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

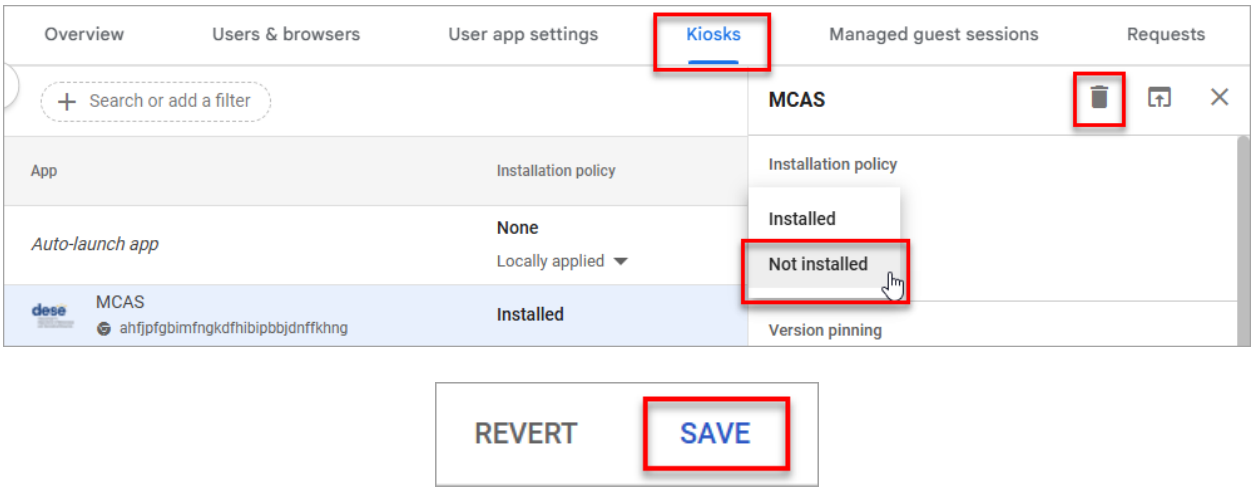
1. Sign in to the **Google Admin Console**.

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.

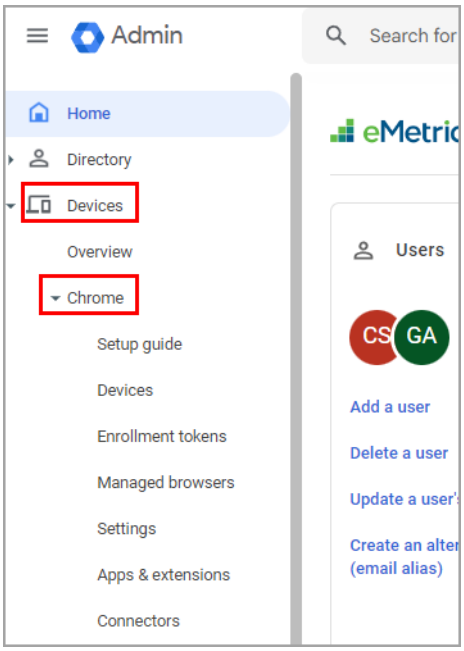


6. Once the MCAS Chrome App has been removed, follow the steps below for installing the MCAS web app and extension.

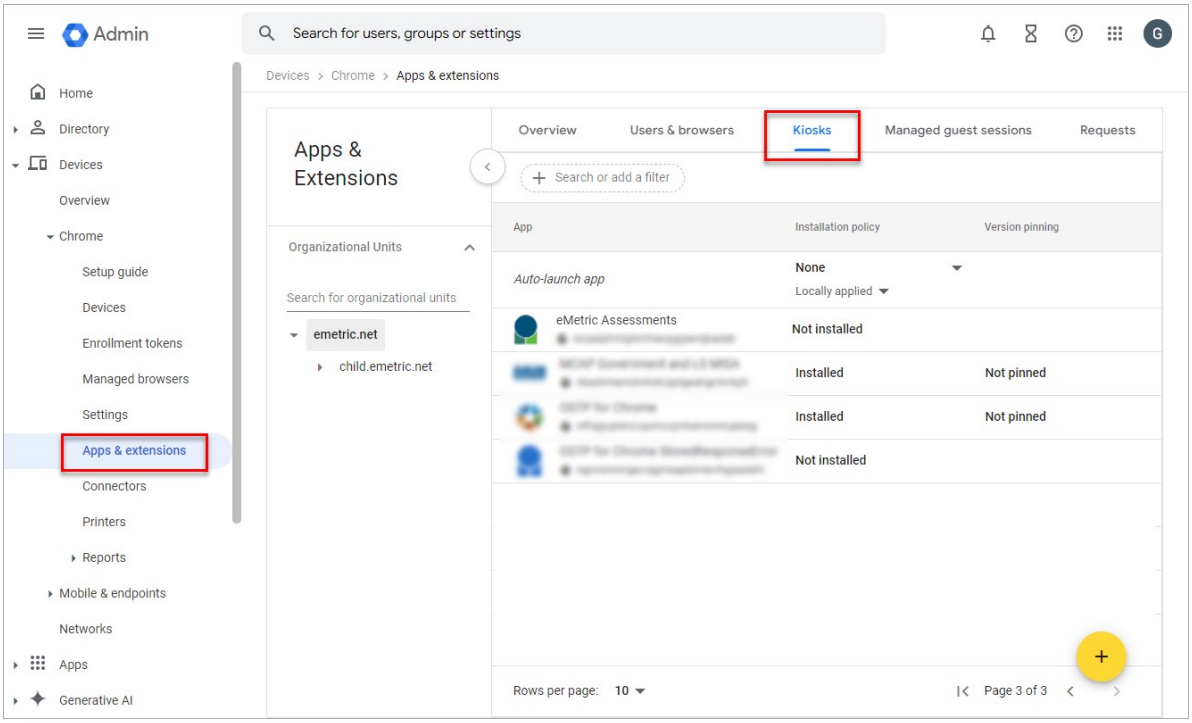
Note: If you do not have a dedicated TC, a DTC or STC can complete all the technology coordinator tasks. Ensure you have the correct administrative rights to make changes to student testing devices.

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**.

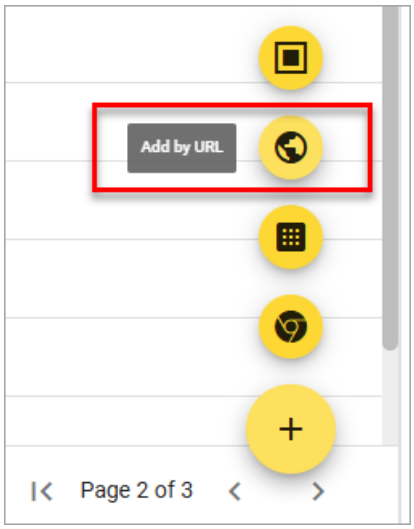


3. Select **Apps & Extensions** and then **Kiosks** and select the **organizational unit (OU)** for which you want to install the MCAS Web App and Extension for ChromeOS.

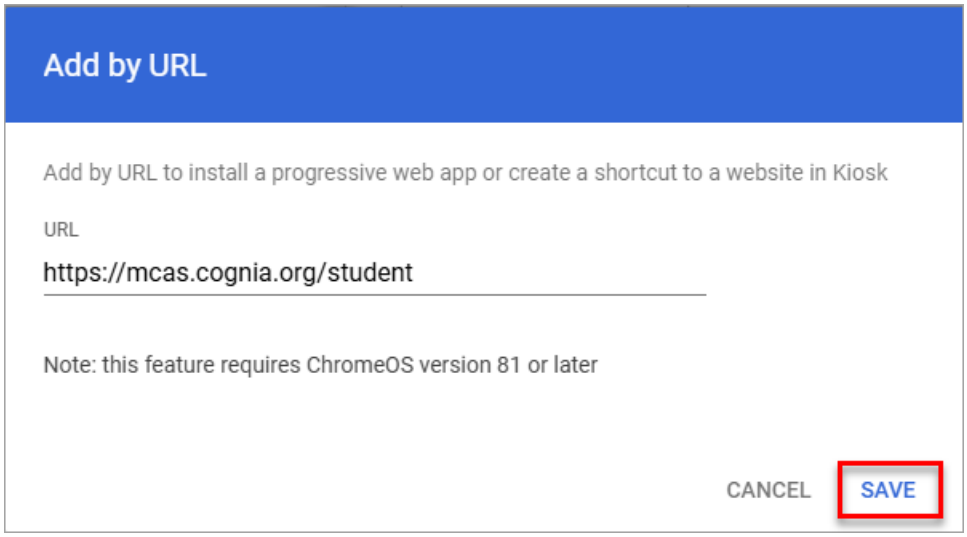


Note: Ensure that child organizational units inherit the app and policy settings from the parent OU. If inheritance is disabled, the kiosk app will not appear on devices in those child OUs and the policy settings and app must be installed locally in the desired child OU.

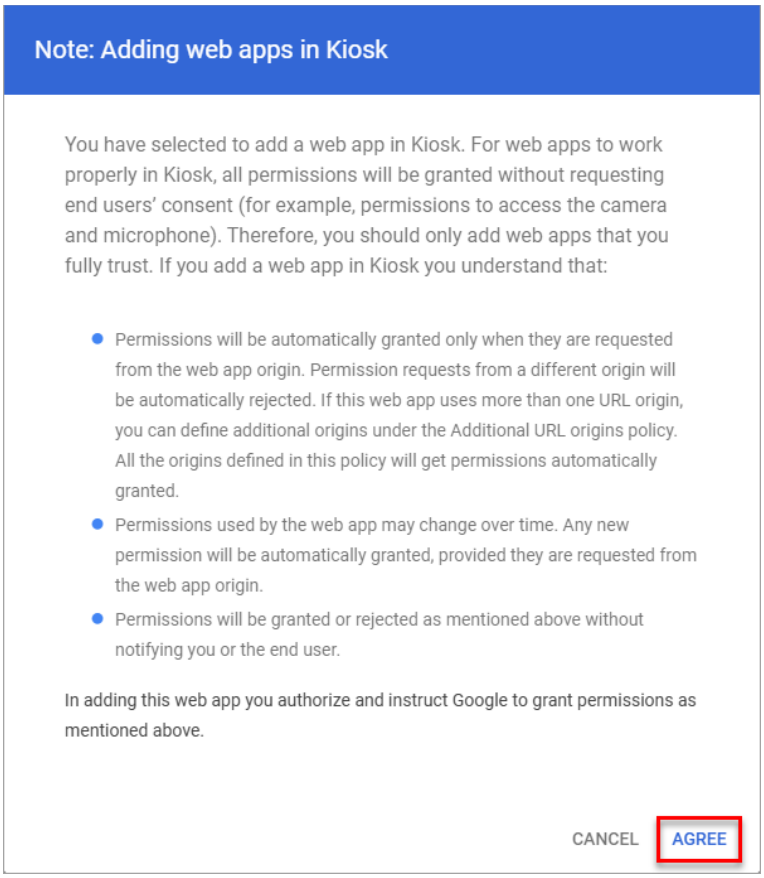
4. Expand the **yellow + button** in the bottom-right corner and select **Add by URL**.



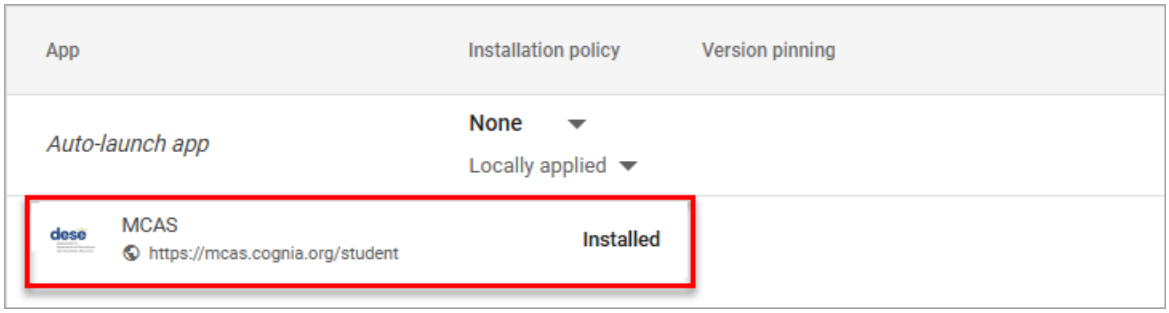
5. Enter https://mcas.cognia.org/student and select **Save.**



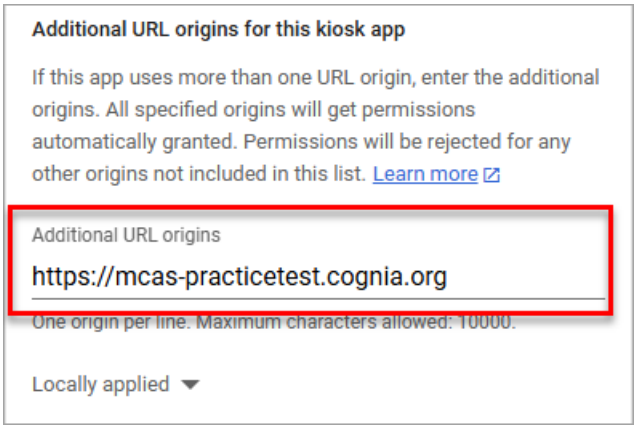
6. Google will then prompt you to allow permissions to this app. Select **Agree**.



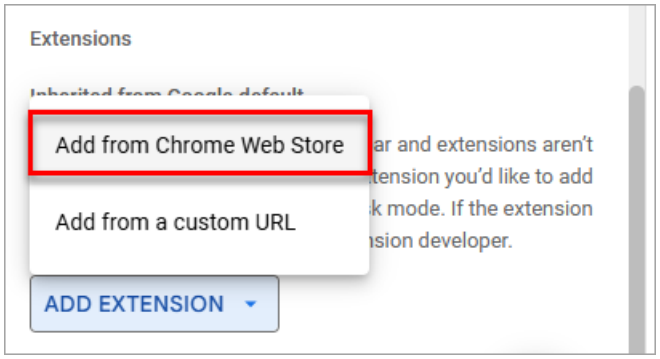
7. The new MCAS web app for ChromeOS appears in the app list.



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.

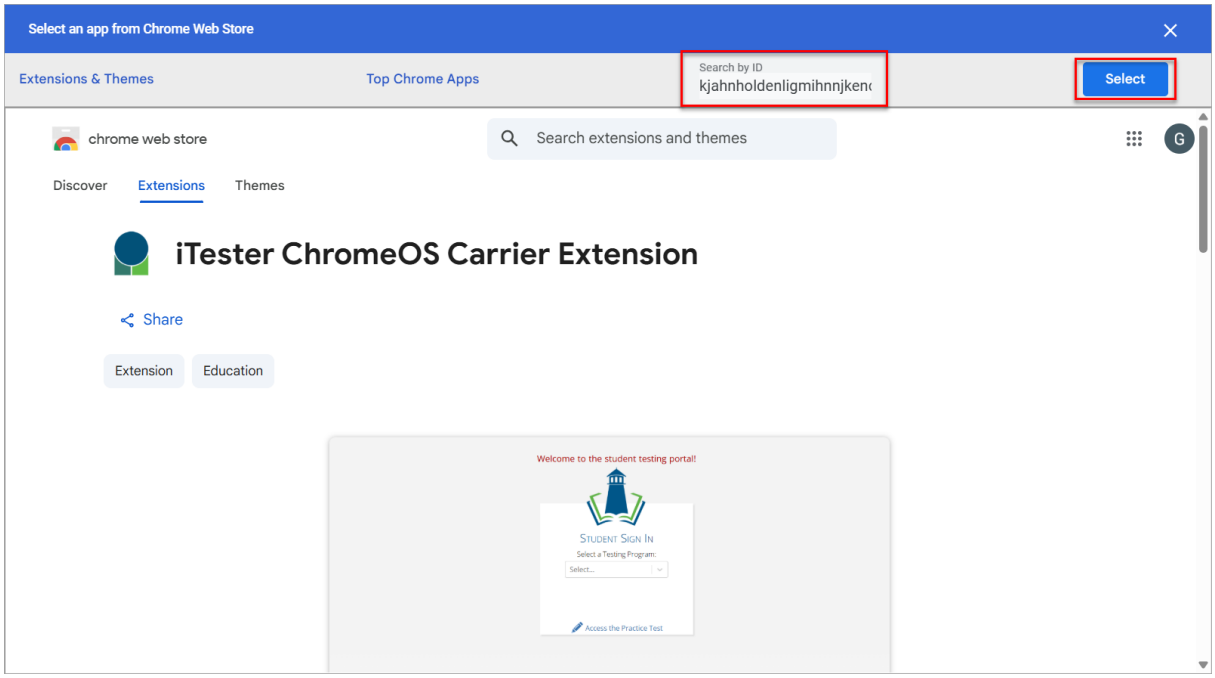


9. Scroll down further on the right-side bar to the **Extension** section. Click **ADD EXTENSION** and from the pop-up list select **Add from Chrome Web Store**.

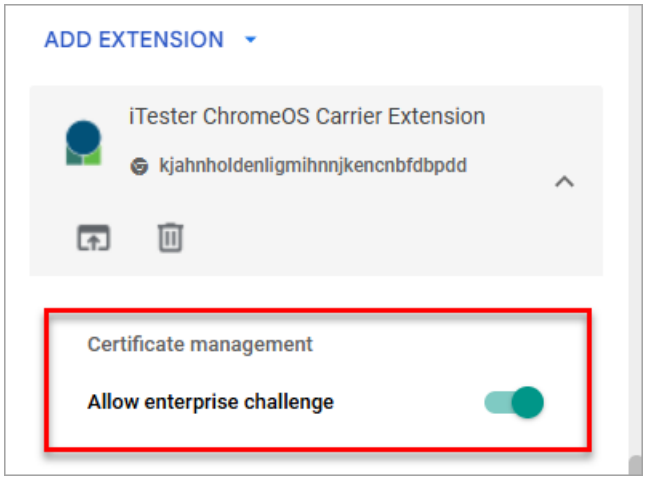


10. In the Chrome Web Store, ensure the iTester ChromeOS Carrier extension ID is entered exactly as it is shown below, with no additional spaces, in the **Search by ID** text box and then select the **Select** button to add the extension.

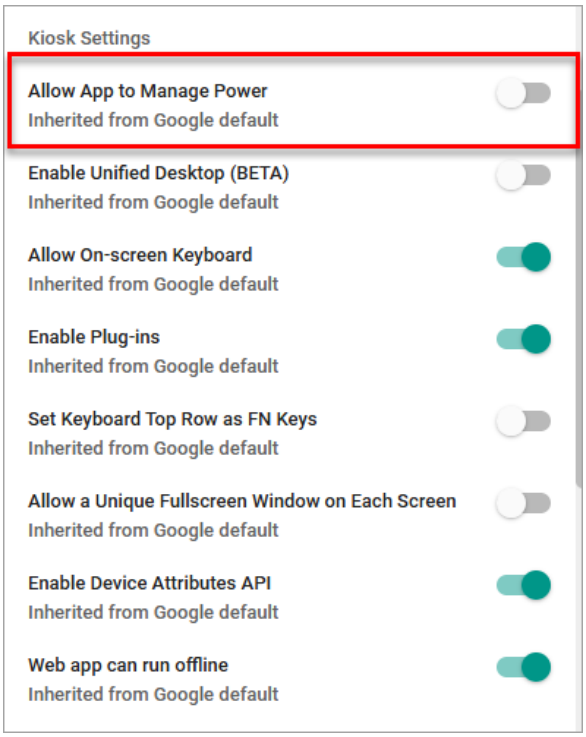
    - **`kjahnholdenligmihnnjkencnbfdbpdd`**



11. Once the extension has been added 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.

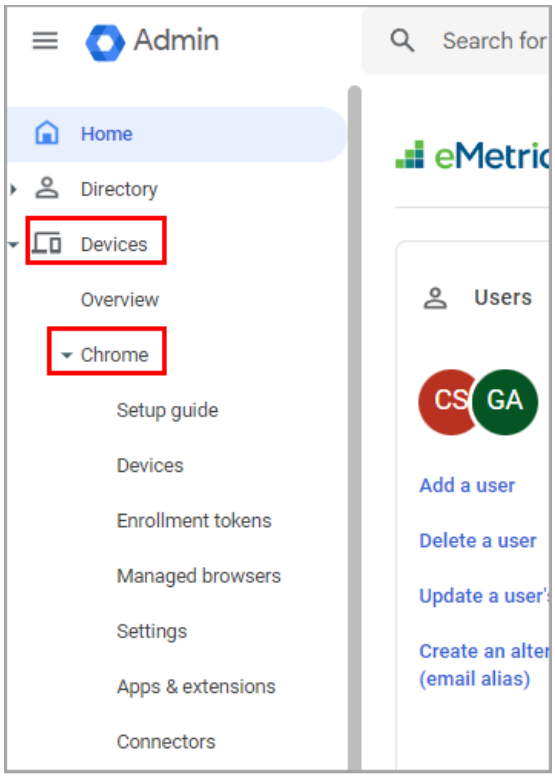


Important Note: Verify in Kiosk Settings that “Allow App to manage power” is **disabled**. To do this, click on **Devices, Apps & Extensions** and then select **Kiosks**. Click on the **MCAS** app name and check to make sure the setting **Allow app to manage power** is **disabled** (slider is moved to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

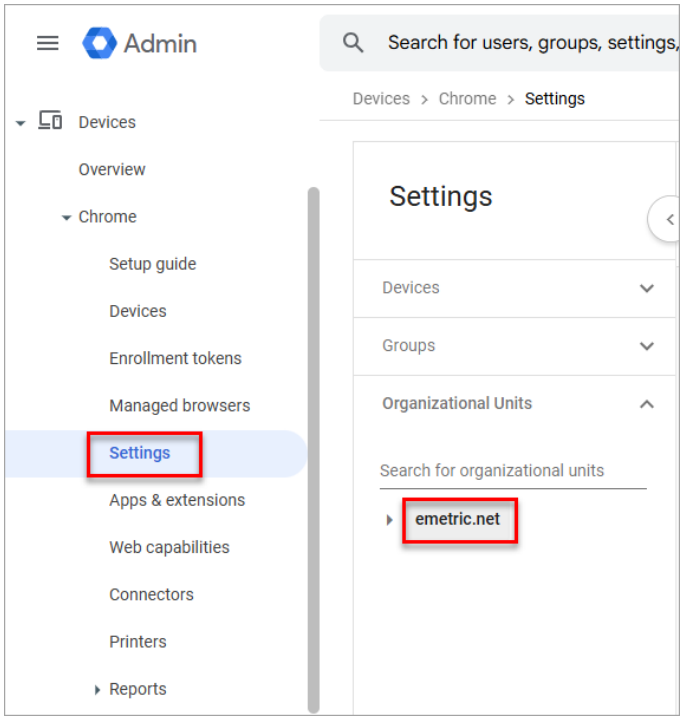


Step 4: Configure Device Settings

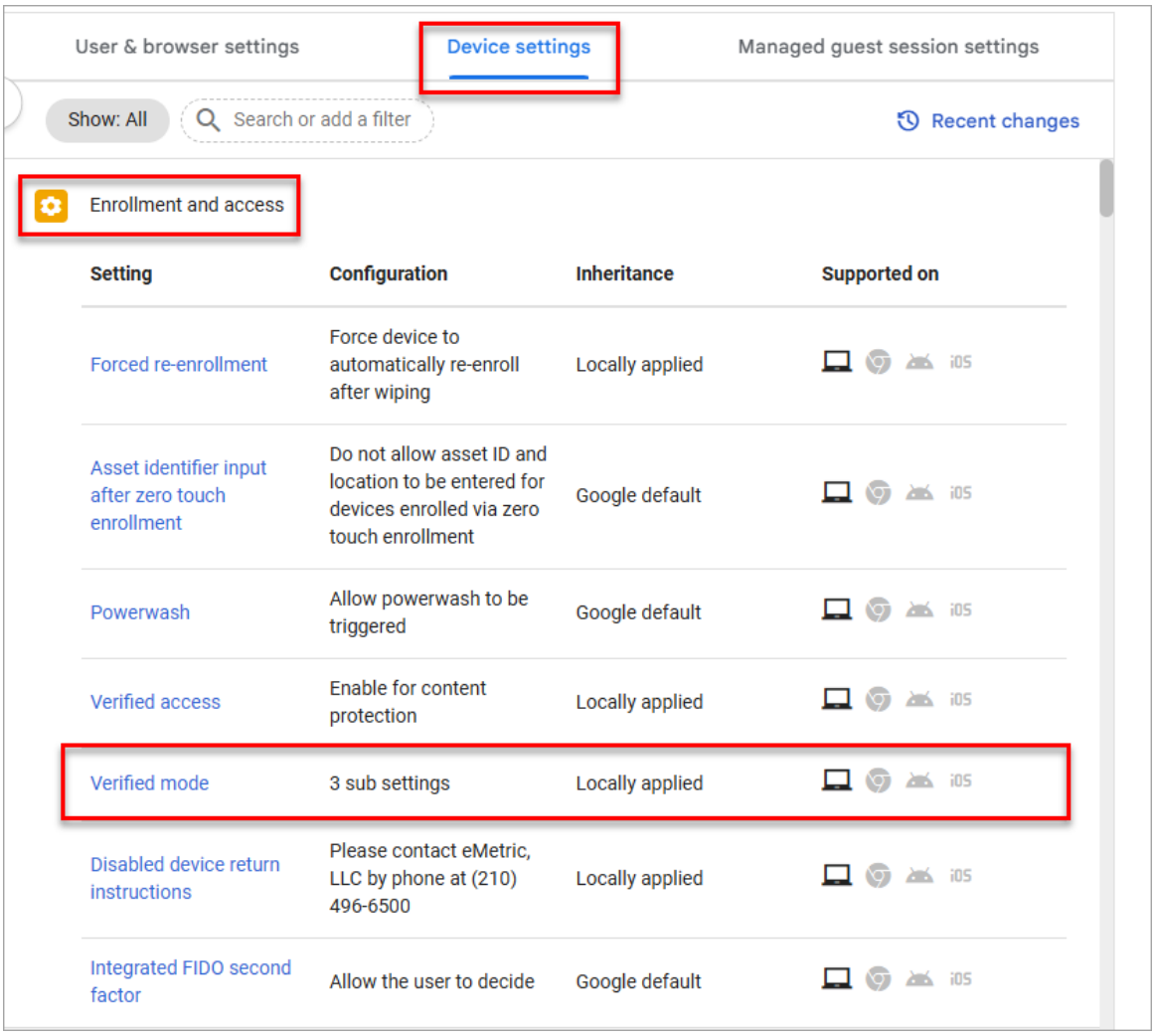
1. In your Google Admin console, navigate to **Devices,** then select **Chrome**.



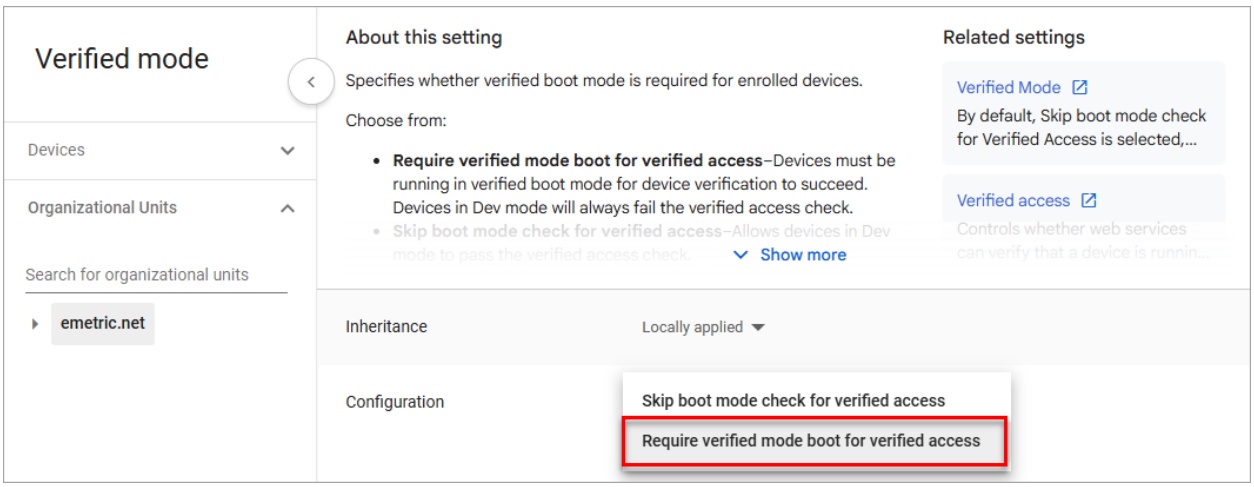
2. Click on **Settings** and then choose the relevant **Organizational Unit** where the MCAS web app is installed. In the example below the top Organizational Unit is emetric.net.



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.



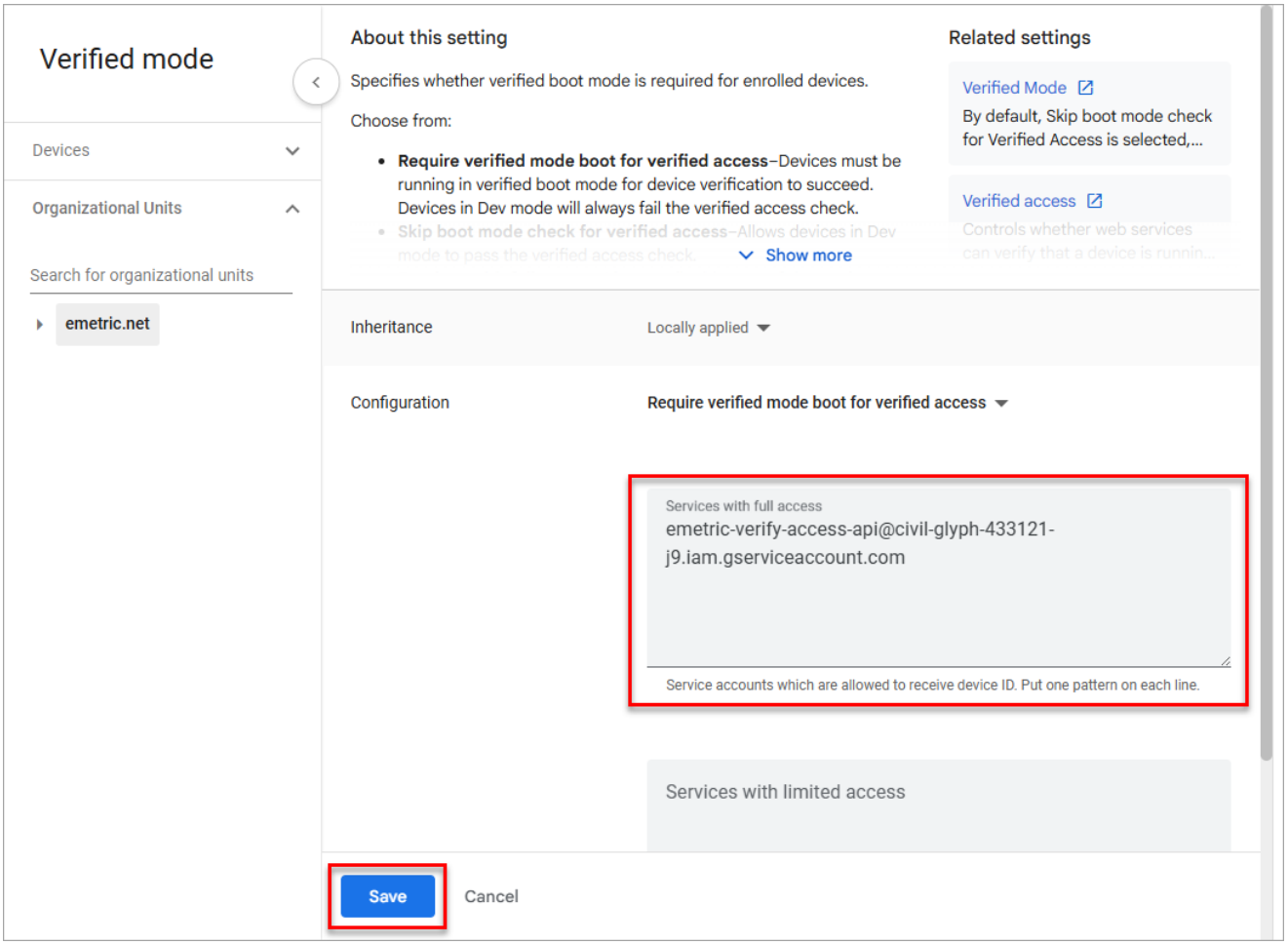
4. Set configuration to: **Required verified mode boot for verified access**.



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.
    - 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.

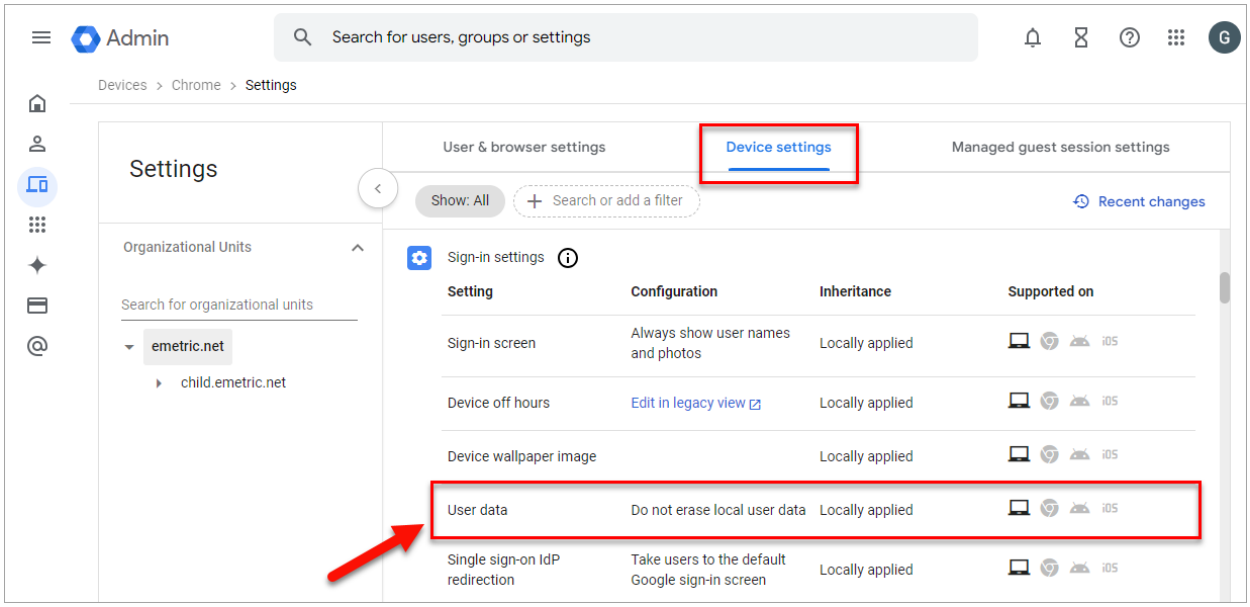
      `emetric-verify-access-api@civil-glyph-433121-j9.iam.gserviceaccount.com`

    - Then select **Save**.

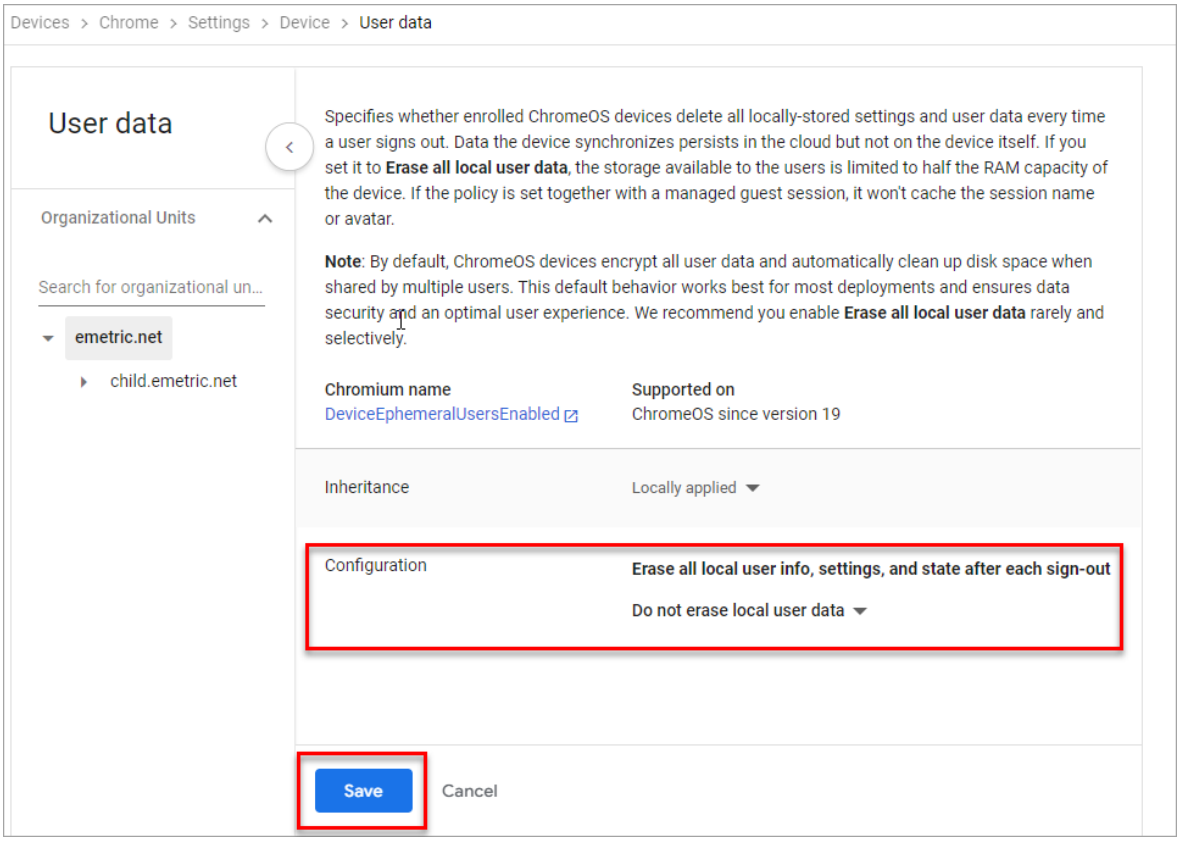


Note: Pay close attention when entering the service account, as any typos or added characters will prevent the app from entering kiosk mode.

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

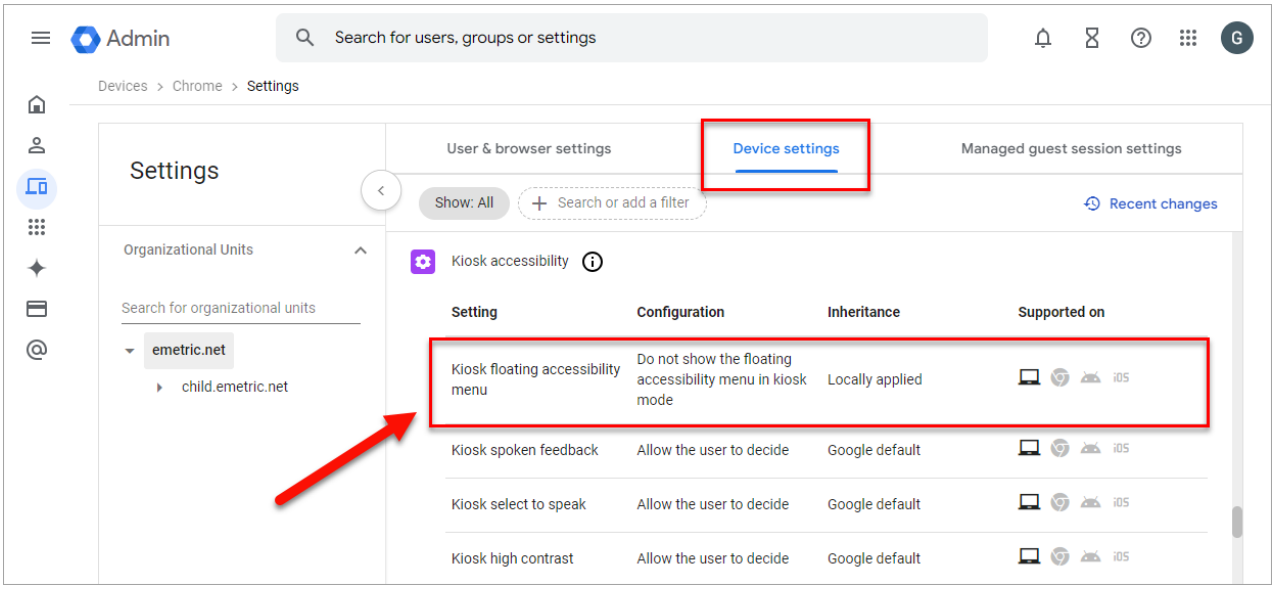


7. Verify that **Do not erase all local data** is set; if not, click on **User Data** to update the setting with the drop-down menu and click **Save**.

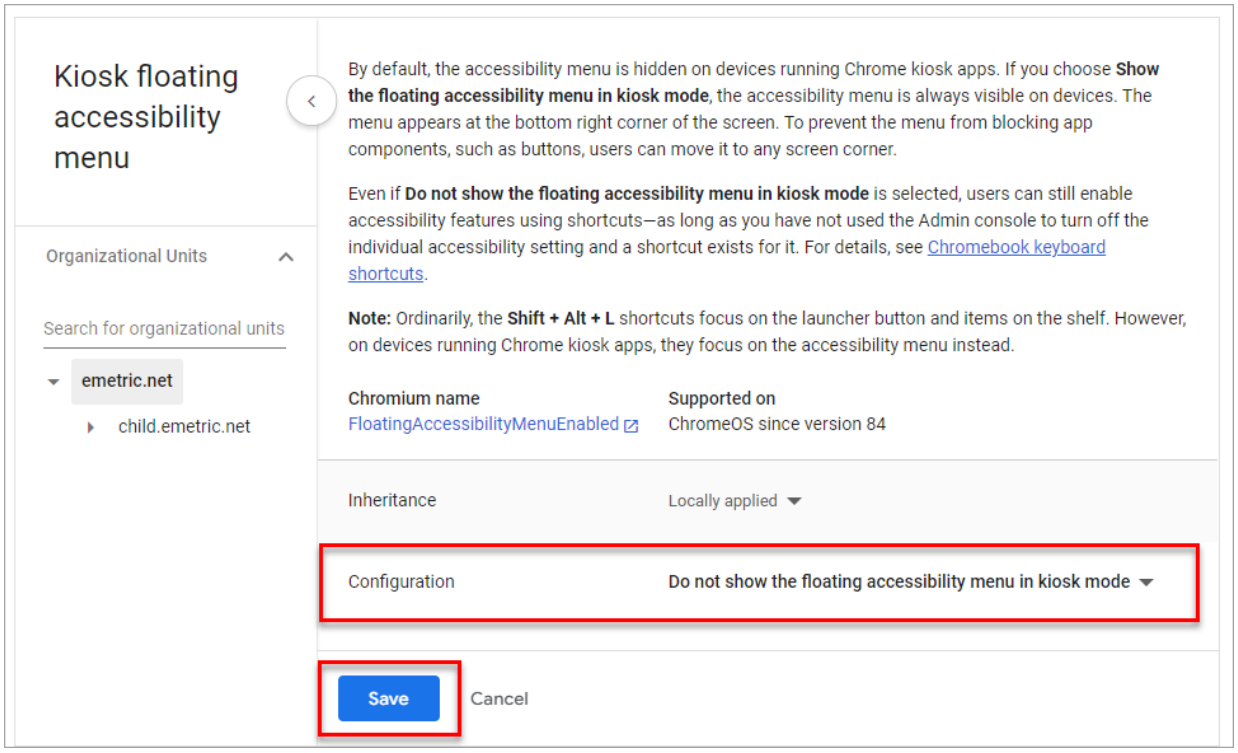


⚠ **Note:** This setting is crucial to allow Chrome local storage to be used to store student responses if network connectivity is lost. If this is not configured, student responses will not be saved to the device in the case of internet disruptions.

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



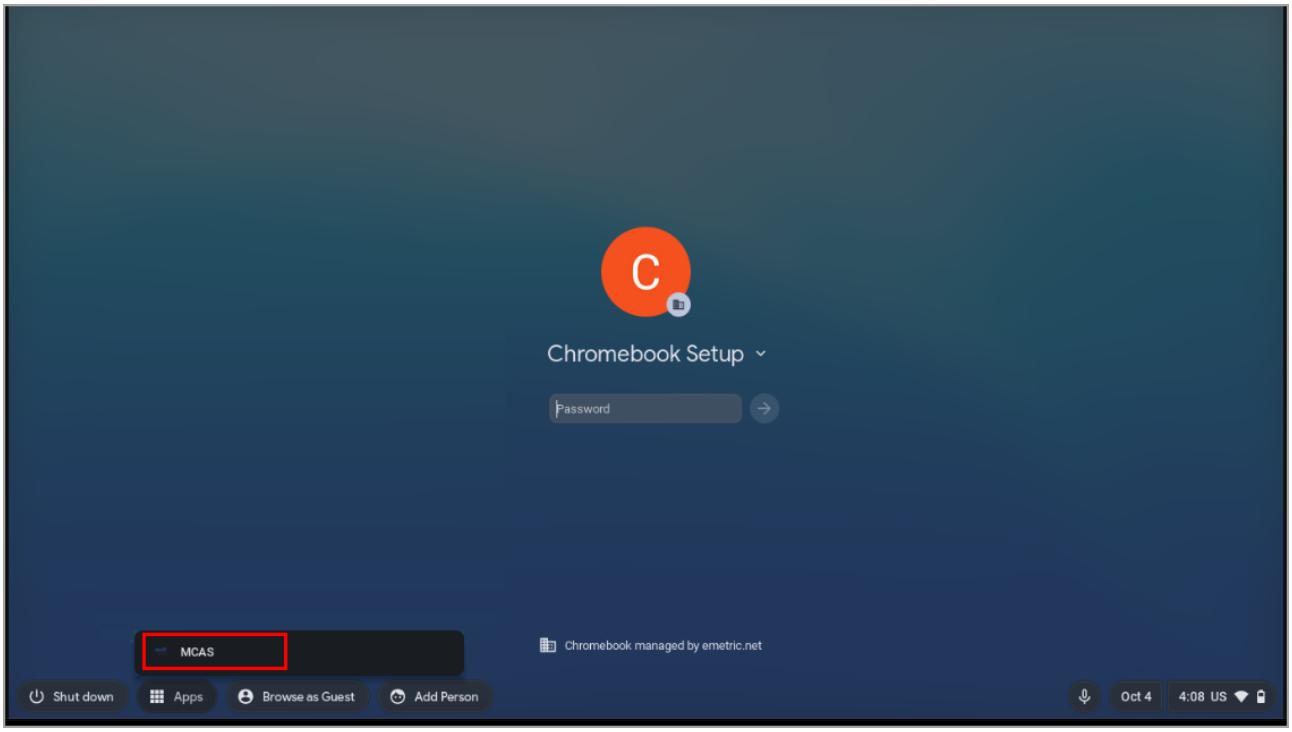
9. Verify that **Do not show the floating accessibility menu in kiosk mode** is set; if not, click on **Kiosk Floating Accessibility Menu** to update the setting with the drop-down menu and click **Save**.



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 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.