ELPA21

Configurations, Troubleshooting, and Advanced Secure Browser Installation Guide for Mac

For Technology Coordinators

2021-2022

Published June 24, 2021

Prepared by Cambium Assessment, Inc.

Configurations, Troubleshooting, and Advanced Secure Browser Installation for Mac

This document contains configurations, troubleshooting, and advanced Secure Browser installation instructions for your network and Mac workstations.

How to Configure Mac Workstations for Online Testing

This section contains additional configurations for Mac.

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

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

Instructions for these configurations appear below.

About Assessment Mode

A feature in macOS 11.4 called Assessment Mode (AM) works with CAI's Secure Browser to lock down Mac workstations for online testing. AM requires no setup. Once the Secure Browser is launched on a Mac workstation running macOS 11.4, 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.

How to Download and Install the Mac Secure Profile

The Secure Profile is a configuration profile that can be used to configure Mac workstations running macOS 10.13-10.15 for online testing. It can be downloaded from your portal's Secure Browser page and must be installed, along with the Secure Browser, before testing begins.

The Secure 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 also 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. If you do not install the Secure Profile, the features listed in this paragraph must be disabled manually. Even if you do install the Secure Profile, the features listed in the bullet points above must still be disabled manually.

Because the Secure Profile configures the operating system regardless of the operating system's current settings, there is no way for CAI to create a configuration profile to roll back the changes. Before you install the Secure Profile, you should back up your device profile's preferences and settings. Once the device is no longer used for testing, the profile can be removed, and your original settings can be reapplied.

To revert configurations made by the Secure Profile if you did not create a backup of your device profile's preferences and settings prior to installation, the features listed in the paragraph above must be re-enabled manually. These features can be re-enabled through System Preferences.

The Secure Profile was last updated in Spring 2021. If you have an older version installed, please download the latest version from your portal and install it using the instructions below.

1. Click the **Download the Secure Profile** link on the Mac tab of your portal's Secure Browser's page to download the Mac Secure Profile.
2. Run the Mac Secure Profile installer.
3. Upon installation, restart your computer.

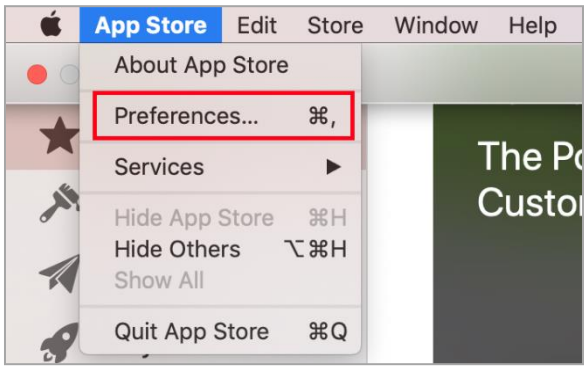
How to Disable Updates to Third-Party Apps

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.

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

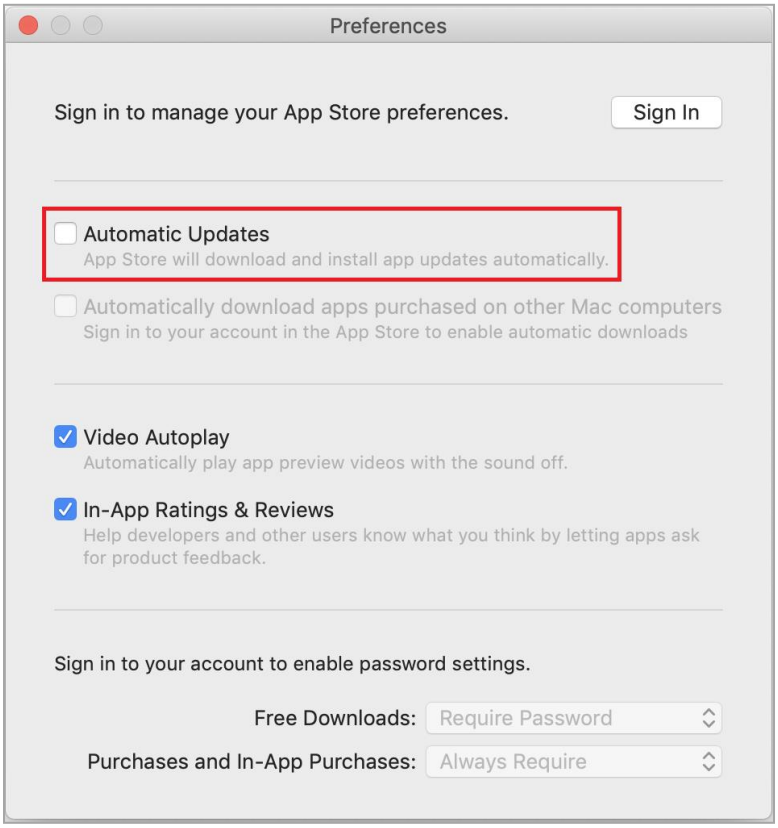
1. Log in to the student's account.
2. Open **App Store**. The ***App Store*** window opens.
3. From the menu bar, select **App Store**.

Figure 1. App Store Menu Bar Options



4. Select **Preferences**. The ***Preferences*** window opens.

Figure 2. App Store Preferences



5. Clear the **Automatic Updates** checkbox.

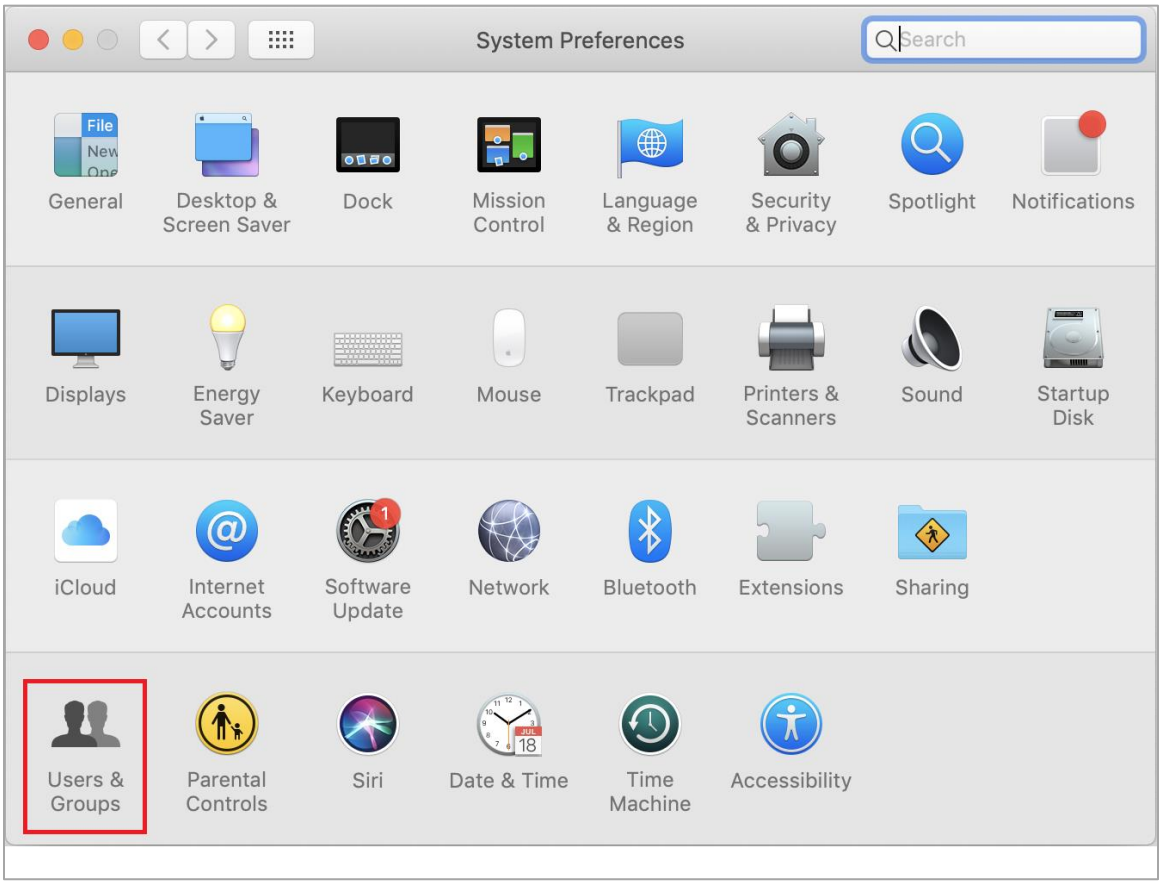
6. Close the ***Preferences*** and ***App Store*** windows.

How to Disable Fast User Switching

Fast User Switching is a feature 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.

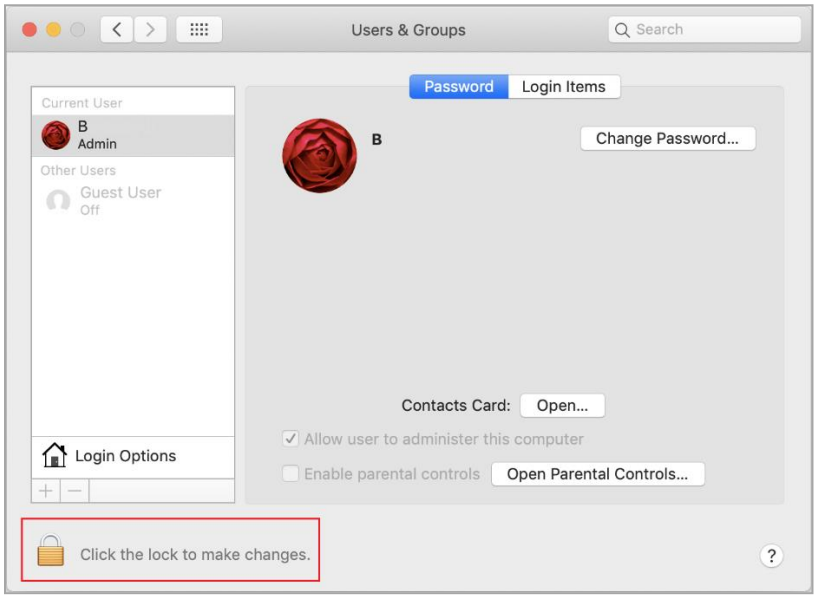
1. Choose Apple menu > **System Preferences**. The ***System Preferences*** window opens.

Figure 3. System Preferences



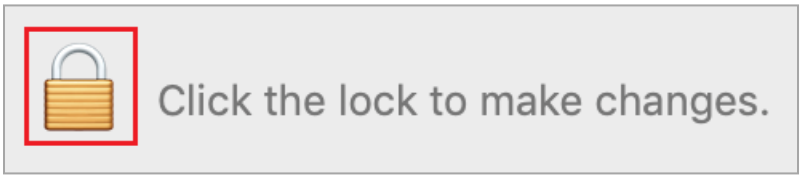
2. Click **Users & Groups**. The ***Users & Groups*** window opens.

Figure 3. Users & Groups



3. If the padlock in the lower left corner is locked, click it and authenticate with administrator credentials.

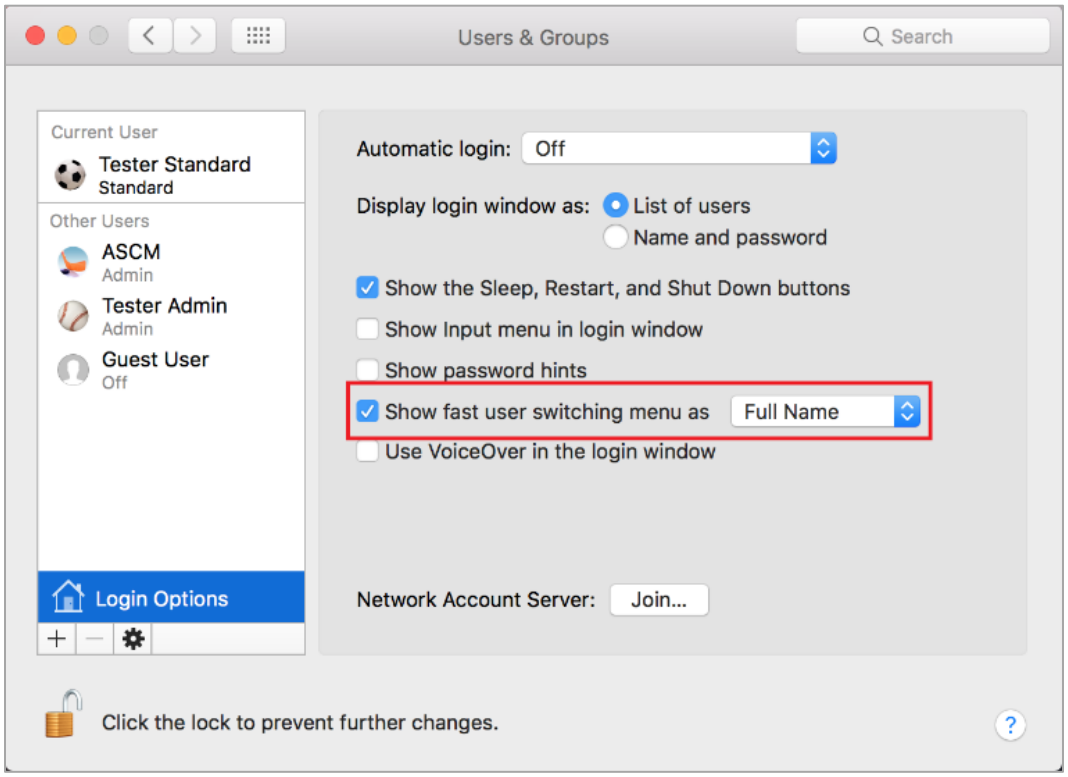
Figure 4. Users & Groups Padlock



4. Click **Login Options**. The ***Login Options*** window opens.

5. Uncheck the **Show fast user switching menu as** checkbox.

Figure 5. Login Options



6. Close the ***Users & Groups*** window.

How to Install 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 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.

How to Install the Secure Browser for Mac Using Advanced Methods

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

How to Clone the Secure Browser Installation to Other Macs

Depending on your networking and permissions, it may be faster to install the Secure Browser onto a single Mac, take an image of the disk, and copy the image to other Macs.

1. On the computer from where you will clone the installation, install the Secure Browser following the directions on your portal. Be sure to run and then close the Secure Browser after the installation.
2. Clone the image.
3. Deploy the image to the target Macs.

How to Uninstall the Secure Browser on Mac

To uninstall a Mac Secure Browser, drag its folder to the Trash.

How to Troubleshoot Mac Workstations

This section contains troubleshooting tips for Mac.

How to Reset Secure Browser Profiles on Mac

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

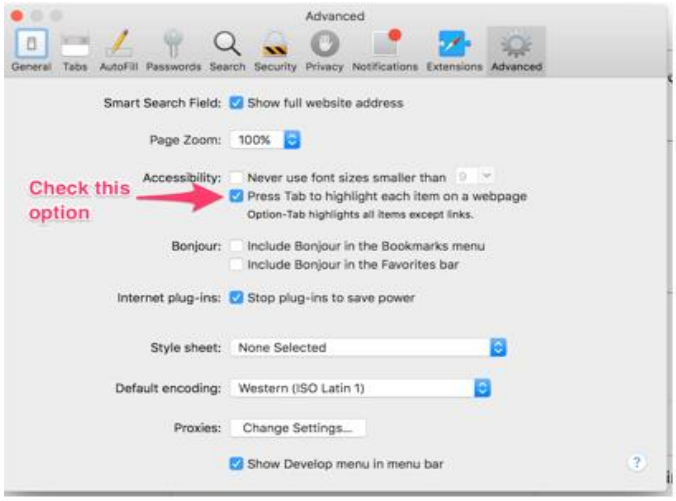
1. Log on as an admin user or as the user who installed the Secure Browser and close any open Secure Browsers.
2. Start **Finder**.
3. While pressing **Option**, select **Go > Library**. The contents of the Library folder appear.
4. Returning to the Library, open the **Caches** folder, and delete the Secure Browser's folder.
5. Restart the Secure Browser.

How to Navigate to the Tool Menu with the Keyboard Using a Safari Browser

Students can use any supported public 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.

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**.

Figure 7. Advanced Safari Preferences



How to Disable 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.

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.

How to Configure Networks for Online Testing

This section contains additional configurations for your network.

Resources to Whitelist for Online Testing

This section presents information about the URLs that CAI provides. Ensure your network's firewalls are open for these URLs. If your testing network includes devices that perform traffic shaping, packet prioritization, or Quality of Service, ensure these URLs have high priority.

URLs for Non-Testing Sites to Whitelist

Table 1 lists URLs for non-testing sites, such as Test Information Distribution Engine and Online Reporting System.

Table 1. CAI URLs for Non-Testing Sites

System	URL
Portal and Secure Browser installation files	https://la.portal.cambiumast.com/
Single Sign-On System	https://sso2.cambiumast.com/auth/realms/louisiana/account
Test Information Distribution Engine	https://la.tide.cambiumast.com/
Reporting System	https://la.reporting.cambiumast.com/

URLs for TA and Student Testing Sites to Whitelist

Testing servers and satellites may be added or modified during the school year to ensure an optimal testing experience. As a result, CAI strongly encourages you to whitelist at the root level. This requires using a wildcard. CAI strongly encourages using wildcards when adding these URLs to your allowlist, as servers may be added or removed from the field without notice.

Table 2. CAI and AIR URLs for Testing Sites

System	URL
Assessment Viewing Application for TA and Student Testing Sites For 2021-2022, users should whitelist both Cambium and AIR URLs listed in this table.	*.cambiumast.com *.tds.cambiumast.com *.cloud1.tds.cambiumast.com *.cloud2.tds.cambiumast.com *.cambiumtds.com *.airast.org *.tds.airast.org *.cloud1.tds.airast.org *.cloud2.tds.airast.org

Ports and Protocols Required for Online Testing

Table 3 lists the ports and protocols used by the Test Delivery System. Ensure that all content filters, firewalls, and proxy servers are open accordingly.

Table 3. Ports and Protocols for Test Delivery System

Port/Protocol	Purpose
80/TCP	HTTP (initial connection only)
443/TCP	HTTPS (secure connection)

How to Configure Filtering Systems

If the school's filtering system has both internal and external filtering, the URLs for the testing sites (see Table 2) must be whitelisted in both filters. Ensure your filtering system is not configured to perform packet inspection on traffic to CAI servers. Please see your vendor's documentation for specific instructions. Also, be sure to whitelist these URLs in any multilayer filtering system (such as local and global layers). Ensure all items that handle traffic to *.tds.cambiumast.com and *.tds.airast.org have the entire certificate chain and are using the latest TLS 1.2 protocol.

How to Configure for Domain Name Resolution

Table 1 and Table 2 list the domain names for CAI's testing and non-testing applications. Ensure the testing machines have access to a server that can resolve those names.

How to Configure Network Settings for Online Testing

Local Area Network (LAN) settings on testing machines should be set to automatically detect network settings.

1. Open **System Preferences**.
2. Open **Network**.
3. Select **Ethernet** for wired connections or **WiFi** for wireless connections.
4. Click **Advanced**.
5. Click **Proxies** tab.
6. Click **Auto Proxy Discovery** checkbox.
7. Click **OK** to close window.
8. Click **Apply** to close **Network** window.
9. Close **System Preferences**.

How to Configure the Secure Browser for Proxy Servers

By default, the Secure Browser attempts to detect the settings for your network's web proxy server. However, users of web proxies should execute a proxy command once from the command prompt. This command does not need to be added to the Secure Browser shortcut. Table 4 lists the form of the command for different settings and operating systems. To execute these commands from the command line, change to the directory containing the Secure Browser's executable file.

Note: Domain names in commands The commands in Table 4 use the domain proxy.com. When configuring for a proxy server, use your actual proxy server hostname.

Table 4. Specifying proxy settings using the command line

Description	System	Command
Use the browser without any proxy	Mac	`./SecureTest -proxy 0 aHR0cHM6Ly9hci50ZHMuY2FtYml1bWFzdC5jb20vc3R1ZGVudA==`
Set the proxy for HTTP requests only	Mac	`./SecureTest -proxy 1:http:proxy.com:8080 aHR0cHM6Ly9hci50ZHMuY2FtYml1bWFzdC5jb20vc3R1ZGVudA==`
Set the proxy for all protocols to mimic the "Use this proxy server for all protocols" of Firefox	Mac	`./SecureTest -proxy 1:*:proxy.com:8080 aHR0cHM6Ly9hci50ZHMuY2FtYml1bWFzdC5jb20vc3R1ZGVudA==`
Specify the URL of the PAC file	Mac	`./SecureTest -proxy 2:proxy.com aHR0cHM6Ly9hci50ZHMuY2FtYml1bWFzdC5jb20vc3R1ZGVudA==`
Auto-detect proxy settings	Mac	`./SecureTest -proxy 4 aHR0cHM6Ly9hci50ZHMuY2FtYml1bWFzdC5jb20vc3R1ZGVudA==`
Use the system proxy setting (default)	Mac	`./SecureTest -proxy 5 aHR0cHM6Ly9hci50ZHMuY2FtYml1bWFzdC5jb20vc3R1ZGVudA==`

Change Log

Location	Change	Date
Throughout	Cutover from 20-21.	6/18/21