

# Getting Started with Chrome Enterprise

## Table of contents

**Congratulations on kicking off your Chrome Enterprise journey! 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 super excited to help you transform how you work. In this guide, we will walk you through how to get started with Chrome Enterprise!**

Table of contents	2
Introduction	3
<b>Deployment: methodology and best practices</b>	4
Deployment methodology checklist	4
Deployment project kick-off	5
Start with the people-side of change	5
<b>Connectivity</b>	6
Manage network profiles	6
Configure Wi-Fi	7
Add Wi-Fi configuration on the device level	7
Wi-Fi setup	8
802.1x deployment	8
Web filtering	9
<b>Device setup and enrollment</b>	10
Paths to Chrome Enterprise enrollment	10
Prerequisites	11
Enrollment	12
Verify enterprise-enrolled devices	14
White Glove Prep Enrollment Service	14

<b>Management</b>	16
Set up accounts and Chrome OS policies	16
Define organizational units and policies	17
Key policy considerations	18
Recommended settings	19
<b>Chrome adoption &amp; change management</b>	21
Chrome deployment workstreams	22
Supporting users through changes	23
Governance	23
Readiness	25
Communications	27
Training	29
Supporting 'going Chrome'	34
<b>Still need help?</b>	35

# Introduction

Thanks for checking out our Getting Started with Chrome Enterprise guide! You may be here for a few reasons, either you have purchased or are interested to purchase a Chrome Enterprise device or a Chrome device and Chrome Enterprise Upgrade.

Lets get some definitions out of the way:

A ***Chrome device*** (Chromebook, Chromebase, Chromebox) is a computing device that runs Chrome OS, an operating system designed for the Cloud developed by Google. What makes these devices unique is that they run in a pure web environment—they automatically update—you don't have to regularly install patches or re-image machines regularly. They boot quickly and have several security features built in.

***Chrome Enterprise Upgrade*** comes included with Chrome Enterprise devices and is available to be purchased for any Chrome device. Chrome Enterprise Upgrade unlocks the built-in business capabilities of Chrome OS for IT to secure, orchestrate, and power the cloud workforce. The upgrade includes advanced security to keep corporate data safe; ensures flexible access to resources regardless of use case; and simplifies orchestration of Chrome devices and other critical infrastructure.

A ***Chrome Enterprise device*** (Chromebook Enterprise, Chromebase Enterprise, Chromebox Enterprise) combines the end user benefits of Chromebooks with the business capabilities of Chrome Enterprise Upgrade and Chrome OS for IT to securely power their cloud workforce. It is a business-focused solution for Chrome devices, Chrome Browser, and Chrome OS. Chrome Enterprise offers cloud-native tools, integrations with third party products, and 24/7 support for IT administrators.

Chrome Enterprise devices can be centrally managed by the [Google Admin console](#). 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 Chrome apps and extensions, and more. With Chrome Enterprise, IT is set free to power their cloud workforce to work securely and effectively from anywhere.

This guide will help provide step-by-step instructions on how to make your purchase, set up your Chrome Enterprise account, enroll devices, share Chrome Enterprise deployment methodology, policy setup, change management, the people-side of change management, best practices, and what to expect along the way.

Note: The recommendations for deploying Chrome 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 contact us at [ask-chrome-channel@google.com](mailto:ask-chrome-channel@google.com)

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 buckets. 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 '[White Glove Preparation](#)' will be covered by "[Device Set-Up and Enrollment](#)."

### 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

### White Glove preparation

- Update Chrome 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 Chrome into their work habits and processes. A successful Chrome deployment blueprint incorporates change management at every step of the Chrome 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 Chromebook 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 Chrome devices?
3. How will work be impacted by switching to Chrome devices?
4. Will Chrome be the primary device or browser?
5. How will you measure the success of the deployment (e.g. 50% of users deployed in 30 days)?
6. How will your users be aware of the shift to Chrome devices?
7. How will you train your users to use Chrome devices?

### An effective change management plan ensures:

- Users understand why using Chromebooks 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 Chromebook
- Users make the personal decision to adopt Chromebooks
- Ongoing engagement and support for users and IT admins

Documenting answers to these questions and following guidance in the [“Chrome Adoption & change management”](#) section below will help you accelerate Chrome Enterprise 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.

## Key features

Chrome devices support all of the most common Wi-Fi protocols: WEP, WPA, WPA2, EAP-TLS, EAP-TTLS, EAP-PEAP, and LEAP. Additionally, some Chrome 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 Chrome 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 app](#) on an Android 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 Chrome devices have access to required URLs.** Chrome 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, see [Enterprise networking for Chrome devices](#).

## Manage network profiles

Wi-Fi networks can be manually added to a Chrome device at any time, but Google recommends using the [Admin console to push Wi-Fi profiles](#). These profiles are downloaded and applied to the Chrome device during the enrollment process. Updates to Wi-Fi network profiles also get pushed during the automatic policy refresh on the Chrome device. The advantages of using the 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 Chrome device customers use WPA2-PSK for simplicity of setup. However, Chrome devices can work in a variety of educational and enterprise environments, including complex Wi-Fi deployment scenarios that require client certificates, 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 on the device level

To apply different settings to a set of users or Chrome 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 Chrome 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” box in the “restrict access to this Wi-Fi network by platform” section. Find additional technical details for network setup [here](#).

ORGANIZATIONS
SETTINGS for Chrome Enterprise Love

---

▼ **Chrome Enterprise Love**

- ▶ Customer Training
- ▶ Deprovisioned Devices
- Device Enrollment
- Test
- ▶ Trusted Testers

### Add Wi-Fi network

**Name**
[Help](#)

**Service set identifier (SSID)**

This SSID is not broadcast

Automatically connect

**Security type**

None ▼

**Proxy settings**

Direct Internet C ▼

**Restrict access to this Wi-Fi network by platform**

This Wi-Fi network will be available to users using:

Mobile devices

Chromebooks

Google meeting room hardware

**Apply network**

by user ▼

Users in this Organizational Unit will automatically get access to this network when signed in.

[ADD](#)
[CANCEL](#)

## Wi-Fi setup

It's often easiest to use an open or unfiltered network to enroll Chrome devices and have a first sync of the management policies. This setup allows the Chrome 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](#).

## 802.1x deployment

Chrome devices support 802.1x authentication. Contact your networking vendor to see how to set up [Chrome devices with client certificates](#). For example, [ClearPass Onboard](#) by Aruba Networks is an extension that handles Chrome device onboarding and installs the certificate in a secure manner.

Google Cloud System Administrators and Partners can find documentation for advanced 802.1x enterprise WiFi network configuration on [Google Cloud Connect](#).

For more information on this topic, see [Manage client certificates on Chrome devices](#).



## 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. See [this list of hosts](#) which must be exempt from SSL inspection.

To get Chrome 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 Chromebooks.

# Device setup and enrollment

If you are deploying a small number of devices, see the [Chrome device Quick Start Guide](#). If you're deploying Chrome Enterprise devices to a larger group or [mass enrolling devices](#), such as multiple office locations, see the instructions below.

## Paths to Chrome Enterprise enrollment

### If you don't have a Chrome Enterprise device

You'll need to [purchase Chrome Enterprise Upgrade](#) or have a Chrome Enterprise device to manage from the [Google Admin](#) console. You may purchase upgrades for a school or business. Additionally, some regions can [purchase Chrome Enterprise Upgrades](#) online.

- From the [Google Admin console](#), check [how many upgrades you have](#) and how to [manage](#) and [renew annual upgrades](#).
- Please contact your Google Chrome device reseller for further details. If you do not have a partner you can search for a Google [Cloud partner in your area](#).

If you're a new customer:

#### Chrome Enterprise Upgrade

1. Customer purchases Chrome Enterprise Upgrade
2. [Reseller](#) has to process Admin Console account order through Google
3. Google sends welcome letter to customer with Admin Console login
4. Customer must [verify domain](#) (within 12 days of receiving welcome letter)
5. Customer [enrolls](#) Chrome device with enterprise login

#### Chromebook Enterprise

1. Customer purchases Chromebook Enterprise device
2. Customer needs to go to: [g.co/ChromeEnterpriseAccount](#) to create a domain/Admin Console Account
3. Customer logs in and sets up Admin Console
4. Customer must [verify domain](#)
5. Customer [enrolls](#) Chrome Enterprise device with enterprise login

If you are a current enterprise customer (i.e. G Suite)

### Chrome Enterprise Upgrade

1. Customer purchases Chrome Enterprise Upgrade
2. [Reseller](#) sends customer enterprise account details to Google through an order
3. Google sends welcome letter to customer with Admin Console login
4. Customer [enrolls](#) Chrome device with enterprise login

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

- Billing - shows Chrome, Android and G Suite subscriptions
- Device management > Chrome > Devices > click Credit card icon to view upgrade totals

### Chromebook Enterprise

1. Customer purchases a Chromebook Enterprise Device
2. Customer [enrolls](#) Chrome Enterprise device with enterprise login

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 Chrome Enterprise devices you'll need to make sure you have the following in place:

*For IT Admin*

### 1. Google Admin console access

Required to configure Chrome Enterprise user and device policies and enable enterprise 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 Chrome Enterprise management and Google Support access.

## 2. Administrator access to primary domain:

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

- [Click here](#) for help finding your administrator.
- Check out [this video](#) to see how to verify your domain.

## 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 in “[User Management](#).” To verify that the user’s access to the Support Portal has been granted, check login access [here](#). File a ticket with support using [this form](#) if you see an “unauthorized” error.

### *For End Users*

Although Google Identity (G Suite account) isn’t required to use a Chrome Enterprise 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.

Again, if you haven’t already, you’ll need to [purchase Chrome Enterprise Upgrade](#) for each device to manage them from the [Google Admin](#) console.

### *For a large number of Chrome Enterprise devices or deploying with G Suite*

If you plan to deploy a large number of Chrome Enterprise devices or deploy them in conjunction with G Suite for the first time, we recommend that you work with a [Google Cloud partner](#).

## Enrollment

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

### **Update Chrome devices to the latest version**

Devices running Chrome OS 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 use a USB recovery stick with the latest version of Chrome OS.

Updating via USB drives is the most effective and efficient method when imaging hundreds or thousands of Chrome Enterprise devices. Updating via USB is a great way to save bandwidth from each device pulling down a full OS update which can exceed 400 MB per device.

- Navigate to Device management > Chrome > Device settings > Device update settings.

## Create a Chrome OS image

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

1. The Manufacturer and Model information of the Chrome Device you wish to update.
2. A USB 2.0, or above, flash drive of 4 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.

## 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 then STOP
4. *Before signing in to the Chrome device, **press Ctrl-alt-E** to bring up the "Enterprise enrollment" dialog window. Alternatively, you can click "More options" at sign-in to choose Enterprise enrollment.*

### You may be automatically prompted to enterprise enroll your device

Chromebook Enterprise devices preinstalled with the latest update will automatically prompt users to enroll the device with their Chrome Enterprise 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 Chrome devices in your organization. For more information about device enrollment, see [Enroll Chrome devices](#).

**IMPORTANT:** If you forget to enterprise enroll your device, you will need to wipe the device and restart enrollment. For details, see our [wipe Chrome device data](#) instructions.

## Verify enterprise-enrolled devices

From the [Admin console](#), you can search and view enrolled Chrome 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. These device policies are enforced on any Chrome device enrolled for management in your domain.

- Access the **list** of Devices via [Chrome Management > Devices](#)
- Manage viewable columns by clicking on the gear icon (top right of the list)
  - Add Chrome version and model by clicking on “Add new column”
- Click into a device to:
  - Move, disable or [deprovision the device](#)
  - 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

Once enterprise-enrolled, admins can:

- [Wipe Chrome device data](#)
- [Force wiped Chrome devices to re-enroll](#)
- [Repurpose or retire Chrome devices](#)

## White Glove Prep Enrollment Service (Optional)

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

The reseller or other organization providing the Chromebooks white glove prep in their staging facility can be provided a non-administrator user account on your G Suite domain. In fact, this enrollment account can even be placed into an organizational unit that has all services disabled.

The actual steps followed by the white glove prep service may include:

- Updating Chrome OS version
- Enrolling into Chrome OS management
- Validation of policies, including preconfigured Wi-Fi networks
- Asset tagging
- Laser etching
- Bundling of peripherals

Please contact your Google Chrome 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 Chromebooks and other Chrome devices, from cloud-based Google Admin console. With Google Admin console you can configure over [200 policy settings](#) such as [Wi-Fi settings](#), selecting [apps to be pre-installed](#), and [forcing devices to auto-update](#) to the latest version of Chrome OS.

Check out [this video](#) to see what you can do with Google Admin console

See [Subscription options](#) | [Purchase upgrades](#)

## Set up accounts and Chrome OS policies

With the Google Admin console, you can centrally organize and manage your fleet of Chrome Enterprise devices. Once you're managing users using Google Admin console refer to the Chrome management section of the Admin console to set device and user policies by organizational unit.

You can view a list of your Chrome Enterprise devices, search for your devices, and view information about the devices (serial number, enrollment status, support end date, enrollment username, and manually-entered notes, such as location) via the Admin console's 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.

These device policies are enforced on any Chrome Enterprise device enrolled for management in your domain. User policies are enforced anywhere your users sign in, including enrolled and non-enrolled Chrome devices. These settings include the ability for you to set security policies and control what apps users can download and access. For more information, see [Managing Chrome devices](#).

In addition to Chrome OS policies, Chrome Browser Cloud Management allows you to manage your browser policies for signed-in users. [Learn how to enroll browsers](#), and enforce 100+ policies for all users who open Chrome on managed devices.



## 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 Admin console:

- Access Chrome management via Devices > Chrome management

Define an organizational structure if you want to customize services access or settings for different users or devices. [Learn about user and device policies.](#)

From the Admin console, you can [enforce 100+ policies](#) and settings that apply when people use your managed devices. You can make Wi-Fi and proxy settings, preinstall apps and extensions, limit access to authorized users, and much more. Make settings for different groups of users, such as teachers versus students, or full-time employees versus temps.

As a Chrome Enterprise admin, you can control settings that apply when people use a managed Chrome device, such as a Chromebook. [Device-level settings apply for anyone who uses the device](#), even if they sign in as a guest or with a personal Gmail account.

User policies are enforced anywhere your users sign in, including enrolled and unenrolled Chrome devices. These settings include the ability for you to set security policies and control what apps users can download and access. For more information, see [Managing Chrome devices](#).

A user's organizational unit determines which services and features are available to that user. A user's domain determines their account username and email address (if they're using Gmail). If you want to apply policies to users in a particular domain, you can place those users in their own organizational unit. But you don't have to. An organizational unit can include users from different domains. And users in a domain can be distributed across any number of organizational units. [Learn how the organizational structure works.](#)

The organizational structure in your Admin console only controls which services and features are available to users. You can build this structure to match your LDAP structure if you want to, but you don't have to.

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

## Key policy considerations

Chrome devices can be configured to work in nearly any school or enterprise environment. When deploying Chrome Enterprise 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 Chrome Enterprise 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 Chrome 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, blacklist 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 Chrome Enterprise 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. [Learn more](#).
- **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 Chrome Enterprise device to be set up for your environment.
2. Set those same settings as policies in the 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 blacklisted) have been set and verified on Chrome Enterprise devices in that organizational unit, you can replicate those settings across the domain.

Chrome devices automatically enroll at the top-level organization. Learn how to [add an organizational unit](#) to apply custom policies to different user cohorts and [move a Chrome Enterprise device to different organizational units](#).

## Recommended settings

In the Admin console under Device management > Chrome management, you can access many settings under User & Device, browser 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 Chrome OS, Browser (Windows, Mac and Linux), or Android devices.
- Change policy inheritance by clicking the dropdown menu on the left of each setting.
- The icons below each setting confirm where the policy is applied.
- Hover each policy to populate a blue question mark icon to learn more about the policy.

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

Allow signed-in users change accounts in their browser window	You can decide to allow or block users from signing in or out of Google Accounts within the browser. Or, you can allow users to sign in only to specific G Suite domains. Learn more about <a href="#">Sign-in Within the Browser</a> .
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 Chrome device to re-enroll in your domain, you should <a href="#">deprovision</a> the device. <a href="#">Learn more about forced re-enrollment</a> .
Screen Lock	Select Always automatically lock screen on idle to increase security and reduce likelihood of someone using your users' computers while they're away.
Pre-installed Apps and Extensions	Choose the web apps that pertain to your users, such as Gmail Offline or Google Drive. You can also blacklist and whitelist apps if you need more control over which apps can be installed by users from the <a href="#">Chrome Web Store</a> .
Pinned Apps	Select which apps to hide or show on the system taskbar. Note: This setting only allows administrator-specified apps, and users will no longer have their own custom set of apps visible on the system taskbar.
Pages to Load on Startup	This is commonly set to an intranet portal or homepage. The downside is that once set, Chrome devices no longer restore the tabs from the most recent browsing session upon restart.

Restrict sign-in to list of users

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) Chrome device.

Erase all local user info, settings, and state after sign-out

Don't enable this; it causes users' policies to re-download upon each sign-in session, unless you need to have the Chrome device wiped of all user states in between user sessions.

Auto-update settings

Leave the auto-update settings to their defaults. Chrome devices self-update every 6 to 8 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 Chrome OS releases work in your organization. See a full list of recommendations in [Deploy auto-updates for Chrome devices](#).

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 Chrome devices before rolling this out to your whole organization. If you use SSO for G Suite sign in on your existing devices, you can consider using [G Suite Password Sync](#).

# Chrome adoption & change management

Introducing new technology and embracing change can be difficult. This is why incorporating change management methodology into each phase of the Chrome 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 Chromebook adoption. A structured change management plan ensures employees:

- Understand the benefits of using Chromebooks
- Possess the knowledge, skills, and ability to use Chromebooks
- Adopt Chromebooks 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

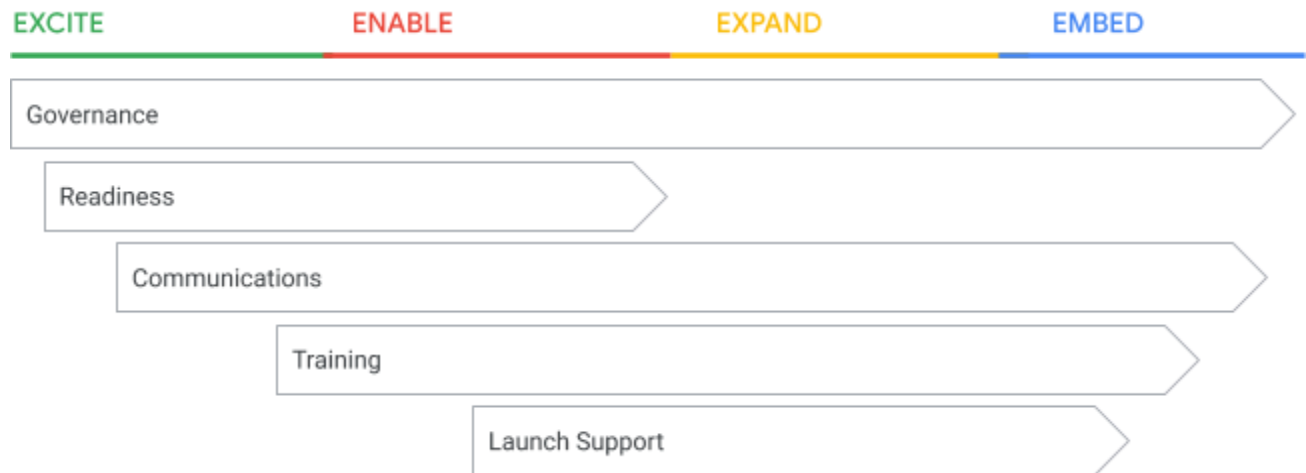
- Deploy services
- Deploy services and execute on support model, training, and communications plans

## Expand

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

## Embed

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



## Chrome 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 & support materials
- Develop a positive buzz

## Supporting users through change

<b>Governance</b>	<ul style="list-style-type: none"><li>• Establish a change leader to be the face of change</li><li>• Select and train “Chrome Champions” to lead the way</li><li>• Lead by example i.e. Senior management</li></ul>
<b>Readiness</b>	<ul style="list-style-type: none"><li>• Identify appropriate user and use case cohorts</li><li>• Assess the impact of change by cohort</li><li>• Define change management success by cohort</li></ul>
<b>Communications</b>	<ul style="list-style-type: none"><li>• Identify communication needs by cohort</li><li>• Develop communication plans for all cohorts</li><li>• Execute campaign</li></ul>
<b>Training</b>	<ul style="list-style-type: none"><li>• Identify training needs by cohort</li><li>• Create a curriculum and deliver training for each cohort</li><li>• Build printable user guides and internal Chrome site</li></ul>
<b>Launch Support</b>	<ul style="list-style-type: none"><li>• Identify communication needs by cohort</li><li>• Develop communication plans for all cohorts</li><li>• Execute campaign</li></ul>

## 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: Chrome Champions**

Chrome 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 Chrome.

### **Recruit a network of Chrome Champions**

- Tech savvy employees excited about Chrome 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 & responsibilities**

- Get trained and proficient on Chrome devices early
- Understand the changes the organization will go through to use Chrome
- 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](#), or leverage Google+ as an alternative to communicate useful info to users



## Readiness

### Who are your users and what are your use cases?

Confirm all the ways your organization will use Chrome 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](#)
- Device management

### Identify cohorts for change management

Identify the users in your organization switching to Chrome 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 Chrome Champions support for every identified cohort.

Examples:

#### Users

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

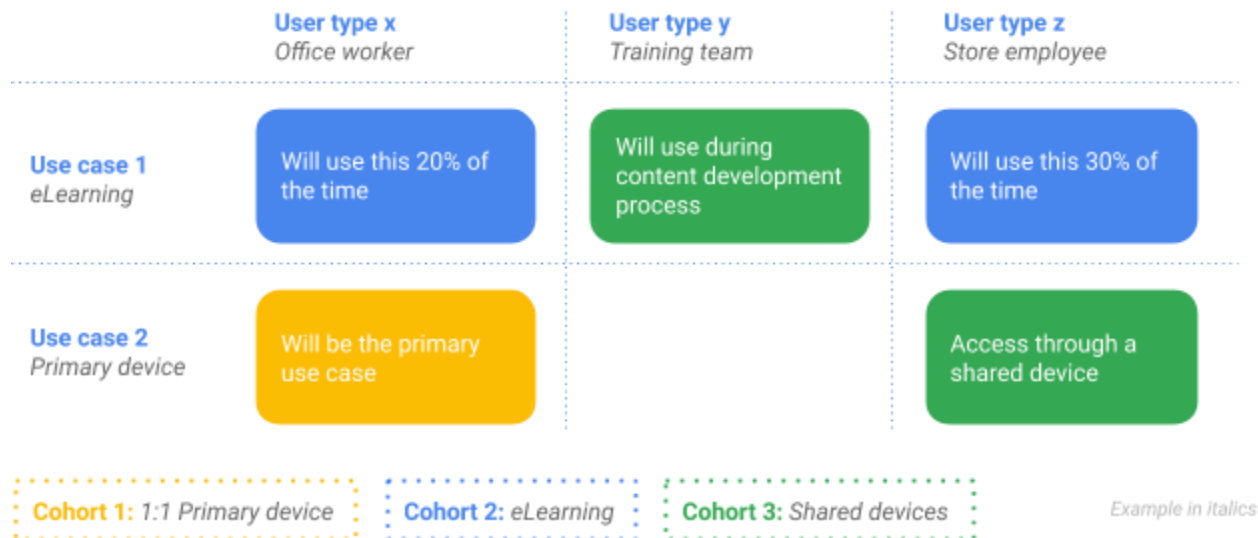
#### Use cases

- 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 Chrome Enterprise devices. List out activities and workflows that will be changed or newly created by using Chrome. Understanding the impacts Chrome 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 Chrome 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 Chrome will improve their work
- Reduces risk related to users acceptance of Chrome
- Utilize the change management cohort analyses 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.

i.e. 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 Chrome.

#### **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 Chrome
- It identifies the benefits of using Chrome and ties these into the vision and strategy of the organization
- The elevator pitch embodies the company's vision of going Chrome
- 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 Chrome 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 Chrome, increases user adoption and reduces the risk of significant disruption during the transition period.

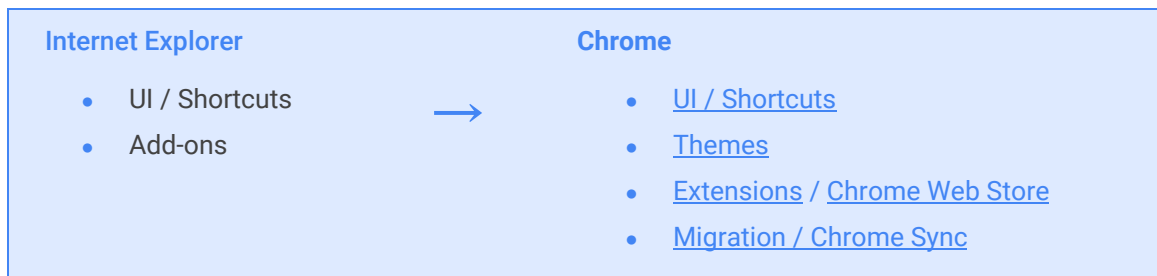
[Check our Productivity and Collaboration blog](#) and [How To Chromebook site](#) for the latest tips and tricks!

### Do a training needs assessment

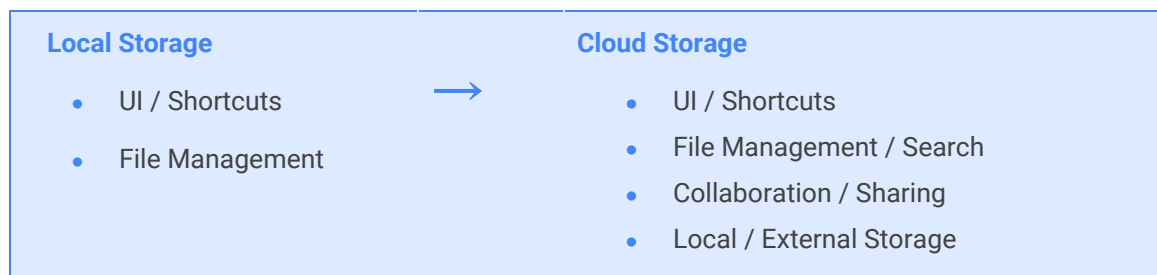
Utilize the Organizational Analyses to document training needs for each cohort. Cohorts are likely to have specific training needs by use case to understand how their work will be changing. A thorough training needs assessment **ensures users become proficient at Chrome, increases user adoption, and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

Examples:

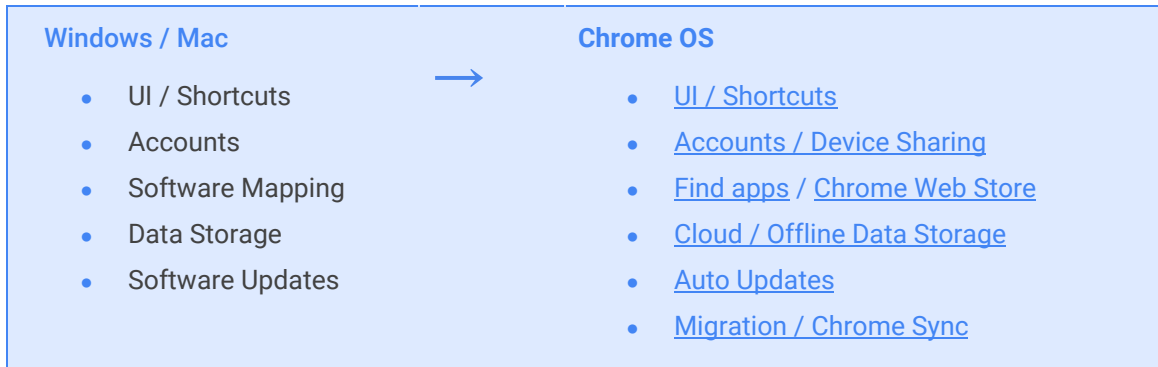
#### Internet Explorer migration - all users



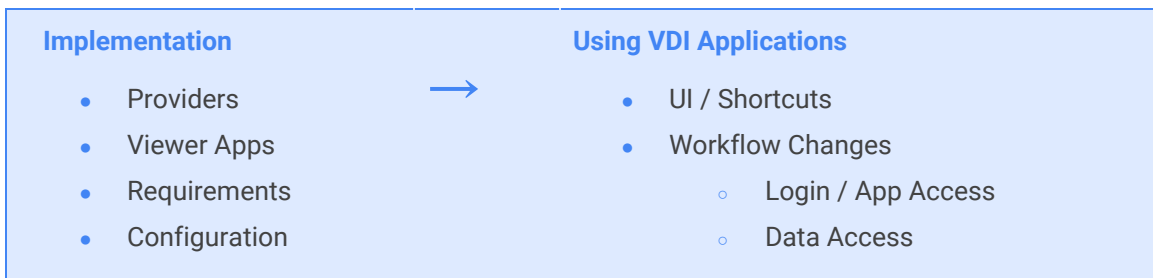
#### File Management - all users



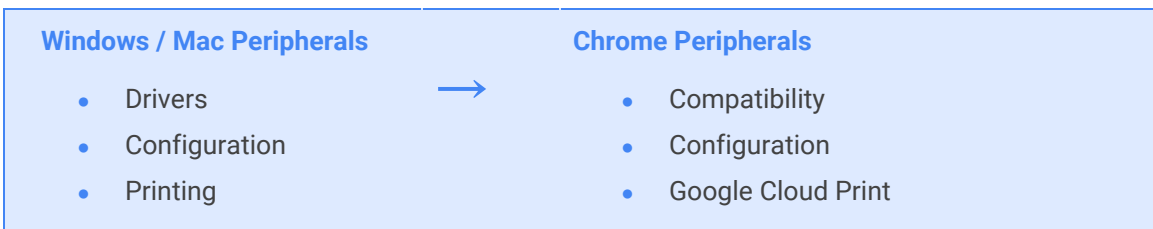
### Chromebook basics - all users



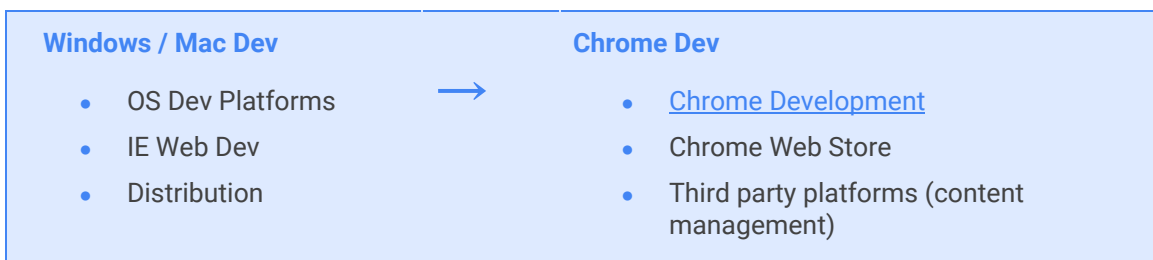
### Using VDI in Chrome - users with legacy app requirements



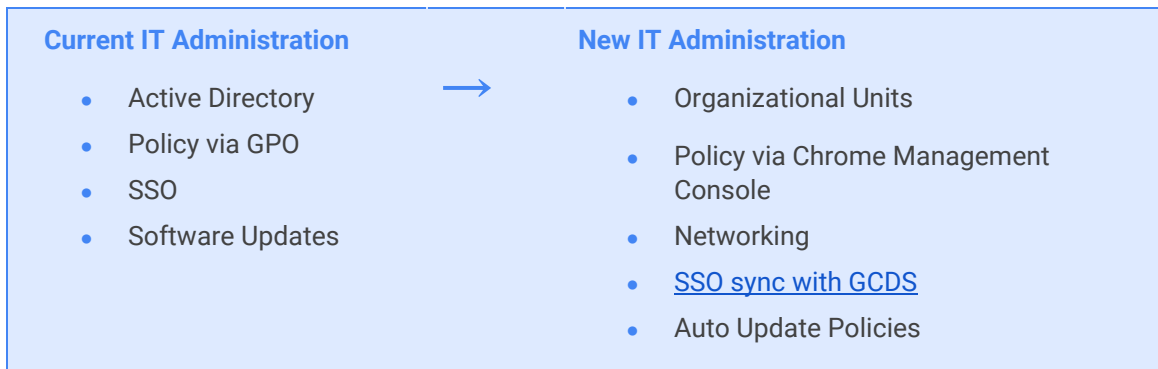
### Chromebook and peripherals - users who depend on the use of peripherals



### App Development - content creators



## Chrome Management Console - IT administrators



### What is your training approach for Chrome Enterprise?

#### 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
<ul style="list-style-type: none"> <li>• Scalable, content is standardized</li> <li>• Typically lower cost than instructor led training</li> <li>• Minimal requirements for logistics</li> <li>• Accessible anywhere at anytime</li> </ul>	<ul style="list-style-type: none"> <li>• Scalable, content is customizable</li> <li>• Typically low to medium cost</li> <li>• Medium requirements for logistics</li> <li>• Accessible anywhere at specific times</li> <li>• Requires partner or customer training resource to facilitate</li> </ul>	<ul style="list-style-type: none"> <li>• Less scalable, content is customizable</li> <li>• Higher requirements for logistics</li> <li>• Requires partner or customer training resource to facilitate</li> <li>• Typically higher retention and impact</li> </ul>

## Modern Training Formats

### Lunch & 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 & 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 Chrome devices is essential to user acceptance. Offer Chrome light-night sessions, training sessions, and self-paced training materials prior to Go-Live to familiarize users with Chrome devices to improve user experience during transition.

## Support the Go-Live

Make the Go-Live a fun experience and utilize Chrome 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 Chrome 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
  - White glove prep for the devices to ensure they are ready to use out of the box

### Engage Chrome Champions

Ensure that the Chrome 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 Chrome 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 publicised
- Demonstrate that feedback is being listened to and acted upon

## Supporting 'going Chrome'

### Encouraging an internal community for self-support

#### Chrome champions program

Encourage an internal support program to help employees help employees. Leverage [Google Guides](#) to create a program for [Chrome Champions](#). Chrome 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.

Incentives for those Chrome 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 realised are communicated back to the user base, quantify the benefits as much as possible
- Ensure that Chrome 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 Chrome initiative and make information

easy to access and consume

# Still need help?

- Check out our [support page](#) or reach out to [ask-chrome-channel@google.com](mailto:ask-chrome-channel@google.com).
- Refer to our Chrome Enterprise [Help Center](#) and [Community](#)
- Check out our [Chrome Enterprise “How-To” Demos](#)
- Chrome device [Tips and Tricks](#)
- [Sign up](#) and follow [Chrome Enterprise release notes](#)
- Chrome Browser downloads and Chrome Enterprise product overviews—[Chrome Browser for enterprise](#)
- Sign up to [join the Chrome Enterprise Customer Forum](#)
- Check out our [Chrome Champions webinars](#)
- Review and share the [Chromebook Employee Adoption Kit](#)

## Additional resources and support

- G Suite, Cloud Identity customers (authorized access only)—[Contact support](#)
- Chrome Browser Enterprise Support—Sign up to [contact a specialist](#)
- [Chromebook Help Center](#) and [Community](#)
- Follow the [Google Chrome blog](#) and [Chrome releases blog](#)
- Chrome version status and timelines—[Chrome Platform Status](#) | [Google Update Server Viewer](#)
- Announcements: [Chrome Releases Blog](#) | [Chromium Blog](#)
- Developers: Learn about [changes to the web platform](#) and features [planned for upcoming releases](#).

## Self-support tips

- In your Chrome browser, visit: `chrome://settings/help`.
- How Chrome releases work—[Chrome Release Cycle](#)
- [How to collect Chrome device logs](#)
- [Fix Chromebook problems \(Chromebook consumers\)](#)
- [Known issues](#) (Chrome Enterprise)
- [Log Analyzer](#) (G Suite Toolbox)—Analyze `/var/log/messages` and `/var/log/chrome/` for errors
- [Administer exams on Chromebooks](#)