IV. MCAS Student Kiosk Installation

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

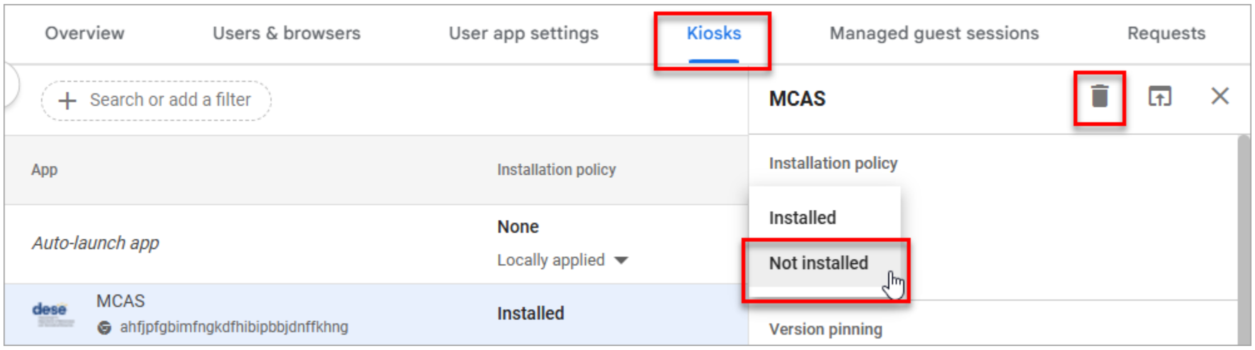
- **New App Required**: The new PWA must be installed on all ChromeOS devices used for testing.
- **Easy Setup**: Step-by-step instructions for setup and configuration are included in this guide below.
- **Extension Pairing**: The PWA will work alongside a Chrome extension to support secure kiosk testing.
- **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.

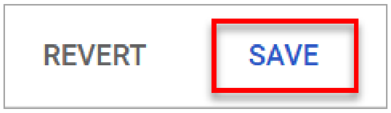
Step 1: Set up your school technology.
Review section II: Technology Guidelines and section III: Technology Setup in detail.

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.





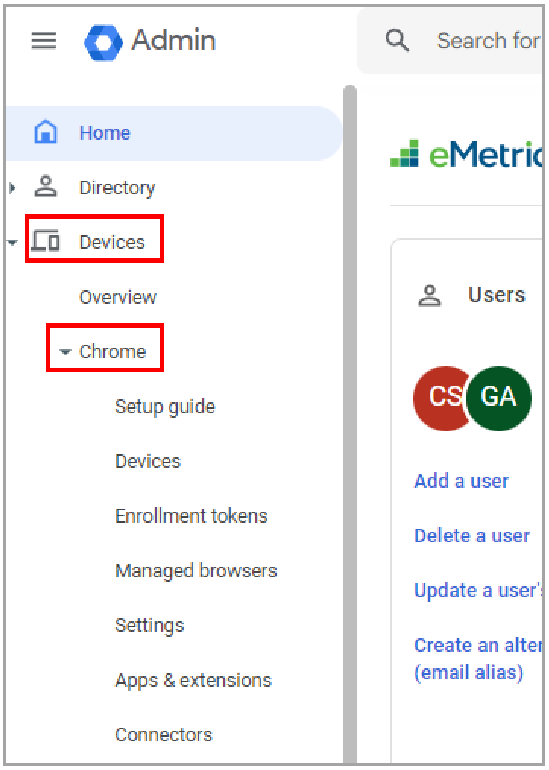
6. Once the MCAS Chrome App has been removed, follow the steps below for installing the MCAS web app and extension.

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.

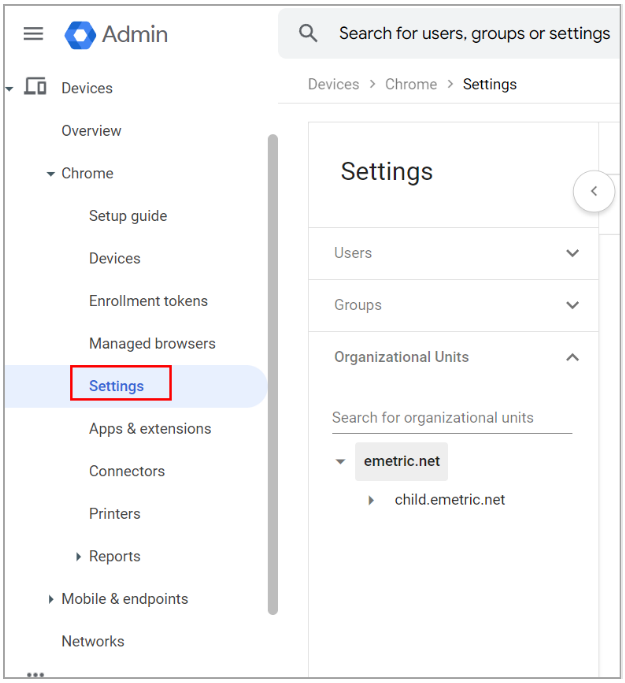
Step 3: Install the MCAS web app for ChromeOS

To install the MCAS web app:

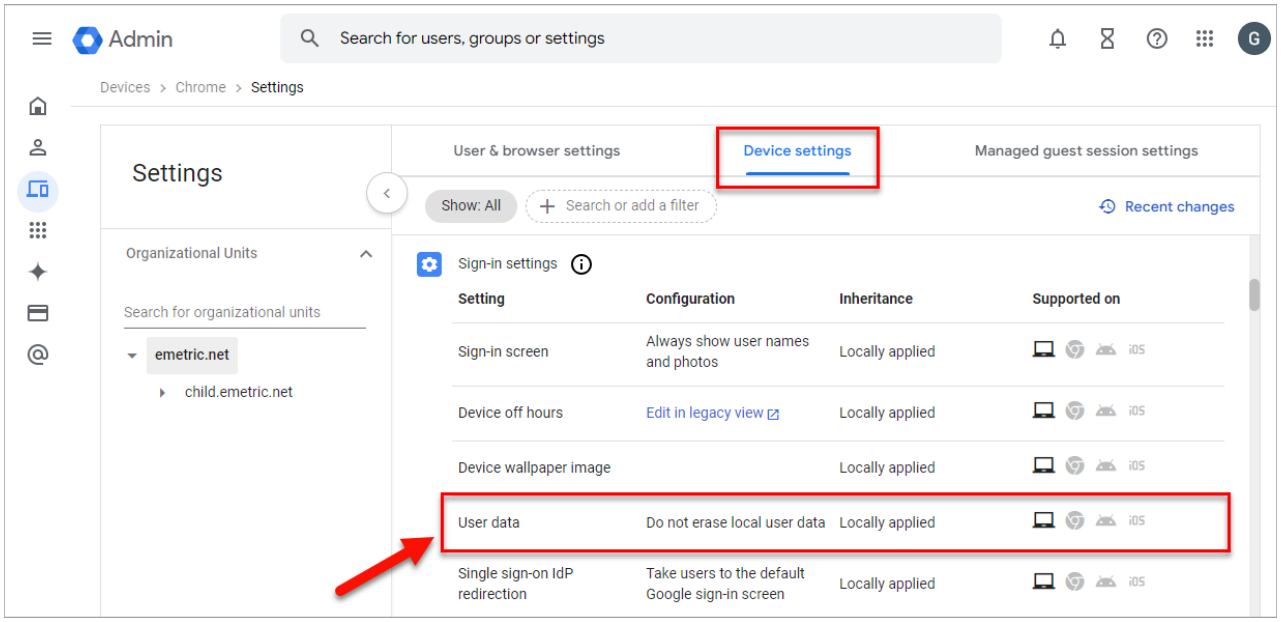
1. As the Chromebook administrator, log in to your ChromeOS management console (https://admin.google.com).
2. Expand the **Devices** menu, and then select **Chrome**.



3. Click on **Settings**.

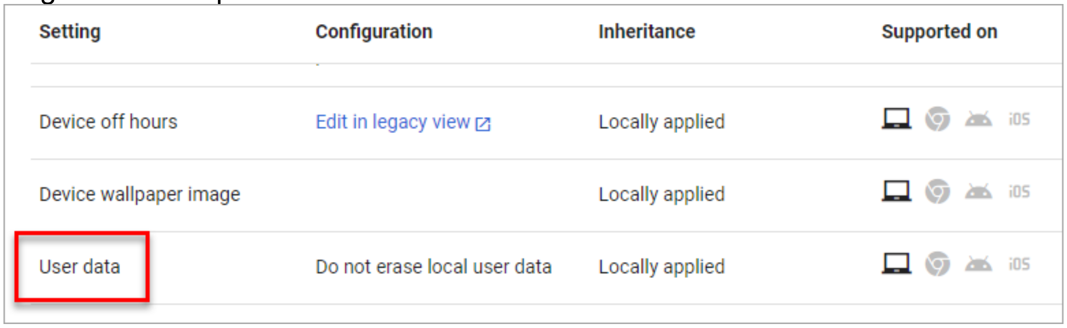


4. Click on the **Device Settings** tab and scroll to **User Data** in the **Sign-In Settings** section.

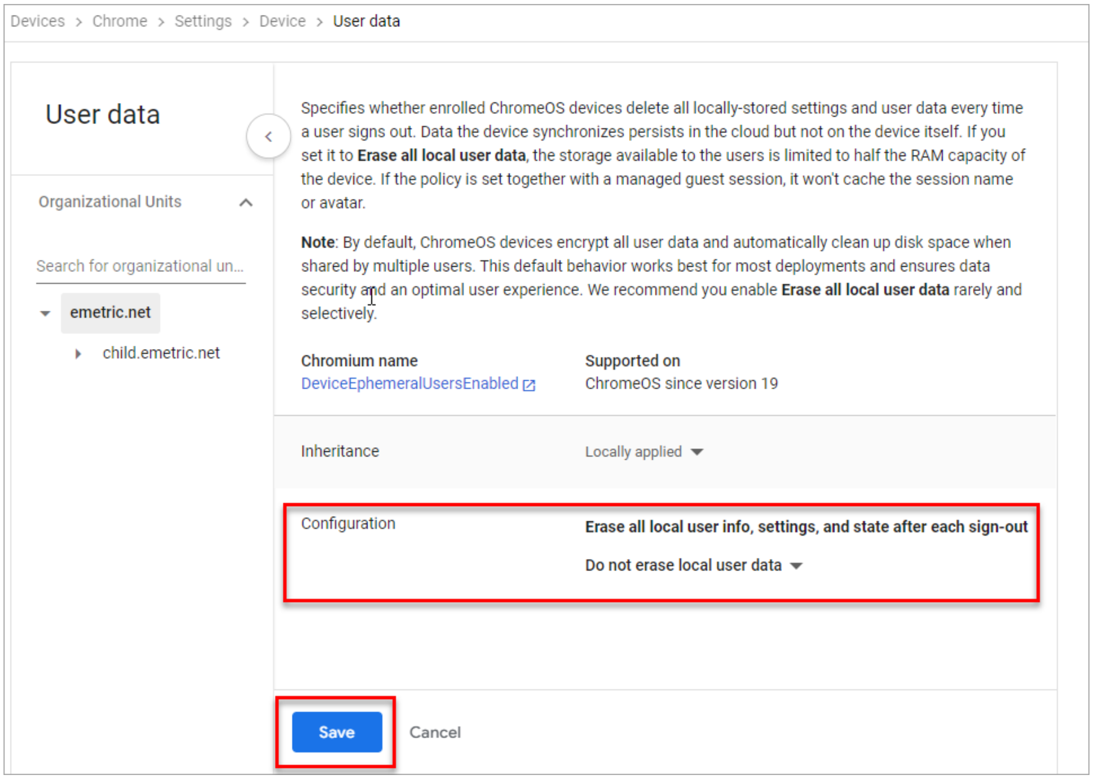


Setting	Configuration	Inheritance	Supported on
Sign-in screen	Always show user names and photos	Locally applied	iOS
Device off hours	Edit in legacy view	Locally applied	iOS
Device wallpaper image		Locally applied	iOS
User data	Do not erase local user data	Locally applied	iOS
Single sign-on IdP redirection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

5. 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**.



Setting	Configuration	Inheritance	Supported on
Device off hours	Edit in legacy view	Locally applied	iOS
Device wallpaper image		Locally applied	iOS
User data	Do not erase local user data	Locally applied	iOS



Devices > Chrome > Settings > Device > User data

User data

Organizational Units

Search for organizational un...

emetric.net

child.emetric.net

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

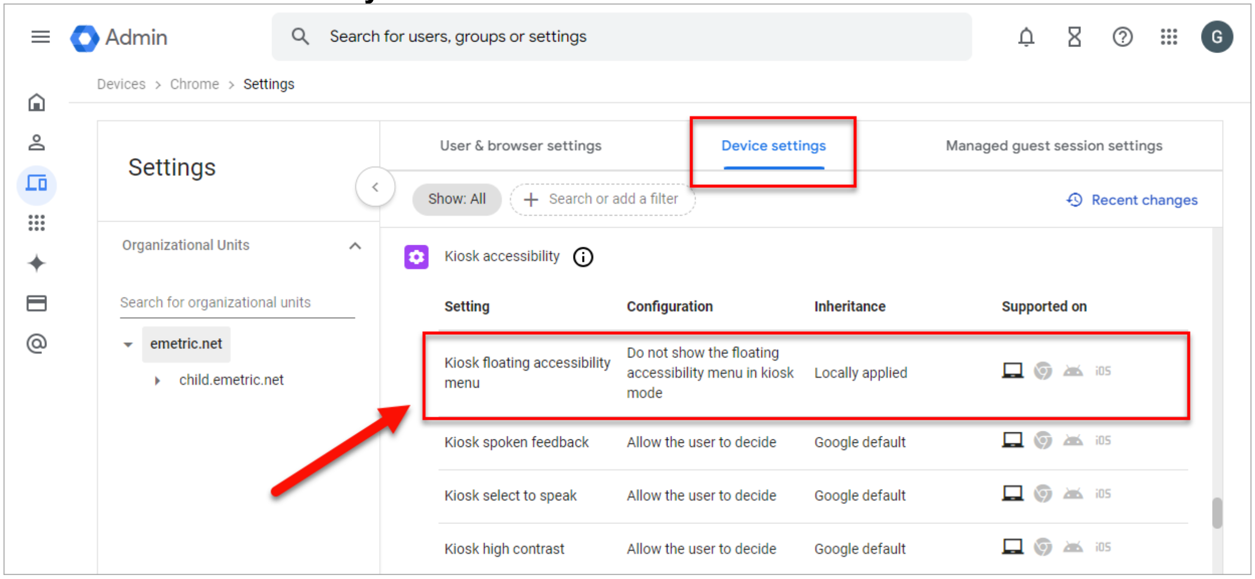
Inheritance: Locally applied

Configuration: Erase all local user info, settings, and state after each sign-out

Do not erase local user data

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.

6. While still in the Device Settings tab, scroll to the **Kiosk Floating Accessibility Menu** in the **Kiosk Accessibility** section.



Devices > Chrome > Settings

Settings

Organizational Units

Search for organizational units

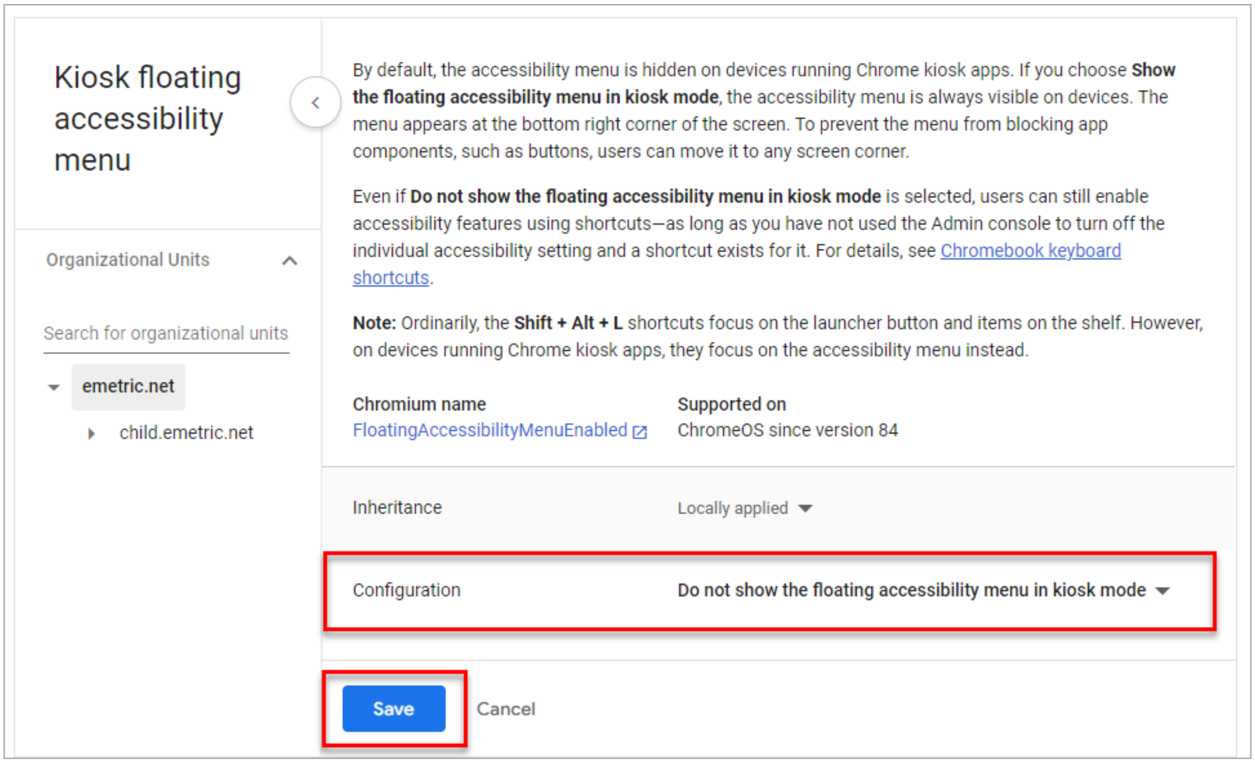
emetric.net

child.emetric.net

Kiosk accessibility

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

7. 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.

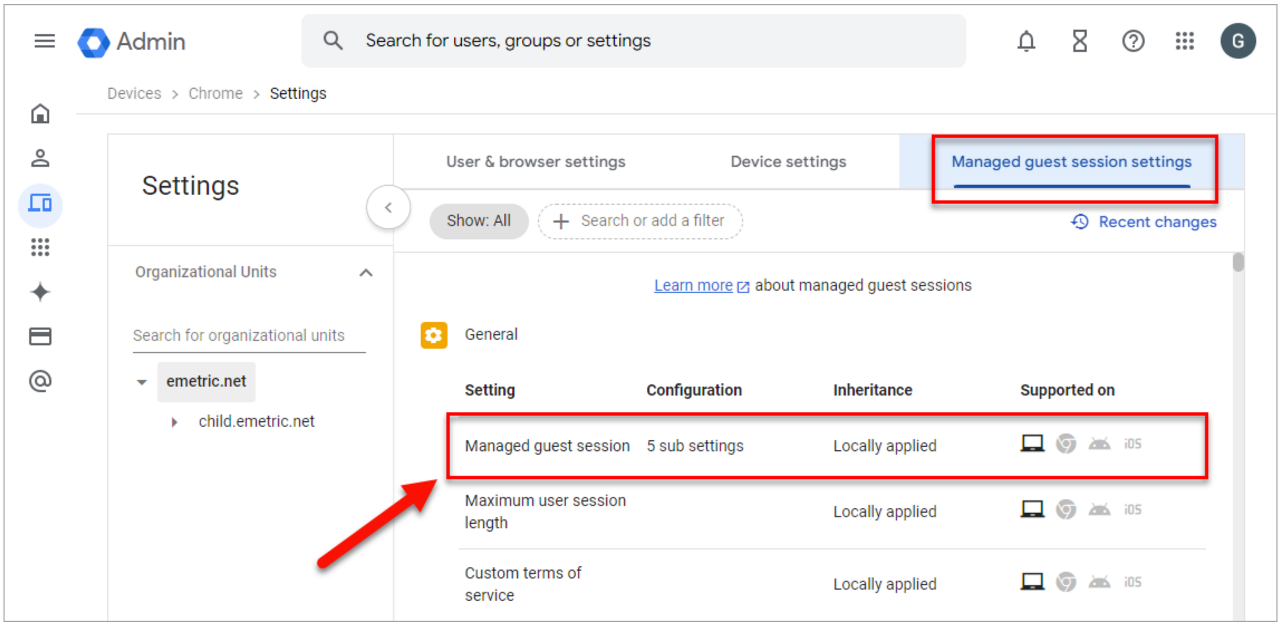
Chromium name	Supported on
FloatingAccessibilityMenuEnabled	ChromeOS since version 84

Inheritance: Locally applied

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

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.

8. On the Settings page, select the **Managed guest session settings** tab and then select **Managed guest session**.

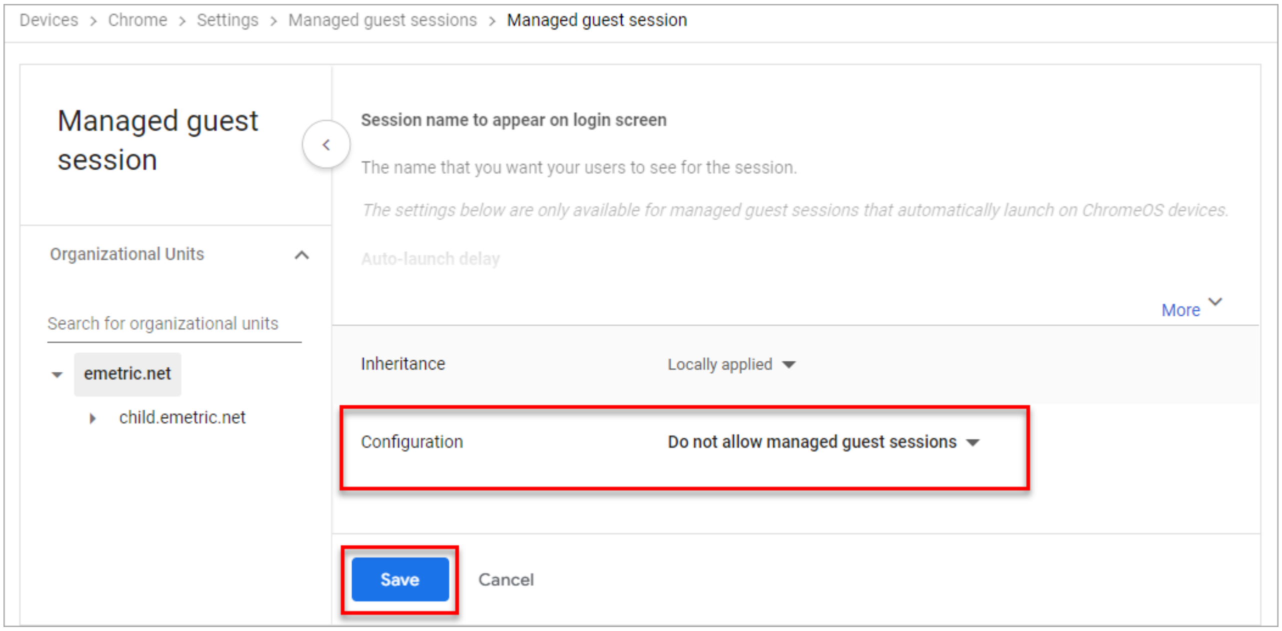


Learn more about managed guest sessions

General

Setting	Configuration	Inheritance	Supported on
Managed guest session	5 sub settings	Locally applied	iOS
Maximum user session length		Locally applied	iOS
Custom terms of service		Locally applied	iOS

9. Ensure that Managed guest session is set to **Do not allow managed guest sessions** and click **Save**.


Devices > Chrome > Settings > Managed guest sessions > Managed guest session
Managed guest session
Organizational Units
Search for organizational units
emetric.net
child.emetric.net
More
Save
Cancel

Session name to appear on login screen

The name that you want your users to see for the session.

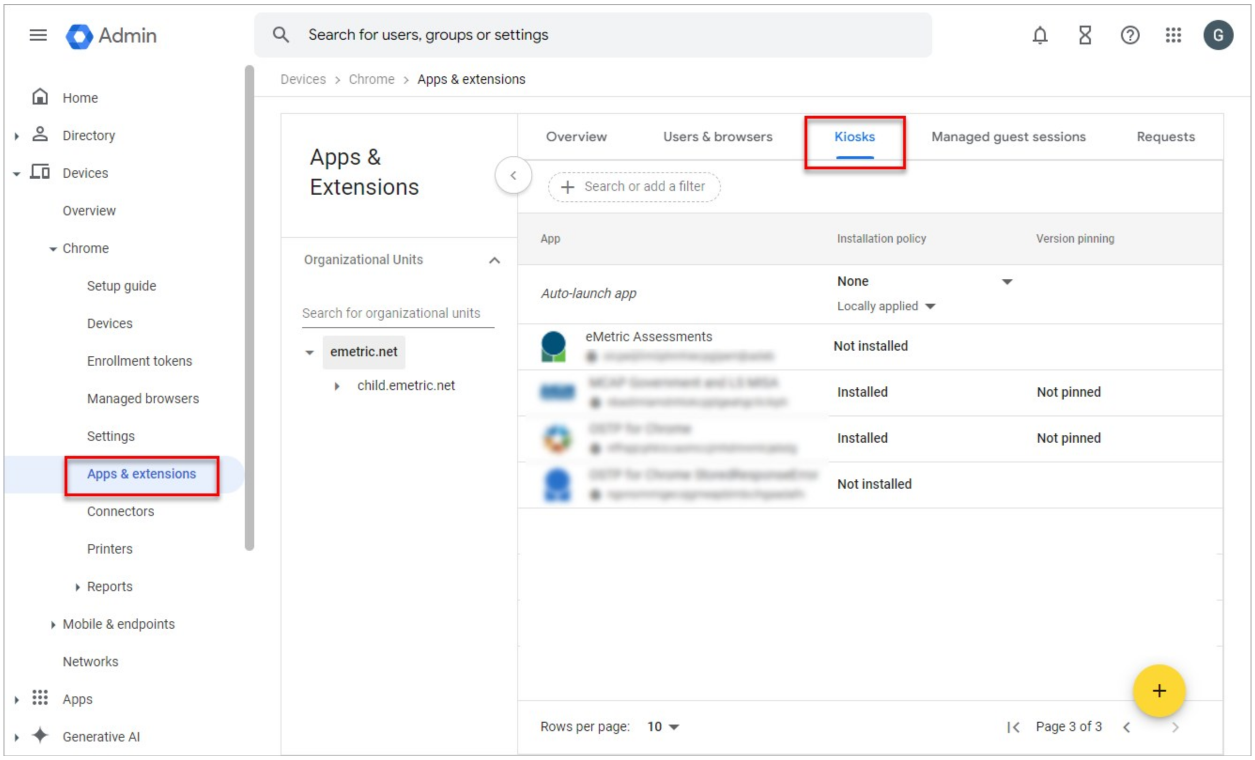
The settings below are only available for managed guest sessions that automatically launch on ChromeOS devices.

Auto-launch delay

Inheritance: Locally applied

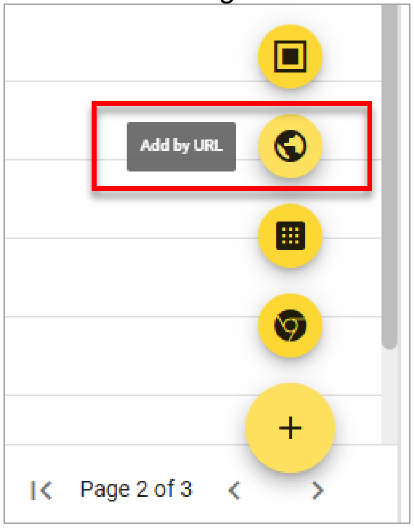
Configuration: Do not allow managed guest sessions

10. Navigate back to the **Chrome** menu on the left side of the screen and select **Apps & Extensions** and then **Kiosks**.

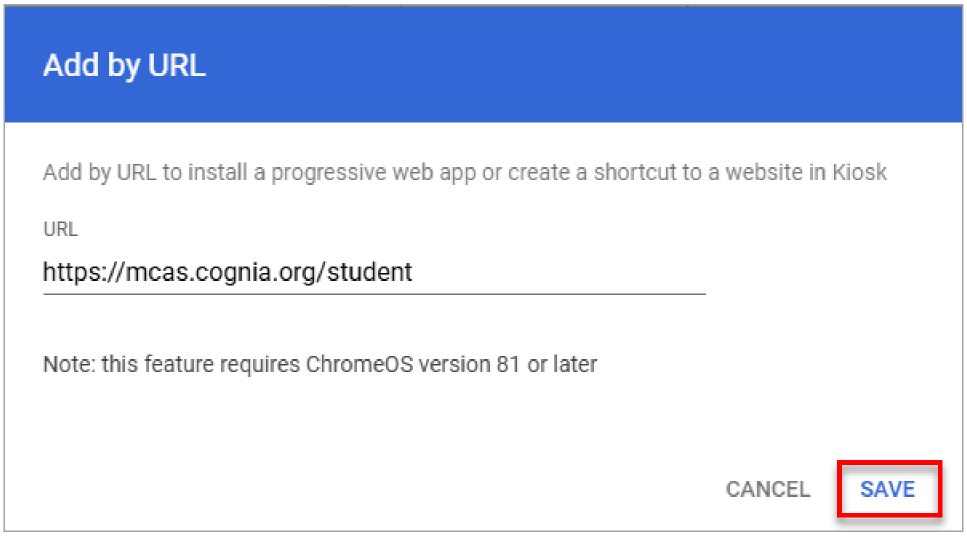


App	Installation policy	Version pinning
Auto-launch app	None Locally applied	
eMetric Assessments [redacted]	Not installed	
[redacted]	Installed	Not pinned
[redacted]	Installed	Not pinned
[redacted]	Not installed	

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



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



Add by URL

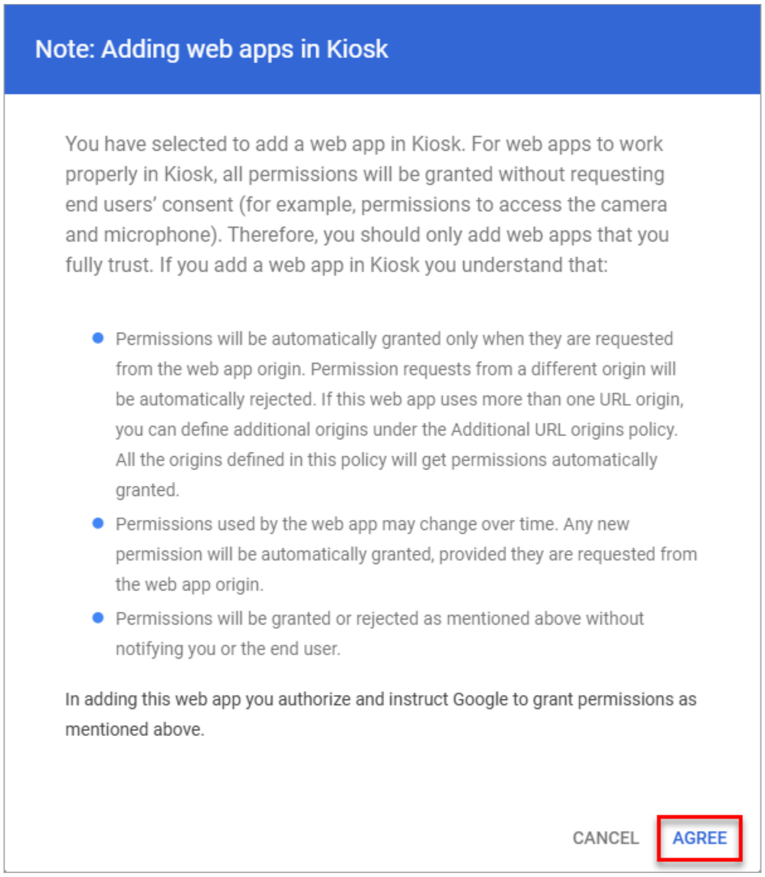
Add by URL to install a progressive web app or create a shortcut to a website in Kiosk

URL

https://mcas.cognia.org/student

Note: this feature requires ChromeOS version 81 or later

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



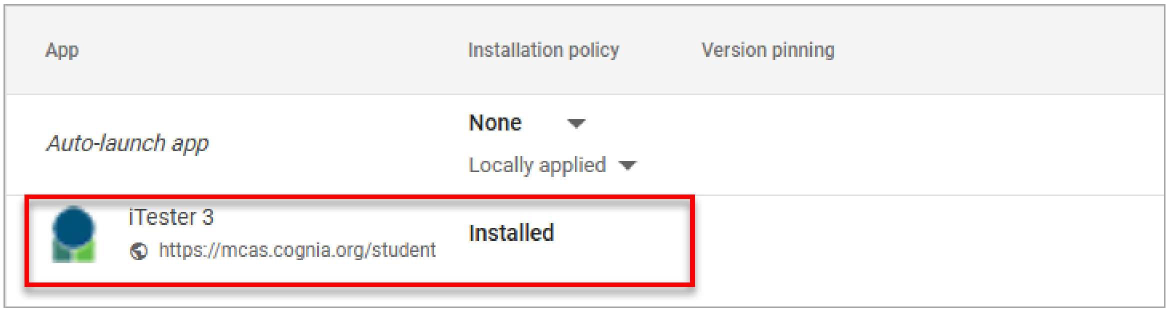
Note: Adding web apps in Kiosk

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.

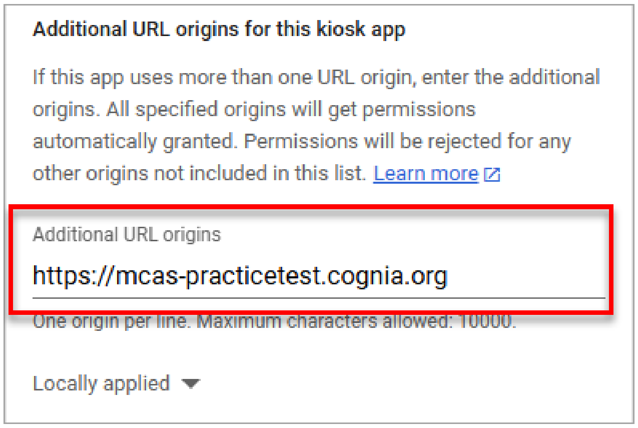
In adding this web app you authorize and instruct Google to grant permissions as mentioned above.

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



App	Installation policy	Version pinning
Auto-launch app	None Locally applied	
iTester 3 https://mcas.cognia.org/student	Installed	

15. Select the MCAS app and scroll down the right-side bar to **Additional URL origins** field to add the following URL, 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

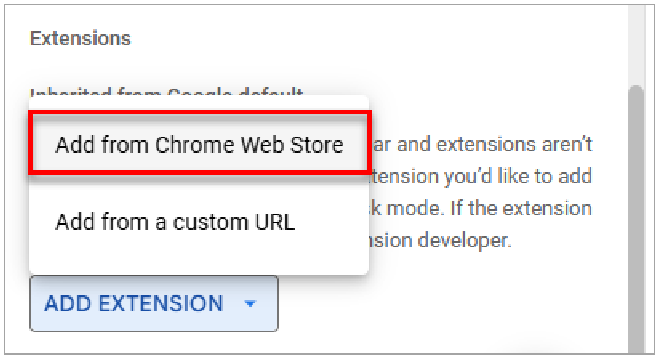
Additional URL origins

https://mcas-practicetest.cognia.org

One origin per line. Maximum characters allowed: 10000.

Locally applied

16. 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**.

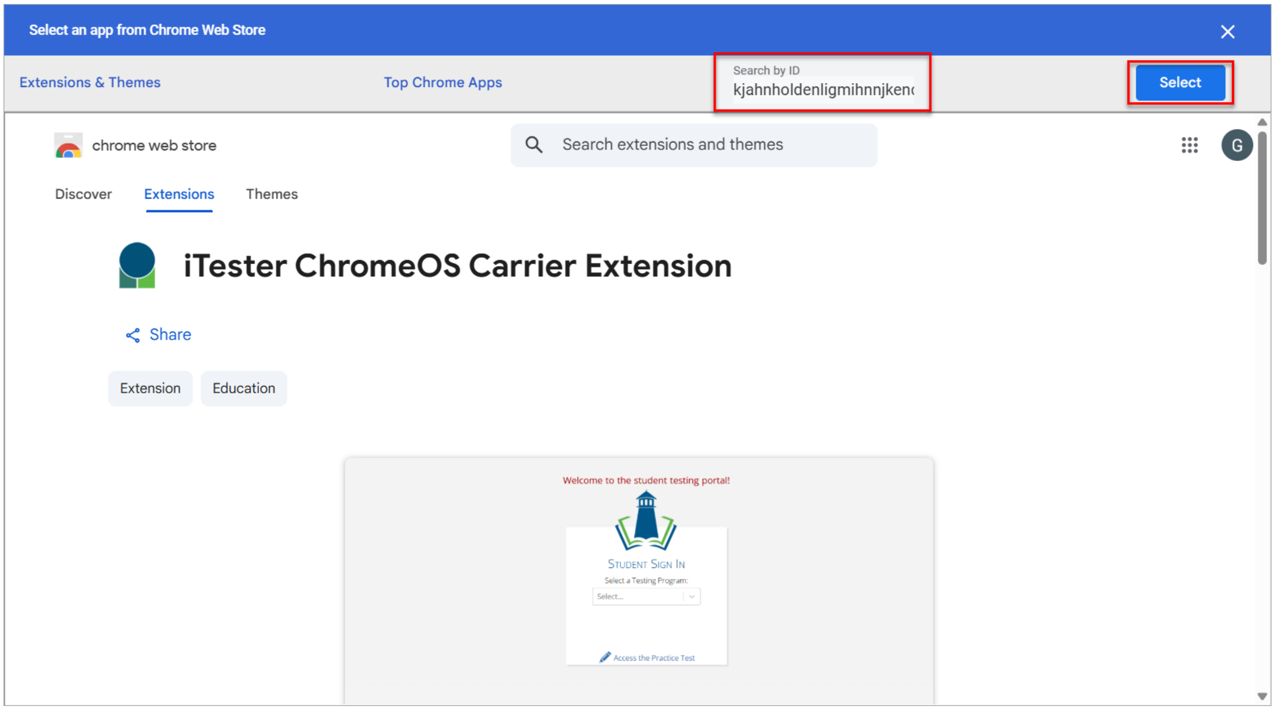


Extensions

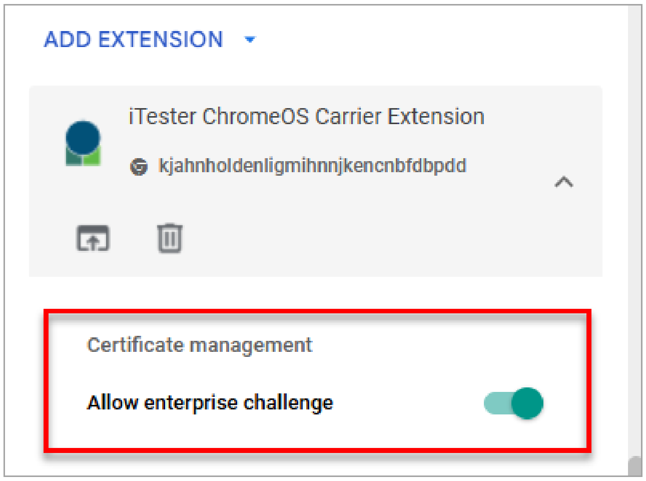
Inherited from Google default

ar and extensions aren't
tension you'd like to add
k mode. If the extension
nsion developer.

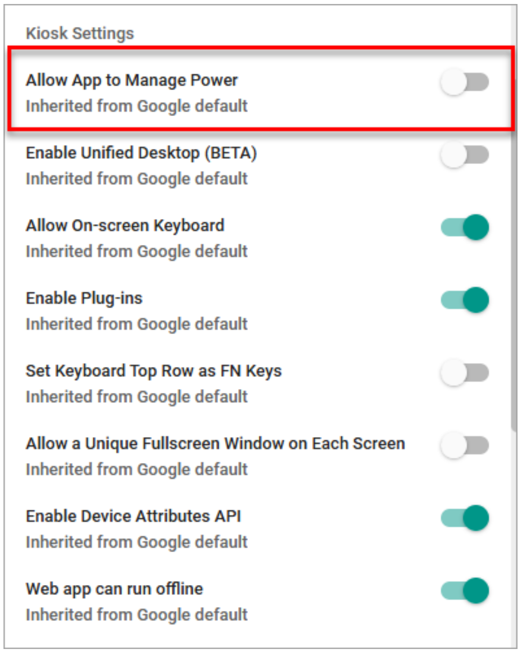
17. In the Chrome Web Store enter the iTester ChromeOS Carrier extension ID **kjahnholdenligmihnnjkencnbfdbpdd** in the **Search by ID** text box and then select the **Select** button to add the extension.



18. 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.


ADD EXTENSION
iTester ChromeOS Carrier Extension
kjahnholdenligmihnnjkencnbfdbpdd
Certificate management
Allow enterprise challenge

⚠ **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).



Kiosk Settings

Allow App to Manage Power
Inherited from Google default

Enable Unified Desktop (BETA)
Inherited from Google default

Allow On-screen Keyboard
Inherited from Google default

Enable Plug-ins
Inherited from Google default

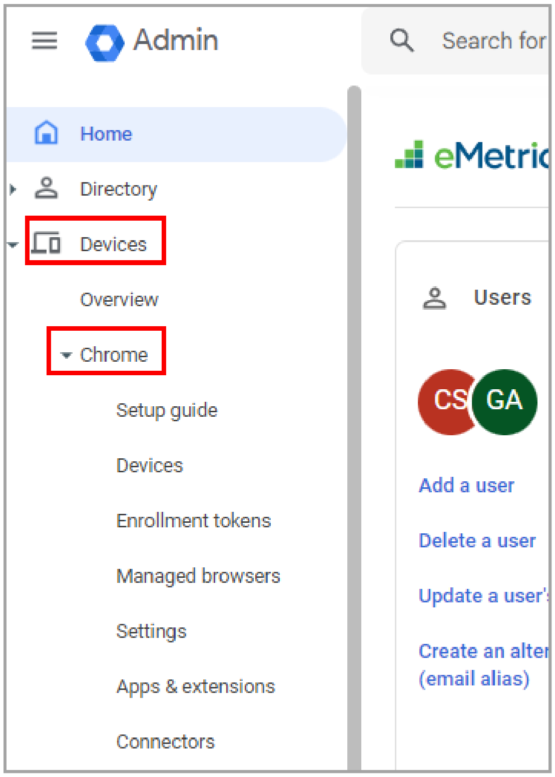
Set Keyboard Top Row as FN Keys
Inherited from Google default

Allow a Unique Fullscreen Window on Each Screen
Inherited from Google default

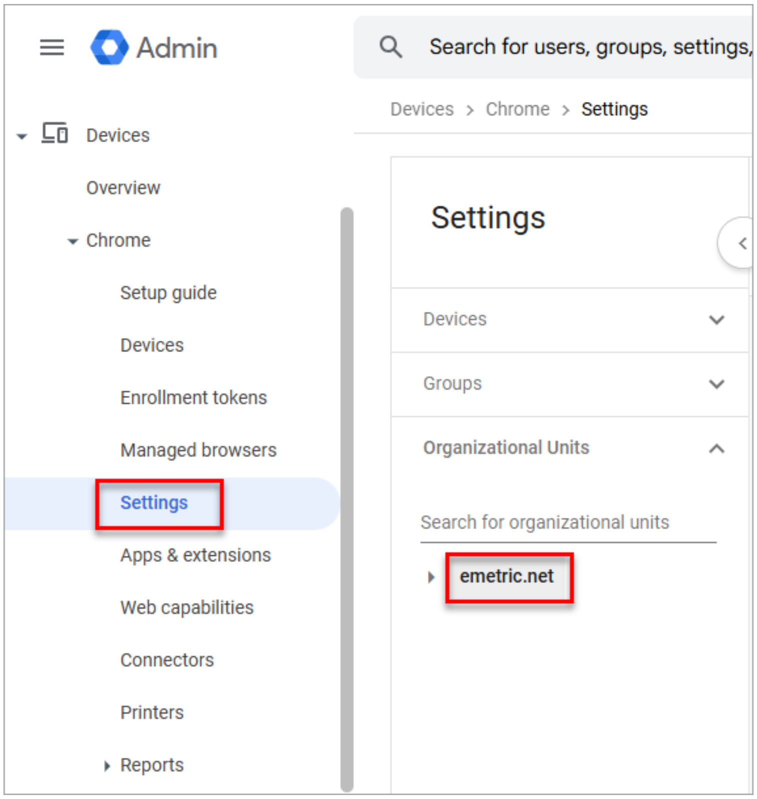
Enable Device Attributes API
Inherited from Google default

Web app can run offline
Inherited from Google default

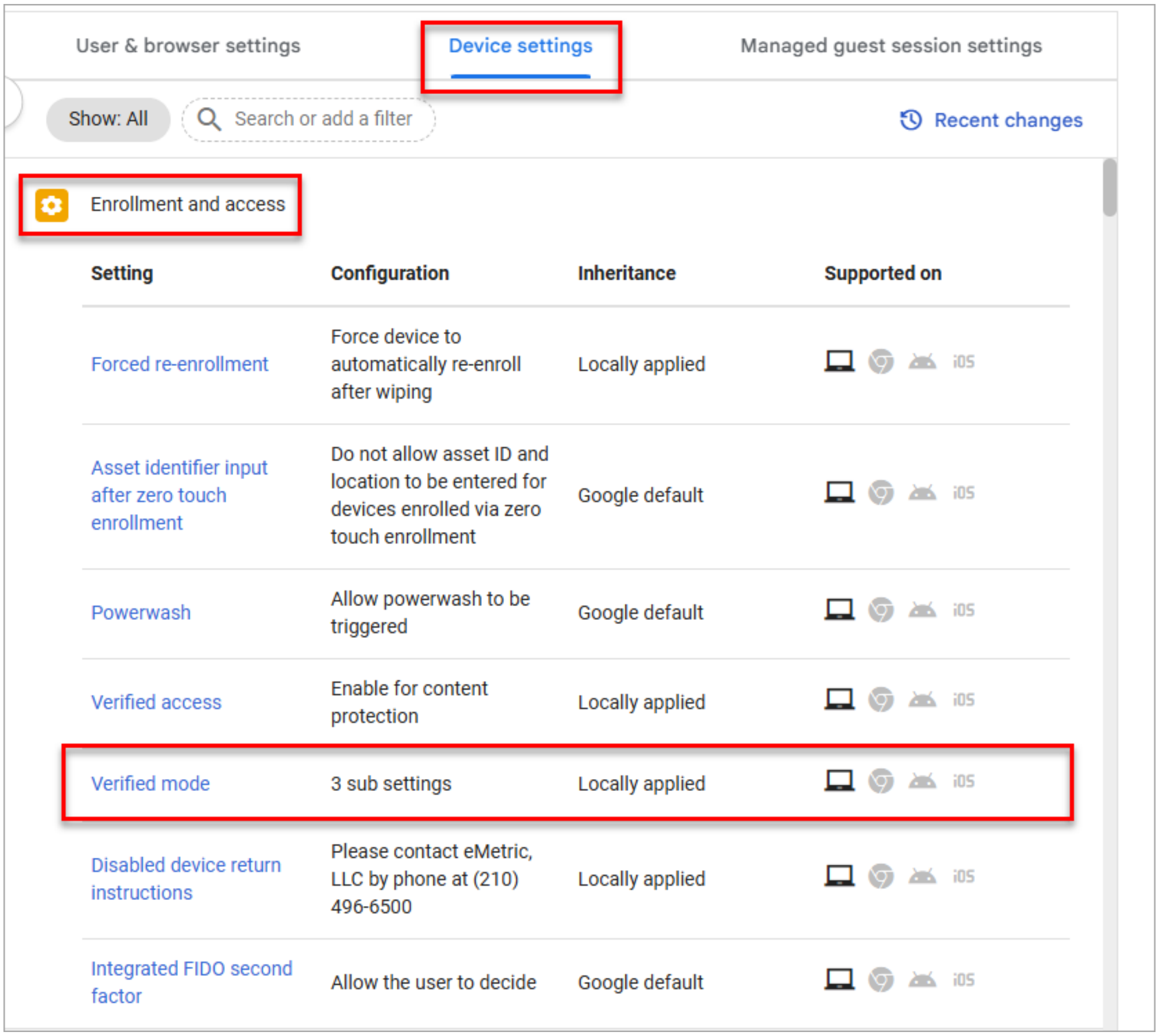
19. Next set up **Verified Mode**. Verified Mode ensures that only enrolled and trusted ChromeOS devices can run the ChromeOS PWA and your testing environment remains secure and authenticated. Go to **Devices** then select **Chrome**.



20. Click on **Settings** and then choose the relevant **Organizational Unit** where the MCAS web app is installed.



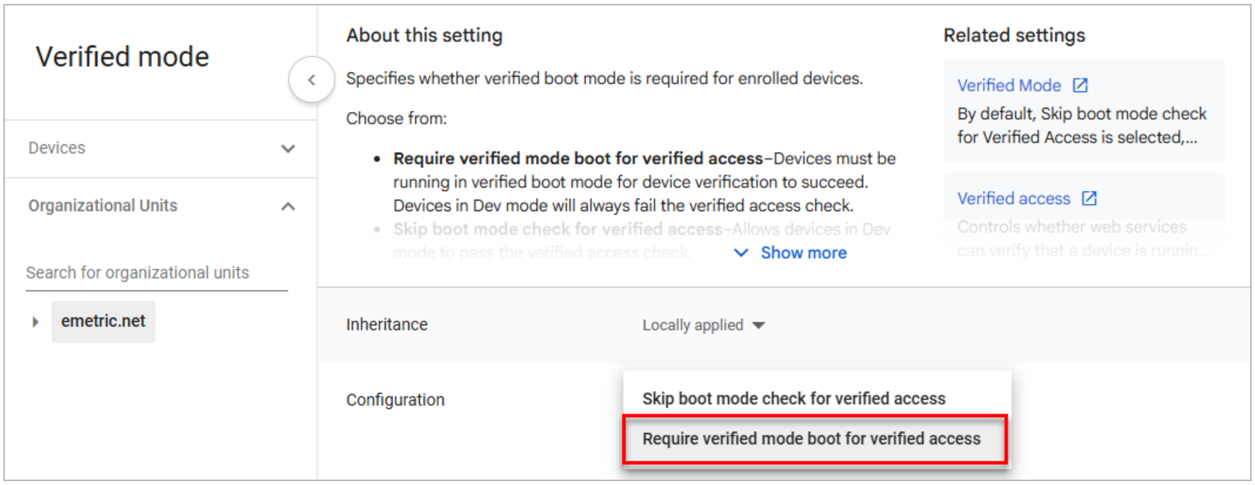
21. Select the **Device settings** tab. Under **Enrollment and access**, select **Verified mode**.



Enrollment and access

Setting	Configuration	Inheritance	Supported on
Forced re-enrollment	Force device to automatically re-enroll after wiping	Locally applied	💻 ◎ 🤖 iOS
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	💻 ◎ 🤖 iOS
Powerwash	Allow powerwash to be triggered	Google default	💻 ◎ 🤖 iOS
Verified access	Enable for content protection	Locally applied	💻 ◎ 🤖 iOS
Verified mode	3 sub settings	Locally applied	💻 ◎ 🤖 iOS
Disabled device return instructions	Please contact eMetric, LLC by phone at (210) 496-6500	Locally applied	💻 ◎ 🤖 iOS
Integrated FIDO second factor	Allow the user to decide	Google default	💻 ◎ 🤖 iOS

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



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.

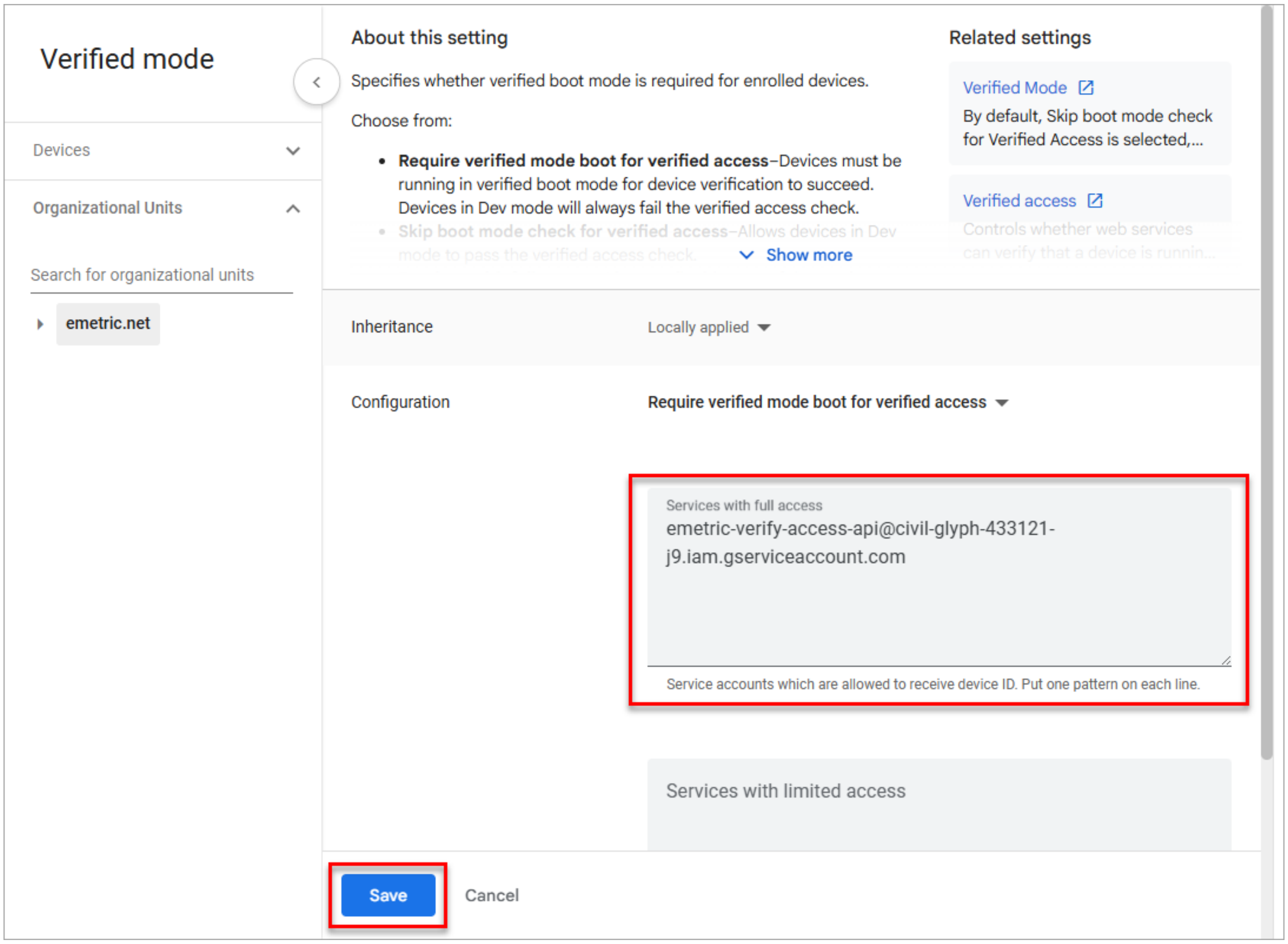
Verified Mode
By default, Skip boot mode check for Verified Access is selected,...

Verified access
Controls whether web services can verify that a device is runnin...

Inheritance: Locally applied

Configuration:
Skip boot mode check for verified access
Require verified mode boot for verified access

23. Under **Services with full access** add the verified access service account **emetric-verify-access-api@civil-glyph-433121-j9.iam.gserviceaccount.com** and then select **Save**.



Verified mode

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.

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 runnin...

Inheritance: Locally applied

Configuration: Require verified mode boot for verified access

Services with full access

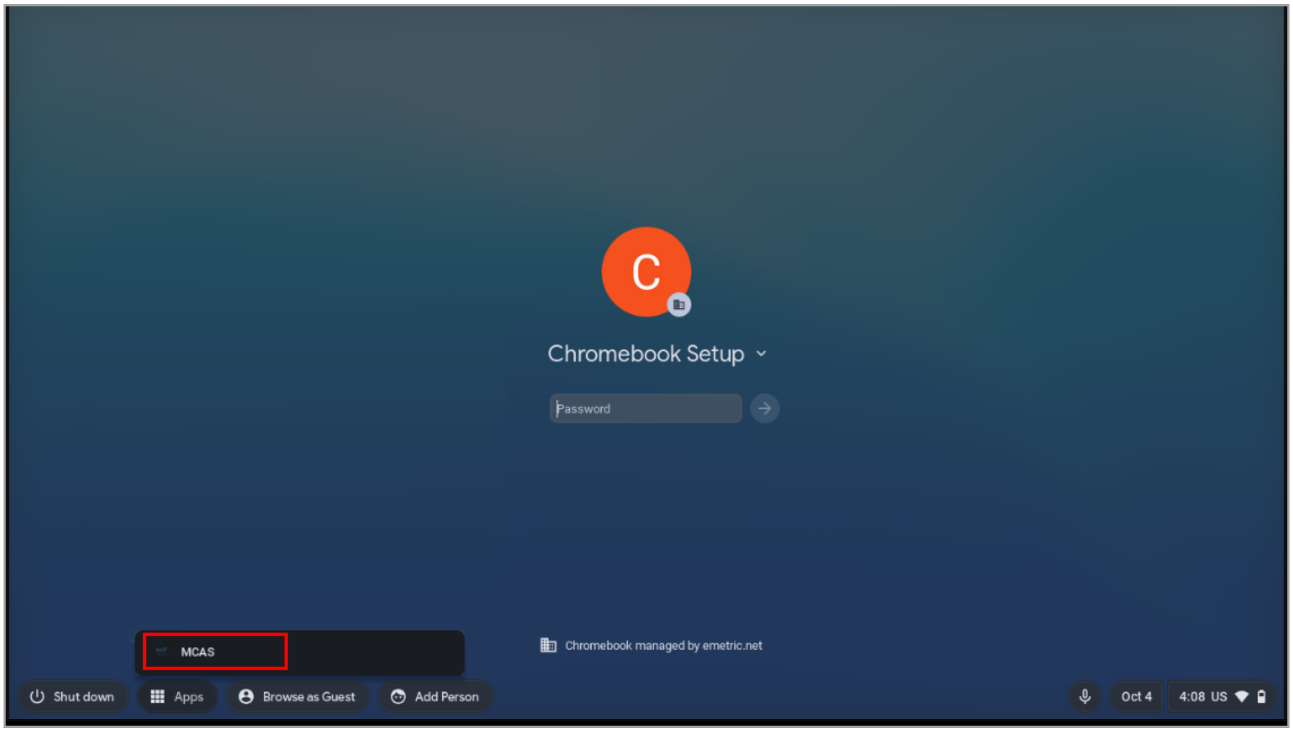
emetric-verify-access-api@civil-glyph-433121-j9.iam.gserviceaccount.com

Service accounts which are allowed to receive device ID. Put one pattern on each line.

Services with limited access

When these steps are completed, the MCAS web app Kiosk 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.

24. When you are ready to conduct Site Readiness for this configuration, see section V: Site Readiness Testing and Site Certification.