

A. ChromeOS Application Installation

Managed Chromebooks

These instructions are for technology coordinators who have access to the Chromebook device management console to administer and manage their Chromebook devices.

New for 2025–26: As part of Google’s ongoing updates to ChromeOS, support for legacy ChromeOS Apps, including the MCAS Chrome app, is being phased out. Starting in the 2025–26 school year, a new **Progressive Web App (PWA)** will be required for all online testing on ChromeOS devices.

What You Need to Know

- **New App Required:** The new PWA must be installed on all ChromeOS devices used for testing.
- **Easy Setup:** Step-by-step instructions for setup and configuration are included in this guide below.
- **Extension Pairing:** The PWA will work alongside a Chrome extension to support secure kiosk testing.
- **Test the New App Before Administration Starts:** We strongly recommend schools and districts coordinate with their ChromeOS administrators to install and test the new PWA on devices at least 4 weeks in advance of the administration window.

Key Stages in the Setup Process

- **Technology Setup:** Review general guidelines and setup information.
- **Uninstall the legacy MCAS Chrome App:** Remove the legacy MCAS Chrome app from your Google Admin Console if it was previously installed.
- **Install the new MCAS Web App for ChromeOS:** Install the new PWA and its accompanying extension.
- **Configure Device Settings:** Configure your Google Admin Console with the recommended device settings.

Step 1: Set up your school technology.

Review section II: [Technology Guidelines](#) and section III: [Technology Setup](#) in detail.

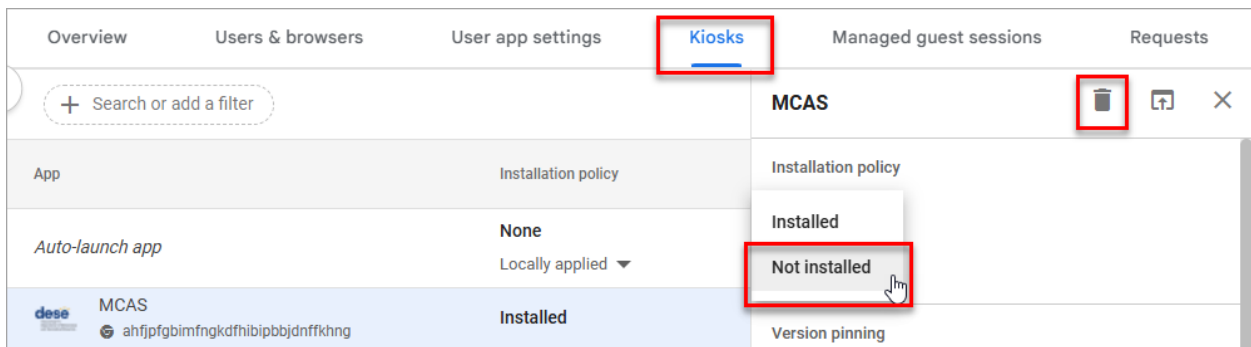
Step 2: If you have the 2024–25 MCAS Student Kiosk app installed, uninstall it by following the directions below.

If your school installed the MCAS Chrome app the previous year, follow the steps below to remove the legacy MCAS Chrome App before adding the MCAS web app for ChromeOS. If you are installing the MCAS Student Kiosk on your Chrome devices for the first time, please skip to step 3: Install the MCAS web app for ChromeOS.

Uninstall the legacy MCAS Chrome App

1. Sign in to the **Google Admin Console**.

2. On the left side, navigate to: **Devices > Chrome > Apps & extensions**.
3. Select the **Kiosks** tab at the top of the page.
4. Select the **organizational unit** for which you want to uninstall the legacy MCAS Chrome App.
5. Select **Not installed** and then **Save** to remove the app from the Chromebooks in the organizational unit. Alternatively, you can go to your top-most organization unit and select the **Delete** icon and then select **Save** to delete the app completely from your Google Admin Console.

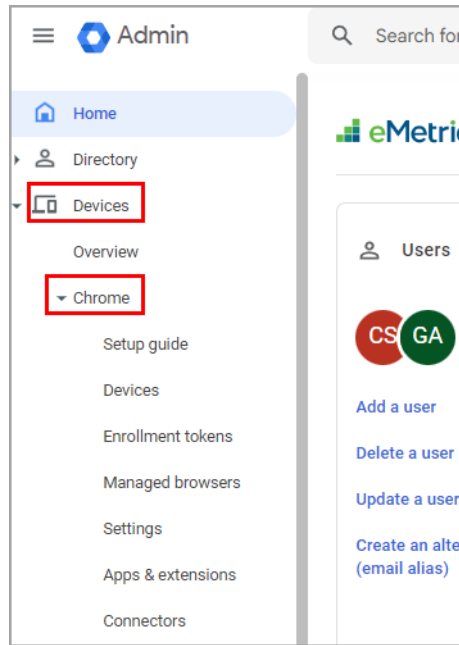


6. Once the MCAS Chrome App has been removed, follow the steps below for installing the MCAS web app and extension.

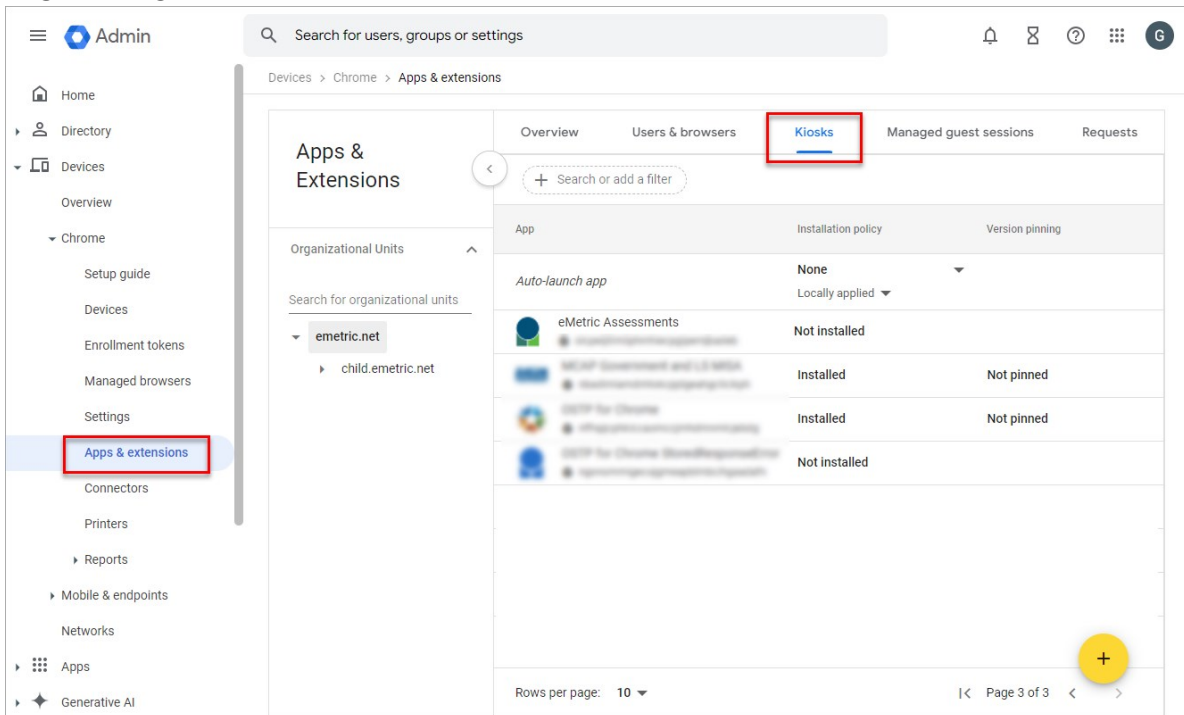
Note: If you do not have a dedicated TC, a DTC or STC can complete all the technology coordinator tasks. Ensure you have the correct administrative rights to make changes to student testing devices.

Step 3: Install the New MCAS Web App for ChromeOS

1. As the Chromebook administrator, log in to your ChromeOS management console (<https://admin.google.com>).
2. Expand the **Devices** menu, and then select **Chrome**.

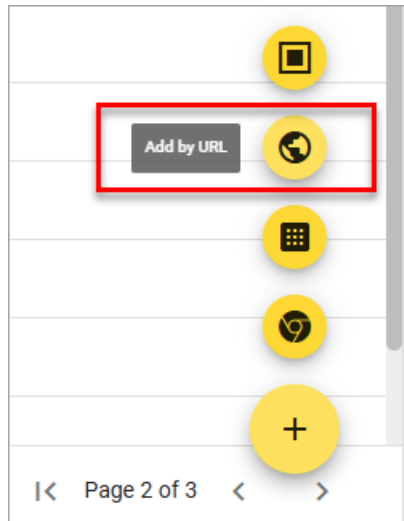


3. Select **Apps & Extensions** and then **Kiosks** and select the **organizational unit (OU)** for which you want to install the MCAS Web App and Extension for ChromeOS.



Note: Ensure that child organizational units inherit the app and policy settings from the parent OU. If inheritance is disabled, the kiosk app will not appear on devices in those child OUs and the policy settings and app must be installed locally in the desired child OU.

4. Expand the **yellow + button** in the bottom-right corner and select **Add by URL**.



5. Enter <https://mcas.cognia.org/student> and select **Save**.

A screenshot of a dialog box titled 'Add by URL'. The dialog has a blue header with the title. Below the header, there is a text area with the instruction: 'Add by URL to install a progressive web app or create a shortcut to a website in Kiosk'. Underneath, the label 'URL' is followed by a text input field containing the URL 'https://mcas.cognia.org/student'. A note at the bottom states: 'Note: this feature requires ChromeOS version 81 or later'. At the bottom right, there are two buttons: 'CANCEL' and 'SAVE'. The 'SAVE' button is highlighted with a red rectangular box.

6. Google will then prompt you to allow permissions to this app. Select **Agree**.

Note: Adding web apps in Kiosk

You have selected to add a web app in Kiosk. For web apps to work properly in Kiosk, all permissions will be granted without requesting end users' consent (for example, permissions to access the camera and microphone). Therefore, you should only add web apps that you fully trust. If you add a web app in Kiosk you understand that:


- Permissions will be automatically granted only when they are requested from the web app origin. Permission requests from a different origin will be automatically rejected. If this web app uses more than one URL origin, you can define additional origins under the Additional URL origins policy. All the origins defined in this policy will get permissions automatically granted.
- Permissions used by the web app may change over time. Any new permission will be automatically granted, provided they are requested from the web app origin.
- Permissions will be granted or rejected as mentioned above without notifying you or the end user.

In adding this web app you authorize and instruct Google to grant permissions as mentioned above.

CANCEL

AGREE

7. The new MCAS web app for ChromeOS appears in the app list.

App	Installation policy	Version pinning
<i>Auto-launch app</i>	None ▼ Locally applied ▼	
 MCAS https://mcas.cognia.org/student		Installed

8. Select the MCAS app and scroll down the right-side bar to **Additional URL origins** field to add the following URL, exactly as shown, <https://mcas-practicetest.cognia.org>.

Additional URL origins for this kiosk app

If this app uses more than one URL origin, enter the additional origins. All specified origins will get permissions automatically granted. Permissions will be rejected for any other origins not included in this list. [Learn more](#)

Additional URL origins

https://mcas-practicetest.cognia.org

One origin per line. Maximum characters allowed: 10000.

Locally applied ▼

9. Scroll down further on the right-side bar to the **Extension** section. Click **ADD EXTENSION** and from the pop-up list select **Add from Chrome Web Store**.

Extensions

Inherited from Google default

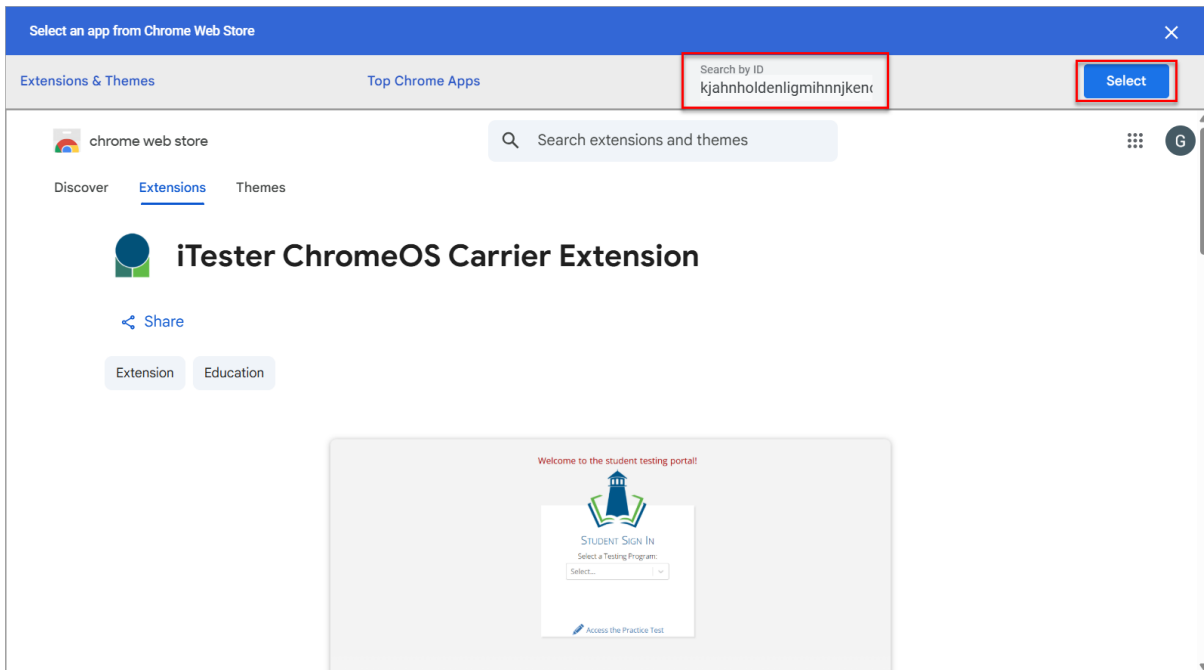
Add from Chrome Web Store

Add from a custom URL

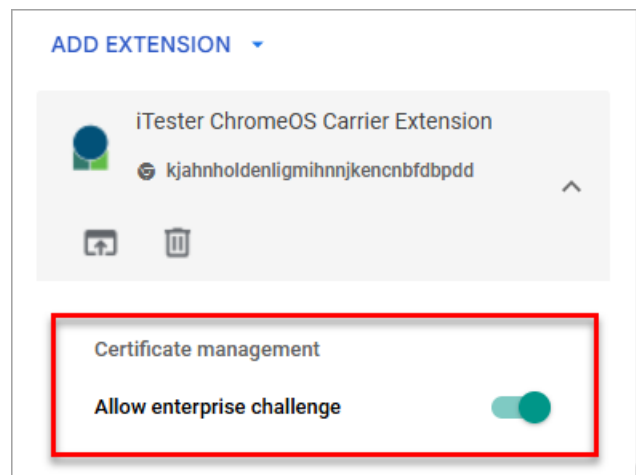
ADD EXTENSION ▼

10. In the Chrome Web Store, ensure the iTester ChromeOS Carrier extension ID is entered exactly as it is shown below, with no additional spaces, in the **Search by ID** text box and then select the **Select** button to add the extension.

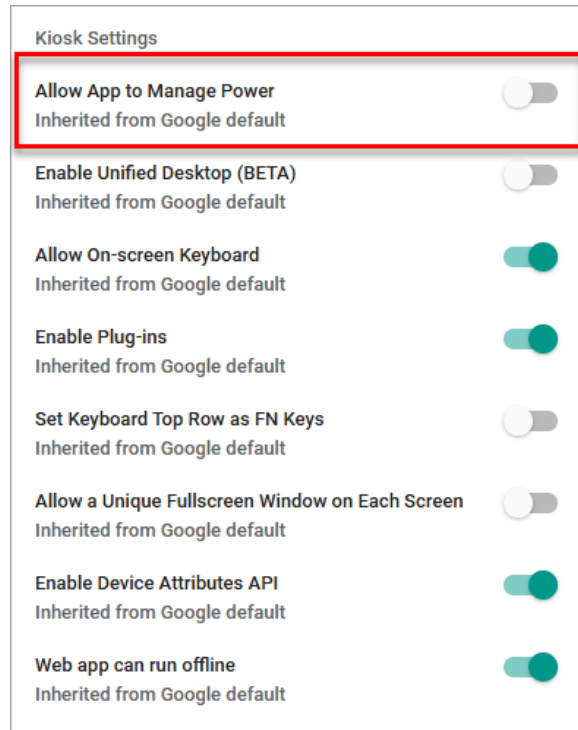
- **kjahnholdenligmihnnjkencnbfdbpdd**



11. Once the extension has been added you need to enable **Allow enterprise challenge**. Under **Certificate management**, enable **Allow enterprise challenge** setting by moving the slider to the right. When it is enabled, it will show as green.

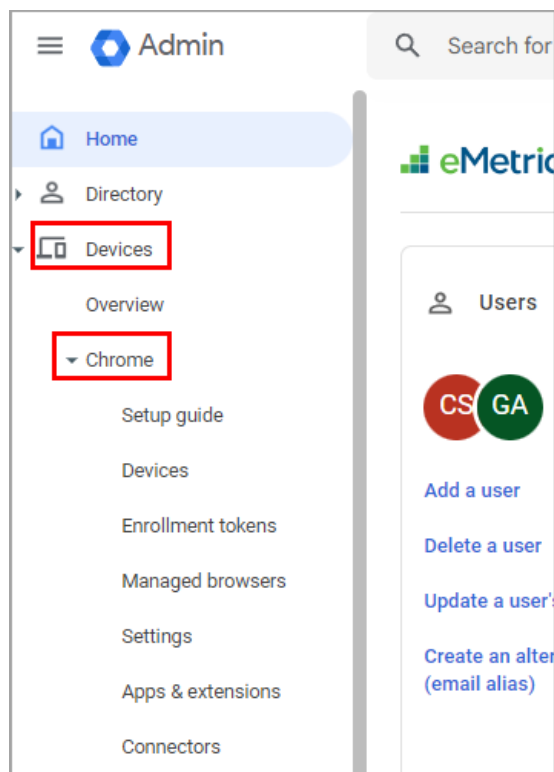


Important Note: Verify in Kiosk Settings that “Allow App to manage power” is **disabled**. To do this, click on **Devices, Apps & Extensions** and then select **Kiosks**. Click on the **MCAS** app name and check to make sure the setting **Allow app to manage power** is **disabled** (slider is moved to the left and not green).

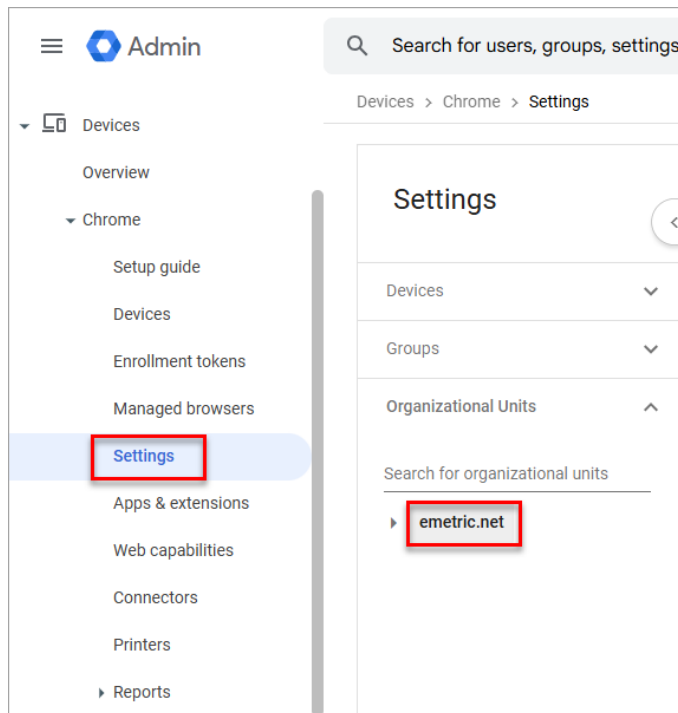


Step 4: Configure Device Settings






























1. In your Google Admin console, navigate to **Devices**, then select **Chrome**.



2. Click on **Settings** and then choose the relevant **Organizational Unit** where the MCAS web app is installed. In the example below the top Organizational Unit is emetric.net.



3. Select the **Device settings** tab. Scroll to **Enrollment and access** and select **Verified mode**. Verified Mode ensures that only enrolled and trusted ChromeOS devices can run the ChromeOS PWA, and your testing environment remains secure and authenticated.

User & browser settings		Device settings		Managed guest session settings	
Show: All		Search or add a filter		Recent changes	
<div style="border: 1px solid red; padding: 2px; display: inline-block;">  Enrollment and access </div>					
Setting	Configuration	Inheritance	Supported on		
Forced re-enrollment	Force device to automatically re-enroll after wiping	Locally applied	   		
Asset identifier input after zero touch enrollment	Do not allow asset ID and location to be entered for devices enrolled via zero touch enrollment	Google default	   		
Powerwash	Allow powerwash to be triggered	Google default	   		
Verified access	Enable for content protection	Locally applied	   		
Verified mode	3 sub settings	Locally applied	   		
Disabled device return instructions	Please contact eMetric, LLC by phone at (210) 496-6500	Locally applied	   		
Integrated FIDO second factor	Allow the user to decide	Google default	   		

4. Set configuration to: **Required verified mode boot for verified access.**

Verified mode

Devices ▼

Organizational Units ▲

Search for organizational units

▶ **emetric.net**

About this setting

Specifies whether verified boot mode is required for enrolled devices.

Choose from:

- Require verified mode boot for verified access**—Devices must be running in verified boot mode for device verification to succeed. Devices in Dev mode will always fail the verified access check.
- Skip boot mode check for verified access—Allows devices in Dev mode to pass the verified access check. [Show more](#)

Inheritance: Locally applied ▼

Configuration: Require verified mode boot for verified access

Related settings

[Verified Mode](#) ↗

By default, Skip boot mode check for Verified Access is selected,...

[Verified access](#) ↗

Controls whether web services can verify that a device is running...

5. In **Verified mode**, ensure the verified access service account is entered exactly as displayed below in the **Services with full access** section. We recommend entering this manually.

- If using copy-paste, right click the email address and select **Copy email address**. Once pasted, ensure all hyphens are included and that there are no spaces before, within, or after the service account text.

emetric-verify-access-api@civil-glyph-433121-j9.iam.gserviceaccount.com

- Then select **Save**.

The screenshot displays the 'Verified mode' configuration page. On the left, there is a sidebar with 'Verified mode' selected. The main content area is divided into 'About this setting' and 'Configuration'. Under 'About this setting', there is a description and a 'Choose from:' section with two options: 'Require verified mode boot for verified access' (selected) and 'Skip boot mode check for verified access'. The 'Configuration' section shows 'Inheritance' as 'Locally applied' and 'Configuration' as 'Require verified mode boot for verified access'. A text area labeled 'Services with full access' contains the email address 'emetric-verify-access-api@civil-glyph-433121-j9.iam.gserviceaccount.com'. Below this text area is a note: 'Service accounts which are allowed to receive device ID. Put one pattern on each line.' At the bottom left, there is a blue 'Save' button and a 'Cancel' link.

Note: Pay close attention when entering the service account, as any typos or added characters will prevent the app from entering kiosk mode.

6. Scroll to the **User Data** section under **Sign-In Settings**.

The screenshot shows the Google Admin console interface. At the top, there is a search bar and navigation icons. The breadcrumb trail reads 'Devices > Chrome > Settings'. The main content area is divided into three tabs: 'User & browser settings', 'Device settings' (which is selected and highlighted with a red box), and 'Managed guest session settings'. Below the tabs, there is a 'Show: All' button and a search filter. The 'Organizational Units' sidebar on the left shows 'emetric.net' and its sub-unit 'child.emetric.net'. The main table lists various settings. The 'User data' setting is highlighted with a red box, and a red arrow points to it from the left. The table has columns for 'Setting', 'Configuration', 'Inheritance', and 'Supported on'.

Setting	Configuration	Inheritance	Supported on
Sign-in settings			
Sign-in screen	Always show user names and photos	Locally applied	Android, iOS
Device off hours	Edit in legacy view	Locally applied	Android, iOS
Device wallpaper image		Locally applied	Android, iOS
User data	Do not erase local user data	Locally applied	Android, iOS
Single sign-on IdP redirection	Take users to the default Google sign-in screen	Locally applied	Android, iOS

7. Verify that **Do not erase all local data** is set; if not, click on **User Data** to update the setting with the drop-down menu and click **Save**.

The screenshot shows the 'User data' configuration page. The breadcrumb trail reads 'Devices > Chrome > Settings > Device > User data'. The page has a left sidebar with 'Organizational Units' and a search bar. The main content area contains a description of the setting, a note, and configuration options. The 'Configuration' section is highlighted with a red box, showing the option 'Do not erase local user data' selected. The 'Save' button is also highlighted with a red box.

User data

Specifies whether enrolled ChromeOS devices delete all locally-stored settings and user data every time a user signs out. Data the device synchronizes persists in the cloud but not on the device itself. If you set it to **Erase all local user data**, the storage available to the users is limited to half the RAM capacity of the device. If the policy is set together with a managed guest session, it won't cache the session name or avatar.

Note: By default, ChromeOS devices encrypt all user data and automatically clean up disk space when shared by multiple users. This default behavior works best for most deployments and ensures data security and an optimal user experience. We recommend you enable **Erase all local user data** rarely and selectively.


Chromium name: [DeviceEphemeralUsersEnabled](#)

Supported on: ChromeOS since version 19

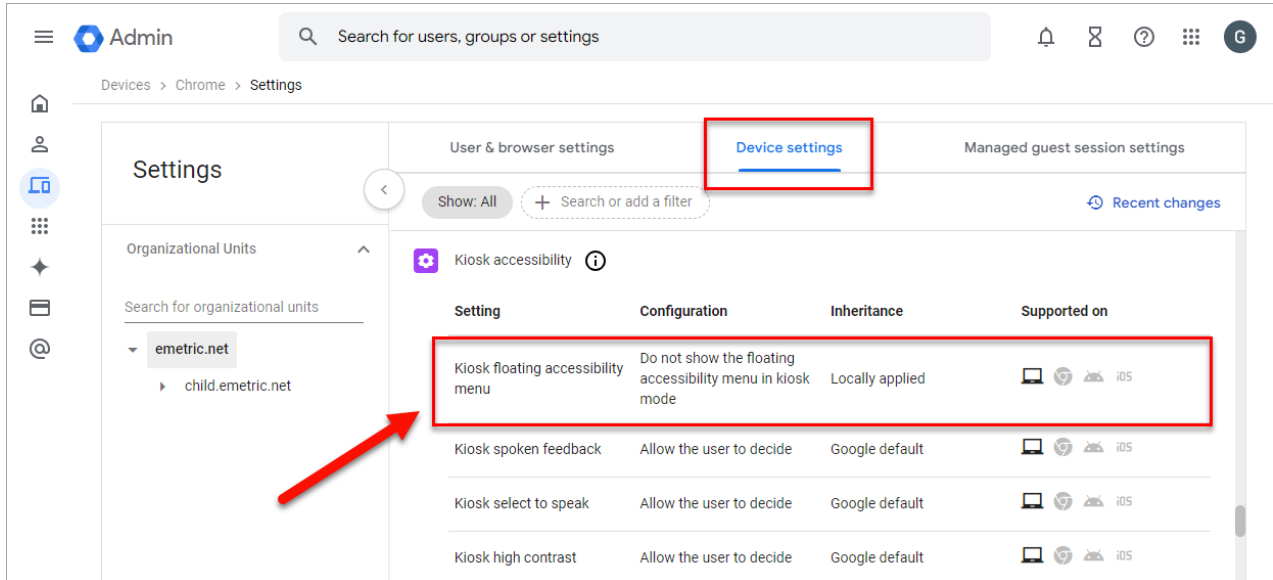
Inheritance: Locally applied

Configuration: Erase all local user info, settings, and state after each sign-out
Do not erase local user data

Save Cancel

 **Note:** This setting is crucial to allow Chrome local storage to be used to store student responses if network connectivity is lost. If this is not configured, student responses will not be saved to the device in the case of internet disruptions.

8. Scroll to the **Kiosk Floating Accessibility Menu** in the **Kiosk Accessibility** section.



The screenshot shows the Google Admin console interface. The top navigation bar includes the 'Admin' logo, a search bar for users, groups, or settings, and utility icons. The breadcrumb trail indicates the path: 'Devices > Chrome > Settings'. The main content area is divided into three tabs: 'User & browser settings', 'Device settings' (highlighted with a red box), and 'Managed guest session settings'. Under 'Device settings', there is a 'Kiosk accessibility' section. A table lists several settings, with the first row, 'Kiosk floating accessibility menu', highlighted by a red box. A red arrow points to this row from the left. The table columns are 'Setting', 'Configuration', 'Inheritance', and 'Supported on'.

Setting	Configuration	Inheritance	Supported on
Kiosk floating accessibility menu	Do not show the floating accessibility menu in kiosk mode	Locally applied	Windows, macOS, Linux, iOS
Kiosk spoken feedback	Allow the user to decide	Google default	Windows, macOS, Linux, iOS
Kiosk select to speak	Allow the user to decide	Google default	Windows, macOS, Linux, iOS
Kiosk high contrast	Allow the user to decide	Google default	Windows, macOS, Linux, iOS

9. Verify that **Do not show the floating accessibility menu in kiosk mode** is set; if not, click on **Kiosk Floating Accessibility Menu** to update the setting with the drop-down menu and click **Save**.

Kiosk floating accessibility menu

By default, the accessibility menu is hidden on devices running Chrome kiosk apps. If you choose **Show the floating accessibility menu in kiosk mode**, the accessibility menu is always visible on devices. The menu appears at the bottom right corner of the screen. To prevent the menu from blocking app components, such as buttons, users can move it to any screen corner.

Even if **Do not show the floating accessibility menu in kiosk mode** is selected, users can still enable accessibility features using shortcuts—as long as you have not used the Admin console to turn off the individual accessibility setting and a shortcut exists for it. For details, see [Chromebook keyboard shortcuts](#).

Note: Ordinarily, the **Shift + Alt + L** shortcuts focus on the launcher button and items on the shelf. However, on devices running Chrome kiosk apps, they focus on the accessibility menu instead.

Chromium name	Supported on
FloatingAccessibilityMenuEnabled	ChromeOS since version 84

Inheritance: Locally applied

Configuration: Do not show the floating accessibility menu in kiosk mode

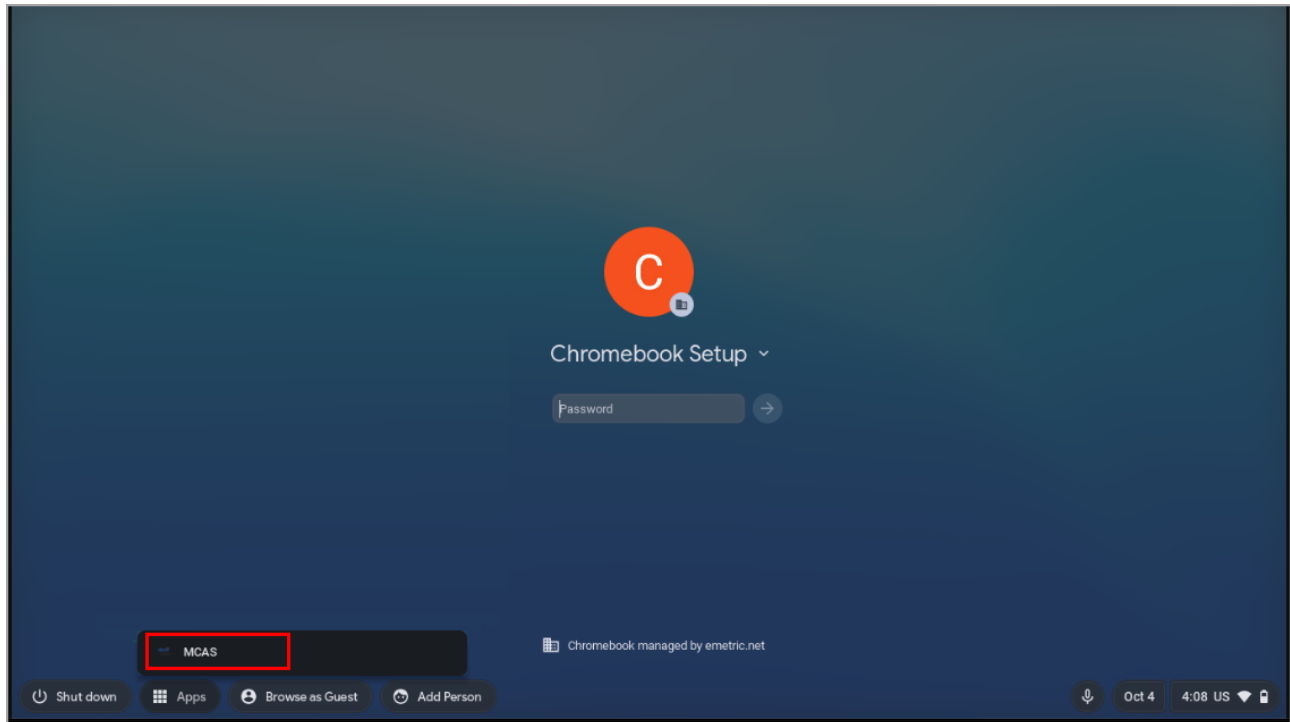
Buttons: Save, Cancel



Note: Students with accommodations that are embedded within the MCAS Student Kiosk, including text-to-speech, word prediction, and speech-to-text, will access these accommodations directly through the MCAS Student Kiosk as they are delivered by the test platform. ChromeOS contains native accessibility features that may appear within the kiosk with a floating menu. Technology coordinators should disable the floating accessibility menu in Google Admin before testing occurs to avoid issues.

Note on Managed Guest Sessions: To avoid students inadvertently entering guest sessions, we recommend disabling managed guest sessions on OUs used for testing. To disable, on the Settings page select the **Managed guest session settings** tab and then select **Managed guest session**. Ensure that Managed guest session is set to **Do not allow managed guest sessions** and click **Save**.

When these steps are completed, the MCAS web app will appear on all Chromebook devices that are in your domain.



Important Note: Students should not log in to Chromebooks using their Google accounts to take an operational test. When the Chromebooks are turned on, simply click the **Apps** link in the bottom row and select the **MCAS** app. The kiosk will open in full- screen mode.

For more information, see the following links:

- [Use Chromebooks for Student Assessments](#)
Important Note: Read “Scenario 1: School sets up Chromebook™ to run as a Single App Kiosk running the exam app.” Do **not** follow the instructions for Scenarios 2 and 3.
- [Manage Device Settings](#), which provides general information for managed Chromebooks.

Once these steps have been verified, run Site Readiness prior to testing. This step is very important to ensure that the PWA has been set up correctly. Step-by-step instructions for completing Site Readiness are in [Part V: Site Readiness Testing and Site Certification](#).