Google Chrome

Chrome Device Deployment Guide

Set up and deploy Chrome devices in your organization

Enterprise & Education

Table of Contents

About this guide

This guide is a companion to the 5-step Chrome Device Quick Start Guide and describes (in greater detail):

- The key decision points when deploying Chrome devices to a large school or business.
- Cloud-based policies, Chrome apps, and specific use cases. For more in-depth documentation, see the Chrome Enterprise Help Center.

This guide specifically focuses on:

- **Setup and enrollment**—How to connect each device to your network, enroll those devices in your domain, and update them to the latest version of Chrome OS.
- **Management**—How to push policies for your domain to fulfill your IT requirements, and how to set up and manage devices running the latest version of Chrome OS.

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. For information on deploying the managed Chrome browser, see Deploy Chrome.

What's described	Instructions, recommendations, and critical considerations for deploying Chrome devices in a school or business environment
Primary audience	IT administrators
IT environment	Chrome OS, web-based environment
Takeaways	Best practices for the critical considerations and decisions of a Chrome device deployment

Last updated: December 13, 2018.
Location of the Document: https://support.google.com/chrome/a/answer/6149448

Introduction

Chrome devices are computers developed by Google that run Chrome OS. What makes these computers 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 devices can be centrally managed by the Google Admin console. You can configure over 200 settings from this web-based console, such as Wi-Fi settings, selecting apps to be pre-installed, and forcing devices to auto-update to the latest version of Chrome OS.

Prerequisites

1. Although Google Identity (G Suite account) isn't required to use a managed Chrome device, we recommend that you've provisioned your users with Google Accounts. See add users to your domain for more information.
2. Once you've done this, you'll need to purchase Chrome device licenses to manage them from the Admin console. Purchase licenses for a school or business. Additionally, organizations in the US or Canada can purchase Chrome Enterprise licenses online.
3. If you plan to deploy a large number of Chrome devices or deploy them in conjunction with G Suite for the first time, we recommend that you work with a Google Cloud partner.

Manage Chrome devices

Chrome devices can be configured to work in nearly any school or enterprise environment. When deploying Chrome 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 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 allows multiple users to share the same Chrome 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.

Connectivity

When setting up wireless for a classroom or business, 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

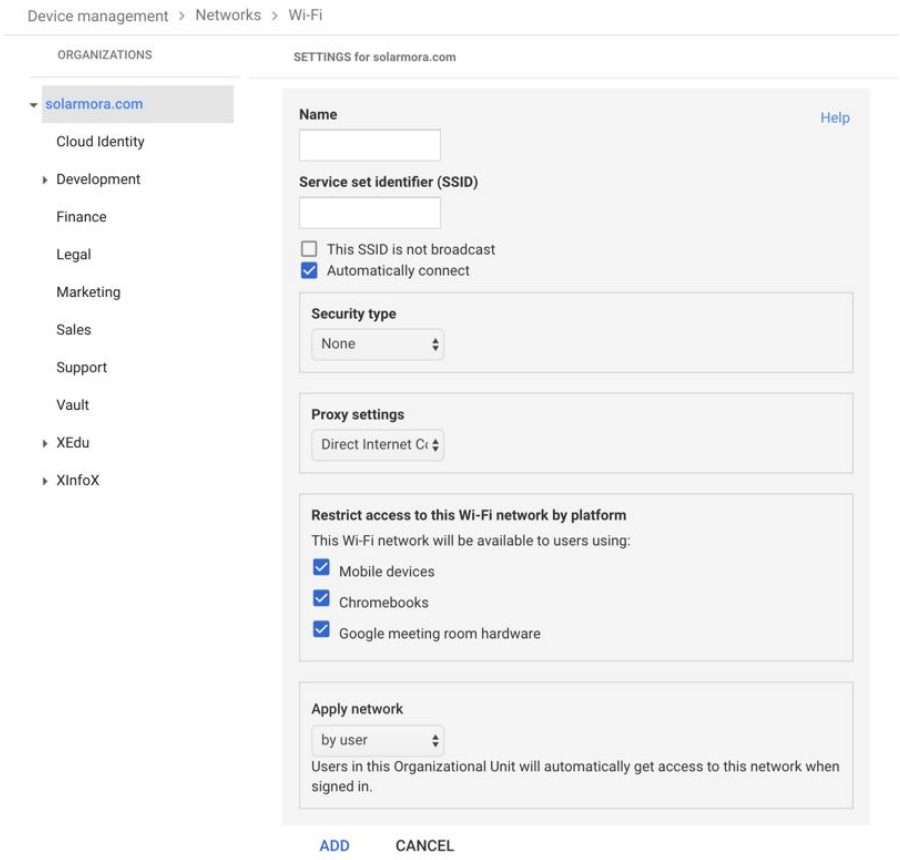
Wi-Fi networks can be manually added to the Chrome device at any time, but Google recommends using the Admin console to push Wi-Fi profiles. These profiles are downloaded and applied to the Chrome device during the enrollment process. Updates to Wi-Fi network profiles also get pushed during the automatic 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

Child organizational units inherit Wi-Fi network profiles from their parent organization. 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.



Wi-Fi setup

It's often easiest to use an open or unfiltered network to enroll the 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.

You'll need to be on the network to download the 802.1x certificate, so you should set up an open WPA/WPA2-PSK network, or you can use USB-to-Ethernet adapters to load the certificate on the device. See Manage networks.

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.

Set up accounts and Chrome OS policies

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

You can view a list of your Chrome 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 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.

Key policy considerations

To set the correct settings for your school or business:

1. Make a note of how you want the model Chrome 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 devices in that organizational unit, you can replicate those settings across the domain.

For more information on using organization units with Chrome devices, see Move a Chrome device to an organizational unit.

Recommended settings

In the Admin console under **Device management > Chrome management**, you can access many settings under **User settings** and **Device settings**. Although most organizations go with the defaults, below are popular settings some organizations customize.

Allow users that are signed-in to the device to 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 Sign-in Within the Browser.
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 deprovision the device. Learn more about forced re-enrollment.

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 Chrome Web Store.
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 each 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.

Prepare your devices for deployment

Before you distribute Chrome devices to your end users, they need to be "staged" to ensure that 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 updates are applied to your fleet of Chrome devices.

If you are deploying a small number of devices, see the Quick Start Guide for streamlined instructions on how to enroll and deploy your devices. If you're deploying Chrome devices to a larger group, such as to multiple classrooms or schools, or to multiple office locations, see the instructions below.

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 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.

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

Prepare your Devices for Enrollment

To prepare and deploy your devices:

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. After accepting the Terms of Service, and *before signing in to the Chrome device*, press **Ctrl-Alt-E**. You will see "enterprise enrollment" in the top left.
4. 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."

5. 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.

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.

Deploy Android apps to Chrome devices

If your organization uses Chrome devices that support Android apps you can force-install or decide which Android apps your users can download. You can make the apps available to users in 3 ways:

- You can force-install apps to devices
- You can create a selection of apps that you allow your users to download
- You can give users access to the full content of the managed Google Play store (not supported for Chrome Education customers)

For more information on how to enable Android apps for Chrome devices in your domain and approve apps for your users, see Use Android apps on Chrome devices.

Before you begin

- Google recommends that you test Android apps for Chrome devices in a pilot organizational unit (OU) before rolling it out to everyone. If you decide you no longer want to use it, you can disable it and continue using your devices in the same way you did before.
- Consult the Android apps on Chrome FAQ for additional information that may be relevant to your deployment.

Running Android apps in kiosk mode

You can use your Google Admin console to install Android apps on managed Chrome devices in locked-down kiosk mode. This allows you to deploy an Android app on a kiosk device, and configure it to launch automatically.

Native printing with Chrome devices

Chrome OS supports native printing that allows users to easily connect to printers and print servers directly without the need for access to any cloud-based infrastructure. Chrome uses the Common UNIX Printing System (CUPS) to support native printing and uses the Internet Printing Protocol (IPP) to support printing to local and network printers.

As an administrator, you can use your Google Admin console to set up CUPS. When you add a printer, it automatically appears in your users' list of Chrome printers, so they can start printing without any further setup. For more information, see Manage local and network printers.

CUPS printing supports printers manufactured by a large and diverse set of manufacturers and supports printing to local and network printers.
For information on additional printing options on Chrome OS, see Print on Chrome devices.

Remote access and Virtualization (Optional)

You can use your Chrome devices to access traditional legacy applications in situations where users require access to:

- Legacy client applications like Microsoft® Office®
- Web pages that require older or Microsoft-only technologies (e.g. require Internet Explorer)
- plugins other than Flash (for example, Java® plugins, or Silverlight) for web apps

Key features

Virtualization apps allow you to run your legacy apps on Chrome devices or use Chrome devices with your existing virtualized application infrastructure. There are several solutions available that use common remote access protocols. For instance:

- Citrix Workspace
- VMware Horizon Client for Chrome
- ChromeRDP

There are also app virtualization solutions such as Chromotif and Fra.me which work well on Chrome OS.

Considerations for application hosting

If the applications you want to access can exist off-premises (for example, Microsoft® Office 365, Oracle® Cloud applications, or hosted SaaS applications), then a hosted solution is usually the easiest to implement, and won't require server setup.

However, if the application you want to access must be hosted within your firewall, or you want to leverage your existing servers or virtual desktop infrastructure (VDI) solutions, these solutions may work better:

- VMware Horizon™ DaaS®
- Chrome Remote Desktop

Special Chrome device deployment scenarios

Chrome devices can be used in a variety of situations, and given their low cost, remote management, and little to no maintenance, they've become popular to deploy for specific business and school use cases. These scenarios range from showing a school calendar on a digital signage display, to shared laptops in a library, to administering student exams. See below for links to additional resources on how to deploy Chrome devices to best meet your needs.

Cloud worker

Chrome devices are great devices for enterprise employees. A chrome device can be assigned to a user as their fulltime device for accessing web applications, productivity tools, and collaborating with co-workers. To learn more about how you can empower cloud workers with Chrome Enterprise, see these videos at Cloud Worker Live.

Kiosk app for single purpose

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

Managed guest session kiosks

You can set up managed guest session kiosks 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 Chrome device. 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.

Student assessments

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 test provider, or through managed guest session kiosks. For details, see Use Chromebooks for Student Assessments.

Readiness checklist for deployment

☐	Network infrastructure	Do you have the Wi-Fi infrastructure in place and bandwidth for all of your devices to connect to the Internet at the same time? • What is your current bandwidth utilization today, before adding Chrome devices? Will your bandwidth meet your estimated demand? • Are there areas of your building without Wi-Fi coverage?
☐	Legacy vs. web application inventory	How many of your users require legacy apps vs. web apps? Are you looking to move toward a wider adoption of web apps and online resources for your users? If so, what's your timeline?
☐	Plug-in usage	Do you know what plugins are required to access the sites your users need to use? Do you need to set up a remoting solution to do this? Learn more
☐	Printers	Have you configured your printers for for native printing (CUPS)? Will you allow all or some of your users to print?
☐	Peripherals	Have you verified that peripherals your users need work with your Chrome devices? For example, test your headsets, barcode scanners, and the other peripherals you need to deploy before rolling them out to these users.
☐	Authentication scheme	How will users sign in to their computers? How will you manage Wi-Fi passwords and access to your Wi-Fi network? Are you relying on SSO for Chrome device authentication? Are you also using G Suite Password Sync (GSPS)? Are you using Cloud Identity?
☐	Project milestone dates	Do you have a timeline for your roll-out? Do you have a way for users to give feedback on their experience with Chrome devices? How long will your evaluation period be, what types of surveys will you give users, and how often will you gather usage data and user feedback?
☐	User training	If you're moving from another platform to Chromebooks, are you conducting user training? If you have a training department, you can create the training in-house. If you don't, some Google Cloud Premier Partners offer Chromebook training.
☐	Help desk readiness	Is your help desk familiar with the Chrome Enterprise Help Center? Reading the resources listed on the following page and attending trainings can help your help desk and IT staff get up to speed speed with Chromebook-related questions.

Additional resources and support

Keep up with what's new in Chrome devices

- Follow the Google Chrome blog and Chrome releases blog
- Follow Chrome Enterprise release notes

G Suite customers can also see:

- G Suite What's new site
- Google Cloud blog

Consult the Help Center

- Chrome Enterprise
- Chromebook (end user)
- Chromebox for meetings
- Learn how to sign in to the Admin console

Self-support tips

- 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

Get support

We provide phone and email support for issues you may experience with Chrome device software and services. See our support options for Chrome devices.