



Smarter Balanced Assessment Consortium: Technical Specifications Manual For Online Testing

For the Spring 2014 Field Test Administration

Updated March 17, 2014

Prepared by the American Institutes for Research®



© Smarter Balanced Assessment Consortium, 2014

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



Table of Contents

Introduction to the Technical Specifications Manual	6
Manual Content.....	6
Other Resources.....	6
Additional Support.....	6
Section I. Network and Internet Requirements	7
Common Network Performance Bottlenecks	7
Bandwidth.....	8
Determining Bandwidth Requirements	8
Total number of students simultaneously testing.....	9
Size of the test content.....	9
Secure browser installation.....	9
Wireless Networking	10
Wireless access points.....	10
Network Diagnostic Tools	11
AIR's Network/Bandwidth Diagnostic Tool.....	11
Microsoft Windows specific tools.....	11
Mac OS X specific tools.....	11
Multi-Platform tools.....	12
Network Configuration	13
Protocols.....	13
Domain name resolution.....	13
Firewall, content filter, and proxy servers.....	13
Quality of Service (QoS)/Traffic shaping.....	13
Certificate revocation list.....	14
Section II. Hardware Requirements.....	16
Smarter Balanced Technology Requirements	16
Other Hardware Recommendations.....	17
Monitor/Screen Displays.....	17
Printers	17
Keyboards	17
Headphones.....	18
Section III. Software Requirements.....	19
Disabling Pop-Up Blockers.....	19
Installing the Verdana Font on Linux Machines	19
Special Note for Windows Users: Fast User Switching.....	20
Disabling Fast User Switching in Windows XP (with Service Pack 3).....	20
Disabling Fast User Switching in Windows Vista or 7	21

Disabling Fast User Switching in Windows 8.0 and 8.1	22
Section IV. Text-to-Braille Hardware and Software	24
Braille Hardware.....	24
Braille Software	24
Requirements for Student Computers.....	24
Configure JAWS to Recognize the Secure Browser.....	24
Applying Settings for Contracted/Uncontracted Braille	25
Requirements for Test Administrator Computers	27
Section V. Secure Browser Installation.....	28
One-by-One (Manual) Installation for Desktops and Laptops.....	29
Network Installation (Network Administrators).....	29
Installation without Administrator Rights.....	29
Windows Secure Browser (Version 6.3).....	30
Installing Windows Secure Browser 6.3.	30
Manually Installing the .msi Package via the User Interface:	30
Installing the .msi package via a script.	31
Manually uninstalling the previous Windows secure browser.	31
Mac OS X Secure Browser for 10.4 and 10.5 (Version 5.6).....	32
Installing Secure Browser 5.6 for Mac OS X 10.4 and 10.5 (with PowerPC).	33
Uninstalling the previous Mac OS X secure browser.	33
Mac OS X Secure Browser for 10.5–10.9 (Version 6.3).....	34
Installing Secure Browser 6.3 for Mac OS X 10.5–10.9 (with Intel).....	35
Uninstalling the previous Mac OS X secure browser.	35
Disabling Spaces in Mission Control on Mac 10.7–10.9 computers.	36
Mac computers and keyboard options for opening applications.....	37
Linux Secure Browser (Version 6.3).....	38
Installing Linux Secure Browser 6.3.	38
Uninstalling the Linux secure browser.....	38
Linux 64-bit Machines and the secure browser.....	39
Network Installation for Windows (Network Administrators).....	40
Installing the secure browser to a shared drive.	40
Pushing the secure browser installation directory from the network to client computers.	41
Installing the Secure Browser on Computers without Administrator Rights (Windows).....	42
Terminal Server/Thin Client Installation (Windows).....	43
NComputing Virtual Desktop Installation (Windows)	44
Network Installation Information for Mac OS X (Network Administrators).....	45
Secure Browsers and Proxy Settings (Updated)	46
Specifying a proxy server to use with the secure browser.....	46
Creating a corresponding desktop shortcut to run the browser using additional parameters.	47

Microsoft Windows	47
Mac 10.4–10.9	48
Linux (Fedora Core 6+ and Ubuntu 9 and 10).....	50
Linux (Ubuntu 11 and 12).....	50
Section VI. Mobile Secure Browsers	51
Introduction	51
Supported Mobile Devices and Operating Systems.....	51
Secure Testing on iPads	51
Secure Testing on Android Tablets	52
iOS (iPad) Secure Browser	53
Downloading and Installing the iOS Mobile Secure Browser	53
Enabling Guided Access	54
Opening the iOS Mobile Secure Browser and Selecting the Assessment Program	55
Activating Guided Access Before a Test Session Begins	56
Deactivating Guided Access After a Test Session Ends	57
Android Secure Browser	58
Downloading and Installing the Android Secure Browser.....	58
Opening the Android Secure Mobile Browser and Changing the Keyboard	58
Opening the Android Secure Browser and Selecting the Assessment Program	61
Closing the Android Secure Browser.....	61
Section VII. Chromebooks	62
Adding the AIRSecureTest Kiosk App to Managed Chromebooks.....	62
Adding the AIRSecureTest App to Non-Managed Chromebooks	63
Google Documentation	63
<i>Opening the Mobile Secure Browser and Selecting the Assessment Program</i>	<i>64</i>
Section VIII. About Text-to-Speech and Voice Packs.....	65
How the Secure Browsers Work	65
Desktop Secure Browsers	65
Mobile Secure Browsers.....	65
Windows: Configuring Text-to-Speech Settings	66
Step 1: Access Control Panel	66
Step 2: Access Speech Options.....	67
Step 3: Set Speech Preferences	67
Mac OS X: Configuring Text-to-Speech Settings	68
Step 1: Access System Preferences	68
Step 2: Access Speech Options.....	68
Step 3: Set Speech Preferences.	68
Linux: Enabling Text-to-Speech and Default Settings	70
About Sound Cards and ALSA Drivers.....	70

Checking Sound on Your Computer	71
Testing Festival for Use with the Text-to-Speech Accommodation.....	74
Setting Defaults for Voice, Reading Speed, and Volume.....	75
Default Voice Settings	75
Default Reading Speed	76
Default Volume Setting	76
Voice Packs Recognized by Secure Browser	77
Appendix A: IP Addresses and URLs for Smarter Balanced Systems	79
IP Addresses and URLs for Smarter Balanced Systems	79
IP Addresses and URLs for Smarter Balanced California Systems	81
Appendix B: School Technology Coordinator Checklist.....	83
Appendix C: District Technology Coordinator Checklist	85
User Support	86
Smarter Balanced Help Desk	86
California Technical Assistance Center (for California Users)	86
Change Log	87

Introduction to the Technical Specifications Manual

This manual provides information, tools, and recommended configuration details to help technology staff in Consortium states prepare computers to be used with the various Smarter Balanced administrations.

Manual Content

This document provides technical information in seven sections, as follows.

- [Section I, Internet and Network Requirements](#), provides information about bandwidth, wireless networking, network configuration, and diagnostic tools.
- [Section II, Hardware Requirements](#), contains information regarding supported tablets, keyboards, headphones, and printers.
- [Section III, Software Requirements](#), provides information about pop-up blockers, installing the Verdana font on Linux machines, and how to disable the Fast User Switching feature in Windows-based computers.
- [Section IV, Text-to-Braille](#), contains hardware and software requirements for student and Test Administrator computers.
- [Section V, Secure Browser Installation](#), provides instructions for downloading and installing the secure browser on each supported operating system, and options for pushing the secure browser out to student computers over a school network.
- [Section VI, Mobile Secure Browsers](#), provides instructions for downloading and installing the secure mobile browsers on supported iPad and Android tablets, including how to enable Guided Access on iPads and the secure browser keyboard on Android tablets.
- [Section VII, Chromebooks](#), provides instructions for adding the mobile secure browser kiosk app to Chromebooks.
- [Section VIII, Text-to-Speech and Voice Packs](#), contains instructions for ensuring that text-to-speech is enabled on supported operating systems.
- The [Appendices](#) contain URLs and IP addresses for Smarter Balanced systems as well as checklists that technology staff at schools and districts can use to ensure student computers are correctly set up for testing.

Other Resources

User guides for systems provided by AIR are posted to the Smarter Balanced portal (<http://sbac.portal.airast.org>).

Additional Support

If you need information that is not provided in this manual or on the Smarter Balanced Assessment Consortium website (www.smarterbalanced.org) or on the Smarter Balanced portal (<http://sbac.portal.airast.org>) or the Smarter Balanced California portal (<http://sbac.portal.airast.org/ca/>), contact the Help Desk.

Contact information is listed on the [User Support](#) page at the end of this document.

Section I. Network and Internet 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 network administrator or technology specialist to find the right contact person in your area. You may also contact the Smarter Balanced Help Desk.

Network configuration settings should include the following:

- Content filters, firewalls and proxy servers should be configured to allow traffic on the protocols and to the servers listed below.
- Session timeouts on proxy servers and other devices should be set to values greater than the average scheduled testing time. If testing sessions are scheduled for 60 minutes, consider session timeouts of 65–70 minutes. This will help limit network interruptions during testing.
- Data cannot be cached.
- If your client network uses any device(s) that performs traffic shaping, packet prioritization, or Quality of Service, the IP addresses below should be given a high priority to guarantee the highest level of performance.

Refer to [Appendix A](#) for a list of URLs and IP addresses that should be open or whitelisted.

Common Network Performance Bottlenecks

All network communications are accomplished using the IP protocol suite. The LAN (local area network) must be able to route IP traffic to and from the Internet. The Test Delivery System is delivered directly through the Internet. Students must access their tests using the appropriate secure browser. (See Section V for secure browser information.) For testing to take place, all workstations where tests will be administered must have reliable Internet connectivity.

In general, the performance of the Test Delivery System will depend on a number of factors, including bandwidth, total number of students simultaneously testing, size of test content, secure browser installation, proxy server (if used) and the wireless networking solution (if used).

Bandwidth

Bandwidth is the measure of the capacity of a network. Utilized bandwidth measures the amount of data traveling across the network at a given point in time. Bandwidth performance can be affected on either of the following networks: internal network (LAN) traffic and Internet traffic from the router. Regardless of hardware or network topology, the LAN should be analyzed to determine the potential for traffic bottlenecks.

The following table displays the estimated average bandwidth used by the secure browser for testing. (Note that there is a one-time exception to these averages; during initial secure browser startup, the load can be greater.) All numbers provided are based on rigorous testing using Wireshark.

Number of Students Testing Concurrently in School/Building	Average Estimated Bandwidth Consumed During Subsequent Startup of Secure Browser*	Average Estimated Bandwidth Consumed During Testing**
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)

* The bandwidth consumed when opening the secure browser and accessing a test for the first time is significantly higher than when opening the secure browser and accessing a test subsequently. The reason for this is that 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 at a later time.

** Bandwidth will vary during a student’s testing experience, as some test pages contain low-bandwidth content, such as selected-response items, and other pages contain higher-bandwidth content, such as animations, audio clips, or American Sign Language videos. Consequently, the estimated average values in this column are based on computing averages from multiple tests and test subjects.

Determining Bandwidth Requirements

Schools need to factor the bandwidth requirements of each test along with all other non-test-related Internet traffic in order to determine how many concurrent test sessions the schools’ Internet connections can support.

- The Field Test includes animations and interactive item types. These may increase the bandwidth required, but the bandwidth should not exceed the peak usage experienced when the test initially loads. **We encourage you to run the diagnostics on your network to determine how many students at a time you can reasonably test for the Field Test.** Refer to the [Network Diagnostics Tools](#) section for information about running diagnostics on your network.
- For wired networks, internal bandwidth is typically not a problem, because new switches generally operate at speeds of between 100M bits per second and 1000M bits per second. However, LAN performance can be hindered in cases where hubs are used instead of switches. A hub device will allow broadcast signals from various network devices to propagate across the network, potentially saturating the network and causing traffic competition and/or collisions of data.
- 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 whether their Internet infrastructure has the capacity to accommodate current and future growth.



Determining whether infrastructure is capable of current and future growth involves a number of steps, including but not limited to: (1) the analysis of the current number of users; (2) current day-to-day Internet bandwidth statistics; and (3) the desired response time for applications.

Total number of students simultaneously testing.

As the number of students testing at one time increases, competition for network bandwidth increases. Network bandwidth resembles highway traffic; as the number of cars traveling on a given road increases, the speed of traffic flow decreases.

Size of the test content.

The size of the test 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 size of a test item, the higher the bandwidth requirement for a given test. For example, ELA tests typically deliver all items associated with a passage at one time, and this may slightly the bandwidth for these tests.

Secure browser installation.

The recommended installation of the secure browser(s) is local installation on each individual testing workstation. It is possible to install the secure browser on a network or shared drive and then have the testing workstations run the secure browser from that drive, but there may be some performance impacts under this configuration. There will be competition for network bandwidth, and the network or shared disk drive will also be subject to some resource competition as there will be multiple clients reading from the network drive, thus slowing the overall processing speed.

Wireless Networking

Over the past several years, there have been several revisions to wireless networking technology.

- 802.11n is the fastest and most recent IEEE wireless standard, with 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.



Wireless Security—Due to the sensitivity of test-related data, it is highly recommended that wireless traffic use WPA2/AES data encryption. Because encryption/decryption is part of the data exchange process, there may be a slight decrease in the overall speed of the network. A properly configured wireless network should provide adequate bandwidth for the testing applications.

Wireless access points.

AIR recommends that schools maintain a ratio of wireless systems to wireless access points (WAPs) of no more than 20 to 1. Typically, the test performance begins to deteriorate after that threshold has been reached. In some instances, older WAPs may also see performance degradation when more than 15 devices are concurrently attached.

Recommendations on the optimal number of student workstations per wireless connection:

The optimal (or maximum) number of student workstations (computers and tablets) supported by a single wireless connection will depend on the type of networking standard being used for the connection. The two most common networking standards are 802.11g (54Mbps) and the newer and faster standard, 802.11n (300Mbps). Both the access point, which emits the wireless signal, and the computer's wireless card, which receives the signal, will use one of these two standards. The recommendations below are based on the standard in use:

	802.11g Access Point	802.11n Access Point
802.11g Wireless Cards	20 workstations or devices	40 workstations or devices
802.11n Wireless Cards	20 workstations or devices	40 workstations or devices
Mix of 802.11g and 802.11n Wireless Cards	20 workstations or devices	40–50 workstations or devices (depending on the ratio of wireless cards used)

Note: Refer to your WAP documentation for specific recommendations and guidelines. Networks using wireless standards other than 802.11g and 802.11n may also work, but early testing using the practice and training tests is recommended.

Network Diagnostic Tools

A performance analysis of the LAN/Internet infrastructure is recommended in order to identify any bottlenecks that may impact test performance. Identifying the diagnostic tool most appropriate for a network depends on the testing operating system, the network administrator's knowledge base and the desired level of network analysis. The Internet offers a number of network diagnostic tools, including, but not limited to, the following:

AIR's Network/Bandwidth Diagnostic Tool

AIR provides a diagnostic tool that can be directly accessed from the Smarter Balanced portal (<http://sbac.portal.airast.org>).

1. From the portal home page, click the [**Practice and Training Tests**] link.
2. Click the [**Diagnostic Tools**] link at the bottom of the page. The Diagnostic Screen page will display.
3. In the Network Diagnostics section, select a test.
4. Select the approximate number of students who may take that test *at one time*.
5. Click [**Run Network Diagnostics Tests**] button.

The results will display your *current* upload and download speed as well as a general idea of whether you can reliably test the given number of students (the number 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.

Microsoft Windows specific tools.

PRTG Traffic Grapher (www.paessler.com/prtg)

This Windows software 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 (www.microsoft.com/whdc/device/network/TCP_tool.msp)

NTttcp 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 the Windows operating system. It combines the functionality of Ping with that of Traceroute (Windows filename: tracert) 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.

Mac OS X specific tools.

Network Utility.app

This tool is built into Mac OS X software (10.4 or greater).

Multi-Platform tools.

Wireshark (www.wireshark.org)

Wireshark (formerly Ethereal) is a network protocol analyzer. It has a large feature set and runs on most computing platforms including Windows, OS X, Linux, and UNIX.

TCPDump (<http://sourceforge.net/projects/tcpdump>)

TCPdump is a common packet sniffer that runs under the command line and is compatible with most major operating systems (UNIX, Linux, Mac OS X). It allows the user to intercept and display data packets being transmitted or received over a network.

A Windows port WinDump is also available (www.winpcap.org/windump/).

Ping, NSLookup, Netstat, Traceroute (in Windows: tracert)

This is a set of standard UNIX network utilities. Versions of these utilities are included in all major operating systems (UNIX, Linux, Windows, and Mac OS X).

Iperf (<http://sourceforge.net/projects/iperf/>)

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.

Network Configuration

Protocols.

All communication with the Test Delivery System takes place over the following Internet port/protocol combinations. Please ensure that the following ports are open for these systems.

Table 1. Ports for Test Delivery System

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

Domain name resolution.

All system URLs must be resolvable by all client hosts attempting to connect to the Test Delivery System. This means that the client workstations should be able to convert the friendly names (URLs) to their corresponding IP address by requesting the information from the DNS server.

For a list of all URLs and IP addresses, refer to Appendix A.

Firewall, content filter, and proxy servers.

Content filters, firewalls, and proxy servers should be configured to allow traffic on the protocols listed above to the applications' servers. In addition, session timeouts on proxy servers and other devices should be set to values greater than the average duration it takes a student to complete a given test. For more information, contact the Smarter Balanced Help Desk.

Schools will need to make sure that information is not blocked in their content filters and that data are not cached. Please ensure that the IP addresses listed in Appendix A are open for these systems.

Quality of Service (QoS)/Traffic shaping.

If the client network utilizes any device(s) that performs traffic shaping, packet prioritization, or Quality of Service, the IP addresses should be given a high level of priority in order to guarantee the highest level of performance.

Certificate revocation list.

Schools should open their firewalls to allow the secure browser to check the certificate authenticity at Symantec VeriSign's Certificate Revocation List (CRL) at <http://crl.verisign.com/>.

Symantec Verisign Recommendations

Note: The following information was provided by [Symantec](#).

It is strongly recommended that any firewall policies and/or access control devices use URLs and not IP addresses. Symantec can change these IP addresses at any time without notification. If possible white list the following entries on your firewall policies and/or access control devices to ensure seamless access to our OSCP services:

- *.thawte.com
- *.geotrust.com
- *.ws.symantec.com

Note: If white listing wildcard entries is not permitted, you can white list the following specific fully qualified domain names (FQDNs):

- oscp.ws.symantec.com
- oscp.geotrust.com
- oscp.thawte.com

If your firewall is configured to allow only a certain set of IP addresses to be accessed from your network, you'll need to take the following actions:

1. [Get the full list of IP addresses for the new sites](#). Complete a short form and then you'll gain access to the site list.
2. Install or add the IP addresses to your existing list – do not replace the old IP addresses and your existing rules for Symantec OSCP IP addresses should not be deleted.

Current Symantec Verisign IP Addresses and Ranges

These IP addresses were obtained from Symantec Verisign on December 5, 2013. As indicated above, you may obtain an updated list of IP addresses by completing the request form.

Table 4. VeriSign IP Addresses

2.22.139.27	2.22.219.27	23.10.27.27	23.13.171.27
23.13.27.27	23.15.155.27	23.34.203.27	23.34.219.27
23.34.235.27	23.35.107.27	23.35.11.27	23.35.171.27
23.35.219.27	23.35.27.27	23.35.43.27	23.35.59.27
23.35.91.27	23.36.11.27	23.36.155.27	23.36.219.27
23.37.139.27	23.37.171.27	23.37.187.27	23.37.43.27
23.38.27.27	23.38.91.27	23.4.155.27	23.4.187.27
23.4.43.27	23.4.59.27	23.41.123.27	23.41.139.27
23.41.155.27	23.41.43.27	23.41.75.27	23.42.11.27
23.42.27.27	23.43.11.27	23.43.139.27	23.43.155.27

23.43.75.27	23.44.155.27	23.44.251.27	23.44.91.27
23.46.107.27	23.46.123.27	23.46.43.27	23.46.75.27
23.47.235.27	23.47.251.27	23.47.27.27	23.49.123.27
23.49.139.27	23.49.155.27	23.49.75.27	23.49.91.27
23.5.11.27	23.5.251.27	23.50.107.27	23.50.155.27
23.50.187.27	23.50.203.27	23.50.75.27	23.50.91.27
23.51.107.27	23.51.123.27	23.51.235.27	23.51.251.27
23.51.27.27	23.51.43.27	23.52.155.27	23.52.27.27
23.52.59.27	23.52.91.27	23.53.107.27	23.53.155.27
23.53.187.27	23.53.27.27	23.53.91.27	23.54.107.27
23.54.139.27	23.54.187.27	23.54.235.27	23.54.91.27
23.55.155.27	23.56.155.27	23.57.107.27	23.57.219.27
23.57.235.27	23.58.171.27	23.58.235.27	23.58.43.27
23.59.139.27	23.59.43.27	23.60.139.27	23.61.187.27
23.61.75.27	23.62.251.27	23.63.139.27	23.64.171.27
23.64.91.27	23.65.11.27	23.65.139.27	23.67.75.27
23.7.139.27	23.7.251.27	23.7.75.27	23.74.19.27
23.9.123.27	23.9.187.27	23.9.91.27	199.7.48.0/20
199.7.71.0/24	199.7.72.0/22	199.7.76.0/24	199.7.48.0 – 199.7.63.25
199.7.71.0 – 199.7.76.255			

Section II. Hardware Requirements

Smarter Balanced Technology Requirements

Please ensure that your school's computers meet the requirements indicated in the Smarter Balanced Technology Requirements (www.smarterbalanced.org/smarter-balanced-assessments/technology/). The information in this section provides information regarding supported operating systems and related hardware recommendations as well as requirements for monitors/screens, printers, keyboards, and headphones.

Table 5 organizes requirements and recommended specifications for each supported operating system for desktops and laptops. Table 6 provides information regarding supported mobile tablets. The supported browsers listed are for operational testing sites, not practice or training test sites.

Table 5. Hardware Requirements for Desktops and Laptops

Supported Operating Systems	Minimum Requirements for Current Computers	Minimum Recommended Specifications
Windows XP (Service Pack 3), Vista, 7, 8.0, 8.1 Server 2003 and 2008	Pentium 233 MHz 128 MB RAM 52 MB hard drive free space	1.3 GHz processor 1 GB RAM 80 GB hard drive
Mac OS X 10.4.4-10.9	Intel x86 or PowerPC G3, G4, or G5 256 MB RAM 200 MB hard drive free space	
Linux Fedora Core 6+ (K12LTSP 4.2+) Ubuntu 9-12	Pentium II or AMD K6-III 233 MHz 64 MB RAM 52 MB hard drive free space	

NComputing and Terminal Services are supported on the following platforms:

- NComputing is supported on computers running Windows XP (Service Pack 3) and Windows 7
- Terminal Services is supported on the Windows 2003 and 2008 servers

Table 6. Supported Mobile Operating Systems and Browsers

Operating System	Supported Devices*	Browsers for TA Sites	Browser for Student Sites
iOS 6.0-7.0	iPad 2, 3, and 4 th generation (Retina Display)	Safari	AIRSecureTest Mobile Secure Browser
Android 4.0.4-4.2	Google Nexus 10 Motorola Xoom Motorola Xyboard Samsung Galaxy Note (10.1) Samsung Galaxy Tab 2 (10.1)	Google Chrome	AIRSecureTest Mobile Secure Browser
ChromeOS 31+	Chromebook	Google Chrome	AIRSecureTest Mobile Secure Browser

Other Hardware Recommendations

The following information is general. Because of the myriad ways school networks and computers can be set up, we encourage you to verify diagnostics, especially with monitor resolution and headphones.

Monitor/Screen Displays

- Screen Dimensions: 10” class or larger; iPads with a 9.5” display are an accepted part of this class
- Resolution: 1024 x 768 or better

Depending on the screen size, some individuals may need to use vertical and/or horizontal scroll bars to view all test-related information. Students may also use the Zoom tool in the online test to enlarge the content on the screen.

Note about brightness/contrast:

Some test items include images that are shaded. Because monitors and screens vary widely, we cannot guarantee that the “default” settings that monitors are shipped with are optimal. Monitor settings may need to be adjusted if a student says test items with shaded images (e.g., pie charts) are very light or cannot be seen.

Printers

Test Administrators can print out test session information and can approve student requests to print stimuli or test items (for students with the print-on-request accommodation). In order to preserve test security, Test Administrators must follow the test security protocols for printed test materials.

We strongly suggest that Test Administrators be connected to a single local or network printer in the testing room. Only the Test Administrator’s computer should have access to this printer.

Special note regarding printing support:

At this time, Apple iOS devices are the only ones that have native printing support (AIR Print, which connects to printers on a wireless network). If users need to print, they must use a computer or mobile device that is connected to a printer.

For information about braille devices, please see [Section IV, Text-to-Braille Hardware and Software](#).

Keyboards

Smarter Balanced is making external keyboards a requirement for tablets for all students. Any form of external keyboard that disables the on-screen virtual keyboard is acceptable. This includes mechanical, manual, and Bluetooth-based keyboards.

Headphones

All ELA tests contain several items that have recorded audio. Students with the text-to-speech accommodation can listen to stimuli or test items being read aloud. Students with a braille accommodation can use the Job Access with Speech (JAWS®) screen reading software to listen to mathematics assessments.

Students taking an English Language Arts (ELA) test or who have a text-to-speech or braille accommodation must be provided with headphones so that they can listen to the audio in these tests. We encourage you to work with your School Test Coordinator to determine how many students will need headphones to ensure that you have an adequate supply on hand



USB headphones are recommended, as they are typically plug-and-play devices.

Text-to-speech requires the use of the secure browser. Students who require text-to-speech for the Practice and Training tests should use the secure browser.

Refer to [Section VIII, About Text-to-Speech and Voice Packs](#), for specific information on verifying that the headphones are recognized by the computer.

Section III. Software Requirements

Please ensure that your school's computer software meet the requirements indicated in the Smarter Balanced Technology Requirements (www.smarterbalanced.org/smarter-balanced-assessments/technology/).

Disabling Pop-Up Blockers

The Test Administrator Interface and TIDE Web sites require pop-up windows to be enabled. Your school administrator or IT staff designee may be able to disable pop-up blockers ahead of time. Navigate to the appropriate menu option to disable pop-up blockers.

To disable pop-up blockers:

- **Firefox:** Tools > Options > Content > uncheck "Block pop-up windows"
- **Google Chrome:** Menu > Settings > Show advanced settings (at the bottom of the screen) > Privacy > Content Settings > Pop-ups > click "Allow all sites to show pop-ups"
- **Internet Explorer:** Tools > Pop-up Blocker > Turn Off Pop-up Blocker
- **Safari:** Application Menu (Safari) > Block Pop-Up Windows (make sure this is unchecked)

Installing the Verdana Font on Linux Machines

Some test items use the Verdana font. Please ensure that you have Verdana appropriately installed on all Linux machines that will be used for testing.

Microsoft TrueType fonts like Verdana are freely available for download and installation on computers running Linux. However, the End User License Agreement for these fonts restricts their direct inclusion in Linux distributions. Therefore, these fonts must be installed as an add-on. Please refer to the Linux secure browser installation document for additional information.

- **Fedora Core 6+ users**
Follow the steps in the "How to Install" section of this website: <http://corefonts.sourceforge.net/>. You will need to build an rpm package of the fonts prior to installing them.
- **Ubuntu 9–12 users**
In a terminal window, enter the following command to install the msttcorefonts package:

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

Special Note for Windows Users: Fast User Switching

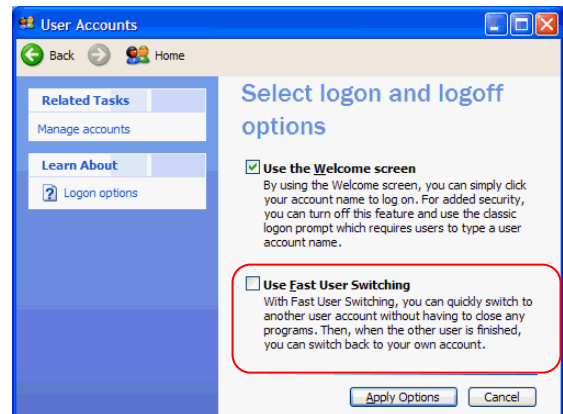
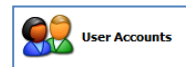
Microsoft Windows (XP with Service Pack 3, Vista, 7, 8.0, and 8.1) allows computers to be configured so that multiple users can log into a computer without requiring one user to log out before another logs in. This feature is called “fast user switching.”

If a student can access multiple user accounts from a single computer, we strongly encourage you to disable the Fast User Switching function. Instructions for doing so follow.

Disabling Fast User Switching in Windows XP (with Service Pack 3)

1. Click [**Start**], click [**Control Panel**], and then click [**User Accounts**].
2. Click [**Change the Way Users Log On or Off**].
 - a. Ensure the **Use the Welcome Screen** option *is* checked.
 - b. Ensure the **Use Fast User Switching** option is *not* checked.
3. Click [**Apply Options**].

**Note: Fast User Switching is not an option if joined to a domain.*

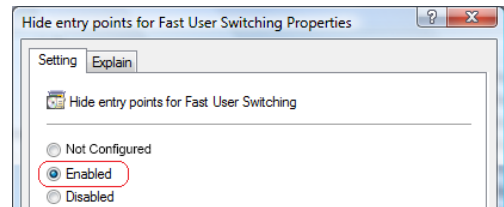
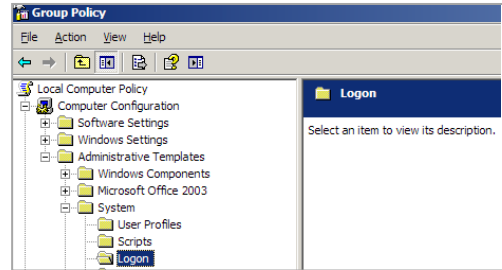
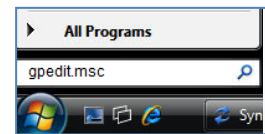


Disabling Fast User Switching in Windows Vista or 7

Method A: Access the Group Policy Editor

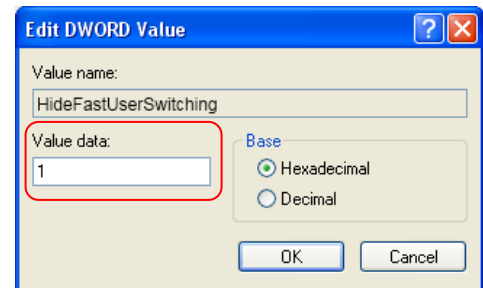
1. Click [**Start**], type **gpedit.msc** in the **Start Search** dialog box, and then press [**Enter**].
2. Navigate to the following location:
Local Computer Policy > Computer Configuration > Administrative Templates > System > Logon
3. Set **Hide entry points for Fast User Switching** to **Enabled**.
4. Close the Fast User Switching properties window.
5. Close the Group Policy window.

Note: Because the Group Policy Editor does not exist in certain editions of Windows Vista, you may need to configure these settings via the registry if this method is unavailable. See Method B for registry instructions.



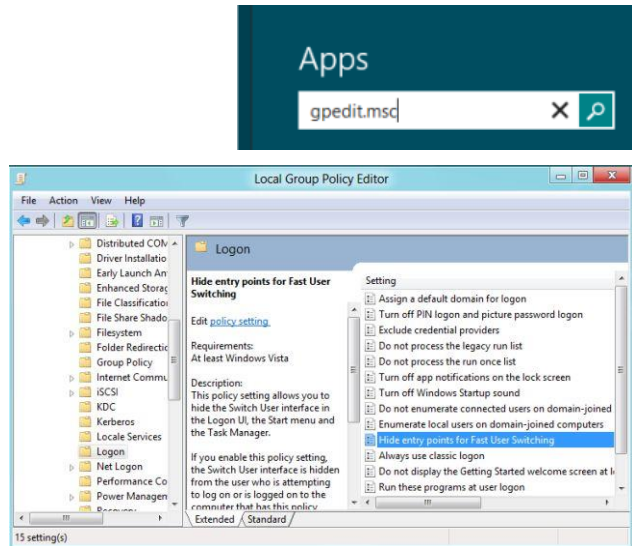
Method B: Access the Registry

1. Click [**Start**], type **regedit.exe** in the **Start Search** dialog box, and press [**Enter**].
2. Navigate to the following location:
HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Windows > CurrentVersion > Policies > System
3. Right-click the **System** folder in the left pane.
4. Click **New, DWORD (32-bit) value**.
5. Type in **HideFastUserSwitching** and press [**Enter**].
6. Click the **HideFastUserSwitching** value.
7. Type **1** into the *Value data* field and click [**OK**].
8. Close the Registry Editor window.

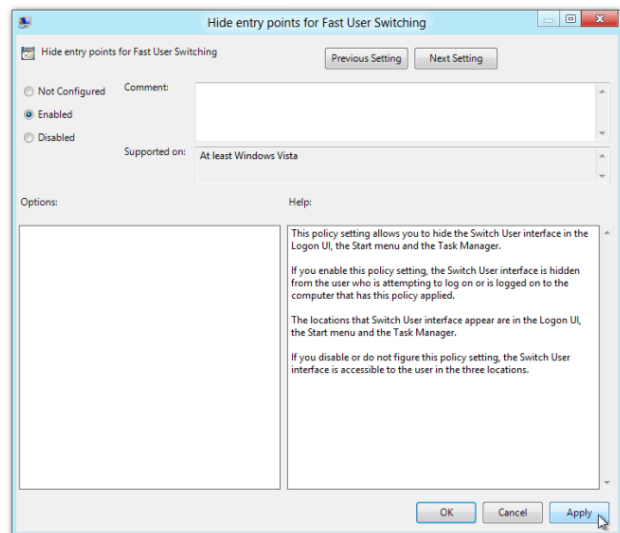


Disabling Fast User Switching in Windows 8.0 and 8.1

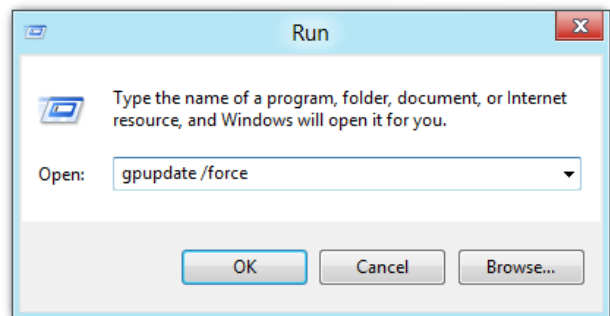
1. Navigate to the Search option (from the home screen, mouse to the lower right corner and then click the Search icon).
2. In the search box, type **gpedit.msc**. Double-click the **gpedit** icon in the Apps pane. The Local Group Policy Editor window will open.
3. Navigate to the following location:
Computer Configuration > Administrative Templates > System > Logon
4. In the Setting pane, double-click “Hide entry points for Fast User Switching.”



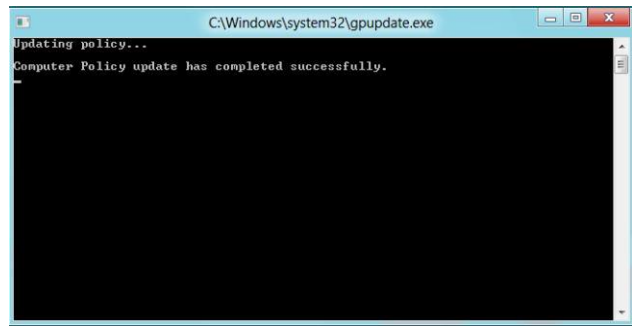
5. Select “Enabled” and then click [OK].



6. Navigate to the Search option (from the home screen, mouse to the lower right corner and then click the Search icon).
7. In the search box, type **run**. The Run dialogue box will open.
8. Enter the command **gpupdate /force** into the text box and then click [OK].
(Note the space before the backslash.)



-
9. The Windows system command box will open. When you see the message “Computer Policy update has completed successfully,” then Fast User Switching has been successfully disabled.



Section IV. Text-to-Braille Hardware and Software

Braille Hardware

The following devices are to be used for students accessing tests with a braille accommodation.

- **For students:** A refreshable braille display. We recommend that the display have a minimum of 40 cells.
- **For Test Administrators:** View Plus Tiger Max Embosser



Reminder: All printed test materials for secure tests must be shredded immediately after a test session ends.

Braille Software

Requirements for Student Computers

- The Student Testing Site currently supports the braille interface on Windows 7 machines only.
- Windows Secure Browser 6.3 must be installed on all machines used for student testing, including tests administered using the Braille interface.
- JAWS Screen Reader (version 12, 13, or 14).
- Refreshable braille display that is compatible with Windows 7 and the version of JAWS that is on the computer. We recommend that the braille display have a minimum of 40 cells.

For more information about JAWS, including product download and purchase, go to <http://www.freedomscientific.com/products/fs/jaws-product-page.asp>.



The following JAWS configuration must be applied to each student computer prior to administering tests using the Braille interface:

1. Configure JAWS to recognize the Secure Browser.
2. Apply settings for Contracted/Uncontracted Braille through JAWS.

Instructions for each requirement follows.

Configure JAWS to Recognize the Secure Browser

1. Open the JAWS **ConfigNames.ini** file.

This file is accessible via the start menu (/All Programs/JAWS 12.0/Explore JAWS/Explore Shared Settings/).

2. Locate the line of text that contains “Chrome=Firefox.” Create a line immediately following this text, and add the following string:

```
SBACSecureBrowser6.3=Firefox
```

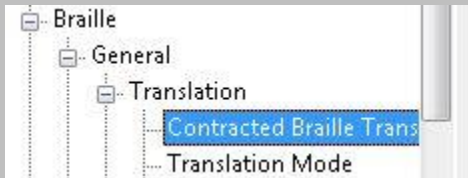
3. Save the file upon completion.

If you receive an error that you do not have permission to save the .ini file to this location, you will first need to save the file to your desktop as **ConfigNames.ini**. After saving the updated .ini file, copy it to the folder containing the original .ini file (referenced in Step 1). You will need to confirm that you want to replace the original file with the file you created.

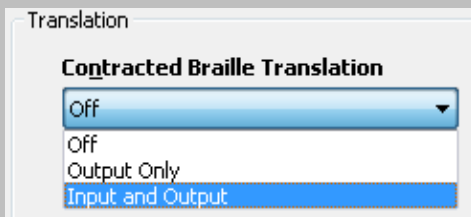
Applying Settings for Contracted/Uncontracted Braille

In order for students to use Contracted or Uncontracted Literary Braille, the correct JAWS setting must be applied *prior* to launching the secure browser.

1. Open the **JAWS Settings Center**. The Settings Center is accessible via the JAWS Menu > Utilities.
2. Select **Firefox** from the “Application” drop-down menu.
3. From the panel on the left side of the window, go to the following option (as pictured):
Braille > General > Translation > Contracted Braille Translation

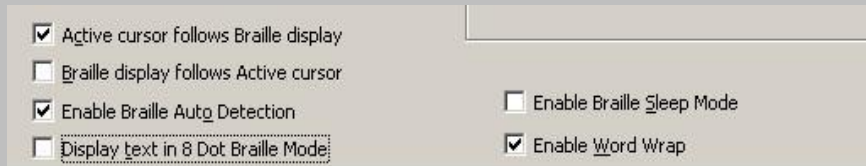


4. For **Uncontracted Braille**, set the value to “Off.”
 For **Contracted Braille**, set the value to “Input and Output.”



Additionally, ensure that the following three settings are checked (and only these settings are checked):

- Active cursor follows Braille display
- Enable Braille Auto Detection
- Enable Word Wrap



5. Click **[Apply]** and then click **[OK]**.



In addition, the following optional JAWS settings may be adjusted for individual students based on student needs prior to administering their assessments.

- Adjust JAWS voice profile (Optional)
- Adjust JAWS speaking speed (Optional)
- Adjust JAWS punctuation (Optional)

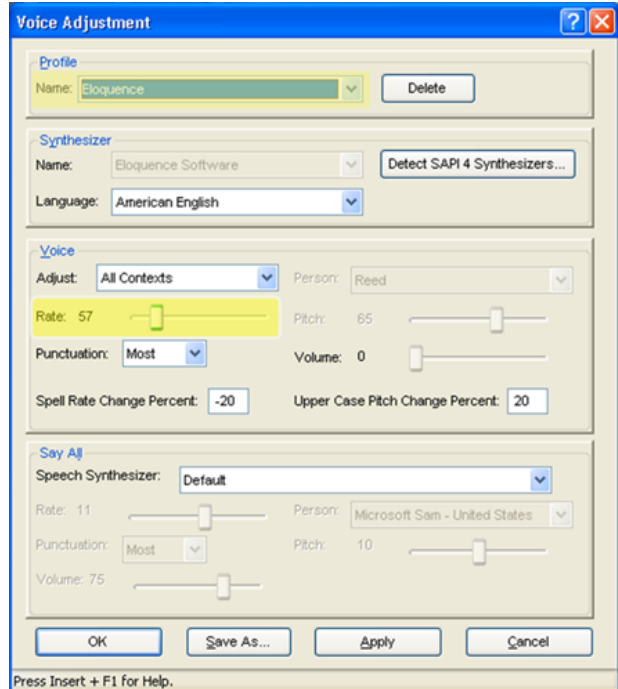
Instructions for each option follows.

If adjusting these optional settings for a student, the steps described for each option must be taken prior to launching the secure browser.

Adjusting JAWS Voice Profile

The JAWS voice profile refers to the voice used by JAWS. Users can adjust the JAWS voice profile by following the instructions below.

1. Go to *JAWS Menu > Options*.
2. Select *Voices > Adjustment*.
3. In the *Profile* section, select a Voice Profile from the Name drop-down menu.
4. Click [OK].



Adjusting JAWS Speaking Rate

Users can adjust the rate of speed that JAWS speaks by following the instructions below.

1. Go to *JAWS Menu > Options*.
2. Select *Voices > Adjustment*.
3. In the *Voice* section, adjust the “Rate” using the slide-bar.
4. Click [OK].

Adjusting JAWS Punctuation

The default JAWS punctuation setting for which the Braille Interface has been optimized is “Most.” This means that JAWS will read most punctuation that appears on the screen. However, users may adjust the JAWS punctuation based on an individual student’s needs and preferences by following the instructions below.

1. Go to *JAWS Menu > Options*.
2. Select *Voices > Adjustment*.
3. In the *Voice* section, select a punctuation setting from the Punctuation drop-down menu. The options include “None,” “Some,” “Most,” and “All.”
4. Click [OK].



Warning regarding ELA assessments and text-to-speech and JAWS

The secure browser is designed to automatically mute audio on ELA assessments. As a result, the sound on the student’s computer will be automatically muted when the student begins the first question on the braille form of the ELA assessment he or she is taking. The sound will automatically turn on again when the student submits the ELA assessment or pauses the test and returns to the login screen.

As a result, students who use the secure browser to access the practice ELA assessments may be unable to hear listening stimuli associated with items. Students may also require assistance with JAWS navigation because they will not be able to hear the JAWS commands. JAWS will still output all commands and text to the refreshable braille display, even with the sound muted.

If you want students to have access to audio during the practice ELA assessments, we recommend using Firefox instead of the secure browser.

Requirements for Test Administrator Computers

TAs administering tests to students who require Braille must have the following software installed on their machine prior to testing. The software is necessary to process these students' print requests.

- **Duxbury Braille Translator 11.1**

This software allows printing of items and reading passages (without images) and can be downloaded from <http://www.duxburysystems.com/dbt.asp?product=DBT%20Win>.

For Oregon users: To download the Duxbury Braille Translator software and acquire a license, contact the BVIS fund administrator for the seat license code.

- **ViewPlusTiger Max Embosser** and the supporting **ViewPlus Desktop Embosser driver**

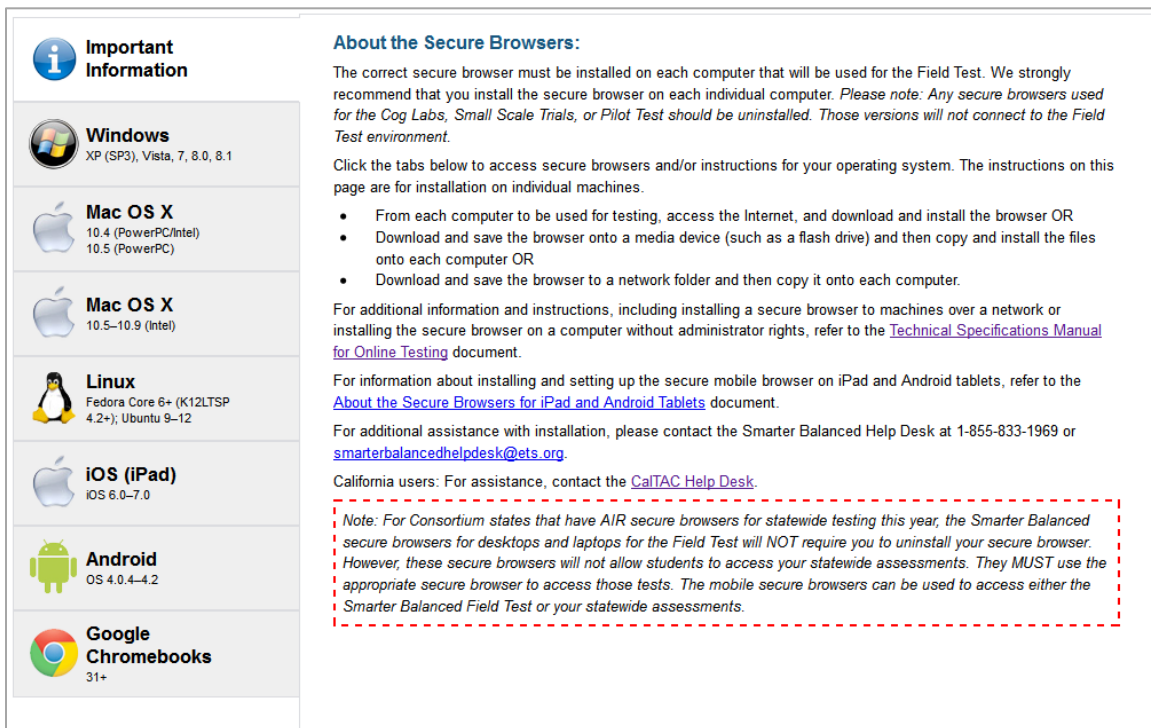
The Desktop Embosser Driver can be downloaded from <http://downloads.viewplus.com/drivers/desktop-braille-embosser/>. The download includes the Tiger Viewer software, which is needed to handle print requests for items and passages that contain tactile or spatial components.

Section V. Secure Browser Installation

All students must use the Smarter Balanced secure browser to access the Field Test. The secure browser prevents students from accessing other computer or Internet applications or copying test information. All computers that will be used for testing must have the correct secure browser installed.

The appropriate secure browser must be installed on each computer that will be used for online testing. All secure browsers can be accessed from the [Smarter Balanced portal](http://sbac.portal.airast.org) (sbac.portal.airast.org).

Figure 1. Smarter Balanced Portal Secure Browser Page



The screenshot shows a webpage titled "About the Secure Browsers:" with a sidebar on the left containing "Important Information" and a list of operating systems: Windows (XP, Vista, 7, 8.0, 8.1), Mac OS X (10.4, 10.5, 10.5-10.9), Linux (Fedora Core 6+, Ubuntu 9-12), iOS (iPad) (6.0-7.0), Android (4.0.4-4.2), and Google Chromebooks (31+). The main content area includes instructions for installation, a note about uninstalling previous versions, and a note for Consortium states regarding statewide testing.

Secure browsers are available for the following operating systems:

- Windows XP (Service Pack 3), Vista, 7, 8.0, and 8.1
- Mac 10.4 (PowerPC or Intel processors) and 10.5 with PowerPC processors
- Mac 10.5, 10.6, 10.7, 10.8, and 10.9 with Intel processors
- Linux Fedora Core 6 and Ubuntu 9–12
- Apple iOS 6.0–7.1
- Android 4.0.4–4.2
- Chrome OS 31+



For Consortium states that already have AIR desktop secure browsers for statewide testing, the secure browsers for Smarter Balanced administrations will NOT require you to uninstall your secure browser. **However, this secure browser will not allow students to access your statewide assessments.** Students MUST use the appropriate secure browser to access those sites.

The secure browser should be installed on each individual computer that will be used for student testing. You can install the secure browser on each individual computer, either one-by-one or through a network.

One-by-One (Manual) Installation for Desktops and Laptops

- From each computer to be used for testing, access the Internet and download and install the browser OR
- Download and save the browser onto a media device (such as a flash drive) and then copy and install the files onto each computer OR
- Download and save the browser to a network folder and then copy it onto each computer.

For any of these options, go to the secure browsers page and download and install the browser to your desired location (an individual computer, a media device, or a network folder).

Network Installation (Network Administrators)

You can push the browser out to all computers through a network by copying browser files from the network to individual computers or through third-party programs to run the installers, such as Apple Remote Desktop.

For additional information, read the [Network Installation for Windows \(Network Administrators\)](#) and [Network Installation Information for Mac OS X](#) sections.

Installation without Administrator Rights

If you must install the secure browser on computers to which you do not have administrator or installation rights, read the [Installing the Secure Browser on Computers without Administrator Rights \(Windows\)](#) section.

Windows Secure Browser (Version 6.3)

This section provides instructions for installing the Windows secure browser on computers with Windows XP (Service Pack 3), Vista, 7, 8.0, or 8.1. Other Windows operating systems are not supported.

You must install version 6.3 of the secure browser on each computer that will be used for online testing.

Note: The installation file for Windows computers is an .msi file, which requires administration rights. The steps below assume an administrator is installing the secure browser.

Installing Windows Secure Browser 6.3.

Manually Installing the .msi Package via the User Interface:

1. From the Windows section on the Download Secure Browser page on the Smarter Balanced portal, click the **[Download Browser]** link. A dialog box will pop up.
Note: This step may vary slightly depending on the browser you are currently using.
 - If presented with a choice to either “Run” or “Save” the file, select “Run.” This will install the secure browser directly without the need to save the installation package to your computer.
 - If you receive a Security Warning at this point, select “Run” from the preceding dialog box.
 - If presented only with the option to **[Save]**, save the file to a convenient location, such as the desktop.
 - Double-click the installation file (SBACSecureBrowser6.3-Win.msi) to open the Secure Browser Setup Wizard. (*Note: This step applies only to users who saved the file to their computer. Users who selected “Run” in Step 1 can go directly to Step 2.*)
2. From the Secure Browser Setup Wizard, follow the instructions on the screen to finish installation. Select the *Standard* installation option to install the browser in its default location: C:\Program Files\SBACSecureBrowser6.3.
3. Click **[Finish]** to launch SBAC Secure Browser 6.3 directly from the Setup Wizard OR double-click the SBAC Secure Browser 6.3 icon that is on the desktop.
4. Upon launching the secure browser, you will see the student login screen.
Note: The browser will fill the entire screen.
5. Click **[Close]** in the upper right corner to exit the browser.

Note: You can also use the following keyboard command to close the Windows secure browser: [Ctrl] + [ALT] + [SHIFT] + [F10]. (If you are using a laptop, you may also need to press the [FN] key before you press F10.)

Installing the .msi package via a script.

Network administrators can install the Windows secure browser via an installation script to be executed by an Admin account in the machine. The script can be written to run without any human interaction (quiet switch) and to install in the default directory (C:\Program Files) or any target directory of choice. Un-installation can also be scripted.

Below are two *generic* scripts: one for installation and one for uninstallation. Both require the script to have visibility to the .msi installation file and can only be executed by an admin account on the machine. (This is a Windows-based restriction, not a secure browser restriction, as the msiexec service that installs .msi files is meant to be used by administrators only.)

Script Conventions:

<Source> = Complete path to the Secure Browser 6.3 msi installation file including .msi installation file name

Example: C:\MSI\SBACSecureBrowser6.3-win.msi

<Target> = Complete path to the location where the Secure Browser should be installed if the default location (C:\Program Files) is not preferred.

Example: C:\MSI\Installation_Dir

Note: the target install directory does not have to be created in advance.

1. **Installation script:** `msiexec /I <Source>/quiet INSTALLDIR=<Target>`

Example: `msiexec /I C:\MSI\ SBACSecureBrowser6.3-win.msi /quiet
INSTALLDIR=C:\MSI\Browser_Install`

2. **Uninstallation script:** `msiexec /X <Source>/quiet`

Example: `msiexec /X C:\MSI\SBACSecureBrowser6.3-win.msi /quiet`

Manually uninstalling the previous Windows secure browser.

If you need to uninstall the previous secure browser for any reason, follow the steps below.

1. Open the Control Panel (from your taskbar, select *Start > Settings > Control Panel*).
2. Select **Add or Remove Programs**.
3. Select SBACSecureBrowser6.0 and click [**Remove**] to open the Uninstall Wizard.
4. Click [**Next**].
5. Click [**Uninstall**] to remove the secure browser.
6. Click [**Finish**] to complete the uninstall process.

Mac OS X Secure Browser for 10.4 and 10.5 (Version 5.6)

This section provides instructions for installing secure browser 5.6 on the following computers:

- Mac 10.4 computers with *either* PowerPC or Intel-based processors
- Mac 10.5 computers with PowerPC processors

How do I know if my Mac 10.5 computer is using a PowerPC or Intel-based processor?

From the Apple drop-down menu, click “About This Mac.” The screen will indicate the operating system version and processor your computer is using.

- If you are using 10.4, download and install secure browser 5.6 using the instructions in this section. (The processor type does not matter.)
- If you are using 10.5 and you see PowerPC, download and install secure browser 5.6 using the instructions in this section.
- If you are using 10.5 and you see Intel, refer to the [Mac OS X Secure Browser for 10.5–10.9 \(Version 6.3\)](#) section for instructions.

Use Secure Browser 5.6



Use Secure Browser 6.3



You must install version 5.6 of the secure browser on all Mac 10.4 and 10.5 computers with PowerPC processors that will be used for online testing. We strongly recommend that you install the secure browser on each individual computer. *Please note: Students must have the correct secure browser in order to access the online assessments.*

Installing Secure Browser 5.6 for Mac OS X 10.4 and 10.5 (with PowerPC).

1. From the Mac OS X 10.4 and 10.5 section on the Download Secure Browser page on the Smarter Balanced portal, click the **[Download Browser]** link. *(If prompted for a download location, select the desktop.) Note: This step may vary slightly depending on the browser version you are using.*
 - If your browser automatically expands the Zip file, you can proceed to Step 3.
 - If your computer opens the Software License Agreement page, proceed to Step 4.
 - If you receive a warning message that the file contains an application, click **[Continue]** and proceed to Step 4.
2. Open the file (SBACSecureBrowser5.6-OSX.dmg) to expand its contents. Double-click the file (SBACSecureBrowser5.6-OSX.dmg) to mount the SBACSecureBrowser5.6 folder on the desktop. *Note: Your computer may automatically expand the file upon download.*
3. Double-click the mounted folder (SBACSecureBrowser5.6).
4. Click **[Accept]** on the Software License Agreement Page.
5. Drag the SBACSecureBrowser5.6 icon to your Applications folder.
Important: *The secure browser must be launched at this point to successfully complete the installation. The browser will disable Exposé (hot corner) settings if they are set and they will remain disabled after the browser is closed. The dock will appear the first time the Exposé settings are being disabled on browser launch. System security will not be affected as applications opened from the dock open in the background and cannot be accessed.*
6. Double-click the **SBACSecureBrowser5.6** icon in the Applications folder to launch the secure browser. Upon launching the secure browser, you will see the student login screen. *Note: The browser will fill the entire screen.*
7. Click **[Close]** in the upper right corner to exit the browser.
Note: You can also use the following keyboard command to close the Mac OS X secure browser: [Ctrl] + [ALT] + [SHIFT] + [F10]. (If you are using a laptop, you may also need to press the FN key before you press F10.)

Uninstalling the previous Mac OS X secure browser.

If you need to uninstall the secure browser for any reason, follow these instructions.

There may be a folder on the desktop named SBACSecureBrowser5.5. Simply drag the folder and related files to the Trash. If the browser was installed to a different location, please be sure to remove it accordingly.

Mac OS X Secure Browser for 10.5–10.9 (Version 6.3)

This section provides instructions for installing secure browser 6.3 on computers with OS 10.5–10.9 and that have Intel-based processors. (Some Mac 10.5 computers have PowerPC processors and others have Intel-based processors. All Mac computers shipped with OS 10.6, 10.7, 10.8, or 10.9 have Intel-based processors.)

Information about disabling Spaces on Mac 10.7, 10.8, and 10.9 computers is also included in this section.

How do I know if my Mac 10.5 computer is using a PowerPC or Intel-based processor?

From the Apple drop-down menu, click “About This Mac.” The screen will indicate the operating system version and processor your computer is using.

- If you see PowerPC, refer to the *Installing Secure Browser 5.6 for Mac OS X* section for instructions.
- If you see Intel, download and install secure browser 6.3 using the instructions in this section.

Use Secure Browser 5.6



Use Secure Browser 6.3



You must install version 6.3 of the secure browser on all Mac 10.5, 10.6, 10.7, 10.8, and 10.9 computers with Intel processors that will be used for online testing. We strongly recommend that you install the secure browser on each individual computer. *Please note: Students must have the correct secure browser in order to access the online assessments.*

Installing Secure Browser 6.3 for Mac OS X 10.5–10.9 (with Intel).

1. From the Mac OS X 10.5–10.9 section of the Secure Browser page on the Smarter Balanced portal, click the **[Download Browser]** link. (If prompted for a download location, select your desktop.) *Note: This step may slightly vary depending on the browser you are currently using.*
 - If your browser automatically expands the Zip file, you can proceed to Step 3.
 - If your computer opens the Software License Agreement page, proceed to Step 4.
 - If you receive a warning message that the file contains an application, click **[Continue]** and proceed to Step 4.
2. Open the file (SBACSecureBrowser6.3-OSX.dmg) to expand its contents. Double-click the file (SBACSecureBrowser6.3-OSX.dmg) to mount the SBACSecureBrowser6.3 folder on the desktop. *Note: Your computer may automatically expand the file upon download.*
3. Double-click the mounted folder (SBACSecureBrowser6.3).
4. Click **[Accept]** on the Software License Agreement page.
5. Drag the SBAC Secure Browser 6.3 icon to your Applications folder.
Important: *The secure browser must be launched to successfully complete the installation.*
 - For **Mac 10.5**, the secure browser will disable Exposé (hot corner) settings if they are set and they will remain disabled after the browser is closed.
 - For **Mac 10.6**, Exposé settings will be disabled only when the secure browser is launched. The dock will appear the first time the Exposé settings are being disabled on browser launch. System security is not affected as applications opened from the dock open in the background and cannot be accessed.
 - For **Mac 10.7, 10.8, and 10.9**, Spaces must be manually disabled before student can use the secure browser. Instructions for disabling the Spaces feature are on the next page.
6. Double-click the **SBACSecureBrowser6.3** icon in the Applications folder to launch the secure browser. Upon launching the secure browser, you will see the student login screen. *Note: The browser will fill the entire screen.*
7. Click **[Close]** in the upper-right corner to exit the browser.

Note: You can also use the following keyboard command to close the secure browser: [Ctrl] + [ALT] + [SHIFT] + [F10]. (If you are using a laptop, you may also need to press the [FN] key before you press [F10].)

Uninstalling the previous Mac OS X secure browser.

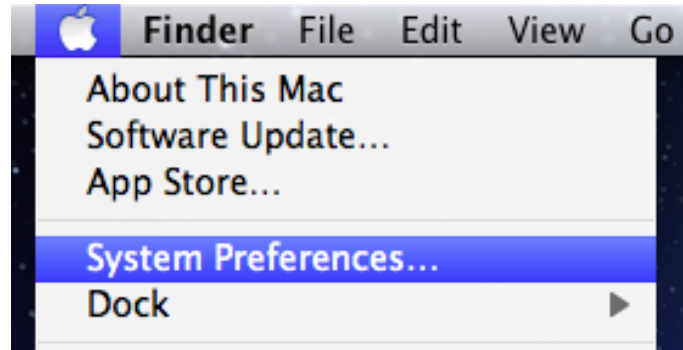
If you need to uninstall the secure browser for any reason, follow these instructions.

There may be a folder on the desktop named SBACSecureBrowser6.1. Simply drag the folder and related files to the Trash. If the browser was installed to a different location, please be sure to remove it accordingly.

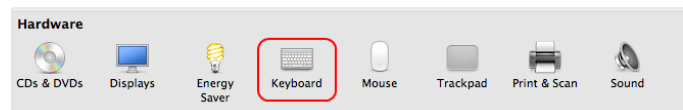
Disabling Spaces in Mission Control on Mac 10.7–10.9 computers.

Follow the instructions below to disable Spaces. Spaces should be disabled on computers that students will be using.

1. Navigate to Apple → System Preferences



2. In System Preferences, click the [Keyboard] icon. The Keyboard window will be displayed.

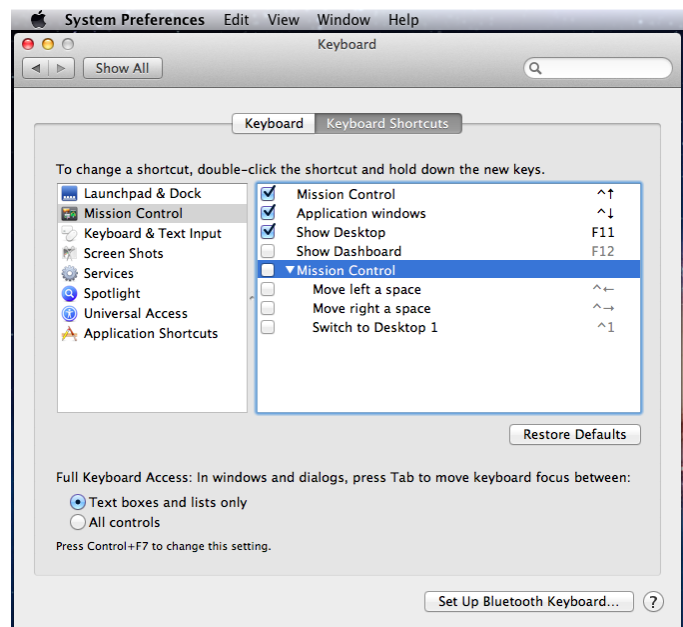


3. Click the [Keyboard Shortcuts] tab. The Keyboard Shortcuts options will be displayed.



Note: Mac 10.9 uses the label [Shortcuts].

4. In the left panel, click “Mission Control.” The right panel will show all Mission Control options.
5. In the right panel, make sure the boxes for the following are NOT checked:
 - Move left a space
 - Move right a space
 - Switch to Desktop 1 (this may already be unchecked.)



6. To re-enable Spaces, follow steps 1–4 again, and check the boxes for spaces.

Mac computers and keyboard options for opening applications.

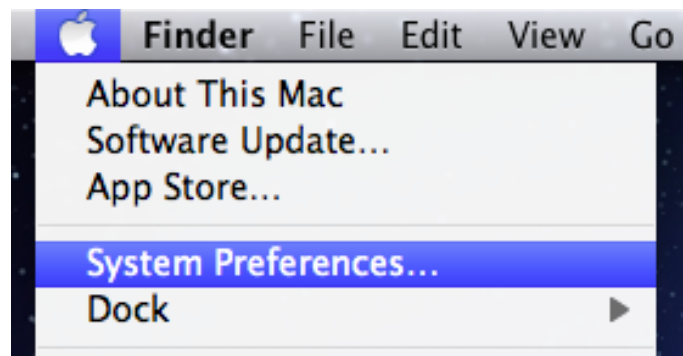
When students use the secure browser for testing, the Test Delivery System conducts regular checks to ensure that other applications are not open. These checks help maintain the integrity of the secure test environment.

Some schools may have Mac computers with keyboards that are configured to launch iTunes and other applications by using direct function keys (e.g., F8). This section contains information on how to disable the function keys for launching applications, including iTunes.

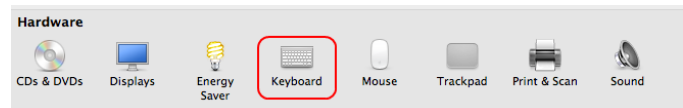
These instructions are based on Mac 10.8 and should be similar for users with other supported Mac OS versions (10.4 and above).

Modifying Keyboard Options in Mac 10.8

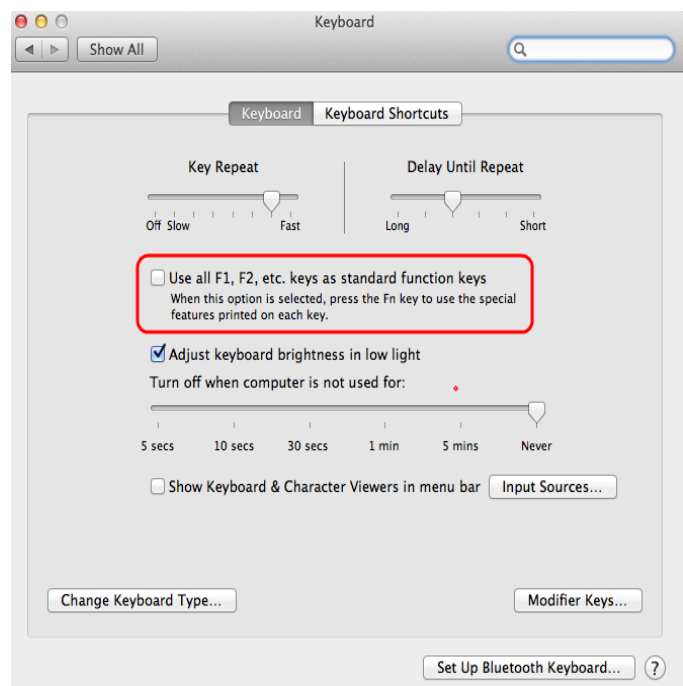
1. Navigate to Apple → System Preferences



2. In System Preferences, click the **[Keyboard]** icon. The Keyboard window will be displayed.



3. On the Keyboard preferences window, you will see an option regarding using all function keys as standard function keys. **Check this option.**



Once this option is checked, you should no longer be able to access applications by simply pressing the 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.

Linux Secure Browser (Version 6.3)

This section provides instructions for installing the Linux secure browser on computers with Linux Fedora Core 6+ (K12LTSP 4.2 and above) or Ubuntu 9–12.

You must install version 6.3 of the secure browser on each computer that will be used for online testing. We strongly recommend that you install the secure browser on each individual computer. *Please note: Students must have the correct secure browser in order to access the online assessments.*

Installing Linux Secure Browser 6.3.

1. From the Linux tab on the Download Secure Browser page on the Smarter Balanced portal, click the [**Download Browser**] link and save the file to your desktop.
2. Right-click the downloaded file (SBACSecureBrowser6.3-Linux.tar.bz2), and select “Extract Here” to expand the file. This creates the SBACSecureBrowser6.0 folder on the desktop.
Note: To expand the compressed image using command line, use the following command:

```
tar jxvf SBACSecureBrowser6.3-Linux.tar.bz2
```

3. Open the SBACSecureBrowser6.3 folder.
 - Double-click the file “install-icon.sh” and select “Run” from the prompt. (*Note: This will create the “SBACSecureBrowser6.3” icon on the desktop.*)*
4. From the desktop, double-click the **SBACSecureBrowser6.3** icon to launch the browser.
5. Upon launching the secure browser, you will see the student login screen.
Note: The browser will fill the entire screen.
6. Click [**Close**] in the upper right corner to exit the browser.

Note: You can also use the following keyboard command to close the Linux Secure Browser: [CTRL] + [ALT] + [SHIFT] + [ESC]. (If you are using a laptop, you may also need to press the [FN] key before you press F10.)

* If you do not want to run the installer, you can extract the files by opening the SBACSecureBrowser6.0 file and selecting “Run” from the options in the message dialog box.

Uninstalling the Linux secure browser.

If you need to uninstall the secure browser for any reason, follow these instructions.

There should be a folder on the desktop named SBACSecureBrowser6.3. Simply drag the folder and the secure browser icon from the Desktop to the Trash. If the browser was installed to a different location, please be sure to remove it accordingly.

Linux 64-bit Machines and the secure browser.

The secure browser is a 32-bit browser. If you have Linux machines that are 64-bit, the secure browser will not launch properly. This is because 64-bit versions of Linux typically do not have 32-bit compatibility libraries installed.

In order for the secure browser to run, the 32-bit compatibility library for your Linux version must be installed. As the commands for doing so vary between Linux distributions, we encourage you to check the documentation for your specific Linux version or setup.

The following command prompts should work for supported versions of Fedora Core 6 K12LTSP and Ubuntu:

Fedora Core 6+ K12LTSP 4.2+: `yum install glibc.i686`

Note: You must run this command as the root user.

Ubuntu: `sudo apt-get install ia32-lib`

Network Installation for Windows (Network Administrators)

You can install the secure browser to all computers on a network by copying browser files from the network to individual computers or through third-party programs to run the installers, such as Apple Remote Desktop.

This section contains information for installing the secure browser via a network. Please follow the appropriate instructions for your network setup.

Installing the secure browser to a shared drive.

1. Install the browser onto your server, following the standard directions available in this document.
2. **Map the network directory** to where you installed the secure browser (in Step 1) on each client machine.
 - a. In the network location where you installed the secure browser, create a shortcut by right-clicking the **SBACSecureBrowser6.3.exe** icon and selecting “Create Shortcut.”
 - Optional: You may want to rename the new shortcut; e.g., SBACSecureBrowser6.3. (This becomes your shortcut link name that you will use in Step 3.)
 - b. In the properties of the shortcut, change the path to **SBACSecureBrowser6.3.exe** to use the mapped path as if on the client machine.
3. To each user (computer) profile, add the following command, which will execute upon login through the user group login script:

```
COPY "<X> \SBACSecureBrowser6.3.1nk" "%USERPROFILE%\Desktop"
```

Note: <X> refers to the shared directory from which the browser will be run. The script will need to reference the correct directory.

Pushing the secure browser installation directory from the network to client computers.

1. Install the browser onto your server, following the standard directions available in this document.
2. Identify the network directory to which you saved the browser file. These instructions will refer to that network directory as <X>.
3. Identify the *target* directory on the local user computers that you will copy the browser file to. These instructions will refer to that directory as <Y>. Make sure that you have *write access* to <Y> on the local computers.

Note: Restricted users will have access only to certain folders on the local computers.

4. Create a shortcut in the network directory by right-clicking the **SBACSecureBrowser6.3.exe** icon and selecting "Create Shortcut." Rename the new shortcut, e.g., "SBACSecureBrowser6.3."

Note: In the shortcut Properties, the "Target" and "Start In" attributes will show the <X> network installation directory.

5. Change the shortcut properties ("Target" and "Start In" attributes) to the local computers' <Y> directory instead of the default <X> network directory. That way the secure browser shortcut will now point to the designated installation directory.
6. Add the following lines to the login script for each user, replacing your actual local and source network directories for <Y> and <X>.

```
IF EXIST <Y> GOTO DONE
XCOPY "<X>" "<Y>" /E /I
COPY "<Y>\SBACSecureBrowser6.3.1nk" "%USERPROFILE%\Desktop"
:DONE
EXIT
```

Installing the Secure Browser on Computers without Administrator Rights (Windows)

We strongly recommend that you install the secure browser on each individual computer. However, if you must use a shared network setup without administrator rights, follow the instructions below.

Once you have installed the browser on one machine, you can simply copy it to restricted accounts on other machines.

1. On a computer on which you have installation rights, download and install the browser, following the standard directions available in this document.
2. Copy the entire folder where the browser was installed (usually, "C:\Program Files\SBACSecureBrowser6.3") to a removable drive or shared network location.
3. Copy the entire directory from the shared location or removable drive to any directory on the target computer.
4. Drag the **SBACSecureBrowser6.3.exe** icon to the desktop to create a convenient shortcut.

Terminal Server/Thin Client Installation (Windows)

The following steps should be taken when computers on a Terminal Services network setup have a shared or generic login account and multiple users need to use that same account when logging into Terminal Services.

1. Create a batch file that runs the logon script for the secure browser.

This creates a unique profile folder in “Application Data” with a unique session name. This can be placed in the “Startup” folder on the “Start” menu (Start → Programs → Startup).

- a) As the Administrator, open Notepad.
- b) Copy and paste the below line into the Notepad file:

```
"C:\Program Files\SBACSecureBrowser6.3\SBACSecureBrowser6.0.exe"  
-CreateProfile %SESSIONNAME%
```
- c) Save the file as a batch file to the desktop (you may call it anything; e.g., **logon.bat**).
- d) Go to “User Configuration,” which is in the Group Policy.
 - Start Menu → Run → type GPEdit.msc → Click [OK]
- e) Navigate to ‘User Configuration’ and expand the ‘Windows Settings’ folder.
- f) Click “Scripts (Logon/Logoff).”
- g) Select “Logon” and go to “Properties” (either by clicking the Properties link on the left or right-clicking “Logon” and selecting “Properties”).
- h) In the “Logon Properties” window, click the [Add] button.
- i) Browse for the “Logon” batch file that you created in Step B.
- j) Click the [OK] button to add the file.
- k) Click the [APPLY] button and the close the “Logon Properties” window.
- l) Close the “Group Policy” window.

2. Create a shortcut on the desktop of each client machine.

This will create shortcuts for the secure browser on the client machines.

- a) On the Terminal Server machine, locate the Secure Browser folder.
C:\Program Files\<<SecureBrowserName> folder\
- b) Right-click the **SBACSecureBrowser6.3.exe** file and select “Send To → Desktop (Create Shortcut).”
- c) Right-click the shortcut icon on the desktop and select “Properties.”
- d) In the ‘Target’ text box, type in the below line as shown:

```
C:\"Program Files"\SBACSecureBrowser6.3\SBACSecureBrowser6.3.exe -  
CreateProfile %SESSIONNAME% (32-bit Windows)  
  
"C: \Program Files (X86)\SBACSecureBrowser6.3\SBACSecureBrowser6.3.exe"  
-CreateProfile %SESSIONNAME% (64-bit Windows)
```
- e) Click [OK] to close the Properties window.
(Optional: If you would like to rename the shortcut on the desktop, select the shortcut, press F2, and rename it from “kiosk.exe” to “SBACSecureBrowser6.3.”)

NComputing Virtual Desktop Installation (Windows)

The following steps should be taken to install the secure browser on a network that uses NComputing virtual desktops.

1. Create a batch file that runs the logon script for the secure browser.

This creates a unique profile folder in “Application Data” with a unique session name. This can be placed in the “Startup” folder on the “Start” menu (Start → Programs → Startup).

- a) As the Administrator, open Notepad.
- b) Copy and paste the below line into the Notepad file:

```
"C:\Program Files\SBACSecureBrowser6.3\SBACSecureBrowser6.3.exe" -  
CreateProfile %SESSIONNAME%
```
- c) Save the file as a batch file to the desktop (you may call it anything; e.g., **logon.bat**).
- d) Go to “User Configuration,” which is in the “Remote Administration Console” window.
 - Start Menu → All Programs → NComputing vSpace → vSpace Console → Expand “Local Computer Policy”
- e) Expand “User Configuration” and expand the “Windows Settings” folder.
- f) Click “Scripts (Logon/Logoff)”
- g) Select “Logon” and go to “Properties” (either by clicking the Properties link on the left or right-clicking “Logon” and selecting “Properties”).
- h) In the “Logon Properties” window, click the [**Add**] button.
- i) Browse for the “Logon” batch file that you created in Step B.
- j) Click the [**OK**] button to add the file.
- k) Click the [**APPLY**] button and then close the “Logon Properties” window.
- l) Close the “Remote Administration Console” window.

2. Create a shortcut on the desktop of each client machine.

Note: This will create shortcuts for the secure browser on the client machines.

- a) On the Terminal Server machine, locate the Secure Browser folder.
C:\Program Files\<<SecureBrowserName> folder\
- b) Right-click the **SBACSecureBrowser6.3.exe** file and select “Send To → Desktop (Create Shortcut)”
- c) Right-click the shortcut icon on the desktop and select “Properties”
- d) In the “Target” text box, type or copy/paste the below line as shown:

```
C:\"Program Files"\SBACSecureBrowser6.3\SBACSecureBrowser6.3.exe -  
CreateProfile %SESSIONNAME% (32-bit Windows)  
"C: \Program Files (X86) \SBACSecureBrowser6.3\SBACSecureBrowser6.3.exe" -  
CreateProfile %SESSIONNAME% (64-bit Windows)
```
- e) Click [**OK**] to close the Properties window.
(Optional: If you would like to rename the shortcut on the desktop, select the shortcut, press F2, and rename it from “SBACSecureBrowser6.0.exe” to “SBACSecureBrowser6.3.”)

3. Login as an admin and run the application once.

Simply launching the secure browser and going to the diagnostics page is sufficient (you do not need to start a test). *Note: In order to launch the Secure Browser on the client machines, users will need to double-click the shortcut created on the desktop.*

Network Installation Information for Mac OS X (Network Administrators)

The appropriate secure browser must be installed on each computer that will be used for online testing. While we strongly recommend that you install the secure browser on each individual computer that will be used, you can also push the browser out to all computers through a network by copying browser files from the network to individual computers or through third-party installation programs.

This document provides network installation instructions for computers using the following supported Mac OS X operating systems: 10.4, 10.5, 10.6, 10.7, 10.8, 10.9, and the Apple Remote Desktop application.

Installing the Mac OS X Secure Browser Using Apple Remote Desktop

1. Log into an administrator computer on your network. This computer should have Apple Remote Desktop installed and running.
2. Download the correct Mac OS X browser from the portal.
3. Click the downloaded icon to unzip and save the .dmg file onto your administrator computer.
4. Open the .dmg file and select the .app file.
5. Open Apple Remote Desktop.
6. In the Apple Remote Desktop window, select a Computer List.
7. Select one or more computers from the Computer List onto which you would like to install the secure browser.
8. Select Manage > Copy Items.
9. Select the browser .app file (from Step 4).
10. Select copy options, including your preferred destination on the target machine.
11. Click [**Copy**].

Secure Browsers and Proxy Settings (Updated)

By default, the secure browsers for Windows, Mac, and Linux are packaged with the proxy setting set to “auto-detect.” This setting can be overridden using the command line or by creating a shortcut.

Specifying a proxy server to use with the secure browser.

These secure browsers attempt to auto-detect the settings for your network’s web proxy server. You have the option to change the settings to use by passing parameters to the proxy executable.

The following proxy values are supported:

- 0–Direct connection, no proxy
- 1–Manual proxy configuration
- 2–Proxy auto-configuration (PAC)
- 4–Auto-detect proxy settings
- 5–System proxy settings (*this is the default*)

Table 7. Proxy Server Commands

Description	Command	Operating System
Run the browser without any proxy	./SBACSecureBrowser6.3 -proxy 0 /kiosk-bin -proxy 0 arch -i386 ./SBACSecureBrowser6.3 -proxy 0 ./SBACSecureBrowser6.3 -proxy 0 SBACSecureBrowser6.3 -proxy 0	Linux Mac 10.4 (all) and 10.5 (PPC) Mac 10.5 (Intel) Mac 10.6–10.9 Windows
Set the proxy for HTTP requests only	./SBACSecureBrowser6.3 -proxy 1:http:foo.com:80 ./kiosk-bin -proxy 1:http:foo.com:80 arch -i386 ./SBACSecureBrowser6.3 -proxy 1:http:foo.com:80 ./SBACSecureBrowser6.3 -proxy 1:http:foo.com:80 ./kiosk-bin -proxy 1:http:foo.com:80	Linux Mac 10.4 (all) and 10.5 (PPC) Mac 10.5 (Intel) Mac 10.6–10.9 Windows
Set the proxy for all protocols to mimic the “Use this proxy server for all protocols” of Firefox	./SBACSecureBrowser6.3 -proxy 1:*:foo.com:80 ./kiosk-bin -proxy 1:*:foo.com:80 arch -i386 ./SBACSecureBrowser6.3 -proxy 1:*:foo.com:80 ./SBACSecureBrowser6.3 -proxy 1:*:foo.com:80 SBACSecureBrowser6.3 -proxy 1:*:foo.com:80	Linux Mac 10.4 (all) and 10.5 (PPC) Mac 10.5 (Intel) Mac 10.6–10.9 Windows

Description	Command	Operating System
Specify the URL of the PAC file	<pre>./SBACSecureBrowser6.3 -proxy 2:proxy.com</pre> <pre>./kiosk-bin -proxy 2:proxy.com</pre> <pre>arch -i386 ./SBACSecureBrowser6.3 -proxy 2:proxy.com</pre> <pre>./SBACSecureBrowser6.3 -proxy 2:proxy.com</pre> <pre>SBACSecureBrowser6.3 -proxy 2:proxy.com</pre>	Linux Mac 10.4 (all) and 10.5 (PPC) Mac 10.5 (Intel) Mac 10.6–10.9 Windows
Auto-detect proxy settings (default)	<pre>./SBACSecureBrowser6.3 -proxy 4</pre> <pre>./kiosk-bin -proxy 4</pre> <pre>arch -i386 ./SBACSecureBrowser6.3 -proxy 4</pre> <pre>./SBACSecureBrowser6.3 -proxy 4</pre> <pre>SBACSecureBrowser6.3 -proxy 4</pre>	Linux Mac 10.4 (all) and 10.5 (PPC) Mac 10.5 (Intel) Mac 10.6–10.9 Windows
Use the system proxy setting	<pre>./SBACSecureBrowser6.3 -proxy 5</pre> <pre>./kiosk-bin -proxy 5</pre> <pre>arch -i386 ./SBACSecureBrowser6.3 -proxy 5</pre> <pre>./SBACSecureBrowser6.3 -proxy 5</pre> <pre>SBACSecureBrowser6.3 -proxy 5</pre>	Linux Mac 10.4 (all) and 10.5 (PPC) Mac 10.5 (Intel) Mac 10.6–10.9 Windows

Creating a corresponding desktop shortcut to run the browser using additional parameters.

Microsoft Windows.

1. Navigate to the location of the Secure Browser program folder.
2. Create a shortcut by right-clicking the “SBACSecureBrowser6.3.exe” executable file.
3. Move the shortcut to the desired location, such as the desktop.
4. Right-click the shortcut icon to edit its properties.
5. In the “Target:” input field, append the additional options after the command, e.g.:

```
“C:\Program Files\SBACSecureBrowser6.3\SBACSecureBrowser 6.3.exe” -proxy 1:http:foo.com:80 (32-bit version)
```

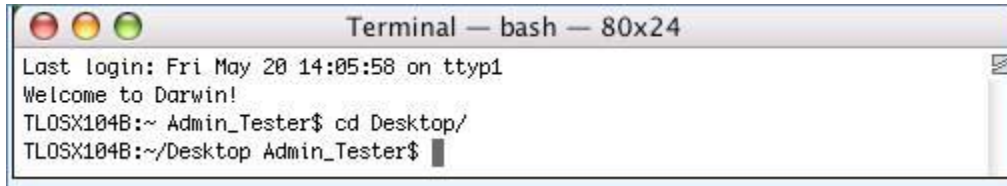
OR

```
“C:\Program Files (x86)\SBACSecureBrowser6.3\SBACSecureBrowser 6.3.exe” -proxy 1:http:foo.com:80 (64-bit version)
```
6. Click [OK].

Mac 10.4–10.9.

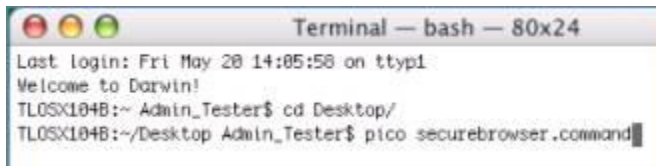
1. From the Terminal application, change to the desktop directory. (Go to Applications > Utilities > Terminal. In Terminal, type the below command and then press [Enter].)

```
cd Desktop
```



2. Create a .command file, using an editor such as pico. To do so, type the command below and then press [Enter]. This creates the securebrowser.command file on the desktop.

```
pico securebrowser.command
```



Note: After you type in the command in step 2 and press [Enter], Terminal should look like this:



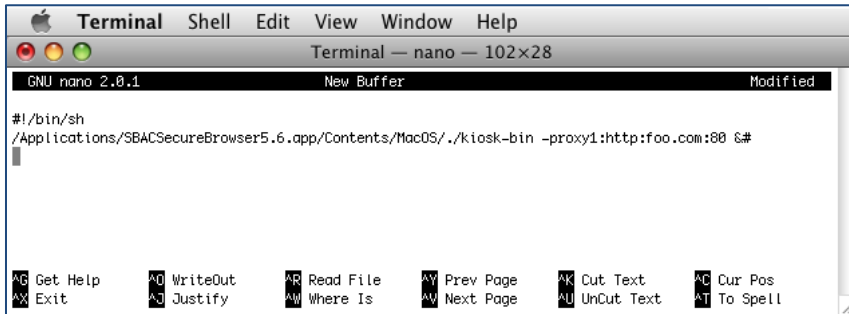
3. Edit the file to be similar to the following, specifying the actual directory path to the secure browser, and the desired proxy options along with an "&" at the end of the line. (In Terminal, enter the appropriate command lines as shown below, pressing [Enter] after each command line (where you see an extra line space, that is where you press [Enter]). Use the appropriate proxy command in the second command line.

Mac 10.4 and 10.5 commands (PPC):

```
#!/bin/sh (press Enter)
```

```
/Applications/SBACSecureBrowser5.6.app/Contents/MacOS/./kiosk
-bin -proxy 1:http:foo.com:80 &
```


Mac 10.4 and 10.5 PPC command sample



Mac 10.5 commands (Intel):

`#!/bin/sh` (press Enter)

```

arch -i386
/Applications/SBACSecureBrowser6.3.app/Contents/MacOS/
SBACSecureBrowser6.3 -proxy 1:http:foo.com:80 &
  
```

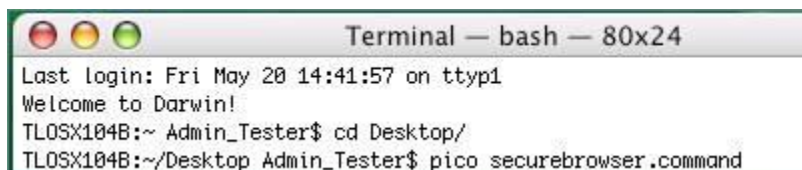
Mac 10.6–10.9 commands:

`#!/bin/sh` (press Enter)

```

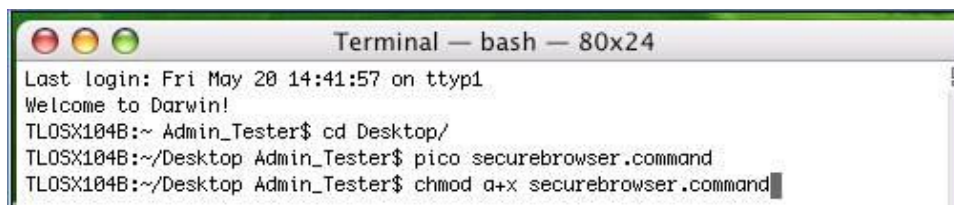
/Applications/ SBACSecureBrowser6.3.app/Contents/MacOS/./
SBACSecureBrowser6.3 -proxy 1:http:foo.com:80 &
  
```

- Save the file and exit the editor by pressing **[Ctrl-O]**, **[Enter]**, and then **[Ctrl-X]**.
Note: Terminal will look like this:



- Execute permission to the shell script file. (In Terminal, type in the command line below and then press **[Enter]**.)

```
chmod a+x securebrowser.command
```



- Close Terminal.
- Click the **[securebrowser.command]** icon on the desktop to open the secure browser with the desired proxy settings.

Linux (Fedora Core 6+ and Ubuntu 9 and 10).

1. Right-click the desktop and select “Create Launcher.”
2. Enter an appropriate name for the shortcut.
3. Enter the full path of the SBACSecureBrowser6.3 proxy command and the additional options.
Example: `/opt/SBACSecureBrowser6.3/./ SBACSecureBrowser6.3 -
proxy 1:http:foo.com:80`
4. Click [OK].

Linux (Ubuntu 11 and 12).

1. Right-click the secure browser desktop icon and select “Copy.”
2. Right-click the desktop and select “Paste.”
3. Right click the newly copied icon and select “Properties.”
4. Append the `-proxy 1:http:foo.com:80` option to the “Command:” field.
5. Click [Close].

Section VI. Mobile Secure Browsers

Introduction

The mobile secure browsers for iPad and Android tablets are designed to support a secure testing environment. These applications require changes to default tablet settings. The first time a mobile secure browser is opened successfully, the Launchpad page will appear. This page will prompt you to select your state and the Smarter Balanced Field Test. Once this step is completed, the student login page will load.

This document contains information about the installation and setup of mobile secure browsers.

Information on test administration, creating and logging into test sessions, and navigating through the test is in the *Online Field Test Administration Manual*, which is available on the Smarter Balanced portal in the [Resources and Documentation](http://sbac.portal.airast.org) section (<http://sbac.portal.airast.org>).

Supported Mobile Devices and Operating Systems

Operating System	Supported Devices	Notes
iOS 6.0–7.1	iPad 2 iPad 3 iPad 4 th generation (Retina Display) iPad Air (see note) <i>Note: The iPad Mini is NOT supported.</i>	All tablet screens must be a minimum of 10" (includes 9.5" iPads) As additional devices are certified, they will be supported by the Smarter Balanced assessments. About iPad Air
Android 4.04–4.2	Google Nexus 10 Motorola Xoom Motorola Xyboard Samsung Galaxy Note (10.1) Samsung Galaxy Tab 2 (10.1)	Based on functional tests performed by Apple and assurances from Apple that the Single App Mode in iOS 6 and Autonomous Single App Mode in iOS 7 work the same way on all models of iPad, Smarter Balanced has agreed to support the iPad Air for the Field Test. <i>Note: Guided Access must be enabled even when iPads are in Single App mode.</i>

Secure Testing on iPads

To ensure a secure test environment, **Guided Access must be enabled and activated** before students can log in to a test session. Guided Access is an iOS feature that allows users to restrict activity to a single application and also prevents taking screenshots or changing to another application. Students will not be able to log in if Guided Access is not enabled and activated.

School technology staff and Test Administrators should all be familiar with Guided Access and ensure that they know how to activate Guided Access on all students' iPads prior to a test session. TAs should also know the passcode for deactivating Guided Access after a test session ends.

In the event that Guided Access is deactivated while a student is testing (if the student knows the Guided Access passcode), the test environment will no longer be secure and the student will be logged out of the test.

The [iOS Secure Browser](#) section contains instructions for enabling, activating, and deactivating Guided Access, as well as completing the Launchpad page steps.

Secure Testing on Android Tablets

The secure browsers for Android tablets require the secure browser keyboard to be selected before students can access the login page. The reason for this is that the default Android keyboard allows predictive text, which would unduly aid students when entering written responses to test items. The secure browser keyboard is a basic keyboard, with no row for predictive text functionality.

The first time you open the Android secure browser, you will be prompted to select the secure browser keyboard. Students cannot access the login page until the secure browser keyboard is selected.

The [Android Secure Browser](#) section contains instructions for opening the Android secure browser, selecting and enabling the secure browser keyboard, and completing the Launchpad page steps.

iOS (iPad) Secure Browser

The secure browser for online testing for iPads can be downloaded from the App store. The process for installing the secure browser is the same as for any other application.

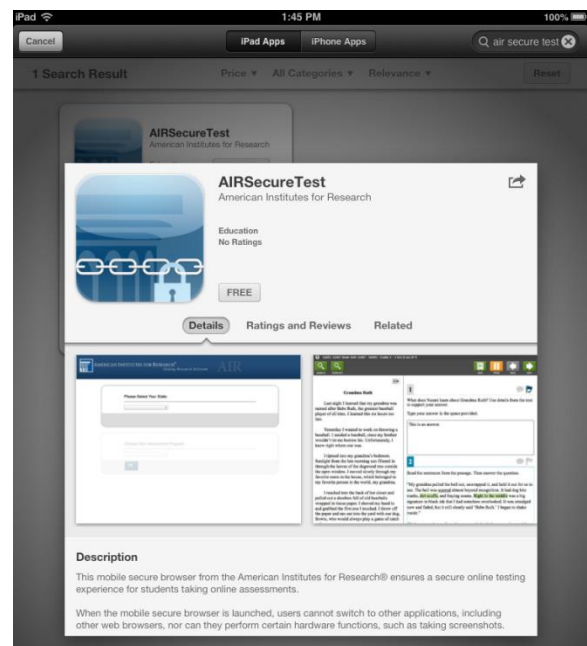
The iPad secure browser is supported on iPads 2 and newer running iOS 6.0–7.1. (The iPad Mini is Not supported.) **The Guided Access feature must also be enabled.**

Downloading and Installing the iOS Mobile Secure Browser

The secure browser for online testing for iPads can be downloaded from the App store. The process for installing the secure browser is the same as for any other application.

1. On your iPad, click the following link. You will be taken to the AIRSecureTest application download page.

<https://itunes.apple.com/us/app/air-secure-mobile-browser/id607002517?mt=8>



2. Tap or select the **[Free]** button. The button will change to say **[Install App]**.



3. Tap or select **[Install App]**.
4. Enter your Apple ID password.



5. The mobile secure browser will download and install onto your iPad. Look for the AIRSecureTest icon.



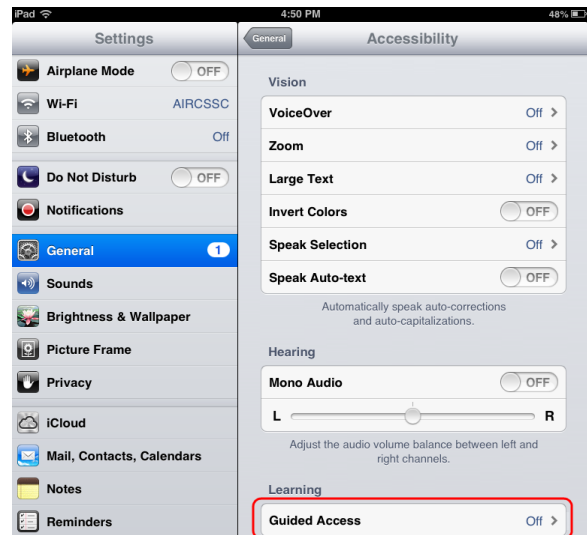
Enabling Guided Access

Note: The instructions in this section are for iOS 6.0. Some icons may be different for iOS 7.0. and 7.1

1. Tap the [**Settings**] icon to open the Settings application.



2. Navigate to General > Accessibility > Learning and tap [**Guided Access**].



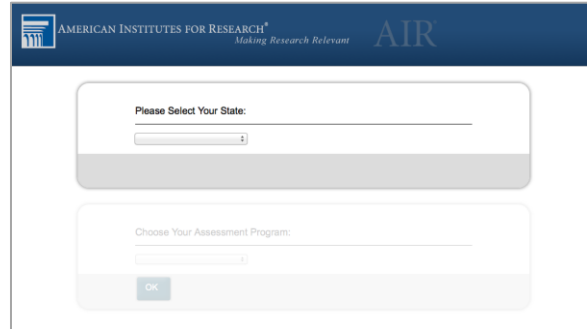
3. Tap [**Off**] to change it to [**On**] (enabled).
4. Set the passcode for Guided Access. This passcode is required to deactivate Guided Access after students are done testing. (If you do not set the passcode now, you will be prompted to set it later.) To set the passcode:
 - a. Tap [**Set Passcode**].
 - b. Enter a 4-digit passcode.
 - c. Confirm the 4-digit passcode. (You may want to write down or save this number in a safe place. There is no ability to “retrieve” a forgotten passcode.)



Opening the iOS Mobile Secure Browser and Selecting the Assessment Program

The first time you open the Mobile Secure Browser, you will see a “Launchpad” page. This Launchpad establishes the test administration your students will log in to.

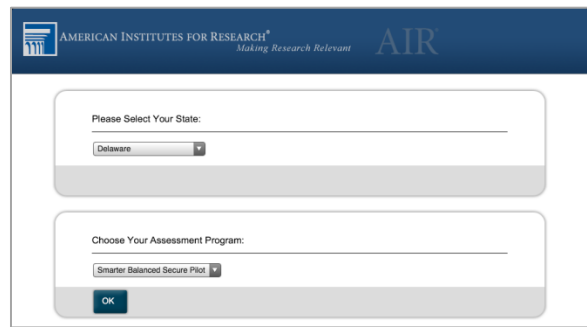
1. Under “Please Select Your State,” select the correct state from the drop-down list.



The screenshot shows the AIR Launchpad interface. At the top, there is a blue header with the AIR logo and the text 'AMERICAN INSTITUTES FOR RESEARCH® Making Research Relevant'. Below the header, there are two main sections. The first section is titled 'Please Select Your State:' and contains a dropdown menu. The second section is titled 'Choose Your Assessment Program:' and contains a dropdown menu and an 'OK' button.

2. Under “Choose Your Assessment Program,” verify or select “Smarter Balanced Field Test.”
3. Tap or select [OK]. The student login page will load.

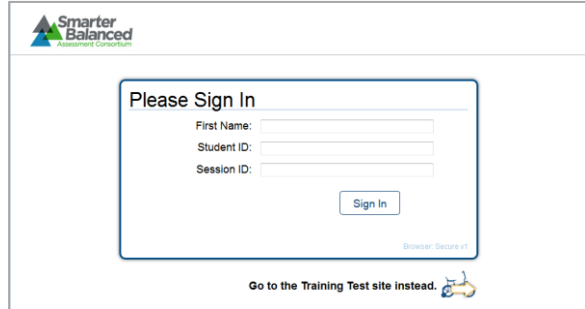
Note: The Launchpad is designed to display only one time. The student login page will display automatically the next time you open the secure browser.



The screenshot shows the AIR Launchpad interface with the 'Please Select Your State:' dropdown menu set to 'Delaware' and the 'Choose Your Assessment Program:' dropdown menu set to 'Smarter Balanced Secure Pilot'. The 'OK' button is visible at the bottom of the second section.

Activating Guided Access Before a Test Session Begins

1. Open the AIRSecureTest app. The student login page should display.



2. Triple-click (press) the Home button at the bottom of the iPad.

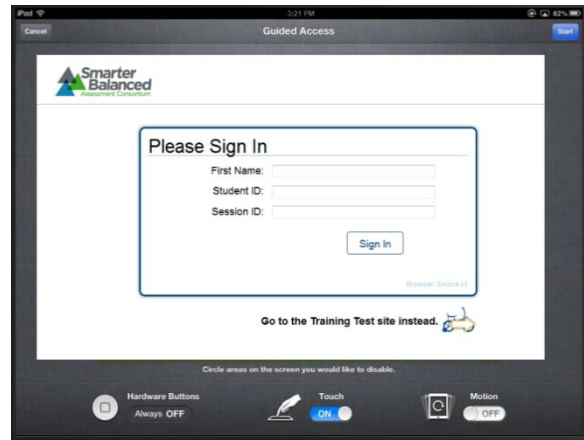


3. The Guided Access options will appear in a border around the secure browser app.

Tap the [**Start**] button in the upper right corner.

A pop-up message will appear saying Guided Access has started.

Note: Disregard the options at the bottom of the screen. When Guided Access is activated, students cannot switch to any other applications or take screenshots.



Deactivating Guided Access After a Test Session Ends

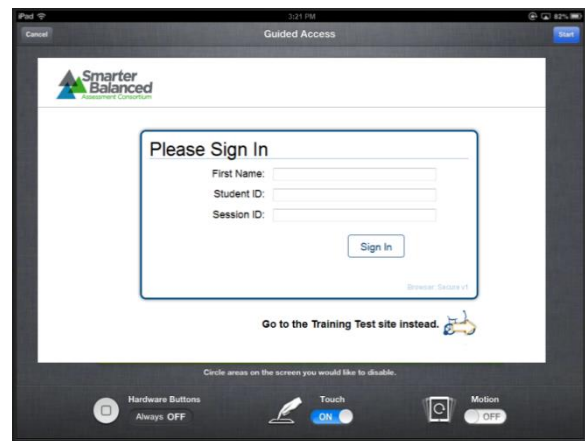
1. Triple-click (press) the Home button at the bottom of the iPad.



2. Enter your Guided Access passcode. This must be the same passcode that you selected when you enabled Guided Access.



3. Tap the [End] button in the upper left corner. A pop-up message will appear saying Guided Access has ended.



Closing the iPad Secure Browser (iOS 6.0–6.1)

1. Double-click (press) the Home button at the bottom of the iPad. This will open the multitasking bar.
2. Press the minus sign on the [AIRSecureTest] icon until it disappears.

Closing the iPad Secure Browser (iOS 7.0–7.1)

1. Double-click (press) the Home button. This will open the multitasking screen.
2. Locate the [AIRSecureTest] app preview and slide it upwards.

Android Secure Browser

The secure browser for online testing for supported Android tablets can be downloaded from the Google Play store. The process for installing the secure browser is the same as for any other application.

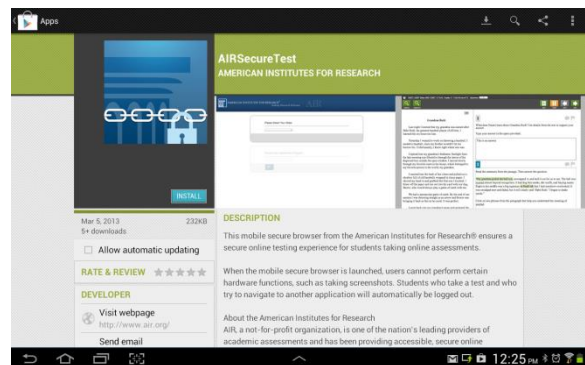
The Android secure browser is supported on the following tablets running at Android 4.0.4–4.2:

- Google Nexus 10
- Motorola Xoom
- Motorola Xyboard
- Samsung Galaxy Note (10.1)
- Samsung Galaxy Tab 2 (10.1)

Downloading and Installing the Android Secure Browser

1. On your Android tablet, click the following link. You will be taken to the AIR Secure Test application page.

https://play.google.com/store/apps/details?id=com.air.mobilebrowser&feature=search_result#?t=W251bGwsMSwxLDEsImNvbS5haXlubW9iaWxiYnJvd3NlciJd



2. Tap or select the [Install] button.



3. The secure mobile browser will download and install onto your Android tablet. Look for the AIRSecureTest icon (the name may be truncated).



Opening the Android Secure Mobile Browser and Changing the Keyboard

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

Notes about the secure browser keyboard and general settings:

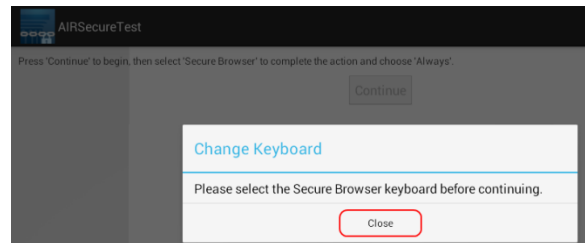
- Once the secure browser keyboard is set, that becomes the default keyboard for all Android tablet applications, not just the secure browser. If you want to return to the default Android keyboard after using the secure browser, you will have to navigate to Settings > Language & Input and uncheck the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

Note: All screenshots in this section were taken with a Samsung Galaxy Tab 2.

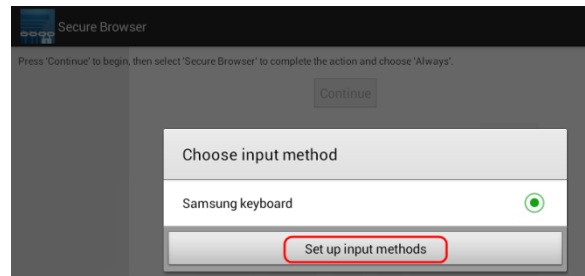
1. Select the secure browser icon on the home screen.



2. You will be prompted to change the keyboard. Select **[Close]**.

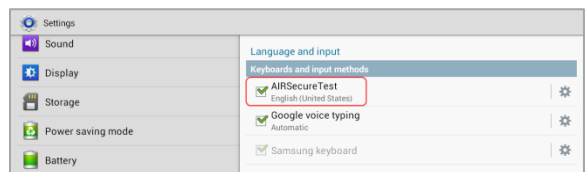


3. Select **[Set up input methods]**. The Language & Input settings screen will automatically open.

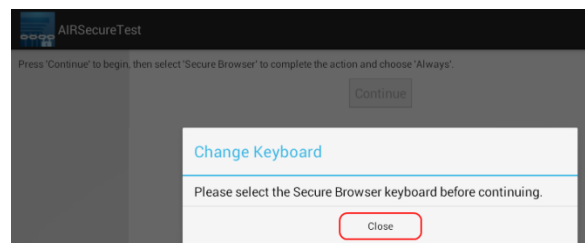


4. Select the checkbox next to "AIRSecureTest" so that a check mark appears.
You will be prompted to acknowledge that this selection is okay. Select **[OK]** to continue.

Note: This action allows the secure browser keyboard to be used by the secure browser application.

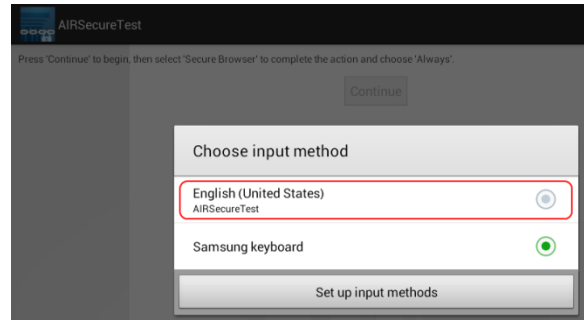


5. Navigate to the secure browser to open it. (You can use the application switcher or go back to "Home" and select the secure browser icon.)
You will be prompted to change the keyboard. Select **[Close]**.

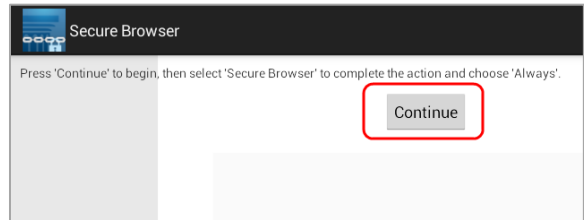


- The Android tablet's default keyboard will still be selected.

Select the checkmark or radio button for the **AIRSecureTest** keyboard.

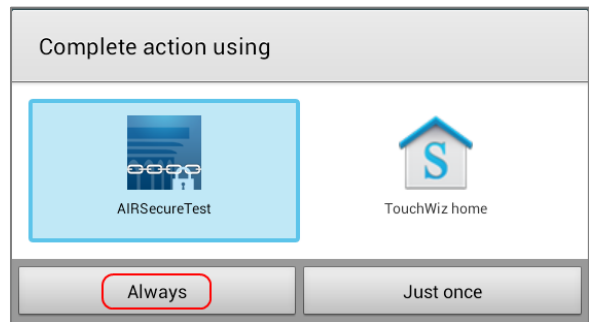


- Select **[Continue]**. You will be prompted to complete the application launch using the preferred method.



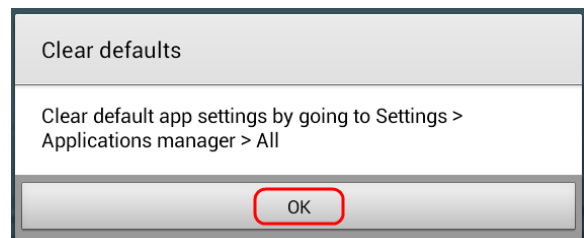
- Select AIRSecureTest (ensure it is shaded and highlighted blue) and then select **[Always]**.

Note: You will have to acknowledge that the secure browser's default settings have changed. (This is a result of selecting the secure browser keyboard.)



- Select **[OK]**.

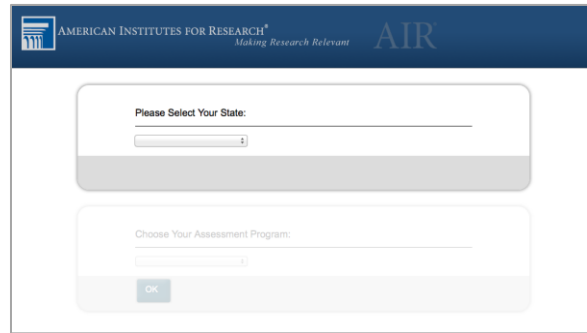
The Launchpad will display. (See the next section for instructions.)



Opening the Android Secure Browser and Selecting the Assessment Program

1. The first time the secure browser successfully opens after selecting the correct keyboard, the Launchpad page will display.

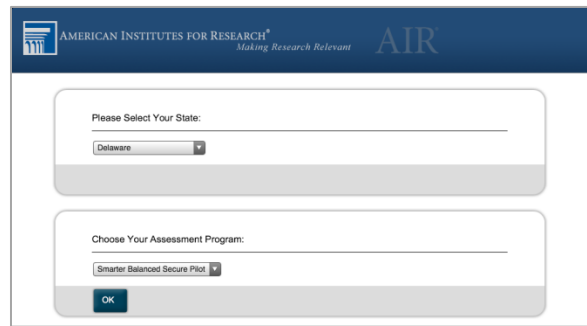
Under “Please Select Your State,” select the correct state from the drop-down list.



The screenshot shows the AIR Launchpad interface. At the top, there is a dark blue header with the AIR logo and the text 'AMERICAN INSTITUTES FOR RESEARCH® Making Research Relevant'. Below the header, there are two main sections. The first section is titled 'Please Select Your State:' and contains a drop-down menu. The second section is titled 'Choose Your Assessment Program:' and contains a drop-down menu and an 'OK' button.


2. Under “Choose Your Assessment Program,” verify or select “Smarter Balanced Field Test.”
3. Tap or select [OK]. The student login page will load.

Note: The Launchpad is designed to display only one time. The student login page will display automatically the next time you open the secure browser.



The screenshot shows the AIR Launchpad interface with selections made. In the 'Please Select Your State:' section, 'Delaware' is selected in the drop-down menu. In the 'Choose Your Assessment Program:' section, 'Smarter Balanced Secure Pilot' is selected in the drop-down menu, and the 'OK' button is highlighted.

Closing the Android Secure Browser

1. Tap the Menu icon [] in the upper right corner.
2. Tap [Exit]. A pop-up message will appear asking you to verify that you want to exit the secure browser.
3. Tap [Exit].

Section VII. Chromebooks

The American Institutes for Research has worked with Google to develop a secure browser kiosk application that can be downloaded onto Chromebooks from the Chrome Web Store. **Using the AIRSecureTest kiosk application requires Chromebooks to run in kiosk mode.**

Note: The AIRSecureTest browser is not a hosted app. In order to support text-to-speech capabilities, AIR developed a packaged kiosk application. As a result, this app must be deployed onto managed Chromebooks via the Chrome Management Console as a kiosk application rather than via a public session. (You may still use public sessions for other applications.)

This section outlines the basic steps for adding the AIRSecureTest app to managed Chromebooks and ensuring that the app runs in kiosk mode. Google has provided documentation for the sole purpose of running kiosk apps on Chromebooks. Links to this information are on the next page.

Adding the AIRSecureTest Kiosk App to Managed Chromebooks

Note: These instructions are for Chrome Device Managers who will add the secure browser to their domain-managed Chromebook devices.

1. As the Chromebook administrator, log into your ChromeOS management console (<https://admin.google.com>).
2. Navigate to **Device management > Chrome management > Device settings**
3. On the Device settings page, scroll down to the “Kiosk Settings” section.
 - Ensure that Single App Kiosk is set to “Allow Single App Kiosk.”

Note: The AIRSecureTest app is not compatible with public sessions. However, you may still use public sessions as necessary for other Chromebook use (e.g., classroom instruction or other test administrations).
4. Click the [**Manage Kiosk Applications**] link. The Kiosk Apps window will appear. You will need to add the AIRSecureTest app.
 - a. Click [**Chrome Web Store**].
 - b. In the search box, type “AIRSecureTest” (without quotes) and press [Enter].
 - c. The AIRSecureTest app will appear. Click the [Add] link. The app will appear in the “Total to install” section.
 - d. Click [**Save**].

Once these steps are complete, the AIRSecureTest app will appear on all managed Chromebook devices.

Students do NOT need to log into Chromebooks to take the test. When Chromebooks is powered up, simply click the [**Apps**] link in the bottom row and select the [**AIRSecureTest**] app. The secure browser will open in full-screen mode.

Important: If you launch the AIRSecureTest app and receive the following error message, then the secure browser is installed properly but not configured to run in kiosk mode:

“The AIRSecureTest application requires kiosk mode to be enabled.”

Ensure that the above steps are completed. The AIRSecureTest app must appear in the Manage Kiosk applications window in Step 4.

Adding the AIRSecureTest App to Non-Managed Chromebooks

Note: These instructions are for installing the secure browser onto individual, non-managed Chromebook devices.

Important: *Non-managed Chromebook devices must not already be configured with user accounts before you enable kiosk mode. If you have already added Google user accounts to a Chromebook, you will need to wipe the device. Google has provided instructions for wiping Chromebook devices: <https://support.google.com/chrome/a/answer/1360642?hl=en>. After you wipe the device, follow the instructions below to enable kiosk mode and install the AIRSecureTest app.*

1. Power on your Chromebook device.
 - a. Follow the steps to advance to the login screen.
 - b. When the login screen appears, press the following key combination: **[Ctrl] + [Alt] + [K]**. This will open the Enable Kiosk Mode screen.

*Note: If the Enable Kiosk Mode screen does not appear, wait 5–10 minutes and then press **[Ctrl] + [Alt] + [K]** again.*
2. Follow the on-screen instructions to enable kiosk mode (click **[Enable]**, and then click **[OK]**).
3. Log in with your Google user account.
4. Add the mobile secure browser to the Chromebook startup screen:
 - a. Open Chrome and enter the following path in the URL bar: **chrome://extensions**.
 - b. Click the check box for “Developer Mode.”
 - c. Click the **[Add kiosk application...]** button at the top of the screen.
 - d. Enter the following AIRSecureTest ID into the “Add kiosk application” text field:
ondcgjblmdblfnmdeoeebaemlckomedj

Note: You can copy the ID if you open the Chrome Web Store and search for the AIRSecureTest app. It appears in the URL.
 - e. Click **[Add]**. The AIRSecureTest application should now appear in the “Manage Kiosk Applications” list.
 - f. Check “Permanently keep this device in kiosk mode.”
 - g. Click **[Done]**.
5. Log out of your Google user account (click the icon in the lower right corner and select **[Sign Out]**).
6. In the Chromebook menu row (at the bottom of the screen), you should see an **[Apps]** link. If you click on it, the AIRSecureTest app should be available. Click the app to launch the browser.

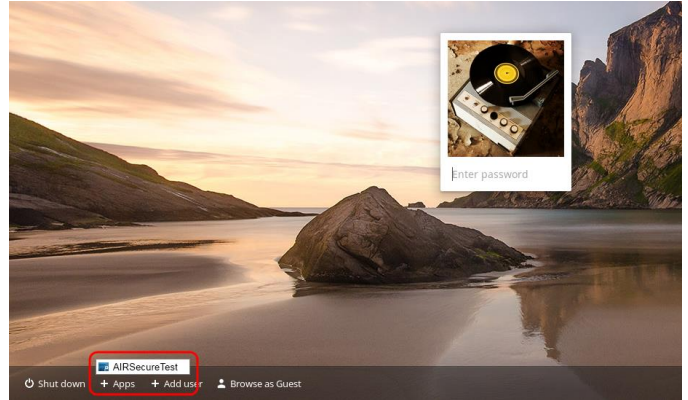
Google Documentation

- Using Chromebooks for Student Assessments:
<https://support.google.com/chrome/a/answer/3273084>
 - Refer to “Scenario 1: School sets up Chromebook to run as a Single App Kiosk running the exam app”
 - Do NOT follow the instructions for Scenarios 2 and 3.
- Managing Device Settings (general information for managed Chromebooks):
<https://support.google.com/chrome/a/answer/1375678>

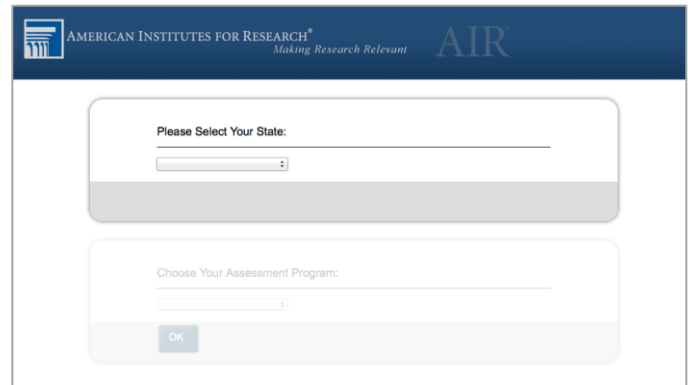
Opening the Mobile Secure Browser and Selecting the Assessment Program

The first time you open the AIRSecureTest mobile secure browser app on a Chromebook, you will see a “Launchpad” page. This Launchpad establishes the test administration your students will log into.

1. In the Chromebooks menu (bottom row), select “Apps” and then select “AIRSecureTest.” The mobile secure browser will open in full-screen mode.



2. Under “Please Select Your State,” select your state from the drop-down list.



3. Under “Choose Your Assessment Program,” verify or select “Smarter Balanced Field Test.”
4. Tap or select [OK]. The student login page will load. The secure browser is now ready for student to use.

Note: The Launchpad is designed to display only once. The student login page will display automatically the next time you open the secure browser.



Section VIII. About Text-to-Speech and Voice Packs

Using text-to-speech requires voice packs to be pre-installed on computers that will be used for testing. For Windows and Mac operating systems, default voice packs are typically pre-installed. For computers running Linux Fedora Core 6+ (K12LTSP 4.2+) or Ubuntu 9–12, voice packs may need to be downloaded and installed.

A number of voice packs for desktops and laptops are available commercially, and AIR researches and tests voice packs for compatibility with the secure browsers. Additionally, not all voice packs that come pre-installed with Windows and Mac operating systems are approved, as the quality of some default voice packs is not optimal for testing. The voice packs listed at the end of this section have been tested and approved for use with the secure browser.

How the Secure Browsers Work

Desktop Secure Browsers

The secure browsers are configured to recognize several known voice packs to provide the text-to-speech accommodation. The secure browsers detect pre-installed voice packs on the students' machines. When a student who is using text-to-speech logs into a test session and has been approved for testing, the secure browser will look for voice packs on the student's machine. When it recognizes an approved voice pack, the one with the highest priority rating will be used.

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.



We strongly encourage users to test the text-to-speech settings before students take a test. You can check these settings from the diagnostic page. Open the secure browser, click the **[Network Diagnostic Tools]** link, and then click the **[Text-to-Speech Check]** button.

Mobile Secure Browsers

The mobile secure browser uses either the device's native voice pack or a voice pack embedded in the secure browser. If additional voice packs are downloaded to a tablet or Chromebook, they will not be recognized by the mobile secure browser.

iOS

Mobile Secure Browser version 2.0 – This app includes an embedded NeoSpeech voice pack; the native iOS voice pack is not available for selection.

Mobile Secure Browser version 2.1

- iOS 6.0–6.1: The embedded NeoSpeech voice pack will be used.
- iOS 7.0: The native iOS voice pack will be used.

Android

The AIRSecureTest app for Android uses the native voice pack available on the supported Android tablet being used.

ChromeOS

The AIRSecureTest kiosk app for Chromebooks uses the native voice pack available on the Chromebook device being used.

Windows: Configuring Text-to-Speech Settings

This section provides information on ensuring that text-to-speech for online testing will work appropriately on computers running Windows XP (Service Pack 3), Vista, 7, 8.0, or 8.1.

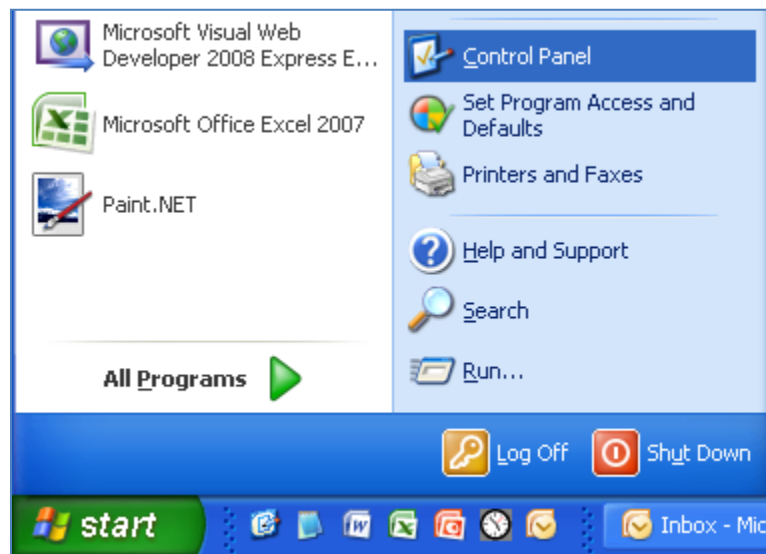
The speech feature on Windows operating systems is user interface (UI) driven. This means that the text-to-speech preferences used to administer the text-to-speech accommodation are located within the computer's system preferences. Follow the steps below to configure text-to-speech preferences.

As a reminder, text-to-speech is available only when the secure browser is used. Students can access the Practice and Training Tests using the secure browser.

Note: The instructions in this section are for computers running Microsoft Windows XP. The process is similar for other Windows operating systems.

Step 1: **Access Control Panel**

Click the [**Start**] button and then click the **Control Panel** link.



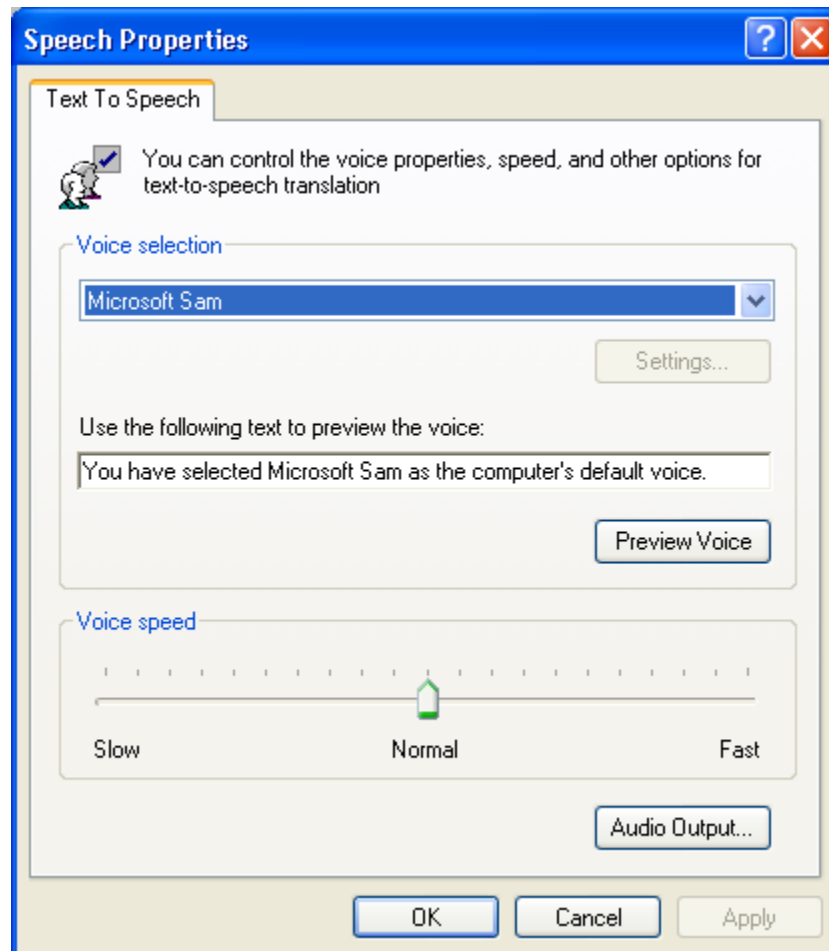
Step 2: *Access Speech Options*

In the Control Panel window, click the [**Speech**] icon. This will bring up the Speech properties window.



Step 3: *Set Speech Preferences*

1. Select your desired **Voice Selection** from the drop-down menu. (You may have only one voice available.)
2. Click [**Preview Voice**] to verify that you can hear the voice.
3. Set the desired Voice speed. Click [**Audio Output**] to listen to the settings. You can adjust the settings as desired.
4. When you are done, click [**OK**] to save your settings, and then click the Red [**X**] at the top right of the screen to close the window.



Mac OS X: Configuring Text-to-Speech Settings

This section provides information on ensuring that the text-to-speech accommodation for online testing will work appropriately on computers running Mac OS X 10.4–10.9.

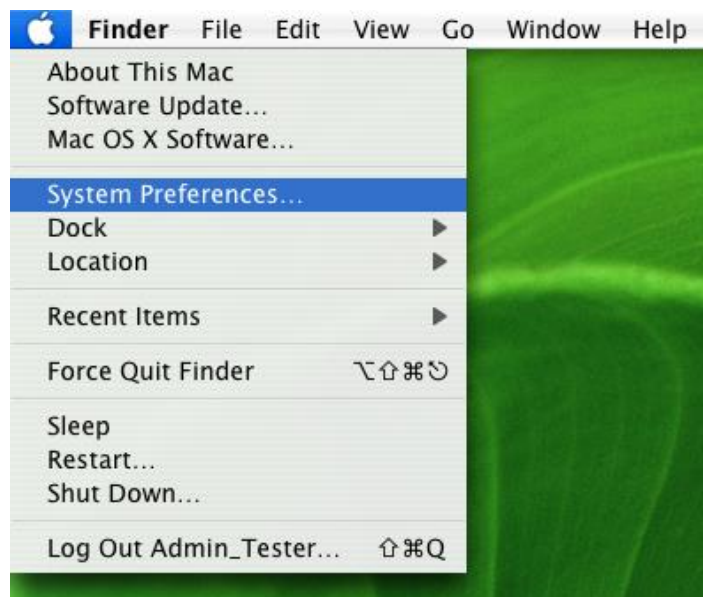
The speech on Mac operating systems are user interface (UI) driven. This means that the text-to-speech preferences used to administer the text-to-speech accommodation are located within the computer's system preferences. Follow the steps below to configure audio preferences to enable the text-to-speech accommodation.

As a reminder, text-to-speech is available only when the secure browser is used. Students can access the Practice and Training Tests using the secure browser.

Note: The instructions in this section are for computers running Mac 10.6. The process is similar for other Mac operating systems.

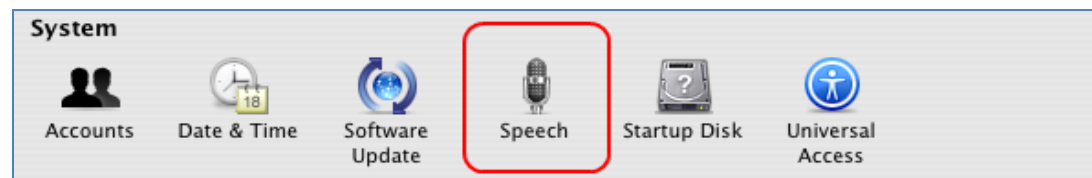
Step 1: Access System Preferences

Click the Apple icon and then click "System Preferences."



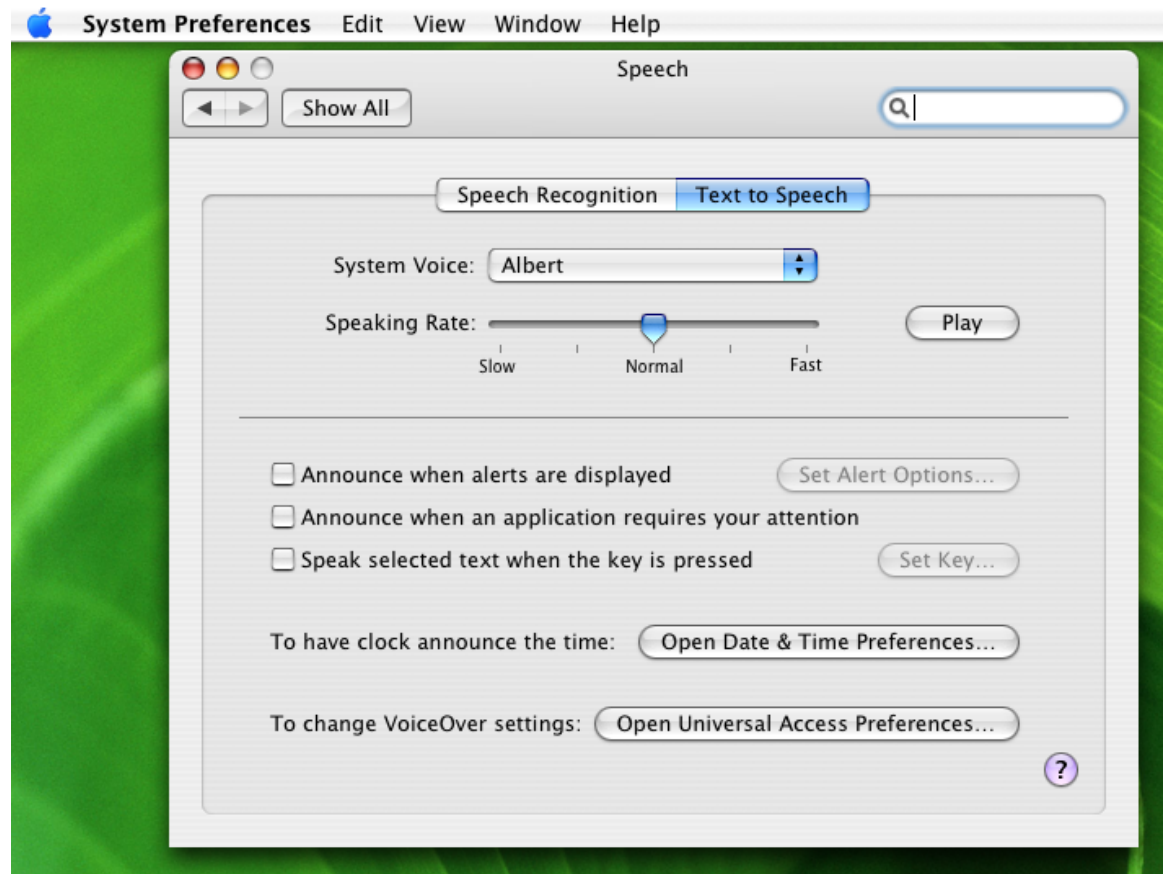
Step 2: Access Speech Options.

In the System Preferences screen, click the [Speech] icon. (This icon typically appears in the "System" row.)



Step 3: Set Speech Preferences.

1. Make sure the **[Text to Speech]** tab is active (it should be blue). You may need to click it to view this screen.
2. Select your desired **System Voice** from the drop-down menu.
3. Set the desired Speaking Rate. Click **[Play]** to listen to the settings. You can adjust the settings as desired. *Note: The speaking rate selected applies to all voices installed on the system.*
4. When you are done, click the red **[X]** at the top left of the screen to save your preferences and close the window.



Linux: Enabling Text-to-Speech and Default Settings

This section provides information for Technology Coordinators on how to ensure that text-to-speech for online testing will work appropriately on computers running Linux Fedora Core 6+ (K12LTSP 4.2+) or Linux Ubuntu 9–12.

Linux is a modular kernel operating system, which means that specific non-used kernel modules may not load when the system is booted up. *If the required kernel modules are not already built in or installed*, this document will not provide you with the information that you need.

As a reminder, text-to-speech is available only when the secure browser is used. Students can access the Practice and Training Tests using the secure browser.

Other Software

In addition to downloading the Linux secure browser, you will also need to download two software programs: *Festival* and *Sound eXchange* (SoX). These programs will ensure that students can hear the audio in the online tests.

- To download *Festival*, click here: <http://www.cstr.ed.ac.uk/projects/festival/>. Instructions for ensuring that Festival works properly are included in this document section.
- To download SoX, click here: <http://sox.sourceforge.net>. This website also contains information on installing and configuring SoX.

Important: The commands provided in this section require you to be logged in as “root.”

About Sound Cards and ALSA Drivers

You can determine what kind of sound card is configured on your Linux system. These file types typically are as follows:

- `/dev/dsp`
- `/dev/dsp1` or `/dev/dsp2` or `/dev/dsp3`, and so on
- `/dev/snd`
- `/dev/asound.conf`

The first three types are device files. You cannot read from or write to these files. However, if you have a MIDI file, you can use that to directly test the sound card. Use the following string to write the MIDI file to your computer’s sound card:

```
cat [MIDI file name] > /dev/dsp
```


Linux provides two tools to configure your sound card:

- `system-config-soundcard` (UI tool)
- `alsamixer` (text-mode tool)

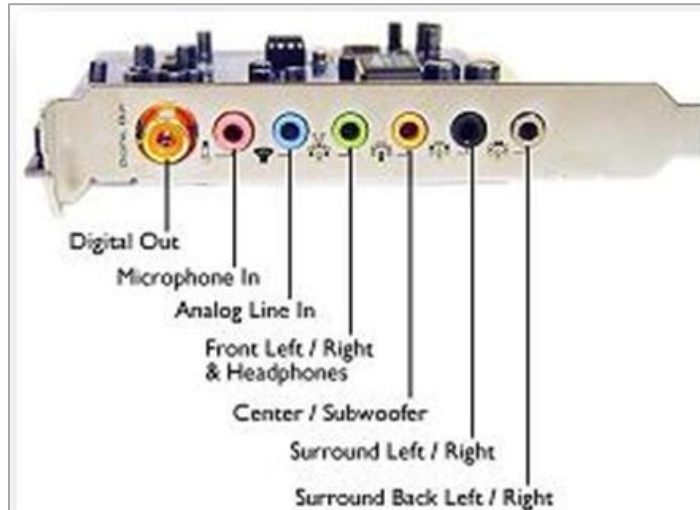
This document provides instructions using the `system-config-soundcard` tool. If you choose to use `alsamixer` to configure your sound card, the steps are very similar.

Checking Sound on Your Computer

If you discover that audio is not working properly on your system, follow the steps in this section.

- Step 1:** Verify that your audio playback devices—e.g., headphones and/or speakers—are connected properly to the sound card. The green jack should always be plugged in to the green port or a port marked with a headphone icon .

Sound card ports



- Step 2:** Check whether `/dev/snd` exists on your computer.

In the command prompt, enter the following command: `ls -la/dev/snd`

- If this *does not* exist, continue to **Step 3**.
- If this *does* exist, skip to **Step 5**.

- Step 3:** If `/dev/snd` does not exist, it is possible that the ALSA audio drivers were not installed or loaded properly when the system booted up.

In the command prompt, enter the following command: `modprobe snd-seq`

This command should run without any errors.

- Step 4:** Check whether `/dev/snd` exists on your computer.

In the command prompt, enter the following: `ls -la/dev/snd`

If this exists, then use Secure Browser to go to the Diagnostics page and check whether the audio works.

- If the audio playback works *without any errors or issues*, skip to **Step 7**.
- If the audio playback *has errors or issues*, continue to **Step 5**.



If you still cannot find `/dev/snd` on your computer, please consult your system administrator for assistance. *Do not continue with the instructions in this document.*

Step 5: At the command prompt, enter: `system-config-soundcard`

This will display a graphic user interface that you can use to fix sound card problems.

Sound card configuration user interface



- a. In the **[Sound Test]** tab, click the Play [] button.
 - If you hear audio, then your sound card is working correctly. Continue to #3.
 - If you did not hear audio, continue to #2 below.
- b. Click the **[System]** tab.
 - Click **[Reload Audio Drivers]** (this step will reinitialize the drivers)
 - Click the **[Sound Test]** tab and click the Play [] button again.
 - If you hear the audio, then your sound card is now working correctly.
 - If the audio is still not working, consult your system administrator for assistance. Do not continue with the instructions in this document.
- c. Click the **[Settings]** tab.

In the section called “Audio Cards Indexer,” look at the first and second columns. The first column is the Index column and contains a number (e.g., 0 or 1). The second column is the name of the sound card installed at the index.

Note the index number in the first column, and continue to Step 6.

Step 6: If the index number in Step 5c is 0, then your computer should have a `/dev/dsp` sound file. Try the audio playback on the secure browser again.

If the index number in Step 5c is anything other than 0, you need to create a link from the index file to the `/dev/dsp` file.

Open the command prompt and type the following command:

```
ln -s /dev/dsp[index] /dev/dsp (where [index] is the index number)
```

Try the audio playback on the secure browser again.

Testing Festival for Use with the Text-to-Speech Accommodation

By default, Linux operating systems use Festival for speech synthesis. Be sure that you have already downloaded and installed Festival appropriately before completing the following steps. These steps will determine whether Festival is configured correctly to work with text-to-speech. (Festival can be downloaded here: <http://www.cstr.ed.ac.uk/projects/festival/>.)

- Step 1:** At command prompt, type `festival`.
The Festival command line will display on the next row.
Enter the following: (`SayText "hello"`), and press **[Enter]**.

If you hear the word "hello" being spoken, then Festival is installed properly.

- Step 2:** In the next Festival command prompt, type the command `libdir` and press **[Enter]**.
The output will display the path name where Festival is installed. For example:

```
/usr/share/festival
```

Make a note of this path name. Navigate to this directory path and look for the file named "audsp."

Note: If this file is not found, then there may be an issue with your Festival installation. If that is the case, do not continue with the instructions in this document until you resolve the installation issue.

- Step 3:** The file "audsp" needs to be added to the list of folders where the operating system searches for executables and other necessary files. It is identified by a system variable called PATH.

- To view the current list, type the following into the command prompt: `echo $PATH`.
- You will also need to run the following command to ensure that the audsp file is easily found:

```
ln -s <audsp path> /bin/audsp
```

- Replace the `<audsp path>` with your computer's path to audsp displayed in Step 2. For example, if `audsp` is located in

```
/usr/share/festival/etc/unknown_RedHatLinux/
```

then the full command prompt should be:

```
ln -s /usr/share/festival/etc/unknown_RedHatLinux/audsp  
/bin/audsp
```

This step creates a symbolic link to the `audsp` file found in the Festival installation directory from any folder that is known to be on the path. (In this case, `/bin` was the primary path.) You may choose any other folder as long as it is known to be a common path for all users.

Setting Defaults for Voice, Reading Speed, and Volume

This section provides an overview of how to change the default settings in Festival. These instructions assume that you have already downloaded and installed the requisite voice packs.

Changing the default settings as described in each section will change the settings for all users.

Default Voice Settings

Step 1: In the command prompt, enter `festival`, and then execute the following commands exactly as shown:

```
festival>libdir
"/usr/share/festival" (Note: This output line may be different)

festival>(voice.list)
(cepstral_miguel
 cmu_us_slt_arctic_hts
 cmu_us_bdl_arctic_hts
 cmu_us_awb_arctic_hts
 ked_diphone
 kal_diphone)

festival>voice_default
ked_diphone
```

Note: The outputs for the commands `libdir`, `voice.list`, and `voice_default` may be different based on your installation.

Step 2: Make a note of the output for the command “`libdir`” in the step above. Change to that directory. (In our installation, it is `/usr/share/festival`.)

Step 3: Open the file `init.scm` for editing.

Step 4: Select any voice from the `voice.list` output in Step 1.
To set up your selection as the default voice, use the following commands:

```
(set! Voice_default `voice_<voice name from the list>)
```

If you chose “`cmu_us_slt_arctic_hts`,” this line would look like:

```
(set! Voice_default `voice_cmu_us_slt_arctic_hts)
```

Default Reading Speed

Depending on the specific needs of the individual students who will use the text-to-speech accommodation, a slower reading speed may be desirable. This also has the effect of making the voice sound deeper.

Step 1: Open the file `init.scm` for editing.

To locate the file, follow steps 1 and step 2 from the *Default Voice Settings* section.

Step 2: Append the following line to the end of `init.scm`.

```
(Parameter.set 'Duration_Stretch <number>)
```

Acceptable values are any number greater than 1. However, experiments have shown that numbers higher than 2 are too slow.

For example, if a slower reading speed is desired, then you can set `<number>` to 1.5 or 2.0.

Default Volume Setting

A default volume may be set by running `system-config-soundcard` or `alsamixer` from the command prompt.

Voice Packs Recognized by Secure Browser

The tables in this section display the voice packs for each operating system (Windows, Mac and Linux) that are currently recognized by the secure browser.

Windows and Mac OS X computers typically ship with at least one default voice pack. Many of these default voice packs are recognized by the secure browser.

Windows XP, Vista, 7, 8.0, 8.1

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

Mac 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

Vendor	Voice Pack	Language
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	English
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

Linux

Vendor	Voice Pack	Language
Festvox (commercial)	cmu_us_awb_arctic_hts	English
Festvox (commercial)	cmu_us_bdl_arctic_hts	English
Festvox (commercial)	cmu_us_jmk_arctic_hts	English
Festvox (commercial)	cmu_us_slt_arctic_hts	English
Festvox (commercial)	kal_diphone	English
Festvox (commercial)	ked_diphone	English

Refer to the section titled “Linux: Enabling Text-to-Speech and Default Settings” for more information on configuring Linux and testing the audio preferences for text-to-speech. For additional information about the Festvox voices, go to the [Festvox web site](#).

Appendix A: IP Addresses and URLs for Smarter Balanced Systems

IP Addresses and URLs for Smarter Balanced Systems

System	URL	IP Address
Smarter Balanced portal/secure browser files	http://sbac.portal.airast.org	108.171.168.180
Single Sign On system	https://sbac.openam.airast.org	184.106.100.135
Test Information Distribution Engine (TIDE)	https://sbac.tide.airast.org	166.78.225.29
Online Reporting System	https://sbac.reports.airast.org	166.78.75.177

The Smarter Balanced testing sites use a cloud-based satellite system for optimal load balancing during testing.

*Note: If your network filtering devices (e.g., proxy servers) and firewalls support wildcards, you may use *.cloud1.tds.airast.org and *.sbacpt.tds.airast.org instead of whitelisting each individual satellite URL listed below.*

System	URL	IP Address
AIRSecureTest Mobile Secure Browser Launchpad	https://mobile.tds.airast.org	50.57.2.88
TA and Student Practice and Training Sites	https://sbacpt.tds.airast.org	69.20.121.89
	sat1.sbactpt.tds.airast.org	69.20.121.90
	sat2.sbactpt.tds.airast.org	74.205.105.232
	sat3.sbactpt.tds.airast.org	74.205.105.233
TA Interface and Student Testing Site	https://sbac.tds.airast.org	198.61.246.201
	https://login1.cloud1.tds.airast.org	173.203.13.43
	https://sat1.cloud1.tds.airast.org	166.78.76.170
	sat2.cloud1.tds.airast.org	166.78.76.171
	sat3.cloud1.tds.airast.org	23.253.30.0
	sat4.cloud1.tds.airast.org	23.253.30.1
	sat5.cloud1.tds.airast.org	23.253.30.2
	sat6.cloud1.tds.airast.org	23.253.30.3
	sat7.cloud1.tds.airast.org	23.253.30.4
	sat8.cloud1.tds.airast.org	23.253.30.5
	sat9.cloud1.tds.airast.org	23.253.30.6
	sat10.cloud1.tds.airast.org	23.253.30.7
sat11.cloud1.tds.airast.org	23.253.29.240	

System	URL	IP Address
TA Interface and Student Testing Site (cont'd)	sat12.cloud1.tds.airast.org	23.253.29.241
	sat13.cloud1.tds.airast.org	23.253.29.242
	sat14.cloud1.tds.airast.org	23.253.29.243
	sat15.cloud1.tds.airast.org	23.253.30.8
	sat16.cloud1.tds.airast.org	23.253.30.9
	sat17.cloud1.tds.airast.org	23.253.30.10
	sat18.cloud1.tds.airast.org	23.253.30.11
	sat19.cloud1.tds.airast.org	23.253.30.24
	sat20.cloud1.tds.airast.org	23.253.30.25
	sat21.cloud1.tds.airast.org	23.253.30.26
	sat22.cloud1.tds.airast.org	23.253.30.27
	sat23.cloud1.tds.airast.org	23.253.30.60
	sat24.cloud1.tds.airast.org	23.253.30.61
	sat25.cloud1.tds.airast.org	23.253.30.62
	sat26.cloud1.tds.airast.org	23.253.30.63
	sat27.cloud1.tds.airast.org	23.253.30.64
	sat28.cloud1.tds.airast.org	23.253.30.65
sat29.cloud1.tds.airast.org	23.253.30.66	
sat30.cloud1.tds.airast.org	23.253.30.67	

Important: Users who try to bookmark a satellite URL (sat1, etc.) will be automatically directed to the main URL. To ensure connection to any of the satellite sites, all URLs and IP addresses should be open or whitelisted.

IP Addresses and URLs for Smarter Balanced California Systems

System	URL	IP Address
Smarter Balanced portal/secure browser files	http://sbac.portal.airast.org	108.171.168.180
Single Sign On system	https://ca.openam.airast.org	166.78.84.236
Test Information Distribution Engine (TIDE)	https://ca.tide.airast.org	192.237.154.47
Online Reporting System	https://ca.reports.airast.org	198.61.245.222

The Smarter Balanced California testing sites use a cloud-based satellite system for optimal load balancing during testing.

*Note: If your network filtering devices (e.g., proxy servers) and firewalls support wildcards, you may use *.cloud1.tds.airast.org and *.sbacpt.tds.airast.org instead of whitelisting each individual satellite URL listed below.*

System	URL	IP Address
AIRSecureTest Mobile Secure Browser Launchpad	https://mobile.tds.airast.org	50.57.2.88
TA and Student Practice and Training Sites	https://sbacpt.tds.airast.org*	69.20.121.89
	sat1.sbacpt.tds.airast.org	69.20.121.90
	sat2.sbacpt.tds.airast.org	74.205.105.232
	sat3.sbacpt.tds.airast.org	74.205.105.233
TA Interface and Student Testing Site	https://sbac.tds.airast.org	198.61.246.201
	https://login3.cloud1.tds.airast.org	198.61.245.221
	https://sat31.cloud1.tds.airast.org	23.253.28.96
	sat32.cloud1.tds.airast.org	23.253.28.97
	sat33.cloud1.tds.airast.org	23.253.26.253
	sat34.cloud1.tds.airast.org	23.253.26.254
	sat35.cloud1.tds.airast.org	162.209.46.116
	sat36.cloud1.tds.airast.org	162.209.46.117
	sat37.cloud1.tds.airast.org	162.209.46.118
	sat38.cloud1.tds.airast.org	162.209.46.119
	sat39.cloud1.tds.airast.org	23.253.194.8
	sat40.cloud1.tds.airast.org	23.253.194.9
	sat41.cloud1.tds.airast.org	23.253.194.10
	sat42.cloud1.tds.airast.org	23.253.194.11
sat43.cloud1.tds.airast.org	23.253.194.12	

System	URL	IP Address
TA Interface and Student Testing Site (cont'd)	sat44.cloud1.tds.airast.org	23.253.194.13
	sat45.cloud1.tds.airast.org	23.253.194.14
	sat46.cloud1.tds.airast.org	23.253.194.15
	sat47.cloud1.tds.airast.org	23.253.194.17
	sat48.cloud1.tds.airast.org	23.253.194.18
	sat49.cloud1.tds.airast.org	23.253.194.19
	sat50.cloud1.tds.airast.org	23.253.27.29
	sat51.cloud1.tds.airast.org	23.253.194.36
	sat52.cloud1.tds.airast.org	23.253.194.37
	sat53.cloud1.tds.airast.org	23.253.194.38
	sat54.cloud1.tds.airast.org	23.253.194.39
	sat55.cloud1.tds.airast.org	23.253.194.52
	sat56.cloud1.tds.airast.org	23.253.194.53
	sat57.cloud1.tds.airast.org	23.253.194.54
	sat58.cloud1.tds.airast.org	23.253.194.55
	sat59.cloud1.tds.airast.org	23.253.194.56
	sat60.cloud1.tds.airast.org	23.253.194.57
	sat61.cloud1.tds.airast.org	23.253.194.58
	sat62.cloud1.tds.airast.org	23.253.194.59

Important: Users who try to bookmark a satellite URL (sat1, etc.) will be automatically directed to the main URL. To ensure connection to any of the satellite sites, all URLs and IP addresses should be open or whitelisted.

Appendix B: School Technology Coordinator Checklist

	Activity	Estimated Time to Complete	Target Completion Date	Reference/ Resources
Direct Responsibilities				
<input type="checkbox"/>	1. Verify that your school's network and internet are properly configured for testing.	5–10 hours	3–4 weeks before testing begins in your school	Section I. Network and Internet Requirements Appendix A
<input type="checkbox"/>	2. Verify that all of your school's computers that will be used for online testing meet the minimum hardware requirements.	5–10 hours	3–4 weeks before testing begins in your school	Section II. Hardware Requirements
<input type="checkbox"/>	3. Work with technology personnel to: <ul style="list-style-type: none"> • Download the secure browser(s) • Conduct network diagnostics • Resolve any technical issues 	5–10 hours	3–4 weeks before testing begins in your school	Download Secure Browser Network Diagnostics Tools
<input type="checkbox"/>	4. Verify that the secure browser is installed and accessible on all computers that will be used for testing.	5–10 hours	3–4 weeks before testing begins in your school	Section V. Secure Browser Installation Section VI. Mobile Secure Browsers Section VII. Chromebooks Secure Browser
<input type="checkbox"/>	5. Disable pop-up blockers and install any necessary plug-ins or software.	5–10 hours	1–2 weeks before testing begins in your school	Section III. Software Requirements
<input type="checkbox"/>	6. On Windows computers, disable Fast User Switching. <i>Reminder: If a student can access multiple user accounts from a single computer, we encourage you to disable the Fast User Switching function.</i>	5–10 hours	1–2 weeks before testing begins in your school	Special Note for Windows Users: Fast User Switching
<input type="checkbox"/>	7. On Mac OS 10.7, 10.8, and 10.9 computers, disable Spaces in Mission Control.	5–10 hours	1–2 weeks before testing begins in your school	Disabling Spaces in Mission Control on Mac 10.7–10.9 Computers

	Activity	Estimated Time to Complete	Target Completion Date	Reference/ Resources
Direct Responsibilities				
<input type="checkbox"/>	8. Install and verify any required accommodation software onto computers that will be used for testing: <ul style="list-style-type: none"> • Braille hardware and software • Text-to-Speech and optional voice packs 			Section IV. Text-to-Braille Hardware and Software Section VIII. About Text-to-Speech and Voice Packs
<input type="checkbox"/>	9. Work with TAs to ensure they know how to close all forbidden applications except those identified as necessary by the District Technology Coordinator.			<i>TA User Guide</i> (available on portal Smarter Balanced portal)
Oversight Responsibilities				
<input type="checkbox"/>	Follow up on any technical issues raised by the School Test Coordinator for resolution.		Throughout testing window	

Appendix C: District Technology Coordinator Checklist

	Activity	Estimated Time to Complete	Target Completion Date	Reference/ Resources
Direct Responsibilities				
<input type="checkbox"/>	Work with District Test Coordinator to ensure timely network and computer setup before testing begins in your district: <ul style="list-style-type: none"> • Verify network is optimized and allows access to the online testing sites • Download the secure browser(s) • Conduct network diagnostics • Resolve any technical issues 	5-10 hours	At least two weeks before testing begins in your district	Section I. Network and Internet Requirements Section V. Secure Browser Installation Section VI. Mobile Secure Browsers Section VII. Chromebooks Secure Browser Appendix A
Oversight Responsibilities				
<input type="checkbox"/>	Work with school-based technology staff to ensure timely completion of secure browser installation on computers that will be used for testing.		At least two weeks before testing begins	
<input type="checkbox"/>	With the District Test Coordinator, work with school-based technology coordinators to disseminate information and resolve technical problems prior to the start of the testing window.		At least two weeks before testing begins	
<input type="checkbox"/>	Be available during the testing window for questions and problem solving.		Ongoing throughout testing window	

User Support

Smarter Balanced Help Desk

Smarter Balanced Field Test Help Desk Contact Information	
Phone	1.855.833.1969
Email	smarterbalancedhelpdesk@ets.org
Hours of Operation	Monday through Friday (see table below for hours)

Smarter Balanced Field Test Help Desk Hours of Operation by Time Zone Effective February 18, 2014 through June 6, 2014	
Time Zone	Hours of Operation
Eastern	7:00 a.m. to 12:00 a.m.
Central	6:00 a.m. to 11:00 p.m.
Mountain	5:00 a.m. to 10:00 p.m.
Pacific	4:00 a.m. to 9:00 p.m.
Hawaii	1:00 a.m. to 6:00 p.m.
U.S. Virgin Islands	7:00 a.m. to 12:00 a.m.

California Technical Assistance Center (for California Users)

CaTAC Contact Information	
Phone	1.800.955.2954
Fax	1.800.541.8455
Email	CaTAC@ets.org
Website	www.californiatac.org
Hours of Operation	7:00 a.m. to 5:00 p.m. Pacific

Change Log

Change	Section	Date
Updated Practice Test information to include the Training Test. Inserted references to Apple IOS 7.1 as appropriate.	Global	March 17, 2014
Updated bandwidth information based on additional, rigorous testing.	Bandwidth	March 17, 2014
Recommendations on the optimal number of student workstations per wireless connection were reformatted.	Wireless access points	March 17, 2014
For ease of reference due to the increased number, URLs and IP addresses were moved to Appendix A.	Network Configuration	March 17, 2014
Updated with current information from Symantec Verisign.	Certificate revocation list	March 17, 2014
Removed specific Mozilla Firefox references, as student computers do not require Firefox.	Section III. Software Requirements	March 17, 2014
Added Google Chrome.	Disabling Pop-Up Blockers	March 17, 2014
Reformatted information into a table. Added information about the iPad Air.	Supported Mobile Devices and Operating Systems	March 17, 2014
Updated Chromebook information.	Section VII. Chromebooks	March 17, 2014
Removed “accommodation” references, and inserted information about voice packs in mobile secure browsers.	Section VIII. About Text-to-Speech and Voice Packs	March 17, 2014
Inserted appendix for ease of reference.	Appendix A: IP Addresses and URLs for Smarter Balanced Systems	March 17, 2014
Inserted links to references/resources. Removed references to administrators other than Technology Coordinators.	Appendix B: School Technology Coordinator Checklist; Appendix C: District Technology Coordinator Checklist	March 17, 2014
Updated Help Desk hours.	User Support	March 17, 2014