

Enable remote workers with Chrome Enterprise

Keep your workforce connected, productive and secure from anywhere

Key benefits of deploying Chrome Enterprise for remote workers

Chrome Enterprise is a modern, secure platform that empowers a remote workforce, allowing employees to be productive from any location and providing IT with the ability to manage devices remotely.

Secure by design

Chromebooks have built-in security to help protect from external threats, security patches can be deployed over WiFi, and IT can remotely disable devices if needed.

Cloud management

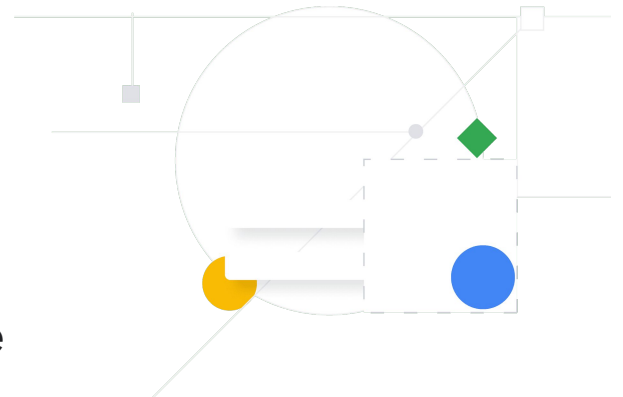
IT admins manage devices and users from anywhere with the Google Admin console. They can easily enforce policies, configure device settings, provide access to VPNs, and force install Chrome apps and extensions across Chrome Browser and OS.

Easy access to apps

Employees can access the apps they need through Chrome Browser, the managed Google Play Store, or VDI solutions. Chromebooks also go hand-in-hand with G Suite and other productivity, collaboration and meeting solutions.

Fast deployment

Businesses can deploy Chromebooks quickly with cloud-based profiles that download users' policies, apps, settings, and bookmarks. No imaging required.



Remote Work Statistics



84% of people work in virtual teams.¹



54% of HR leaders indicated that poor technology is the biggest barrier to effective remote working.²

Chrome Device Deployment Guide

This is a guide for IT administrators who want to deploy Chrome devices to enable remote workers. In this guide, you'll learn:



How to enroll Chrome devices.



How to use the Google Admin console to remotely manage Chrome devices.



Key configuration settings for cloud-based policies and Chrome apps.



How to set and deploy device and user policies across your organization.

Access the guide [here](#).

¹https://www.citrix.com/content/dam/citrix/en_us/documents/other/workforce-flexibility-can-drive-greater-engagement-and-productivity.pdf

²<https://www.gartner.com/smarterwithgartner/with-coronavirus-in-mind-are-you-ready-for-remote-work/>

5 tips to keeping your remote workforce empowered and secure with Chrome Enterprise

1 Configure network settings to allow for remote access

Make sure devices have the right policies for Wi-Fi, Ethernet, and virtual private network (VPN) access. Additionally, add and manage certificates from the Google Admin console.

[Learn more](#)

2 Keep corporate data secure with the ability to disable devices remotely

Administrators can disable a Chrome device directly from the Google Admin console if it's lost or stolen and even post a message that lets the finder know where to return it.

[Learn more](#)

3 Check Google Safe Browsing settings to keep your employees and data secure

With Google Safe Browsing, users are warned of malicious sites before they navigate to them, deterring negligent behavior. IT admins can enable and configure this setting from the Google Admin console. [Learn more](#)

4 Resolve technical issues with Chrome Remote Desktop

Chromebooks are easy to use and have the familiar Chrome Browser. However, if users are having issues, IT administrators can provide remote support with Chrome Remote Desktop. This feature allows IT admins to access a user's device and help resolve issues quickly. [Learn more](#)

5 Manage Chrome browser from the cloud

Manage Chrome browsers on all operating systems through the Google Admin console so your IT can apply policies from anywhere. This gives IT the flexibility to work from different locations and ensures browsers are secure on both public and private networks. [Learn more](#)

Other resources to get started:

- Online [Chromebook simulator](#) with interactive tutorials for employees
- [Install apps and extensions](#) on managed Chrome devices
- See more Chrome [policies](#) for users and browsers
- [Learn more](#) about Chrome Enterprise

To learn more about enabling remote workers with Chrome Enterprise, visit CDW.com/google



“Most employees take their Chromebooks home at night. If weather or disasters prevent them from coming to the office, business goes on.”

Paul Driscoll

Business Systems Manager,
Third Bridge

