D. Monitor Settings

Ensure that all monitors used for testing are set to the default color settings. If a student will use the zoom in/out tool, review the recommended screen resolutions in Table 4 below:

Table 4. Monitor Settings

Required Zoom Level for Student	Recommended Screen Resolution
100% (No Zoom)	1024 x 768 (or Higher)
150%	1920 x 1080 (or Higher)
200%	1920 x 1080 (or Higher)
300%	1920 x 1080 (or Higher)

Note: Students should use the screen resolution that is most comfortable for them; the resolutions listed are recommendations only. The student or test administrator may set the zoom level within the MCAS Student Kiosk when the student logs in at the time of testing.

IV. MCAS Student Kiosk Installation

A. ChromeOS App 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.

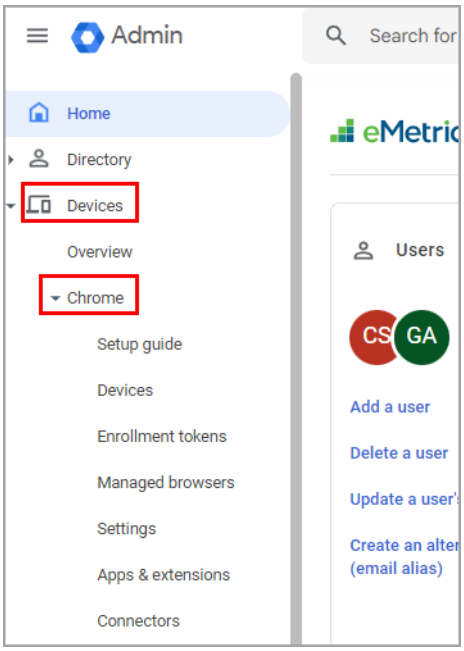
Note: For ease of copying configuration URLs into the Google Management Console, a Quick Copy Guide is available for download on the MCAS Resource Center.

Step 1: Set up your school technology.

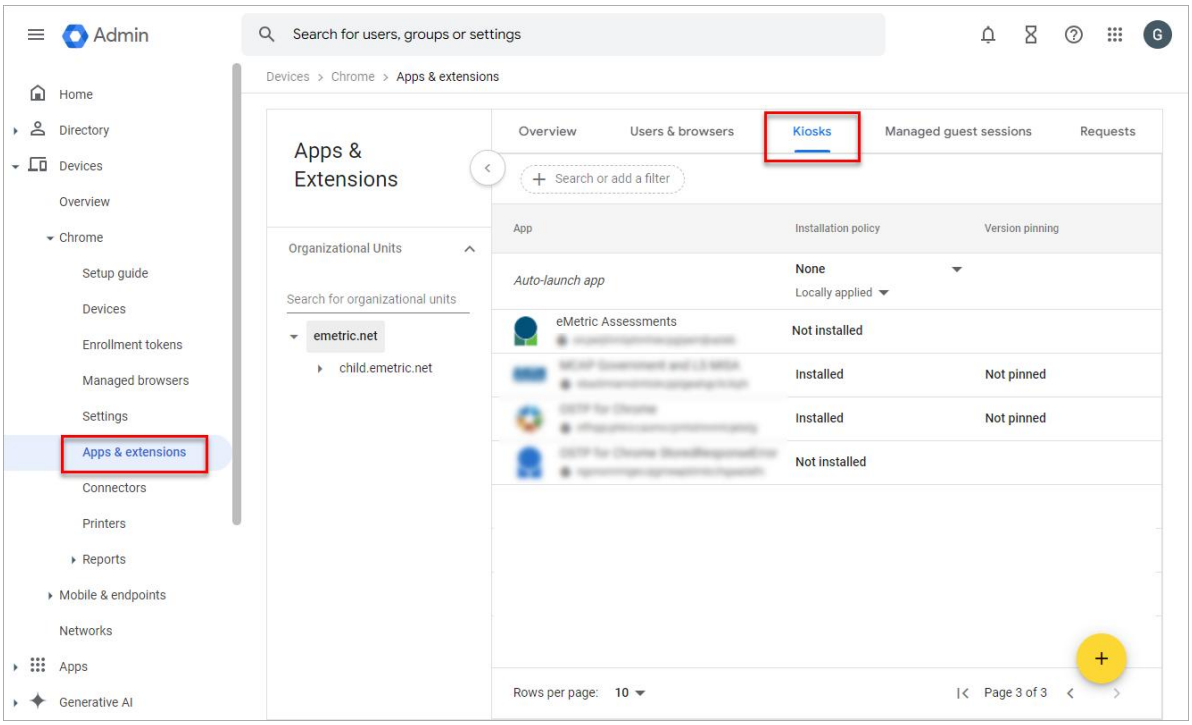
Review section II: Technology Guidelines and section III: Technology Setup in detail. If the MCAS Web App for ChromeOS was previously installed for the 2025–26 school year, confirm that all previous configuration requirements remain in place and complete steps 10–13 in the ChromeOS instructions, which outline new steps to disable Chrome Accessibility features.

Step 2: Install the 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**.

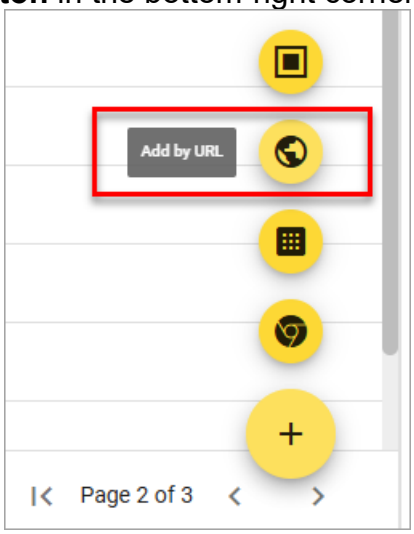


3. Select **Apps & Extensions** and then **Kiosks** and select **the organizational unit (OU) for which you want to install the MCAS Web App and Extension for ChromeOS.**

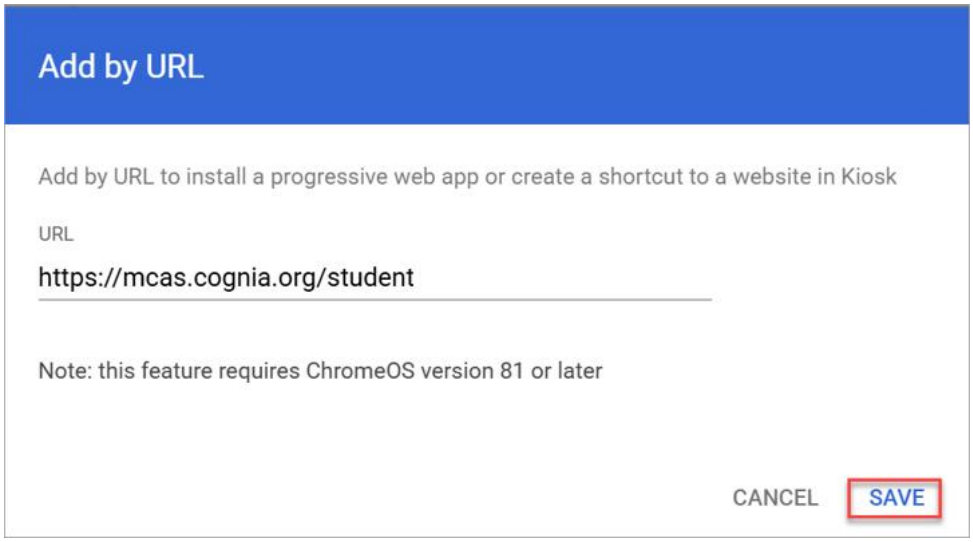


Note: Ensure that child organizational units inherit the app and policy settings from the parent OU. If inheritance is disabled, the kiosk app will not appear on devices in those child organizational units (OUs) and the policy settings and app must be installed locally in the desired child OU.

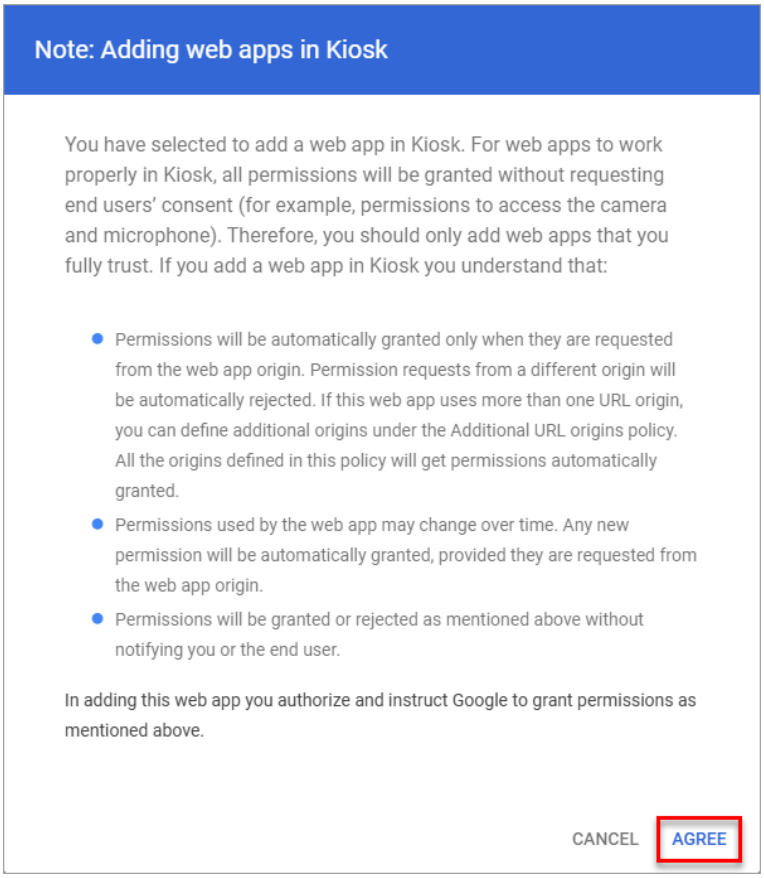
4. Expand the **yellow + button** in the bottom-right corner and select **Add by URL**.



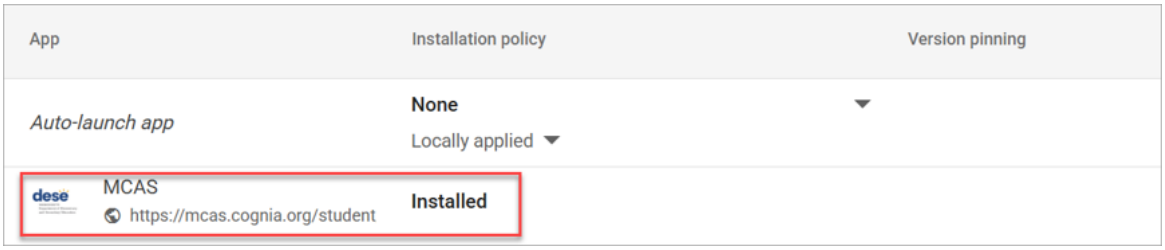
5. Enter https://mcas.cognia.org/student and select **Save.**



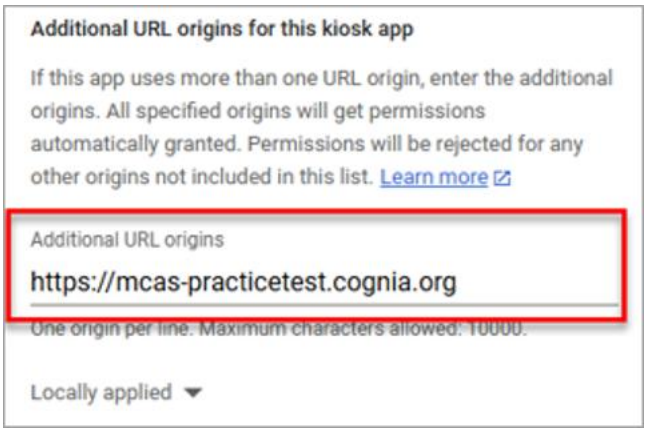
6. Google will then prompt you to allow permissions to this app. Select **Agree**.



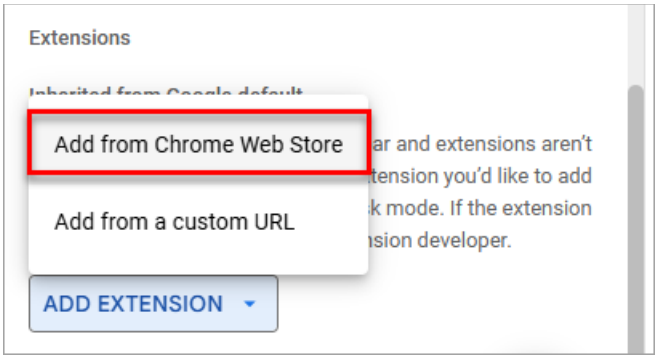
7. The MCAS web app for ChromeOS appears in the app list.



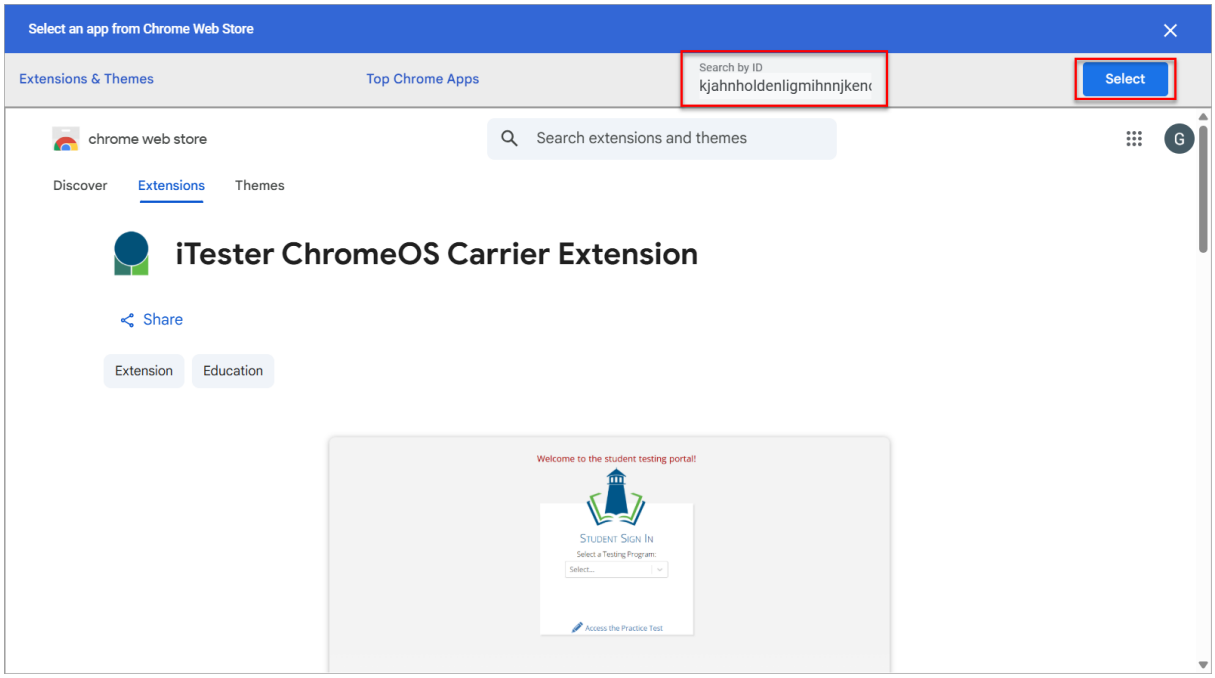
8. Select the MCAS web app and scroll down the right-side bar to **Additional URL origins** field to add the following URL, exactly as shown: https://mcas-practicetest.cognia.org.



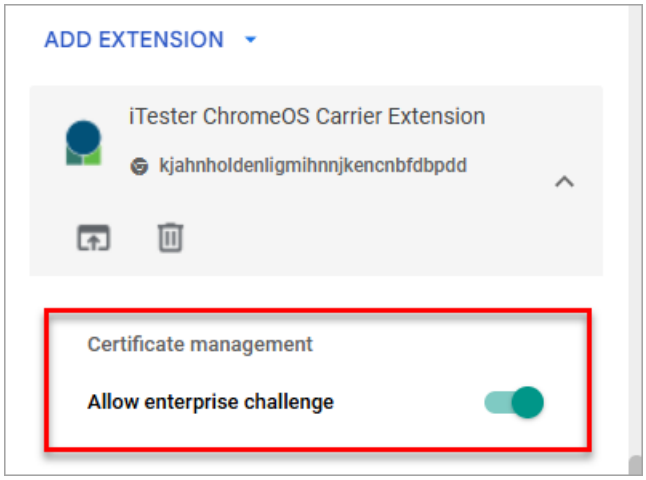
9. Scroll down further on the right-side bar to the **Extension** section. Click **ADD EXTENSION** and from the pop-up list select **Add from Chrome Web Store**.



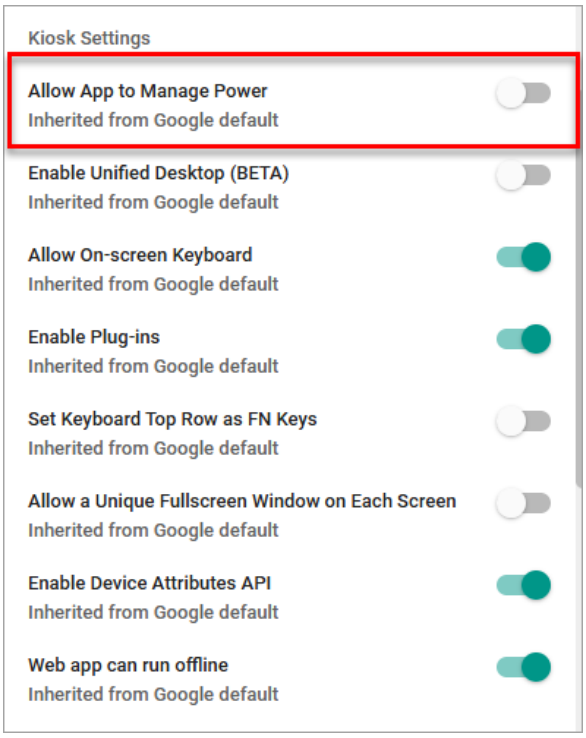
10. In the Chrome Web Store, ensure the iTester ChromeOS Carrier extension ID is entered exactly as it is shown below, with no additional spaces, in the **Search by ID** text box and then select the **Select** button to add the extension.
    - **`kjahnholdenligmihnnjkencnbfdbpdd`**



11. Once the extension has been added, 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.

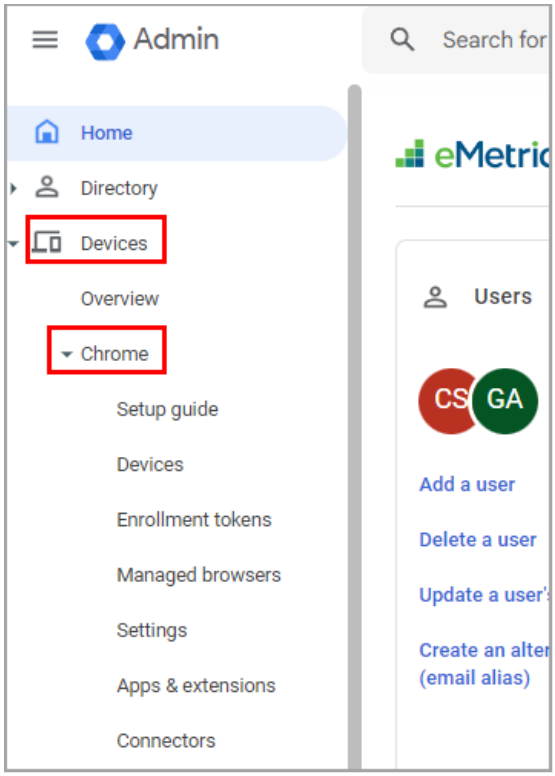


Important Note: Verify in Kiosk Settings that “Allow App to manage power” is **disabled**. To do this, click on **Devices, Apps & Extensions** and then select **Kiosks**. Click on the **MCAS** app name and check to make sure the setting **Allow App to Manage Power** is **disabled** (slider is moved to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

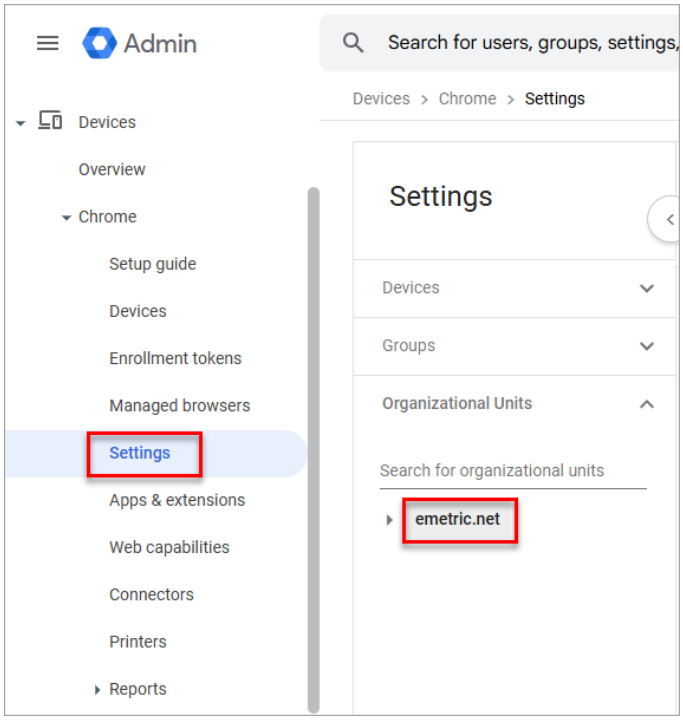


Step 3: Configure Device Settings

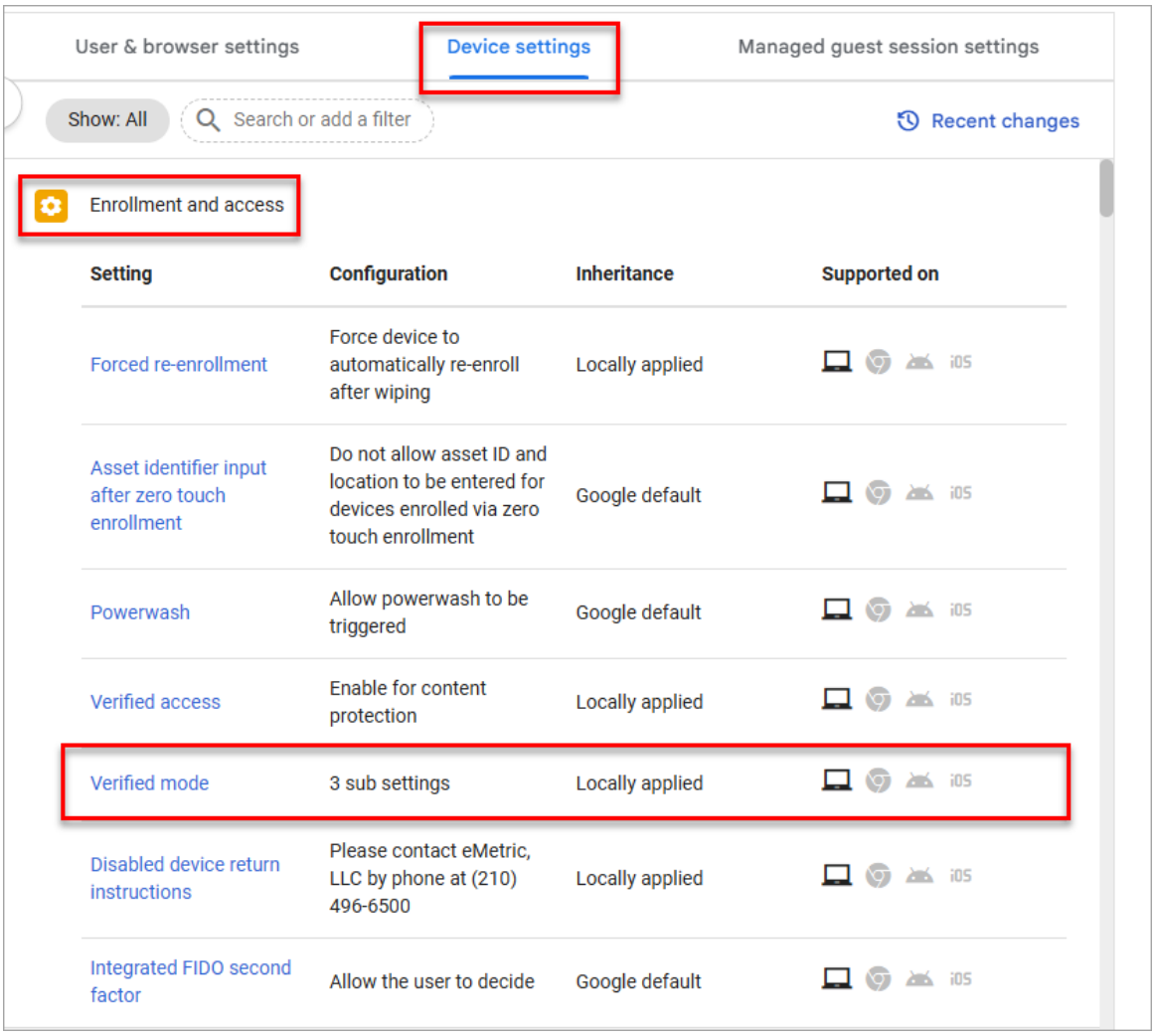
1. In your Google Admin console, navigate to **Devices,** then select **Chrome**.



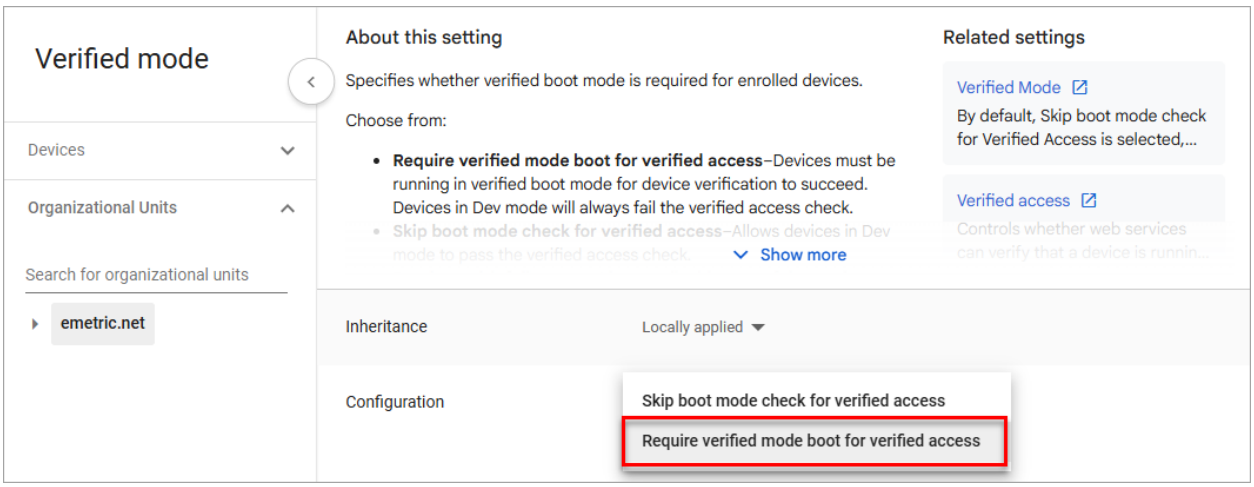
2. Click on **Settings** and then choose the relevant **Organizational Unit** where the MCAS web app is installed. In the example below the top Organizational Unit is emetric.net.



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.



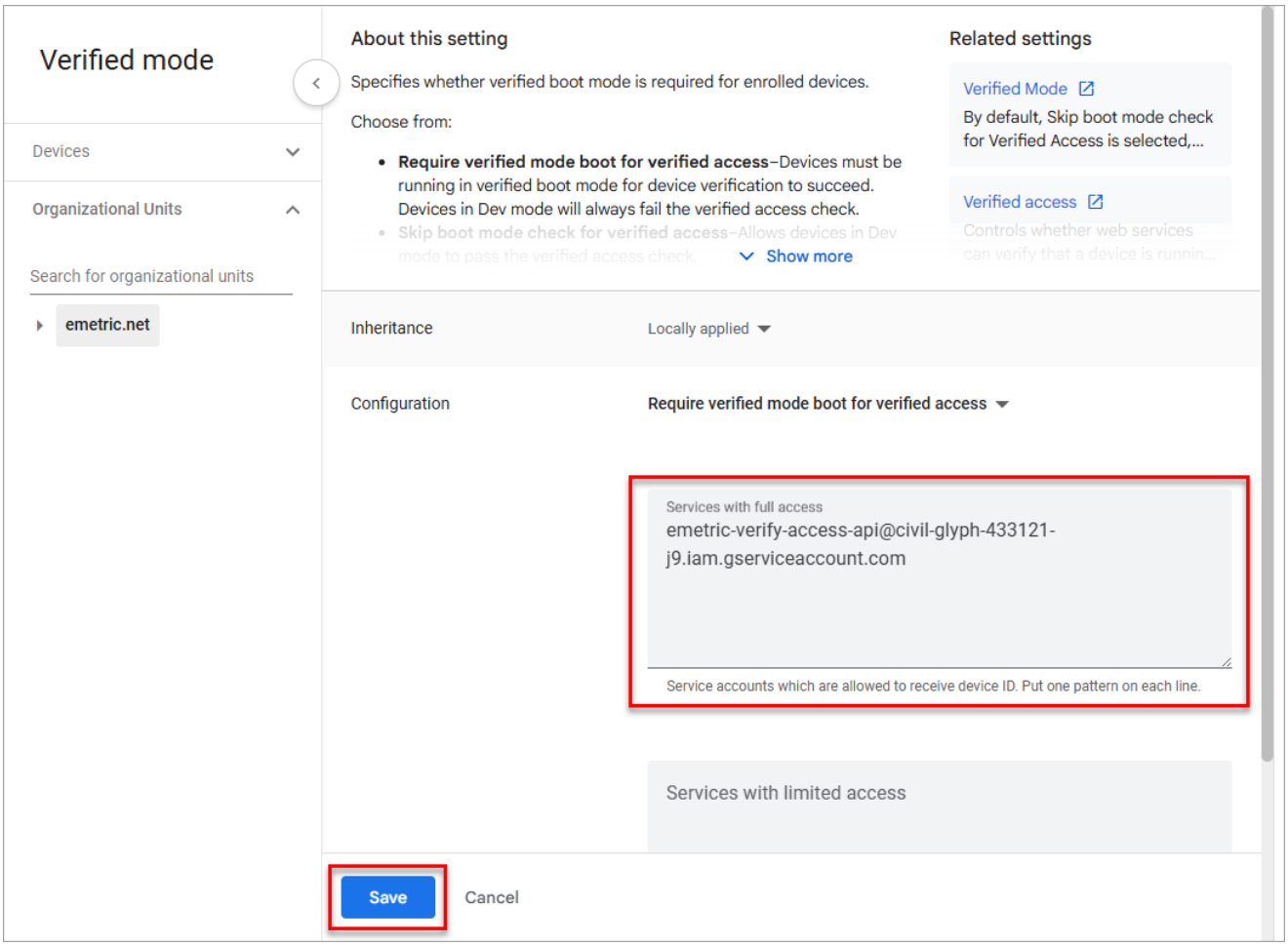
4. Set configuration to: **Required verified mode boot for verified access**.



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.
   - Ensure all hyphens are included and that there are no spaces before, within, or after the service account text:

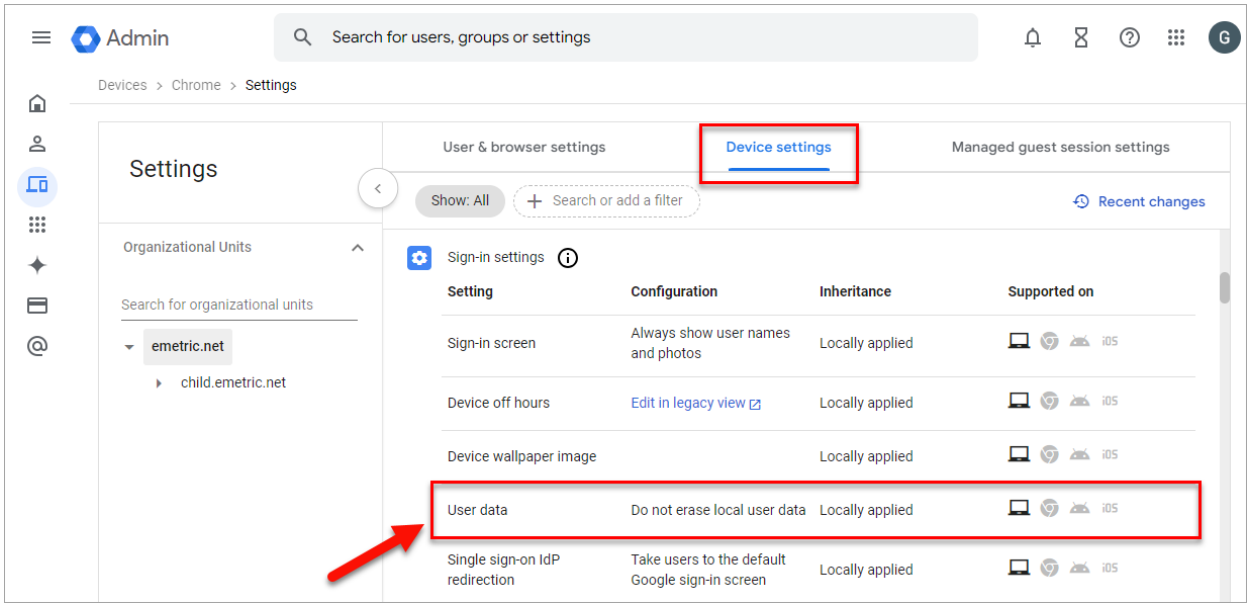
     `emetric-verify-access-api@civil-glyph-433121-j9.iam.gserviceaccount.com`

   - Then select **Save**.

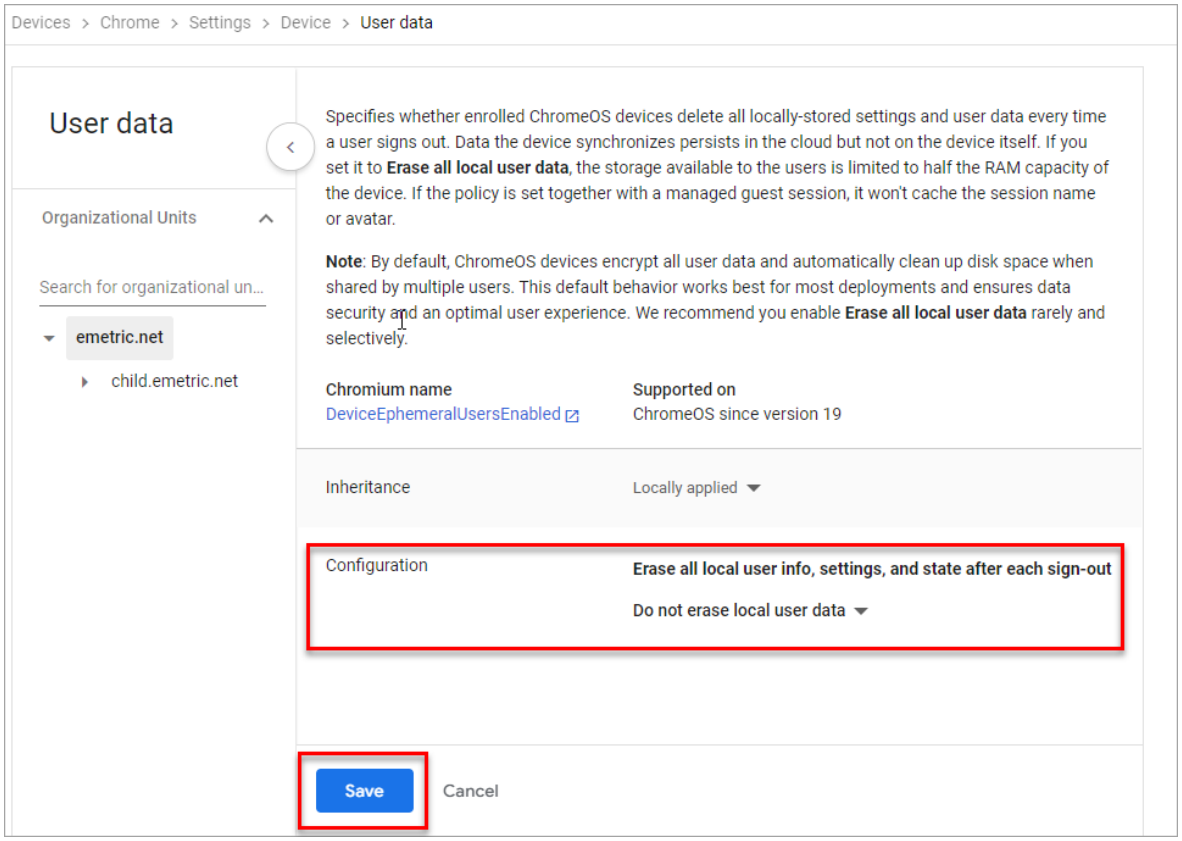


Note: Pay close attention when entering the service account, as any typos or added characters will prevent the app from entering kiosk mode.

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

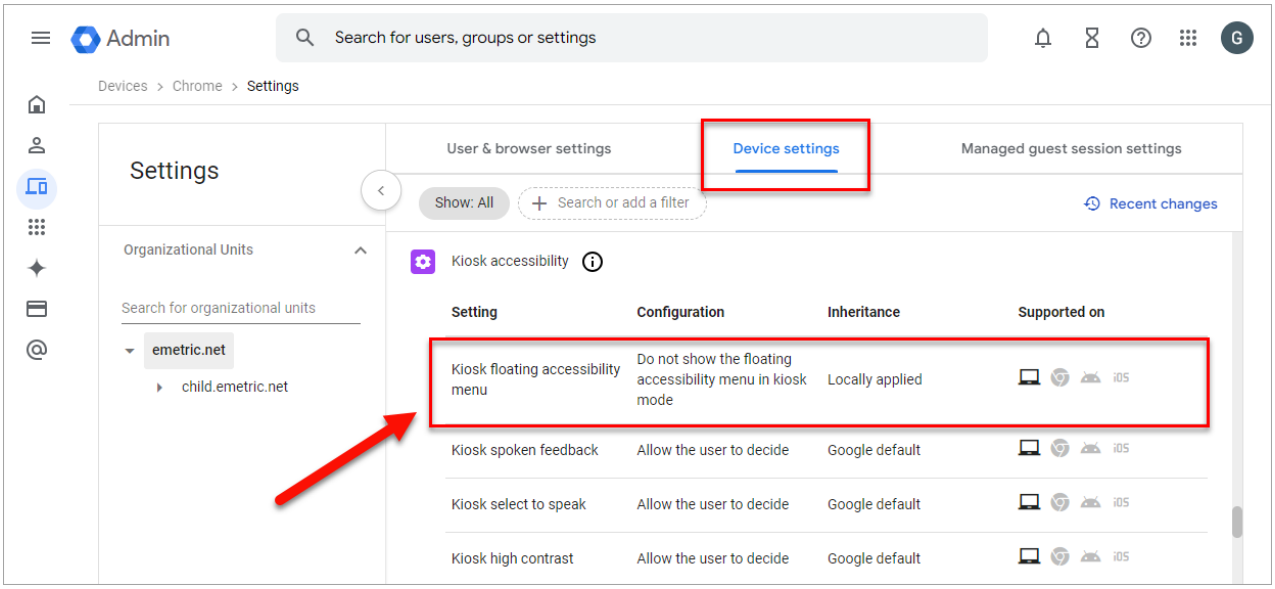


7. Verify that **Do not erase all local data** is set; if not, click on **User Data** to update the setting with the drop-down menu and click **Save**.

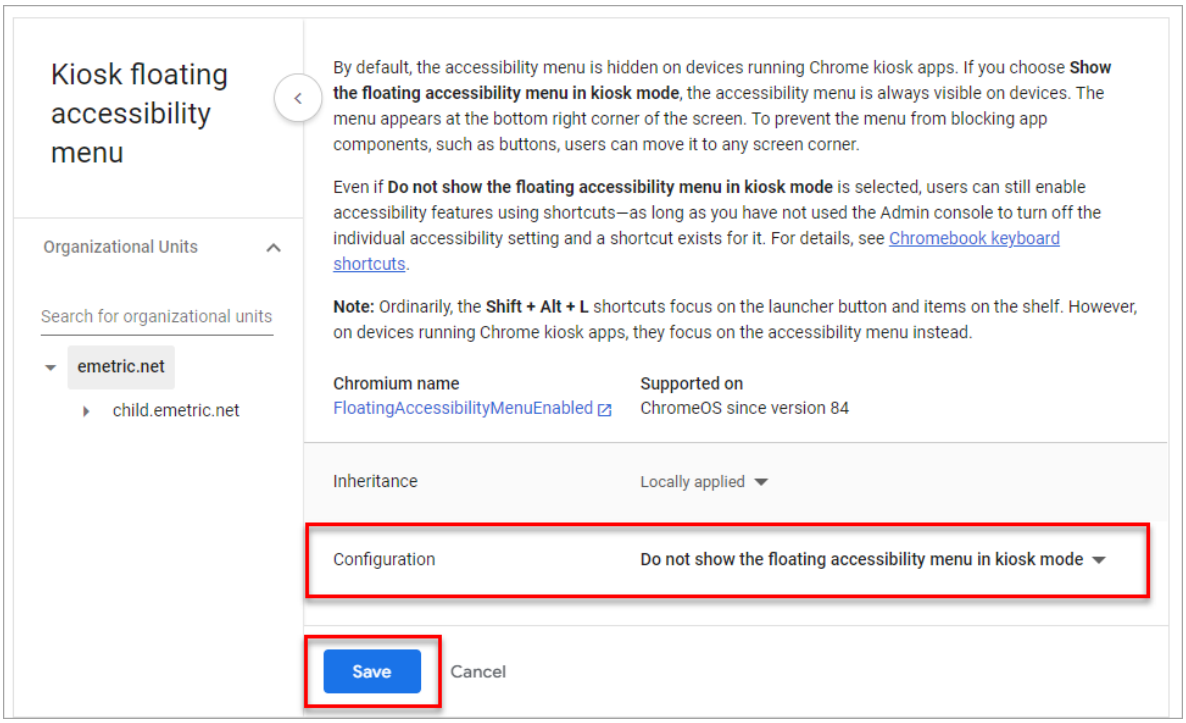


⚠ **Note:** This setting is crucial to allow Chrome local storage to be used to store student responses if network connectivity is lost. If this is not configured, student responses will not be saved to the device in the case of internet disruptions.

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



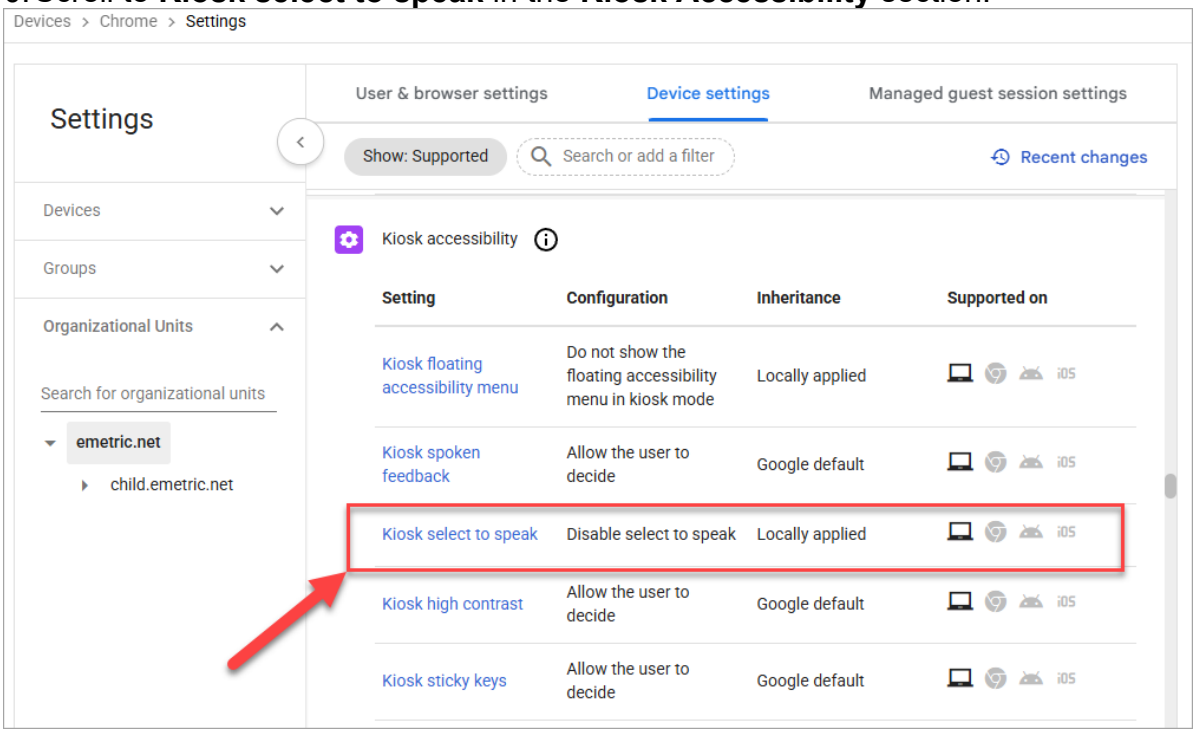
9. Verify that **Do not show the floating accessibility menu in kiosk mode** is set; if not, click on **Kiosk Floating Accessibility Menu** to update the setting with the drop-down menu and click **Save**.



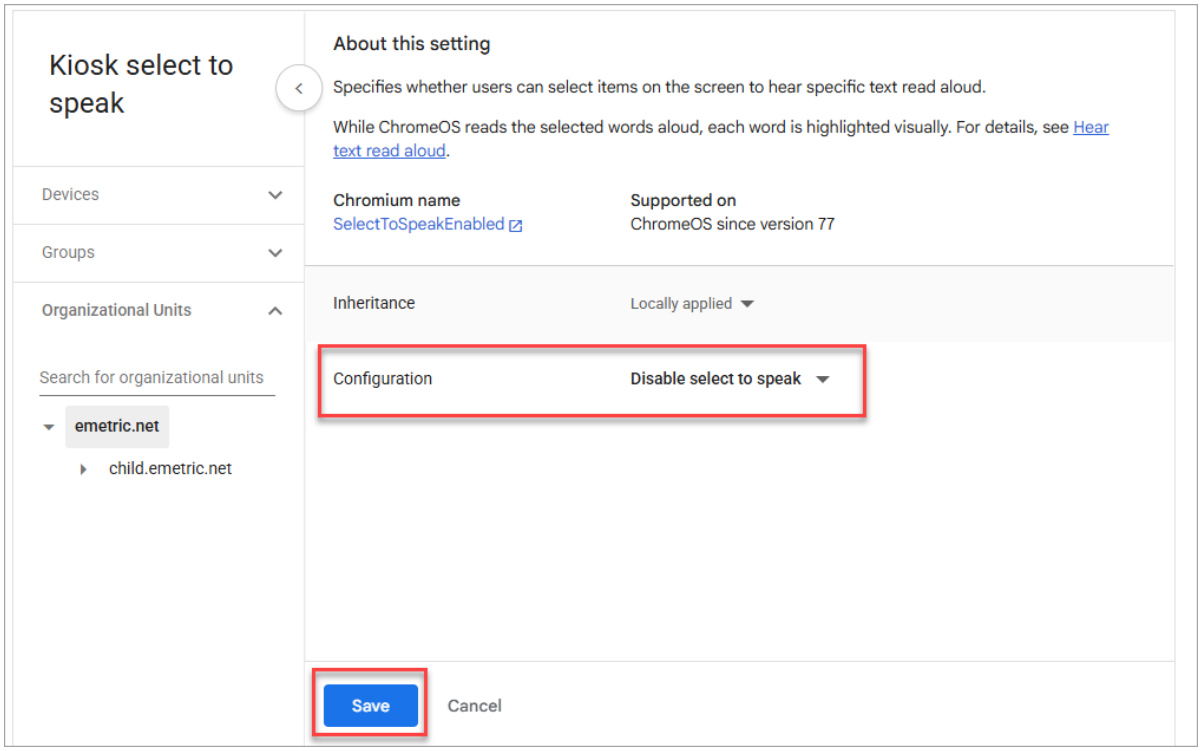
Note: Students with accommodations that are embedded within the MCAS Student Kiosk, including text-to-speech, word prediction, and speech-to-text, will access these accommodations directly through the MCAS Student Kiosk as they are delivered by the test platform. ChromeOS contains native accessibility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

New for 2026–27: Certain accessibility features are not automatically disabled by removing the floating menu above. Additional steps are required to disable these Chrome Accessibility features, as described in steps 10–13 below.

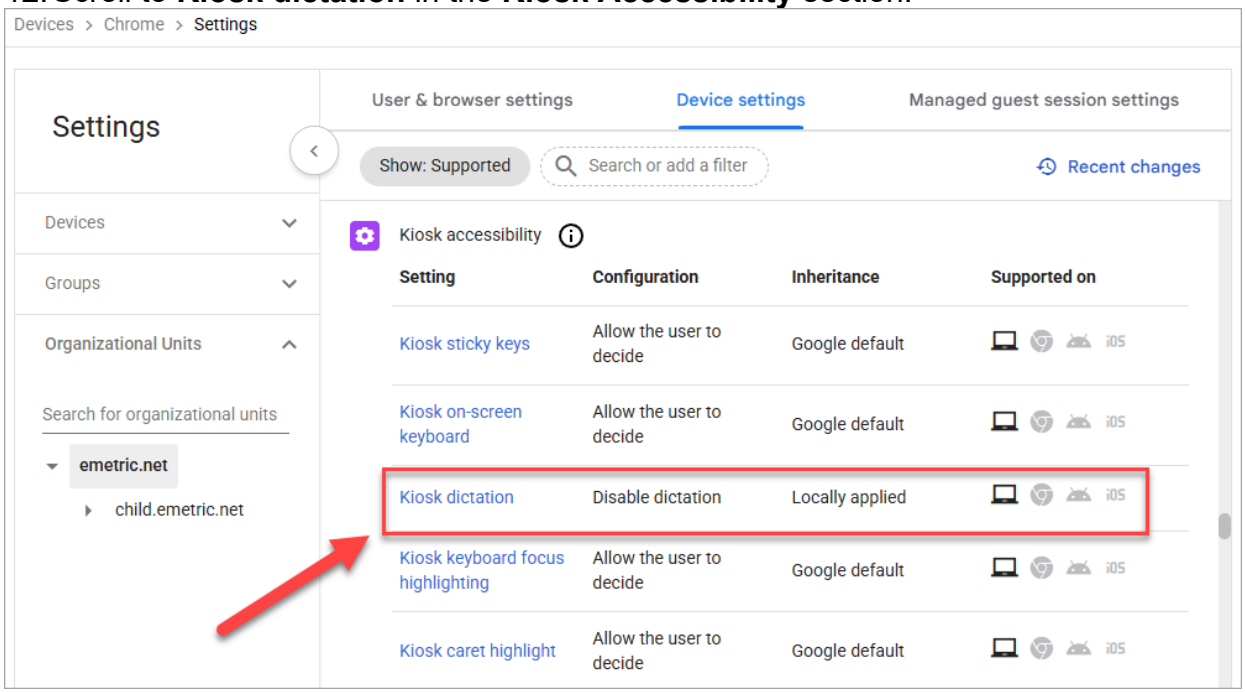
10. Scroll to **Kiosk select to speak** in the **Kiosk Accessibility** section.



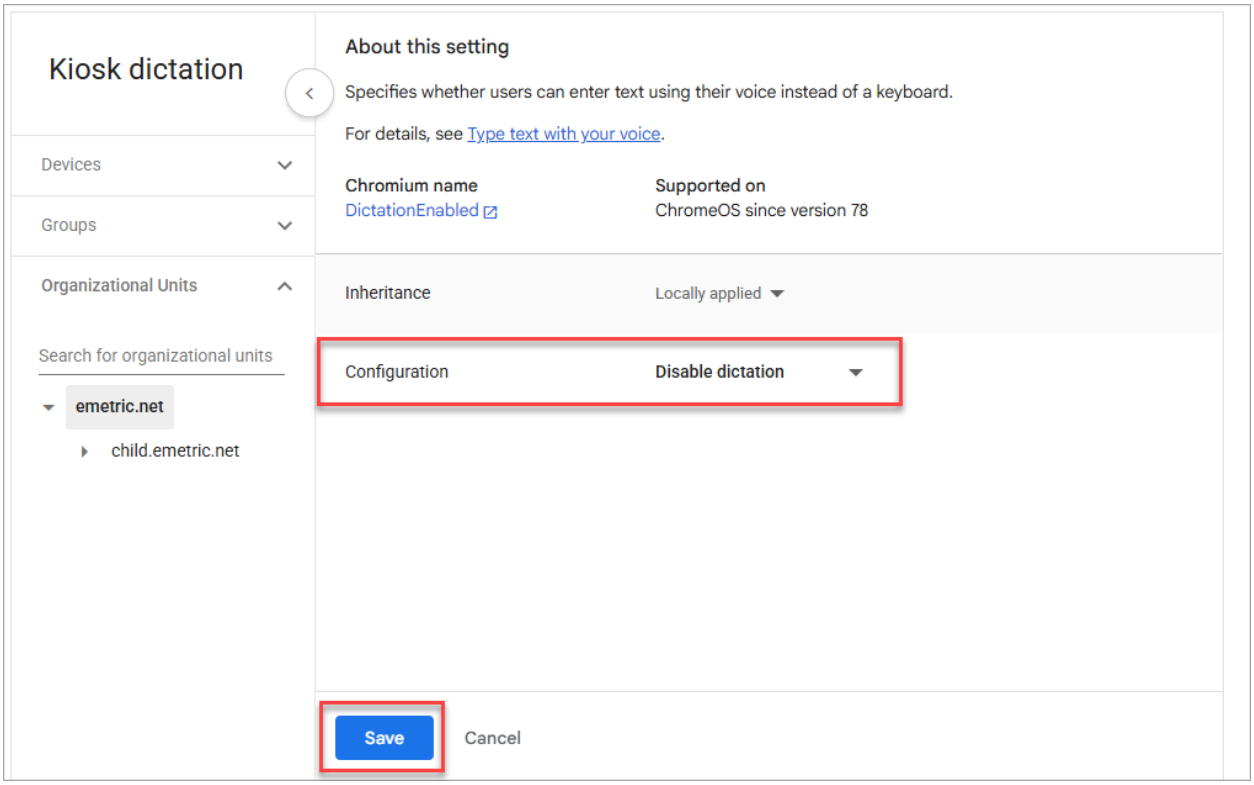
11. Verify that **Disable select to speak** is set; If not, click on **Kiosk select to speak** to update the setting with the drop-down menu and click **Save**.



12. Scroll to **Kiosk dictation** in the **Kiosk Accessibility** section.

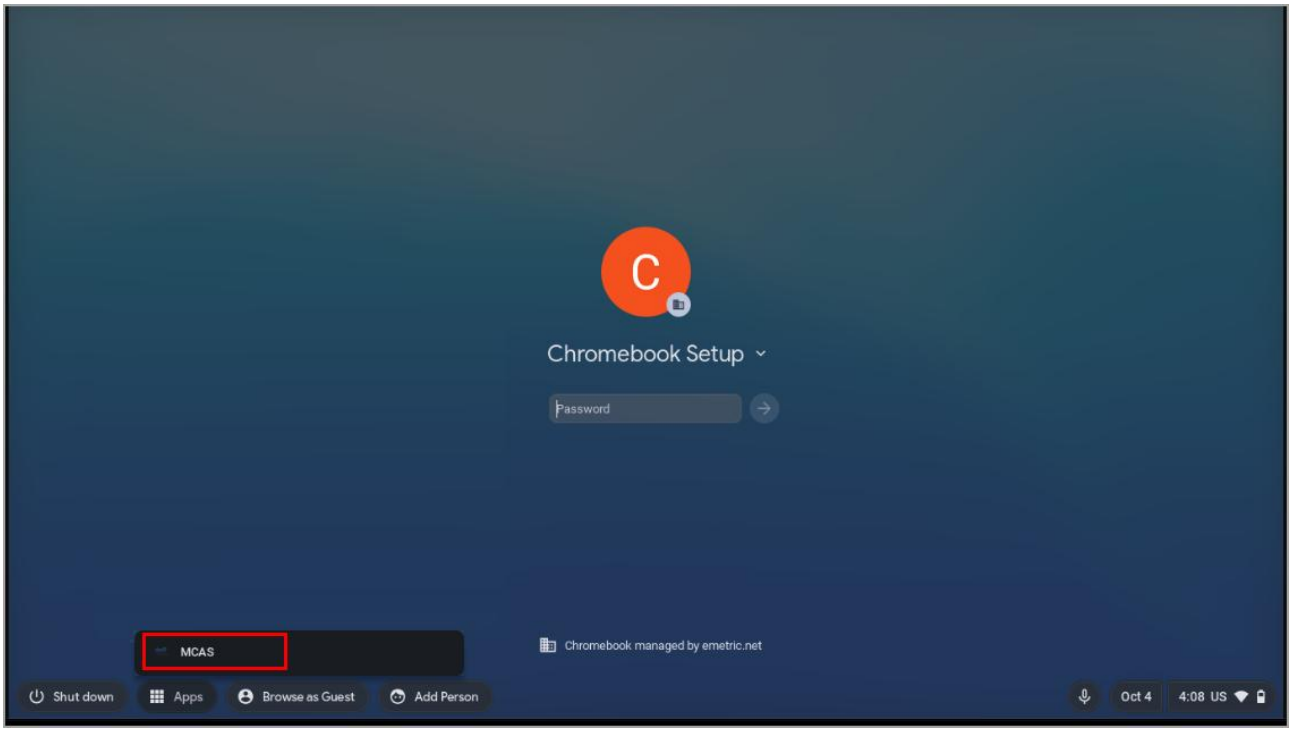


13. Verify that **Disable dictation** is set; If not, click on **Kiosk dictation** to update the setting with the drop-down menu and click **Save**.



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, refer to 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.

B. iPadOS App Installation

Step 1: Set up your school testing environment

Review section II: Technology Guidelines and section III: Technology Setup in detail.