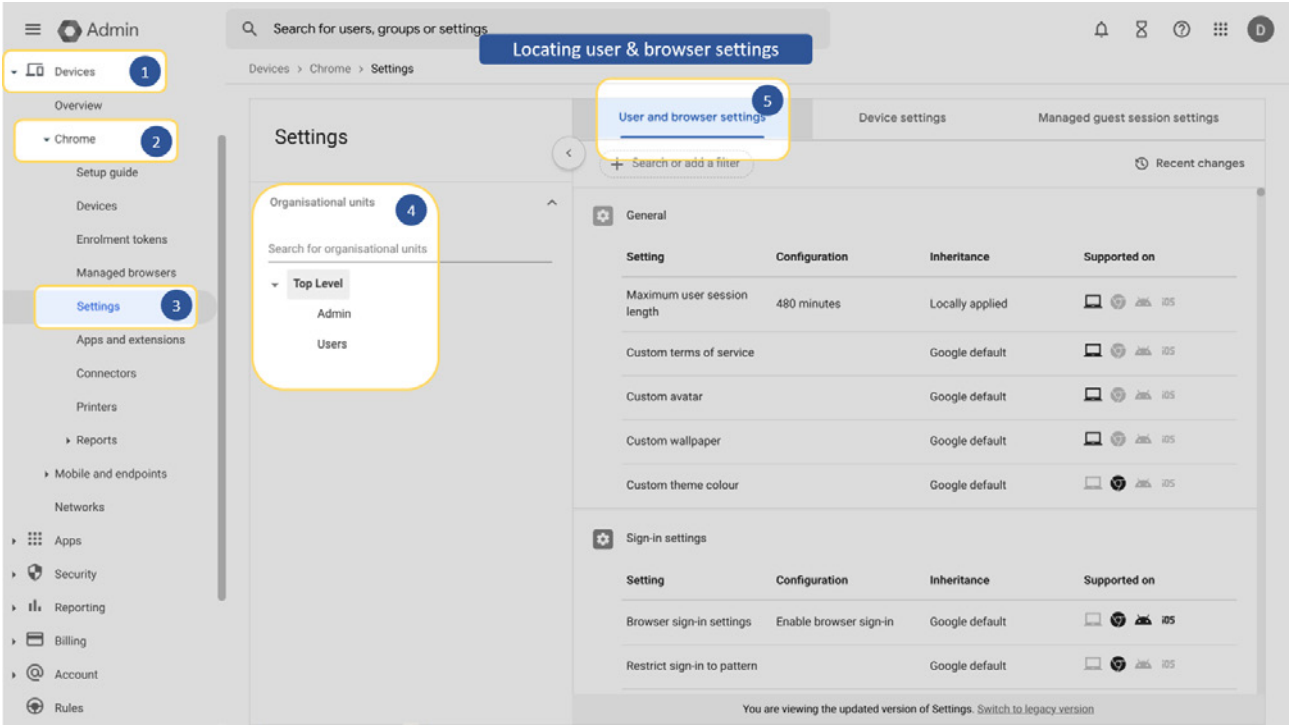
Configure password settings



ChromeOS allows you to configure password settings in the Google admin console as shown above. The following table shows recommended password configurations. For further advice on creating strong passwords, refer to ASD's ACSC's advice on passphrases and password managers.

Category	Setting	Organisational Unit to configure	Configuration	Comments
Password management	Password management	Apply this setting to: **Top level OU**	**Strength – Enforce strong password** ☑ Ticked **Length** 8 – 100 characters **Strength and length enforcement – Enforce password policy at next sign-in** ☑ Ticked **Reuse – Allow password reuse** ☐ Unticked **Expiry** 365 days	The 'enforce strong password' setting will prevent users from setting weak passwords, for example: 'password123'. A minimum password length of 8 characters is sufficient when used in conjunction with multi-factor authentication.

Configure user and web browser settings



ChromeOS user and browser settings are configured in the Google admin console as shown above. The following table shows recommended user and browser configurations. Note that browser settings are only applied to the Chrome web browser. If you allow your users to install alternative web browsers from the Google Play Store you will need to apply equivalent security measures to those web browsers.

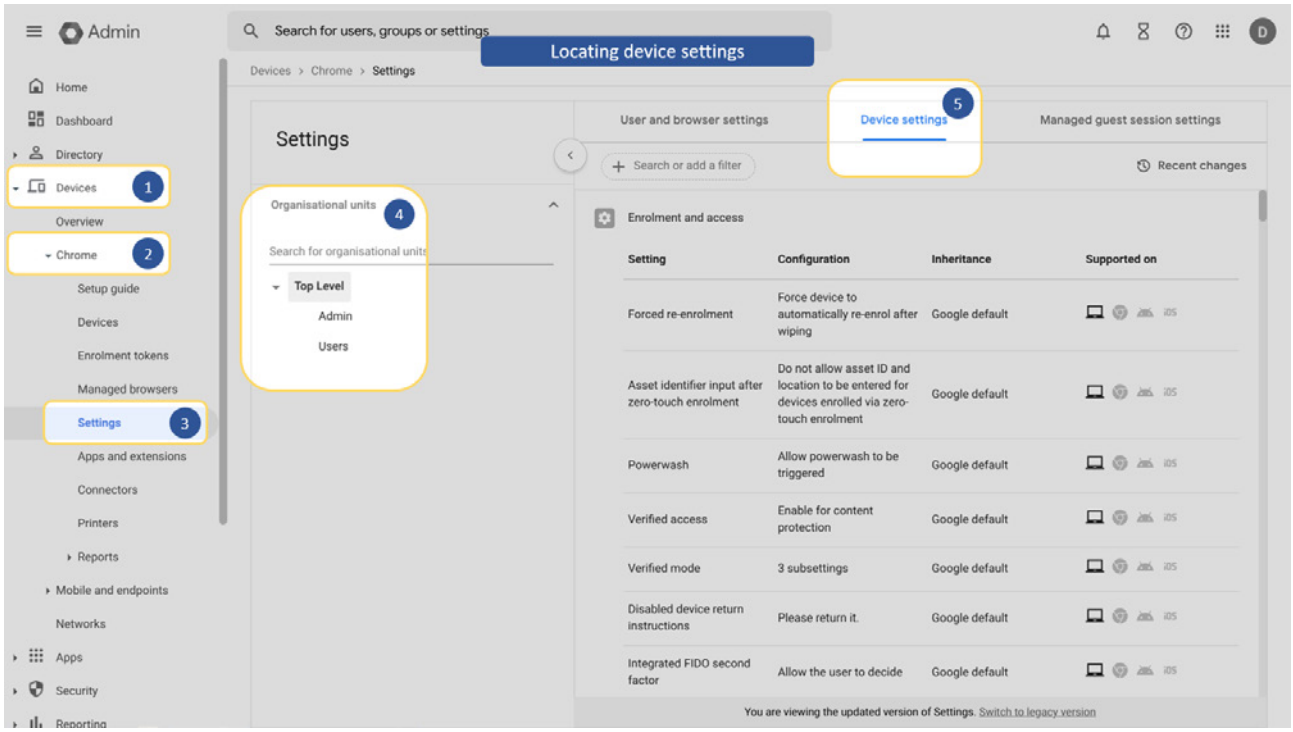
Category	Setting	Organisational Unit to configure	Configuration	Comments
General	Maximum user session length	**Top level OU**	1,440 minutes	This setting requires users to re-authenticate periodically. Set according to your business' needs. 1,440 minutes (24 hours) is a good guide. Note that the Google admin console has a fixed session length of 60 minutes.
Enrolment controls	Enrolment permissions	**Top level OU**	Only allow users in this organisation to re-enrol existing devices (cannot enrol new or deprovisioned devices)	This setting allows standard users to re-enrol existing devices but not enrol new ones.
		Admin OU	Allow users in this organisation to enrol new devices (or to re-enrol existing ones)	Apply this setting to your admin organisational unit so that admins can control which devices are enrolled in your business.

Category	Setting	Organisational Unit to configure	Configuration	Comments
Site isolation	Site isolation	Top level OU	Require site isolation for all websites, as well as any origins below [add origins, if required]	This setting protects against malicious code from one website infecting other processes.
Security	Google online login frequency	Top level OU	Force online login flow for Google Accounts [Set to 0 days]	This setting requires users to always login through Google's online login flow. Google's online login flow enforces your MFA policy every time. Google's offline login flow only enforces your MFA policy under certain conditions.
	Enable leak detection for entered credentials	Top level OU	Enable leak detection for entered credentials	With this setting enabled, Google will check if entered credentials match known leaked credentials.
Remote Access	Remote access clients	Top level OU	[Set to organisation's domain. For example: yourdomain.com]	If you receive remote access support from a managed service provider, you may need to allow their domain as well.
	Remote access hosts	Top level OU	[Set to organisation's domain. For example: yourdomain.com]	This setting allows hosts that are registered on the listed domains to be shared.
Network	Allow Basic authentication for HTTP	Top level OU	HTTPS is required to use Basic authentication scheme	These settings prevent users from using insecure internet protocols and technologies. These settings may interfere with old websites or old network infrastructure (for example, old routers and switches). Consider upgrading any websites or network infrastructure that rely on these less secure protocols and technologies.
	SSL error override	Top level OU	Block users from clicking through SSL warnings	
Content	Flash	Top level OU	Block sites from running Flash and do not allow the user to enable it (recommended)	
	URL Blocking	Users OU	[Add the following URL to the block list for standard users chrome://flags]	Flags allow users to enable and configure experimental Chrome features. Access to flags should be disabled for standard users as some experimental features can compromise security. Use this setting to list any other URLs you would like to block for standard users, or any other organisational unit.

Category	Setting	Organisational Unit to configure	Configuration	Comments
User experience	Developer tools	Top level OU	Never allow use of built-in developer tools	If you have a group of users that need access to developer tools, consider placing them in a separate organisational unit with this setting enabled.
	Multiple sign-in access	Top level OU	Block multiple sign-in access for users in this organisation	If multiple sign-in access is enabled, some settings configured in the admin console may not apply to users.
	Sign-in to secondary accounts	Top level OU	Block users from signing in to or out of secondary Google Accounts	This control helps to maintain separation between admin accounts, other work accounts and personal accounts.
	Browser guest mode	Top level OU	Prevent guest browser logins	Prevent guest browser logins so that users cannot circumvent web browser controls that apply to their organisational unit.
	Disabled system features	Top level OU	Disable Crosh	If you have users that require access to the Chrome Shell (Crosh), consider creating an organisational unit that grants access for those users.
Power and shutdown	Idle settings	Top level OU	**AC screen lock delay in seconds** 900 **Battery screen lock delay in seconds** 900	This setting protects against unauthorised access to unattended devices. Set a screen lock delay of no more than 15 minutes (900 seconds). The remaining idle settings can be configured according to your needs. To balance the requirement to re-authenticate after a short screen-lock time, consider allowing users to 'quick unlock' with fingerprint or PIN. This setting can be found under: Devices → Chrome → Settings → User and browser settings → Security → Quick unlock.
Browser reporting	Managed browser reporting	Top level OU	Enable managed browser cloud reporting	Managed browser cloud reporting must be enabled if you want users to be able to request access to extensions.
	Event reporting	Top level OU	Enable event reporting	Event reporting can assist admins to detect security issues, as well as detect and respond to a cyber security incident.

Category	Setting	Organisational Unit to configure	Configuration	Comments
Chrome Safe Browsing	Safe Browsing protection	Top level OU	Safe Browsing is active in the enhanced mode. This mode provides better security but requires sharing more browsing information with Google	These settings protect against malicious websites, downloads and ads.
	Download restrictions	Top level OU	Block malicious downloads	
	Disable bypassing Safe Browsing warnings	Top level OU	Do not allow user to bypass Safe Browsing warning	
	Sites with intrusive ads	Top level OU	Block ads on sites with intrusive ads	
Chrome updates	Relaunch notification	Top level OU	Force relaunch after a period **Time period (hours)** 48 **Initial quiet period (hours)** 0	For updates to take effect, devices require a relaunch. This setting ensures that timely updates are applied by forcing relaunch after a set period. Set the force relaunch period to no more than 48 hours. Set the initial quiet period to 0 hours so that users are notified as soon as an update is available. This setting also allows you to set a window of time for ChromeOS to relaunch that suits your needs.
Virtual machines (VMs) and developers	Linux virtual machines (BETA)	Top level OU	Block usage for virtual machines needed to support Linux apps for users	This setting prevents users from turning on the Linux development environment. If you have users that require access to the Linux development environment, consider setting up an organisational unit that grants only those users access.

Configure device settings

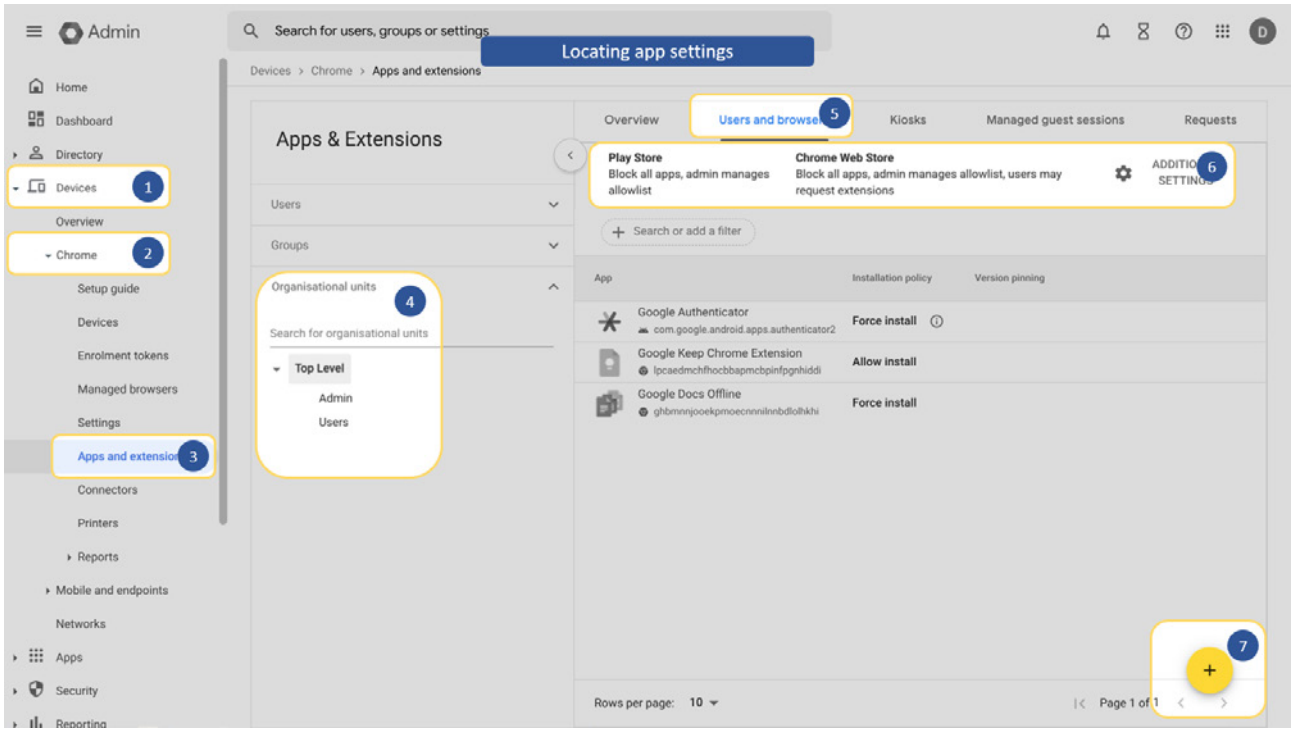


ChromeOS device settings are configured in the Google admin console as shown above. The following table shows recommended device settings configurations. Be aware that many of the security settings applied in this guidance do not apply to devices in developer mode.

Category	Setting	Organisational Unit to configure	Configuration	Comments
Enrolment and access	Forced re-enrolment	Apply this setting to: **Top level OU**	Force device to automatically re-enrol after wiping	This setting prevents devices from entering developer mode. If you have users that need access to developer mode, consider creating an organisational unit for their devices with this setting disabled.
	Disabled device return instructions	**Top level OU**	[add business-specific device return instructions]	Consider adding a return address and contact number. This information will be displayed on the screen of any devices that an administrator marks as 'disabled' in the admin console, thus making them easier to return.
Sign-in settings	Guest Mode	**Top level OU**	Disable guest mode	Your settings will not all apply to users in guest mode. Disable guest mode to prevent settings from being circumvented.
	Sign-in restriction	**Top level OU**	Restrict sign-in to a list of users **Allowed users** [limit to your organisation's domain, for example: *@ yourdomain.com]	This setting helps to maintain separation between your work and personal accounts. It also encourages users to conduct business on their work accounts where they are protected by your desired settings. Note, the '*' symbol is a wildcard that allows all email addresses within the listed domain.

Category	Setting	Organisational Unit to configure	Configuration	Comments
Device update settings	Auto-update settings	Top level OU	**Allow devices to automatically update OS version** Allow updates **Target version** Use latest available version **Roll back to target version** Do not roll back OS **Release channel** Stable channel **Roll-out plan** Default (devices should update as soon as a new version is available) **Auto-reboot after updates** Allow auto-reboots **Updates over mobile** Allow automatic updates on all connections, including mobile **Peer to peer** Do not allow peer to peer auto-update downloads **Block devices and user sessions after** No warning **If they are not running at least latest version** [set to most recent listed version] **Extend this period, where devices that are not receiving automatic updates are not yet blocked to** 1 week **Update downloads** Use HTTPS for update downloads	These settings will help to keep your devices up to date with the latest security patches and security features.
User and device reporting	Report device OS information	Top level OU	Enable all OS reporting	Logs and reports can assist admins to detect security issues, as well as detect and respond to a cyber security incident.
	Report device hardware information	Top level OU	Enable all hardware information reporting	
	Device system log upload	Top level OU	Enable device system log upload	
Other settings	TPM firmware update	Top level OU	Block users from performing TPM firmware update	It is recommended that admins test TPM firmware updates before rolling them out to all devices. Consider installing TPM firmware updates on a test device and monitoring it for a few days to ensure it continues to function correctly.
		Admin OU	Allow users to perform TPM firmware update	

Configure app settings



ChromeOS allows you to control what apps and extensions users can install. Doing so reduces the risk that users may accidentally install a malicious app or extension. Application control is managed through the Google admin console as shown above. Note that you add apps to configure using the yellow 'plus' button in the bottom right hand corner of the screen. The following table shows recommended app settings configurations.

Category	Setting	Organisational Unit to configure	Configuration	Comments
Allow/ block mode	Allow/ block mode	Apply this setting to: **Top level OU**	**Play Store** Block all apps, admin manages allowlist **Chrome Web Store** Block all apps, admin manages allowlist, users may request extensions	Admins will be able to manage what apps from the Google Play Store and Chrome Web Store can be installed. Apps can be either allowed, force installed or blocked. If you choose to add an alternative web browser to your allowlist, you will need to secure it with security measures that are equivalent to the settings in this guidance that apply to the Chrome web browser. Note, removing an app from the allowlist will not uninstall it from devices. It will only prevent installs from that point forward. If you would like to force a previously installed app to uninstall, you must add it to the blocklist.
Additional application settings	External extensions	**Top level OU**	Block external extensions from being installed	If you have users that require access to an external extension, consider creating an organisational unit for them that permits approved external extensions.

Backups

Why backups are important

Implementing regular backups will assist your small business or enterprise to recover and maintain its operations in the event of a disruptive or destructive cyber security incident. Backups should include everything your small business or enterprise needs to start operating again. For most small businesses and enterprises, this includes data, apps and settings. Your important data likely include more than just documents; they may include:

- emails
- messages
- photos
- videos
- audio records
- logs
- branding
- calendars
- contacts
- tasks.

Regularly test that you can restore from your backups to give you confidence that you can quickly recover your business' operations in the event of a disruptive or destructive cyber security incident.

Choosing a backup solution

There are several ways a small business or enterprise can manage their backups. Popular methods include backing up to a cloud service, an external storage device or a combination of both. ASD's ACSC has published guidance on how to back up your files and devices, including factors you should consider when choosing your backup solution. There are several third-party cloud backup services that integrate with Google Workspace. If you decide to use a third-party cloud backup service, ensure you set up notifications for failed backups so that errors can be addressed promptly.

Storing files in Google Drive

Google Drive is Google's built-in cloud storage and file sharing platform. However, Google Drive does not have all the features of a traditional backup and recovery solution because it was not designed for that purpose.

Google Drive has version history and file recovery features, however these features have time limitations that should be considered before deciding to use it in lieu of a dedicated backup and recovery solution. Dedicated backup and recovery solutions typically retain backups for as long as required. In contrast, Google Drive can only recover files within the following constraints:

- standard users can recover files from their trash folder that were deleted in the past 30 days
- admins can recover files that were permanently deleted in the past 25 days
- up to 100 previous file versions are retained for a period of 30 days.

Having a copy of your data outside of the Google ecosystem also provides redundancy in the event that your Google account is compromised or there is a Google Drive failure.

Google's data management tools

Google offers data governance, export and recovery tools that integrate with ChromeOS and Google Workspace. While these tools are not designed to perform traditional backup and recovery functions, they can complement your business's backup solution. These tools include:

- Google Vault – an information governance, data retention and discovery tool.
- Google Takeout – a feature that allows individual users to export their Google Workspace data.
- Google Workspace Data Export – a tool that allows admins to export all Google Workspace data in their organisation once per month.

Backing up apps and settings

For most small businesses and enterprises, there is no need to create a backup of ChromeOS settings as these settings are cloud-managed and can be pushed to newly enrolled devices.

If your small business or enterprise uses web apps or Google Play Store apps, ensure you back up any important data these apps hold.

This guide recommends disabling the ChromeOS Linux development environment, unless your business has a requirement to use it. However, if your small business or enterprise does use the Linux development environment, follow Google's guidance on backing up your Linux files and apps.

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

Neither the Commonwealth nor Google accepts responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

For more information, or to report a cyber security incident, contact us:
cyber.gov.au | 1300 CYBER1 (1300 292 371)

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre