Getting started with ChromeOS

Table of contents

Congratulations on getting started with ChromeOS! If you are an expert Google Admin, feel free to skip to the sections that are relevant to you. If you are new, then we are excited to help you transform how you work. In this guide, we will walk you through the basics of ChromeOS.

Introduction

Thanks for checking out our Getting started with ChromeOS guide! You may be here for a few reasons: you have purchased or are interested in purchasing ChromeOS devices and Device Management.

Let's get some definitions out of the way:

- A ***ChromeOS device*** (Chromebook, Chromebook Plus, Chromebase, Chromebox, Tablet, devices updated with ChromeOS Flex) is a computing device that runs ChromeOS, an operating system designed for the Cloud developed by Google. What makes these devices unique is that they automatically update, you don't have to install patches or re-image machines regularly, they boot quickly and have several security features built in.
- **Device management:**
    - Device management comes included with ChromeOS Enterprise devices (these include Chromebook Enterprise, Chromebase Enterprise, Chromebox Enterprise, and Chromebook Plus Enterprise) and are available to be purchased for ChromeOS devices for education or enterprise separately (in some cases, Chromebooks with Chrome Education Upgrade included are available).
    - Our device management solution allows IT admins to manage and secure devices at scale, through the cloud based Google Admin console. Features include advanced security to keep corporate data safe; ensures flexible access to resources regardless of use case; and simplifies orchestration of ChromeOS devices and other critical infrastructure. The following ChromeOS device management solutions are available to suit clients' different needs; *Chrome Enterprise Upgrade, Chrome Education Upgrade, Kiosk and Signage Upgrade,* and *Chrome Non-Profit Upgrade*.
- Google Admin console is used to centrally manage ChromeOS devices. As an IT administrator for a business or school, you can manage enterprise features for Chrome users across a range of devices. With Google Admin console, you can enforce policies, set up Chrome features for users, provide access to your internal VPNs and Wi-Fi networks, force install apps and extensions, and more.

This guide will help provide instructions on how to make your purchase, set up your account, enroll devices, share ChromeOS deployment methodology, policy setup, change management, best practices, and what to expect along the way.

Note: The recommendations for deploying ChromeOS devices in school and business settings were gathered through our work with a variety of customers and partners in the field. We thank our customers and partners for sharing their experiences and insights.

Have a question or need assistance?

Check out our support page or for general questions, refer to the Chrome Enterprise Help Center.

Deployment: methodology and best practices

Before you start enrollment and deployment of devices you'll want to make sure you have the right methodology and configuration in place to ensure successful performance and adoption.

Deployment methodology checklist

Here is a checklist that customers and internal Google teams have used to prepare devices for deployment. Before you execute, make sure you do your due diligence on each of these categories. In the sections below we'll walk you through "Deployment Project Kick-off" and "Configure Infrastructure". "Define organizational units and policies" will be covered in 'Management' and "Managed provisioning preparation" will be covered by Device deployment

- ❑ Deployment project kick-off
  - ☐ Define deployment team
  - ☐ Deployment blueprint
  - ☐ Develop project plan
- ❑ Configure infrastructure
  - ☐ Network connectivity
  - ☐ Verify bandwidth capacity
  - ☐ Printing solution
- ❑ Define organization units and policies
  - ☐ Console management
  - ☐ Admin roles defined
  - ☐ OU hierarchy
  - ☐ Device policy
  - ☐ User policy
- ❑ Managed provisioning preparation
  - ☐ Update ChromeOS to the latest build
  - ☐ Enroll device in company domain
  - ☐ Prepare for shipping
  - ☐ Test and verify device configuration
  - ☐ Verify hardware setup
  - ☐ Policy on the device
  - ☐ Policy for the end user
  - ☐ Create deployment checklist

Deployment project kick-off

Adopting a new workflow is not something that happens overnight. The process is sequential and aligns with the fundamental components that make up communications, training, and engagement to assist employees to integrate ChromeOS into their work habits and processes. A successful ChromeOS deployment blueprint incorporates change management at every step of the ChromeOS adoption journey.

Start with the people-side of change

People are at the core of every organizational change project. Our primary goal is to establish a structured approach to manage the people-side of ChromeOS device adoption.

Key decisions

1. Who internally will be responsible for this deployment being a success?
2. Who are your users and how will they be using ChromeOS devices?
3. How will work be impacted by switching to ChromeOS devices?
4. Will ChromeOS devices be the users' primary devices?
5. How will you measure the success of the deployment (for example 50% of users deployed in 30 days)?
6. How will your users be aware of the shift to ChromeOS devices?
7. How will you train your users to use ChromeOS devices?

An effective change management plan ensures:

- Users understand why using ChromeOS devices is a better way to work
- Communications are customized for users, answering the questions they care about
- Users are trained and ready to use their ChromeOS device
- Users make the personal decision to adopt ChromeOS devices
- Ongoing engagement and support for users and IT admins

Documenting answers to these questions and following guidance in the "ChromeOS Adoption and change management" section will help you accelerate ChromeOS adoption within your organization.

Connectivity

When setting up wireless for your organization, be sure that you have adequate wireless coverage throughout the building, and that you have sufficient Internet bandwidth for all of your devices to work online. For additional details on how to manage networks, troubleshooting, setting up VPNs and more please review the Connectivity help article.

Key features

ChromeOS devices support all of the most common Wi-Fi protocols: WEP, WPA, WPA2, EAP-TLS, EAP-TTLS, EAP-PEAP, and LEAP. Additionally, some ChromeOS devices have 3G or 4G mobile Internet access hardware, which work as long as there's cellular coverage and a cellular data plan.

Evaluation and deployment tips

Proper evaluation and preparation of your organization's network infrastructure is a key step to ensuring the best experience for your users. IT administrators should ensure there's adequate connectivity and bandwidth, especially in a high-density area, such as a corporate office or school, where many ChromeOS devices are used concurrently.

- **Test Wi-Fi coverage and density** to evaluate whether additional access points may be needed. You can do this with the third-party Wifi analyzer apps on a mobile device.
- **Perform a wireless infrastructure and topology survey** of all buildings, prior to school/company-wide deployments, to ensure you have adequate wireless coverage. It's usually best to have a partner specializing in wireless topology conduct the following:
    - **Site Survey**—You must first analyze both your existing Wi-Fi network along with surrounding interference from devices or other Wi-Fi networks.
    - **Deploy**—Deploy or reposition access points with proper security, channel selection, and Receive/Transmit (Rx/Tx) power.
- **Ensure ChromeOS devices have access to required URLs.** ChromeOS devices require access to Google's network to function correctly, and to receive policies and security updates. If you limit internet access in your environment, you must ensure that your deployed devices can still access these specific google URLs without going through an authenticated proxy or SSL inspection.

For more in-depth information, access points and bandwidth considerations see Enterprise networking for ChromeOS devices.

Manage network profiles

Wi-Fi networks can be manually added to a ChromeOS device at any time, but Google recommends using Google

Admin console to push network profiles. These profiles are downloaded and applied to the ChromeOS device during the enrollment process. Updates to Wi-Fi network profiles also get pushed during the automatic policy refresh on the ChromeOS device. One advantage of using Google Admin console for pushing these configurations is that the pre-shared key (PSK) can be sufficiently complex and never needs to be shared with end users.

Configure Wi-Fi

Many ChromeOS device customers use WPA2-PSK for simplicity of setup. However, ChromeOS devices can work in a variety of educational and enterprise environments, including complex Wi-Fi deployment scenarios that require client certificates, Single Sign-On (SSO), and where web filtering solutions are deployed. Below are tips on how to set up Wi-Fi and optional network settings.

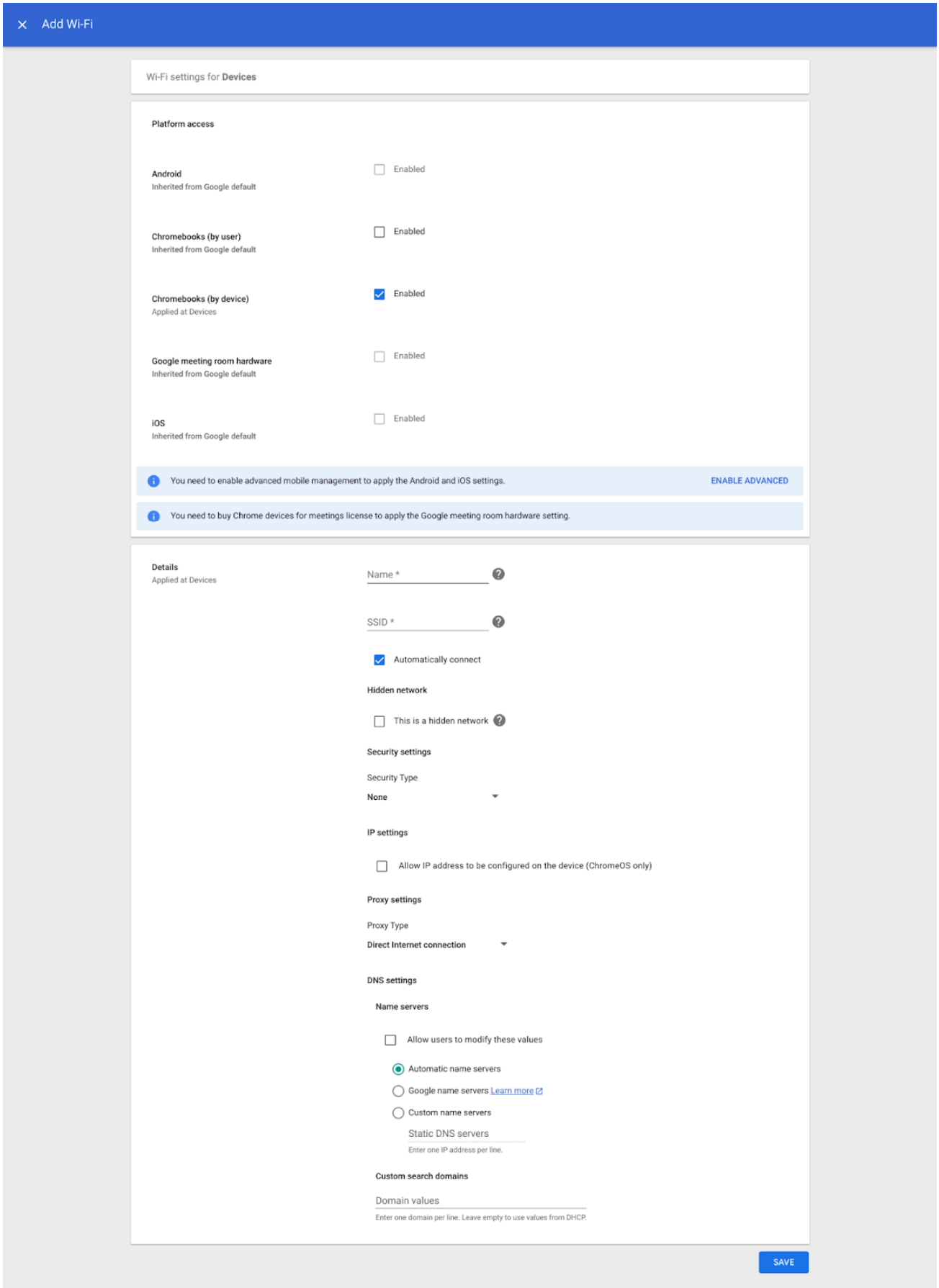
Add Wi-Fi configuration at the device level

To apply different settings to a set of users or ChromeOS devices, place them in their own organizational unit below your top-level, or parent organization. You can then apply settings to just that organizational unit. For more detail on organizational units please reference the Management section below.

Child organizational units inherit Wi-Fi network profiles from their parent organization, unless you break inheritance manually by selecting the organizational unit you wish to customize.

- Learn how the organizational structure works, understand Chrome policy management and steps to move ChromeOS devices to different organizational units.

To set up a profile, you need to provide network information such as SSID and Security type. Pay particular attention to the service set identifier (SSID) and passphrase, both of which are case-sensitive. When defining a new Wi-Fi network profile, you also need to check the “automatically connect” box and the “chromebooks (by user)” box in the “platform access” section. Find additional technical details for network setup here.


Add Wi-Fi
Wi-Fi settings for Devices
Platform access
Android
Inherited from Google default
Enabled
Chromebooks (by user)
Inherited from Google default
Enabled
Chromebooks (by device)
Applied at Devices
Enabled
Google meeting room hardware
Inherited from Google default
Enabled
iOS
Inherited from Google default
Enabled
You need to enable advanced mobile management to apply the Android and iOS settings.
ENABLE ADVANCED
You need to buy Chrome devices for meetings license to apply the Google meeting room hardware setting.
Details
Applied at Devices
Name *
SSID *
Automatically connect
Hidden network
This is a hidden network
Security settings
Security Type
None
IP settings
Allow IP address to be configured on the device (ChromeOS only)
Proxy settings
Proxy Type
Direct Internet connection
DNS settings
Name servers
Allow users to modify these values
Automatic name servers
Google name servers Learn more
Custom name servers
Static DNS servers
Enter one IP address per line.
Custom search domains
Domain values
Enter one domain per line. Leave empty to use values from DHCP.
SAVE

Wi-Fi setup

It's often easiest to use an open or unfiltered network to enroll ChromeOS devices and have a first sync of the management policies. This setup allows the ChromeOS device to receive the IT administrator-defined network profiles. After you've configured the devices, remove this temporary enrollment network from the list of preferred networks; see forget a network.

Client certificates

ChromeOS devices support 802.1x authentication and as an IT admin you have several options to deploy client certificates on ChromeOS devices, such as using the Google Cloud certificate connector, the Google certificate enrollment extension, and third-party extensions.

If you're looking to deploy certificates using the Simple Certificate Enrollment Protocol (SCEP) in your organization, we have prepared a detailed guide to setup Certificate Enrollment for ChromeOS via SCEP.

Web filtering

Organizations with network filtering devices doing Secure Socket Layer (SSL) inspection generally require a custom root certificate to be added to the Authorities tab in chrome://settings/certificates. While this works for most user-driven web requests, some system-level requests don't use this certificate to protect the user against certain kinds of security risks. To ensure that ChromeOS devices work with TLS inspection or networks restricting external traffic, you need to allow this list of hostnames.

To get ChromeOS devices to work on a network with SSL inspection, see set up networks with SSL content filters, which explains how to install a custom root certificate on all domain users who sign in to your organization's enrolled ChromeOS devices.

Wi-Fi for Re-enrollment

If you are using a secure network and preventing your users from joining on their own, you may want to set up a second SSID to enable device re-enrollment. When troubleshooting, a common action is to powerwash or hard reset devices. This clears all configured policies. In order to re-enroll and obtain device policies a connection to the internet must be established. A second SSID firewalled to only access the Google servers required to retrieve the policy can make the power washing of a device a simple process. A cellular hotspot or ethernet internet connection can also be used for this process.

Device deployment

If you are deploying a small number of devices, follow the online version of our Quick Start Guide. If you're deploying ChromeOS devices to a larger group or mass enrolling devices, such as multiple office locations, see the instructions below.

Paths to ChromeOS enrollment

If you don't have a ChromeOS enterprise device

You'll need to purchase ChromeOS device management to manage from the Google Admin console. You may purchase ChromeOS device management for a school or business. See the ordering options for additional details.

- From the Google Admin console, check how many licenses you have and how to manage and renew annual upgrades.
- Please contact your Google ChromeOS device reseller for further details. If you do not have an authorized partner you can search for a Google Cloud partner in your area.

If you're a new **Enterprise** customer:

Standalone ChromeOS device management

1. Customer purchases ChromeOS device management; Chrome Enterprise Upgrade, or Kiosk and Signage Upgrade
2. Reseller has to process Google Admin console account order through Google
3. Google sends welcome letter to customer with Google Admin console login
4. Customer must verify domain
5. Customer enrolls ChromeOS device

ChromeOS devices with device management included

1. Customer purchases a ChromeOS device with device management included
2. Customer needs to go to: https://chromeenterprise.google/os/upgrade to create a Google Admin console Account
3. Customer logs in and sets up Google Admin console
4. Customer must verify domain
5. Customer enrolls ChromeOS device

If you're a new **Education** customer:

Standalone ChromeOS device management

1. Customer requests approval for Google Workspace for education and verifies their domain
2. Customer purchases ChromeOS device management; Chrome Education Upgrade
3. Reseller processes order through Google
4. Google sends welcome letter to customer
5. Customer enrolls ChromeOS device

ChromeOS devices with device management included

1. Customer requests approval for Google Workspace for education and verifies their domain
2. Customer purchases a ChromeOS device with device management included
3. Customer enrolls ChromeOS device

If you're a new **Nonprofit** customer:

Standalone ChromeOS device management

1. Customer requests a Google for Nonprofits account and waits for verification.
2. Customer activates Google Workspace for Nonprofits and verifies their domain
3. Customer purchases ChromeOS device management; Chrome Non-Profit Upgrade
4. Reseller processes order through Google
5. Google sends welcome letter to customer
6. Customer enrolls ChromeOS device

ChromeOS devices with device management included

1. Customer requests a Google for Nonprofits account and waits for verification.
2. Customer activates Google Workspace for Nonprofits and verifies their domain
3. Customer enrolls ChromeOS device

If you are a current Google customer (for example Google Workspace):

Standalone ChromeOS device management

1. Customer purchases ChromeOS device management; Chrome Enterprise Upgrade, Chrome Education Upgrade, Chrome Non-Profit Upgrade, or Kiosk and Signage Upgrade
2. Reseller sends customer Google Admin console account details to Google through an order
3. Google sends welcome letter to customer
4. Customer enrolls ChromeOS device

ChromeOS device with device management included

1. Customer purchases a ChromeOS device with device management included
2. Customer enrolls ChromeOS device

From the Google Admin console check your upgrade totals in two locations:

- Billing > Subscriptions - shows Chrome, Android and Google Workspace subscriptions
- Devices > Chrome > Devices > click “Upgrades” to view upgrade totals

Check out our “How-To” demo videos playlist for step by step instructions on topics such as domain verification, Google Admin console, and enterprise enrollment.

Prerequisites

To deploy and centrally manage a fleet of ChromeOS devices you’ll need to make sure you have the following in place:

For IT Admin

1. Administrator access to primary domain:

Domain ownership must be claimed with Google in order to enable ChromeOS device management policies in the Google Admin console and to gain access to Google Cloud Support Center. Administrator access to the primary domain will be needed.

- Click here for help finding your administrator.
- Follow the article to verify your domain.

2. Google Admin console access

Required to configure user and device policies and enable device enrollment. Log in here.

- If you do not have Super Admin access to the Google Admin console, you'll need to create an account or get delegated access from your Super Admin.
    - Connect with a Super Admin at your organization to gain access to the Google Admin console. The Super Admin must assign your user account the roles and privileges for ChromeOS device management and Google Support access.

3. Access to Phone Support, Help Assistant and Google Cloud Support Center:

Super Administrators can delegate support access to domain users to manage tickets for account recovery and support ticket logging. In the support portal, the Super Admin must add the delegated user to a role that has Support privilege. To verify that the user's access to the Support Portal has been granted, check login access here.

For End Users:

Although Google Identity (Google Workspace account) isn't required to use a ChromeOS device, we recommend that you've provisioned your users with Google Accounts which allows them to have access to Google services. See how to add users to your domain for more information.

For a large number of ChromeOS devices or deploying with Google Workspace:

If you plan to deploy a large number of ChromeOS devices or deploy them in conjunction with Google Workspace for the first time, we recommend that you work with a Google Cloud partner.

Enrollment

Before you distribute ChromeOS devices to your end users, they need to be "staged" to ensure users have an optimal experience. The minimum requirement is to enroll the ChromeOS devices into your domain for management. This way, any future device policy update is applied to your fleet of ChromeOS devices.

Take a look at the Google Admin console setup guides

You can find practical setup guides in the Google Admin console at Devices > Chrome > Setup guide that will walk you through many common tasks like creating users and OUs, enrolling devices, setting policies, and many more.

Update ChromeOS devices to the latest version

Devices running ChromeOS automatically check for and download updates when connected to Wi-Fi or Ethernet. Devices are updated to the latest version unless there is a restriction that is placed by the admin in the device update settings. However, if you need to update many devices and want to conserve network bandwidth, you can cache the update locally on a caching server. Squid Cache is open source software which can be used to support caching. You can also manually update devices using a USB.

Create a ChromeOS image

To manually update ChromeOS devices to the latest version of ChromeOS using a USB stick, you will need:

1. The Manufacturer and Model information of the ChromeOS devices you wish to update.
2. A USB 2.0, or above, flash drive of 8 GB or larger
3. Chrome browser, running on ChromeOS, Microsoft Windows or macOS
4. Install Chromebook Recovery Utility and choose the correct make and model for the device to make the USB recovery disk.

Please go here for additional details on updating devices, device recovery, or wiping a device.

Note: A stable release may take a week before being available in the image burner tool.

Manual Enrollment

Steps to enterprise enroll your device

To enterprise enroll your devices (check out this video for step by steps instructions):

1. Create USB recovery devices or update your devices over the air. The USB method is recommended for more than 10 devices.
2. After rebooting, select the language, keyboard type, and Wi-Fi network.
3. Accept the Terms of Service.
4. *Before signing in to the ChromeOS device*, **press Ctrl-alt-E** to bring up the “Enterprise enrollment” dialog window. Alternatively, you can click “Enterprise Enrollment” at sign-in to choose Enterprise enrollment.

You may be automatically prompted to enterprise enroll your device

ChromeOS Enterprise devices (these include Chromebook Enterprise, Chromebase Enterprise, Chromebox Enterprise, and Chromebook Plus Enterprise) preinstalled with the latest update will automatically prompt users to enroll the device with their Google managed account after accepting the end-user license agreement and prior to sign-in. If you are not prompted, you may select Ctrl+Alt+E to enroll.

5. Enter a username and password (either administrator or enrollment user of the domain) and click “Enroll device”

   After you successfully enroll the device, you’ll get a message that "Your device has successfully been enrolled for enterprise management."

6. Click “Done” to return to the initial sign-in page. You should see “This device is managed by *yourdomain.com*” at the bottom of the page.

Repeat these steps for all of the ChromeOS devices in your organization. For more information about device enrollment, see enroll ChromeOS devices.

Best practices for manually enrolling a large volume of devices

- Avoid using a super-admin account to enroll devices, instead you can create accounts solely for the purpose of enrolling devices, these do not require admin privileges and you can create multiple accounts, remove any services associated with them (for example Google workspace) thus reducing the account’s overall access. The setting allowing this is set to “Allow” by default, under the policy named “Enrollment permissions”.
- The enrollment accounts can be directly positioned in the organizational unit where you want your devices to reside in, and have your devices enroll automatically into that OU instead of the default behavior where devices are positioned in the root OU (top-level OU). You can change this by going to the *user and browser settings* of your target OU and changing the policy value of “*Device enrollment*” to “*Place ChromeOS device in user organization*”. For example, if you want your device to enroll into your “*Kiosk devices”* OU, you would change the setting above in that OU, create an enrollment account in the same OU and use it to enroll your Kiosk devices directly into it.
- When manually enrolling many devices with the same account, it is very likely you will get a login challenge for the account, to facilitate a successful challenge and avoid enrollment interruptions you can:
  - Disable 2fa for your enrollment accounts, considering they do not have admin privileges and services associated.
  - Use the employee ID for verification method:

i. Add an employee ID to your enrollment accounts by going to the user details and editing their *User information*.
ii. Go to Security > Authentication > login challenges and enable the option to “Use Employee ID to keep my users more secure” for the organizational units of your enrollment accounts.
iii. You can then share this Employee ID with your technician or contractor enrolling the devices and when they get a login challenge, this Employee ID can be used to successfully finish the enrollment process.

IMPORTANT: If you forget to enroll your device**,** you will need to wipe the device and restart enrollment. For details, see our wipe ChromeOS device data instructions.

Zero-touch enrollment

An alternative to manual enrollment, Zero-touch enrollment (ZTE) allows the automatic enrollment of devices through a pre-provisioning partner. When ZTE is used, your devices will first appear in your console with a status of “Pre-provisioned” and as soon as the device connects to the internet, it will automatically enroll, changing its status to “Provisioned”. Zero-touch enrollment is the best option for hybrid and remote workers who receive their ChromeOS device directly at home, as well as devices in remote locations where there is no local IT support.

To get started, check out the zero-touch enrollment help article, and make sure to verify your devices are compatible, and that you have an authorized pre-provisioning partner.

You will need to provide a pre-provisioning token and your customer ID to your pre-provisioning partner. A unique token can be created per organizational unit (OU), allowing you to choose the location of where your device will be enrolled and avoiding to manually move them afterwards.

Mass enrollment

Another alternative to manual enrollment, especially when dealing with a large volume of devices, is mass enrollment. Through the use of an external 3rd party device, you can have the steps required to enroll your devices execute autonomously, greatly increasing the number of ChromeOS devices a single person can enroll in a given time.

To get started, check out the mass enroll Chromebooks help article.

Deployment scenarios

ChromeOS devices can be used in a variety of situations, and given their high security, remote management, and little to no maintenance, they’ve become popular to deploy for business and education use cases. Below you can find some of the most common uses.

Cloud and frontline workers

ChromeOS devices are great for enterprise employees. A ChromeOS device can be assigned to a user as their full time device for accessing web applications, productivity tools, and collaboration. It can also be used as an agent device in contact centers, as a clinician or shared device in Healthcare, in Manufacturing and many more scenarios. Learn more.

To learn more about how you can empower cloud workers with ChromeOS, see these videos at Cloud Worker Live.

Kiosk applications for single purpose

You can create a kiosk app for a single purpose; for example, having customers fill out a credit application, fill out a survey in a store, or student registration information. Learn more.

Digital Signage

You can use Chromeboxes for digital signage displays, such as school calendars, digital billboards, restaurant menus, and interactive games. You can create a hosted app or packaged app and launch it full-screen in Single App Kiosk mode. Learn more.

Public Session devices

You can set up Public Session devices for locations like an employee break room, store displays, or as a shared device in a library, where users don't need to sign in to use the ChromeOS device and instead use a Managed Guest Session. Learn more.

Student Assessment

Chromebooks are a secure platform for administering student assessments, and when set up properly, these devices meet K–12 education testing standards. With Chromebooks, you can disable student access to browse the web during an exam, and disable external storage, screenshots, and the ability to print.

You can configure Chromebooks for student tests in a variety of ways, depending on the nature of the exam: as a Single App Kiosk, on a domain provided by the test provider, or through Public Session kiosks. For details, see use Chromebooks for Student Assessments.

Educators

You can provide your educators and school staff with Chromebooks managed in the same environment as your student Chromebooks, allowing them to work from the same interface and taking advantage of features for teachers and tools like Screencast while benefiting from the security of ChromeOS. Learn more about Chromebook Plus for education.

ChromeOS Flex deployment

ChromeOS Flex provides the opportunity to install ChromeOS on devices running Microsoft Windows or MacOS, allowing you to take advantage of your existing hardware while benefiting from all the advantages of ChromeOS. Before getting started with ChromeOS Flex you should check the following:

1. Check if your device is included in the list of certified models.
2. Make sure you understand the differences between ChromeOS Flex and ChromeOS.
3. Take a look at the ChromeOS Flex frequently asked questions.

Once you have installed ChromeOS Flex on a device, you can enroll it to your domain using ChromeOS device management (solutions include; Chrome Enterprise Upgrade, Kiosk and Signage Upgrade, Chrome Non-Profit Upgrade and Chrome Education Upgrade) and manage it the same way as other ChromeOS devices.

Installation

To install ChromeOS Flex you will need:

1. A USB 2.0, or above, flash drive of 8 GB or larger
2. Chrome browser, running on ChromeOS, Microsoft Windows or macOS
3. Install the Chromebook Recovery Utility

Once ready, follow the steps in the ChromeOS Flex installation guide that will guide you through the bootable USB creation, device boot from USB, installation, and enrollment.

We recommend that you also review the ChromeOS Flex Deployment best practices to further secure your devices.

Mass deployment

When you need to install ChromeOS Flex on a large volume of devices (100 or more), you can utilize mass deployment tools for a faster deployment, such as:

- Microsoft Windows Deployment Services (WDS)
- Microsoft Windows System Center Configuration Manager (SCCM)
- Clonezilla

The steps and requirements for each one can be found in the links above. Once deployed, don't forget to enroll your devices.

Verify enterprise-enrolled devices

From the Google Admin console, you can search and view enrolled ChromeOS devices and see information about the devices (serial number, enrollment username and status, asset ID, policy sync data, support end date, and manually-entered notes, such as location) via the devices list. Drilling down into each device by serial number also allows you to view details, such as the device's installed OS version, MAC address, and last signed-in user. Some

useful tips are:

- Manage viewable columns by clicking on the gear icon (top right of the list)
- Click into a device to:
    - Move, reboot, remote desktop, capture logs, reset, disable, deprovision the device, or change the upgrade type
    - View Hardware and OS information, custom fields and system activity and troubleshooting data such as volume level, memory usage, CPU utilization, disk space and Wi-Fi signal strength
- Check your available ChromeOS device management upgrades by clicking on “Upgrades” at the top.
- Add filters to your list view, some common filters are Upgrade type, Chrome version, OS version compliance, Model, etc.

Once enterprise-enrolled, admins can:

- Wipe ChromeOS device data
- Force wiped ChromeOS devices to re-enroll
- Repurpose or retire ChromeOS devices

Managed provisioning Enrollment Service (Optional)

The managed provisioning service is designed to allow a “zero IT touch” deployment of ChromeOS devices. The benefit of allowing a reseller to perform managed provisioning is that your ChromeOS devices arrive ready to use. Users are able to unbox their own ChromeOS device or remove the ChromeOS device from the computer cart and are able to be productive without any setup. Of course, ChromeOS devices, like any end-user computing device, do require some setup to associate it to the right management policies in the Google Admin console. This service is provided by many authorized resellers prior to shipment.

The reseller or other organization providing ChromeOS devices managed provisioning in their staging facility can be given a non-administrator user account on your Google Admin console domain for enrollment. In fact, this account can be placed into an organizational unit that has all services disabled.

The actions performed by a service partner in a *managed provisioning* service may include:

- Updating ChromeOS version
- Enrolling into ChromeOS device management
- Validation of policies, including pre configured Wi-Fi networks
- Asset tagging
- Laser etching

- Bundling of peripherals

Please contact your Google ChromeOS device reseller for further details or if you do not have a partner you can search for a Google Cloud partner in your area.

Management

As an IT admin for a business or school, you can manage ChromeOS devices from the cloud-based Google Admin console. Within the Google Admin console you can configure over 600 policy settings such as Wi-Fi settings, selecting apps to be pre-installed, and forcing devices to auto-update to the latest version of ChromeOS.

Check out this video for a quick introduction to the Google Admin console.

Set up accounts

Admin accounts

The Google admin console requires that at least one user in your organization be a super administrator, this account has access to all features in the Google Admin console and Admin API and can manage every aspect of your organization's account, it is recommended to have at least two super administrators to avoid account lockouts.

Additionally, you can create custom roles for admins who will have a reduced access to the Google Admin console and even assign them to specific organizational units so they can manage only the devices and users registered under their OU.

Enrollment accounts (optional)

You can use a non-administrator account to enroll ChromeOS devices and additionally, choose to have your devices placed in the OU your enrollment user belongs to.

By default, when a device is enrolled it is placed in the top-level organizational unit, to change this go to Devices > Chrome > Settings > Users and Browsers and look for the policy “Device enrollment”.

User accounts

If you plan to have your users sign-in to their devices you will need user accounts, you can add one user at a time, or in bulk, furthermore, you can setup Single Sign-On for your users, and configure user auto-provisioning from Entra ID (formerly Azure AD), sync data with your LDAP server, and sync passwords with your Active Directory.

For Kiosk mode and Managed Guest Sessions, user accounts are not required.

Define organizational units and policies

Once you're managing users using the Google Admin console, you can set device and user policies by organizational unit from the Chrome management section of the Google Admin console:

- Access Chrome management via Devices > Chrome

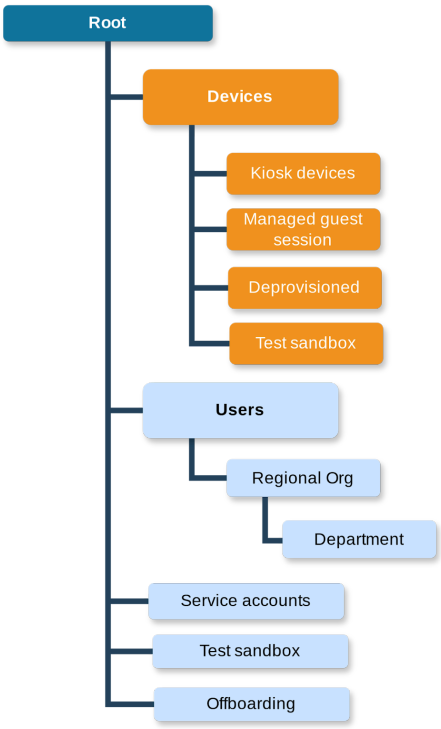
Define an organizational structure if you want to customize services access or settings for different users or devices and take a moment to understand the differences between the different types of policies as this will allow you to create a more dynamic Organizational Unit structure. Learn more about user and device policies.

Device-level settings apply for anyone who uses the device, even if they sign in as a guest or with a personal Gmail account, these policies can also apply to devices in Managed Guest session mode and Kiosk mode. Here you will find settings like auto-update policies, forced re-enrollment, sign-in screen policies, kiosk power settings, power and shutdown, and much more.

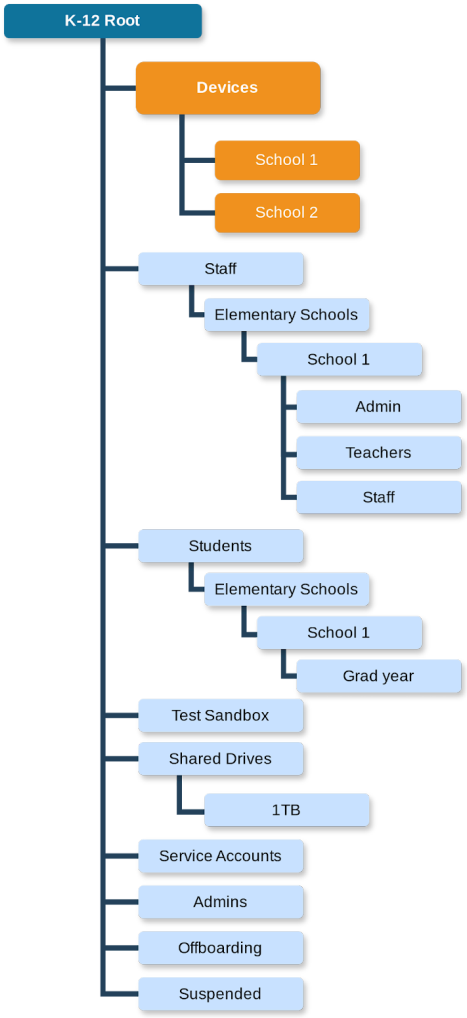
User settings are enforced anywhere your users sign in, including enrolled and unenrolled ChromeOS devices. These settings include the ability for you to set security policies, user experience, control what users can download and access, and much more. For more information, see set Chrome policies for users and browsers.

A user's organizational unit determines which services and features are available to that user. Learn how the organizational structure works and decide on your organization's OU structure, some best practice examples can be found below:

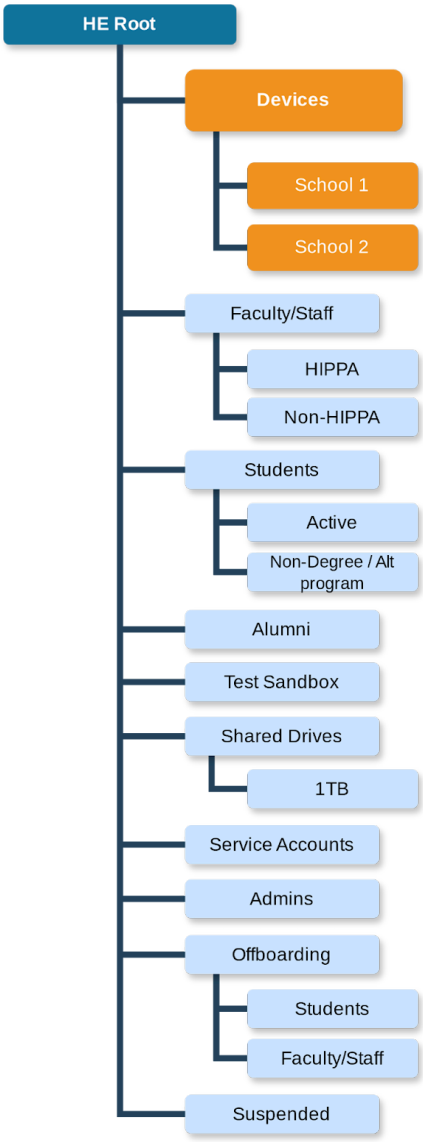
Enterprise example



K-12 Education example



Higher education example



Best practice: Splitting your Devices and Users into separate OUs gives you more flexibility, allowing you to apply Device policies independently of the user profiles and policies you have.

The organizational structure in your Google Admin console only controls which services and features are available to users. You can build this structure to match your LDAP structure, however it is not necessary to do so, your Google organizational structure can follow a different design depending on your needs.

If you do want to replicate your LDAP organization in your Google Admin console's organizational structure, you can do so using our Google Cloud Directory Sync tool.

In addition to ChromeOS policies, Chrome Enterprise Core and Chrome Enterprise Premium allow you to manage your browser policies for signed-in users. Learn how to enroll browsers, and enforce policies for all users using Chrome on devices like Windows or MacOS.

Key policy considerations

ChromeOS devices can be configured to work in nearly any school or enterprise environment. When deploying ChromeOS devices, you (as the administrator) can control the Wi-Fi network access, web filtering, pre-installed apps, and a variety of other things through:

- Device Policies—Can be used to enforce settings and policies on your organization's managed ChromeOS devices regardless of who signs in. For example, you can restrict sign-in to specific users, block guest mode, and configure auto-update settings. Learn more.
- User Policies—Can be used to enforce settings and policies on your organization's users, regardless of which ChromeOS device they're using. For example, an IT administrator can pre-install apps for specific users, enforce Safe Browsing, set up Single Sign-On (SSO), block specific plugins, block-list specific URLs, manage bookmarks, and apply dozens of other settings to users across your organization. Learn more.
- Managed Guest Session Policies—Can be used to configure settings for shared devices in your domain. Managed Guest Sessions allow multiple users to share the same ChromeOS device without the need to sign in or authenticate. You can enforce settings, such as logging the user out after a specific amount of time.
- Kiosk Policies—Kiosk apps have additional special privileges to control device-wide settings such as restricting IME features and network settings of the device. Kiosk apps run a single Chrome app full screen and do not allow switching to another application. Common use cases include standardized testing applications for schools, digital signage displays, and single purpose devices used in retail kiosks, call centers and VDI thin clients.

To set the correct settings for your business:

1. Make a note of how you want the model ChromeOS device to be set up for your environment.
2. Set those same settings as policies in the Google Admin console using a single organizational unit for testing.
3. Once the settings (such as default page to load upon startup, web apps to be preinstalled, or URLs to be blocklisted) have been set and verified on ChromeOS devices in that organizational unit, you can replicate

those settings across the domain.

ChromeOS devices automatically enroll at the top-level organization. Learn how to add an organizational unit to apply custom policies to different user cohorts or device groups and move a ChromeOS device to different organizational units. Alternatively, you can leverage the enrollment technique explained before in this document to have devices enroll directly into the organizational unit you need them in.

Apps and extensions

You can view and configure applications and extensions at Devices > Chrome > Apps and Extensions. Choose the Web, Android*, or Chrome apps that pertain to your users, such as Gmail Offline or Google Drive, automatically install apps, pin them to the taskbar and block-list or allow-list apps if you need more control over which apps and extensions can be installed by users from the Chrome Web Store or the Play Store.

Removal of pre-installed apps: you can remove pre-installed applications by adding them to the list here and selecting “Block”. Note that for your already signed-in users to see this change, they will have to remove their account and add it again to the device, all users signing-in for the first time to a device will see this change immediately.

**Android apps are only available for signed-in users on ChromeOS devices. Not available on ChromeOS Flex devices or devices in Managed Guest mode or Kiosk mode.*

Recommended settings

In the Google Admin console under Devices > Chrome > Settings, you can access many policies under User and Browsers, Device, and Managed Guest Session settings.

- Filter for a setting by typing in a keyword > Enter in the “Search or add filter” section.
- Settings can be locally applied per Organization Unit or inherited from the top domain for ChromeOS, Browser (Windows, Mac and Linux), or Android devices.
- You can check the policy inheritance directly in this view through the “Inheritance” column and you can also use the Inheritance filter in the search bar to review only policies applied locally or those Inherited.
- The icons in each setting confirm where the policy is applied: ChromeOS devices, Browser for Windows, Mac and Linux, Android devices, iPhones and iPads.

- Click on each policy to learn more about it, the values available and their effect.

Although most organizations go with the defaults, below are popular settings some organizations customize.

Forced re-enrollment	Google recommends that you don't turn this setting off. This setting forces a wiped device to re-enroll into your domain. If you don't want a ChromeOS device to re-enroll in your domain, you should deprovision the device. Learn more about forced re-enrollment.
Idle settings: Screen Lock	Select to automatically lock screen on idle or lid close to increase security and reduce likelihood of someone using your users' computers while they're away. You can also add a screen lock delay for when the device is on AC and Battery.
Pages to Load on Startup	This is commonly set to an intranet portal or homepage. The downside is that once set, ChromeOS devices no longer restore the tabs from the most recent browsing session upon restart.
Sign-in restriction	Restricting sign-ins to **@yourdomain.com* prevents users from signing in with a consumer Gmail account or another non-domain account. You can control who is allowed to sign in to a managed (enrolled) ChromeOS device.
Auto-update settings	Leave the auto-update settings to their defaults. ChromeOS devices self-update every 4 weeks, bringing new features, bug fixes, and security vulnerability patches. We also recommend you keep 5% of your organization on the Beta or Dev channels to test how future ChromeOS releases work in your organization. See a full list of recommendations in deploy auto-updates for ChromeOS devices and ChromeOS release best practices. Note: To stop background downloading of updates before the device is enrolled and rebooted, press Ctrl+alt+E on the End User License Agreement screen. Otherwise, downloaded updates that should have been blocked by policy might be applied when the user reboots the device.
Single Sign-On	For organizations using Single Sign-On (SSO), test to make sure a small number of your users can sign in to their ChromeOS devices before rolling this out to your whole organization. Check the full guide on how to configure SAML Single Sign-on (SSO) for ChromeOS devices and how to set up Single Sign-On (SSO) and user provisioning between Microsoft Entra ID and ChromeOS.
Security	The *Elevating Security config guide* provides a set of recommended policy settings to maximize the security of your devices and users.

Additional considerations

Printing

The Google Admin Console offers a comprehensive suite of functionalities for the administration of printing within an organization. These functionalities empower administrators to exert control over access to printing devices, print servers, and setting up printing partners.

- Printer Management: Administrators are granted the ability to add, remove, and configure printers, which includes the specification of printer names, locations, and access authorizations.
- Manage printer servers: Administrators can add, remove CUPS print servers from the Google Admin console.
- Setup printing partner: Administrators can set up the printing services provided by a printing partner by creating an Internet Printing Protocol (IPP) based print queue to send print jobs via the network or adding the printer using an extension.

Chrome management APIs

Admins can leverage Chrome Management APIs to programmatically interact with their environment, automating, scaling and exporting information, below are some of the most common ones.

Chrome Management Telemetry API

This API allows you to monitor the operation and health of devices running ChromeOS, and obtain information such as the status of the battery, CPU, storage, memory, networking, updates, audio, wifi strength and more as well as telemetry events coming from your devices. For more information and to see code samples and test the API check out the Telemetry API guide.

Directory API

This API allows you to manage ChromeOS devices by obtaining identifying device information and performing actions such as moving, updating, deprovisioning and disabling. See the directory API guide for more details.

Chrome Policy API

The Chrome Policy API allows Chrome admins to view and manage Chrome policies programmatically, making it possible to list policies applied, modify, and delete them. For more information, common use cases and code samples see the Chrome policy API guide.

GAM

GAM (Google Apps Manager) is an open-source command-line tool that allows administrators to manage ChromeOS and other Google Workspace services from the command line. GAM can be used to perform a wide range of tasks, including:

- Managing user accounts
- Managing devices
- Configuring Chrome policies
- Reporting
- etc

GAM is a powerful tool that can be used to streamline the management of ChromeOS and other Google Workspace services. It is especially useful for organizations with a large number of ChromeOS devices or users.

Key Features of GAM

- Cross-platform support: GAM is available for Windows, macOS, and Linux.
- Command-line interface: GAM's command-line interface makes it easy to automate tasks and integrate with other systems.
- Extensive documentation: GAM has extensive documentation that makes it easy to learn how to use the tool.
- Active community: GAM has a large and active community of users who are willing to help others.

Benefits of Using GAM

There are many benefits to using GAM, including:

- Increased efficiency: GAM can help administrators to automate tasks and manage ChromeOS more efficiently, allowing the creation of scripted tasks and bulk operations.
- No Cost: it is open source and has no cost.

Apps Script

Apps Script is a Google Library of serverside javascript. It can be used with Google APIs to automate actions. It works well in association with Google editors like Google Sheets. Apps Script can be used in ways like GAM with more flexibility to interact with other APIs. Apps Script is offered at no cost.

Data Loss Prevention

Data Loss Prevention (DLP) identifies signals and implements rules: clipboard actions, screen sharing, printing, e-privacy screens, etc. DLP restrictions can be applied by individual URL (for web apps) and by type (Android, Linux and VDI). Policies are enforced on the device based on rules, in both online and offline situations.

DLP actions

With DLP, specific actions are blocked | allowed | reported based on pre-specified rules.

- Block: users cannot take action.
- Warn: user is asked to confirm if they want to proceed despite risks.
- Report: user is not blocked from taking action; action is reported to admin.
- Allow: user is allowed to take action: action is not reported to admin.

DLP Functionality

- Clipboard, Screen capture, Screen sharing, Printing and ePrivacy restriction
- Integration with the security investigation tool
- Managed users and Managed guest sessions
- Any ChromeOS device

Some things to note:

- Source can only be a URL. Patterns supported.
- Kiosk mode is not supported.
- Android, Linux VDI treated as one blob for example I can restrict copy/paste from a URL to all Android or VDI apps but not individual ones.

To configure DLP, refer to this article.

ChromeOS adoption and change management

Introducing new technology and embracing change can be difficult. This is why incorporating change management methodology into each phase of the ChromeOS deployment project empowers customers to meet project objectives, deliver on time and within budget. Organizations must take the time to assess their user groups and training needs for each cohort. Cohorts typically have specific training needs by use case to understand how their work will be changing.

Our primary goal is to establish a structured approach to manage the people-side of ChromeOS adoption. A structured change management plan ensures employees:

- Understand the benefits of using ChromeOS devices
- Possess the knowledge, skills, and ability to use ChromeOS devices
- Adopt ChromeOS devices to achieve business objectives

Share the Chromebook Employee Adoption Kit for step by step guidelines to encourage deployment success.

Applying change management will enable the team to proactively identify and address challenges that have the potential to derail the project and keep focus on setting the vision for success. We like to think of change management in four stages:

Excite

- Engage stakeholders
- Build sponsorship, define scope, and plan your support model, communications, and training

Enable

- Deploy services
- Deploy services and execute on support model, training, and communications plans

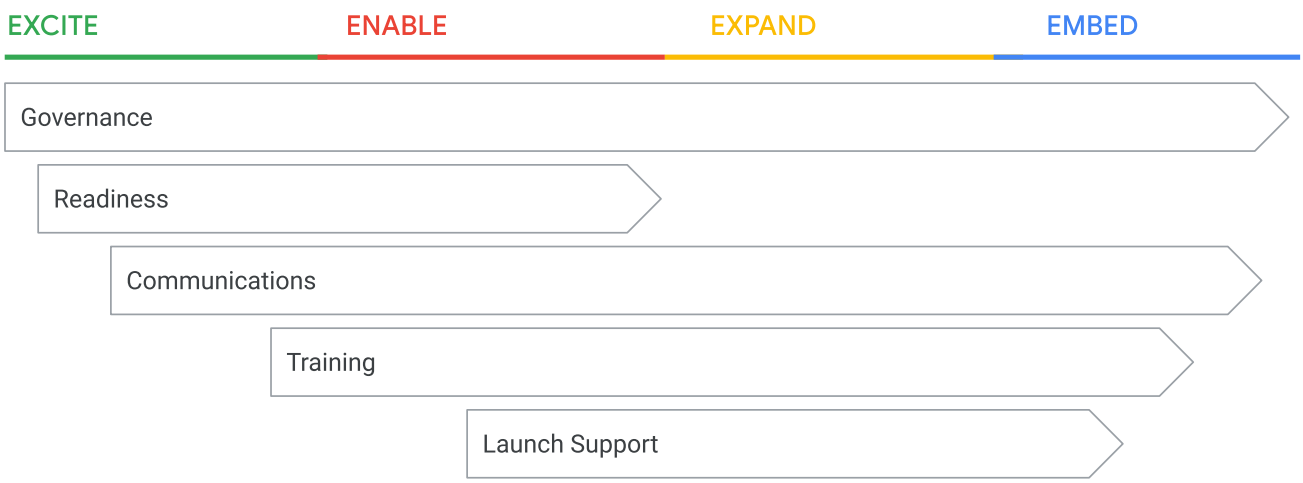
Expand

- Grow adoption
- Establish a Google team, run Transformation Labs, and manage support operations

Embed

- Measure and promote successes

- Measure adoption progress, promote success stories, and support users through self-help
- Adoption and change management workstreams



ChromeOS deployment workstreams

Technical Configuration

- Ensure users have best possible experience
- Identify integration points
- Enable early troubleshooting of technical challenges

Project Management

- Keep project on track
- Organize resources
- Ensure stakeholder alignment
- Manage Go-Lives

Change Management

- Reduce organizational switching cost
- Ensure users are fully leveraging product capabilities
- Provide appropriate training and support materials
- Develop a positive buzz

Supporting users through change

Governance	• Establish a change leader to be the face of change • Select and train “ChromeOS Champions” to lead the way • Lead by example i.e. Senior management
Readiness	• Identify appropriate user and use case cohorts • Assess the impact of change by cohort • Define change management success by cohort
Communications	• Identify communication needs by cohort • Develop communication plans for all cohorts • Execute campaign
Training	• Identify training needs by cohort • Create a curriculum and deliver training for each cohort • Build printable user guides and internal ChromeOS site
Launch Support	• Identify communication needs by cohort • Develop communication plans for all cohorts • Execute campaign

Governance

Who internally will be responsible for this project being a success?

Establish a Change Leader to be the face of change. Leadership and engagement creates a unified vision for change, inspiring and motivating employees to accept change. Active, visible leadership is the number one criteria for a successful deployment.

Attributes of a good sponsor

- A senior member of the business to be the face of change (not IT)
- Someone who will lead by example
- A well known, respected and influential individual within the organization
- Ability to actively provide support throughout the project

Roles and responsibilities

- Sign-off on the project “elevator pitch”
- Announce the project to the organization
- Align leadership teams around project goals, efforts and messages
- Address leader or employee resistance
- Celebrate project successes

Tips for success

- Active, committed, and visible executive sponsorship is critical for success and improves employee engagement and maximizes employee buy-in

Support the Go-Live: ChromeOS Champions

ChromeOS Champions are designed to improve the onboarding experience and promote user adoption. The program ensures a fast, manageable Go-Live by offering peer-to-peer support for users switching to ChromeOS.

Recruit a network of ChromeOS Champions

- Tech savvy employees excited about ChromeOS and willing to champion adoption
- Will provide peer to peer support during roll out
- Form part of the Innovation Council post Go Live to ensure product adoption
- Aim for at least one person per physical location

Roles and responsibilities

- Get trained and proficient on ChromeOS devices early
- Understand the changes the organization will go through to use ChromeOS
- Rally enthusiasm among colleagues and collect feedback and questions
- Provide peer-to-peer support during Go-Live (floor walking, Q&A sessions, etc.)
- Help maintain internal FAQs, helpful information and tips and tricks.

Readiness

Who are your users and what are your use cases?

Confirm all the ways your organization will use ChromeOS devices as identified during initial project scoping. Understanding your organization's use cases allows you to create the necessary content for communications and training assets.

Examples:

- Computing
  - Chrome and web applications only (cloud driven)
  - Desktop virtualization
    - Utilize existing virtualization infrastructure
    - Build out new virtualization infrastructures
- Digital signage and Kiosk
- eLearning
- Managed guest sessions

Identify cohorts for change management

Identify the users in your organization switching to ChromeOS and group them together by their applicable use case(s). Knowing your user groups and their needs ensures that you send the appropriate communications and training to the right users. It is recommended to have ChromeOS Champions support for every identified cohort.

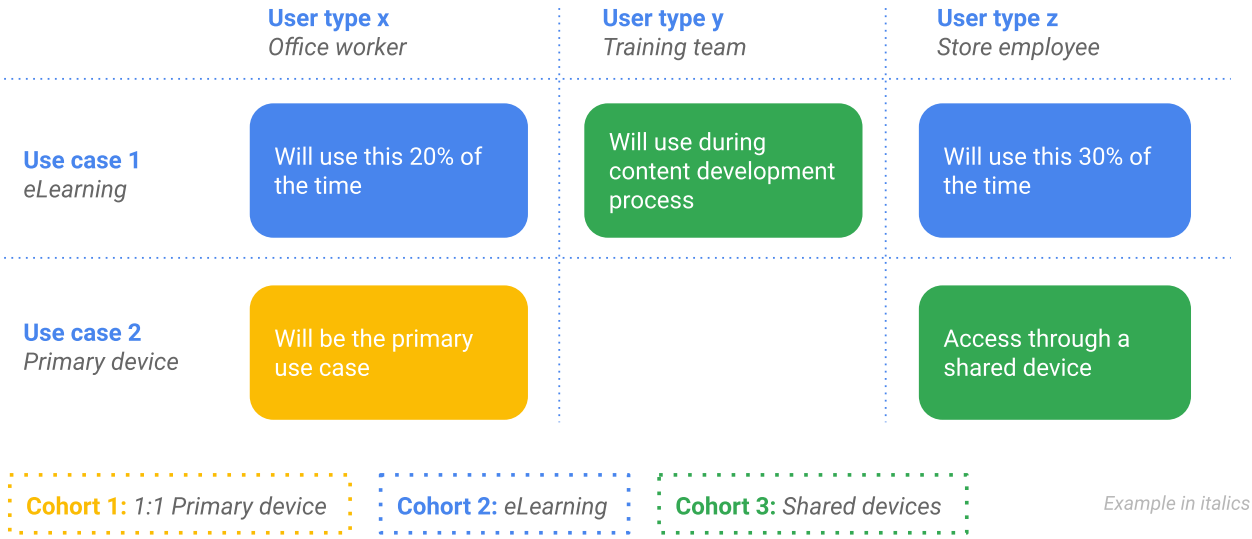
Examples:

Users
- Executive
- Admin staff
- IT administrator
- Manager
- Worker
- End User Support

Use cases
- Computing
- Desktop virtualization
- Digital Signage
- Kiosk
- eLearning
- Managed guest sessions
- Device Management
- Chromebox for Meetings

Cohorts
- Manager, Worker, Admin staff - Computing
- Worker - Digital Signage
- IT Admin - Device management

Map out cohort



Change impact assessment

Consider which work activities will be changed by using ChromeOS devices. List out activities and workflows that will be changed or newly created by using ChromeOS. Understanding the impacts ChromeOS devices have on work life allows you to create the necessary content for communications and training assets.

Do a cohort analysis for change impact

Identify cohorts in your organization affected by major changes in the way work will be done. Knowing your cohorts and their change impact ensures that you provide the appropriate communications and training curriculum to the right users.

Examples:

- Application compatibility (and what to do when there is a gap)
- Administration policy mapping / alternatives
- Cloud file management, i.e. Google Drive
- Printing
- Peripheral compatibility

- Device sharing
- Support / help desk

How will you measure the success of deployment?

Set benchmarks

Clearly define how you will **measure the success of ChromeOS before you start** so that you can track things as you deploy. Tracking metrics provides a way to detect problems early and course correct if needed. Identify key metrics that tie back into why the organization bought devices in the first place.

Examples:

- Training and education data
- Number of participants in training
- Number of help-desk tickets vs. before
- User survey data
- User readiness survey data
- Deployment happiness survey data
- Employee business data
- Average cost or performance per employee

Communications

How will your users become aware of the change?

Plan your communications

There is no such thing as 'over communicating' during change, and there are a myriad of resources to help get the message out.

Send the right message to the right person

- Communications should be customized for different cohorts, answering the questions that they care

about

- Communications should be relevant to the recipient so users understand how switching to ChromeOS will improve their work
- Reduces risk related to users acceptance of ChromeOS
- Utilize the change management cohort analysis to create communications content pertinent to each cohort

Send the right message via the right channel

Identify the right communication channel(s) to reach users within the organization, and evaluate effectiveness of each communication.

For example Email, Internal collaboration, User guides, Internal Website, Groups, Chromebook how-to videos

How will you communicate change to your organization?

Develop a communication campaign that aligns with deployment

Sync communications with the rollout in order to deliver the greatest impact and drive desired behavior.

Inform and excite your users

Investing in communications and multiple communication channels builds employee awareness of and excitement for adopting ChromeOS.

Reinforce key messages to drive lasting adoption

Continue engaging with users to provide updates, tips and tricks, and share adoption stories.

How will you execute to generate momentum?

Create an elevator pitch

- An elevator pitch quickly and succinctly explains why the company is moving to ChromeOS
- It identifies the benefits of using ChromeOS and ties these into the vision and strategy of the organization

- The elevator pitch embodies the company's vision of going ChromeOS
- It should be compelling and relevant to users

Embody the elevator pitch in everything

Incorporate the messaging of the elevator pitch in all of your communications materials to reinforce the message.

Brand your campaign

Naming your ChromeOS project ensures the project is visible and easy to communicate.

Cultural change

Excite your employees to drive momentum for change

- Contests to encourage initial adoption
- Support internal adoption communities

Training

Projects are most successful when multiple training formats are used

- Use an experienced partner to deliver training
- Leverage existing Learning and Development team for assistance to schedule and coordinate
- Schedule 50% of training classes after launch
- Define Compulsory and Optional Training

What training will be required for users in your organization?

A thorough training needs assessment ensures users become proficient in ChromeOS, increases user adoption and reduces the risk of significant disruption during the transition period.

Check our Productivity and Collaboration blog and How To Chromebook site for the latest tips and tricks!

Do a training needs assessment

Utilize the Organizational Analysis to document training needs for each cohort. Cohorts are likely to have specific training needs by use case to understand how their work will be changing. A thorough training needs assessment **ensures users become proficient at ChromeOS, increases user adoption, and lowers the risk of significant disruption** during the transition period.

Examples:

Internet Explorer migration - all users

Internet Explorer		Chrome
• UI / Shortcuts • Add-ons	→	• UI / Shortcuts • Themes • Extensions / Chrome Web Store • Migration / Chrome Sync

Chromebook basics - all users

Windows / Mac		ChromeOS
• UI / Shortcuts • Accounts • Software Mapping • Data Storage • Software Updates	→	• UI / Shortcuts • Accounts / Device Sharing • Find apps / Chrome Web Store • Cloud / Offline Data Storage • Auto Updates • Migration / Chrome Sync

Using VDI in ChromeOS - users with legacy app requirements

Implementation		Using VDI Applications

• Providers
• Viewer Apps
• Requirements
• Configuration
	→	• UI / Shortcuts
		• Workflow Changes
		  ◦ Login / App Access
		  ◦ Data Access

File Management - all users

Local Storage		Cloud Storage
• UI / Shortcuts • File Management	→	• UI / Shortcuts • File Management / Search • Collaboration / Sharing • Local / External Storage

Chromebook and peripherals - users who depend on the use of peripherals

Windows / Mac Peripherals		ChromeOS Peripherals
• Drivers • Configuration • Printing	→	• Compatibility • Configuration • Google Cloud Print

Google Admin console - IT administrators

Current IT Administration		New IT Administration
• Active Directory • Policy via GPO • Single Sign-OnSSO • Software Updates	→	• Organizational Units • Policy via Google Admin console • Networking • SSO sync with GCDS • Auto Update Policies

App Development - content creators

Windows / Mac Dev		Chrome Dev
• OS Dev Platforms		• Chrome Development

• IE Web Dev • Distribution	→	• Chrome Web Store • Third party platforms (content management)

What is your training approach for ChromeOS?

Create a training curriculum

Use the Training Needs Assessment to identify the appropriate training channel(s) and ensure training resources are readily available for your users.

Traditional types of training

Self-paced eLearning	Remote instructor-led training	Classroom training
• Scalable, content is standardized • Typically lower cost than instructor led training • Minimal requirements for logistics • Accessible anywhere at anytime	• Scalable, content is customizable • Typically low to medium cost • Medium requirements for logistics • Accessible anywhere at specific times • Requires partner or customer training resource to facilitate	• Less scalable, content is customizable • Higher requirements for logistics • Requires partner or customer training resource to facilitate • Typically higher retention and impact

Modern Training Formats

Lunch and Learn

- Scalable. Content is standardized
- High retention and impactful
- Boosts employee morale
- Can be in-person or remote

Enhanced device collection process

- Can be in-person or remote
- Build a simple collection process where users attend a small number of dynamic training sessions targeting

key points as they queue up to collect their new device

- Ensures everyone gets a minimum amount of training before they start their device
- Can also include post-collection steps to ensure that the device is configured/enrolled and working properly

Drop-in Expert bar

- Experts available on request to provide help when needed
- Can be temporarily deployed to support a new change and/or permanently integrated into an existing support capability

Tips for success

- Facilitating users gaining comfort with ChromeOS devices is essential to user acceptance. Offer ChromeOS light-night sessions, training sessions, and self-paced training materials prior to Go-Live to familiarize users with ChromeOS devices to improve user experience during transition.

Support the Go-Live

Make the Go-Live a fun experience and utilize ChromeOS Champions to perform floor walking, peer-to-peer support, updates with the project team, and escalate any issues.

- Go through one or two dry runs of the deployment process before deployment - refine the checklist as needed
- Verify that a select group of users can sign-in
- Get the Early Adopters to become Champions for the full rollout - this generates excitement and helps with staffing up the initial support model

Launch Support Checklist

- ❑ Create onboarding experience
- ❑ Day 1 user checklist
- ❑ Engage ChromeOS Champions
- ❑ Seek feedback
- ❑ Address impacts

Create an onboarding experience

- Create advocates by planning a fun and positive experience during user transition
- Consider whether they run their old hardware for a parallel period, or whether there is a swap
- Allow for users to test Chrome browser for a certain period before launch to ease with transition (Note that this helps getting users 100% migrated to cloud working but creates additional step)
- Provide the appropriate accessories to enable them for success such as:
    - Monitors / Compatible docking stations / Mobile display/ USB adaptors
    - Protective cases
    - Privacy filters for users that travel
    - Managed provisioning for the devices to ensure they are ready to use out of the box

Engage ChromeOS Champions

Ensure that the ChromeOS Champions are active and visible during go-live, and encourage them all to:

- Walk the floors helping people out
- Be visible with some kind of branding
- Drive healthy discussion on enterprise social platforms
- Track issues and provide feedback to the project team

Seek feedback through multiple channels

- Feedback from ChromeOS Champions
- User surveys
- Monitor enterprise social platforms and provide answers to the feedback in a structured way
- Decide on the forum to address questions and issues and ensure this is well publicized
- Demonstrate that feedback is being listened to and acted upon

Supporting “going ChromeOS”

Encouraging an internal community for self-support

ChromeOS champions program

Encourage an internal support program to help employees help employees. Leverage Google Guides to create a program for ChromeOS Champions. ChromeOS Champions are voluntary based employees who assist end users and form a team to advocate for end user questions. Creating such a program reduces the number of Support issues handled by IT support teams, essentially creating your own version of Tier 1 help-desk support.

Schools can create such programs with students. Some OEMs offer a Chromebook Repair program supporting technical education with students. Students work as Tier 1 support and repair Chromebooks.

Incentives for those ChromeOS Champions who take the most tickets or answer the most questions can be rewarded in the form of employee of the month, gift cards, or for expert level: premium chromebook.

Promote long term adoption

- Call out adoption successes early on during the change process
- Ensure that the benefits being realized are communicated back to the user base, quantify the benefits as much as possible
- Ensure that ChromeOS is now embedded as the “normal” way of working. Make sure that this includes updates to processes such as “new joiners” who will have missed the initial onboarding education phase
- Consider creating a switcher program to encourage users to trade in their old device for a chromebook with an option to switch back.

Tips for success

- Keep proactively reminding the community of users of the ChromeOS initiative and make information easy to access and consume

Still need help?

Get Support

- Check out our support page
- Refer to our Chrome Enterprise Help Center and Community
- Check out our Chrome Enterprise “How-To” Demos
- ChromeOS device Tips and Tricks for end users
- Sign up and follow Chrome Enterprise release notes
- Chrome browser downloads and Chrome Enterprise product overviews — Chrome browser for enterprise
- Are you a partner? check out our Chrome OnAir webinars
- Review and share the Chromebook Employee Adoption Kit

Self-support tips

- In your Chrome browser, visit: chrome://settings/help.
- How to collect ChromeOS device logs
- Fix Chromebook problems (for end users)
- Known issues (Chrome Enterprise)
- Log Analyzer (Google Workspace Toolbox)—Analyze /var/log/messages and /var/log/chrome/ for errors

Additional resources

- Chrome browser Enterprise Support—Review how to get Chrome support for your organization
- Chromebook Help Center and Community
- Announcements: Follow the Google Chrome blog, the Chrome releases blog and the Chromium Blog
- ChromeOS update tracker, Chrome Platform status and Chromium data (releases, schedules)
- Developers: Learn about changes to the web platform and follow the Chrome for Developers Youtube channel