Hawai'i Statewide Assessment Program

Technical Specifications Manual for Online Testing

For Technology Coordinators

2016–2017

Published June 15, 2017

Prepared by the American Institutes for Research®

Table of Contents

List of Tables

List of Figures

Introduction to the Technical Specifications Manual

This manual provides information about hardware, software, and network configurations for running various testing applications provided by American Institutes for Research (AIR).

The *System Requirements for Online Testing* lists the minimum hardware and software requirements for online testing. Ensure your hardware complies with those requirements before undertaking the tasks described in this manual.

Manual Content

This guide contains the following sections:

- Section I, Network Configuration and Testing, provides information about configuring networks, and lists helpful networking diagnostic tools.
- Section II, Hardware Configuration, provides guidance regarding the proper infrastructure for printers and wireless access points (WAP).
- Section III, Software Configuration, outlines configurations for operating systems (desktop, laptop, and mobile).
- Section IV, Text-to-Speech Requirements, outlines configurations for enabling text-to-speech settings on desktop operating systems. This section also lists the voice packs recognized by the secure browser on those operating systems.
- Appendix A, URLs Provided by AIR, lists AIR's URLs that should be whitelisted in your firewalls.
- Appendix B, Technology Coordinator Checklist, lists the activities required to prepare a facility for online testing.
- Appendix C, Scheduling Online Testing, provides a worksheet for estimating the required time to administer an online test.
- Appendix D, User Support, explains how to contact the help desk.

Document Conventions

Table 1 describes the conventions appearing in this user guide.

Table 1. Document Conventions

Element	Description
	**Note:** This symbol accompanies helpful information or reminders.
	**Warning**: This symbol accompanies information regarding actions that may cause loss of data.
	**Caution**: This symbol accompanies information regarding conflicting or incorrect configurations.
	**Tip:** This symbol accompanies advice about performing a task efficiently.
text	Boldface indicates an item you click or a drop-down list selection.
`filename`	Monospaced text indicates a directory, filename, or text you enter in a field or at the command line.

Intended Audience

This publication is intended for technology coordinators responsible for configuring the hardware, software, and network in a school's online testing environment. You should be familiar with the following concepts:

- Networking—Bandwidth, firewalls, whitelisting, and proxy servers.
- Configuring operating systems—Control Panel in Windows, System Preferences in OS X, Settings in iOS, and the Linux command line.
- Configuring web browsers—Settings in Chrome, Safari, Firefox, and Internet Explorer.

Other Resources

- For information about supported operating systems, see the *System Requirements for Online Testing*.

- For information about installing secure browsers, see the *Secure Browser Installation Manual*.
- For information about securing a computer before a test session, see the *Guide to Navigating the Online HSAP Administration*.
- For information about supported hardware and software for Braille testing as well as information about configuring JAWS see the *Braille Requirements and Testing Manual*.

The above resources as well as test administration manuals and user guides for other systems are available on the Hawai'i Statewide Assessment Program portal (alohahsap.org).

Section I. Network Configuration and Testing

Your network's configuration has a significant impact on Test Delivery System's (TDS) performance. An improperly configured network can slow a TDS's responsiveness, and possibly impact students' scores or an assessment's integrity. The following sections provide guidance on properly configuring your network, and list popular tools for diagnosing network bottlenecks.

Network Configuration

This section provides guidance or requirements pertaining to networking configurations for online testing.

General Requirements

A stable, high-speed (wired or wireless) Internet connection is required for online testing. The response time for each assessment depends on the reliability and speed of your school's Internet network.

If your Internet connection is not working or stops working, students will need to complete their tests at a later time or on another day. Any answers they have already submitted will be saved, and students will resume their tests where they left off. (Students will return to the first unanswered item in the test.)

For the online testing applications to work properly, you may need to verify your network settings. If you are not sure whether your network is properly configured or you have questions, contact your school's network administrator or technology specialist or your Complex Area IT Manager (see table below). Complex Area Information Technology Managers are available to provide support to the school technology coordinators or designated technology point(s) of contact. You may also contact the Hawai'i Statewide Assessment Program (HSAP) Help Desk.

Complex Area IT Manager	Complex Area
Ben Meyer	Section Head/Supervisor
Blain Shinno	Farrington-Kaiser-Kalani
Stuart Yasui	Kaimuki-McKinley-Roosevelt
Dean Yoshida	Aiea-Moanalua-Radford
Kory Takemoto	Leilehua-Mililani-Waialua
Jon Kinoshita	Pearl City-Waipahu
Jordan Higa	Campbell-Kapolei
Ramon Cordero	Nanakuli-Waianae
Daijo Kaneshiro	Kailua-Kalaheo
Nicholas Alexander	Castle-Kahuku
Grant Yamamoto	Hilo-Waiakea-Laupahoehoe

Paul Sakamoto	Kau-Keaau-Pahoa
Jennifer Morgan	Honoka'a-Kealakehe-Kohala-Konawaena
Peter Ah Kee	Baldwin-Kekaulike-Maui
Ross Uedoi	Hana-Lahaina-Lana'i-Molokai
Byron Kapali	Kapaa-Kauai-Waimea

Guidance for Determining Required Bandwidth

Bandwidth is the measure of a network's capacity or utilization, usually measured in terms of bits per second. Your network should have enough bandwidth to support online testing at the required performance level. For example, if a testing program requires that web browsers display test items within 10 seconds after sending a request, then the network must have enough bandwidth to support that requirement.

In an online testing environment, the following factors contribute to determining the required bandwidth:

- **Number of Students Simultaneously Testing**—As the number of students testing at one time increases, the required bandwidth also increases.

- **Size of the Test Content**—The size of a test's content is determined by two factors: (1) the number of items on the test and (2) the average size of each item. The more items a test contains and the larger the average test item, the higher the bandwidth requirement for a given test. For example, some writing tests have a few questions to which the student composes a response, and these tests are small. In contrast, some science tests have animations or simulations; these tests are large.

- **Hubs or Switches**—LAN performance can be hindered when hubs are used instead of switches. A hub broadcasts signals from various network devices to propagate across the network, potentially saturating the network and causing traffic competition or data collisions. If you use hubs, ensure they have enough bandwidth to handle the propagation.

- **ISP Router**—For Internet networks, the most common bottleneck is the ISP's router connection, which typically operates at speeds of between 1.5M bits per second and 100M bits per second. Network administrators should spend time prior to test administration determining if their Internet infrastructure has the capacity to accommodate online testing at the required performance level.

- **Encryption**—Encryption at WAPs may contribute to bandwidth usage. If you use encryption, ensure the WAPs have enough bandwidth to prevent degradation of performance.

- **Required Response Time**—When a network's bandwidth cannot service the amount of data requested by clients, latency starts to accumulate and the students experience delays. Ensure your network's bandwidth is high enough to support the required response times between the browsers and the servers.

Table 2 displays the estimated average bandwidth used by the secure browser for testing. When designing your network for online testing, ensure that the available bandwidth can support these values.

Table 2. Average Bandwidth Used by Secure Browser for Testing

Number of Students Testing Concurrently in School or Building	Average Estimated Bandwidth Consumed During Subsequent Startup of Secure Browser[a]	Average Estimated Bandwidth Consumed During Testing[b]
1	8K bits/second	5–15K bits/second
50	400K bits/second	250–750K bits/second (0.25–0.75M bits/second)
100	800K bits/second	500–1500K bits/second (0.5–1.5M bits/second)

[a] Bandwidth consumed when opening the secure browser and accessing an assessment for the first time is significantly more than when opening the secure browser and accessing an assessment subsequently. This is because the initial launch of the secure browser downloads non-secure cacheable content (not test content) that can be immediately accessed upon opening the secure browser later.

[b] The values in this column are based on averages from tests in a variety of subjects.

Required Ports and Protocols

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)

Configuration for Domain Name Resolution

Appendix A, URLs Provided by AIR, lists 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 Session Timeouts

Session timeouts on proxy servers and other devices should be set to values greater than the average time it takes a student to participate in a test session or to complete a given test. For example, if your school determines that students will test in 60-minute sessions, then consider setting the session timeout to 65 or 70 minutes.

Data Caching

Data caching is a technique by which an intermediate server checks if it can serve the client's requests instead of a downstream server. While data caching is a good strategy in some situations, its overhead is detrimental in the online testing environment. Ensure all intermediate network elements, such as proxy servers, do not cache data.

Configuring Quality of Service and Traffic Shaping

If your testing network includes devices that perform traffic shaping, packet prioritization, or Quality of Service (QoS), ensure the URLs in Appendix A, URLs Provided by AIR, have high priority.

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.

Certificate Revocation List

To use a certificate revocation list, ensure your firewalls allow the URL http://crl.verisign.com/.

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.

Table 4. 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**.**

   a. Go to step 1 of the **Note** under the **Important Service Announcement** on this page**.**

   b. Click the **Get the full list of IP addresses** link.

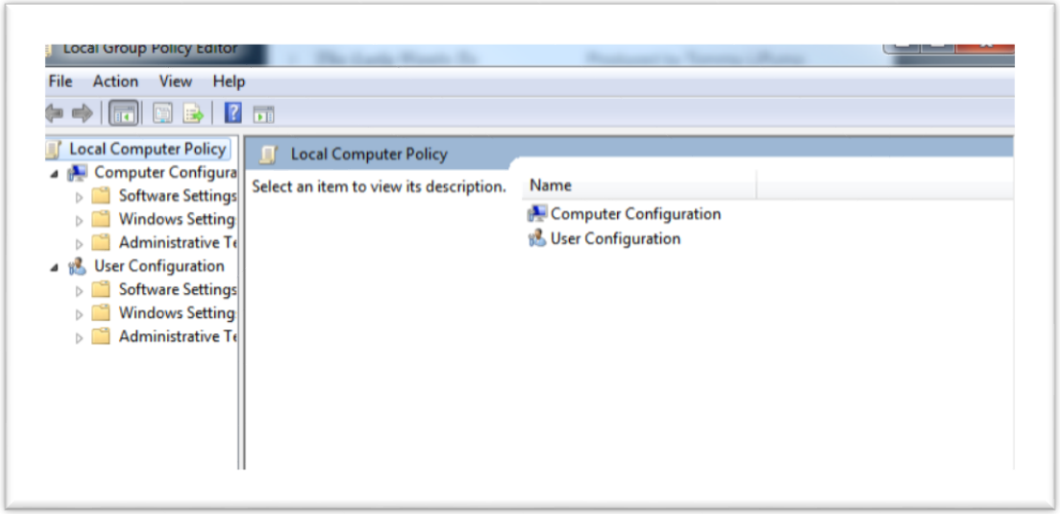
2. Complete the short form then click **Continue** to gain access to the most current list.

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

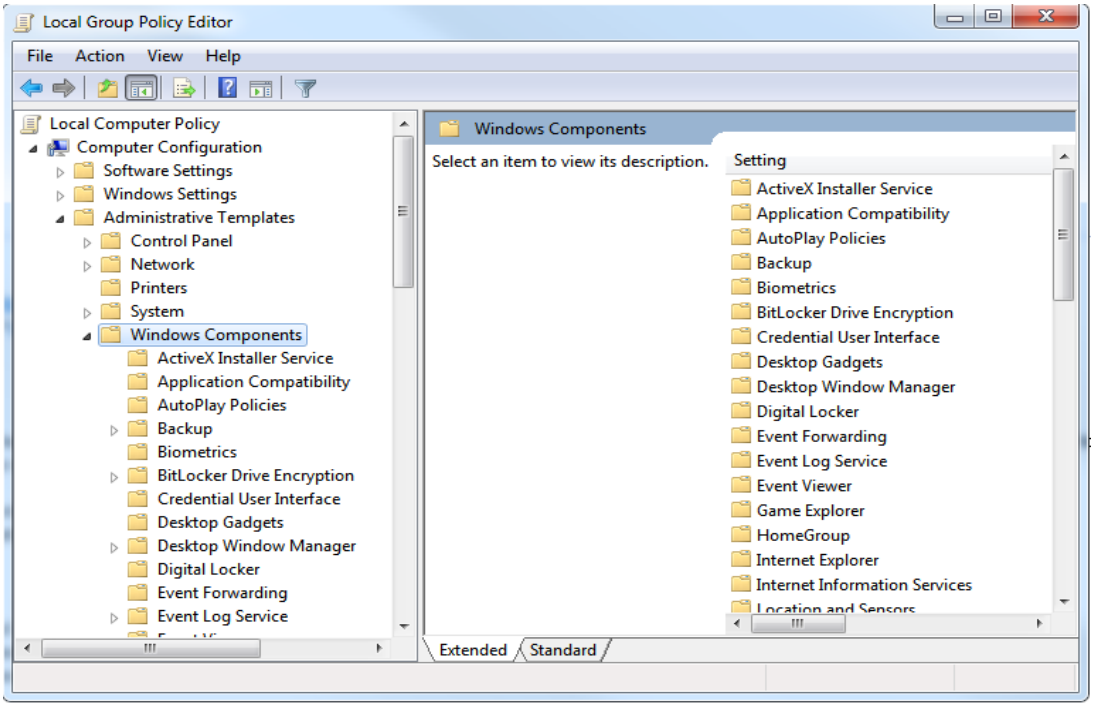
Blocking Device Touch Input Using the Group Policy Editor

Some tablets and devices have Touch features that may need to be disabled before testing. The following procedure describes how to disable the Touch feature on these devices using the Group Policy Editor:

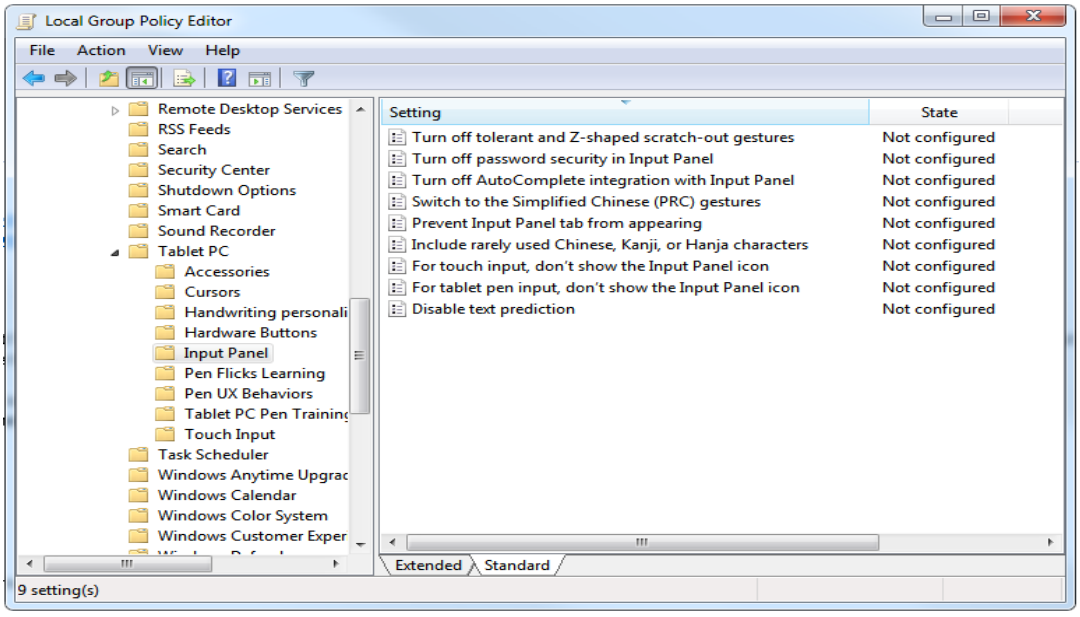
1. Type gpedit.msc in the *Search* box on the **Start** menu. The ***Local Group Policy Editor*** window appears.



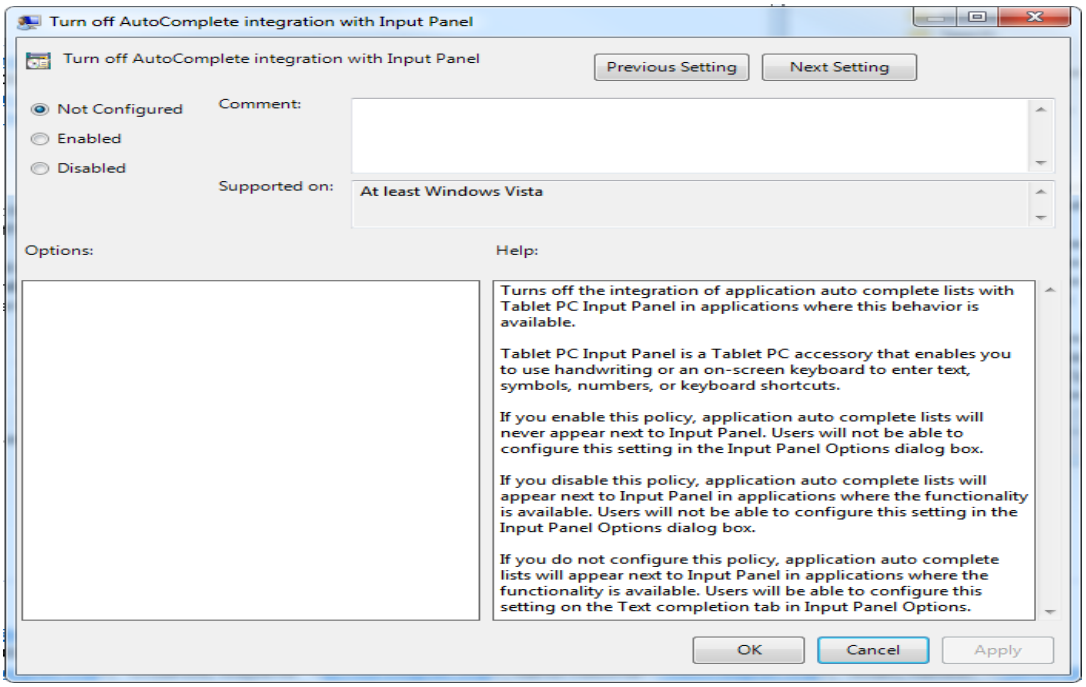
2. Navigate to **Computer Configuration\Administrator Templates\Windows Components**



3. Scroll down to the **Tablet PC** folder, then select **Input panel**. The following screen displays.



4. Enable the following items in the *Setting* column:
    a. Turn off AutoComplete integration with Input Panel
    b. Prevent Input Panel tab from appearing
    c. For tablet pen input, don't show the Input Panel icon
    d. For touch input, don't show the Input Panel icon
    e. Disable text prediction
5. To enable an item in the *Setting* column, double-click on that item. The following screen will display that will allow you to enable or disable your selected item as required.



6. Select **Enabled**, and click **OK**.
7. Close the ***Local Group Policy Editor*** window.

Network Diagnostic Tools

You should do a performance analysis of your networking infrastructure to identify any bottlenecks that may impact test performance. The choice of diagnostic tool depends on the operating system running the tool, the network administrator's technical knowledge, and the desired level of network analysis. A number of network diagnostic tools are available, as described in the following sections.

AIR's Network/Bandwidth Diagnostic Tool

AIR provides a diagnostic tool that can be directly accessed from the student sample test login page.

1. On the sample test login page, click **Run Diagnostics**. The ***Diagnostic Screen*** page opens.

2. In the *Network Diagnostics* section, select a test.

3. Select the approximate number of students who may take that test *at one time*.

4. Click **Run Network Diagnostics Tests**.

The tool displays your current upload and download speed as well as a general idea of whether you can reliably test the number of students you entered in step 3. You may want to run this test several times throughout the day to verify that your upload and download speeds remain relatively consistent.

Windows-Specific Tools

PRTG Traffic Grapher

PRTG (www.paessler.com/prtg) monitors bandwidth usage and other network parameters via Simple Network Management Protocol (SNMP). It also contains a built-in packet sniffer. A freeware version is available.

NTttcp

NTttcp (www.microsoft.com/whdc/device/network/TCP_tool.mspx) is a multithreaded, asynchronous application that sends and receives data between two or more endpoints and reports the network performance for the duration of the transfer.

Pathping

Pathping is a network utility included in Windows. It combines the functionality of the `ping` and `tracert` commands by providing details of the path between two hosts and ping-like statistics for each node in the path based on samples taken over a time period.

OS X-Specific Tools

Network Utility.app

This tool is built into OS X.

Multi-Platform Tools

Wireshark

Wireshark (www.wireshark.org) is a network protocol analyzer. It has a large feature set and runs on most platforms including Windows, OS X, and Linux.

TCPDump

TCPDump (http://sourceforge.net/projects/tcpdump) is a common packet sniffer that runs from the command line on Linux and OS X. It can intercept and display data packets being transmitted or received over a network. A Windows version WinDump is available (www.winpcap.org/windump/).

Ping, NSLookup, Netstat, Traceroute

This is a set of standard UNIX network utilities. Versions of these utilities are included in Linux, Windows, and OS X.

Iperf

Iperf (http://sourceforge.net/projects/iperf/) measures maximum TCP bandwidth, allowing the tuning of various parameters and User Datagram Protocol (UDP) characteristics. Iperf reports bandwidth, delay jitter, and datagram loss.

Section II. Hardware Configuration

This section provides topology guidance for printers and WAPs. It also provides a reference for hardware configurations that support Braille testing.

Connections between Printers and Computers

Test Administrators can print test session information and approve students' requests to print stimuli or test items (for students with the print-on-request accommodation). Nevertheless, to maintain a secure test environment, the Test Administrator's computer should be connected to a single local or network printer in the testing room, and only the Test Administrator's computer should have access to that printer.

Wireless Networking and Determining the Number of Wireless Access Points

Wireless networking standards have evolved over the years, with the following being the most commonly deployed:

- 802.11ac has a theoretical throughput of up to 1G bits per second.
- 802.11n has a throughput of up to 300M bits per second.
- 802.11g has a theoretical throughput of up to 54M bits per second.
- 802.11b has a theoretical throughput of 11M bits per second.

The recommended number of devices supported by a single wireless connection depends on the standard used for the connection. The two most common networking standards are 802.11g (54Mbps) and 802.11n (300Mbps). Table 5 lists recommendations for network topology in which the WAP provides 802.11g and the testing devices provide 802.11g, 802.11n, or a mixture of the two. Refer to your WAP documentation for specific recommendations and guidelines for these or other standards.

Table 5. Recommended Ratios of Devices to Wireless Access Points

Testing Device	Ratio of Devices to 802.11g WAP	Ratio of Devices to 802.11n WAP
802.11g	20	40
802.11n	20	40
Mix of 802.11g and 802.11n	20	40–50 (depending on the mix of wireless cards used)

Recommendations for 802.11ac routers are under investigation.

Regardless of the number of WAPs, each should be configured to use WPA2/AES data encryption.

Hardware for Braille Testing

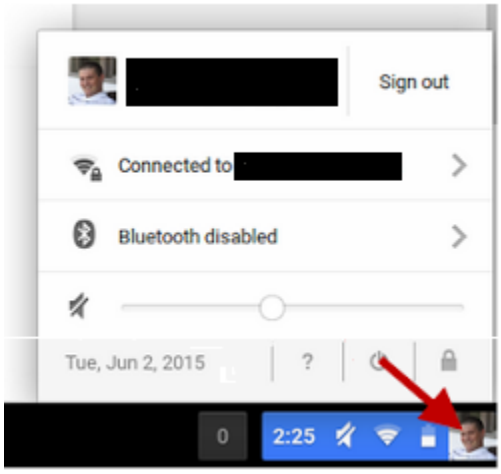
For information about Braille hardware and software requirements, refer to the *Braille Requirements* document, which is available on the Hawai'i Statewide Assessment Program portal (alohahsap.org).

Turning off ChromeVox

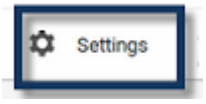
Some Chromebook users may find that ChromeVox reads the non-test elements of the secure browser and the test, which poses a security issue. Users will need to disable this before starting to test.

To disable ChromeVox before launching the Secure Browser:

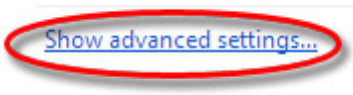
1. Sign in to your Chromebook.
2. Click the status area, where your account picture appears, or press **Alt** + **Shift** + **s**.



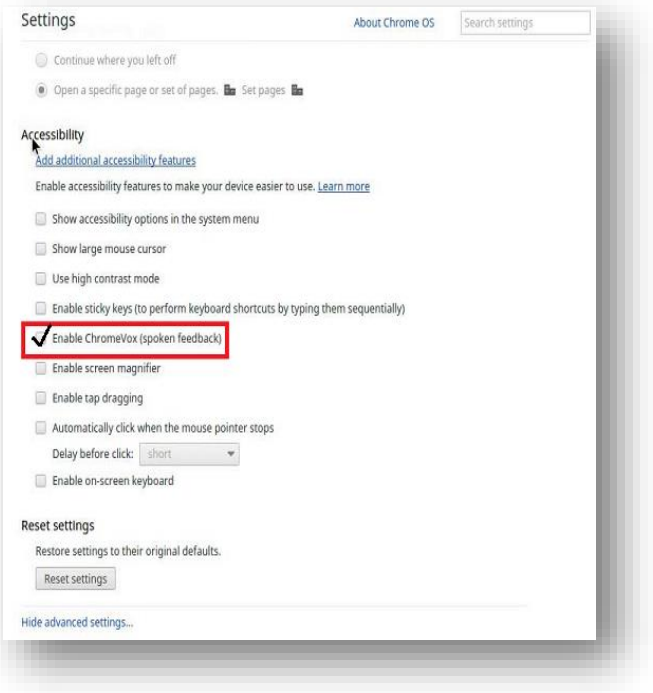
3. Click **Settings**.



4. At the bottom, click **Show advanced settings,** which will be at the bottom of the page.



5. In the "Accessibility" section, uncheck the box to turn off ChromeVox (Spoken feedback).



In the case that the Secure Browser has already been launched, you can use the following keyboard command to disable ChromeVox: **Ctrl + Alt + Z.**

Section III. Software Configuration

This section describes how to configure the operating systems and web browsers for online testing.

Warning: Support for All Operating Systems on Devices Used for Testing

Operating systems that become available but do not appear on the Supported Browsers page on the portal (alohahsap.org) are not supported. Do not upgrade to new operating systems on computers that will be used to administer online assessments without ensuring the updates meet the required specifications.

Configuring Commercially Available Browsers

This section describes how to configure commercially available browsers (Chrome, Safari, Firefox, and Internet Explorer) for online testing.

Enabling Pop-Up Windows

AIR's systems provide informational messages or warnings using pop-up windows. Therefore, enable pop-up windows on those web browsers using AIR's systems.

The following list describes how to enable pop-up windows on many browsers. If your browser is not on this list, consult its user documentation.

Enabling Pop-Up Windows for All Domains

The following instructions enable pop-up windows for *all domains*. If you prefer to limit pop-up windows to only those coming from AIR's domains, use the instructions in Enabling Pop-Up Windows only for AIR domains.

- **Chrome:** Menu > Settings > Show advanced settings (at the bottom of the screen) > Privacy > Content Settings > Pop-ups > mark **Allow all sites to show pop-ups**.
- **Chrome browser on Android tablets**: Menu > Settings > Advanced > Content Settings > Block pop-ups > clear checkbox.
- **Firefox (Windows):** Tools > Options > Content > clear **Block pop-up windows**. (Firefox on OS X and Linux is similar.)
- **Internet Explorer:** Internet Options > Privacy tab > clear **Turn On Pop-up Blocker**.
- **iOS Safari:** Settings > Safari > Block Pop-ups (toggle to "off" mode).
- **Safari:** Safari > clear **Block Pop-Up Windows**.

Enabling Pop-Up Windows only for AIR domains

You can allow pop-up windows only from AIR's domains. The following list describes how to enable domain-specific pop-up windows on many browsers. If your browser is not on this list, consult its user documentation. The list of AIR domains to use in these instructions appears in Appendix A, URLs Provided by AIR.

- **Chrome:** Menu > Settings > Show advanced settings (at the bottom of the screen) > Privacy > Content Settings > Pop-ups > click **Manage Exceptions**. Enter the domain names and select **Allow** for each.
- **Chrome on Android tablets:** N/A
- **Firefox:** Tools > Options > Content > click **Exceptions**. Enter domain names and select **Allow** for each.
- **Internet Explorer:** Internet Options Privacy tab > Settings. Enter the domain names and click **Add** for each.
- **Safari and iOS Safari:** N/A

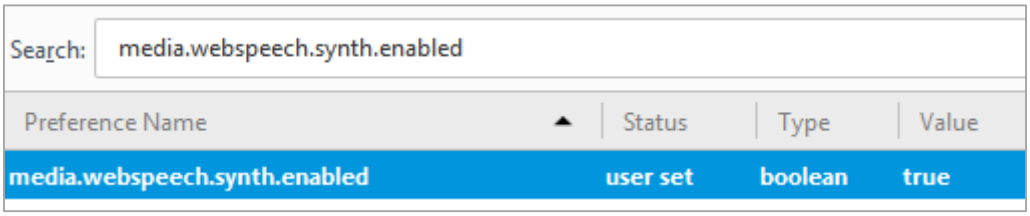
Enabling Text-To-Speech on Firefox

Firefox versions 45 and later includes a webspeech feature that provides text-to-speech. By default this feature is disabled. If you want to use webspeech with Firefox, enable it using the following procedure.

To enable webspeech on Firefox

1. In the Firefox address bar, type `about:config`. A warning appears.
2. Click **I'll be careful, I promise**. A list of preferences appears.
3. In the *Search* field, type `media.webspeech.synth.enabled`.
4. Double-click the preference so that its value changes to `true`. See Figure 1.

Figure 1. Enabling webspeech on Firefox



5. Restart Firefox.

Optimal Installation Scenario for Secure Browsers

The *Secure Browser Installation Manual* describes several scenarios for installing the secure browser. Some scenarios describe how to install the secure browser into a shared network folder, and students run the secure browser from that folder. This is arguably the fastest way to deploy the secure browser in a testing environment, but there are some performance impacts. Running the secure browser creates competition among the students' clients for two resources: LAN bandwidth and shared disk drive. This performance impact can be avoided by installing the secure browser locally on each machine.

Configuring Windows for Online Testing

This section describes how to configure Windows for online testing.

Disabling Fast User Switching

Microsoft Windows (Vista, 7, 8.0, 8.1, 10, and 11) has a "Fast User Switching" feature that allows more than one user to be logged in at the same time. This is a security risk because students can potentially start a new Windows session during the test and use that session to search the Internet for answers. The following sections describe how to disable Fast User Switching for different versions of Windows.

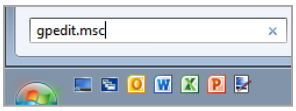
Disabling Fast User Switching in Windows Vista and 7

This section describes how to disable Fast User Switching under Windows Vista and Windows 7. The process is similar for later versions of Windows.

Option A: Access the Group Policy Editor

The following procedure describes how to disable Fast User Switching using the Group Policy Editor. Some editions of Windows Vista do not support this configuration through the Group Policy Editor; in such cases, configure Fast User Switching through the registry. See Option B below for instructions.

1. Click **Start**, type `gpedit.msc` in the search box.
   The Local Group Policy Editor window appears.

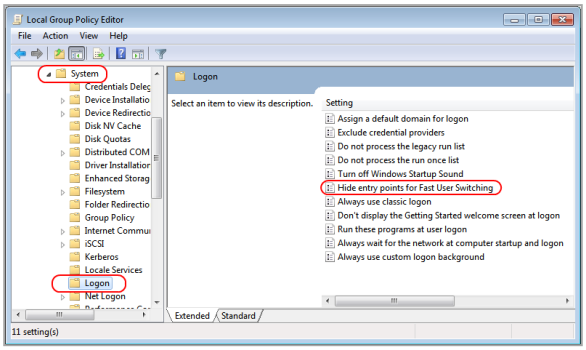


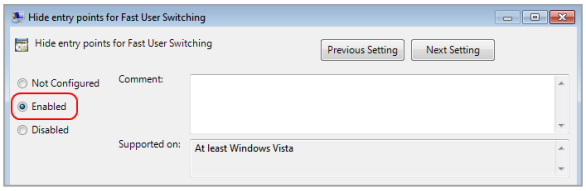
2. Navigate to `Local Computer Policy > Computer Configuration > Administrative Templates > System > Logon`.

3. Double-click **Hide entry points for Fast User Switching**.

4. Select **Enabled**, and click **OK**.

5. Close the Local Group Policy Editor window.

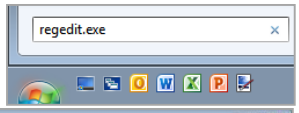


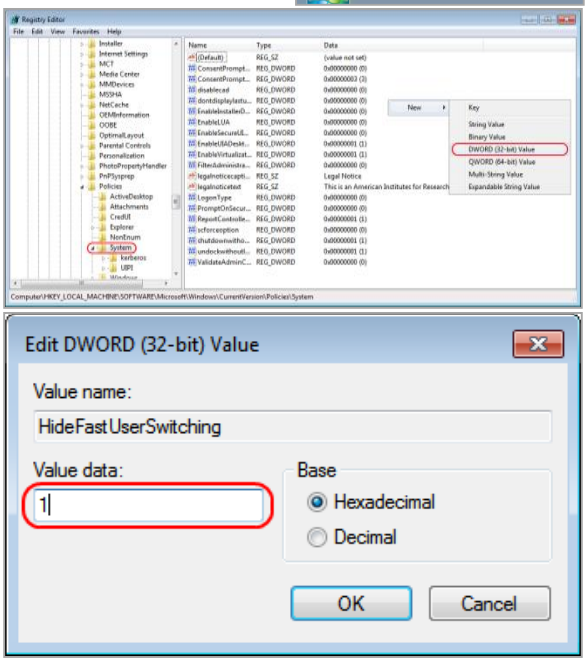


Option B: Access the Registry

The following procedure describes how to disable Fast User Switching using the Windows registry.

1. Click **Start**, type `regedit.exe` in the **Start Search** dialog box, and press **Enter**.
2. Navigate to `HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Windows > CurrentVersion > Policies > System`.
3. Right-click the **System** folder.
4. Click **New, DWORD (32-bit) value**.
5. Type `HideFastUserSwitching` and press Enter.
6. Double-click the **HideFastUserSwitching** value.
7. In the **Value data** field, enter `1`.
8. Click **OK**.
9. Close the Registry Editor.

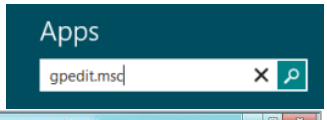


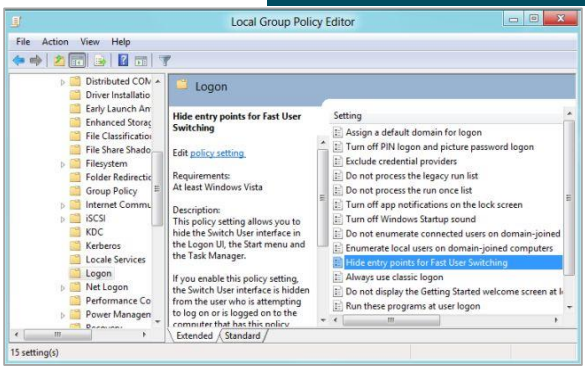


Disabling Fast User Switching in Windows 8.0 and 8.1

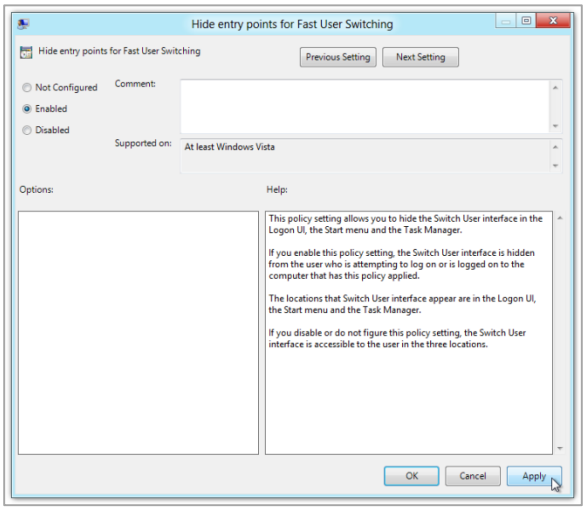
The following procedure describes how to disable Fast User Switching under Windows 8.0 and 8.1.

1. In the Search charm, type `gpedit.msc`. Double-click the gpedit icon in the Apps pane. The Local Group Policy Editor window opens.
2. Navigate to `Computer Configuration > Administrative Templates > System > Logon`.
3. In the Setting pane, double-click **Hide entry points for Fast User Switching**.



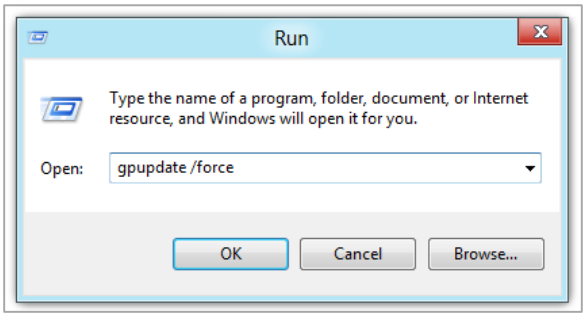


4. Select **Enabled** and then click **OK**.

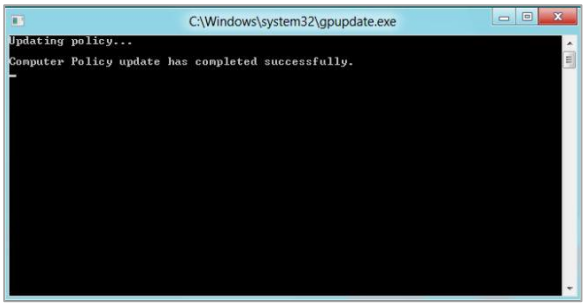


5. In the Search charm, type `run`. The Run dialog box opens.

6. Enter the command `gpupdate /force` into the text box and then click **OK**. (Note the space before the backslash.)



7. The command window opens. When you see the message `Computer Policy update has completed successfully`, this will be your notification that Windows has successfully disabled Fast User Switching.

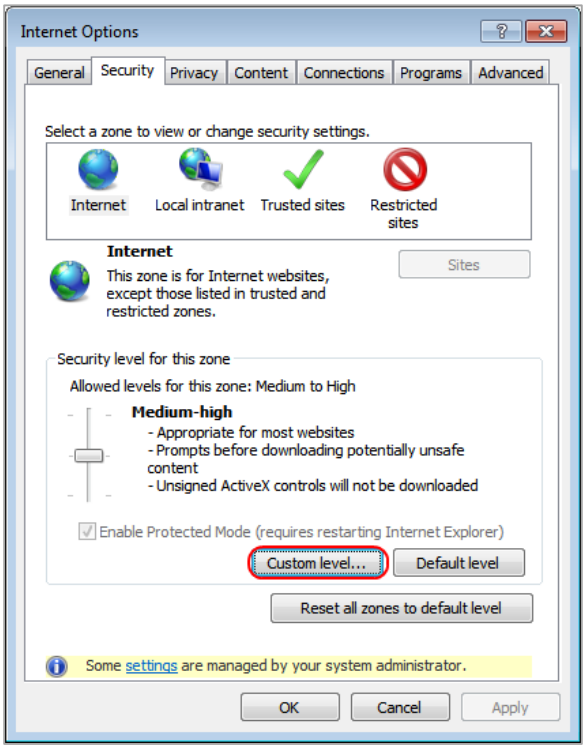


Enabling Web Fonts in Internet Explorer 11

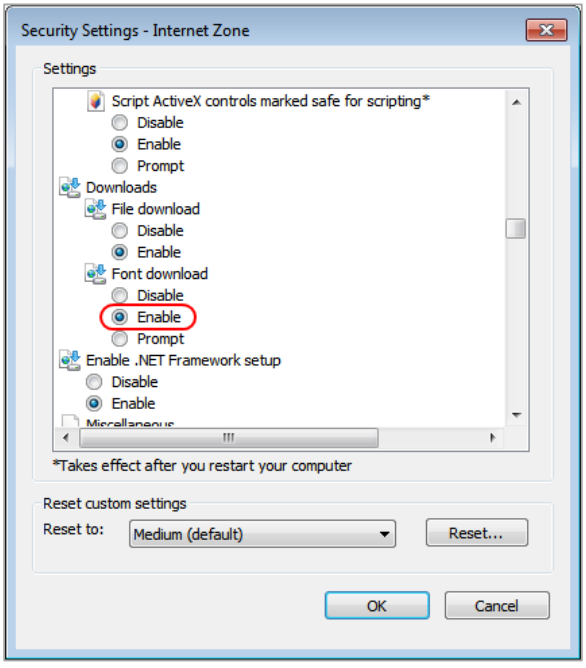
Some applications, such as sample tests or THSS, display test items that may require web fonts. The following procedure describes how to enable web fonts in Internet Explorer 11.

To enable web fonts in Internet Explorer:

1. In Internet Explorer, open the tools menu and select **Internet Options**. The Internet Options dialog box opens.
2. Click the **Security** tab.
3. Click the **Custom Level** button. The Security Settings dialog box opens.



4. Scroll to `Font Download` and mark the **Enable** radio button.
5. Click **OK**. The Security Settings dialog box closes.
6. Click **OK**. The Internet Options dialog box closes.



Installing Windows Media Pack for Windows 8.1 N and KN

Some versions of Windows 8.1 are not shipped with media software installed. As a result, you may need to install software to enable students to listen to and record audio as well as watch videos.

Microsoft provides additional information as well as a download package for computers with the following Windows 8.1 versions:

- Windows 8.1 N
- Windows 8.1 N/K with Bing
- Windows 8.1 Enterprise N
- Windows 8.1 Pro N
- Windows 8.1 Pro N/K for EDU

AIR encourages downloading this software and ensuring it works with sample websites and video and audio files prior to installing the Windows secure browser. Installation instructions are provided on Microsoft's download page.

Microsoft Resources:

- About the Media Feature Pack for Windows 8.1 N and Windows 8.1 KN Editions: April 2014 (http://support.microsoft.com/kb/2929699/en-us)
- Download Media Feature Pack for N and KN Versions of Windows 8.1 (http://www.microsoft.com/en-us/download/details.aspx?id=42503)

Configuring ZoomText to Recognize the Secure Browser

When displaying a test with a print-size accommodation above 4× magnification, the secure browser automatically enters streamlined mode. If you want to retain the standard layout of a test but display it with a print magnification above 4×, then consider using ZoomText—a magnification and screen-reading software that you can use with the secure browser.

1. If ZoomText is running, close it.
2. In the Windows Explorer, go to the installation directory for your version of ZoomText. For example, if you have ZoomText version 10.1:
    - Go to `C:\Program Files (x86)\ZoomText 10.1\` (Windows 64-bit)
    - Go to `C:\Program Files\ZoomText 10.1\` (Windows 32-bit).
3. In a text editor, open the file `ZoomTextConfig.xml`.

4. Search for line containing the `D2DPatch` property, similar to the following:

```
<Property name="D2DPatch" value ="*,~dwm,~firefox,~thunderbird"/>
```

5. In the `value` attribute, add the prefix for your state's secure browser:

```
<Property name="D2DPatch" value
="*,~dwm,~firefox,~hisecurebrowser,~thunderbird"/>
```

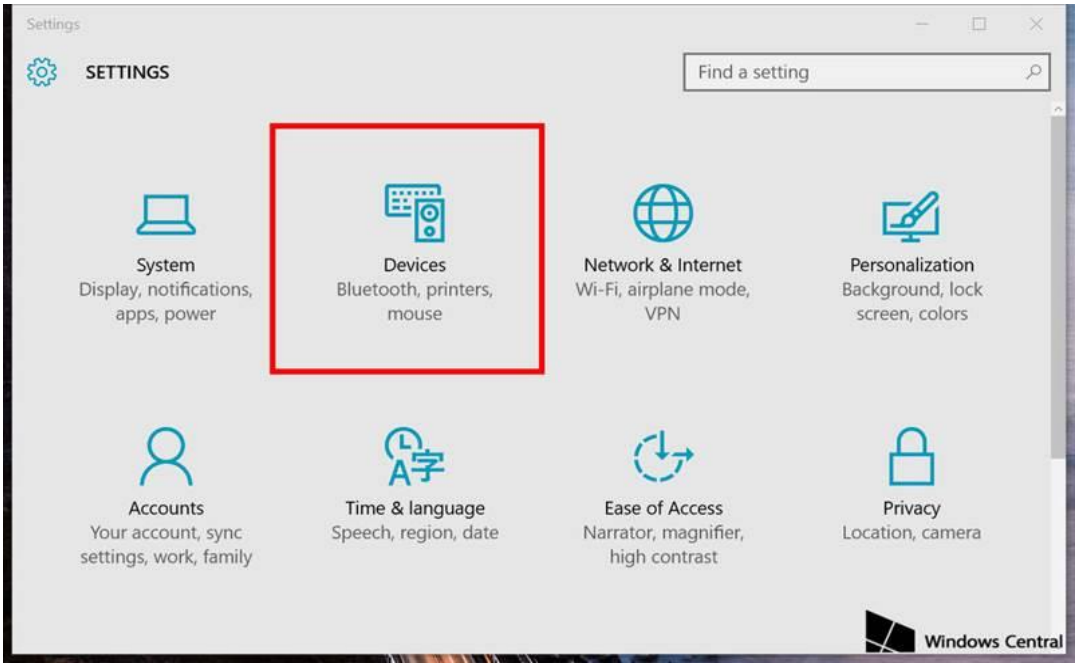
6. Save the file, and restart ZoomText.

Touch Keyboard on Microsoft Surface Pro 3 Tablet

Some Surface Pro 3 users accessing the touch keyboard are seeing the touch keyboard disappear when they click outside a text box or when they type an answer into a text box and then click next. The keyboard fails to reappear when users click back inside the next text box. To avoid these issues, users must set the touch keyboard to automatically show up.

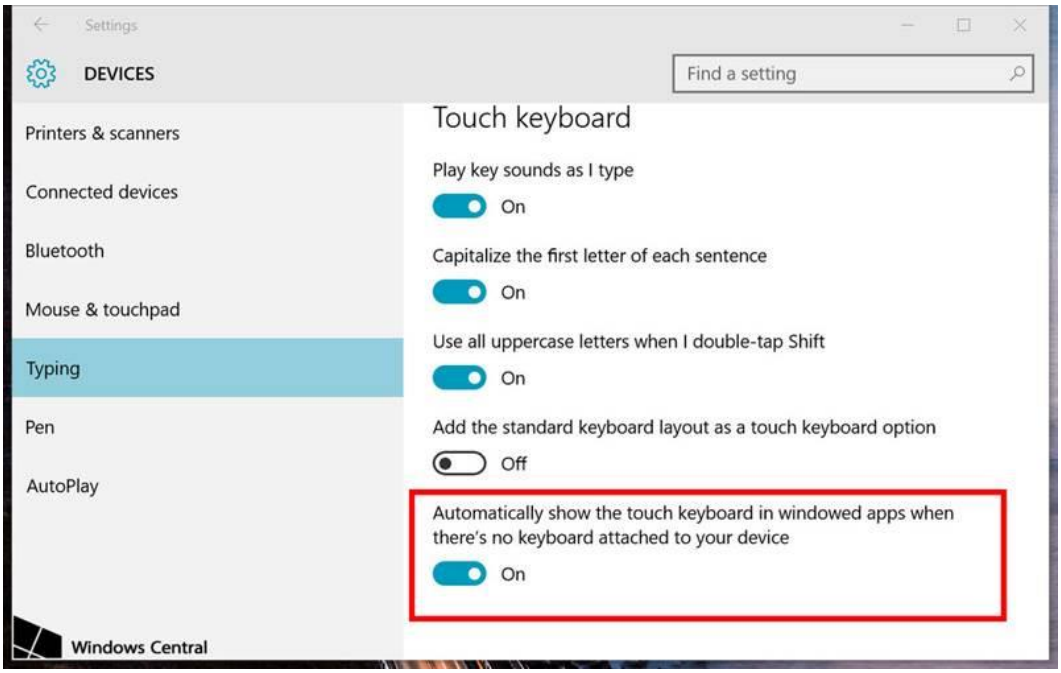
To set the touch keyboard to automatically show up:

1. Go to **Settings** (keyboard shortcut: **Windows + I**)



2. Go to **Devices** > **Typing**

3. Scroll down and toggle on: *Automatically show the touch keyboard in windowed apps when there's no keyboard attached to your device*.



Configuring Mac OS X for Online Testing

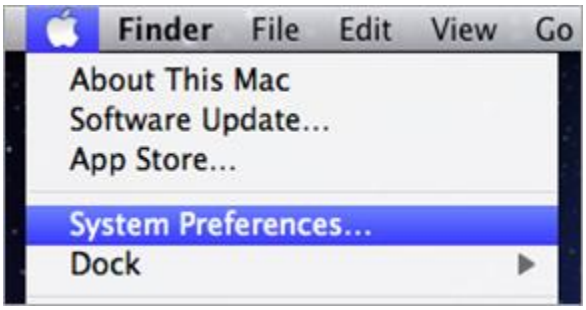
This section describes how to configure Mac OS X for online testing.

Disabling Exposé or Spaces

Mac OS X 10.7 and later includes an Exposé or Spaces feature that allows running more than one desktop session. This is a security risk because students can potentially start a new desktop session during the test, and use that session to search the Internet for answers. The following procedure explains how to disable Exposé or Spaces on those versions of OS X. (You can disable Spaces quickly from the command line; see Disabling Spaces and Application Launches from the Command Line for details.)

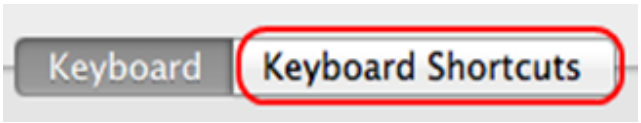
To disable Exposé or Spaces:

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

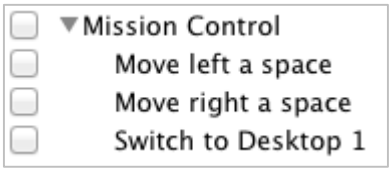


2. Click **Keyboard**. The Keyboard window opens.

3. Click the **Keyboard Shortcuts** or **Shortcuts** tab.



4. In the left panel, click **Mission Control**. The right panel lists all Mission Control options.
5. In the right panel, clear the following checkboxes:
   - Move left a space
   - Move right a space
   - Switch to Desktop 1



To re-enable Exposé or Spaces, follow steps 1–4, and mark the boxes for spaces.

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 10.7 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.

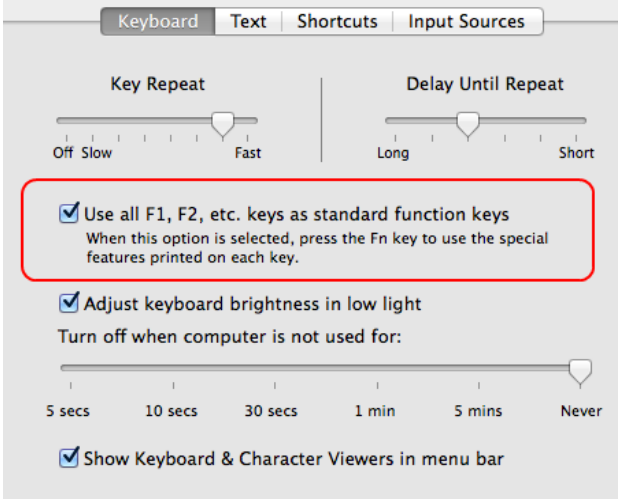
The following instructions are based on OS X 10.9; similar instructions apply for other versions of OS X. (You can disable application launches quickly from the command line; see Disabling Spaces and Application Launches from the Command Line for details.)

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.)



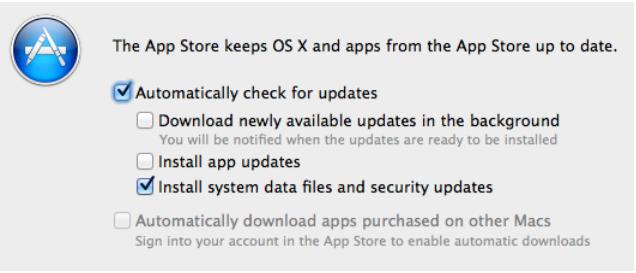
Disabling Updates to Third-Party Apps

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 OS X.

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**.

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 OS X.

To disable updates to iTunes:

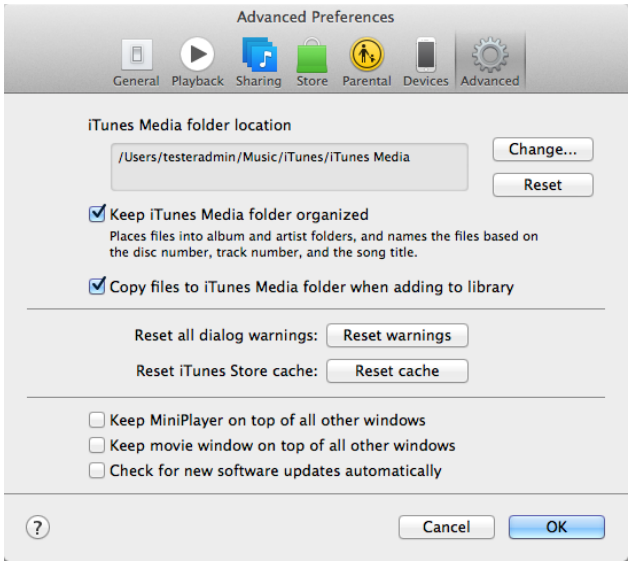
1. Log in to the student's account.

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 10.7 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 OS X.

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.

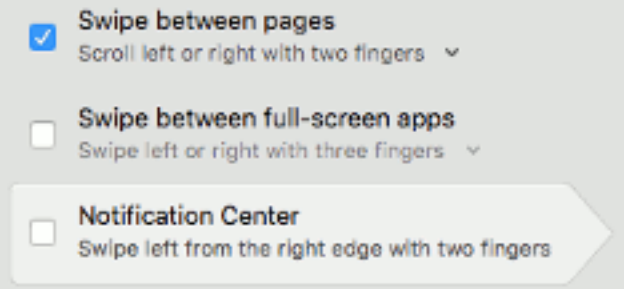
Disabling Display of Notification Center

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 OS X.

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 Exposé or Spaces and Disabling Application Launches from Function Keys describe how to configure OS X 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 OS X 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 10.8.5 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 Exposé or Spaces, 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 OS X. This configuration is stored in the file `~/Library/Preferences/com.apple.symbolichotkeys.plist`. If you have many OS X 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:

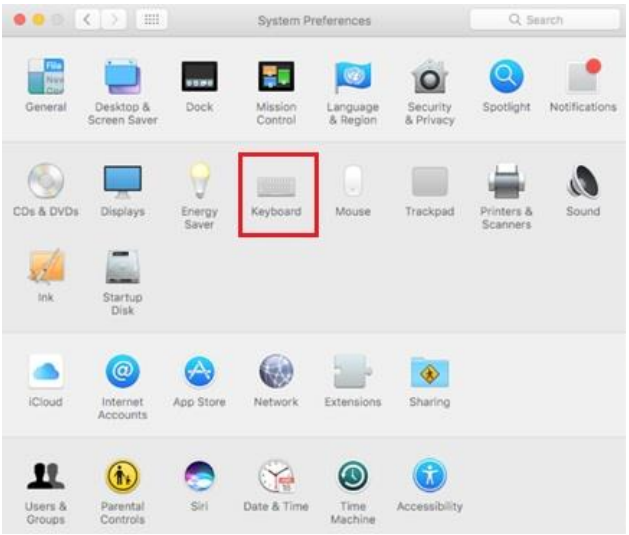
- File Distributor
- Apple's Active Directory Client and Directory Utility
- Apple's Open Directory and Profile Manager
- Centrify & PowerBrokers Identity Enterprise
- Apple Remote Desktop

Disabling Dictation and Siri

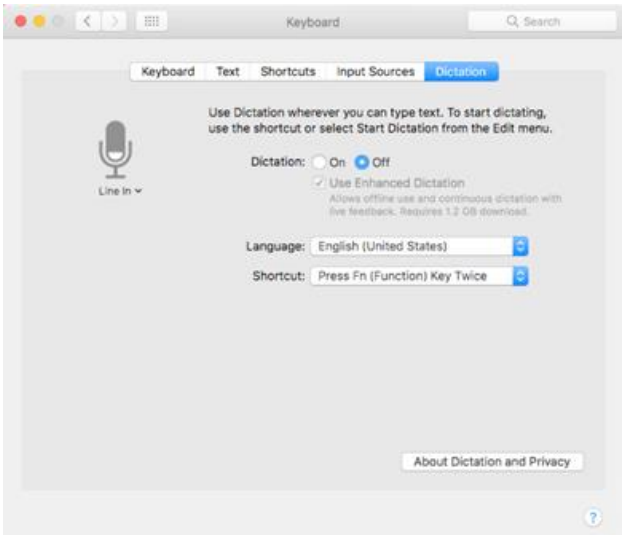
As students can speak into an OS X device utilizing the dictation feature which suggests words or spellings that may compromise testing security. Use the following procedure to disable dictation.

*To disable **Dictation** in an OS X device:*

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

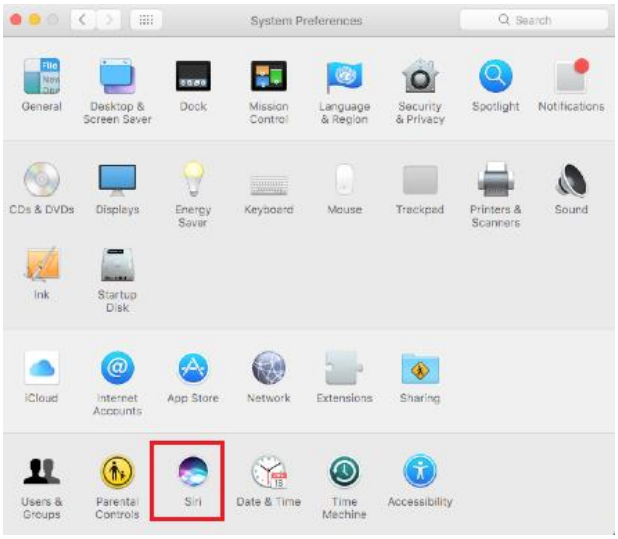


2. Turn the **Dictation** option to **Off**.

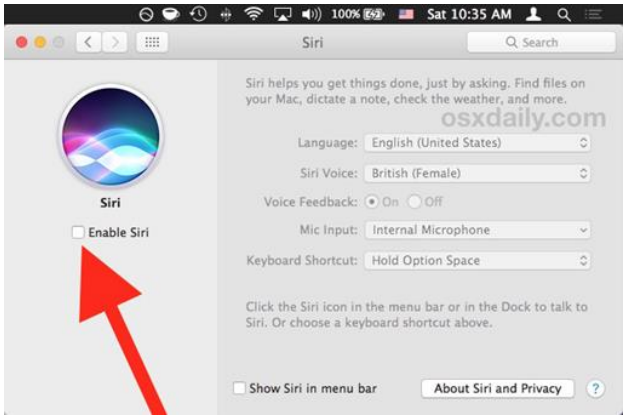


To disable the Siri feature:

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



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

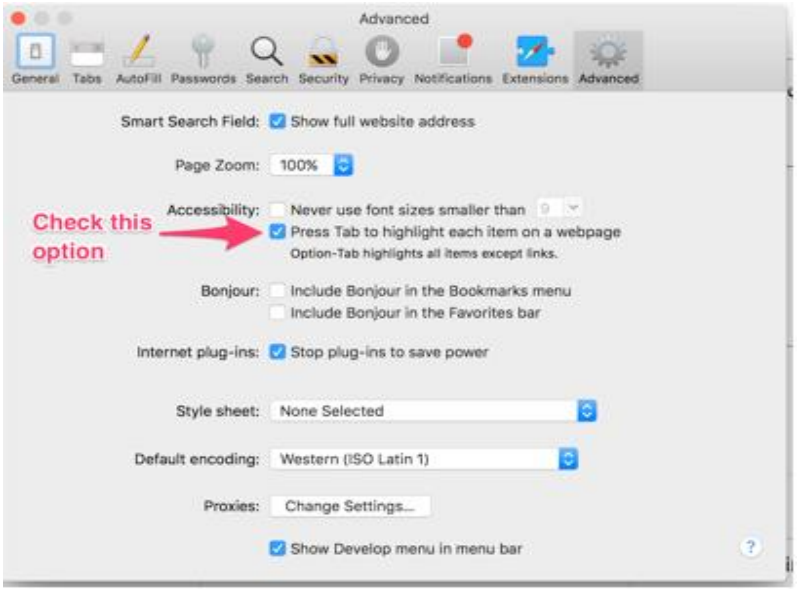


With Siri disabled, the menu bar icon is removed, the Dock icon is hidden, the Tool Bar icon is removed (if applicable to your Mac), and the Siri service is completely turned off and unable to activate for any reason.

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 that have Text-to-Speech accommodation enabled for practice tests will need to use Secure Browser.



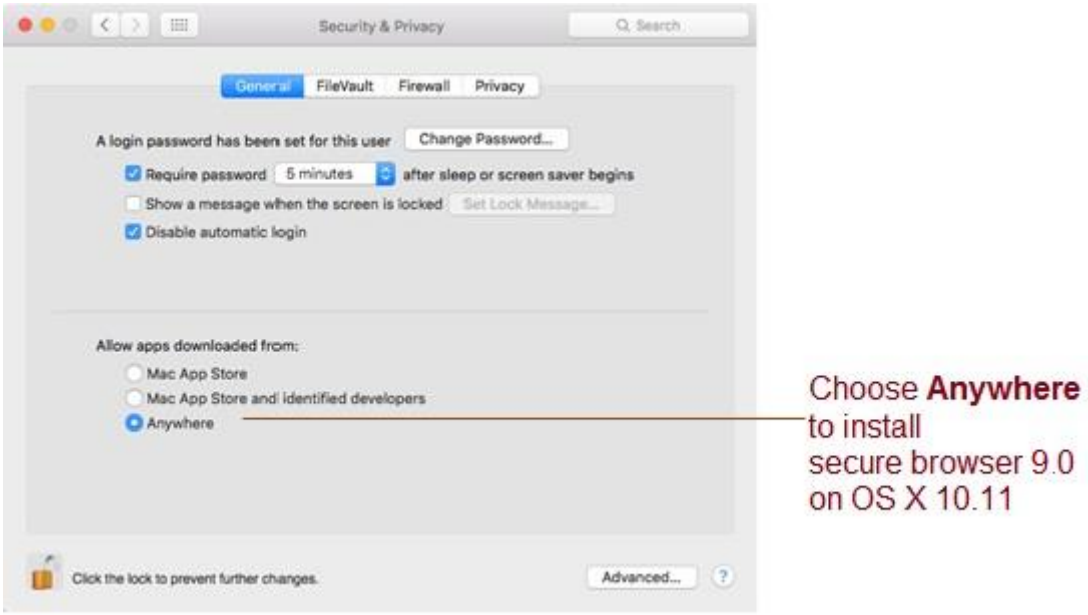
Preparing to Install Secure Browser 9.0 or later on OS X 10.11

When installing a new copy of Secure Browser 9.0 or later on OS X 10.11 (El Capitan), Gatekeeper indicates the program is from an unidentified source. This is because Gatekeeper does not recognize the secure browser's application signature. You need to adjust OS X's security settings prior to the installation, and then reset the settings after the installation. (Gatekeeper does recognize the secure browser's installation signature when *upgrading* to Secure Browser 9.0 or later on OS X 10.11, so you do not need to perform this procedure when upgrading.)

To prepare OS X 10.11 for installing Secure Browser 9.0 or later:

1. Open **System Preferences**.
2. Choose **Security and Privacy**.
3. Under **General**, click the lock and type your password to enable changes.

4. Under **Allow apps downloaded from**, choose **Anywhere**, and choose **Allow From Anywhere** in the confirmation message.



5. Install the secure browser. Detailed installation instructions are available in the *Secure Browser Installation Manual*.

6. After installing the secure browser, restore your security settings.

Configuring Linux for Online Testing

This section describes how to configure Linux for online testing.

Adding Verdana Font

Some tests have content that requires the Verdana TrueType font. Therefore, ensure that Verdana is installed on Linux machines used for testing. The easiest way to do this is to install the Microsoft core fonts package for your distribution.

- Fedora, Red Hat, and openSUSE—Follow the steps in the "How to Install" section of the following website: http://corefonts.sourceforge.net/.

- Ubuntu—In a terminal window, enter the following command to install the msttcorefonts package:

```
sudo apt-get install msttcorefonts
```

Configuring iOS

This section describes how to configure mobile devices running iOS.

Configuring for Guided Access

Guided Access restricts the iOS to a single application and prevents taking screenshots. This ensures a secure test environment. (You may want to use Single App mode, which is easier to enable and activate than Guided Access; for more details about this configuration, see Configuring Using Autonomous Single App Mode.)

The procedure in this section only *enables* Guided Access; to *activate* Guided Access before a test, see the *Guide to Navigating the Online HSAP Administration*.

To configure for Guided Access:

1. Tap **Settings**.

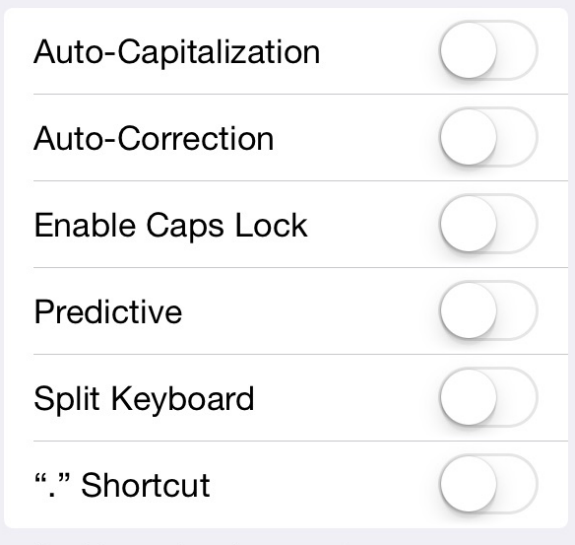
2. Navigate to General > Accessibility > Learning, and turn on **Guided Access**.
3. Set the passcode for Guided Access. (Test Administrators use this passcode to deactivate Guided Access after a test.)
   a. Tap **Set Passcode**.
   b. Enter a passcode.
   c. Confirm the passcode.
4. Save the passcode in a safe place. There is no ability to retrieve a forgotten passcode.

5. On devices with iOS 7 or later, disable keyboard functions by doing the following:

   a. Under **Settings**, tap **General** > **Keyboard**.

   b. Turn off all settings.

Figure 2. Keyboard Settings for iOS 8.1 (other versions of iOS are similar)



Configuring Using Autonomous Single App Mode

If you have iOS tablets running version 8.0 or higher, and if you have a Mac running version 10.10 or higher, then you can use Autonomous Single App Mode (ASAM) to quickly create a secure testing environment on all iPads used for testing. (Tablets running a version earlier than 7.1 require Guided Access; for details about this configuration, see Configuring for Guided Access.) Compared to Guided Access, ASAM requires less time to prepare for test sessions; there is no need to activate Guided Access on each iPad before each test session.

Save Time with Automatic Assessment Configuration If you are using iPads with iOS 9.3.2 or later, you can use the automatic assessment configuration that comes with the AIRSecureTest app. For details, see Using Automatic Assessment Configuration.

Overview of Autonomous Single App Mode and the Secure Testing Environment

To manage multiple iPads using ASAM, you need to do the following:

Step 1: Creating a Mobile Device Management Profile

Step 2: Restricting Features in iOS 8.1.3 or later

Step 3: Creating a Supervisory Profile

Step 4: Placing iPads in Autonomous Single App Mode

After completing these four steps, each time a student starts a test, the iPad enters ASAM and the test environment is secure.

Step 1: Creating a Mobile Device Management Profile

The first step in provisioning iPads with ASAM is to create an MDM profile. Any profile with default settings is compatible with the secure browser. However, you may wish to restrict certain features in devices with iOS 8.1.3 or later (see Step 2: Restricting Features in iOS 8.1.3 or later). Deploy the profile to a host that the iPads can access.

Creating an MDM profile is beyond the scope of this specification manual. The following references provide introductory information:

- *IT in the Classroom*, available at https://www.apple.com/education/it/mdm/.
- *Apple Configurator Help*, available at https://help.apple.com/configurator/mac/2.0/.
- *Pro tip: Use OS X Server Profile Manager for MDM*, available at http://www.techrepublic.com/article/pro-tip-use-os-x-server-profile-manager-for-mdm/.

Step 2: Restricting Features in iOS 8.1.3 or later

You must restrict features in supervised devices with iOS 8.1.3 or later that may give students an unfair testing advantage, including the dictionary, predictive keyboard, spell check, auto-correction, and share selected text.

Note: The current version of Apple Configurator does not allow you to restrict these features. You must use a third-party MDM solution such as Casper or AirWatch to create a profile that implements these restrictions.

To restrict features in iOS 8.1.3 or later:

- In the Custom Settings section of the MDM solution, insert the profile key for each of the features listed in Table 6.

Table 6. Profile Keys for Features in iOS 8.1.3 or Later

Feature	Profile Key	Value
Dictionary, Share Selected Text[a]	`<key>allowDefinitionLookup</key>`	`False`
Predictive Keyboard	`<key>allowPredictiveKeyboard</key>`	`False`
Spell Check	`<key>allowSpellCheck</key>`	`False`
Auto-Correction	`<key>allowAutoCorrection</key>`	`False`

[a] Share Selected Text is available since iOS 9. Disabling Dictionary also disables this feature.

The following snippet turns off the iPad's auto-correction feature. The snippets for dictionary, predictive keyboard, and spell check are similar.

```
<dict>
   <key>allowAutoCorrection</key>
   <false />
   <key>PayloadDisplayName</key>
   <string>Restrictions</string>
   <key>PayloadDescription</key>
   <string>RestrictionSettings</string>
   <key>PayloadIdentifier</key>
   <string>31eb53ac-3a08-46f7-8a0a-82e872382e15.Restrictions</string>
   <key>PayloadOrganization</key>
   <string></string>
   <key>PayloadType</key>
   <string>com.apple.applicationaccess</string>
   <key>PayloadUUID</key>
   <string>56199b2c-374d-4152-bc50-166d21fa9152</string>
   <key>PayloadVersion</key>
   <integer>1</integer>
</dict>
```

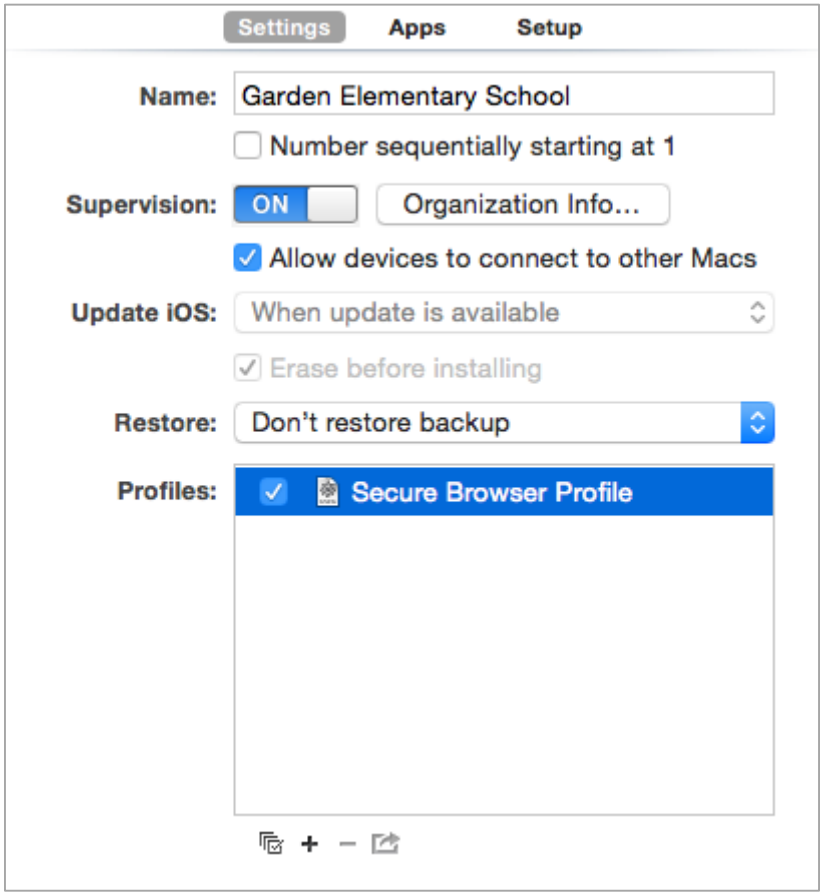
Step 3: Creating a Supervisory Profile

To create a supervisory profile:

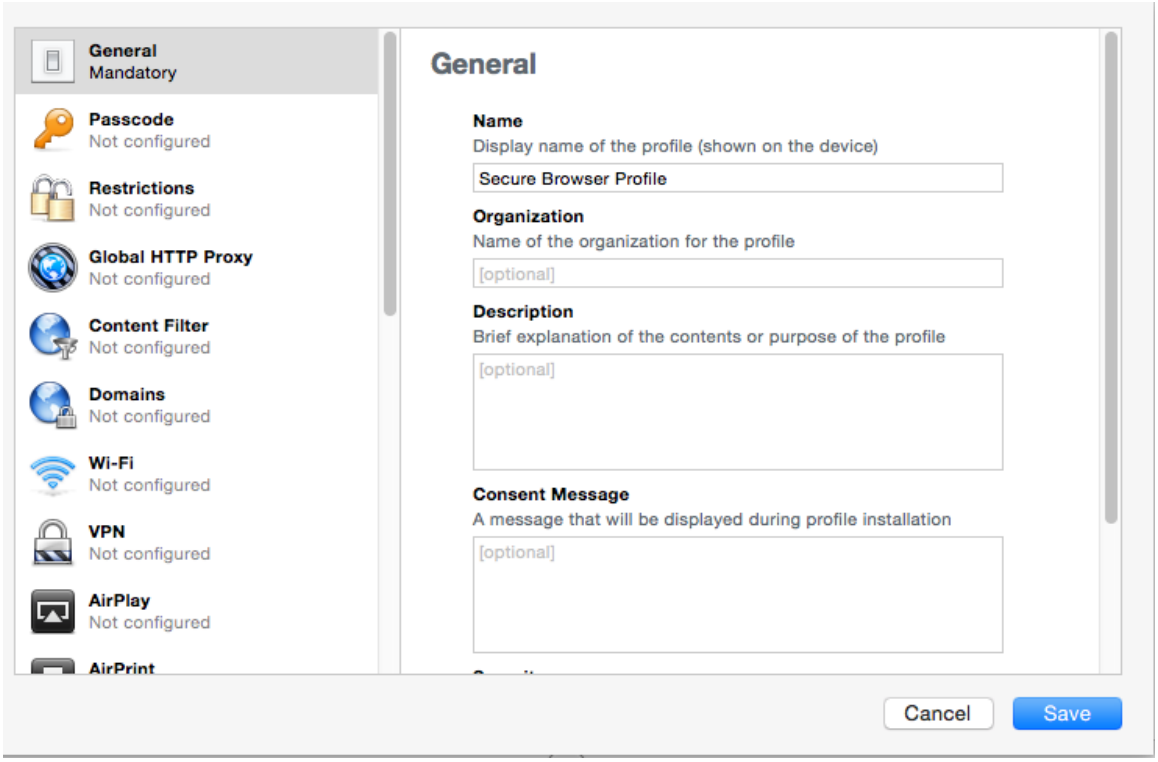
1. On a Mac 10.10 or later, download and install Apple Configurator from the Mac App Store. When the installation completes, open Apple Configurator.

2. Click **Prepare**, then **Settings**. The Settings window appears.

Figure 3. Settings Window in Apple Configurator



3. Click **+** below the Profiles list and select **Create New Profile…**. A configuration window appears.



4. In the **General** section, in the *Name* field, enter a name for the profile.
5. In the **Restrictions** section, click **Configure**. A list of restrictions appears.
6. Make any required changes to the restrictions, or retain the default settings.
7. Click **Save**. You return to the Settings tab, and the profile appears in the Profiles list.
8. Click to export the profile to the Mac.

Creation of the supervisory profile is complete.

Step 4: Placing iPads in Autonomous Single App Mode

TIP: Installing on multiple iPads at once. Before starting this procedure, connect the iPads to the Mac through a USB hub. That way you can perform the installation on many of them at one time.

To install the MDM profile, supervisory profile, and secure browser:

9. On the Mac where you performed Step 3: Creating a Supervisory Profile, open the Apple Configurator.

10. From the **Apple Configurator** menu, select **Preferences**. The ***Preferences*** window opens.

11. Under **General**, make sure the **Automatically refresh** and **Remove apps and profiles Configurator did not install** boxes are unchecked.

12. Close the ***Preferences*** window.

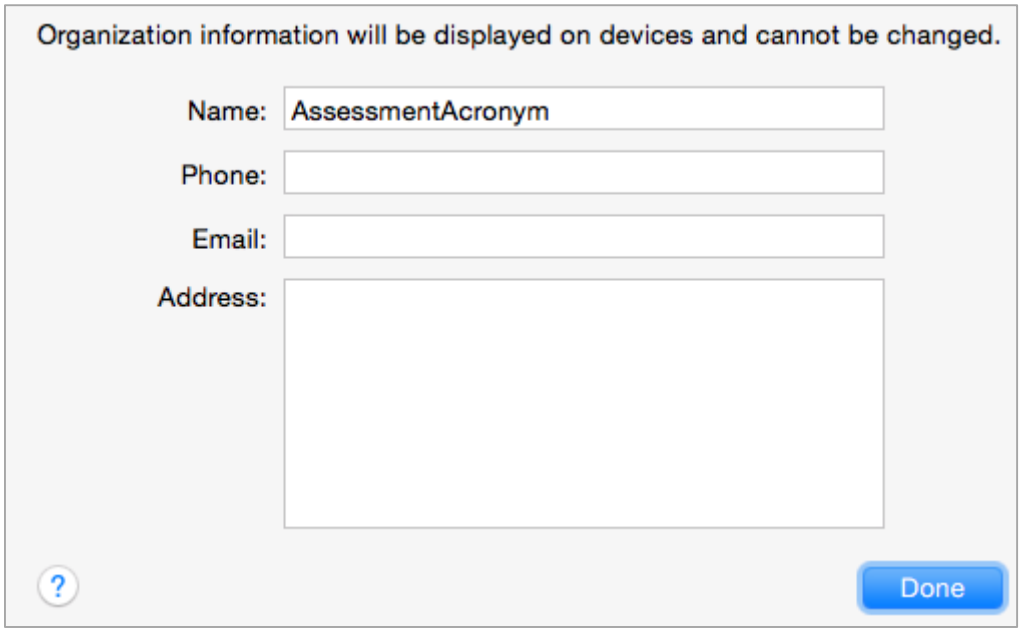
13. Back in Apple Configurator, click **Prepare**, then **Settings**. The Settings window appears (see Figure 3).

14. In the *Name* field, enter a name to apply to the iPads.

15. *Optional:* Mark the **Number sequentially starting at 1** checkbox. This adds a number to each iPad's name. For example, if the Name field is Garden Elementary School, and if three iPads are connected, each device receives the name `Garden Elementary School 1`, `Garden Elementary School 2`, and `Garden Elementary School 3`.

16. Set *Supervision* to **On**.

17. Click **Organization Info…** The ***Organization Info*** window appears.



18. In the *Name* field, enter HSAP and then click **Done**. The ***Organization Info*** window closes.

19. If the profile you created in Step 3: Creating a Supervisory Profile does not appear in the Profiles list, import it by doing the following:

    a. Click **+** below the Profiles list and select **Import Profile…**.

    b. Navigate to the profile you saved in step 8 on page 41, and then click **Open**.

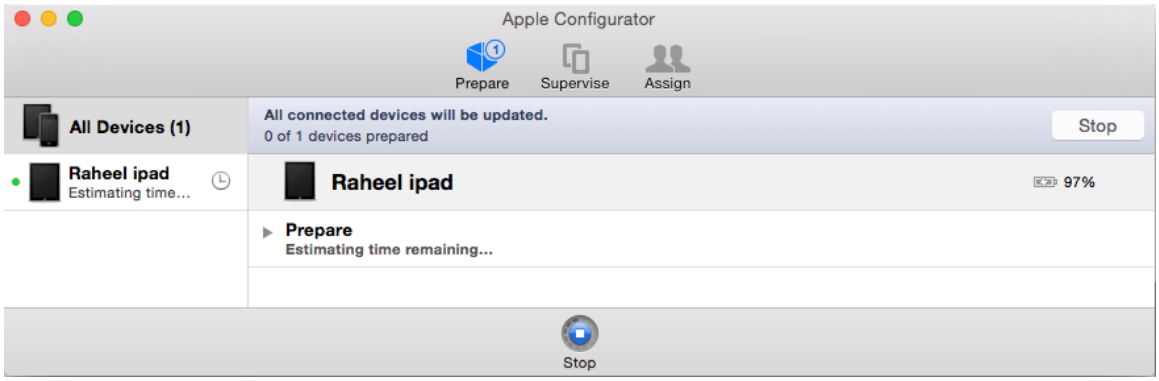
20. Mark the checkbox for the profile you want to prepare onto the iPads (see Figure 3).

21. Connect each iPad to the Mac via a USB cable or USB hub.

22. On each connected iPad, uninstall any existing versions of the secure browser.

23. In the Apple Configurator, under the Prepare tab, click **Prepare** at the bottom of the window. A confirmation message appears.

24. Click **Apply** in the confirmation message. Preparation starts and may take several minutes, after which the iPad restarts. The Apple Configurator displays progress messages during the preparation.



Note: iOS Upgrade Apple Configurator may force the iPads to upgrade to the latest version of iOS.

25. After the iPad restarts, follow the prompts on the iPad to configure it until the home screen appears.

26. *Optional:* Confirm the supervisory profile is installed on the iPad. Go to **Settings > General > Profiles**. The profile name you used in step 4 on page 41 appears under Configuration Profiles.

27. On the iPad, download and install the MDM profile you created in Step 1: Creating a Mobile Device Management Profile.

28. After the MDM profile installation completes, install the secure browser onto the iPad. You can take a copy of the secure browser for iOS from alohahsap.org. (Detailed instructions for installing the secure browser are in the section "Installing the Secure Browser on iOS" of the *Secure Browser Installation Manual*.)

29. *Optional:* After installation completes, test it by doing the following:

    a. Open the Secure Browser.

    b. Log in to a test site.

    c. Select a test, have the TA approve the test.

    d. Start the test. The iPad enters ASAM.

30. Repeat steps 21–29 to prepare additional iPads.

31. In the Apple Configurator, click **Stop** and close the Apple Configurator.

Setting the iPad into ASAM is complete. When a student starts a test, the iPad enters ASAM mode.

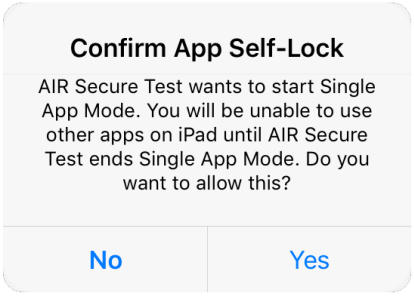
Using Automatic Assessment Configuration

If you are using iPads with iOS 9.3.2 or later, you can use Automatic Assessment Configuration. This configuration includes a preset profile in the AIRSecureTest app that automatically suppresses the features listed in Table 6.

Caution: Conflicting MDM Profiles MDM profiles for managed iPads override the automatic assessment configuration. If you want to use automatic assessment configuration, delete any existing MDM profiles from the Apple Configurator.

When a student taps **Begin Test Now** on an iPad with Automatic Assessment Configuration, a message similar to Figure 4 appears.

Figure 4. Notification When Starting Test with Automatic Assessment Configuration

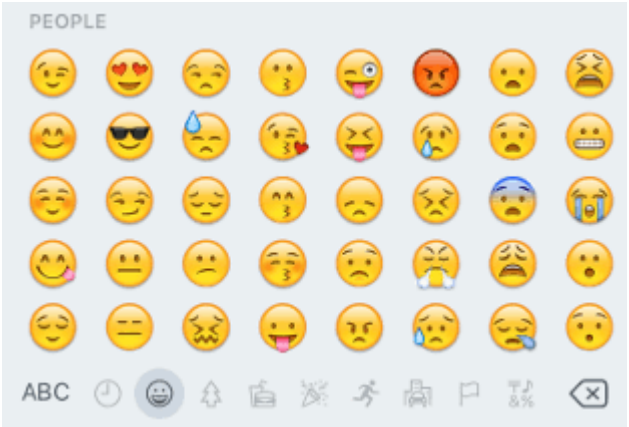


Removing the Emoji Keyboard

Emoticons are characters that express an emotion or represent a facial expression, such as a smile or a frown. Some text messaging apps replace sequences of characters with an emoticon, such as replacing :-) with ☺.

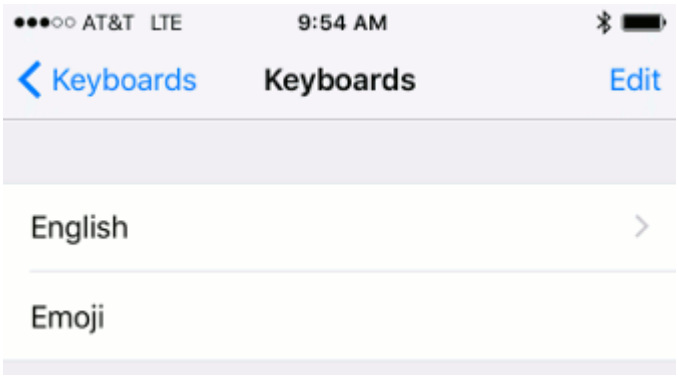
iOS has an Emoji keyboard that contains emoticons. This keyboard, if activated, can be confusing for test-takers or scorers. Use the following procedure to remove the emoji keyboard from an iOS device.

Figure 5. Emoji Keyboard



To remove the Emoji keyboard:

1. Tap **Settings**.
2. Navigate to **General > Keyboard**.
3. Tap **Keyboards**.
4. Delete `Emoji` from the list by sliding it to the left.

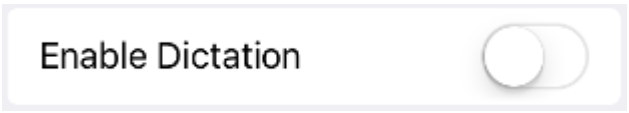


Disabling Dictation

Starting with iOS version 8, a dictation feature is available. As students speak into an iOS device, the dictation feature suggests words or spelling that may compromise testing security. Use the following procedure to disable dictation.

To disable dictation:

1. Tap **Settings**.
2. Navigate to **General > Keyboard**.
3. Turn off `Enable Dictation`.



Configuring Android

This section describes how to configure mobile devices running Android.

Enabling the Secure Browser Keyboard

The default keyboard for the Android allows predictive text, which may provide students with hints for answers to tests. For this reason, the secure browser for Android requires that a mobile secure browser keyboard be configured for the secure browser itself. The secure browser keyboard is a basic keyboard, with no row for predictive text functionality.

The first time you open the Mobile Secure Browser on an Android tablet, you will be prompted to select the secure browser keyboard.

About the Secure Browser Keyboard and General Settings

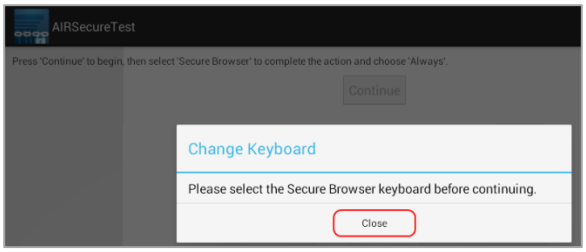
Once the secure browser keyboard is set, it becomes the default keyboard for all Android tablet applications, not just for the secure browser. If you want to return to the default Android keyboard after using the secure browser, you will need to navigate to Settings > Language & Input and uncheck the secure browser keyboard.

If you change back to the default Android keyboard, you will be prompted to select the secure browser keyboard the next time you open the secure browser. The secure browser will not allow you to access the student login page until the secure browser keyboard has been selected.

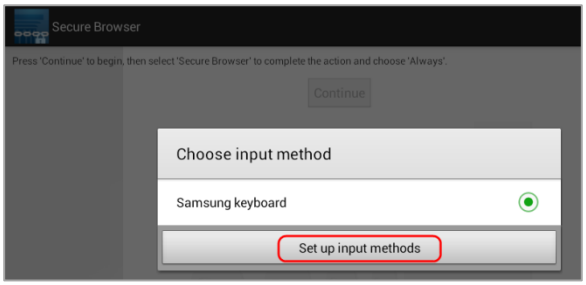
The following procedure describes how to enable the secure browser keyboard. The screen shots were taken with a Samsung Galaxy Tab 2; other Android versions may vary.

1. Select the secure browser icon on the home screen.

2. A Change Keyboard message appears. Tap **Close**.

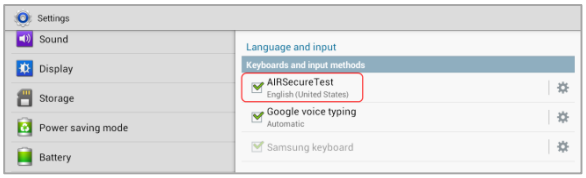


3. Tap **Set up input methods**. The Language and Input settings screen opens.



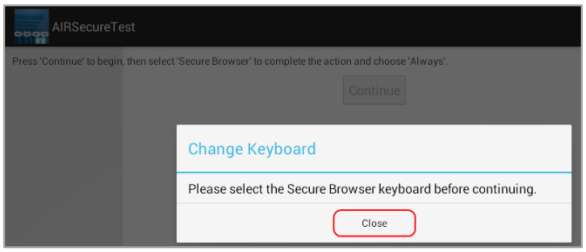
4. Select the checkbox next to `AIRSecureTest` so that a checkmark appears.

5. You will be prompted to acknowledge that this selection is okay. Select **OK** to continue. Note: This action allows the mobile secure browser to use the secure browser keyboard.



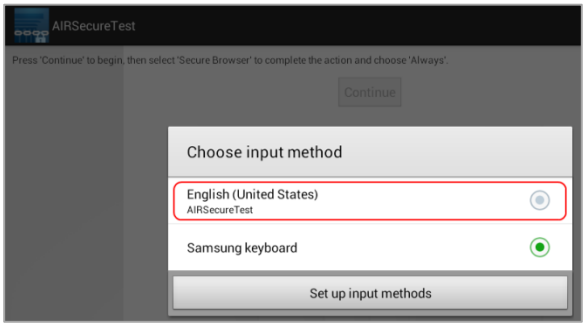
6. Navigate to the secure browser to open it. (You can use the application switcher or go back to “Home” and select the secure browser icon.)

7. You will be prompted to change the keyboard. Select **Close**.

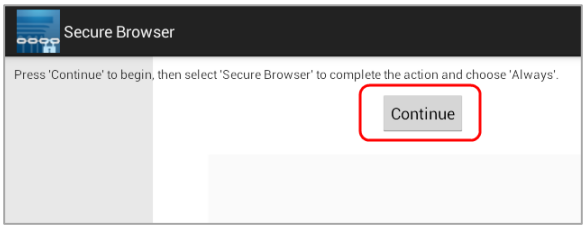


8. The Android tablet’s default keyboard will still be selected.

9. Select the checkmark or circle for the **AIRSecureTest** keyboard.



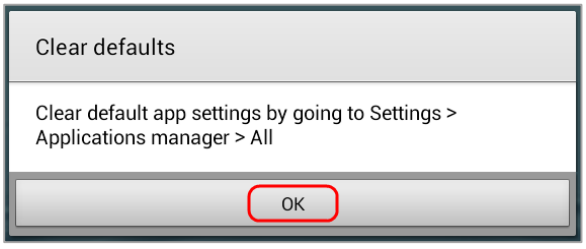
10. Select **Continue**. You will be prompted to complete the application launch using the preferred method.



11. Select AIRSecureTest (ensure it is shaded and highlighted blue) and then select **Always**.

12. You will need to acknowledge that the secure browser’s default settings have changed. (This is a result of selecting the secure browser keyboard.)

13. Select **OK**.



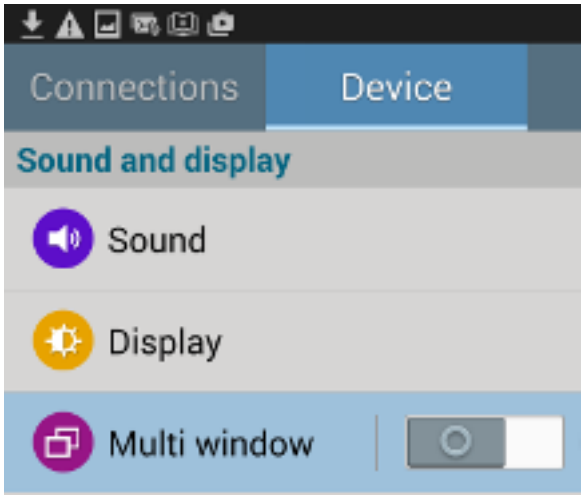
Disabling the Multi-Window on Samsung Tablets

Samsung tablets are equipped with a multi-window feature to display app launchers. Depending on the available app launchers, the multi-window can compromise testing security. To avoid this scenario, disable the multi-window on Samsung tablets.

The following instructions are based on Android 4.4 on a Samsung tablet; similar instructions apply for other versions of Android on Samsung tablets.

To disable the multi-window:

1. Tap **Settings**.
2. Navigate to **Device > Sound and display**.
3. Turn off **Multi window**.

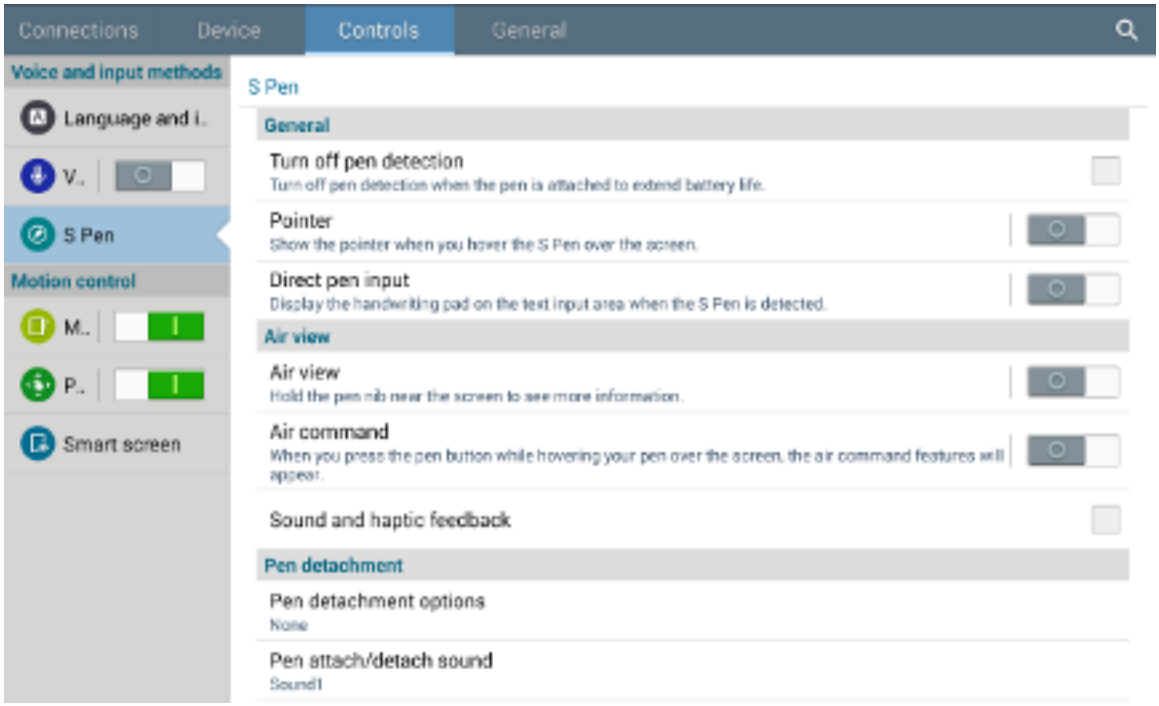


Disabling the Stylus on Samsung Galaxy Note

The Samsung Galaxy Note stylus is capable of launching apps—a situation that can compromise testing security. To avoid this scenario, disable the stylus feature.

To disable the stylus:

1. Tap **Settings**.
2. Navigate to **Controls > Voice and input methods**.
3. Tap **S Pen**.
4. Disable all of the available features.



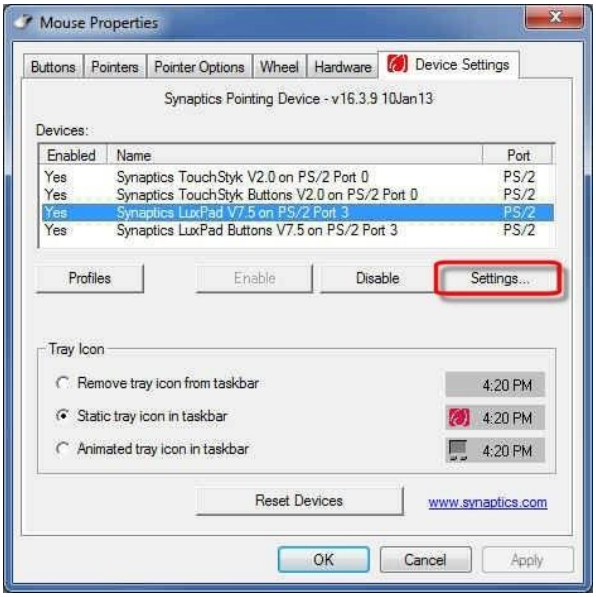
Disabling Two-finger Scrolling Feature in HP Notebooks with Synaptics TouchPad

The trackpad software on the HP stream notebooks can cause the secure browser to close and display an “environment not secure” error. This can occur when a student tries to use the advanced trackpad features such as scrolling gesture with the trackpad. The Synaptics Touchpad driver is the driver that allows full use of all features of the trackpad. To avoid this error and the closing of the secure browser, disable the TouchPad two-finger scrolling Feature.

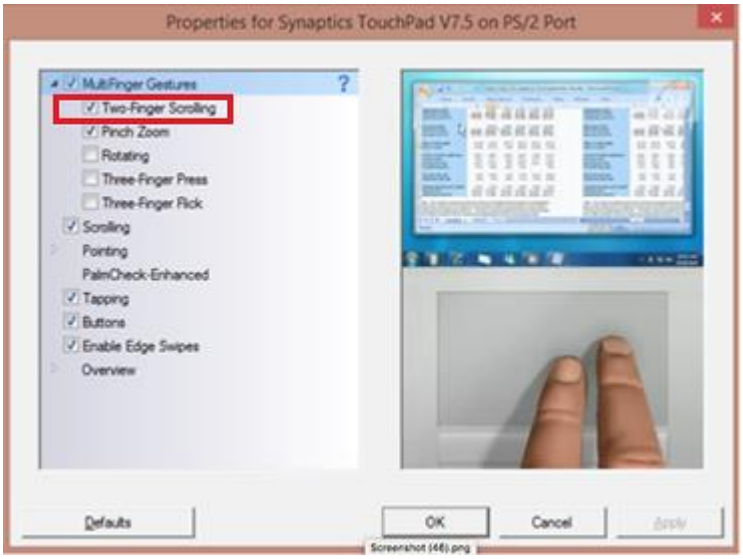
To disable the TouchPad feature in HP notebooks with Synaptics TouchPad:

1. Click the **Start** menu (), and then type mouse in the search field.

2. Select **Mouse** from the list of options.
3. Click the **Device Settings** tab.
4. From the **Devices** list, select **Synaptics LuxPad V7.5**, and then click **Settings.**



5. Uncheck **Two-Finger Scrolling**.



6. Click **Close**, and then click **OK**.
7. In the **Mouse Properties** window, click **Apply**.

Configuring Chrome OS

This section describes how to configure auto-updates to Chrome OS.

Warning: Student monitoring software (such as Hapara, etc.) may not be used during testing. This software may run on the student tablets, such as Chromebooks, when the Secure Browser has been launched in Kiosk mode, but the test coordinator, technology coordinator and/or others who may have access to the parent computer may not use these program(s) during testing. Access to students' screens via student monitoring software during testing is considered to be a test security violation.

Disabling Auto-Updates for Chrome OS

Because AIR supports Chrome OS up to a specific version, you may want to disable auto-updates. For example, if AIR supports up to Chrome OS version 49, and version 49 is installed on your Chromebooks, you can prevent auto-updates to any later version. (Alternatively, you can allow auto-updates to a specific version supported by AIR; for details, see the section Limiting Chrome OS Updates to a Specific Version.)

To disable auto-updates for Chrome OS:

1. Display the Device Settings page by following the procedure in ***Manage device settings***, https://support.google.com/chrome/a/answer/1375678?hl=en. The steps in that procedure assume that your Chromebooks are managed through the admin console.

2. From the *Auto Update* list, select **Stop auto-updates**.

3. Click **Save**.

Limiting Chrome OS Updates to a Specific Version

Because AIR supports Chrome OS up to a specific version, you may want to prevent your Chromebooks from auto-updating beyond that version. For example, if AIR supports up to Chrome OS version 49, and version 48 is installed on your Chromebooks, you can allow auto-updates up to version 49, and prevent auto-updates to any later version. (Alternatively, you can disable auto-updates entirely; for details, see the section Disabling Auto-Updates for Chrome OS.)

To limit Chrome OS updates to a specific version:

1. Display the Device Settings page by following the procedure in ***Manage device settings***, https://support.google.com/chrome/a/answer/1375678?hl=en. The steps in that procedure assume that your Chromebooks are managed through the admin console.

2. From the *Auto Update* list, select **Allow auto-updates**.

3. From the *Restrict Google Chrome version to at most* list, select the required version.

4. Click **Save**.

Installing CloudReady on PCs and Macs

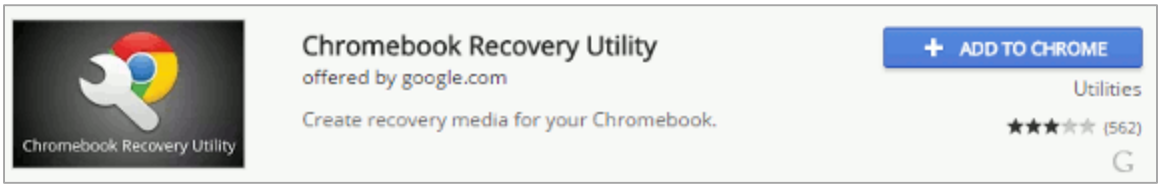
CloudReady is a reduced-feature operating system, built on the same technology as Chrome OS, that runs on hardware with limited resources. If your school has older hardware that does not run newer versions of Windows or OS X, consider installing CloudReady on those machines. This installation can postpone or prevent a costly hardware upgrade.

Warning: Loss of data The procedure described in this section erases all data on the computer on which you are installing CloudReady. Be sure to back up all necessary data before starting this procedure.

To install CloudReady:

1. Ensure the computer on which you are installing CloudReady—
    - is one of the supported models listed in https://docs.google.com/document/d/1yPxKAmNFaJwk0kwikF5iROFMOxiinmkW_9KeI1u5jVo/edit?pli=1.
    - has a USB port.
    - can boot from a USB drive.
2. Purchase a Neverware license for the computer. Licenses are available from http://www.neverware.com/. (Bulk licenses may be available.)
3. If you received a USB drive from Neverware with the CloudReady image, proceed to step 18. Otherwise, prepare a bootable image by following steps 4 through 17. Ideally, perform these steps on a computer on which the Google Chrome web browser is already installed.
4. Obtain a blank 8 GB USB drive.
5. Install Google Chrome if it is not already installed.
6. In a web browser, go to the URL for the image file provided to you by Neverware. This URL downloads a file with a name similar to `cloudready_site646.bin`. Note the location of the file on your computer.
7. Insert the USB drive into the computer.
8. Start Chrome, and navigate to the Chrome web store at https://chrome.google.com/webstore/.

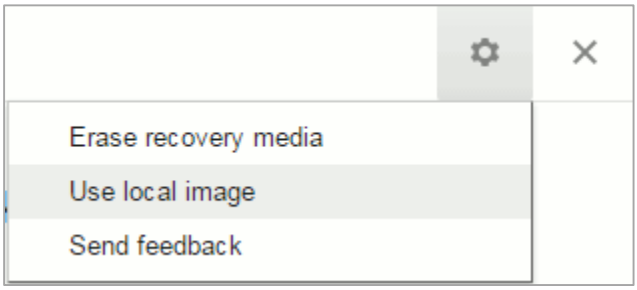
9. Search for the app *Chromebook Recovery Utility*.



10. Click **ADD TO CHROME**, and in the confirmation prompt click **Add app**.

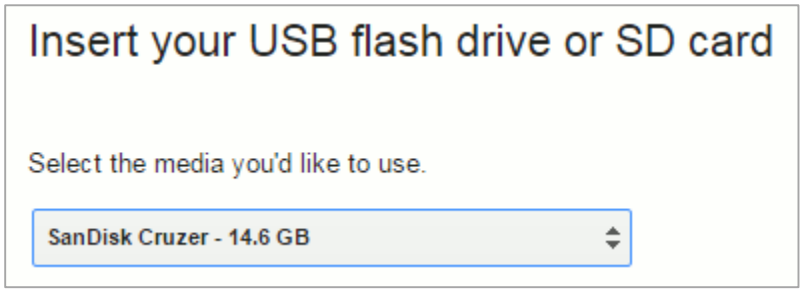
11. After installation, click **Launch App**.

12. Click ⚙ in the top-right corner and select **Use local image**.



13. Navigate to the file image file that you downloaded in step 6.

14. In the next screen, select the USB drive you inserted in step 7.



15. Click **Continue**.

16. In the next screen, click **Create Now**. The recovery utility creates a bootable image of CloudReady onto the USB drive. This operation takes 15–30 minutes.

17. When copying is complete, eject the USB drive from the computer.

18. On the computer where you are installing CloudReady, do the following:

    a. Back up all files you want to save. The installation procedure erases all data on the computer.

b. Boot the computer from the USB drive. Booting and installation take 10–15 minutes, depending on your hardware. When the installation is complete, your computer turns off.

c. Remove the USB drive, and power on the computer.

d. Install the AIRSecureTest Kiosk App; see the *Secure Browser Installation Guide* for details.

Configurations for Braille Requirements

For information about configuring operating systems and software for Braille testing, see the *Braille Requirements* document, which is available on the Hawai'i Statewide Assessment Program portal (alohahsap.org).

Section IV. Text-to-Speech Requirements

This section contains information about text-to-speech requirements.

Overview of 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 and Training Tests 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.

Voice Pack Selection on Mobile Versions of Secure Browsers

The mobile secure browser uses either the device's native voice pack or a voice pack embedded in the secure browser. Additional voice packs downloaded to a mobile device are not

recognized by the mobile secure browser. Table 7 lists the voice packs used by mobile versions of the secured browser.

Table 7. Voice Packs on Mobile Versions of the Secure Browser

Platform	Voice Pack Used by Secure Browser
iOS 8.0–10.x	Native iOS voice pack.
Android	Native Android voice pack.
Chrome OS	Native Chromebook voice pack.

About NeoSpeech Voice Packs for Windows

Pursuant to an agreement between NeoSpeech and the American Institutes for Research (AIR), authorized users may download and install specific licensed NeoSpeech voice packs for use on supported Windows computers (Windows Vista, 7, 8.0, 8.1, 10, and 11).

These voice packs can be used instead of the default Windows voice packs for English and the commercial Spanish voice packs from Cepstral. (The default Windows voice packs as well as the Cepstral voice packs for Windows may still be used for text-to-speech, if desired.)

- The Julie voice pack is for English text-to-speech users.
- The Violeta voice pack is for Spanish text-to-speech users.

The NeoSpeech voice pack is to be used only in conjunction with, and not separate from, the online assessments provided by AIR's Test Delivery System.

The NeoSpeech voice packs can be downloaded from TIDE. Installation instructions are also available in TIDE.

Configuring Windows Text-to-Speech Settings

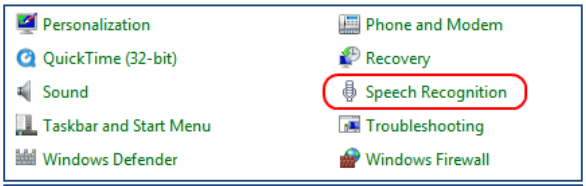
This section explains how to configure Windows for using text-to-speech with the secure browser. The text-to-speech feature is available on Windows versions as listed in the *System Requirements* document.

The instructions in this section are for Windows 7. The process is similar for other versions of Windows.

Note: The following instructions apply only to voice packs supplied with Windows and possibly other third-party voice packs. To install NeoSpeech voice packs, see the publication *NeoSpeech Voice Packs Installation Guide*, available in TIDE by clicking **Resources > Voice Packs**.

1. Open the Control Panel window, and select **Speech Recognition**.

2. In the Speech Recognition window, select **Text to Speech**.



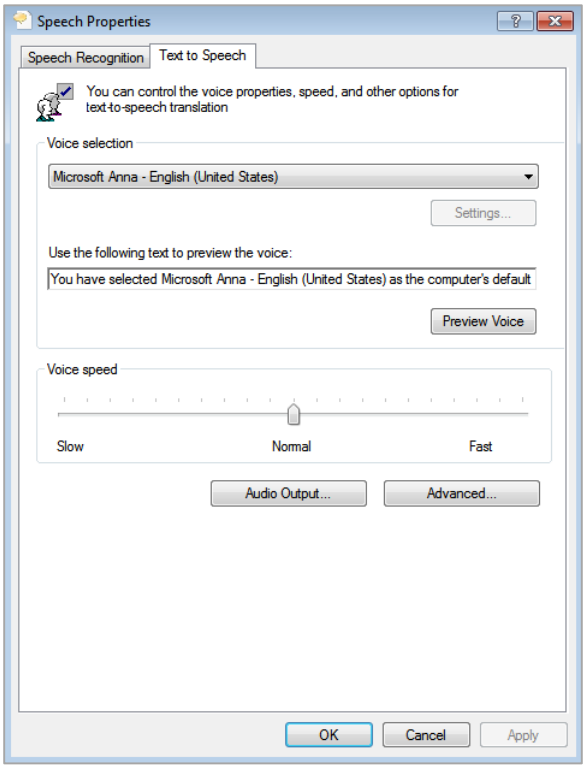
3. Configure default text-to-speech preferences.

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

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

   c. *Voice speed:* If necessary, adjust the voice speed. Drag the slider to make the voice speak slower or faster. To listen to the rate, select **Audio Output**.

   d. When you are done, click **OK** to save your settings and then close the Speech Properties window.

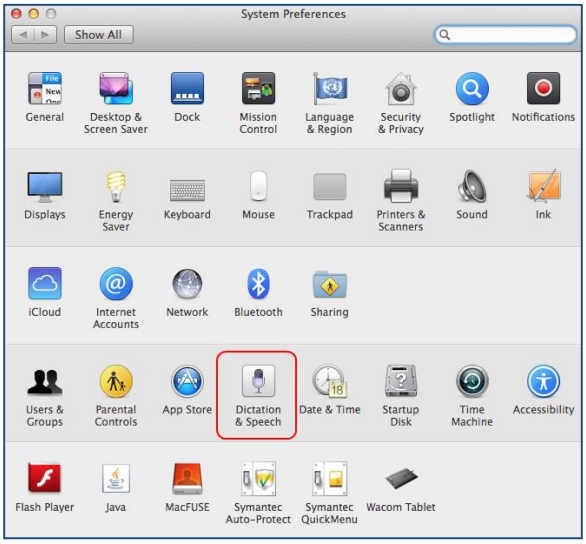


Configuring OS X Text-to-Speech Settings

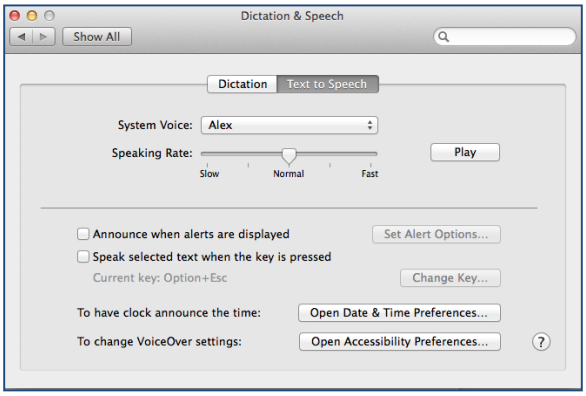
This section explains how to configure Mac OS X for using text-to-speech with the secure browser. The text-to-speech feature is available on OS X versions as listed in the *System Requirements* document.

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

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



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



   - *System Voice:* If multiple voice packs are available, select the default voice.
   - Select **Play** to see whether the selected voice requires a rate adjustment.
   - *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**.
   - When you are done, click the red **X** in the upper left corner to save your settings and close the Speech window.

Text-to-Speech and Mobile Devices

Text-to-speech (TTS) includes a feature that allows students to pause and then resume TTS in the middle of a passage. The pause feature does not work on mobile devices. Consequently, consider testing students who require TTS on desktop or laptop computers.

Voice Packs Recognized by Desktop Secure Browsers

The tables in this section display the voice packs for Windows and OS X that are currently recognized by the secure browser.

Voice Packs for Windows

Table 8. Voice Packs Recognized by Secure Browsers—Windows

Vendor	Voice Pack	Language
Windows (pre-installed)	Julie	English
Windows (pre-installed)	Kate	English
Windows (pre-installed)	Michael	English
Windows (pre-installed)	Michelle	English
Windows (pre-installed)	MSAnna	English
Windows (pre-installed)	MS_EN-GB_HAZEL	English
Windows (pre-installed)	MS_EN-US_DAVID	English
Windows (pre-installed)	MS_EN-US_ZIRA	English
Windows (pre-installed)	MSMary	English
Windows (pre-installed)	MSMike	English
Windows (pre-installed)	MSSam	English
Windows (pre-installed)	Paul	English
Windows (pre-installed)	Violeta	Spanish
Cepstral (commercial)	Cepstral_David	English
Cepstral (commercial)	Cepstral_Marta	Spanish
Cepstral (commercial)	Cepstral_Miguel	Spanish
NeoSpeech (commercial)	VW Julie	English
NeoSpeech (commercial)	VW Violeta	Spanish

Voice Packs for OS X

Table 9. Voice Packs Recognized by Secure Browsers—OS X

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
Mac (pre-installed)	Samantha	English
Mac (pre-installed)	Tom	Spanish
Mac (pre-installed)	Vicki	English
Mac (pre-installed)	Victoria	English
Mac (pre-installed)	Diego	Spanish
Mac (pre-installed)	Javier	Spanish
Mac (pre-installed)	Marta	Spanish
Mac (pre-installed)	Monica	Spanish
Mac (pre-installed)	Paulina	Spanish
Infovox (commercial)	Heather Infovox iVox HQ	English
Infovox (commercial)	Rosa Infovox iVox HQ	Spanish

Appendix A. URLs Provided by AIR

This appendix presents information about the URLs that AIR provides. Ensure your network's firewalls are open for these URLs.

URLs for Non-Testing Sites

Table 10 lists URLs for non-testing sites, such as Test Information Distribution Engine, Online Reporting System, and Learning Point Navigator.

Table 10. AIR URLs for Non-Testing Sites

System	URL
Portal and secure browser installation files	alohahsap.org
Single Sign On System	hi.sso.airast.org
Test Information Distribution Engine	hitide.org
Online Reporting System	hsa.reports.airast.org
Teacher Hand-Scoring System	hi.tss.airast.org

URLs for Testing Sites

Testing sites provide test items as well as support services such as dictionaries and thesauruses.

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 11. AIR URLs for Testing Sites

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

Online Dictionary and Thesaurus

Some online assessments contain an embedded dictionary and thesaurus provided by Merriam-Webster. The Merriam-Webster URLs listed in Table 12 should also be whitelisted to ensure that students can use them during testing.

Table 12. 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

Appendix B. Technology Coordinator Checklist

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

	Activity	Estimated Time to Complete	Target Completion Date	Reference
☐	Verify that all of your school's devices that will be used for online testing meet the operating system requirements.	5–10 hours	3–4 weeks before testing begins in your school	*System Requirements*
☐	Verify that your school's network and Internet are properly configured for testing, conduct network diagnostics, and resolve any issues.	5–10 hours	3–4 weeks before testing begins in your school	Network Configuration and Testing
☐	Install the secure browser on all devices that will be used for testing.	5–10 hours	3–4 weeks before testing begins in your school	*Secure Browser Installation Manual*
☐	Enable pop-up windows and review software requirements for each operating system.	5–10 hours	1–2 weeks before testing begins in your school	Software Configuration
☐	On **Windows** computers, disable Fast User Switching. If a student can access multiple user accounts on a single computer, you are encouraged to disable the Fast User Switching function.	5–10 hours	1–2 weeks before testing begins in your school	Disabling Fast User Switching
☐	On **Mac 10.7–10.12**, disable Spaces in Mission Control.	5–10 hours	1–2 weeks before testing begins in your school	Disabling Exposé or Spaces
☐	Install any required text-to-speech software on devices that will be used for testing and verify that installation.	5–10 hours	1–2 weeks before testing begins in your school	Text-to-Speech Requirements
☐	On **iPads**, ensure that Guided Access or ASAM is enabled and that TAs know how to activate Guided Access.	5–10 hours	1–2 weeks before testing begins in your school	Configuring for Guided Access
☐	On **Android** tablets, ensure that the secure browser keyboard is enabled.	5–10 hours	1–2 weeks before testing begins in your school	Enabling the Secure Browser Keyboard

Appendix C. Scheduling Online Testing

Number of Computers and Hours Required to Complete Online Tests

We recommend that schools arrange their computer resources to accommodate the number of students who will be testing at the same time for ease of test administration. The Sample Test Scheduling Worksheet below shows how to estimate the number of testing hours needed to administer one testing opportunity.

Note: This worksheet may need to be modified based on your network setup. You may want to work with your Test Administrator to adapt this worksheet as necessary so that you do not risk overloading your wired or wireless network.

Sample Test Scheduling Worksheet

For each school, enter the following for each online test:

Number of computers available for testing at once:

Number of students who need to take the test:

Number of Test Administrators who need a computer:

Estimated number of hours needed per student to complete the test. This estimate should include approximately 15 minutes for students to get set up and logged in as well as the average estimated time to complete the test.

Number of hours that must be scheduled to administer the test:
(students + TAs) x hours ÷ computers =

Example:

- School A has a total of 60 student computers available for testing at once.
- 120 students in grade 5 will need to take the Math assessment.
- Number of hours needed to administer test: 120 students x 1 hour per student ÷ 60 computers = 2 hours (plus 15 minutes for setup).

Appendix D. User Support

If this document does not answer your questions, please contact the Hawai‘i Statewide Assessment Program Help Desk.

The Help Desk will be open Monday–Friday from 7:30 a.m. to 4:00 p.m. HST (except holidays).

Hawai‘i Statewide Assessment Program Help Desk

Toll-Free Phone Support: 1-866-648-3712

Email Support: hsaphelpdesk@air.org

If you contact the Help Desk, you will be asked to provide as much detail as possible about the issues you encountered. You may choose to use the *Help Desk Intake Form*, available on the alohahsap.org portal website in the **Resources >> Technology Coordinators** section.

Include the following information:

- Test Administrator name and IT/network contact person and contact information
- SSIDs of affected students
- Results ID for the affected student tests
- Operating system and browser version information
- Any error messages and codes that appeared, if applicable
- Information about your network configuration:
    - Secure browser installation (to individual machines or network)
    - Wired or wireless Internet network setup

Appendix E. Change Log

This Change Log can be used to identify specific changes that are made to any of the information included in the original document throughout the current school year.

Change	Section	Date
Added instructions for enabling Text-To-Speech on Firefox	Enabling Text-To-Speech on Firefox (new section)	9/26/16
Clarified typical scenario for the use of ZoomText	Configuring ZoomText to Recognize the Secure Browser	9/26/16
Added List of Figures	List of Figures	11/2/16
Added screen shot of message student sees when using Automatic Assessment Configuration	Using Automatic Assessment Configuration	11/2/16
Added new topic - Keyboard Navigation to Tool Menu using a Safari Browser	Configuring Mac OS X for Online Testing	12/22/16
Added information about the prohibited use of student monitoring software	Configuring Chrome OS	12/22/16
Added new topic - Disabling Dictation and Siri	Configuring Mac OS X for Online Testing	1/26/17
Updated “Keyboard Navigation to Tool Menu using a Safari Browser” section to include the use of public browsers	Configuring Mac OS X for Online Testing	1/26/17
Revised instructions to access Symantec OCSP list	Network Configuration: Configuring for Certificate Revocations	2/2/17
Added new sub-section: Disabling Two-finger Scrolling Feature in HP Notebooks.	Configuring Android	3/3/17
Added procedures to block Tablet Touch Input.	Network Configuration: Blocking Tablet Touch Input Using the Group Policy Editor	3/3/17
Added additional explanatory verbiage.	Configuring Mac OS X for Online Testing: Disabling Dictation and Siri	3/3/17
Updated obsolete hyperlink.	Network Configuration: Configuring for Certificate Revocations	3/3/17
Changed the section title. Added information to the introductory paragraph.	Blocking Device Touch Input Using the Group Policy Editor	3/8/17

Change	Section	Date
Added instructions for turning off ChromeVox.	Turning off ChromeVox (new section)	3/27/17
Added instructions regarding the touch keyboard on Microsoft Surface Pro 3 Tablet.	Touch Keyboard on Microsoft Surface Pro 3 Tablet	6/15/17