|  |
| --- |
| Connecting devices to Google Workspace |

Computers used for work should be set up so people can sign in with their work credentials. Each person should have a unique account (ie, no shared logins).

This simplifies login processes for Google Workspace services as they will automatically sign in on your work account. It provides additional security controls such as being able to reset the person’s password remotely and ensuring your staff are using strong passwords. It also prevents staff from having admin access to your environment.

This document describes the steps to connect your devices to Google Workspace using the setup and operation of Google Credential Provider for Windows (GCPW).

### Outcomes:

An admin can do the first-time setup of Windows and GCPW

A non-admin can then sign into that device with their Google Workspace credentials (an account that's never been used on that device previously)

A different admin can sign in to that device and get local admin permissions

### Licensing Prerequisites:

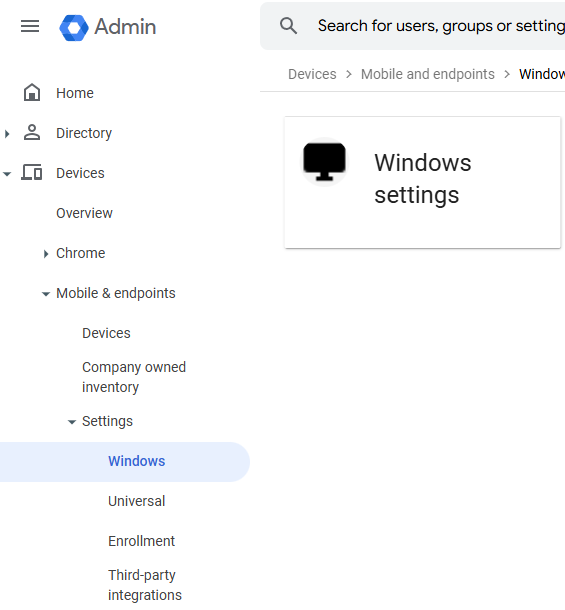
**GCPW:** Supported on most Google Workspace subscriptions, including the Business Standard and Education Fundamentals.

**GCPW with Windows device management:** Requires at least Business Plus or Education Standard.

The base tier allows admins to install the software and have users log in as their Google Workspace accounts. The next tier includes Windows Device Management which enables control of various windows features like admin accounts.

### Google Workspace Admin Configuration:

As an administrator in the Google Workspace Admin console, go to Menu, Devices, Mobile & endpoints, Settings and then Windows:



Click on the Google Credential Provider for Windows Setup tab:

A screenshot of a computer

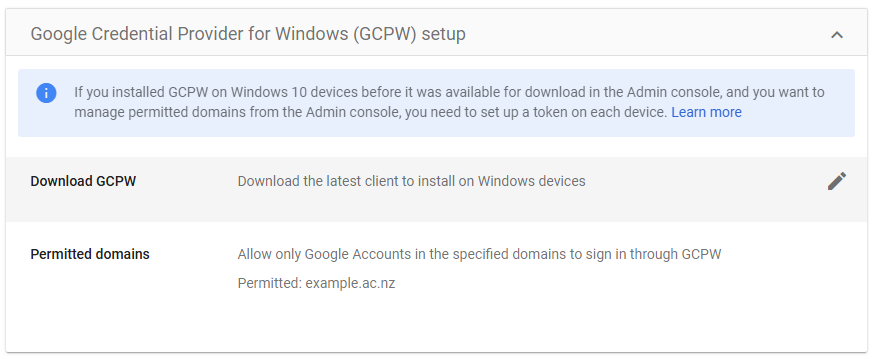
Description automatically generated

Click to edit the Permitted domains section, enter your Google Workspace domain name, click Add Domain, then click Save

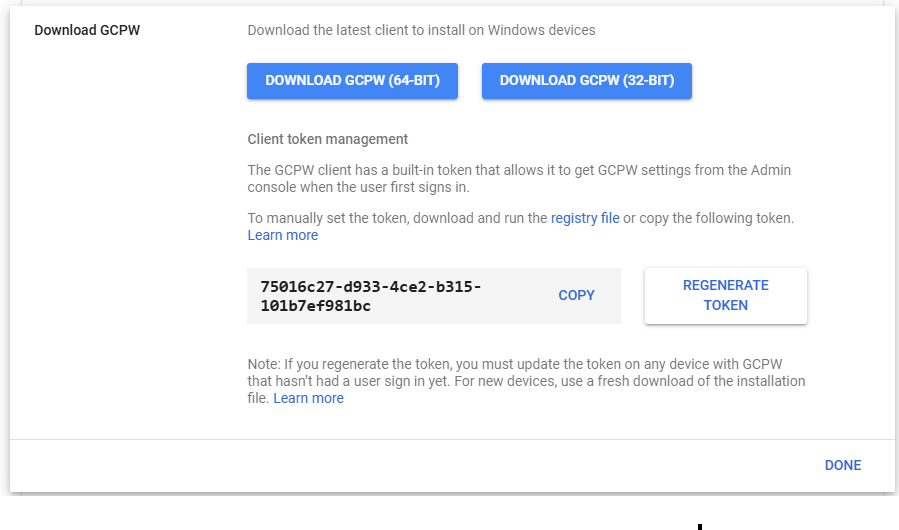
A screenshot of a computer

Description automatically generated

Mouseover, and then Click on the Download GCPW text – it will highlight and turn grey:



This window will appear, click on Download GCPW (64-BIT)



An executable will be downloaded. Use this file to connect end user devices into Google Workspace.

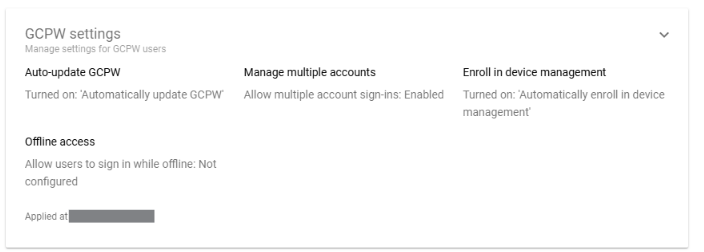
A screenshot of a computer

Description automatically generated

Navigate back to Windows settings using the breadcrumb at the top:



Select the CGPW Settings window and open it by clicking on it:



For each of these options, select those that make sense for your workplace requirements.

Leave Auto-Update on, as this will keep the helper up to date

Enabling multiple accounts to log in means that a multiple users can log into a device

Enrolling in device management only is relevant if Business Plus or Education Standard is the license your organisation runs. This allows control of which users are administrators by the CGPW helper

Offline access is relevant if you wish to limit how long a device can be offline before Google Workspace logins aren’t allowed anymore.

If your organisation isn’t licensed for Business Plus or Education Standard – as in, you’re on the Free Tier of Google Workspace, and don’t have to pay for it – then skip ahead to the installation section.

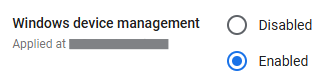
### Enabling Windows Device Management

Open the Windows Management Setup Pane by clicking on it:

A white background with black text

Description automatically generated

Modify the radio button to Enabled, and click Save



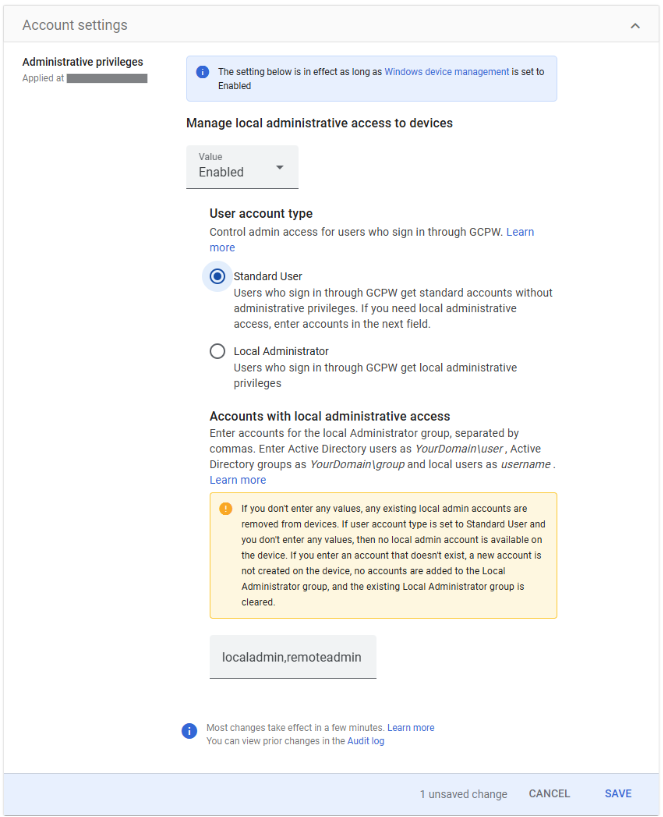
Use the breadcrumb bar at the top to navigate back to *Windows Settings*

Edit Account settings

A white background with a black and white line

Description automatically generated with medium confidence

This section allows administrators to set the administrative access levels on a device.



In this section, admins can configure several options:

To enable or leave this section unconfigured

The default windows permissions level a Google Workspace user will log in as

Configuration of named administration level accounts.

In the example above, any Google Workspace user can log on as a Standard User account without administrative rights on Windows.

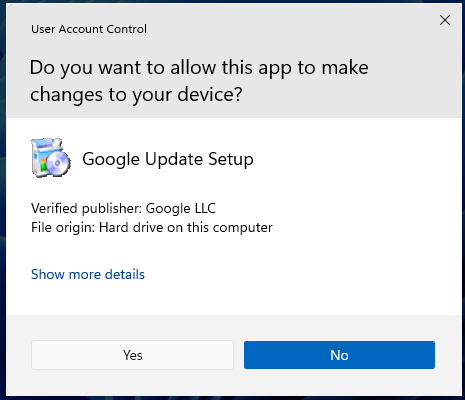
Two named accounts are set to have administrative privileges, one a local admin for a break glass backup account local to the machine, and another, a shared remote admin Google Workspace user.

**Note**: If this Administrative Privileges section is enabled, local administrators on devices are managed only through this portal. **Any existing local administrators are removed.**

### Installation of the GCPW helper program on end-user devices:

Copy the file downloaded (will have the filename gcpwstandaloneenterprise64.exe) in the section above onto each end-user device you wish to enable GCPW on.

On the device, as an administrative user, double click to run the installer. When it runs, it may prompt to run with elevated privileges. Click Yes to proceed.



The installation will complete in less than a minute, and show an Installation Completed message once done.

On the target device, Download and install Google Chrome: <https://www.google.com/chrome/>

When someone logs in with GCPW, Google Chrome automatically picks up their logon details from the login event, and they’ll be able to open Gmail on their account in Chrome without having to enter any extra details.

Restart the device. Expect to wait around 15 minutes after restart for the device to be able to log in Google Workspace Users.

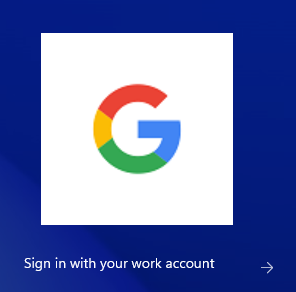
### End user Experience:

To log in for the first time, click on the Add work account option that’ll appear in the bottom left of the logon screen

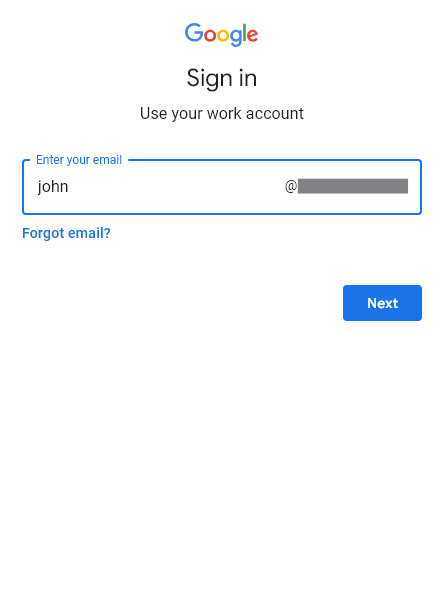
A blue background with white text

Description automatically generated

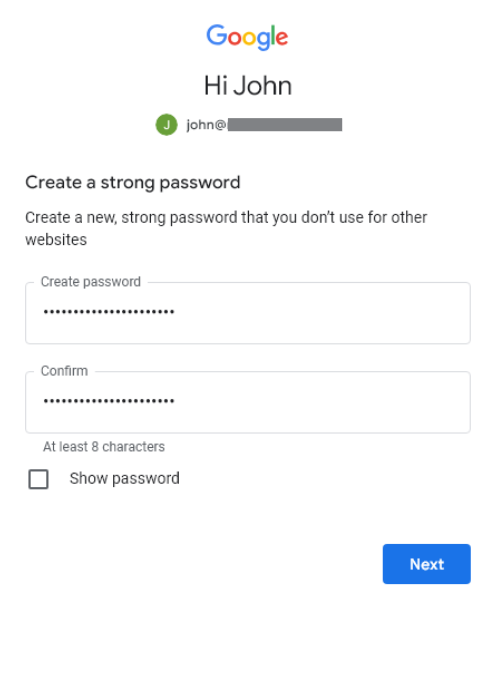
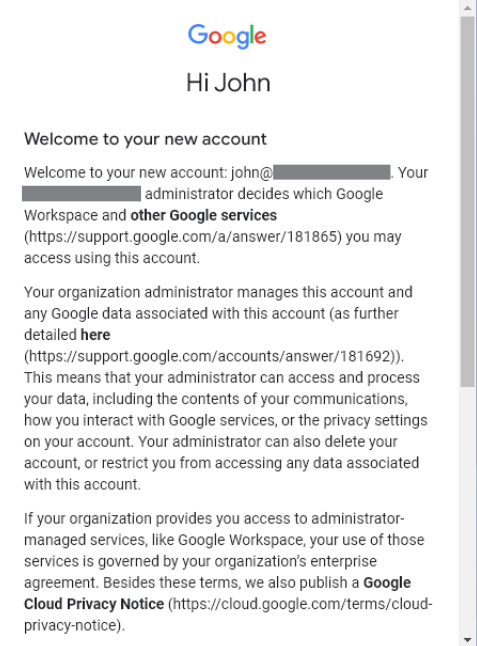
Click the right arrow to sign in:



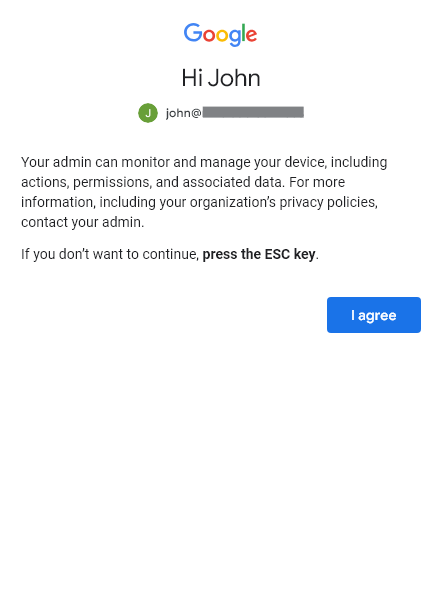
A google sign-in will then pop up:

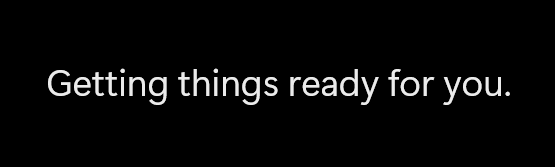


If the user hasn’t logged in before, they’ll be prompted to accept the Terms and Conditions, then reset their password:



If windows device management is enabled, this screen will show up:



All going well, Windows will build a local profile, and log the user in.

**Notes:**

Administrators will need to log in a second time to gain administrative privileges, these aren’t attached on the first login.

Sometimes the first login will fail with a “Logon failure: the user has not been granted the requested logon type at this computer”. Retrying or waiting 10 minutes or so seems to fix this problem, and it doesn’t occur after the profile has been built.

Google Workspace users added aren’t added to the Remote Desktop group, so can’t RDP in. This needs to be managed manually or via a different tool.

### References:

Installation documentation: [Install Google Credential Provider for Windows - Google Workspace Admin Help](https://support.google.com/a/answer/9250996?hl=en)

Plan Comparisons: [Compare Google Workspace editions - Business - Google Workspace Admin Help](https://support.google.com/a/answer/6043385#device-management)