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

For Technology Coordinators

2019-2020

Published July 17, 2019

Prepared by the American Institutes for Research®

Table of Contents

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 Networks for Online Testing

This section contains additional configurations for your network.

Which Resources to Whitelist for Online Testing

This section presents information about the URLs that AIR 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.

Which URLs for Nontesting Sites to Whitelist

Table 1 lists URLs for nontesting sites, such as the Test Information Distribution Engine (TIDE) and Online Reporting System (ORS).

Table 1. AIR URLs for Nontesting Sites

System	URL
Portal and Secure Browser installation files	oh.portal.airast.org
Single Sign-On System	sso1.airast.org
Test Information Distribution Engine	oh.tide.airast.org
Online Reporting System	oh.reports.airast.org

Which 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, AIR strongly encourages you to whitelist at the root level. This requires using a wildcard.

Table 2. AIR URLs for Testing Sites

System	URL
TA and Student Testing Sites	*.airast.org *.tds.airast.org *.cloud1.tds.airast.org *.cloud2.tds.airast.org

Which Ports and Protocols Are 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. 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).

How to Configure for Domain Name Resolution

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

How to Configure for Certificate Revocations

AIR's servers present certificates to the clients. The following sections discuss the methods used to check those certificates for revocation.

How to Use the Online Certificate Status Protocol

To use the Online Certificate Status Protocol (OCSP), ensure your firewalls allow the domain names listed in Table 4. The values in the Patterned column are preferred because they are more robust due to use of the wildcard (*).

Table 4. Domain Names for OCSP

Patterned	Fully Qualified
*.thawte.com	ocsp.thawte.com
*.geotrust.com	ocsp.geotrust.com
*.ws.symantec.com	ocsp.ws.symantec.com

If your firewall is configured to check only IP addresses, do the following:

1. Get the current list of OCSP IP addresses from Symantec. The list is available at https://www.symantec.com/content/en/us/enterprise/other_resources/OCSP_Upgrade_-_New_IP_Addresses.txt.

2. Add the retrieved IP addresses to your firewall's whitelist. Do not replace any existing IP addresses.

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 5 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 5 use the domains foo.com and proxy.com. When configuring for a proxy server, use your actual testing domain names as listed in the section Which Resources to Whitelist for Online Testing.

Table 5. Specifying proxy settings using the command line

Description	System	Command
Use the browser without any proxy	Mac	`./OHSecureBrowser -proxy 0 aHR0cHM6Ly9vaC50ZHMuYWlyYXN0Lm9yZy9zdHVkZW50Lw0K`
Set the proxy for HTTP requests only	Mac	`./OHSecureBrowser -proxy 1:http:foo.com:80 aHR0cHM6Ly9vaC50ZHMuYWlyYXN0Lm9yZy9zdHVkZW50Lw0K`
Set the proxy for all protocols to mimic the "Use this proxy server for all protocols" of Firefox	Mac	`./OHSecureBrowser -proxy 1:*:foo.com:80 aHR0cHM6Ly9vaC50ZHMuYWlyYXN0Lm9yZy9zdHVkZW50Lw0K`
Specify the URL of the PAC file	Mac	`./OHSecureBrowser -proxy 2:proxy.com aHR0cHM6Ly9vaC50ZHMuYWlyYXN0Lm9yZy9zdHVkZW50Lw0K`
Auto-detect proxy settings	Mac	`./OHSecureBrowser -proxy 4 aHR0cHM6Ly9vaC50ZHMuYWlyYXN0Lm9yZy9zdHVkZW50Lw0K`
Use the system proxy setting (default)	Mac	`./OHSecureBrowser -proxy 5 aHR0cHM6Ly9vaC50ZHMuYWlyYXN0Lm9yZy9zdHVkZW50Lw0K`

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, do the following:

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

b. In Finder, display the **Library** folder. Open the **Application Support** folder.

c. Delete the folder containing the Secure Browser.

d. 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/ OHSecureBrowser --CreateProfile profile_name, where profile_name is unique among all testing computers.

3. Clone the image.

4. 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 Configure Mac Workstations for Online Testing

This section contains additional configurations for Mac.

Several features on Mac workstations must be disabled before testing begins. Some of these can be disabled via the Mac Secure Profile and some can only be disabled manually. If you choose not to use the Mac Secure Profile, all must be disabled manually.

The Mac Secure Profile disables the following:

- Hot keys for enabling Dictation, Mission Control, and Spaces
- Trackpad gestures for accessing Lookup, Space Switching, Expose, and Notification Center

It also sets function keys to standard functions.

The Profile does not disable the following:

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

How to Install the Mac Secure Profile

The Mac Secure Profile is a script that can be used to configure Mac workstations for online testing. The profile can be downloaded from your portal's Secure Browser page. Upon installation, the profile disables the hot keys for enabling Dictation, Mission Control, and Spaces and the trackpad gestures for accessing Lookup, Space Switching, Expose, and Notification Center and also sets function keys to standard functions for all users of the Mac that it is deployed to. The following instructions describe how to download, install, and configure the Mac Secure Profile.

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.

Figure 1. Download Mac Secure Profile

How to Disable Updates to Third-Party Apps

Updates to third-party apps may include components that compromise the testing environment. This section describes how to disable updates to third-party apps.

The following instructions are based on OS X 10.9; similar instructions apply for other versions of Mac OS.

1. Log in to the student's account.
2. Choose Apple menu > **System Preferences**. The ***System Preferences*** dialog box opens.
3. Click **App Store**. The ***App Store*** window opens.

Figure 2. App Store Window

4. Mark **Automatically check for updates**.
5. Clear **Download newly available updates in the background**.
6. Clear **Install app updates**.
7. Mark **Install system data files and security updates**.

How to Disable Updates to iTunes

You must disable updates to iTunes prior to testing. If iTunes updates pop up during a test, the Secure Browser will pause the test, and the student will be kicked out of the testing session.

The following instructions are based on OS X 10.9; similar instructions apply for other versions of Mac OS.

1. Log in to the student's account.
2. Start iTunes.
3. Select **iTunes > Preferences**.
4. Under the **Advanced** tab, clear **Check for new software updates automatically**.
5. Click **OK**.

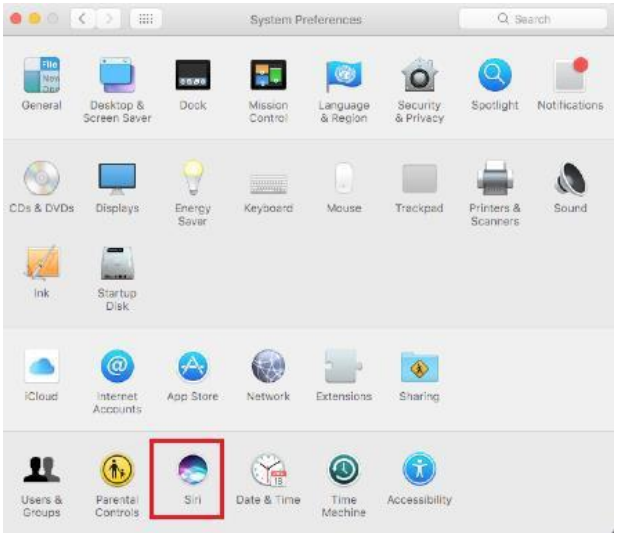
Figure 3. Advanced Preferences

How to Disable Siri

Siri is a virtual assistant that uses voice commands to answer questions and perform actions on Mac desktops and laptops. If Siri is not disabled, students could potentially have access to features and information that they should not have access to while taking a secure assessment.

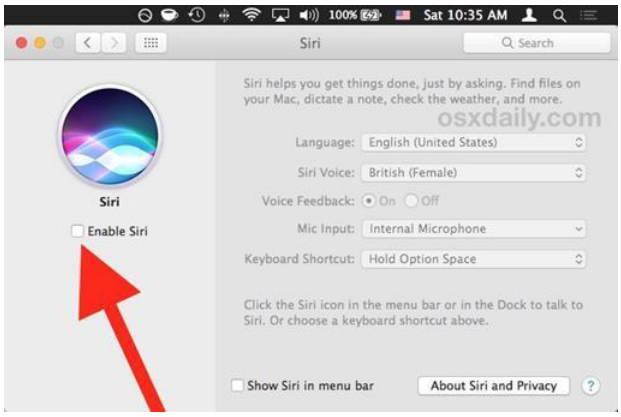
1. Go to **System Preferences** and choose **Siri** from the control panel options.

Figure 4. System Preferences > Siri



2. Uncheck the box next to **Enable Siri**.

Figure 5. Siri



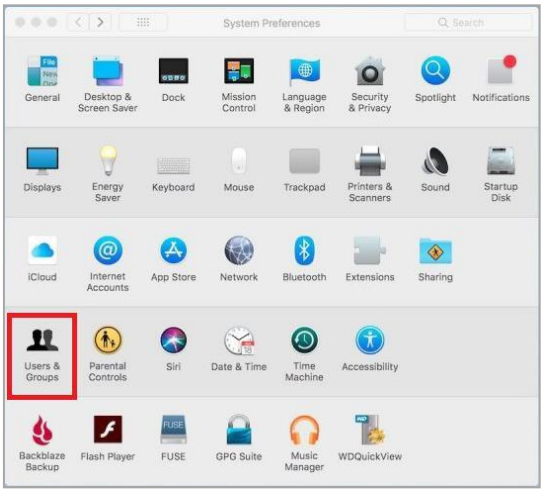
With Siri disabled, the menu bar icon is removed. Depending on your Mac, Siri can still be activated from the dock or the Touch Bar. It's important to note that while in a test, the AIRSecureBrowser app will detect if a user tries to enable Siri during testing, and the app will disconnect the student from the test.

How to Disable Fast User Switching

Fast User Switching is a feature in Mac OS X 10.9 and higher 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. The following instructions describe how to disable Fast User Switching.

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

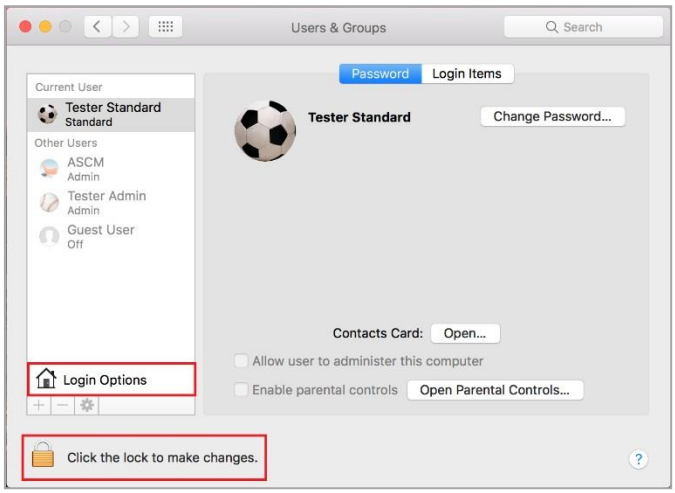
Figure 6. System Preferences > Users & Groups



2. In System Preferences, click **Users & Groups**. The ***Users & Groups*** window opens.

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

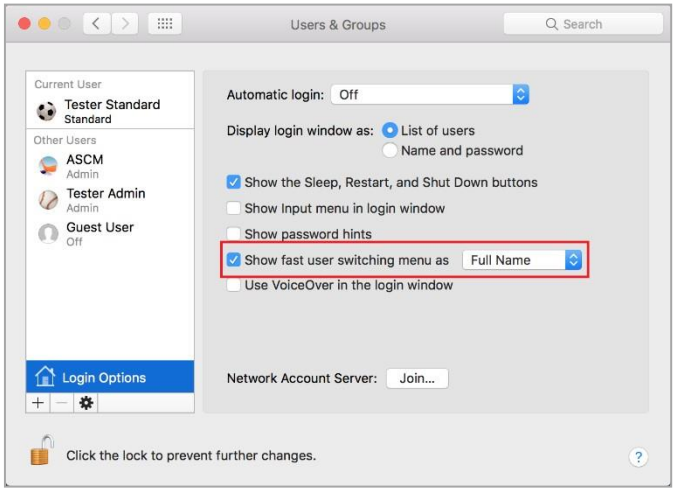
Figure 7. Users & Groups



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

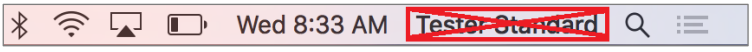
5. Uncheck the **Show fast user switching menu as…** checkbox.

Figure 8. Login Options



Fast User Switching is now disabled. The Fast User Switching icon no longer appears in the menu bar.

Figure 9. Menu Bar



How to Troubleshoot Mac Workstations

This section contains troubleshooting tips for Mac.

How to Reset Secure Browser Profiles on Mac

If the Ohio 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.

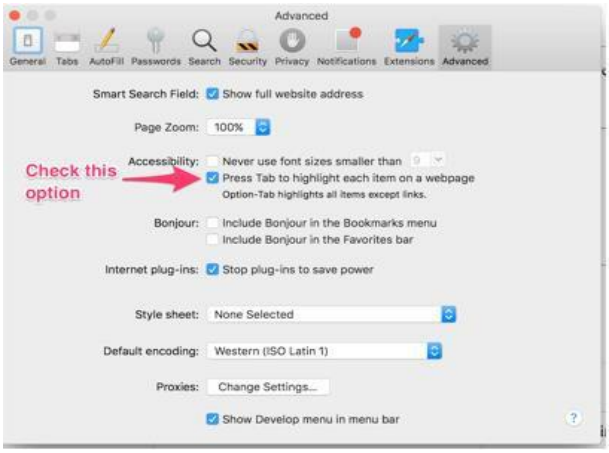
How to Navigate to Tool Menu with the Keyboard Using a Safari Browser

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.

NOTE: Students who have text-to-speech (TTS) accommodations 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**.

Figure 10. 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.