For the website containing this document, click HERE

Google for Work

Chrome Device Deployment Guide

Set Up and Deploy Chrome Devices in Your School or Business

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 for Work and Education 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.
- **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.

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 for Work.

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

Publication date: December 15, 2014.
Help URL: https://support.google.com/chrome/a/answer/6149448
Short link: http://goo.gl/Yd3RC7

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 wipe the 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 100+ settings from this web-based console, such as and Wi-Fi, pre-install apps, and force the computer to auto-update to the latest version of Chrome. (For brevity, Chrome OS will be referred to as just "Chrome" in this guide.)

Prerequisites

1. Although a Google Apps account isn't required to use a managed Chrome device, we recommend that you've provisioned your users for Google Apps and have set up accounts for them. See sign up for Google Apps and add users to your domain.

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.

3. If you plan to deploy a large number of Chrome devices or deploy them in conjunction with Google Apps for the first time, we recommend that you work with a Google for Work 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.

- **Public Session Policies**—Can be used to set up settings for shared devices in your domain. Public 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 or even launching the device as a Single App Kiosk. Learn more.

Connectivity

When setting up wireless for a classroom or business, be sure that you have adequate wireless coverage throughout the room, 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. Especially in a high-density area, such as a corporate office or school, where many Chrome devices are used concurrently, IT administrators should ensure there's adequate connectivity and bandwidth.

- **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.
- **For school/company-wide deployments—**Consider doing a wireless infrastructure and topology survey of all the buildings to make sure that 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.

For more in-depth information, see Enterprise networking for Chrome devices.

Manage network profiles

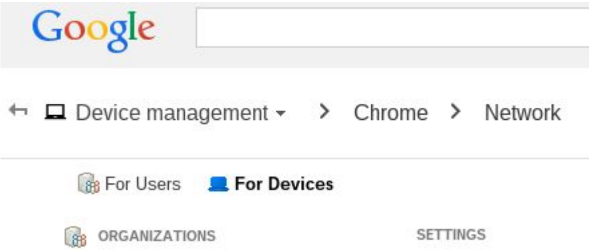
Wi-Fi networks can be manually added to the Chrome device at any time, but Google recommends pushing Wi-Fi profiles via the Admin console. (Learn how to Sign in to your Admin console). These profiles are downloaded and applied to the Chrome device during the enrollment process. Updates to Wi-Fi network 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 include certificate management, SSO, and web filtering solutions. Below are tips on how to set up Wi-Fi and optional network settings.

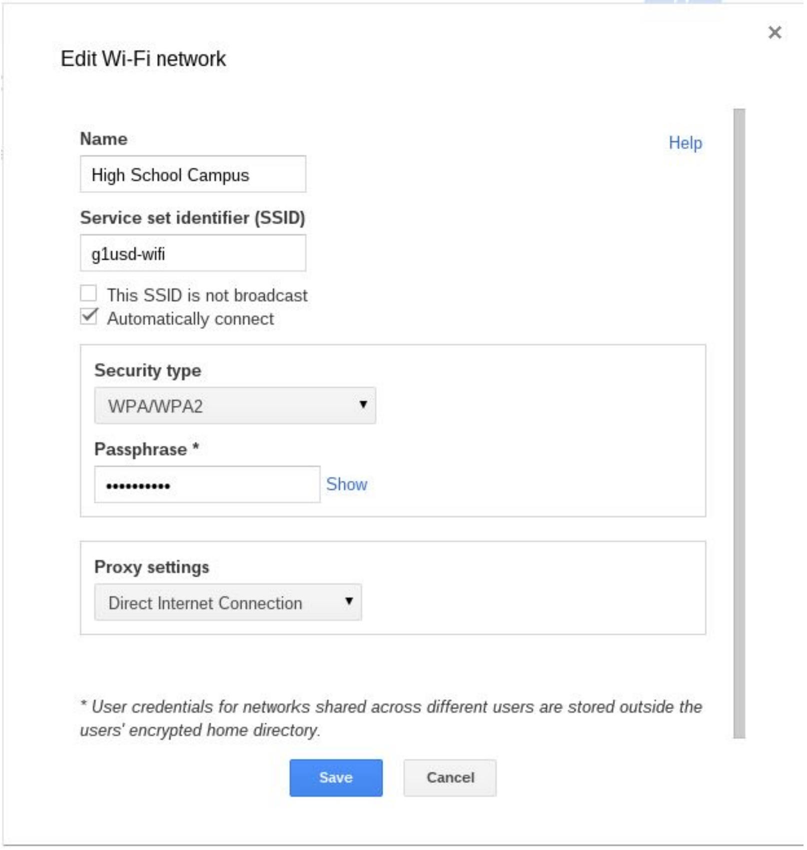
Add Wi-Fi configuration on the device level

We recommend that you set up at least one wireless network **For Devices** at the top organizational level in your domain and set it to **Automatically connect**. This ensures that the Chrome device can access this Wi-Fi network at the sign-in screen. Wi-Fi network profiles are inherited down to child organizational units. When defining a new Wi-Fi network profile, ensure that **For Devices** is selected.



Verify Wi-Fi configuration options

Verify that the Wi-Fi configuration options are correct. Pay attention to the service set identifier (SSID) and passphrase, both of which are case-sensitive. We recommend that you test this configuration on a newly enrolled Chrome device to make sure it auto-connects before enrolling a large number of devices. The Wi-Fi network profile can be edited and saved in a dialog box similar to this:



Edit Wi-Fi network

Name: High School Campus

Service set identifier (SSID): g1usd-wifi

□ This SSID is not broadcast

☑ Automatically connect

Security type: WPA/WPA2

Passphrase *: ••••••••••

Proxy settings: Direct Internet Connection

** User credentials for networks shared across different users are stored outside the users' encrypted home directory.*

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 via certificates. Contact your networking vendor to see how to be set up Chrome devices with the Chrome Certificate Management Extension API. For example, ClearPass Onboard by Aruba Networks is an extension that handles Chrome device onboarding and installs the certificate in a secure manner.

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.

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 policies

With the Google Apps Admin console, you can centrally organize and manage your fleet of Chrome devices. Once you're managing users via the Admin console and purchase Chrome device licenses, from the Chrome management section of the Admin console, you can set device policies by organizational unit as well as user policies, including 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. The 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.

Policies are inherited in the organizational unit hierarchy. Thus, settings at the top level are reflected in the lower levels of the organizational unit hierarchy, unless a setting override is made at the lower level. The key is to have more general settings at the top levels and more specific settings within each organizational unit (e.g. middle school versus high school student organizational units).

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.

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 sig-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 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 Google Apps sign in on your existing devices, you can consider using Google Apps Password Sync.

Tip: We're regularly adding new features, such as Public Session Kiosk and the ability to run Chrome devices in single-app mode. To stay up to date, see Manage Chrome devices.

Prepare your devices for deployment

Prior to distributing the 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

There are two ways to update Chrome devices to the latest version of Chrome. One way is to start up the devices and go to `about:chrome` in the browser’s address bar. This will update the device to the latest version of Chrome through an over-the-air update. If you need to update many devices and want to conserve network bandwidth, you can also update the device from a USB recovery stick with the latest version of Chrome.

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:

1. In the address bar, go to `about:chrome`.
2. Stick a USB drive (4 GB or larger) formatted for USB 2.0 into the Chrome device.
3. Go to `chrome://imageburner` to create a USB recovery device using the built-in image creation tool in Chrome OS.

The image creation tool creates a USB stick with the latest available stable release of Chrome OS. Alternatively, you can use the Chromebook Recovery Utility in the Chrome Web Store.

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

When creating the image:

- Make sure you're using the latest stable release of Chrome OS to image each device.
- If you run into issues while enrolling the device, you may need to wipe and re-enroll the device.
- Once successful, you can use the Admin console to apply settings to all devices in your organization by going to **Device Management > Chrome**.

Prep and deploy all of your devices

To prep and deploy all of your devices:

1. Create USB recovery devices using the built-in image creation tool on a Chromebook at `chrome://imageburner`.

2. Follow these instructions to use a USB recovery stick to wipe and re-image your Chrome device with the latest version of Chrome OS. This re-imaging can take as little as 5 minutes, to over 20 minutes, depending on the device.

3. After rebooting, select the language, keyboard type, and Wi-Fi network.

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

5. Click **Enroll device**.

   After you successfully enroll the device, you see a note appears, stating that "Your device has successfully been enrolled for enterprise management."

6. Click **Done** to return to the initial sign-in page, where you can see the text “This device is managed by *yourdomain.com*” at the bottom.

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 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 Google Apps 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 about what they offer.

Print with Chrome devices

To print from a Chrome device, you use Google Cloud Print (GCP). Because a Chrome device doesn't have print drivers installed on the device itself, using the GCP service sends your print job to Google's servers, which format the file correctly with the required print drivers. Then, Google's servers send the print job to a printer you've configured with GCP.

Many organizations choose to use and set up their existing printers with GCP using a Windows®, Mac®, or Linux® computer. GCP can also be configured with print servers and cloud-ready printers. These printers don't need a computer to work with GCP, but are connected to directly to the Internet, and can print directly from GCP.

Considerations for organizations

- Use a naming scheme for each GCP printer that includes the location of each printer, so that users can search for printers by building and floor.
- Currently, GCP doesn't allow page number monitoring or allow for simple integration with print payment systems, if you charge users for print jobs.
- GCP currently supports 2 user roles for printers: owner and user. GCP also supports user-to-user sharing and sharing with Google Groups.
- Some organizations create at least 2 groups, such as Users and Teachers, or Employees and Vendors. Some restrict what printers users can print from by restricting which printers are shared with the user group.
- Printers that are shared automatically begin appearing in users' Print dialog boxes. They can be searched for by name or location, making discovery simple and intuitive.

Integration with existing infrastructure

You can use GCP with your existing print server by running Google Cloud Print as a Windows service or on a Linux server. If you don't have a print server, you can use GCP to print from a PC connected to your printer.

For more information, see:

- Connect your classic printers
- Connect your printer to Google Cloud Print
- Cloud Print Help Center

Local printing

Additionally, developers can configure Google Cloud Print 2.0-compatible printers to print locally. This process, although technical to set up, allows local printing over Wi-Fi via your local area network through mDNS discovery. Learn more

Remote access and Virtualization (Optional)

The best user experience with a Chrome device is using web apps and extensions available in the Chrome Web Store. However, you may want to use your Chrome devices for remote access to your legacy applications. This applies to users who require the following:

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

Key features

Remote access allows you to run your legacy apps on Chrome devices or use Chrome devices with your existing infrastructure. There are several solutions available that utilize common remote access protocols while providing an HTML5 or Native Client front end that can render with Chrome devices. For instance:

- Remote Desktop Protocol (RDP) equivalent technologies that allow you to connect to a server either on your premises or off premises.
- Virtual Desktop Infrastructure (VDI) providers, such as Citrix or VMware, offer Chrome web apps or HTML5 clients to access their VDI servers

Considerations for application hosting

If the applications to which you'd like access can exist off-premises (e.g. Microsoft® Office 365, Oracle® Cloud applications, or hosted SaaS applications), then a hosted solution is usually much easier to implement and requires no server setup.

If, however, you have software that must be hosted from within your firewall, or you'd like to leverage your existing servers or existing 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.

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

Public Session kiosks

You can set up Public Session kiosks for locations like an employee breakroom, 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 Public 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 Google Cloud Print? 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 Google Apps Password Sync (GAPS)?
	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 for Work Premier Partners like Dito offer Chromebook training.
	Help desk readiness	Is your help desk is familiar with troubleshooting steps in the 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 on Google+

Google Apps customers can also see:

- Google Apps What's new site
- Google for Work blog

Consult the Help Center

- Chrome for Work and Education
- Chromebook (end user)
- Chromebox for meetings

Self-support tips

- How to collect Chrome device logs
- Known Issues (Chromebook consumers)
- Known issues (Chrome for Work and Education customers)
- Log Analyzer (Google Apps 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.