south dakota
DEPARTMENT OF EDUCATION
Learning. Leadership. Service.

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

## For Technology Coordinators

2018–2019

Published November 14, 2018

*Prepared by the American Institutes for Research®*

Descriptions of the operation of the Test Information Distribution Engine, Test Delivery System, and related systems are property of the American Institutes for Research (AIR) and are used with the permission of AIR.

# 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.

## Additional Configurations for Networks

This section contains additional configurations for your network.

### Whitelisting Resources 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.

#### URLs for Non-Testing Sites

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

Table 1. AIR URLs for Non-Testing Sites

| System | URL |
|---|---|
| Portal and Secure Browser installation files | http://sd.portal.airast.org/ |
| Single Sign-On System | https://sso1.airast.org/auth/realms/maac/account |
| Test Information Distribution Engine | https://maac.tide.airast.org |
| Online Reporting System | https://sd.reports.airast.org |
| AIRWays Reporting System | https://sd.airways.airast.org |

#### URLs for TA and Student Testing Sites

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<br>Assessment Viewing Application | *.airast.org<br>*.tds.airast.org<br>*.cloud1.tds.airast.org<br>*.cloud2.tds.airast.org |

### URLs for Online Dictionary and Thesaurus

Some online assessments contain an embedded dictionary and thesaurus provided by Merriam-Webster. The Merriam-Webster URLs listed in Table 3 should be whitelisted to ensure that students can use them during testing.

Table 3. AIR URLs for Online Dictionaries and Thesauruses

| Domain Name | IP Address |
|---|---|
| media.merriam-webster.com | 64.124.231.250 |
| www.dictionaryapi.com | 64.124.231.250 |

## Required Ports and Protocols

Table 4 lists the ports and protocols used by the Test Delivery System. Ensure that all content filters, firewalls, and proxy servers are open accordingly.

Table 4. Ports and Protocols for Test Delivery System

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

## Configuring 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).

## Configuration for Domain Name Resolution

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

# Configuring for Certificate Revocations

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

### Online Certificate Status Protocol

To use the Online Certificate Status Protocol (OCSP), ensure your firewalls allow the domain names listed in Table 5. The values in the Patterned column are preferred because they are more robust.

Table 5. Domain Names for OCSP

| Patterned | Fully Qualified |
|---|---|
| *.thawte.com | oscp.thawte.com |
| *.geotrust.com | oscp.geotrust.com |
| *.ws.symantec.com | oscp.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.

# Configuring Network Settings for Online Testing

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

*To set LAN settings to auto-detect on Mac machines:*

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**.

## Configuring 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 6 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 6 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 "URLs for Testing Sites" in the *Technical Specifications Manual for Online Testing*.

Table 6. Specifying proxy settings using the command line

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

# Additional Instructions for Installing the Secure Browser for Mac

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

## Cloning 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.

*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 on your portal. 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/SDSecureBrowser --CreateProfile profile_name`, where `profile_name` is unique among all testing computers.
3. Clone the image.
4. Deploy the image to the target Macs.

## Uninstalling the Secure Browser on Mac

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

# Additional Configurations for Mac

This section contains additional configurations for Mac.

## Disabling Application Launches from Function Keys

When students use the Secure Browser for testing, the Test Delivery System conducts regular checks to ensure that other applications are not open. These checks help maintain the integrity of the secure test environment.

Starting with OS X versions 10.9 and later, some Mac computers are factory configured to launch iTunes and other applications by pressing the function keys (e.g., F8) on the keyboard. If a student accidentally presses the function key, the Secure Browser assumes that a forbidden application is running and pauses the student's test. To avoid this scenario, disable the use of function keys to launch applications.

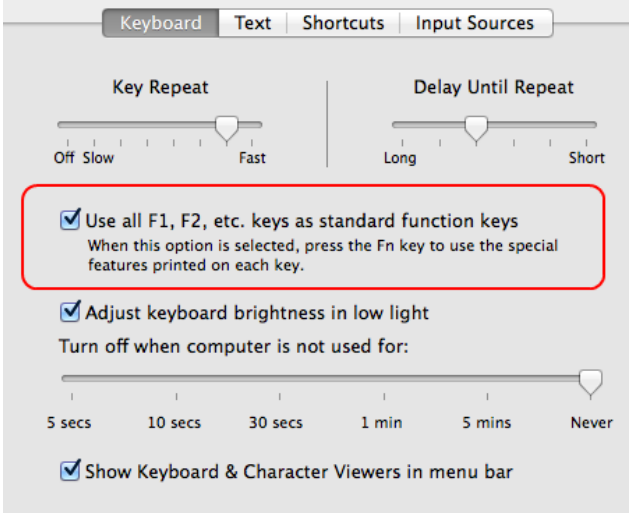
The following instructions are based on OS X 10.9; similar instructions apply for other versions of Mac OS. (You can disable application launches quickly from the command line; see Disabling Spaces and Application Launches from the Command Line for details.)

*To disable application launches from function keys:*

1. Choose Apple menu > **System Preferences**.
2. In System Preferences, click **Keyboard**. The Keyboard window opens.


3. In the Keyboard window, mark **Use all F1, F2, etc. keys as standard function keys**.

If you need to launch iTunes or another application, press the Fn key and then press the desired function key. This combination will launch the application. (Doing so while taking a test causes the Secure Browser to pause the test.)



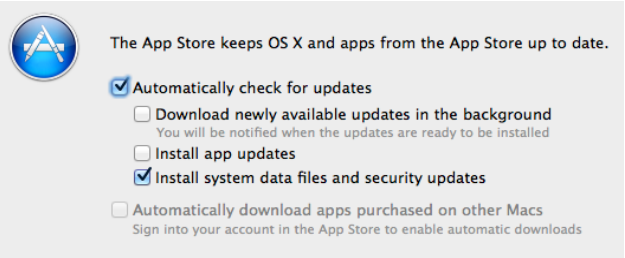

## Disabling Updates to Third-Party Apps

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.

*To disable updates to third-party apps:*

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.




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**.

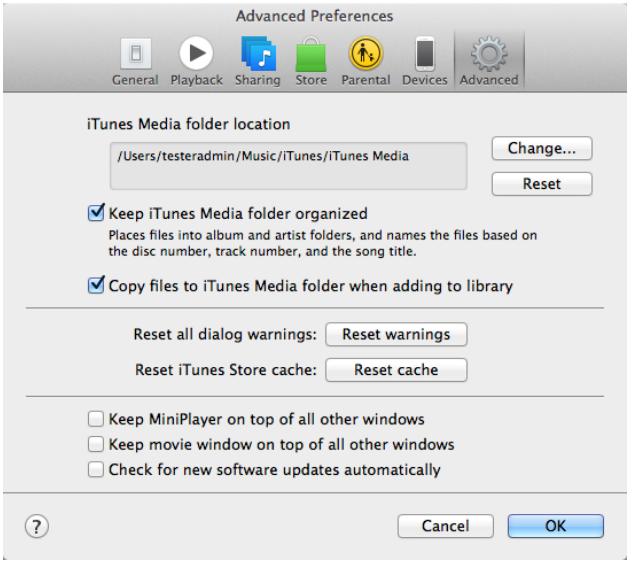
## Disabling Updates to iTunes

Updates to iTunes may be incompatible with the Secure Browser. This section describes how to disable updates to iTunes.

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

*To disable updates to iTunes:*

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**.



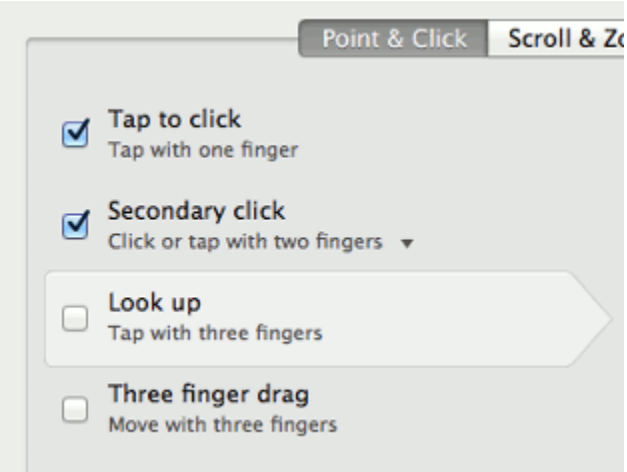
## Disabling Look-up Gesture

OS X versions 10.9 and later include a look-up gesture; highlighting a word and then tapping with three fingers on the trackpad displays a dictionary for the highlighted word—a feature that can compromise testing security. This section describes how to disable the look-up gesture.

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

*To disable the look-up gesture:*

1. Choose Apple menu > **System Preferences**.
2. Click **Trackpad**. The Trackpad window opens.
3. Click the **Point and Click** tab.
4. Clear the **Look up** checkbox.



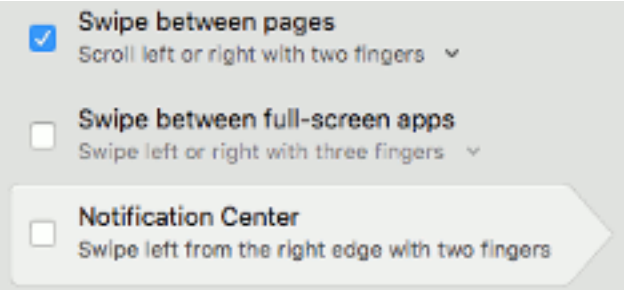

## Disabling Display of Notification Center

OS X versions 10.10 and later include Notification Center, which displays system information when swiping to the left with two fingers from the right edge of the trackpad. Depending on its contents, Notification Center can compromise testing security. This section describes how to disable the gesture for displaying Notification Center.

The following instructions are based on OS X 10.10; similar instructions apply for later versions of Mac OS.

*To disable the gesture for displaying Notification Center:*

1. Choose Apple menu > **System Preferences**.
2. Click **Trackpad**. The Trackpad window opens.
3. Click the **More Gestures** tab.
4. Clear the **Notification Center** checkbox.



## Disabling Spaces and Application Launches from the Command Line

The sections Disabling Mission Control and Disabling Application Launches from Function Keys describe how to configure Mac OS through the desktop. This section describes how to perform those configurations from the command line, which can be faster than working through the desktop. To perform this task, you need to be familiar with logging in to Mac machines through Terminal or other terminal emulator.

*To disable spaces and application launches from the command line:*

1. Log in to the machine as the user that runs the Secure Browser.

2. Enter the following commands:

```
defaults write com.apple.symbolichotkeys AppleSymbolicHotKeys -dict-add 79
"{enabled = 0; value = {parameters = (65535,123, 262144); type = standard; }; }"

defaults write com.apple.symbolichotkeys AppleSymbolicHotKeys -dict-add 80
"{enabled = 0; value = { parameters = (65535, 123, 393216); type = 'standard'; };
}"

defaults write com.apple.symbolichotkeys AppleSymbolicHotKeys -dict-add 81
"{enabled = 0; value = { parameters = (65535, 124, 262144); type = 'standard'; };
}"

defaults write com.apple.symbolichotkeys AppleSymbolicHotKeys -dict-add 82
"{enabled = 0; value = { parameters = (65535, 124, 393216); type = 'standard'; };
}"
```

**TIP** You can paste these lines into a text file, and run the file from the command line.

These commands modify the file `~/Library/Preferences/com.apple.symbolichotkeys.plist`.

3. If you logged in to a computer running OS X 10.9 or later, log out and then log back in.

If you need to restore Spaces and the default application launchers, repeat steps 1–3. In step 2, change `enabled = 0` to `enabled = 1`.

## Disabling Spaces and Application Launches on Remote Machines

The sections Disabling Mission Control, Disabling Application Launches from Function Keys, and Disabling Spaces and Application Launches from the Command Line describe procedures for configuring a secure test environment in Mac OS. This configuration is stored in the file `~/Library/Preferences/com.apple.symbolichotkeys.plist`. If you have many Mac testing machines, it may be easier to push this file to those machines instead of configuring each one individually.

You can push the configuration file to remote machines using a variety of tools, such as the following:

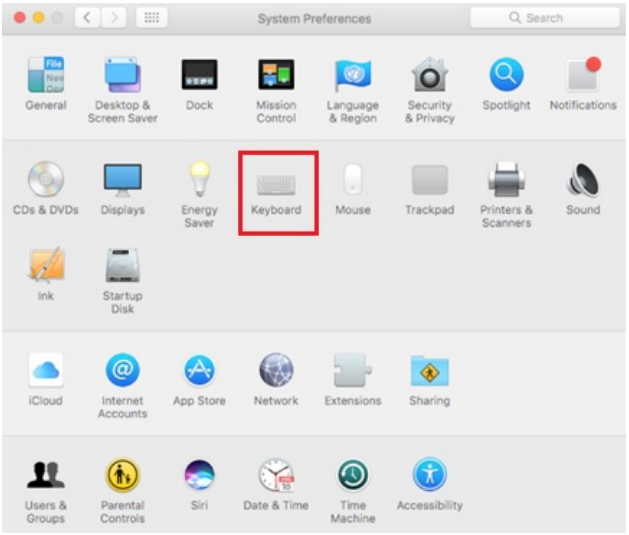
- File Distributor
- Apple's Active Directory Client and Directory Utility
- Apple's Open Directory and Profile Manager
- Centrify & PowerBrokers Identity Enterprise
- Apple Remote Desktop

## Disabling Dictation

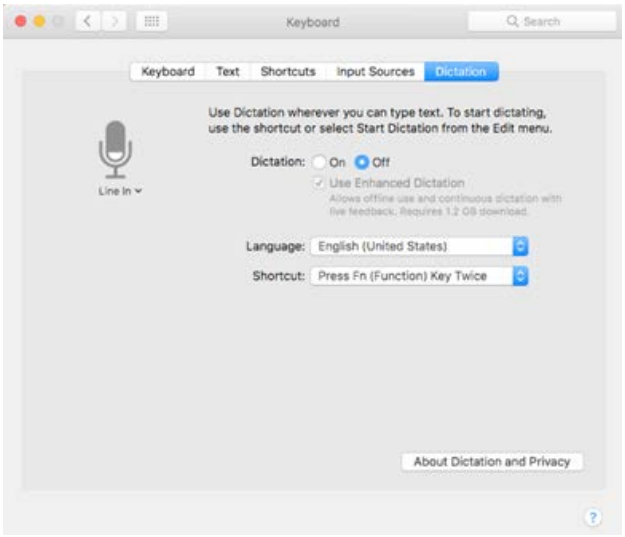
Students can speak into a Mac device utilizing the dictation feature, which suggests words or spellings that may compromise testing security. Use the following procedure to disable dictation.

*To disable **Dictation** in a Mac device:*

1. Go to **System Preferences** and click **Keyboard**, then click **Dictation**.




2. Turn the **Dictation** option to **Off**.

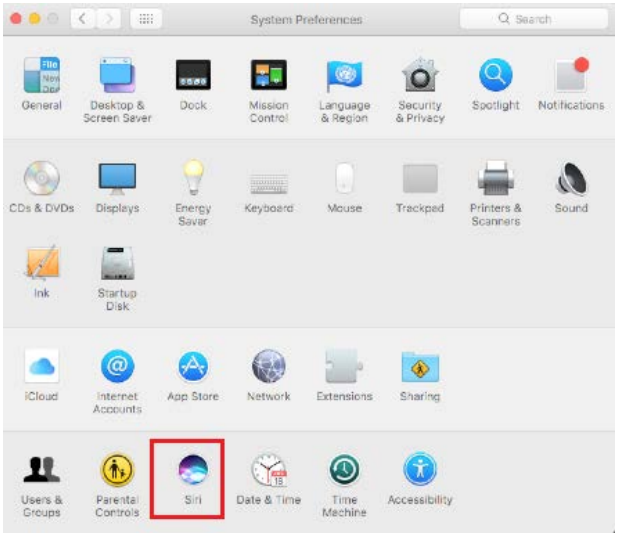



## Disabling Siri

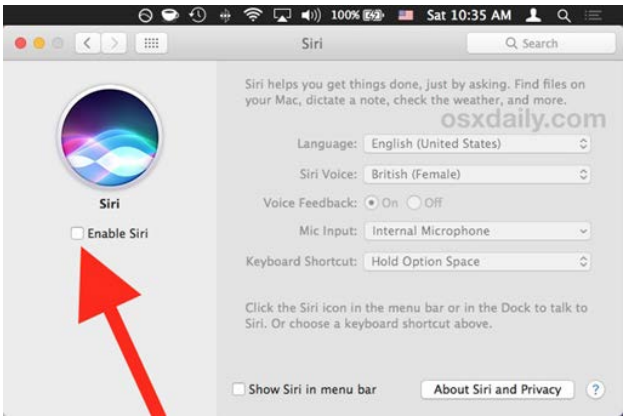
Siri is a virtual assistant that uses voice commands to answer questions and perform actions on Mac desktops and laptops. If Siri is not disabled, students could potentially have access to features and information that they should not have access to while taking a secure assessment.

*To disable the Siri feature*:

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




2. Uncheck the box next to **Enable 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.

## Disabling Custom Keys

Some Mac users have encountered "Error Code 11673 – Custom Keys Enabled" after installing the newest Secure Browser. The following procedure explains how to disable custom keys.

*To disable custom keys:*

1. Launch **System Preferences**.
2. Open **Keyboard**.
3. Click **Keyboard Shortcuts** tab.
4. Uncheck all boxes under **Mission Control** and **Screen Shots**.

## Disabling Mission Control

Mission Control is a feature in Mac OS X 10.9 and later that allows users to switch to open applications running in the background. The following procedure explains how to disable Mission Control. It is recommended to complete this procedure via a batch file when you log in.

*To disable Mission Control:*

1. Open **Terminal**.
2. Enter the following command to disable Mission Control and restart the Dock. **Note:** Restarting the dock is necessary for this change to take place.

```
defaults write com.apple.dock mcx-expose-disabled -bool TRUE && killall Dock
```

# Troubleshooting for Mac

This section contains troubleshooting tips for Mac.

## Resetting Secure Browser Profiles on Mac

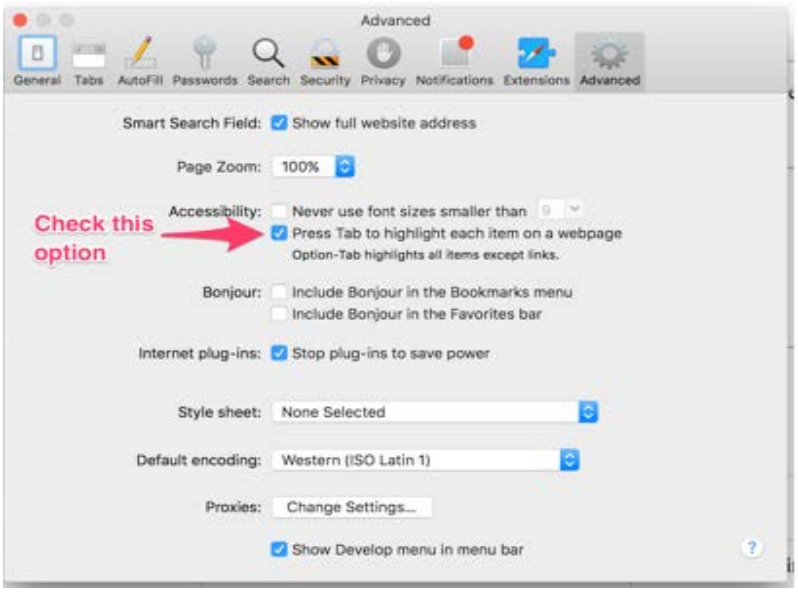
If the Help Desk advises you to reset the Secure Browser profile, use the instructions in this section.

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. 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 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) accommodation enabled for practice tests will need to use the Secure Browser.



## Disabling Text-to-Speech Keyboard Shortcut

A feature in macOS 10.12 (Sierra) and macOS 10.13 (High Sierra) 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 AIR researches and tests voice packs for compatibility with the Secure Browsers. 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 whitelisted by the Secure Browser.

## Using Text-to-Speech

Students using text-to-speech for the practice tests must log in using a supported Secure Browser. Students can also verify that text-to-speech works on their computers by logging in to a practice test session and selecting a test for which text-to-speech is available.

**Note:** We strongly encourage schools to test the text-to-speech settings before students take operational tests. You can check these settings through the diagnostic page. From the student practice test login screen, click the **Run Diagnostics** link, and then click the **Text-to-Speech Check** button.

## How the Secure Browser Selects Voice Packs

This section describes how AIR's Secure Browsers select which voice pack to use.

### 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.

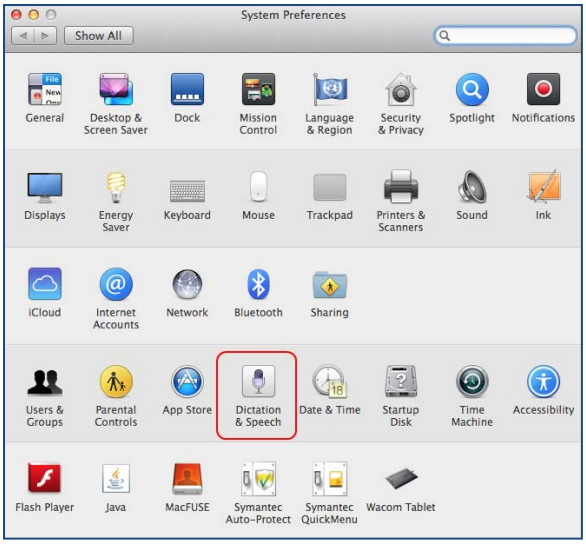
If any of the approved voice packs has also been set as the default voice on the computer, then that voice pack will always get the highest priority.

## Configuring Mac Text-to-Speech Settings

This section explains how to configure Mac OS for using text-to-speech with the Secure Browser. The text-to-speech feature is available on Mac OS versions as listed in the *System Requirements* document.

The instructions in this section are for OS X 10.9. The process is similar for other versions of Mac OS.

1. Open System Preferences, and select **Dictation & Speech**.



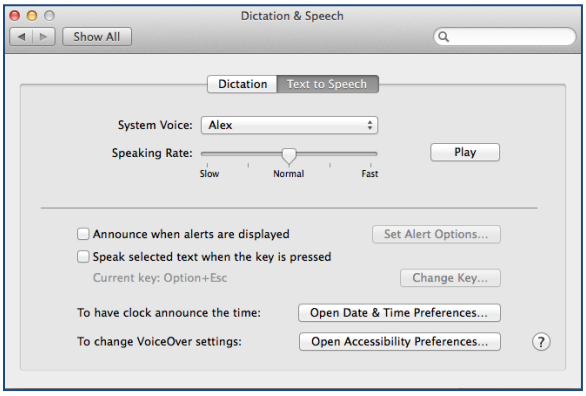
2. In the Text to Speech section, configure your default text-to-speech preferences.

   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. To listen to the rate, select **Play**.

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




## Voice Packs Recognized by Desktop Secure Browsers

The tables in this section display the voice packs for Mac that are currently recognized by the Secure Browser.

### Voice Packs for Mac

Table 7. Voice Packs Recognized by Secure Browsers—Mac

| Vendor | Voice Pack | Language |
|---|---|---|
| Mac (pre-installed) | Agnes | English |
| Mac (pre-installed) | Alex | English |
| Mac (pre-installed) | Bruce | English |
| Mac (pre-installed) | Callie | English |
| Mac (pre-installed) | David | English |
| Mac (pre-installed) | Fred | English |
| Mac (pre-installed) | Jill | English |
| Mac (pre-installed) | Junior | English |
| Mac (pre-installed) | Kathy | English |
| Mac (pre-installed) | Princess | English |
| Mac (pre-installed) | Ralph | English |

| Vendor | Voice Pack | Language |
|---|---|---|
| Mac (pre-installed) | Samantha | English |
| Mac (pre-installed) | Vicki | English |
| Mac (pre-installed) | Victoria | English |
| Infovox (commercial) | Heather Infovox iVox HQ | English |