Florida
Statewide Assessments

Configurations, Troubleshooting, and Advanced Secure Browser Installation Guide for macOS and iPadOS

2021–2022

Updated 2/1/2022

FSA
ELA & Mathematics
Assessments

NGSSS
Science & Social Studies
Assessments

Table of Contents

Configurations, Troubleshooting, and Secure Browser Installation for macOS and iPadOS

This document contains instructions for installing the Secure Profile and the Secure Browser for macOS, installing the SecureTestBrowser App for iPadOS, as well as configurations, troubleshooting, and advanced Secure Browser installation instructions for your network and macOS and iPadOS devices.

It is recommended that before a macOS machine is configured for testing, administrators create a backup of the device profile's preferences and settings as the Secure Profile will override these settings. Once the device is no longer being used for testing, the Secure Profile can be removed, and the original settings can be reapplied. Alternatively, you can create a testing profile to be used only for Florida Statewide Assessments.

How to Configure macOS Workstations for Online Testing

Mac workstations running macOS 10.13-10.15 require the following configurations be performed before testing begins:

- Download and install the Secure Profile
- Download and install the Secure Browser
- Disable third-party app updates
- Disable fast user switching

Instructions for these configurations appear below.

About Assessment Mode

A feature in macOS 11.4 and iPadOS called Assessment Mode (AM) (formerly known as Automatic Assessment Configuration (AAC)) works with CAI's Secure Browser to lock down Mac workstations and iPads for online testing. AM requires no setup. Once the Secure Browser is launched on a Mac workstation running macOS 11.4 or an iPad, AM kicks in automatically. Workstations running macOS 11.4 or higher require no further configuration prior to testing.

For more information about AM, including a list of features it disables, please visit https://support.apple.com/en-us/HT204775.

Installing the Secure Profile for macOS

The Secure Profile is a configuration profile that can be used to configure Mac workstations running macOS 10.13-10.15 for online testing. Please note that the Secure Profile was updated in Spring 2021. If you have an older version installed, you must update to the most recent

version available on the [*Secure Browsers*](#) page when upgrading to Secure Browser 12.5 or Secure Browser 14. If the Secure Profile was installed manually, remove the Secure Profile from *System Preferences > Profiles* before running the new Secure Profile.

First, download the Secure Profile from the bottom of the [Secure Browsers](#) page, install it, and restart your computer. The Secure Profile can also be installed on multiple devices all at once using any commercially available mobile device management (MDM) application you already use to manage your devices. After installing the profile, the computer should be restarted so that all settings can take effect.

The Secure Profile automates manual steps that take place to secure the device after installing the Secure Browser. The profile disables the hot keys for enabling Mission Control, Spaces, Screenshots, and Dictation and the trackpad gestures for accessing Lookup, App Exposé, Launchpad, and Show Desktop. It sets function keys to standard functions for all users of the Mac to which it is deployed and disables Voice Control and the menu pop-up that appears when triple-tapping the power button on Touch Bar-enabled devices. It also prevents the device from receiving files via AirDrop and the ability to have your Mac identify items under the pointer.

Second, download the Secure Browser from the top of the [Secure Browsers](#) page and install it using the instructions below.

Installing Secure Browser for macOS

This procedure installs Secure Browser on desktop and laptop computers running macOS. The steps in this procedure may vary depending on your version of macOS and your web browser.

1. Remove any previous versions of the secure browser by dragging its folder to the Trash.
2. Open the **Downloads** folder and double-click FLSecureBrowser-OSX.dmg to display its contents.
3. Drag the **FLSecureBrowser** icon to the desktop.
4. Double-click the **FLSecureBrowser** icon on the desktop to launch the secure browser. (You must launch the secure browser to complete the installation.) The secure browser opens displaying the student login screen. The browser fills the entire screen and hides the dock.
5. To exit the browser, click **X** in the upper-right corner of the screen.
6. Ensure all background jobs, such as virus scans or software updates, are scheduled outside of test windows. For example, if your testing takes place between 8:00 a.m. and 3:00 p.m., schedule background jobs outside of these hours.

Installing the SecureTestBrowser App for iPadOS

This section contains instructions for downloading and installing SecureTestBrowser and selecting your state and assessment program. The process for installing the mobile secure browser is the same as for any iPadOS application.

1. Click **Download** on the App Store. (You can also search for SecureTestBrowser in the App Store to find the secure browser app.) The download page opens.

2. Tap **GET**. The iPad downloads and installs the Secure Browser, and the icon changes to **OPEN**.

3. After installation, a SecureTestBrowser icon appears on the iPad's home screen.

4. Open **SecureTestBrowser**.

5. Configure your test administration by selecting your state and assessment program from the dropdown lists and tapping OK.

Additional Instructions for Installing the Secure Browser for macOS

This section contains additional installation instructions for installing the Secure Browser for macOS.

Cloning the Secure Browser Installation to Other macOS Machines

Depending on your networking and permissions, it may be faster to install the Secure Browser onto a single macOS machine, take an image of the disk, and copy the image to other macOS machines. The Secure Profile will also need to be installed on each machine as outlined in the Installing the Secure Profile for macOS section.

To clone the Secure Browser installation to other computers:

1. On the computer from where you will clone the installation, do the following:

   a. Install the Secure Browser following the directions above. Be sure to run and then close the Secure Browser after the installation.

   b. In Finder, display the **Library** folder.

   c. Open the **Application Support** folder.

   d. Delete the folder containing the Secure Browser.

   e. Delete the **Mozilla** folder.

2. Create a shell script that creates a new Secure Browser profile when a user logs in. The basic command to create a profile is

   ```
   <install_directory>/Contents/MacOS/FLSecureBrowser -CreateProfile -profile_name
   ```
   where
   ```
   profile_name
   ```
   is unique among all testing computers.

3. Clone the macOS image.

4. Deploy the image to the target macOS machines.

Uninstalling the Secure Browser on macOS

To uninstall an macOS Secure Browser, drag its folder to the Trash.

Additional Configurations for macOS

This section contains additional configurations for macOS. Note that the macOS Secure Profile automatically disables the following:

- Hot keys for enabling Mission Control, Spaces, Screenshots, and Dictation
- Trackpad gestures for Lookup, App Exposé, Launchpad, and Show Desktop

It also sets function keys to standard functions for all users of the Mac to which it is deployed, disables Voice Control, and disables the menu pop-up that appears when triple-tapping the power button on Touch Bar-enabled devices. The Profile does not disable the following:

- Updates to third-party apps
- Updates to iTunes
- Fast user switching

Disabling Updates to Third-Party Apps

Updates to third-party apps may include components that compromise the testing environment. On workstations running macOS 10.13-10.15, these should be disabled. This section describes how to disable updates to third-party apps. This configuration applies to all supported versions of macOS.

The following instructions are based on macOS 10.14; similar instructions apply for other supported versions of macOS.

To disable updates to third-party apps:

1. Log in to the student's account.

2. Open **App Store**. The *App Store* window opens.

3. From the menu bar, select **App Store**.

4. Select **Preferences**. The *Preferences* window opens.
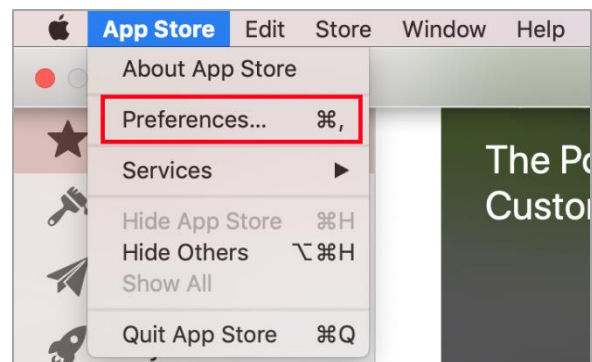
5. Clear the *Automatic Updates* checkbox.

6. Close the *Preferences* and *App Store* windows.
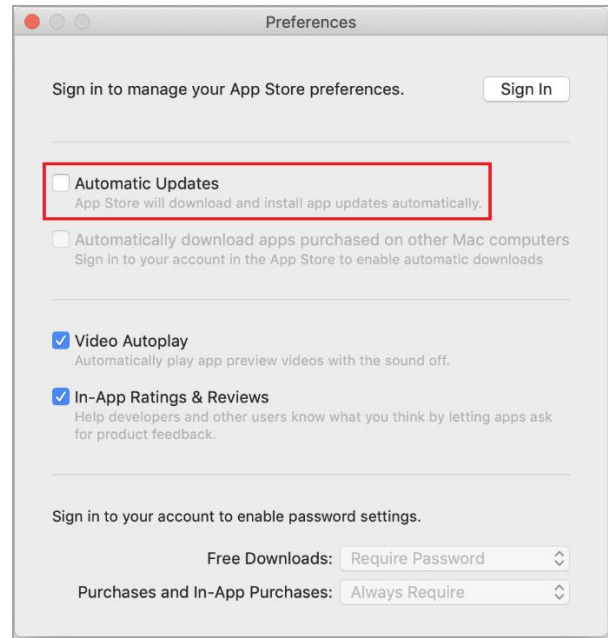
Disabling Fast User Switching

Fast User Switching is a feature in macOS that allows for more than one user to be logged in at the same time. If Fast User Switching is not disabled and students try to access it during a test, the Secure Browser will pause the test. Fast User Switching should be disabled on all workstations running macOS 10.13-10.15. The following instructions describe how to disable Fast User Switching. This configuration applies to all supported versions of macOS.

1. Choose Apple Menu > **System Preferences**.

2. Select **Users & Groups**. The *Users & Groups* window opens.

3. If the padlock in the lower left corner is locked, click it, and authenticate with admin credentials.
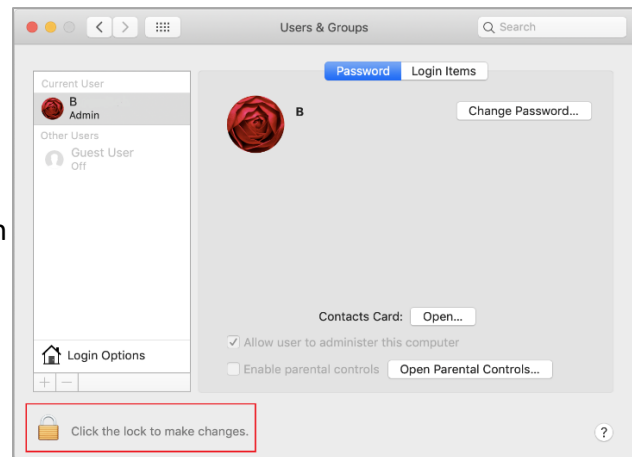
4. Select **Login Options**. The *Login Options* window opens.

5. Clear the **Show fast user switching menu as**… checkbox.

6. Close the **User & Groups** window.
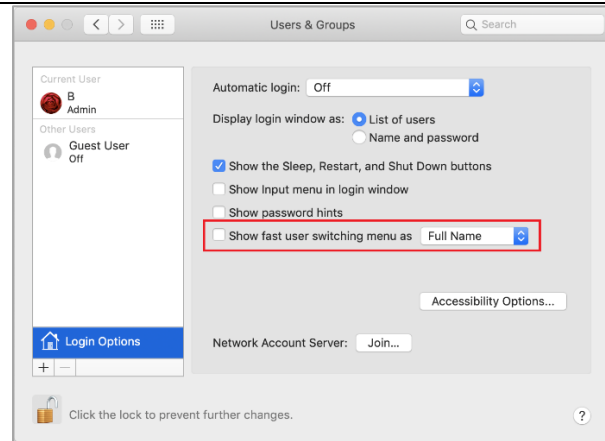
Fast User Switching now disabled. Icon should no longer appear in menu bar.

Installing Rosetta 2

If you are running the Secure Browser on Apple silicon devices, you must first install Rosetta 2.

Rosetta 2 may already be installed on your Apple silicon device if you needed it to run another Intel-based application. If it is not already installed, a prompt to install it will appear the first time you launch the Secure Browser.

Rosetta 2 can also be deployed to multiple devices at once through scripting or mobile device management (MDM).

For more information about Rosetta 2, including instructions to install it, please see https://support.apple.com/en-us/HT211861.

Additional Configurations for iPadOS

This section contains additional configurations for iPadOS.

> **Note:** As a reminder, please refer to the About Assessment Mode section for more information on the Assessment Mode (AM) feature.

Managing iPadOS Automatic Updates

CAI recommends disabling iPadOS automatic updates, so your iPads are not updated to a version that is not yet supported. To disable automatic updates on individual iPads, see Apple's instructions at https://support.apple.com/en-us/HT202180#automatic. If you use MDM software, you can use to disable updates on multiple iPads at once.

Using MDM to Disable Classroom Observation

You can use the following key value to disable access to the Classroom observation feature on student devices. This key is defined as part of the Restrictions profile payload and is documented in the Configuration Profile Reference.

allowScreenShot	Boolean	If set to false, users can't save a screenshot of the display and are prevented from capturing a screen recording; it also prevents the Classroom app from observing remote screens. Defaults to true.

Disabling Voice Control for iPads

iPads running any supported version of iPadOS have access to a feature called Voice Control that is not automatically disabled by Assessment Mode (AM). Voice Control allows users to control an iPad using voice commands. If this feature is enabled on iPads that are used for testing, students may be able to access prohibited features and apps, such as web browsers, during a test. Voice Control is disabled by default on iPads. If it has never been enabled on an iPad, you have nothing to do. If it has been enabled, you must disable it before a student takes a test as it is not automatically disabled by the Secure Profile. Voice Control can be disabled through accessibility settings. The following instructions describe how to disable Voice Control.

1. Select **Settings**.
2. Select **Accessibility**.
3. Select **Voice Control**.

Accessibility Settings – Voice Control
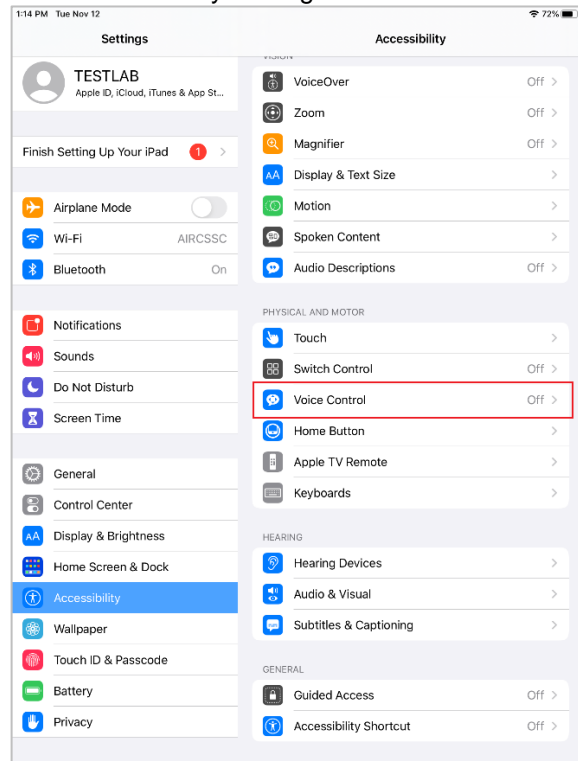
4. Toggle the **Voice Control** switch to the left to disable Voice Control.
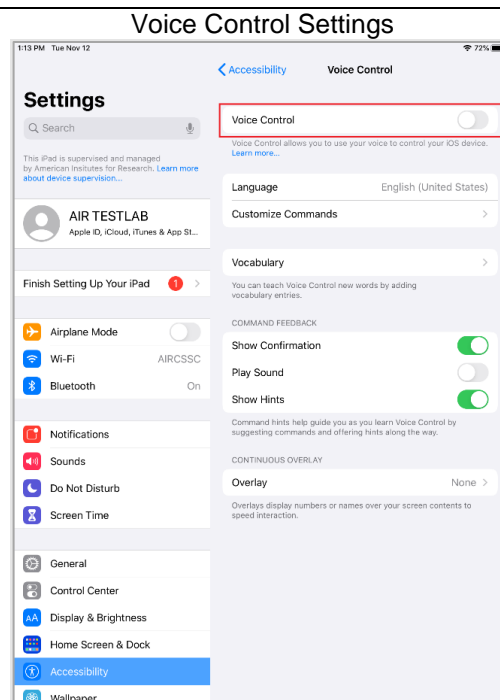
Voice Control Settings

Disabling VoiceOver for iPads

iPads running any supported version of iPadOS have access to a feature called VoiceOver that is not automatically disabled by Assessment Mode (AM). VoiceOver is a gesture-based screen reader that allows users to receive audible descriptions of what is on the screen of their iPad. VoiceOver also changes touchscreen gestures to have different effects and adds additional gestures that allow users to move around the screen and control their iPads. If VoiceOver is not disabled on iPads, students may be able to access unwanted apps during a test. VoiceOver can be disabled through accessibility settings. The following instructions describe how to disable VoiceOver.
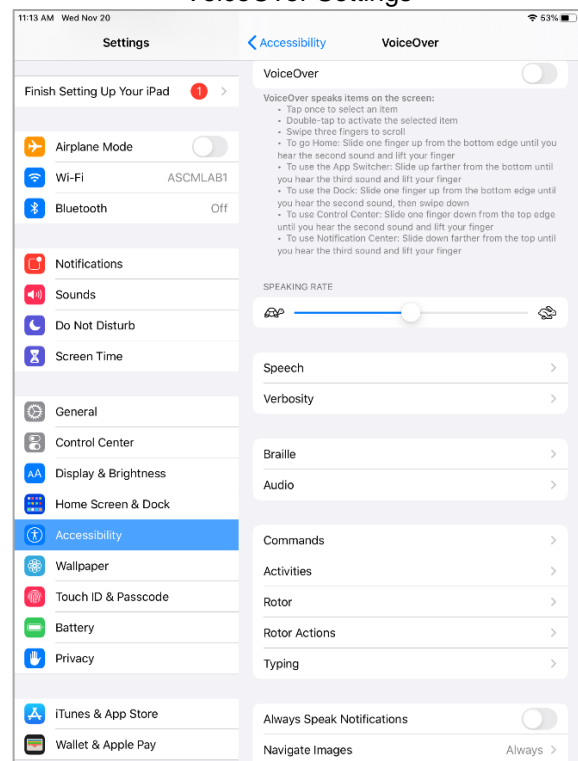
1. Select **Settings**.

2. Select **Accessibility**.

3. Select **VoiceOver**.

Accessibility Settings: VoiceOver
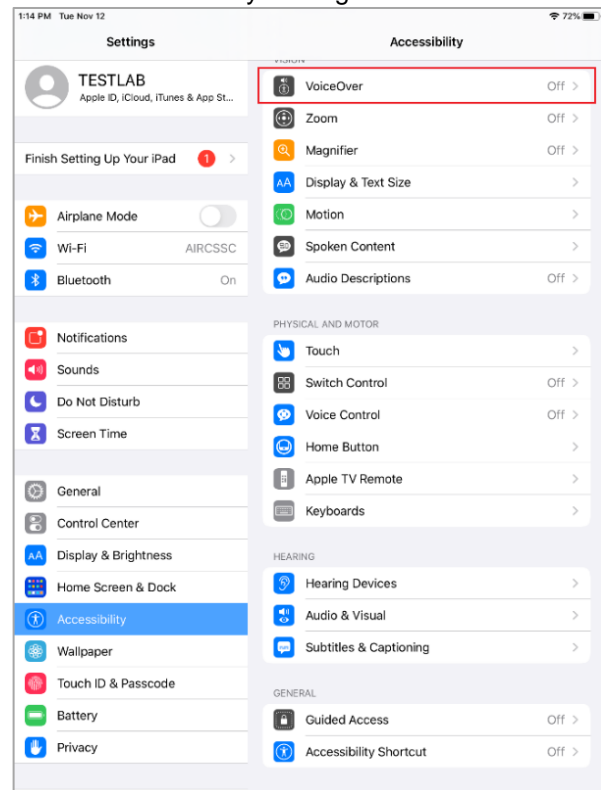
4. Toggle the **VoiceOver** switch to the left to disable VoiceOver.

VoiceOver Settings

Disabling Emoji Keyboard for iPads

iPads running any supported version of iPadOS have an emoji keyboard enabled by default. If the emoji keyboard is not disabled, students will be able to enter emoticons into a test, which can be confusing for scorers.

The emoji keyboard can be disabled through keyboard settings. The following instructions describe how to disable the Emoji Keyboard.

1. Select **Settings**.

2. Navigate to **General > Keyboard**.

3. Select **Keyboards**.

4. Delete Emoji from the list by sliding it to the left and selecting **Delete**.

Keyboards Setting
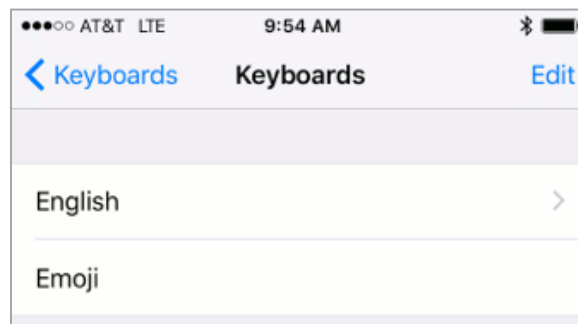
Disabling Smart Punctuation

With iPadOS devices, students may receive a login failure when "Smart Punctuation" is enabled for the keyboard as the default apostrophe is not recognized.

To avoid error messages from appearing for users with apostrophes in their names:

1. Select **Settings**.

2. Select **General**.

3. Select **Keyboards**.

4. Turn off **Smart Punctuation**.

Troubleshooting for macOS

This section contains troubleshooting tips for macOS.

Unsupported Operating System/Browser Error

If users attempt to run Secure Browser 12.5 on macOS 11.4, they will see an unsupported operating/browser combination page. Install Secure Browser 14 on macOS 11.4 devices.

If users run Secure Browser 14 on anything under macOS 11 (10.15 and below), they will receive an error message stating this application is only compatible with macOS 11. Install Secure Browser 12.5 on versions 10.13–10.15.

Resetting Secure Browser Profiles on macOS

If the Help Desk advises you to reset the Secure Browser profile, use the instructions in this section.

1. Log on as an admin user or as the user who installed the Secure Browser and close any open Secure Browsers.

2. Start **Finder**.

3. While pressing **Option**, select **Go > Library**. The contents of the **Library** folder appear.

4. Open the **Application Support** folder, and delete the folder containing the Secure Browser.

5. Returning to the Library, open the **Caches** folder, and delete the Secure Browser's folder.

6. Restart the Secure Browser.

Keyboard Navigation to Tool Menu Using a Safari Browser

Students can use any web browser for practice tests, and navigate to the Tool menu using standard methods, with the exception of Safari. To access the Tool menu using Safari, enable the "Press tab to highlight each item on a webpage" option in Safari Preferences, as shown below.

NOTE: Students who have text-to-speech (TTS) accommodation enabled for practice tests will need to use the Secure Browser.

1. Open Safari, and from the Safari menu, click **Preferences**.

2. Click **Advanced**.

3. Mark the checkbox **Press tab to highlight each item on a webpage**.
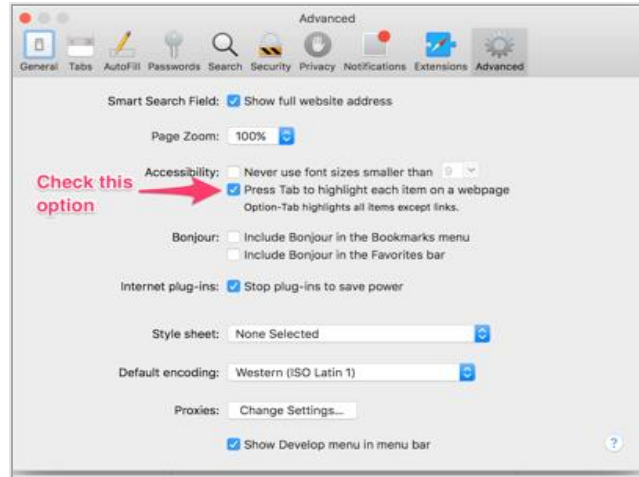
Disabling Text-to-Speech Keyboard Shortcut

A feature in macOS 10.12 and later allows users to have any text on the screen read aloud by selecting the text and hitting a preset key or set of keys on the keyboard. By default, this feature is disabled and must remain disabled so as not to compromise test security. This section describes how to toggle this feature.

To toggle text-to-speech keyboard shortcut:

1. From the Apple menu, select **System Preferences**.
2. Select **Accessibility**.
3. Select **Speech**.
4. To enable this feature, check the **Speak selected text when the key is pressed** checkbox. To disable, deselect the checkbox.

Troubleshooting Text-to-Speech

Using text-to-speech requires at least one voice pack to be installed on testing computers.

A number of voice packs are available for desktop computers, and CAI researches and tests voice packs for compatibility with the Secure Browser. Additionally, not all voice packs that come pre-installed with operating systems are approved for use with online testing. The voice packs listed at the end of this section have been tested and are allowed by the Secure Browser.

Using Text-to-Speech

Students using text-to-speech for the practice tests must log in using the Secure Browser.

We strongly encourage schools to test the text-to-speech settings before students take operational tests. You can check these settings by running a practice test or the Infrastructure

Trial with text-to-speech enabled or through the diagnostic page. From the student practice test login screen, click the **Run Diagnostics** link, and then click the **TTS Check** button.

How the Secure Browser Selects Voice Packs

This section describes how CAI's Secure Browsers select which voice pack to use. It is recommended that students use the same voice pack that is used for instruction.

Voice Pack Selection on Desktop Versions of Secure Browsers

When a student who is using text-to-speech starts a test, the Secure Browser looks for voice packs on the student's machine. Upon recognizing an approved voice pack, the Secure Browser uses the one with the highest priority.

If any of the approved voice packs has also been set as the default voice on the computer, then that voice pack will always get the highest priority. Currently, MAC OS Alex is one of the Voice packs used by CAI to check for proper pronunciation.

Configuring macOS Text-to-Speech Settings

This section explains how to configure macOS for using text-to-speech with the Secure Browser. The text-to-speech feature is available on macOS versions as listed on the Secure Browsers page.

The instructions in this section are for macOS 10.12. The process is similar for other versions of macOS.

1. Choose Apple Menu > **System Preferences**.

2. Click **Accessibility**.

3. From the pane on the left side, select **Speech**.
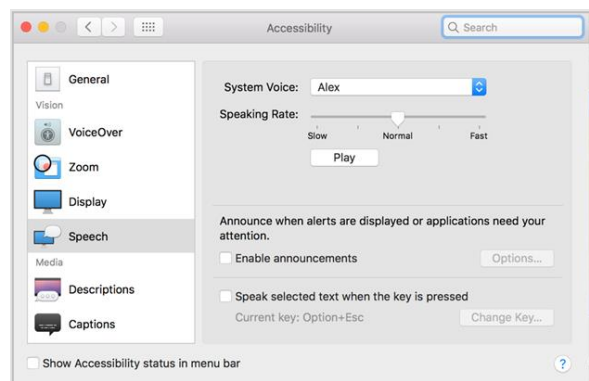
4. Configure your default TTS preferences.

    a.   *System Voice*: If multiple voice packs are available, select the default voice.

    b.   Select **Play** to see whether the selected voice requires a rate adjustment.

    c.   *Speaking Rate: If necessary, adjust the voice speed. Drag the slider to make the voice speak slower or faster.*

    d.   *When you are done, click the red X in the upper left corner to save your settings and close the Accessibility window.*

Voice Packs Recognized by Desktop Secure Browsers

The table below displays the voice packs for macOS that are currently recognized by the Secure Browser.

Voice Packs for macOS

Voice Packs Recognized by Secure Browsers—macOS

Vendor	Voice Pack	Language
macOS (pre-installed)	Agnes	English
macOS (pre-installed)	**Alex**	**English**
macOS (pre-installed)	Bruce	English
macOS (pre-installed)	Callie	English
macOS (pre-installed)	David	English
macOS (pre-installed)	Fred	English
macOS (pre-installed)	Jill	English
macOS (pre-installed)	Junior	English
macOS (pre-installed)	Kathy	English
macOS (pre-installed)	Princess	English
macOS (pre-installed)	Ralph	English
macOS (pre-installed)	Samantha	English
macOS (pre-installed)	Vicki	English
macOS (pre-installed)	Victoria	English
Infovox (commercial)	Heather Infovox iVox HQ	English

macOS and iPadOS Technology Coordinator Checklist

This checklist can be printed out and referred to during review of networks and computers used for testing.

Activity	Target Completion Date	Reference
For all Operating Systems		
☐ Verify that all of your school's computers/devices that will be used for online testing meet the operating system requirements.	3–4 weeks before testing begins in your school	Supported Systems & Requirements
☐ Install Secure Browser 12.5 on all 10.13–10.15 computers/devices that will be used for testing. Install Secure Browser 14 on all macOS 11 computers/devices that will be used for testing.	3–4 weeks before testing begins in your school	Configurations, Troubleshooting, and Secure Browser Installation for macOS and iPadOS
☐ Verify that your school's network and Internet are properly configured for testing, including Allowlisting procedures, conducting network diagnostics, and resolving any issues.	3–4 weeks before testing begins in your school	Technology Setup for Online Testing
☐ Enable pop-up windows and review configuration requirements for each operating system.	1–2 weeks before testing begins in your school	Configurations, Troubleshooting, and Secure Browser Installation for macOS and iPadOS
For macOS and iPadOS		
☐ Prior to downloading the secure browser, install the secure profile for macOS on all computers/devices that will be used for testing.	3–4 weeks before testing begins in your school	Configurations, Troubleshooting, and Secure Browser Installation for macOS and iPadOS
☐ Complete remainder of additional configurations.	1–2 weeks before testing begins in your school	Additional Configurations for macOS
☐ Install any required text-to-speech software on computers that will be used for testing with that accommodation and verify the installation.	1–2 weeks before testing begins in your school	Using Text-to-Speech

Florida Help Desk and User Support

If this document does not answer your questions, please contact the Florida Help Desk.

The Help Desk will be open **Monday–Friday from 7:00 a.m. to 8:30 p.m. Eastern Time** (except holidays or as otherwise indicated on the Florida Statewide Assessments Portal).

Toll-Free Phone Support: 1-866-815-7246

Email Support: FloridaHelpDesk@CambiumAssessment.com

In order to help us effectively assist you with your issue or question, please be ready to provide the Help Desk with detailed information that may include the following:

- Device, operating system, and browser version information

- Any error messages and codes that appeared, if applicable

- Information about your network configuration:

  o Secure browser installation (to individual machines or network)

  o Wired or wireless Internet network setup

Change Log

Location	Change	Date
Throughout Guide	Removed references to iOS and OS X.	9/2/21
Disabling Sleep Mode on macOS 11	Removed section.	9/2/21
Disabling Smart Punctuation	Updated instructions.	9/2/21
Throughout Guide	Updated links to new portal.	9/2/21
About Assessment Mode	Removed reference of Secure Browser 12.6.	2/2/22