



MCAS Student Kiosk Technology Guide

2025-2026 MCAS Test Administrations

Updated January 26, 2026



This document was prepared by the
Massachusetts Department of Elementary and Secondary Education
Pedro Martinez, Commissioner

The Massachusetts Department of Elementary and Secondary Education, an affirmative action employer, is committed to ensuring that all of its programs and facilities are accessible to all members of the public. We do not discriminate on the basis of age, color, disability, national origin, race, religion, sex, gender identity, or sexual orientation. Inquiries regarding the Department's compliance with Title IX and other civil rights laws may be directed to the Human Resources Director, 135 Santilli Highway, Everett, MA 02149. Phone: 781-338-6105.

© 2026 Massachusetts Department of Elementary and Secondary Education
Permission is hereby granted to copy any or all parts of this document for non-commercial educational purposes. Please credit the "Massachusetts Department of Elementary and Secondary Education."

Massachusetts Department of Elementary and Secondary Education 135 Santilli Highway, Everett, MA 02149
Phone 781-338-3000 TTY: N.E.T. Relay 800-439-2370 www.doe.mass.edu



Important Contact Information and Resources

Contact: **MCAS Service Center**

For questions on:

- general test administration support
- MCAS Portal and MCAS Student Kiosk such as
 - user accounts
 - technology support and readiness
 - student registration process and loading files
 - viewing student data
 - scheduling tests
- locating resources
- shipments of materials

Hours: 7:00 a.m.–5:00 p.m., Monday–Friday

Web: mcas.onlinehelp.cognia.org

Email: mcas@cognia.org

Telephone: 800-737-5103 TTY: 888-222-1671

Contact: **DESE Office of Student Assessment Services**

For questions on:

- policy, such as assigning accessibility features and accommodations
- student participation
- testing irregularities, including test security incidents and technology failures
- reactivating tests for CBT
- student data and SIMS (See note below regarding SIMS.)

Questions regarding SIMS data should be directed to the district's SIMS contact (go to profiles.doe.mass.edu/search/search.aspx?leftNavID=11239, select **SIMS Contact** from the **Function** menu, and click **Get Results**).

Hours: 8:00 a.m.–5:00 p.m., Monday–Friday during test administration windows

Between 7:00 a.m. and 8:00 a.m. during the test administration windows, MCAS Service Center representatives will receive calls to 781-338-3625, answer questions regarding logistics, and take messages for Department staff, which will be returned during our regular business hours.

Web: www.doe.mass.edu/mcas/admin.html

Email: mcas@mass.gov

Telephone: 781-338-3625

Table of Contents

I. INTRODUCTION.....	1
A. Technology Overview	1
B. Overview of Steps for Technology Coordinators	1
II. TECHNOLOGY GUIDELINES	3
A. Operating System Support Plan	3
B. MCAS Student Kiosk Device Specifications.....	4
C. MCAS Portal Browser Specifications	5
D. Accommodations with Supported Operating Systems	5
III. TECHNOLOGY SETUP	5
A. Network Connectivity	5
B. Bandwidth.....	7
C. Thin-Client Environments	7
D. Monitor Settings.....	7
IV. MCAS STUDENT KIOSK INSTALLATION.....	8
A. ChromeOS Application Installation	8
B. iPadOS Application Installation	22
C. Linux	25
D. MacOS	31
E. Windows OS	38
V. SITE READINESS TESTING AND SITE CERTIFICATION	45
A. Purpose.....	45
B. Using the Site Readiness Tool.....	45
C. Site Certification.....	53
APPENDIX A: STUDENT TOOLS, ACCESSIBILITY FEATURES, AND ACCOMMODATIONS UNAVAILABLE FOR SITE READINESS	56
APPENDIX B: MCAS STUDENT KIOSK ERROR MESSAGE GUIDANCE FOR TECHNOLOGY STAFF	57

Document updates:

Updated January 13, 2026: Section IV A: ChromeOS Application Installation has been reordered for clarity. Clarified ChromeOS set up step 10 on page 13 in the section Install the New MCAS Web App for ChromeOS and step 5 on page 18 in the section Configure your Device Settings.

Updated January 26, 2026: Section V B: Added information about the System Set-Up link that is shown on the MCAS Student Kiosk sign in screen for Windows and ChromeOS devices.

I. Introduction

This document is intended for technology staff responsible for setting up the MCAS computer-based testing technology.

MCAS computer-based testing will use the following components:

- the **MCAS Portal**, the test administration and management website for district test coordinators, technology coordinators, principals/school test coordinators, test administrators, and other staff as needed
- the **MCAS Training Site**, where test coordinators, principals, technology coordinators, and test administrators can practice the tasks required in the MCAS Portal
- the **MCAS Student Kiosk**, the student testing platform

This document contains information on technology requirements, instructions for installing the MCAS Student Kiosk and conducting Site Readiness testing on student devices used for computer-based testing, and guidance on error messages that could occur when using the MCAS Student Kiosk.

For more information on working with the MCAS Portal, see the *Guide to the MCAS Portal*, which is available in the [MCAS Resource Center](#).

A. Technology Overview

The MCAS Student Kiosk is used by students for secure online testing. The kiosk restricts access to other computer applications during testing and is a cross-platform application. The kiosk runs on Windows®, Mac®, and Linux® operating systems, iPad® tablets, and Chromebook™ notebook computers.

Information on using third-party accessibility or accommodations software with the kiosk can be found in [Appendix E: Using Assistive Technology as an MCAS Test Accommodation](#) of the *Accessibility and Accommodations Manual for the 2025–2026 Test Administrations*.

B. Overview of Steps for Technology Coordinators

The MCAS Student Kiosk is installed and set up by a Technology Coordinator (TC). District Test Coordinators (DTCs) and School Test Coordinators (STCs) can also perform these tasks.

After your DTC or STC has set up your TC account, you will receive your user account information via email. If you have not received your account information with your login credentials, contact your DTC or STC.

Follow the steps below to install and set up the MCAS Student Kiosk for your school. Further information on each step is provided in subsequent sections.

1. Review the Technology Guidelines in Section II of this document to ensure that you have the correct devices and equipment for student testing.
2. Configure your network to support student testing on the kiosk by following the instructions in Section III: Technology Setup.
3. Download and install the appropriate MCAS Student Kiosk to each student testing device by following the instructions in Section IV: MCAS Student Kiosk Installation below:
 - [ChromeOS application](#)
 - [iPadOS application](#)
 - [Linux](#)
 - [MacOS](#)
 - [Windows](#)

If your student testing devices have the MCAS Student Kiosk installed from the 2024–25 school year, please see the table below and the instructions in each section linked above.

Kiosk Installed in 2024–25	Action Required for MCAS Testing in 2025–26
ChromeOS	Uninstall the old MCAS kiosk app from the ChromeOS management console. Add the new MCAS Web app and extension.
iPad	Manually update the kiosk if automatic updates are not enabled.
Linux	Uninstall the old kiosk and then download and install the new kiosk.
MacOS	Schools are not required to uninstall the old kiosk. They will need to download and install the new kiosk.
Windows	Schools are not required to uninstall the old kiosk. They will need to download and install the new kiosk.

4. Complete [Site Readiness](#), using the Site Readiness tool, and certify that the school's devices and technology are ready for testing. All schools should complete Site Readiness to confirm that the school's technology infrastructure has been set up correctly and that testing devices meet minimum requirements and have been properly configured.

Note: To ensure that the school technology setup is ready for MCAS testing, it is recommended to complete Site Readiness at least four weeks prior to testing. When all the configurations that will be used for student testing are ready, [certify](#) that the site is ready for student testing.

Contact the MCAS Service Center with any questions about technology guidelines, downloading the MCAS Student Kiosk, and the Site Readiness tool.

II. Technology Guidelines

A. Operating System Support Plan

The table below describes eMetric's plan for supporting operating systems during the upcoming school year for MCAS computer-based testing. This plan helps districts and schools manage operating system deployments based on the support timelines.

Districts and schools can use the support plan below to anticipate technology needs for the 2025–26 school year. Students testing on devices that do not meet the technology guidelines may encounter performance-related issues during testing. OS updates should not be made during the spring testing windows.

Please note the following major updates:

- Windows 10 is no longer supported
- eMetric has updated their Chrome OS support policy to support a larger number of ChromeOS versions each year, as described in the table below.

Table 1. Operating System Support Plan

Operating System	Version	Version Release Date	End of Support Date	eMetric Support Policy
Chrome OS™	138+ 132+ LTS	July 2025 April 2025	End of 2025–26 school year (June 2026)	eMetric supports the versions of ChromeOS that are current as of July of each school year. These versions will be supported through the end of the school year (June). Schools are not recommended to use beta versions of ChromeOS, as this may result in errors.
iPadOS®	17.7+	September 2024	End of 2025–26 school year	eMetric supports the latest three major versions that are supported by Apple.
	18.5+	September 2024	End of 2026–27 school year	
	26	September 2025	End of 2027–28 school year	

Operating System	Version	Version Release Date	End of Support Date	eMetric Support Policy
Linux®, Fedora™ (64-bit only)	42	April 2025	End of 2025–26 school year	eMetric supports the latest version of Fedora.
macOS®	14.7+	September 2023	End of 2025–26 school year	eMetric supports the latest three major versions that are supported by Apple.
	15.5+	September 2024	End of 2026–27 school year	
	26	September 2025	End of 2027–28 school year	
Windows®	11 (22H2, 23H2, 24H2)	October 2021	October 2031	eMetric supports major versions of Windows that are supported by Microsoft. The latest supported minor versions of Windows are supported.

B. MCAS Student Kiosk Device Specifications

Students must use devices that meet the specifications provided in the table below.

Table 2. Student Device Specifications

System Requirements – All Hardware	
Connectivity	Student devices must be able to connect to the internet via wired or wireless networks.
Screen Size	9.7" screen size or larger/ "10-inch class" tablets or larger "11-inch class" tablets or larger are highly recommended
Screen Resolution	1024 x 768 or larger
Browser Requirements	
Browsers (used for practice tests only)	Chrome 138 or newer Firefox 140 or newer Microsoft Edge 138 or newer Safari 18.5 or newer
Desktop and Laptop Specific Requirements	
CPU	1.3 GHz

Memory	2 GB (4GB is strongly recommended for best performance)
--------	---

C. MCAS Portal Browser Specifications

The MCAS Portal is accessible via the following browsers on desktops and laptops:

- Chrome 138 or newer
- Firefox 140 or newer
- Microsoft Edge 138 or newer
- Safari 18.5 or newer

D. Accommodations with Supported Operating Systems

Certain accommodations in the MCAS Student Kiosk are only supported on specific operating systems as described in the table below.

Table 3. Accommodations with Supported Operating Systems

Accommodation	Supported Operating System
Compatible Assistive Technology	Windows
Mouse Pointer	Windows, macOS, ChromeOS, and iPadOS*
Screen Reader	Windows (NVDA, JAWS)
Speech-to-Text Standard	Windows, macOS, ChromeOS, and iPadOS
Speech-to-Text Special Access	Windows, macOS, ChromeOS, and iPadOS
Word Prediction Standard	Windows, macOS, ChromeOS, and iPadOS
Word Prediction Special Access	Windows, macOS, ChromeOS, and iPadOS

*iPadOS: It is highly recommended to use an external mouse.

III. Technology Setup

A. Network Connectivity

All student testing devices should have access to the internet and be able to access the server using HTTP/HTTPS protocols on ports 80 and 443.

Allow the following sites on ports 80 and 443 in content filtering proxies or other locally used proxy software.

- <https://mcas.cognia.org>
- <https://mcas-training.cognia.org>
- <https://mcas-practicetest.cognia.org>

- fonts.googleapis.com/
- themes.googleusercontent.com/
- googleusercontent.com/
- <https://cognito-identity.us-west-2.amazonaws.com>
- <https://cognito-identity.us-east-1.amazonaws.com>
- <https://eventsapi.emetric.net/maprod/router>
- app.getsentry.com
- dc.services.visualstudio.com
- az416426.vo.msecnd.net
- speech.beta.cowriter.dev
- wss://*.cowriter.dev
- <https://ws.cowriter.dev/>
- <https://www.google.com/speech-api>

If you are working with sandboxing applications, complete one of the following steps while installing the kiosk, and contact the MCAS Service Center with questions:

- Choose a network folder location for local caching.
- Make sure the default location, such as **C:\Users\user\AppData\Local\emetric (%localappdata%/emetric)**, and its contents are not deleted by the sandboxing applications.

Note: Student testing data, including encrypted responses, will be saved to the indicated location only if the network connection or internet connection is lost during the test. Students will be able to continue testing without interruption, but their testing data will be saved in the indicated folder.

A note about OneDrive:

OneDrive notifications may interfere with the kiosk and student test taking experience. If OneDrive attempts to steal the screen's focus during testing, the kiosk will display a white screen. The student will then have to click anywhere on the white screen to regain focus in the kiosk; once clicked they will be able to resume testing where they left off. To prevent this, schools should use one of the following approaches:

- If OneDrive is not needed or used on student devices, schools are recommended to disable OneDrive during student testing.
- If OneDrive cannot be disabled, please take necessary steps to prevent any administrative actions, including file sharing or synchronization and administration updates to OneDrive settings, that would trigger a OneDrive notification during student testing.

B. Bandwidth

The ability of a school's network to support a given number of online testers is a function of the available bandwidth between the student's test device and the data center serving the test content, the number of students who will be downloading tests, and the size of the test content. The Site Readiness tool's Connection Capacity Test will measure the bandwidth between a student's test device and the data center and determine the number of tests that can be downloaded at the school simultaneously. Use the results of this test to gauge the impact your bandwidth will have on student testing.

Schools with low internet bandwidth (i.e., an internet download speed of less than 1.5 Mbps or an internet upload speed of less than 256 Kbps) should stagger student start times by 1–2 minutes to reduce the likelihood of interruptions.

C. Thin-Client Environments

When using thin-client environments, such as Terminal Services, Citrix, or LTSP, make sure that there is enough memory, CPU, and bandwidth on the server to accommodate multiple student test sessions. The application requires a minimum of 80 MB of memory per client session and performance can vary depending on the size and type of the test. Allowing multiple sessions on an improperly sized thin-client environment will result in poor performance.

Additionally, schools using thin-clients need to be cautious when there is 1 GB or less of physical memory on the student testing device. In this case, a local installation is strongly recommended. As a rule, if you can use the Chrome™ browser to access web-based email or web-based streaming services on all student testing devices simultaneously, then testing should go well.

In thin-client environments, the accounts students use to log in to the student testing devices (not the MCAS test login) must be unique for each student. Also, each account must have its own dedicated user profile.

For assistance, contact the MCAS Service Center at mcas@cognia.org or 800-737-5103.

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: These are only recommended screen resolutions. Use the screen resolution the student is most comfortable with. 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 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.

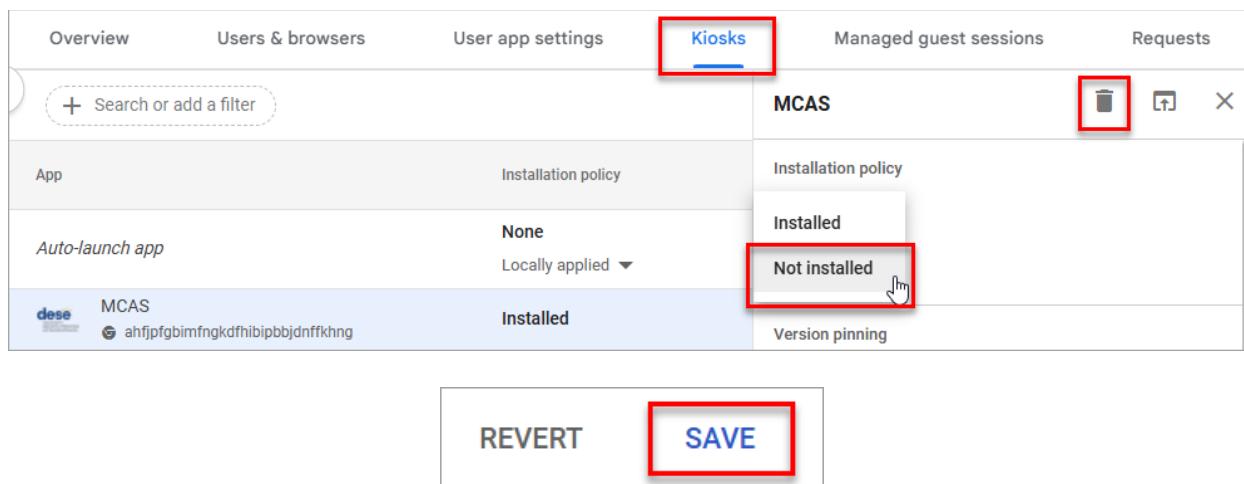
Review section II: [Technology Guidelines](#) and section III: [Technology Setup](#) in detail.

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.



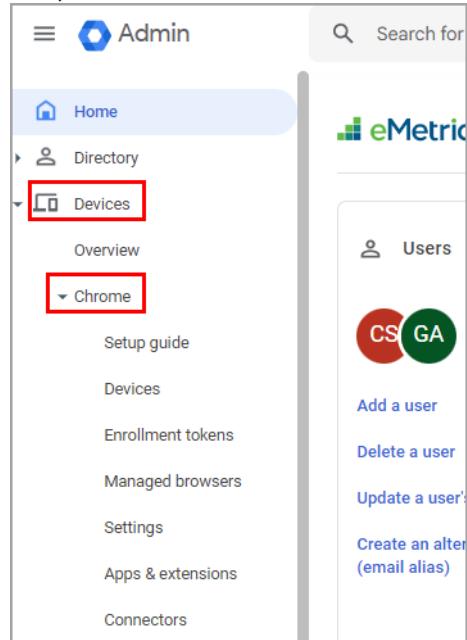
6. Once the MCAS Chrome App has been removed, follow the steps below for installing the MCAS web app and extension.

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.

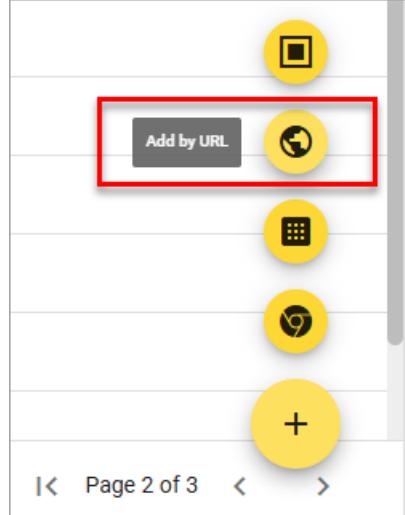
The screenshot shows the Admin interface with the 'Apps & extensions' menu selected. The 'Kiosks' tab is highlighted with a red box. The table lists apps installed on kiosks, including 'eMetric Assessments' (Not installed), 'eMetric for Chrome' (Installed, Not pinned), and 'eMetric for Chrome (Mobile)' (Not installed). A yellow circle with a plus sign is in the bottom right corner of the table.

App	Installation policy	Version pinning
Auto-launch app	None Locally applied	
eMetric Assessments	Not installed	
eMetric for Chrome	Installed	Not pinned
eMetric for Chrome (Mobile)	Installed	Not pinned

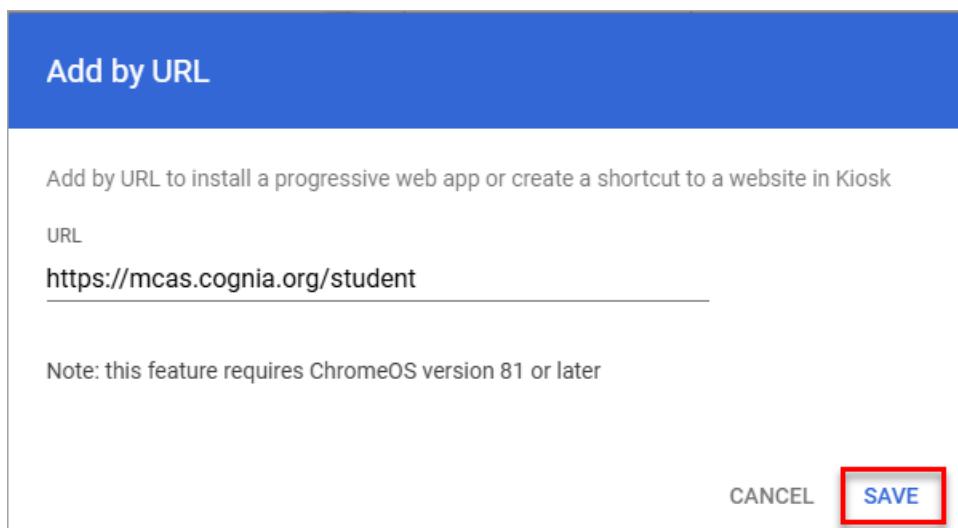
Note: Ensure that child organizational units inherit the app and policy settings from the parent OU. If inheritance is disabled, the kiosk app will not appear on devices in

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**.

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

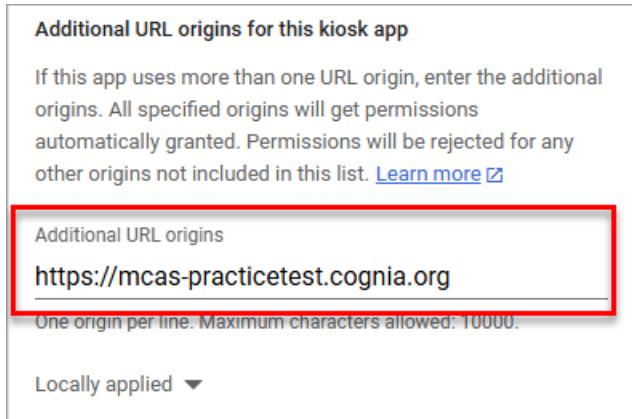
If this app uses more than one URL origin, enter the additional origins. All specified origins will get permissions automatically granted. Permissions will be rejected for any other origins not included in this list. [Learn more](#)

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**.

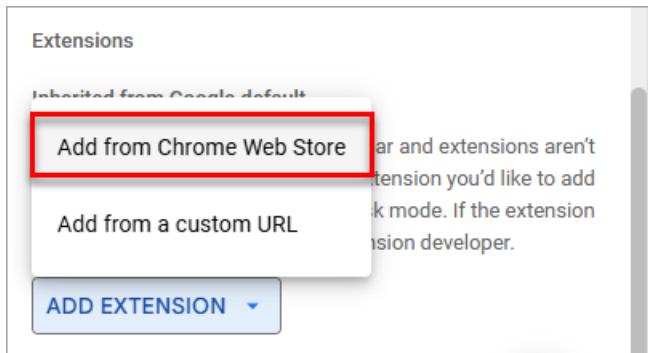
Extensions

Inherited from Google default

Add from Chrome Web Store

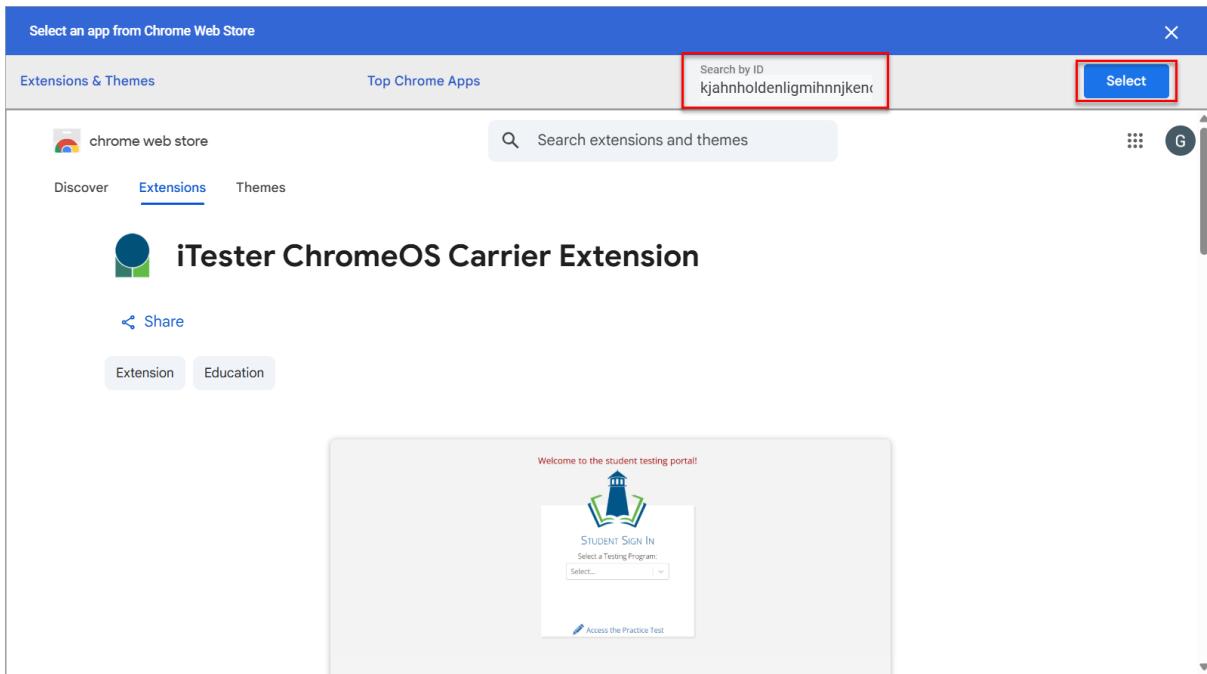
Add from a custom URL

ADD EXTENSION ▾

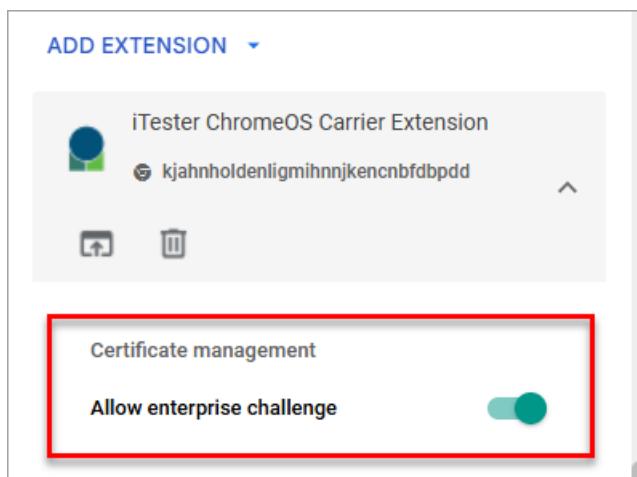


10. In the Chrome Web Store, ensure the iTester ChromeOS Carrier extension ID is entered exactly as it is shown below, with no additional spaces, in the **Search by ID** text box and then select the **Select** button to add the extension.

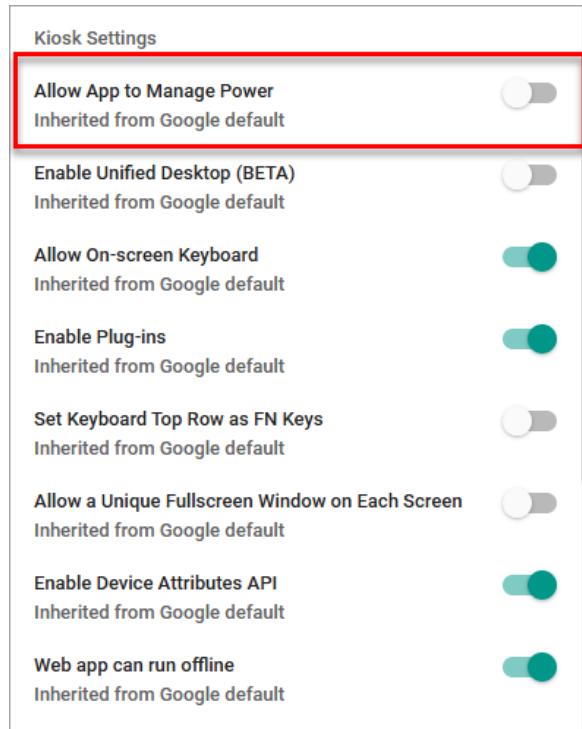
- **`kjahnholdenligmihnnjkencnbfdbpdd`**



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.

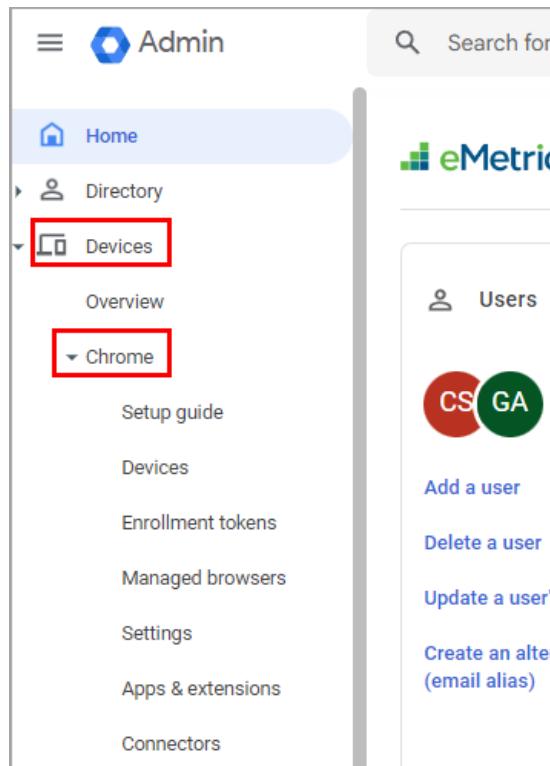


Important Note: Verify in Kiosk Settings that “Allow App to manage power” is **disabled**. To do this, click on **Devices, Apps & Extensions** and then select **Kiosks**. Click on the **MCAS** app name and check to make sure the setting **Allow app to manage power** is **disabled** (slider is moved to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

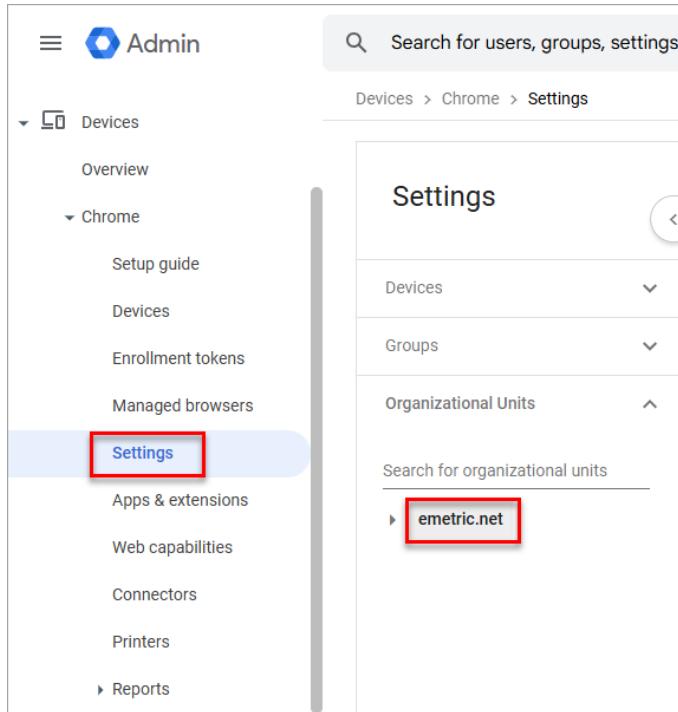


Step 4: Configure Device Settings

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`.



The screenshot shows the Google Admin console interface. On the left, there is a navigation sidebar with the following structure:

- Devices (selected)
- Overview
- Chrome
 - Setup guide
 - Devices
 - Enrollment tokens
 - Managed browsers
 - Settings** (selected)
 - Apps & extensions
 - Web capabilities
 - Connectors
 - Printers
 - Reports

On the right, the main content area is titled "Settings" and shows the following structure:

- Devices
- Groups
- Organizational Units
 - Search for organizational units
 - 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	
 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

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

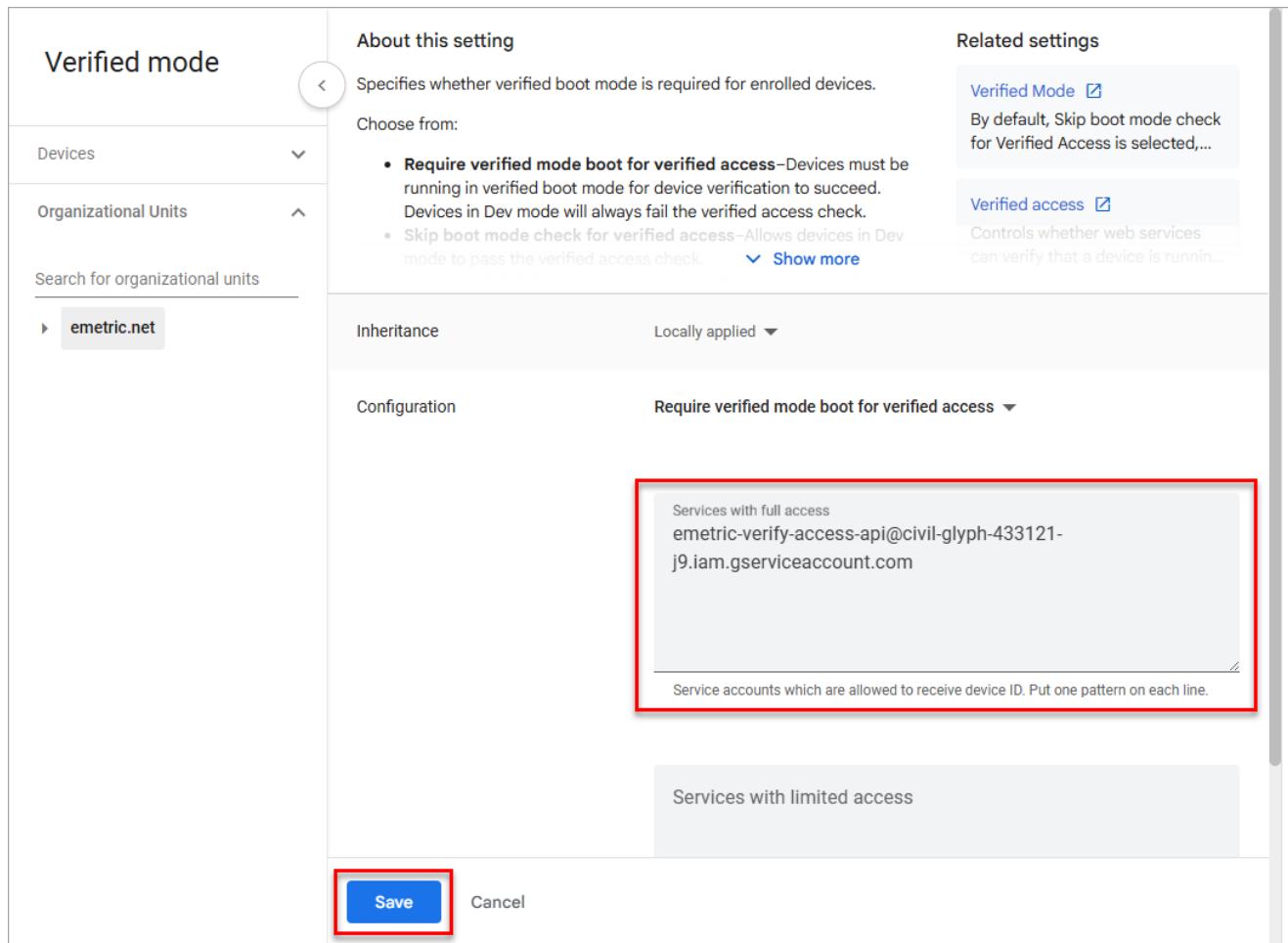
Verified mode	About this setting	Related settings
Devices	Specifies whether verified boot mode is required for enrolled devices. Choose from: <ul style="list-style-type: none">Require verified mode boot for verified access—Devices must be running in verified boot mode for device verification to succeed. 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 <input checked="" type="checkbox"/> By default, Skip boot mode check for Verified Access is selected,...
Organizational Units		Verified access <input checked="" type="checkbox"/> Controls whether web services can verify that a device is running...
Search for organizational units		
emetric.net	Inheritance Locally applied	
	Configuration  	

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 shows the 'Verified mode' settings screen. The left sidebar shows 'Devices' and 'Organizational Units'. The main content area is titled 'About this setting' and describes the requirement for verified boot mode. It includes a 'Choose from:' section with two options: 'Require verified mode boot for verified access' (selected) and 'Skip boot mode check for verified access'. A 'Show more' link is available for the second option. Below this is an 'Inheritance' section with 'Locally applied' selected. The 'Configuration' section shows 'Require verified mode boot for verified access'. The 'Services with full access' section contains the service account 'emetric-verify-access-api@civil-glyph-433121-j9.iam.gserviceaccount.com', which is highlighted with a red box. A note below says 'Service accounts which are allowed to receive device ID. Put one pattern on each line.' At the bottom, there are 'Save' and 'Cancel' buttons, with 'Save' also highlighted with a red box.

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**.

Device settings

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

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.

Configuration	Supported on
DeviceEphemeralUsersEnabled	ChromeOS since version 19

Inheritance

Locally applied

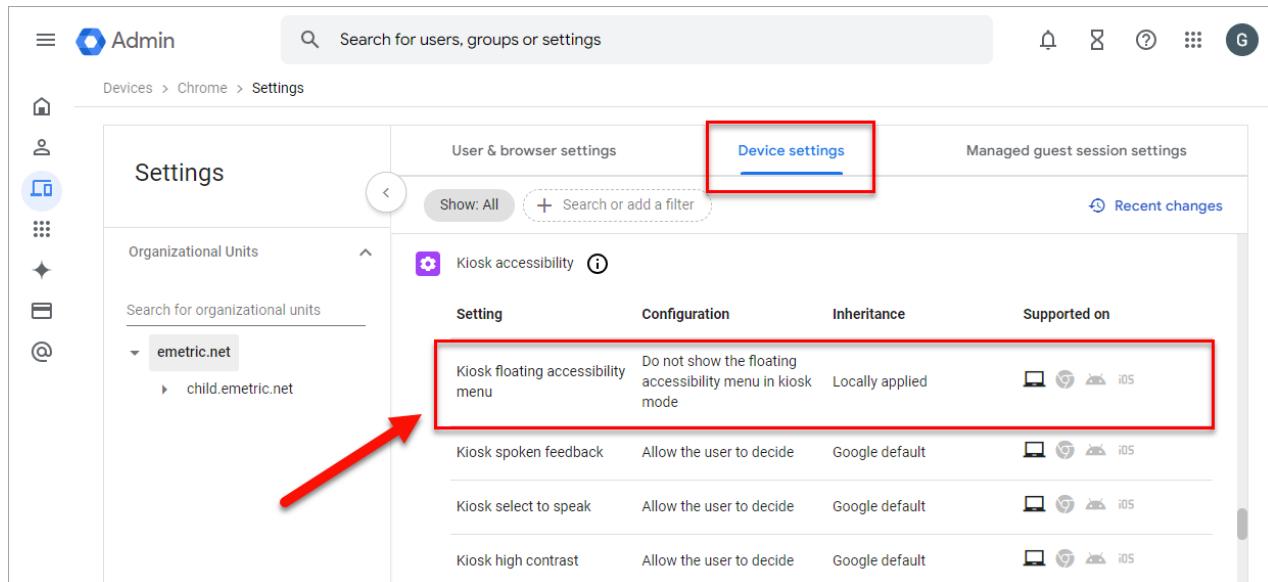
Configuration

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 left sidebar has icons for Home, Devices, Groups, Organizational Units, and Email. The main navigation bar shows 'Admin' with a gear icon, a search bar 'Search for users, groups or settings', and various status icons. The path 'Devices > Chrome > Settings' is visible. On the left, under 'Settings', 'Organizational Units' is expanded to show 'emetric.net' and 'child.emetric.net'. The main content area is titled 'User & browser settings' with a sub-section 'Kiosk accessibility'. A red box highlights the 'Device settings' tab in the top navigation bar. Another red box highlights the 'Kiosk floating accessibility menu' row in the table below, which is also pointed to by a red arrow from the left sidebar.

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

Organizational Units

Search for organizational units

emetric.net

child.emetric.net

Chromium name: FloatingAccessibilityMenuEnabled

Supported on: ChromeOS since version 84

Inheritance: Locally applied

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

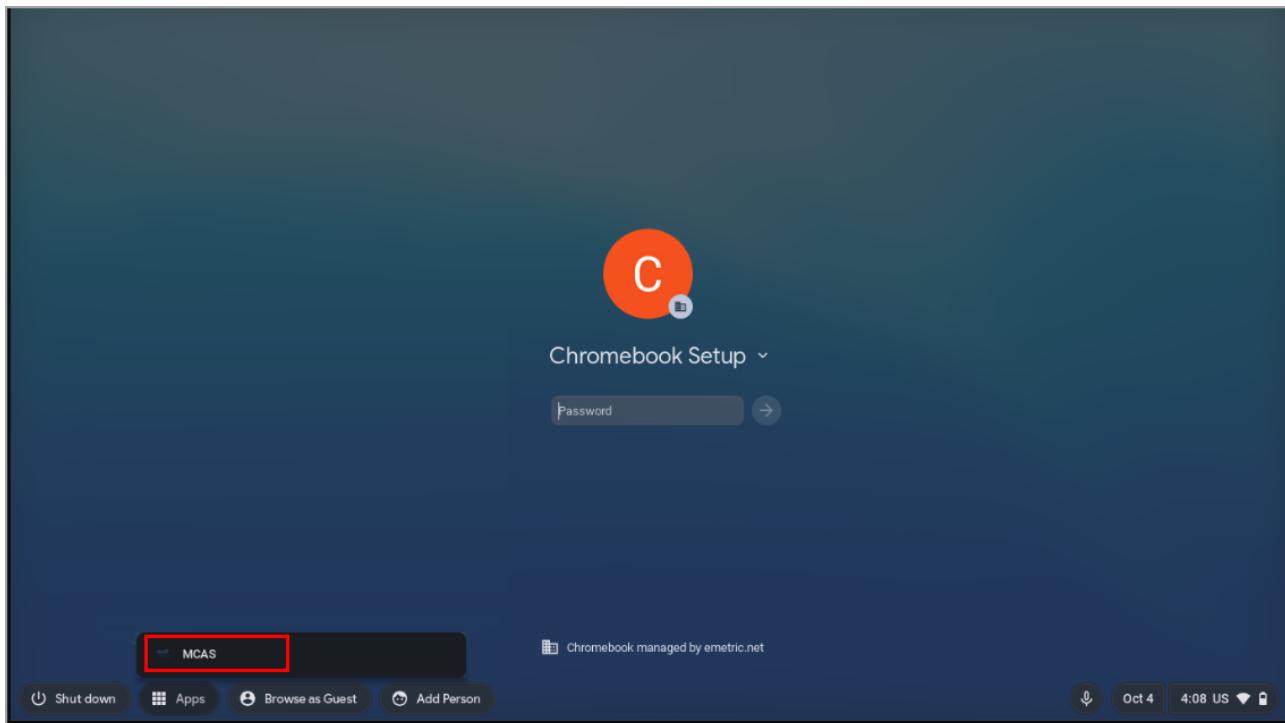
Save Cancel



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](#).

B. iPadOS Application Installation

Step 1: Set up your school testing environment

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

Step 2: Update or download the iTester App.

If the iTester app was installed on your devices in the previous school year, the app will need to be updated.

- If automatic updates are enabled, no action is required.
- If automatic updates are not enabled on the iPad, follow the steps below to update the iTester app.

1. Open the **App Store** on the iPad
2. Tap your **Apple ID icon** or your profile picture in the top right corner.
3. Scroll down to see pending updates.
4. Tap **Update** next to the iTester app.

If the iTester app was not installed on your devices previously, follow the steps below to install the iTester application.

Download the iTester App from the Apple App Store

The iTester iPad application is a Single Instance application. Technology coordinators will select the MCAS during the initial setup of the app. If you do not already have the iTester app on your iPad, download it from the Apple App Store following the steps below.

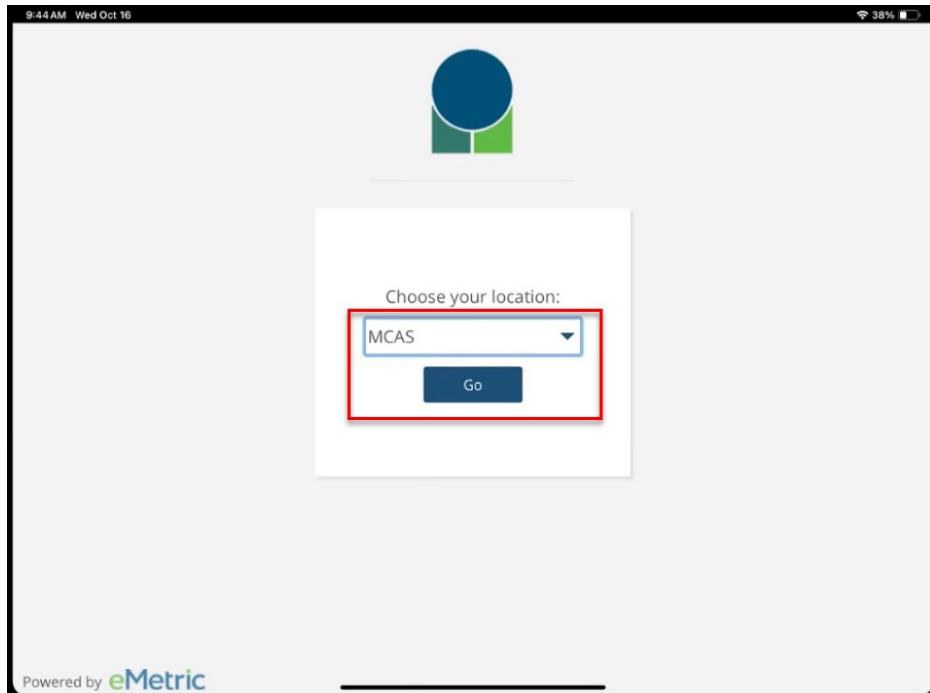
1. Open the **App Store** on the iPad.



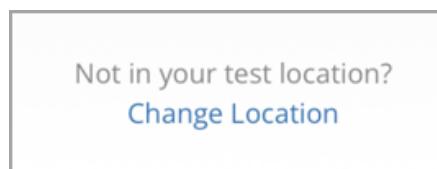
2. Search for **iTester**.
3. When you locate the iTester app, click **Get** to download it to the iPad.



4. Launch the iTester app.
5. Choose **MCAS** from the drop-down menu and then click **Go**. You will be directed to the student sign in screen for the MCAS Student Kiosk.



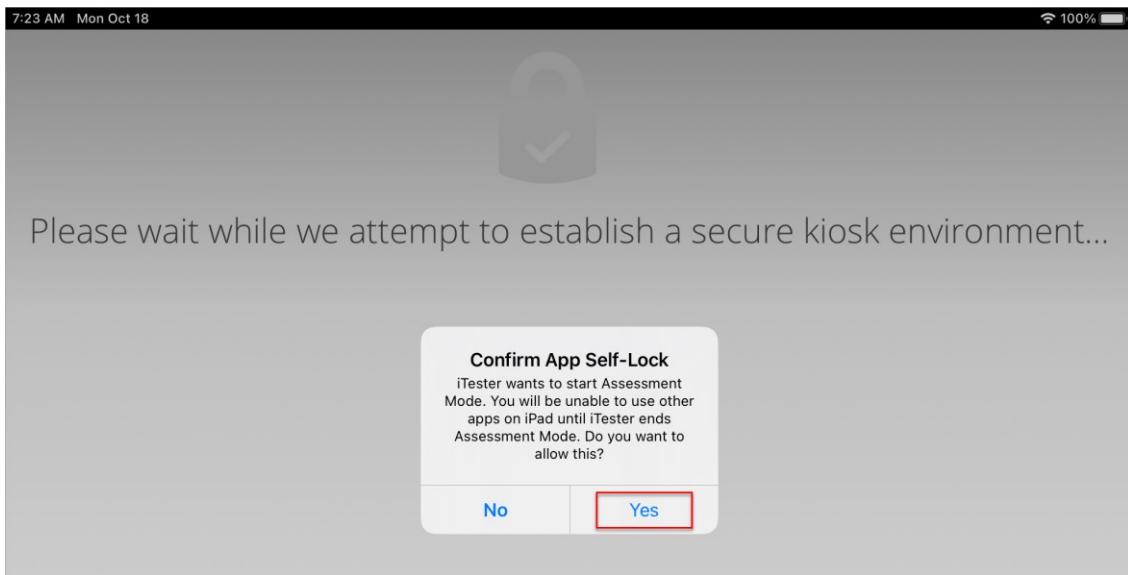
Note: If you select the wrong program in the **Choose your location** drop-down menu, select **Change Location** on the iTester login page.



6. When you are ready to complete Site Readiness for this configuration, see section V: [Site Readiness Testing and Site Certification](#).

Automatic Assessment Configuration

A feature in iPadOS called Assessment Mode (AM) (formerly known as Automatic Assessment Configuration [AAC]) works with iTester to lock down an iPad for online testing. Technology coordinators do not need to do anything to set up AM. When a student launches the iTester App and logs in to a test, and then logs in to a test session, AM will automatically prompt the user to enter single app mode.



This action disables features such as auto correction, define, spell check, predictive keyboard and some keyboard shortcuts. For a complete list, visit this [Apple Support page](#).

This feature helps ensure a secure test environment without requiring technology coordinators to use Mobile Device Manager Software or manually turn on guided access and change keyboard settings. AM is the preferred method of securing the iTester App and should be used in place of guided access. If guided access is on, it will override AM; therefore, guided access should be turned off to allow AM to function. No additional setup is necessary to enable AM.

C. Linux

Step 1: Set up your school technology

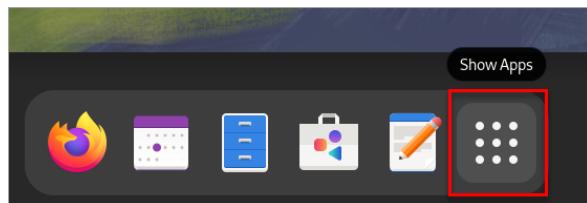
Review section II: [Technology Guidelines](#) and section III: [Technology Setup](#) in detail.

Step 2: Uninstall the MCAS Student Kiosk from the previous year.

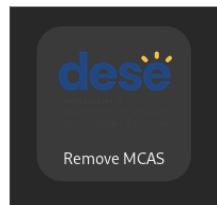
The Linux kiosk is updated each year. If your devices have a previous version of the Linux MCAS Student Kiosk, it will need to be uninstalled before downloading and installing the latest version. To uninstall a previous version of the MCAS Student Kiosk for Linux follow the steps below.

If your devices do not have a previous year's kiosk installed, skip to step 3: Download the MCAS Student Kiosk.

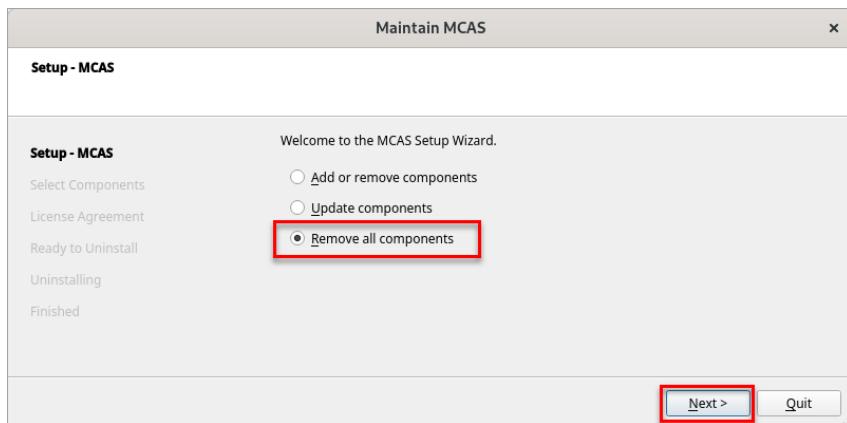
1. On the desktop of the device, select **Show Apps**.



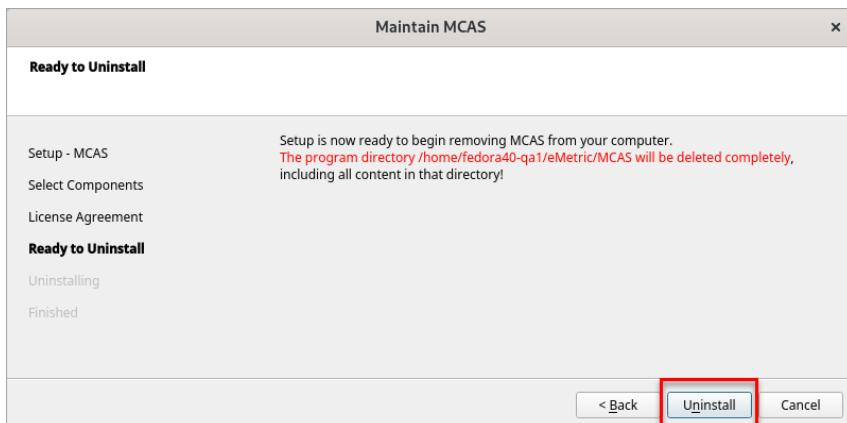
2. Select the icon **Remove MCAS**.



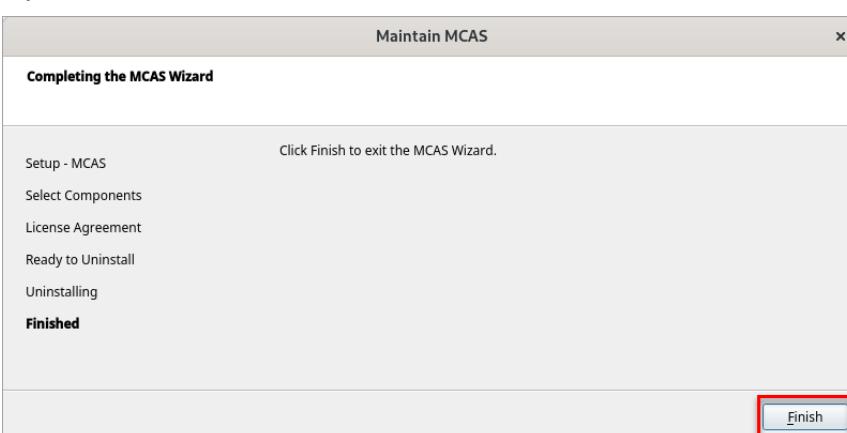
3. Select **Remove all components** and then select **Next**.



4. Select **Uninstall**.



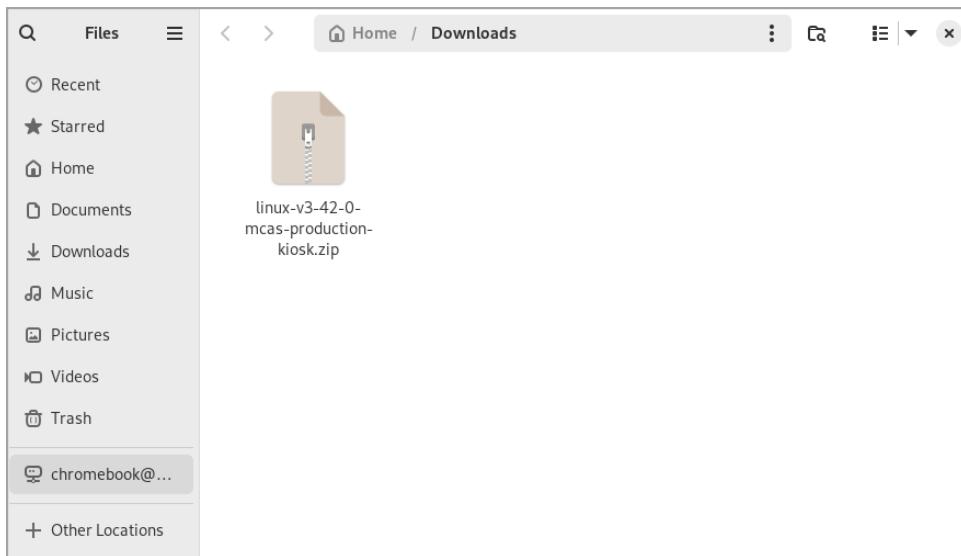
5. Once completed, select **Finish** to exit the MCAS Wizard.



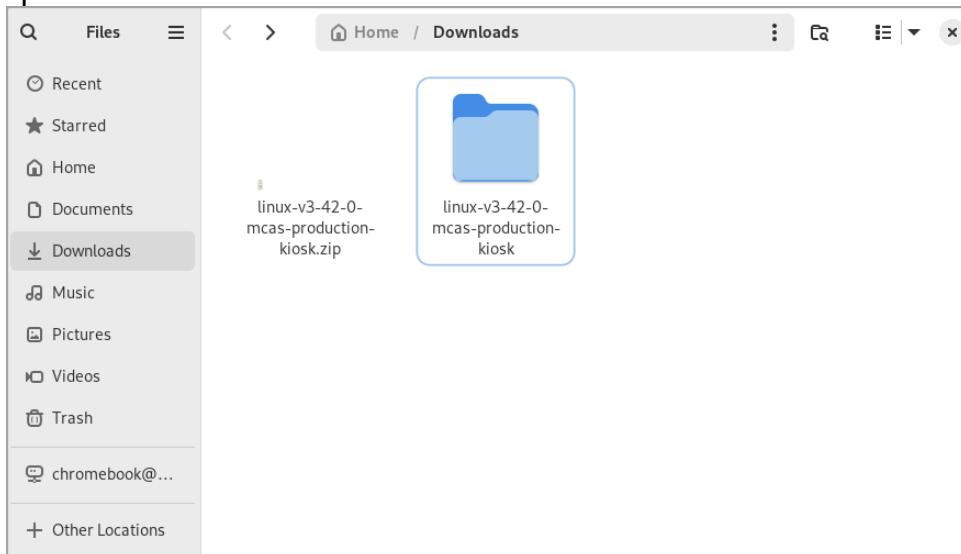
Follow the steps below to install the kiosk on all student testing devices running Linux.

Step 3: Download the MCAS Student Kiosk

1. Go to the [MCAS Portal](#) and log in with your username and password. If you need assistance logging in to the MCAS Portal, contact your school or district test coordinator.
2. On the portal home page, click **Administration**.
3. On the Administration home page, click **Student Kiosk for Linux**. The file will download to the “Downloads” folder.



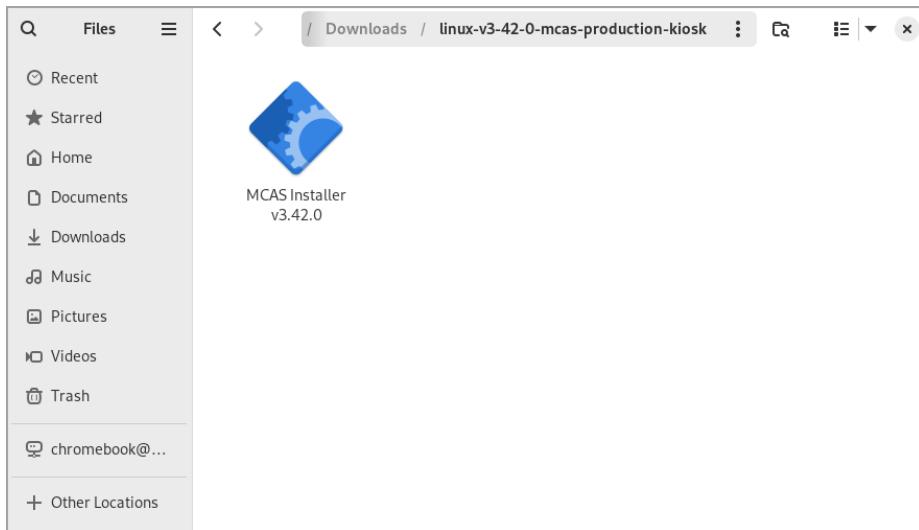
4. Extract the installation file from the zipped package to a location on the computer.



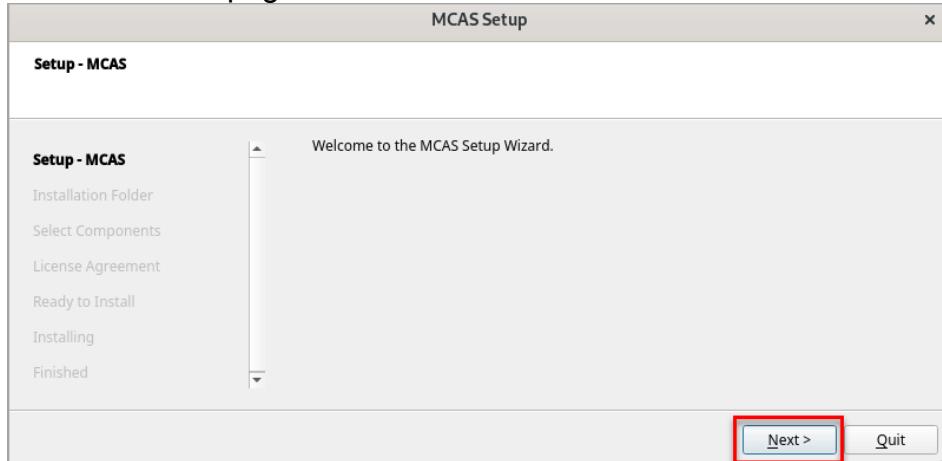
Step 4: Install the downloaded Kiosk

Upon completion of extraction of installation file:

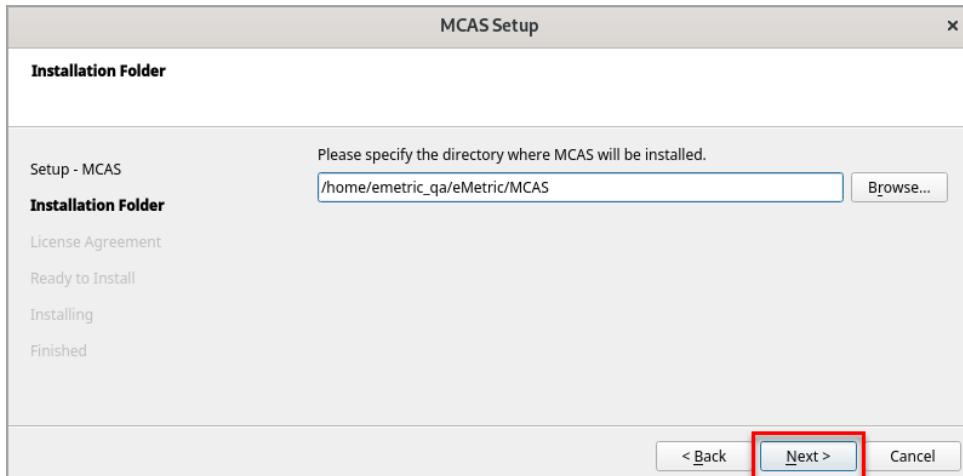
1. Navigate to the kiosk installer file and execute.



2. Read the Welcome page and click **Next** to continue.



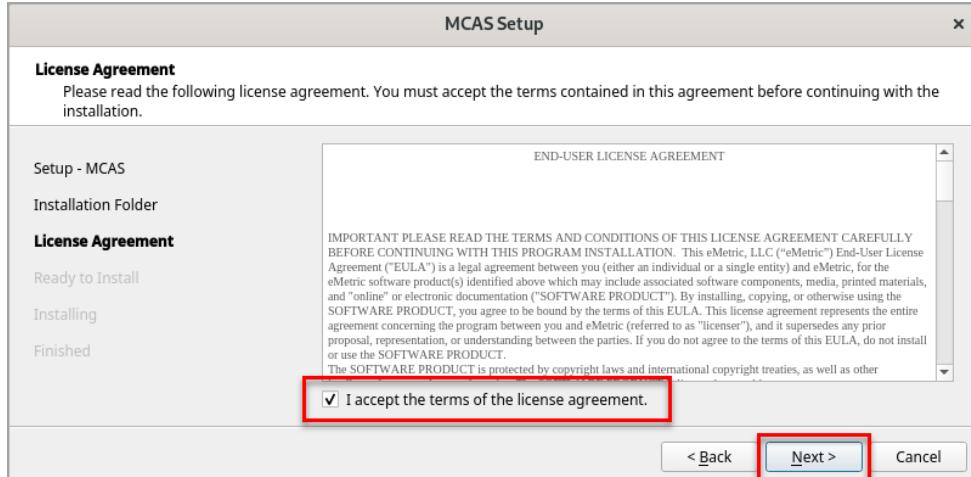
3. Use the default folder location for installation or click **Browse** and type a different installation location in the space provided. Then click **Next** to continue.



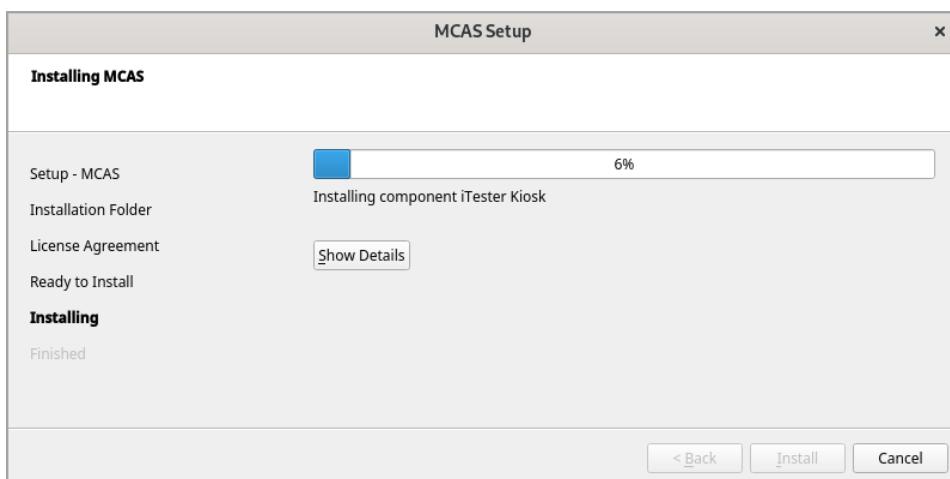
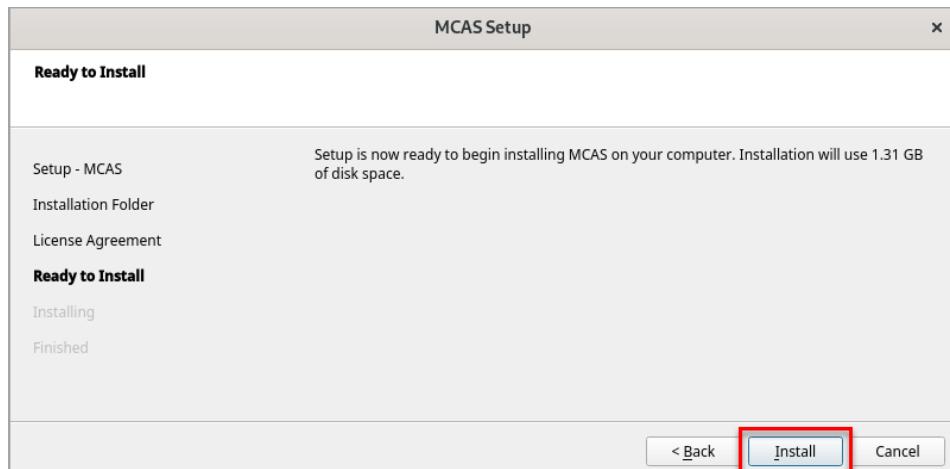
It is recommended that the kiosk is installed on the testing device instead of a network installation to avoid network connection issues (see section III part A, [Network Connectivity](#)).

Important: In the event the student loses internet connectivity during testing, responses will be stored to this location. Additionally, this folder must have the appropriate permissions to allow test takers to write data.

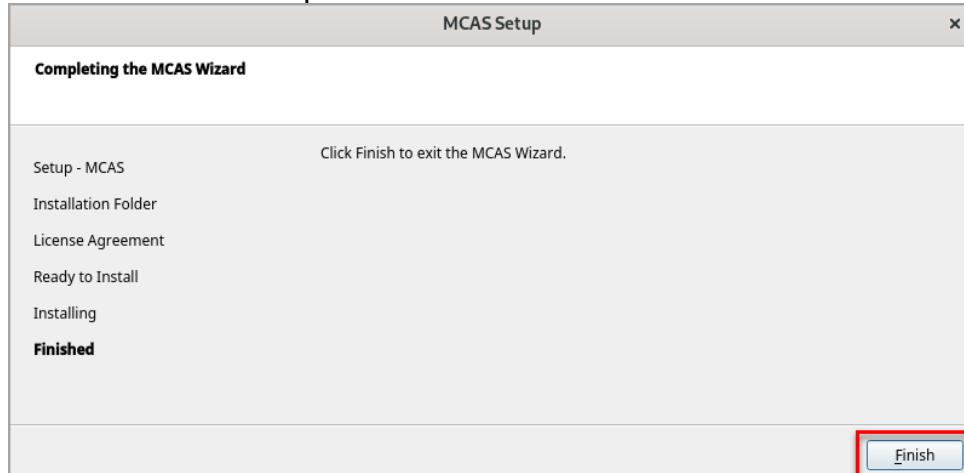
4. Read the License Agreement and check the **I accept the terms of the license agreement** check box. Click **Next** to continue.



5. Click **Install**, a blue bar will be shown to show the progress as the kiosk is installed.



6. Click **Finish** to exit Setup.



7. When you are ready to complete Site Readiness for this configuration, see section V: [Site Readiness Testing and Site Certification](#).

D. MacOS

Step 1: Set up your school technology

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

Step 2: Download the MCAS Student Kiosk

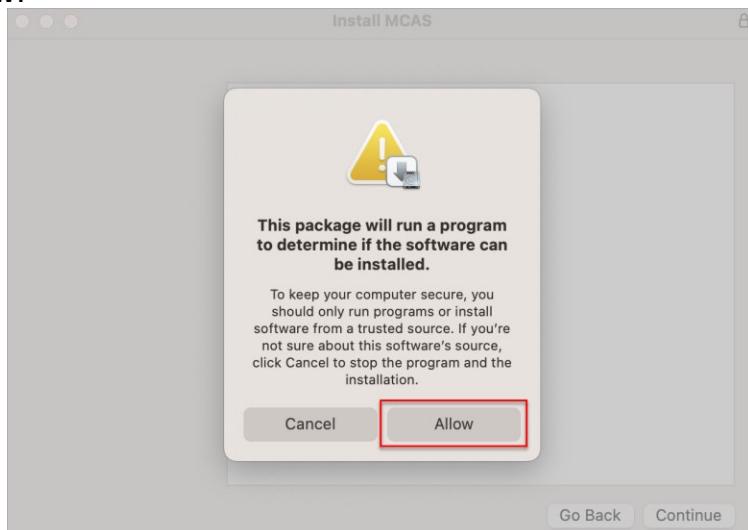
The macOS kiosk is updated each year. If your devices have a previous version of the MCAS Student Kiosk, the kiosk does not need to be uninstalled. The new kiosk can be installed on top of the old version, by following the instructions below.

1. Go to the MCAS Portal and log in with your username and password. If you need assistance logging in to the MCAS Portal, contact your school or district test coordinator.
2. On the portal home page, click **Administration**.
3. On the Administration home page, click **Student Kiosk for Mac**. The kiosk will download to the device.

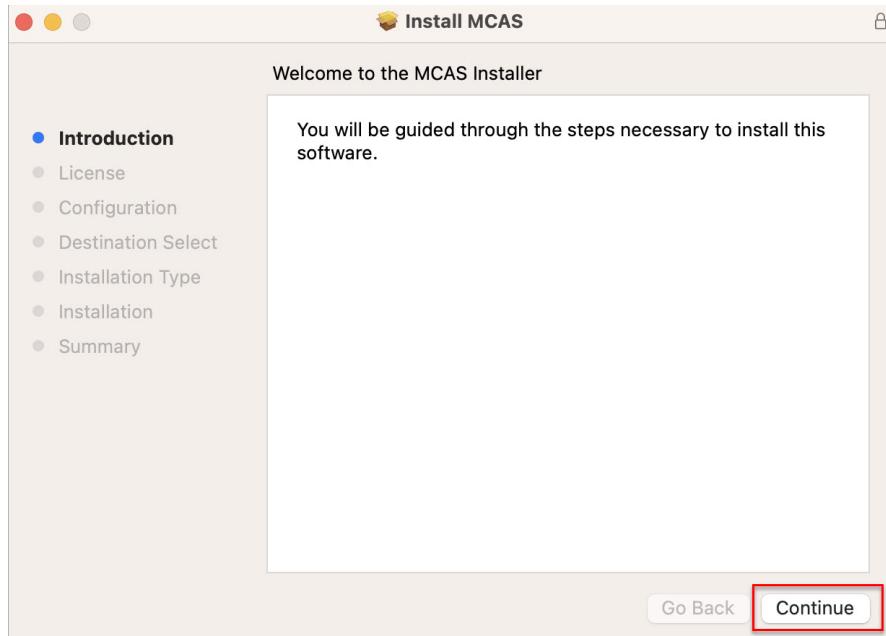
Step 3: Install the downloaded Kiosk

Upon completion of the download process:

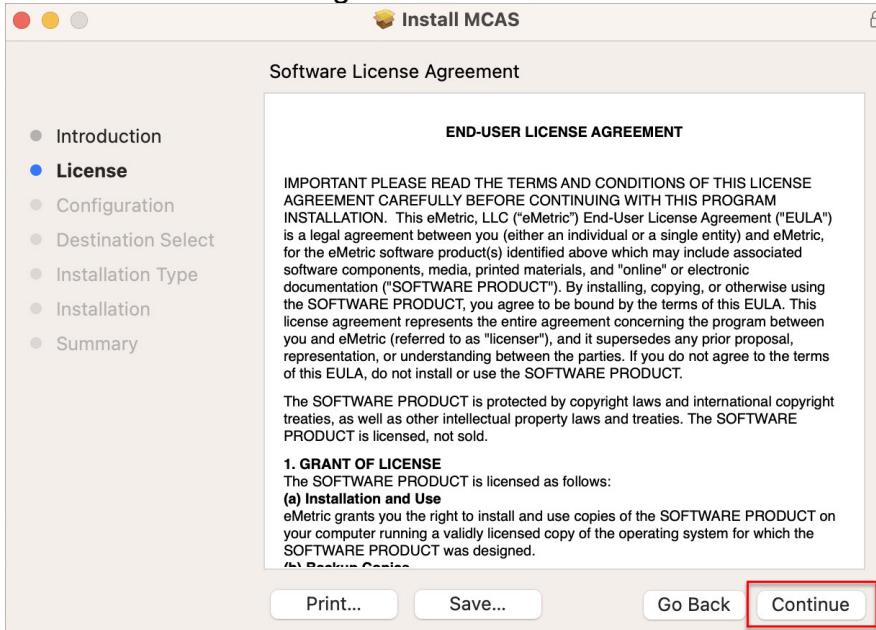
1. Navigate to the file location you specified during the File Save process.
2. The package will run a program to determine if the software can be installed. Click **Allow**.

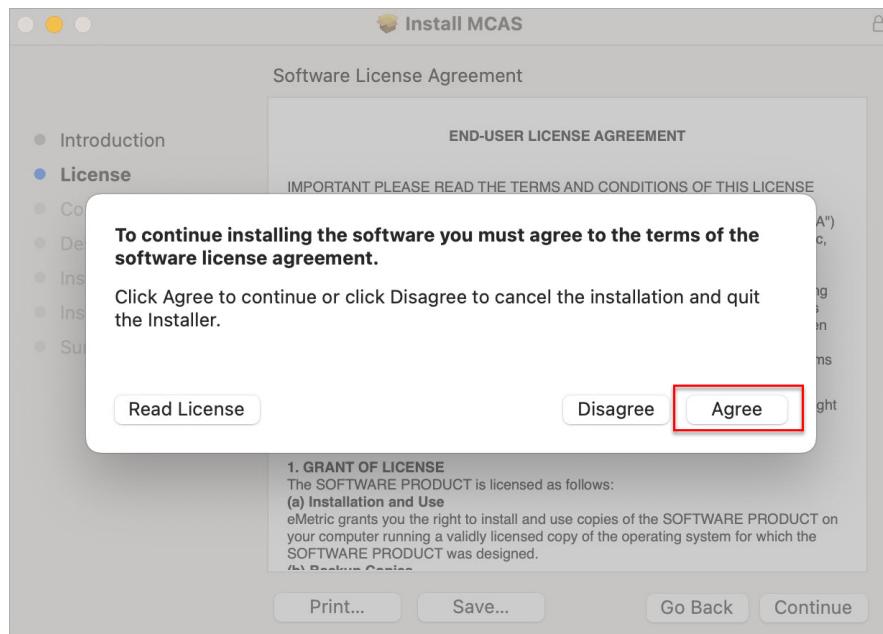


3. Read the instructions and click **Continue**.



4. Read the Software License Agreement and then click **Continue** and then **Agree**.





5. Indicate where you would like to store student responses.

Important: In the event the student loses internet connectivity during testing, responses will be stored to this location. Additionally, this folder must have the appropriate read/write permissions to allow test takers to write data to this location.

Choose from the following two options:

- **User's Home Directory:**

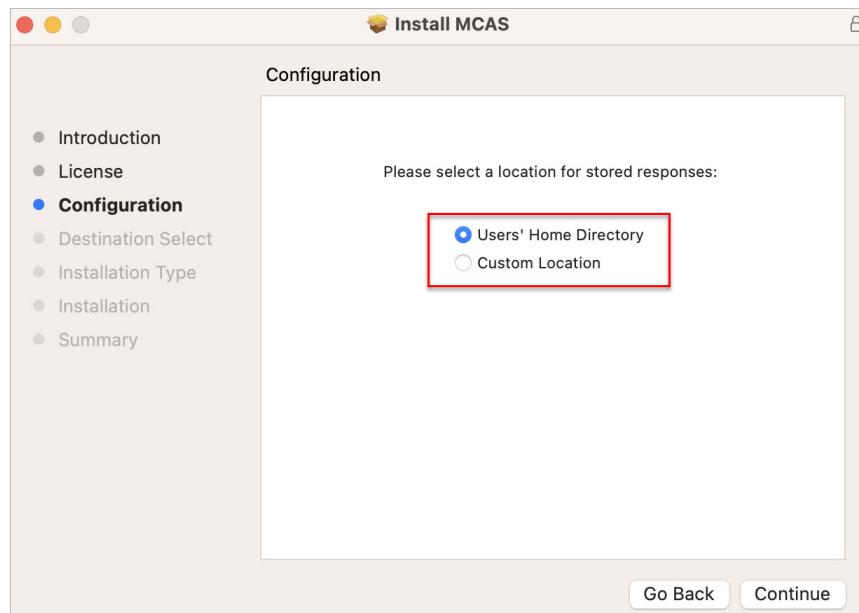
During kiosk installation, if you choose the default option to store the stored response files in the user profile, these files will have names similar to the format below:

**~ /Library/Application
Support/eMetric/MCAS/Storage/iTesterSync_AD849G-DA56-19F3-
73K39823DJS3**

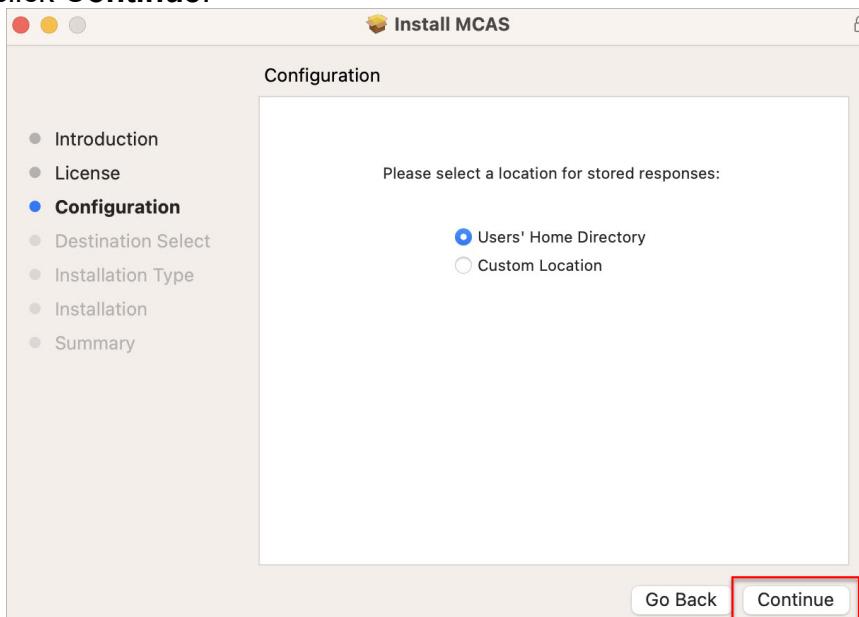
- **Custom location:**

If you select **Save in the following directory**, you must manually enter the alternate path.

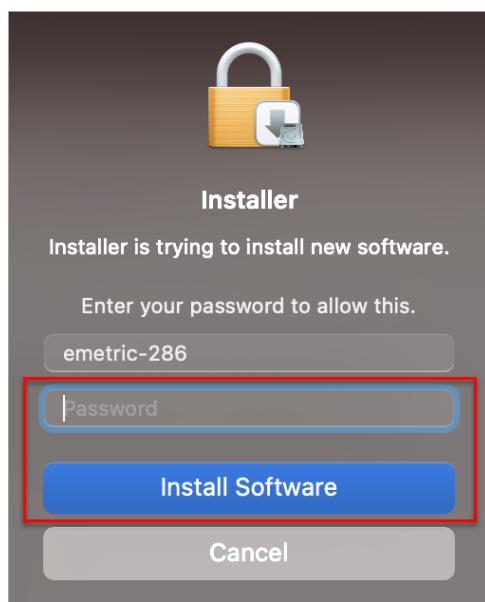
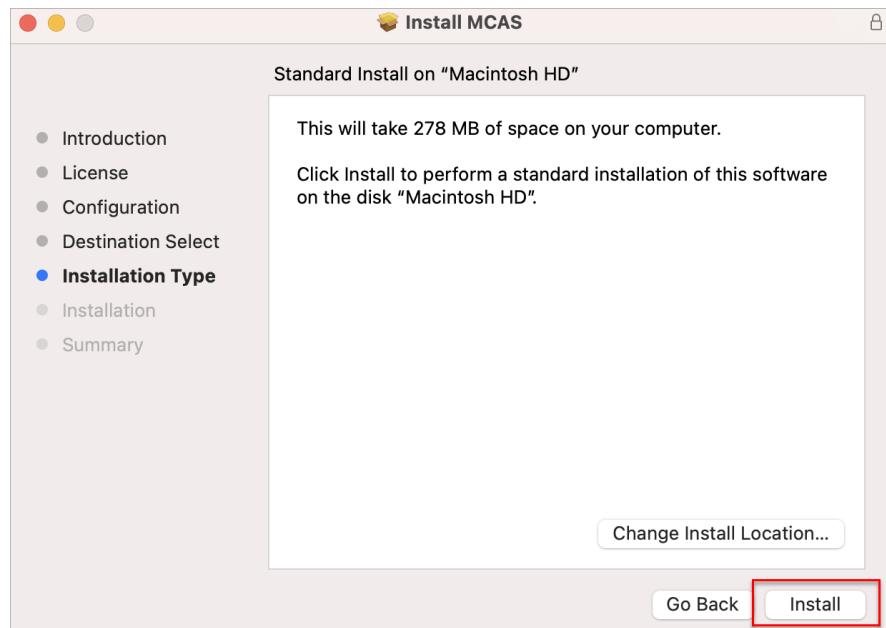
For more information on selecting a location for stored responses or retrieving stored responses, contact the MCAS Service Center at mcas@cognia.org or 800-737-5103.



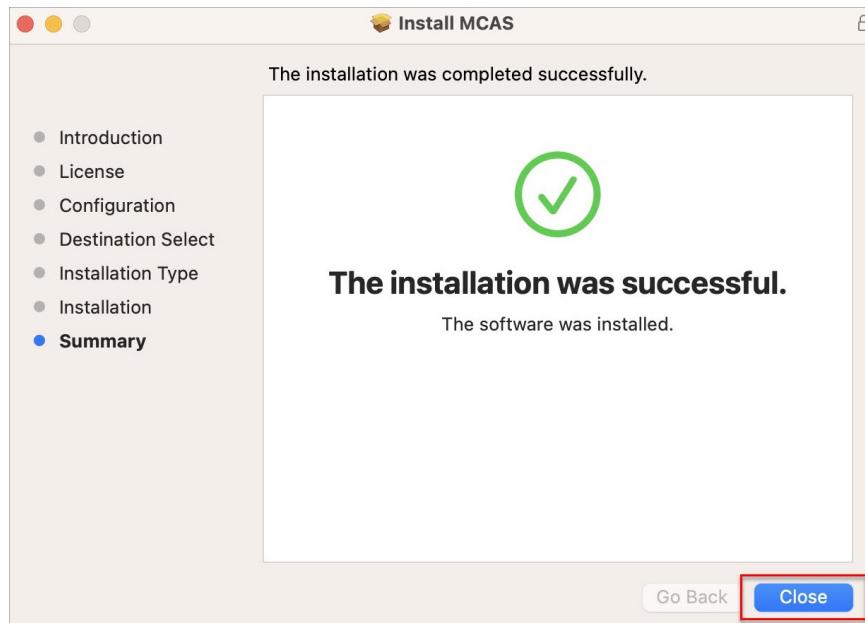
6. Then click **Continue**.



7. Verify installation type and click **Install**. You may be required to enter your admin password.

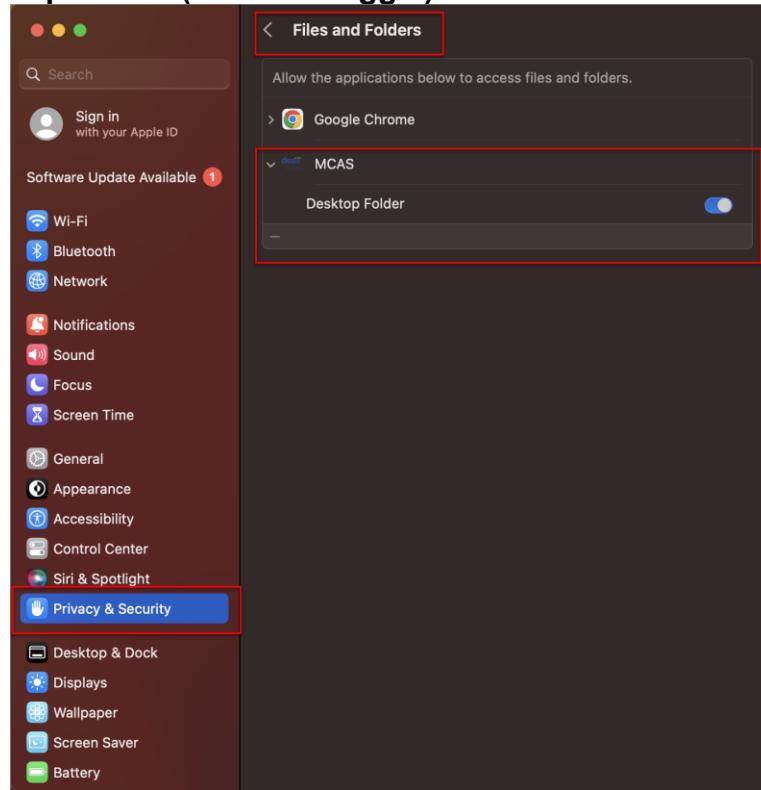


8. When the installation is complete, click **Close**.



9. For enhanced security measures, grant the testing application access to **Desktop Folder**. To grant access follow the path below:

Click **System Settings > Privacy and Security > Files and Folder > MCAS > Desktop Folder (Turn on Toggle)**.



10. If you are using a newer system running MacOS 15.0 or greater with an M2 processor chip you will need to install Rosetta. This can be accomplished by launching the MCAS Student Kiosk for the first time.

After launching the MCAS Student Kiosk you will be prompted:

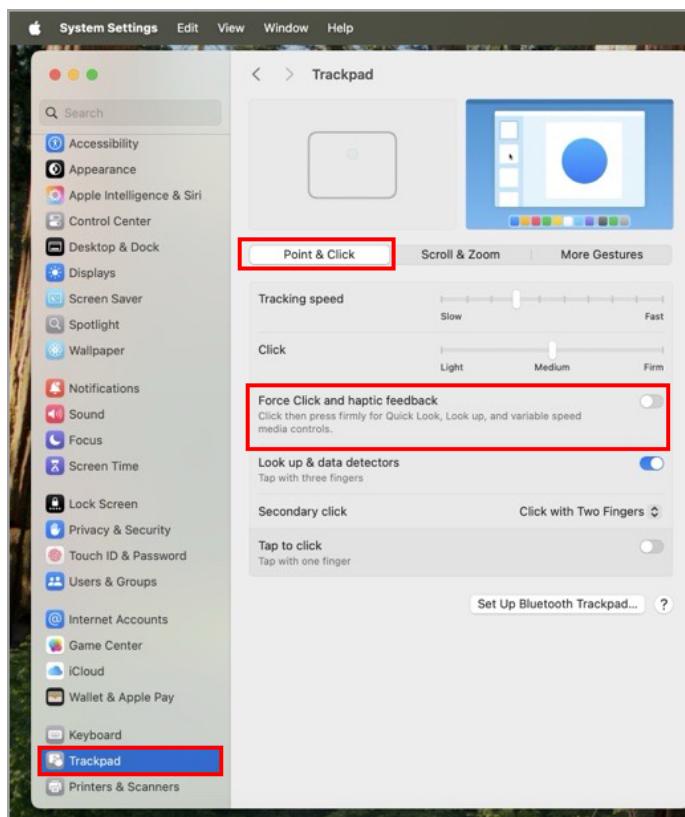
To open “MCAS,” you need to install Rosetta. Do you want to install it now?

Select **Install**.

Note: Rosetta enables Intel-based features to run on Apple silicon Macs. Reopening applications after installation is required to start using Rosetta.

11. Force Click will need to be disabled for MacBooks with Force Touch trackpads. By disabling Force Click, the trackpad will function as normal and will only disable the secondary press features, not disable the trackpad itself. To disable, follow the path below:

Click System Settings > Trackpad > Point & Click > Force Click and haptic feedback (Turn off Toggle).



Note: This setting will only be available if the MacBook has a Force Touch trackpad.

12. When you are ready to complete Site Readiness for this configuration, see section V: [Site Readiness Testing and Site Certification](#).

Note: Students should avoid using **Command (⌘) + Q** to exit the application. Using this shortcut to exit the application can sometimes trigger an unexpected error. This is a system-wide feature and not specific to our application. Instead, always use the in-app Exit button or logout options provided in the interface.

E. Windows OS

Step 1: Set up your school technology

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

Step 2: Download the MCAS Student Kiosk

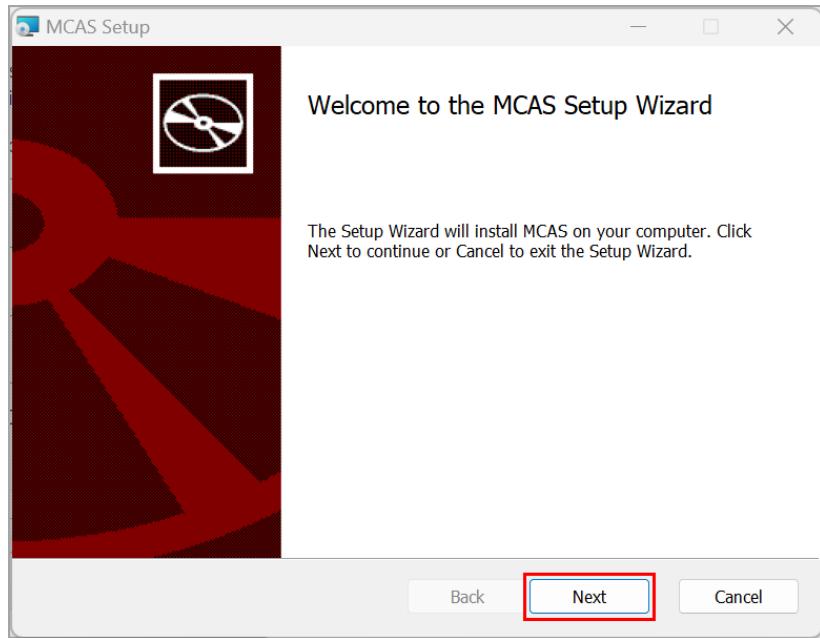
The Windows kiosk is updated each year. If your devices have a previous version of the MCAS Student Kiosk, the kiosk does not need to be uninstalled. The new kiosk can be installed on top of the old version by following the steps below.

1. Go to the [MCAS Portal](#) and log in with your username and password. If you need assistance logging in to the MCAS Portal, contact your school or district test coordinator.
2. On the portal home page, click **Administration**.
3. Click **Student Kiosk for Windows** to download the MCAS Student Kiosk to the device.

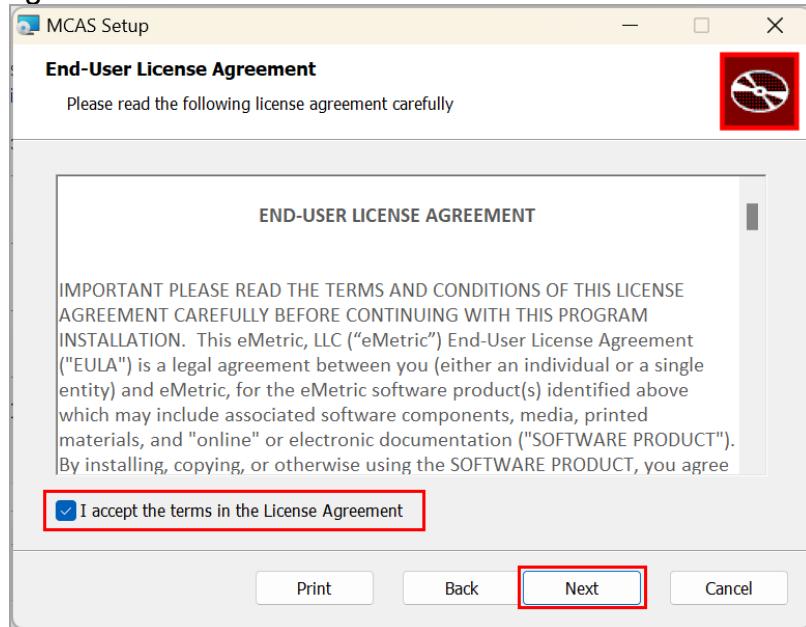
Step 3: Install the Downloaded Kiosk

The MCAS Student Kiosk for Windows can be installed on the school network or on each individual student testing device. It is recommended that the kiosk is installed on each individual device to avoid network connection issues. For installing on each individual student testing device follow the steps below, or follow the steps for [Windows MSI Package Scripted Installation](#), or follow the steps for [Windows MSI Package Installation Via Group Policy](#).

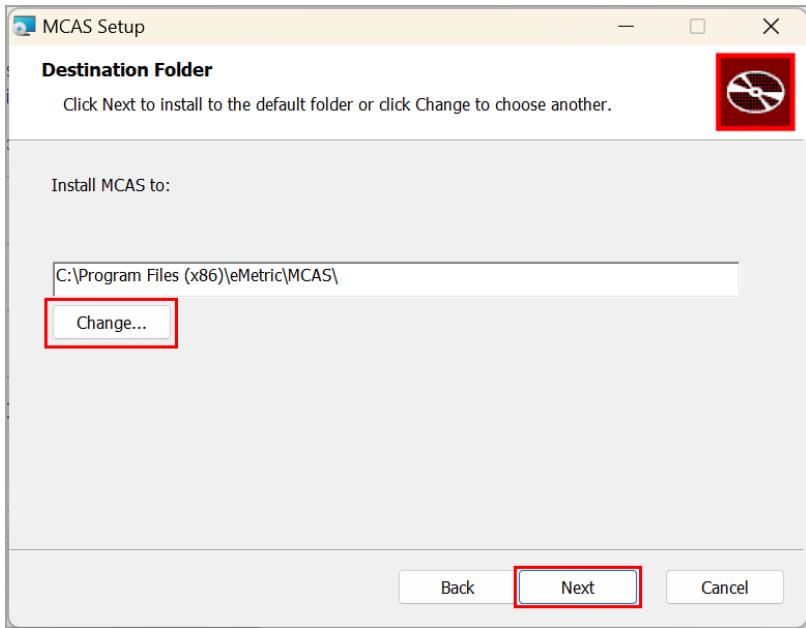
1. Click the installation file in the Downloads folder on the device. The Setup Wizard will open. Read the instructions and then click **Next** to continue.



2. Read the End-User License Agreement and check the I accept the terms in the License Agreement check box. Click **Next** to continue.



3. Use the default folder location for installation or click **Change** and type a different installation location in the space provided. Then click **Next** to continue.

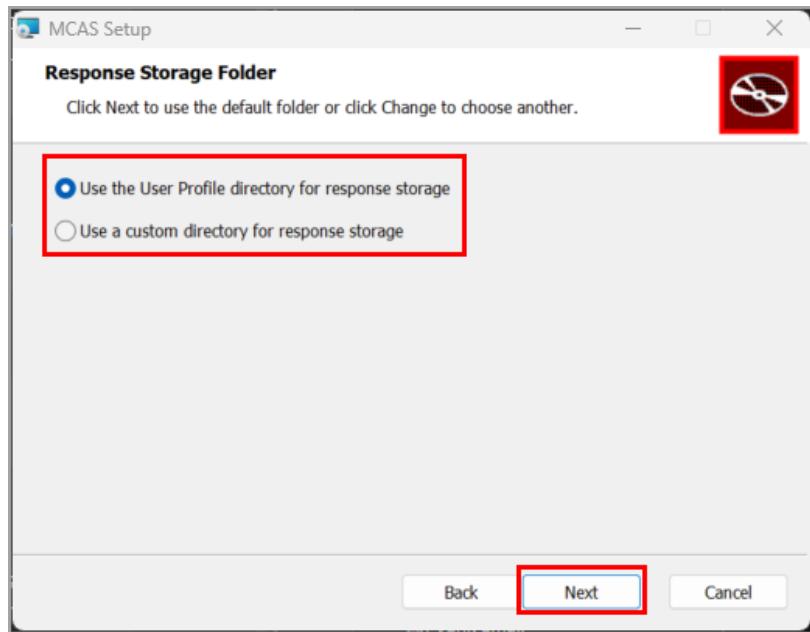


Note: You can choose to install the kiosk in a shared network folder or a local folder on the student testing device. It is recommended that the kiosk is installed on the individual student testing device instead of a network installation to avoid network connection issues (see section III, part A: [Network Connectivity](#)).

4. Select the directory to store student responses.

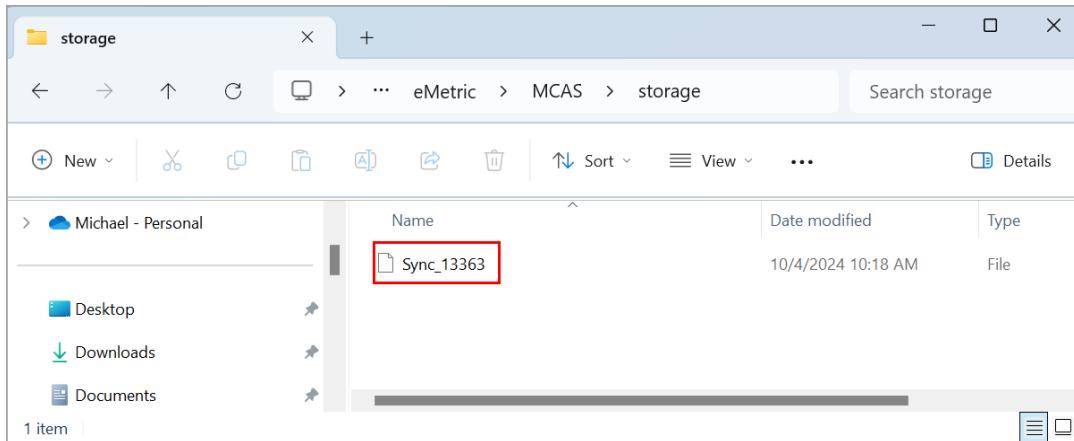
Important: In the event the student loses internet connectivity during testing, responses will be stored to this location. Additionally, this folder must have the appropriate permissions to allow test takers to write data.

Choose from the following two options, then click **Next**.



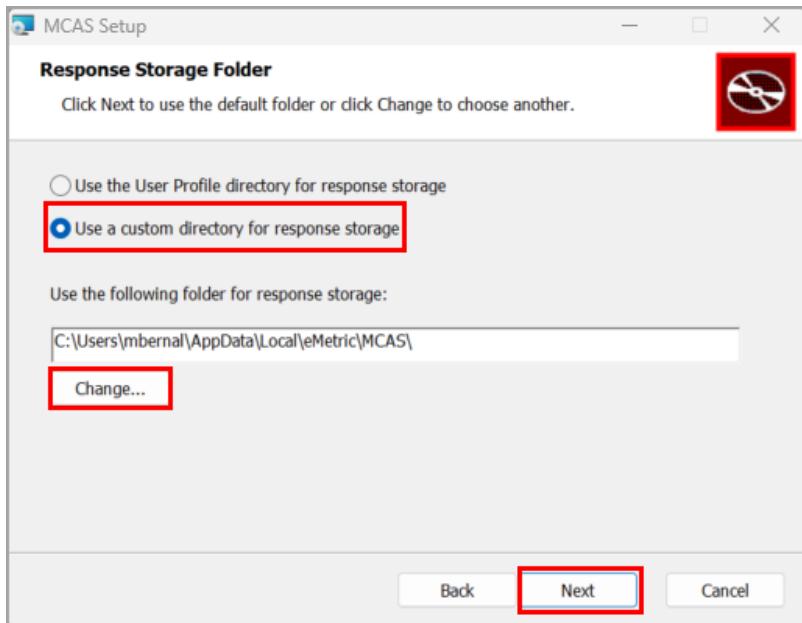
- **Use the User Profile directory for response storage:**

During kiosk installation, if you choose the default option to store the stored response files in the user profile, these files will have names like this format:

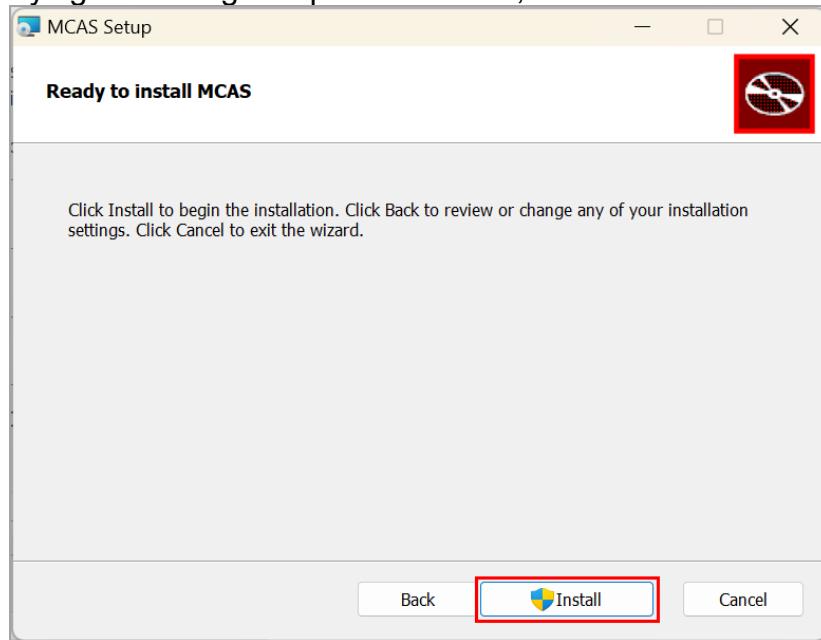


- **Use a custom directory for response storage:**

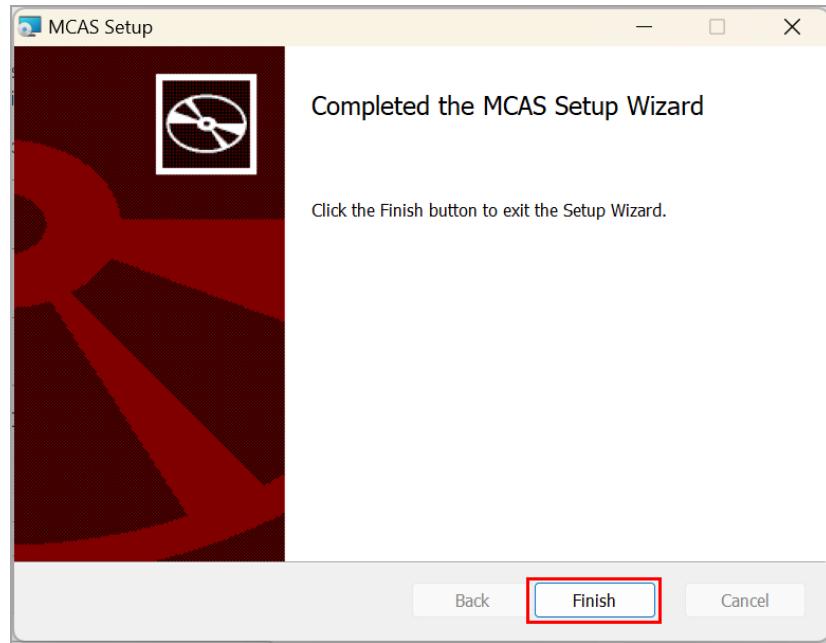
If you select **Save in the following directory**, you must manually enter the alternate path.



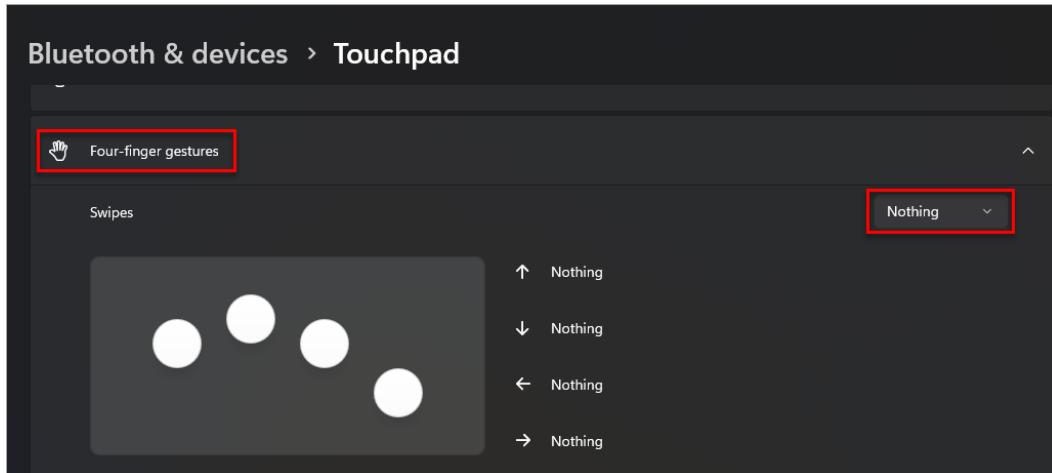
5. After verifying the storage response location, click **Install**.



6. Click **Finish** to complete the installation.



7. For Windows devices with touchpads, Four-finger gestures for swiping will need to be disabled. To disable go to **Settings > Bluetooth & devices > Touchpad**. Then locate Four-finger gestures and expand the section. Next, change the drop-down menu for Swipes to **Nothing**.



8. When you are ready to complete Site Readiness for this configuration, see section V: [Site Readiness Testing and Site Certification](#).

Windows MSI Package Scripted Installation

Network administrators can install the MCAS Student Kiosk via an installation script to be executed by an Admin account on the machine. The script can be written to run without any human interaction (quiet switch) and to install in the default directory (C:\Program Files) or any target directory of choice. Uninstalling the client can also be scripted.

Below are generic scripts that can be used for installation and uninstallation.

Script Examples

- <Source> = Complete path to the MCAS Student Kiosk MSI installation file, including .msi installation file name. Example: C:\Downloads\MCAS.msi
- <Target> = Complete path to the location where kiosk should be installed other than the default location (C:\Program Files). Example: C:\ MCAS\Installation_Dir
- <APPDATALOCATION> = Complete path to the location for storing the cache and encrypted student responses created due to network interruptions. Example: D:\Cache.

Note: Ensure that this location is excluded from system restore software.

Installation Script

```
msiexec /I "<Source>" /quiet INSTALLDIR="<>Target>"  
ITESTERAPPDATALOCATION="<>APPDATALOCATION>" INSTALLLEVEL=2
```

Example: msiexec /I "C:\Downloads\MCAS.msi" /quiet
INSTALLDIR="C:\ MCAS" ITESTERAPPDATALOCATION="D:\Cache"
INSTALLLEVEL=2

Warning: If you do not specify ITESTERAPPDATALOCATION, then the Local Application Data folder located in the User Profile of the actively logged-in user will be used by default. If you do not specify INSTALLLEVEL=2, then the configuration required for setting the <APPDATALOCATION> will not be created.

Uninstallation Script

```
msiexec /X "<Source>" /quiet
```

Example: msiexec /X "C:\Downloads\MCAS.msi" /quiet

Windows MSI Package Installation Via Group Policy

Network administrators can use Microsoft Active Directory Group Policy to distribute the MCAS Student Kiosk MSI package to all client computers.

Follow the step-by-step instructions described in Microsoft's [Knowledge Base article](#).

Note: Default installation locations will be used when using Group Policy to distribute the MCAS Student Kiosk. This option will also not allow systematically specifying a network location for caching and storing encrypted student responses created due to network interruptions. The local Application Data folder located in the User Profile of the actively logged-in user will be used by default.

Windows Network Kiosk Installation

To install the MCAS Student Kiosk on a school network:

1. Complete the local kiosk installation listed above on the machine that will host the application.

2. Configure the stored response location to network share or leave as default during installation.
3. On the student testing devices, create a shortcut to the application on the network. The shortcut created should point to MCAS.exe.
4. Ensure that users have read/write/modify access to stored response directory configured in Step 3.

V. Site Readiness Testing and Site Certification

A. Purpose

The MCAS Portal includes a Site Readiness tool for schools and districts to assess their readiness for online testing via the MCAS Student Kiosk and to identify any potential technology-related issues before testing begins to ensure a smooth testing experience. The Site Readiness tool is used to verify that testing devices meet the minimum requirements and have been properly configured. DESE will follow up with schools that do not complete Site Readiness.

The Site Readiness tool includes the **System Set-Up Test** and the **Student Interface Test**.

- The **System Set-Up Test** tests bandwidth, connectivity, screen resolution, and the text-to-speech function.
- The **Student Interface Test** provides sample test questions to determine whether the device is capable of correctly displaying and navigating test content in the MCAS Student Kiosk. The Student Interface Test also allows technology coordinators to test the student tools, including the Line Reader, Text Highlighter, and Notepad, to confirm they are functioning properly.

To administer the Site Readiness test, the technology coordinator launches the MCAS Student Kiosk on each device configuration (i.e., device type and operating system) being used for testing at that site and then uses the Site Readiness login for the assigned school to run the test. For example, if you will be testing on Windows 11 and different versions of supported ChromeOS, then we recommend testing 2 to 3 devices on Windows 11 and 2 to 3 devices on each ChromeOS version that will be used. Then, the technology coordinator certifies the site (school) in the MCAS Portal to indicate to the school and district test coordinators that the site's technology is ready for testing.

Note: The Site Readiness tool must be conducted using the secure MCAS Student Kiosk. The test does not need to be conducted on the browsers used for practice tests.

B. Using the Site Readiness Tool

It is crucial that the Site Readiness tool is run on **every** device type or device configuration that will be used for testing. The results for each device tested will be captured and displayed on the Site Readiness Details page within the MCAS Portal.

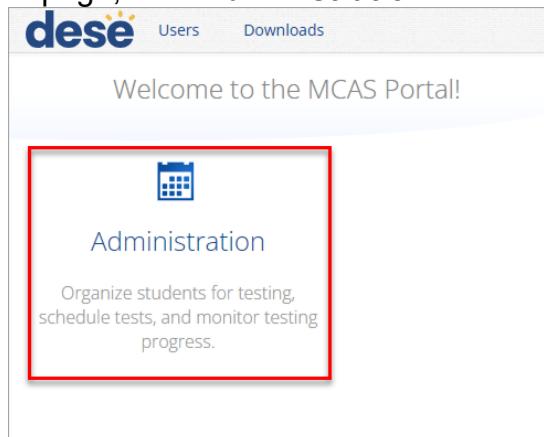
Note: Starting with iPadOS 13, Apple made a change with the user agent for iPadOS. Due to this change, iPads do not populate in the Site Readiness tab of the MCAS Portal. If you are an iPad school or district, we recommend running the Site Readiness tool on a few iPads to ensure they pass the System Set-Up and Student Interface tests

without issues and recommend an alternative method of communicating this information to test coordinators.

After reviewing the [Technology Guidelines](#) and installing the MCAS Student Kiosk, follow the instructions below.

Step 1: Locate the Site Readiness credentials in the MCAS Portal

1. Log in to the [MCAS Portal](#) with your username and password.
2. On the Portal home page, click **Administration**.



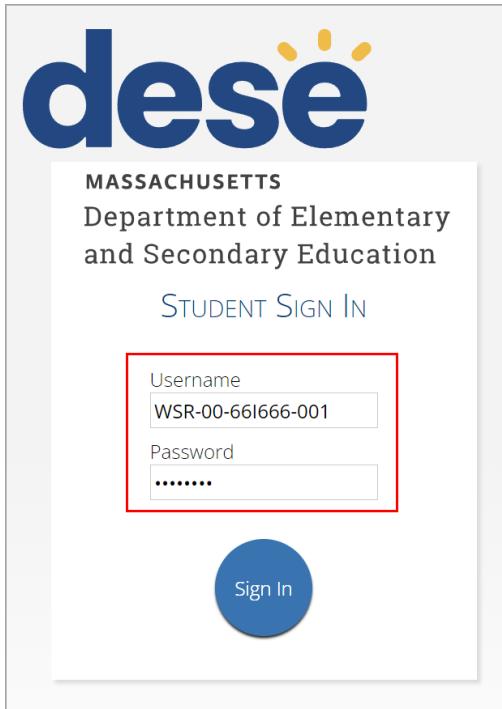
3. The Site Readiness account information appears at the bottom of the Administration home page.

A screenshot of the MCAS Administration home page. At the top, there is a message: 'Welcome to the MCAS Portal. This site provides access to MCAS test administration and reporting tasks. If you need assistance with this site, please contact the MCAS Service Center: mcas@cognia.org (email), 800-737-5103 (phone), 888-222-1671 (TTY), or live chat by clicking [here](#).'. Below this, there is a table for 'Technology Coordinators' with download links for various devices. At the bottom, there are fields for 'Proctor password for' and 'Site Readiness login for'. The 'Site Readiness login for' field and its associated password information are highlighted with a red box.

4. Make a note of the username and password for the school, which you will use to log in to the MCAS Student Kiosk.

Step 2: Conduct Site Readiness on every Device Configuration

1. Launch the MCAS Student Kiosk on the device.
2. Log in to the MCAS Student Kiosk with the Site Readiness username and password provided for the school (shown above).



Important Note: Use the Site Readiness login credentials exclusively for the school only, and do not use the credentials for any other purposes. Do not use the Site Readiness credentials for any other school.

On Windows and ChromeOS devices, users will see a System Set-Up link next to the exit button on the MCAS Student Kiosk sign in screen. This link **should not be used** for Site Readiness testing. Users must use the Site Readiness login credentials to complete Site Readiness, as described above.

3. Under **System Set-Up Test**, click **Check System Set-Up** to begin the test.

The screenshot shows the SiteReadiness User interface. At the top, it says "Hello, SiteReadiness User". Below that, it displays student information: State Student ID (3768-39894), Date of Birth (3/2/1998), and Grade (1). Below the information, it says "The following tests have been scheduled for you:" and lists "System Set-Up Test" and "Student Interface Test". The "Check System Set-Up" button is highlighted with a red box.

The screen resolution, host URL (mcas.cognia.org), and operating system for the device are listed at the top of the System Set-Up Test page. The System Set-Up Test consists of four parts: the Connection Capacity Test, the Connectivity Check, the Screen resolution check, and the Text-to-Speech check. The results of each test appear as soon as it is completed.

The screenshot shows the System Set-Up Test results page. At the top, it says "System Set-Up Test". Below that, it shows "Screen Resolution: 1920x1080", "Host:mcas.cognia.org", and "Operating System:window 15.0.0". The results are listed in a numbered list:

- ① **Connection Capacity Test Results: 913 Simultaneous Test Downloads**
Your download speed is **60.89 Mbps**. Based upon the current calculated download speed between your testing device and the data center, a maximum of **913** students may simultaneously log-in and download the test. If you plan to test more than **913** students during the same period of time, divide them into groups of no more than **913** students and stagger the groups' test log-in by 1-2 minutes.
- ② **Connectivity Check passed.**
All connectivity checks passed.
- ③ **Screen resolution passed.**
Current screen resolution is at least 1024x768.
- ④ **Text-to-Speech check has begun.**
Test Text-to-Speech

Does Text-to-Speech work?

Yes **No**

4. The **Connection Capacity Test** evaluates your site's capacity for simultaneous test downloads. It provides the current download speed between the testing device and the testing servers (data center), and, based on that speed, it provides the maximum number of students that may simultaneously log in and download a test session.

If you plan to test more students concurrently than the recommended number of simultaneous test downloads, it is recommended that you divide the students into groups no greater than the number of recommended simultaneous test downloads and stagger each group's test log in by 1–2 minutes. This will reduce the likelihood of interruption during sign in.

5. The **Connectivity Check** is designed to ensure the testing device has access to both the kiosk's local storage folder, where student responses will be saved if the test device loses internet connectivity, and the testing servers.

- If the Connectivity Check fails with the following message:

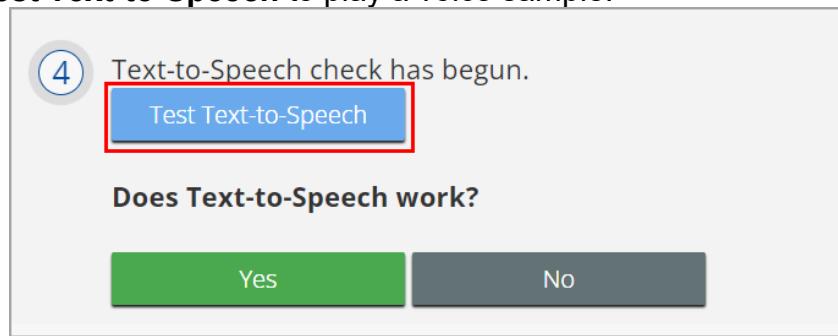
“The connectivity check failed. Please check your read and write permissions to the storage folders and try again or contact Support for further assistance. Error Code: 6004 – StorageWriteFail”

This means that the MCAS Student Kiosk does not have the proper permissions for the storage folder. The kiosk requires read, write, and modify permissions on Windows and Read & Write on Mac.

- If the test fails for any reason other than “Error Code:6004 - StorageWriteFail,” contact the MCAS Service Center.

6. The **Screen resolution test** will ensure that the testing device meets the required screen size and resolution for an optimal testing experience. If this test fails, adjust the screen resolution of the device.

7. The **Text-to-Speech test** will ensure that this accommodation is operating as expected for students who have this accommodation. In the Text-to-Speech field, click **Test Text-to-Speech** to play a voice sample.



- If you can hear the voice sample, click **Yes**.
- If you cannot hear the voice sample, click **No**, and fix your audio connection. You will need to verify that there is a voice package installed on your machine, that there is an audio playback device connected to the testing device (e.g., internal speakers, external speakers, headphones),

the volume is not muted and is audible, and that the desired audio playback device is set as the default device.

8. When you are done, click **Return** to return to the Site Readiness page.

System Set-Up Test

Screen Resolution: 1920x1080 Host:mcas.cognia.org Operating System:window 15.0.0

① **Connection Capacity Test Results: 978 Simultaneous Test Downloads**
Your download speed is **65.26 Mbps.** ⓘ
Based upon the current calculated download speed between your testing device and the data center, a maximum of **978** students may simultaneously log-in and download the test. If you plan to test more than **978** students during the same period of time, divide them into groups of no more than **978** students and stagger the groups' test log-in by 1-2 minutes.

② **Connectivity Check passed.**
All connectivity checks passed.

③ **Screen resolution passed.**
Current screen resolution is at least 1024x768.

④ **Text-to-Speech check passed.**

Test Finished.
Return

You've completed the System Set-Up Test. Please click the Return button to go back to the main selection page.
Take the Student Interface Test in order to complete site readiness testing on this device.

- If all the system checks are successful, you are ready to begin the next Site Readiness test.
- If one or more system checks fail, adjust your configuration as needed and re-run the System Set-Up test.

9. When the System Set-Up test is completed, click the blue **Check Student Interface** button.

Not SiteReadiness User? [Exit](#)

Hello, SiteReadiness User

3768-39894 State Student ID	3/2/1998 Date of Birth	1 Grade
--------------------------------	---------------------------	------------

The following tests have been scheduled for you:

System Set-Up Test

[Check System Set-Up](#)

Student Interface Test

[Check Student Interface](#)

Note: If you run the **Check Student Interface** test on a Chromebook and you receive the error message **“This test must be taken with the kiosk or mobile app”**, this is an indication that the MCAS web app and extension are not installed correctly in Google Admin console. Reference the installation steps in part IV section A: ChromeOS Application Installation, particularly step 23 on page 21.

10. Read the instructions on the page and then click **Continue**.

Student Interface Test

[Check Student Interface](#) [Directions](#)

This is the site readiness student interface review test. Please interact with the screen the way a student would. Contact the MCAS Resource Center with any questions or concerns.

[Continue](#)

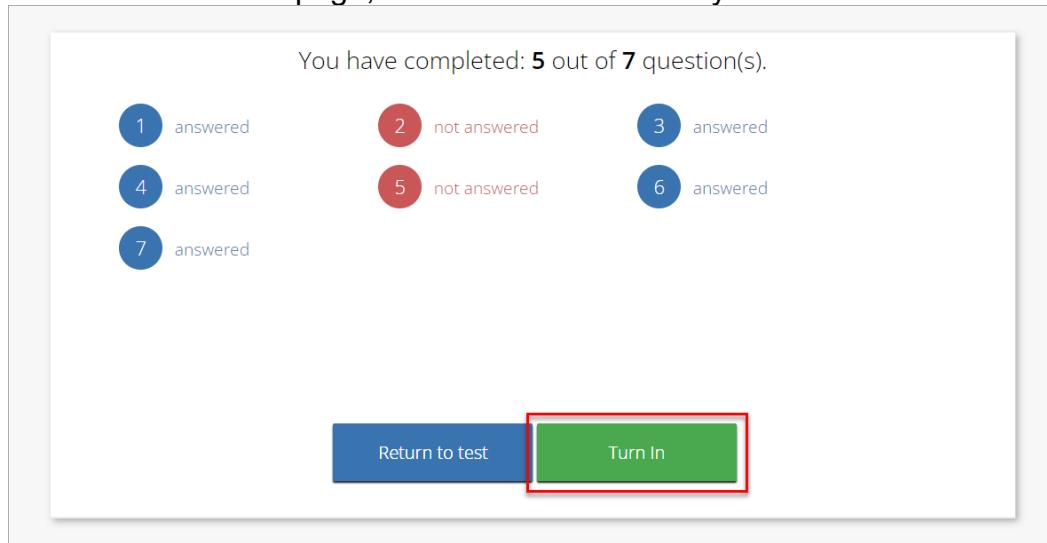
[Exit](#)

11. Confirm that you can effectively respond to a few questions. Click on and try out a few student tools, such as the Notepad and Line Reader, to make sure you can use them. To activate a tool, click on the tool in the tool bar and use it in the test

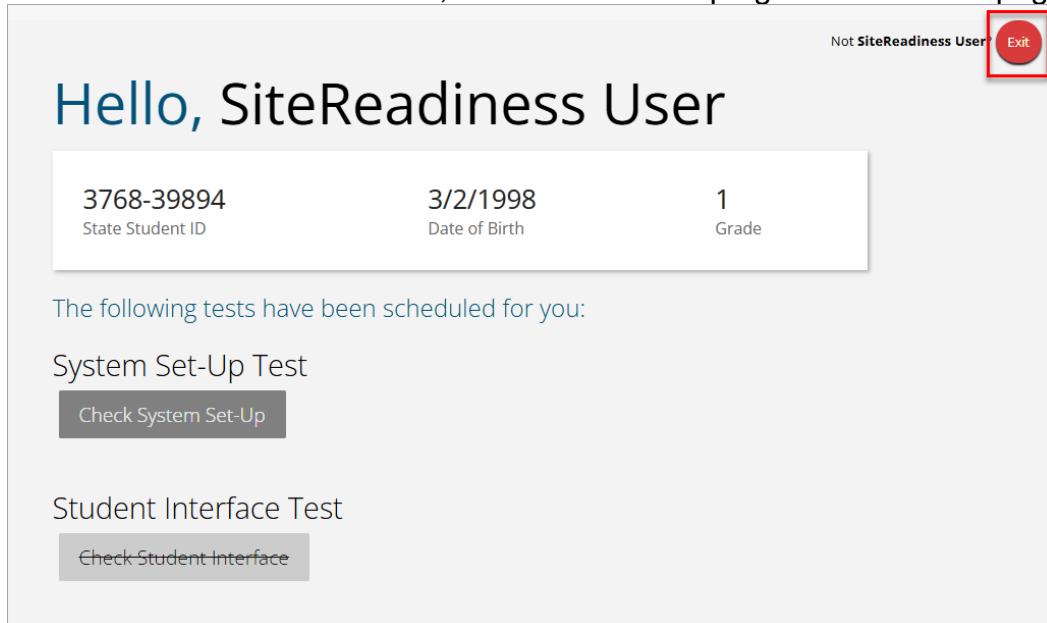
interface. On the constructed response question, ensure you can type in the response box.

Note: Certain tools, accessibility features, and accommodations will be available in the Student Kiosk for operational testing but will not be available in Site Readiness. See Appendix A for additional information.

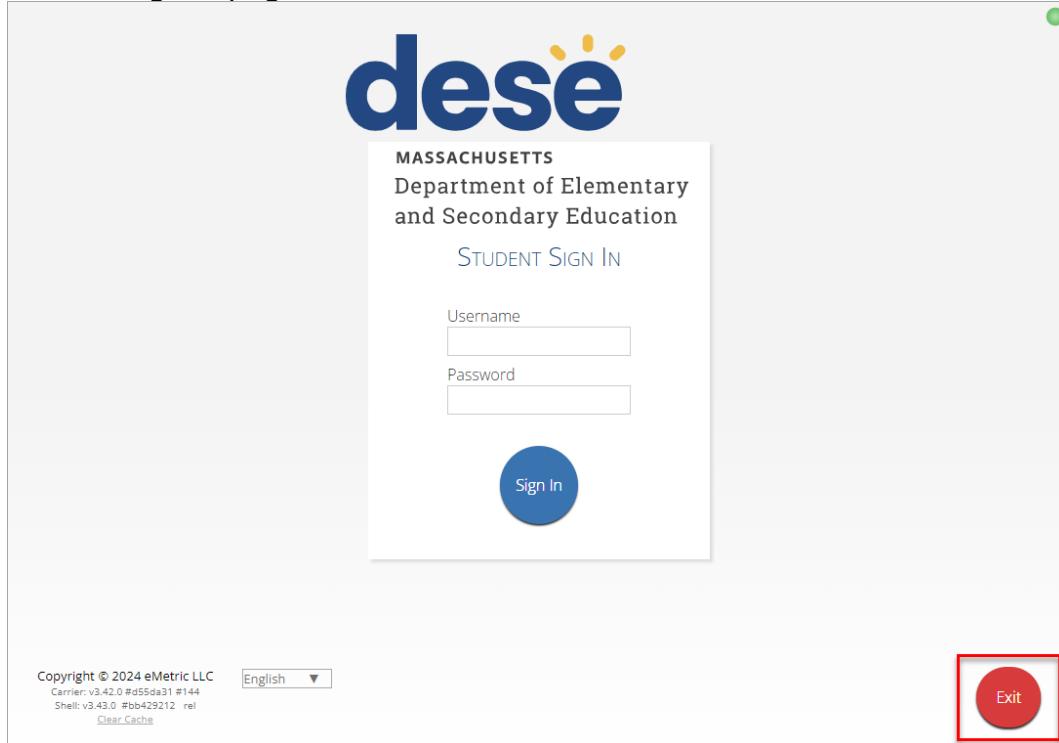
12. On the last test question page, click **Finish**.
13. On the Test Review page, click **Turn In** to submit your test.



14. To confirm, click **Turn In** again. You should return to the Site Readiness page where the test session is grayed out.
15. To exit the Site Readiness tool, click **Exit** in the top right corner of the page.



16. To close the MCAS Student Kiosk, click **Exit** at the bottom right corner of the student sign-in page.



If you have questions about the Site Readiness tool, contact the MCAS Service Center.

C. Site Certification

After all device configurations for your school have successfully completed Site Readiness, the technology coordinator must certify the site for testing.

1. Log in to the MCAS Portal with your username and password.
2. Click **Administration**.
3. Click **Site Readiness** at the top of the page.



4. On the Site Readiness page, locate the school to be certified, and then click **View Details**.

Site Readiness in Cyber Valley Sch1-001			
<input type="button" value="Cyber Valley Sch1-001 (Cyber Valley)"/>			
School	Number of Devices Tested	Date and Time	Certified By
Cyber Valley Sch1-001	1		<input type="button" value="View Details"/>

5. On the Site Readiness Details page, verify that all the devices or device configurations for this location have successfully run the Site Readiness tool and meet the technology requirements.
6. Click **Certify Site Readiness** and click **Yes** to confirm in the pop-up window.

Site Readiness Details			
<input type="button" value="Cyber Falls Sch1-001 (Cyber Falls)"/>			
Device Name	os	Screen Size	Date and Time
emetric-244.local	mac 14.6.0	1440x900	9/24/2024 2:36:50 PM
emetric-244.local	mac 14.6.0	1440x900	9/26/2024 5:25:38 PM
eMetric-250	window 10.0.0	1536x864	9/24/2024 1:43:05 PM
eMetric-250	window 10.0.0	1536x802	9/27/2024 7:10:36 PM
eMetrics-MacBook-Air.local	mac 13.0.0	1440x900	9/24/2024 1:47:01 PM

Showing 1 - 5 of 5

Site Certification

I certify that Site Readiness tests have been performed on the above machines and any noted issues have been resolved.

*Date and time is in Eastern Standard Time.

7. The **Site Certification** section updates with the date and time when the site was certified and the username of the user who certified the site for testing.

Site Readiness in Cyber Valley Sch1-001			
<input type="button" value="Cyber Valley Sch1-001 (Cyber Valley)"/>			
School	Number of Devices Tested	Date and Time	Certified By
Cyber Valley Sch1-001	1	9/25/2024 4:18:39 PM	Demo_DTC

Showing 1 - 1 of 1

*Date and time is in Eastern Standard Time.

District and school test coordinators can also view when the site was certified and who certified the site on the Site Readiness tab without having to click into the Site Readiness Details.

Site Readiness in Cyber Valley				
<input type="button" value="Cyber Valley"/>				
School 	Number of Devices Tested 	Date and Time 	Certified By 	
Cyber Valley Sch1-001	13	10/4/2024 6:02:49 PM	Demo_DTC	View Details
Cyber Valley Sch2-002	1			View Details
Cyber Valley Sch4-004	1			View Details
Cyber Valley Sch8-008	1			View Details

Showing 1 - 4 of 4

*Date and time is in Eastern Standard Time.

This certification indicates to the district or school test coordinator that the technology coordinator has tested the devices at the site and ensured they are operating as expected and meet the technology requirements, acknowledging that the site is ready for testing. Once complete, technology coordinators should inform their school test coordinators.

Appendix A: Student Tools, Accessibility Features, and Accommodations Unavailable for Site Readiness

The following tools, accessibility features, and accommodations will be available in the MCAS Student Kiosk for operational testing but will not be available in Site Readiness.

- Ruler
- ASL video edition for grade 10 math and June high school science (A6.2)
- Calculator (SA4)
- Compatible assistive technology

Appendix B: MCAS Student Kiosk Error Message Guidance for Technology Staff

This appendix lists potential error messages that could occur when testing with the MCAS Student Kiosk. With each error message, guidance and troubleshooting steps are provided.

Internet Connectivity

If internet connection is lost during MCAS testing, students are able to continue testing in the MCAS Student Kiosk, but may receive one of the following error messages, as described below. Technology coordinators should complete the steps listed to ensure that all student responses are submitted for scoring. Please contact the MCAS Service Center at 800-737-5103 with any questions.

Error Message	What does it mean?	Steps for Technology Staff
1. Please raise your hand and notify your proctor: Your response is not able to be stored. To avoid losing your response, your test cannot be continued until connection to the storage location is reestablished.	The access to the storage location was lost after the student began testing due to loss of network connectivity.	<ol style="list-style-type: none">1. Click Retry Now.2. If the connection to the storage location is reestablished, the MCAS Student Kiosk will return to the screen the student was on.3. If after several attempts to retry, the connection is not restored, contact the MCAS Service Center to confirm the student responses were received up to when the student received this error.4. The Service Center will confirm whether all responses have been captured and whether the student can move to a new device.5. Once it has been confirmed that all responses have been captured up to the error message, the student can then be moved to a different device if needed.6. The student will then be able to log in and continue testing where they left off.
2. Please raise your hand and notify your proctor. A connection to the network	Internet connectivity was lost after the student began testing and was	<ol style="list-style-type: none">1. Do not move the student to a different device.2. The test administrator should click Send Responses.

Error Message	What does it mean?	Steps for Technology Staff
could not be established. Your test has been saved offline.	not restored by the time the student clicked Turn in Test . The student's responses will be saved to the local folder, which should have been configured when the MCAS Student Kiosk was initially installed.	<ol style="list-style-type: none"> The page will refresh after about 10 seconds. If the connection is restored, the responses will be uploaded, and test will be submitted. If the connection is not restored, the Send Responses button will reappear. The test administrator then must enter the proctor password, acknowledging the message to ensure the kiosk will be relaunched. Once the internet connection is restored, relaunch the kiosk on the device that the student tested on. When launched, the responses that were stored on the local device will be uploaded for scoring. If the student responses are captured, their status will update from In Progress to Finished in the MCAS Portal. If there is a delay in the receipt of student responses, or if the student logs into a different device prior to the original device uploading the responses, the test status will remain In Progress.
3. The offline student responses on this machine could not be processed. Please contact Support to continue. (ErrorCode:1003)	This could be due to a drop in internet while uploading stored responses. The kiosk will not be able to launch until this is resolved.	<ol style="list-style-type: none"> Click Refresh. This will attempt to upload the responses again. If successful, the student will be brought to the login page. If unsuccessful, the page will not change. Schools have the option to export responses. Cognia strongly recommends this process be completed by the technology coordinator or school test coordinator. Click Export Responses. The user will need to save the responses locally. When storing responses locally on the device, it is very important to note the exact location where the file is being stored. Once exported, the coordinator should exit the kiosk, log in to the Chromebook and open File explorer. Contact the MCAS Service Center for next steps on what to do with these exported files to ensure the responses are captured for scoring.

Error Message	What does it mean?	Steps for Technology Staff
		<ol style="list-style-type: none"> 6. After Cognia confirms that the responses have been captured, delete the responses saved locally.

Launching the Kiosk

The error messages described below could occur when launching the MCAS Student Kiosk.

Error Message	What does it mean?	Steps for Technology Staff
1. No internet connection found.	There is no internet connection on the device and the kiosk cannot launch.	<ol style="list-style-type: none"> 1. Click Try again. 2. If the internet connection has been reestablished, the MCAS Student Kiosk will be launched. 3. If you receive the error message again, establish an internet connection and click Try again to launch the MCAS Student Kiosk. 4. If you are unable to establish an internet connection, click Exit to exit the application. 5. Next step would be to establish an internet connection before launching the kiosk again.
2. Please exit the kiosk and install the latest version.	The kiosk being launched on the testing device is an older version.	<ol style="list-style-type: none"> 1. Select Exit, to close out of the kiosk. 2. If the device is Windows, macOS or Linux, download and install the latest version of the MCAS Student Kiosk available in the MCAS Portal or the MCAS Resource Center. For iPadOS verify the iTester app is up to date and for ChromeOS verify that the MCAS App is up to date.
3. A new version of the app is available. Please update.	There was an update to the kiosk shell that was released while the kiosk was left open or already launched on the student testing device.	<ol style="list-style-type: none"> 1. Click Update. The kiosk will update to the latest version, and your student will be able to log in.

During a Test

The error messages describe below could occur while your student is logged into a test. These error messages are in addition to the internet connectivity error messages described earlier in the document.

Error Message	What does it mean?	Steps for Technology Staff
1. This test must be taken with the kiosk or mobile app.	The student is trying to access a secure test using the browser or trying to access a secure test on a Chromebook where the PWA is not launching in kiosk mode, meaning the PWA for MCAS has not been installed correctly.	<ol style="list-style-type: none">1. Click Exit. This will exit the student out of the student interface.2. If the student was in a browser trying to access a secure test, have them log in to the test using the MCAS Student Kiosk.3. If the student was using the MCAS PWA on a Chromebook to access a secure test, then the technology coordinator will need to verify the PWA was installed correctly. Reference the installation steps in Part IV Section A: ChromeOS Application Installation, particularly step 23 on page 21.4. Once the installation has been corrected, have the student log back in to their test.
2. Please raise your hand; your test session has timed out.	The student timed out of their test session due to inactivity, meaning they have been inactive in the test for 60 minutes.	<ol style="list-style-type: none">1. Click Exit. This will exit the student out of the kiosk.2. When the student is ready to continue testing, they will log back into the kiosk and select the session they wish to continue and they will be prompted for a proctor password. Proctor will enter the password and the student will resume testing where they left off. Any questions that the student responded to prior to their session timing out will be locked.
3. There is a problem because somebody else has logged into your test session. You have been logged out for security reasons.	The student has logged in to their test session on two separate devices or someone else has logged into the MCAS Student Kiosk with the same credentials.	<ol style="list-style-type: none">1. Click Exit. This will exit the student out of the kiosk.2. Have the student log back into their test, verify the student's test resumes where they left off and have them continue testing.3. If the student's test does not resume where they left off, contact the MCAS Service Center.

Screen Freezing Issues

The following screen freezing issues could occur while your student is logged into a test using the MCAS Student Kiosk. The issues described below will not show an error message in the kiosk.

Error	Steps for Technology Staff
1. The MCAS Student Kiosk becomes unresponsive, frozen, or stops working as expected. For example, a student cannot drag a response to a goal box.	1. Click Pause/Exit and then select Exit Test . 2. From the MCAS Student Kiosk login screen, click Clear Cache in the lower right-hand corner. 3. You will be asked “Are you sure?”. Click Yes , and the kiosk will close and then launch. 4. Have the student log back into their test, verify that the kiosk is responding, and then have the student resume testing.
2. The student cannot type in the constructed response box. The response box is frozen or non-responsive.	1. Check if the constructed response box has a character or word counter and verify if the student has reached the maximum characters or words allowed. If they have, they will not be able to type in the constructed response box. 2. If there is a limit and they have not reached it, click Pause/Exit and then select Exit Test . 3. From the MCAS Student Kiosk login screen, click Clear Cache in the lower right-hand corner. 4. You will be asked “Are you sure?”. Click Yes , and the kiosk will close and then launch. 5. Have the student log back into their test, verify that they can type in the constructed response box and have the student resume testing. If the response box is still not responsive contact the MCAS Service Center.