CollegeBoard

NEW MEXICO
Public Education Department

Quick Guide for Setting Up Your Digital Testing Technology

For Digital Tests in the SAT® Suite of Assessments

Fall 2019

Published August 28, 2019
Prepared by the American Institutes for Research®

To learn more visit **digitaltesting.collegeboard.org**

Quick Guide for Setting Up Your Digital Testing Technology

AIR's Test Delivery System (TDS) has two components: the **Test Administrator (TA) Interface** and the **Student Interface**.

- Proctors use the TA Interface to create and manage test sessions from any web browser.
- Students access and complete their tests through the Student Interface via the Secure Browser.

This document explains in 4 steps how to set up technology in your schools and district:

Step 1. Setting up the proctor workstation
Step 2. Setting up student workstations
Step 3. Configuring your network for digital testing
Step 4. Configuring assistive technologies

STEP 1: SETTING UP THE PROCTOR WORKSTATION

It is unlikely that any setup is required for your proctor workstations. Nearly any modern device, including mobile devices like tablets and phones, with any modern browser can be used to access the TA site and administer a testing session. The TA Interface is a website. Any device you already use to check your email, browse Facebook, read news articles, or watch YouTube should be capable of administering tests.

If your school uses a firewall or other networking equipment that blocks access to public websites, you may need to whitelist AIR websites. For a list of websites you should whitelist, see the "Whitelisting Resources for Digital Testing" section in the document titled *Configurations, Troubleshooting, and Advanced Secure Browser Installation for Windows, Mac, or Chrome OS or Configurations and Troubleshooting for Linux.*

STEP 2: SETTING UP STUDENT WORKSTATIONS

In order for students to access digital tests, each student workstation needs the Secure Browser installed on it. The Secure Browser is AIR's customized web browser designed to keep tests secure by locking down the student desktop and preventing the student from accessing anything except their test. Unlike conventional web browsers, the Secure Browser displays the student application in full-screen mode with no user interface to the browser itself. It has no back button, next button, refresh button, or URL bar. Students open the Secure Browser and are taken exactly where they need to go.

To get started setting up your student workstations, you should first make sure your device is supported.

For a list of supported desktops and laptops and related hardware requirements, see the following table:

Desktops & Laptops		
Supported Operating Systems	**Minimum Requirements**	**Recommended Specifications**
Windows 7 SP1 (Professional and Enterprise) 8, 8.1 (Professional and Enterprise) 10, 10 in S Mode, Versions 1507-01803, 1809, 1903a (Educational, Professional, and Enterprise[a]) Server 2012 R2, 2016 R2 (thin client)	1 GHZ Processor 1 GB RAM (32-bit) 2 GB RAM (64-bit) 16 GB hard drive (32-bit) 20 GB hard drive (64-bit)	1.4 GHZ Processor 2 or more GB RAM 20 or more GB hard drive space
Mac OS X 10.9-10.15[a]	1 GHZ Processor 1 GB RAM (32-bit) 2 GB RAM (64-bit) 16 GB hard drive (32-bit) 20 GB hard drive (64-bit)	1.4 GHZ Processor 2 or more GB RAM 20 or more GB hard drive space
Linux (64-bit or 32-bit)[b] Fedora 28-30[a] LTS (Gnome) Ubuntu 16.04 LTS (Gnome)	1 GHZ Processor 1 GB RAM (32-bit) 2 GB RAM (64-bit) 16 GB hard drive (32-bit) 20 GB hard drive (64-bit) Required libraries/packages: GTK+ 2.18 or higher GLib 2.22 or higher Pango 1.14 or higher X.Org 1.0 or higher (1.7+ recommended) libstdc++ 4.3 or higher libreadline6:i386 (required for Ubuntu only) GNOME 2.16 or higher	1.4 GHZ Processor 2 or more GB RAM 20 or more GB hard drive space Recommended libraries/packages: In addition to the required libraries listed under minimum requirements, the following should be installed: NetworkManager 0.7 or higher DBus 1.0 or higher HAL 0.5.8 or higher
Linux (64-bit only)[b] Ubuntu 18.04, 20.04[a] LTS (Gnome)	1 GHZ Processor 2 GB RAM 20 GB hard drive space In addition to all libraries and packages listed above, Ubuntu 18.04 LTS (Gnome) also requires the following libraries: Sox Net-tools	1.4 GHZ Processor 2 or more GB RAM 20 or more GB hard drive space

a Support for this version is anticipated upon the completion of testing following its release.

b ARM-powered devices such as the Raspberry Pi are not supported for online testing.

For a list of supported tablets and Chromebooks, see the following table:

Tablets and Chromebooks	
Supported Operating Systems	**Supported Tablets**
iOS (iPads) 11.4, 12.2, 13[a], iPadOS[a]	4th Generation (Retina Display) 5th Generation (Retina Display) 6th Generation (Retina Display) iPad Air iPad Air 2 iPad Pro
Windows 8, 8.1 (Professional & Enterprise) 10 (Educational, Professional, & Enterprise)	AIR supports any tablet running these versions of Windows, but has done extensive testing only on Surface Pro, Surface Pro 3, Asus Transformer, and Dell Venue.
Chrome OS 75+	For a full list of supported Chromebooks, see https://support.google.com/chrome/a/answer/6220366. Chromebooks manufactured in 2017 or later must have an Enterprise or Education license to run in kiosk mode, which is necessary to run the Secure Browser. Chromebooks running in Tablet Mode and tablets running Chrome OS are not supported. Touchscreen features can be used on Chromebooks when available. AIR only supports versions of Chrome OS released on Google's stable channel.

a Support for this version is anticipated upon the completion of testing following its release.

For a list of supported NComputing solutions for Windows, see the following table:

NComputing		
Supported Server Host	**Supported Server Software**	**Supported Terminal**
Windows Server 2012 R2 Windows Server 2016 R2 Windows 10	vSpace PRO 10	L300, L350, firmware version 1.13.xx

For a list of supported terminal servers for Windows, see the following table:

Terminal Servers	
Supported Terminal Server	**Supported Thin Client**
Windows Server 2012 R2, 2016 R2	Any thin client that supports a Windows server. Thin clients allow access only to the program running on the host machine. Zero clients, which allow access to other programs on the client machine, are not supported.

All supported computers, laptops, tablets, and approved testing devices must meet the following requirements:

Testing Device	Requirement
Screen Dimensions	Screen dimensions must be 10" or larger (iPads with a 9.7" display are included in the support).
Screen Resolution	All devices must meet the minimum resolution. Larger resolutions can be applied as appropriate for the monitor or screen being used. Desktops, laptops, and tablets: **1024 x 768**
Keyboards	The use of external keyboards is highly recommended for tablets that will be used for testing and required when taking the SAT with Essay.
Mice	Wired two- or three-button mice can be used on desktops or laptops. Mice with "browser back" buttons should not be used.

Installing the Secure Browser

Once you have made sure your device is supported, you are ready to download and install the Secure Browser. This section explains where you can go to download the Secure Browser and how to install it.

The Secure Browser is available for all major operating systems listed above. You can download the Secure Browser from College Board's digital testing portal where you can also find basic installation instructions.

If you are a Technology Coordinator and it is your responsibility to manage a large number of machines across your school or district, you can likely use the same tools you are already familiar with to push the Secure Browser out to all of your machines at scale. For example, the Secure Browser ships as a MSI package which enables use of MSIEXEC.

If you are from a small school, you can follow the basic installation instructions on the digital testing portal to install the Secure Browser. The Secure Browser is installed the same way as most other software. You will be asked to download a file, open that file, and follow prompts along the way to install the Secure Browser. If you are familiar with installing software, install the Secure Browser the same way.

For iPads and Chromebooks, the AIRSecureTest app is the AIR's mobile version of the Secure Browser. It is available in each app store to download and install. The first time you open this app, it will ask you to choose your state or organization and assessment program. Your choice is saved and from then on, the Mobile Secure Browser works just like the desktop version, allowing you to access operational tests, practice tests, and the network diagnostic tool. You can also use any mobile device management utility to install the Secure Browser on multiple managed devices and configure those devices.

For schools and districts seeking advanced installation instructions for Windows, Mac, or Chrome OS, including instructions on how to install the Secure Browser on multiple devices, see the following document for your operating system:

- *Configurations, Troubleshooting, and Advanced Secure Browser Installation for Windows*
- *Configurations, Troubleshooting, and Advanced Secure Browser Installation for Mac*
- *Configurations, Troubleshooting, and Advanced Secure Browser Installation for Chrome OS*

- *Configurations and Troubleshooting Guide for Linux*

Other Configurations

For devices running Windows, Mac, Linux, or Chrome OS, there are a few additional configurations before secure testing can begin.

Several necessary configurations for Mac workstations can be performed by installing the Mac Secure Profile. For more information, see the section titled “Installing the Mac Secure Profile”

A feature in iOS called Automatic Assessment Configuration works with AIR’s Secure Browser to prepare an iPad for online testing.

All devices running on Chrome OS or iOS must be configured to access College Board Assessments. After AIRSecureTest is installed, launch the Secure Browser and access the launchpad. Select “College Board (SAT, PSAT 10 and PSAT 8/9)” from the States/Organizations and Assessments dropdown.

Disabling Fast User Switching for Windows

Fast User Switching is a feature in Windows 7, 8, 8.1, and 10 that allows for more than one user to be logged in at the same time. If Fast User Switching is not disabled and students try to access it during a test, the Secure Browser will pause the test.

Fast User Switching can be disabled using the Local Group Policy Editor or Registry Editor. For instructions on how to disable Fast User Switching, see the “Disabling Fast User Switching” section in the document titled *Configurations, Troubleshooting, and Advanced Secure Browser Installation for Windows*.

Disabling App Pre-launching for Windows

Application Prelaunch in a feature in Windows 10 that allows Universal Windows Platform apps, such as the Photos app or Edge web browser, to prelaunch and run in the background even if a user didn’t open the apps themselves. Users will be unable to start the Secure Browser with these apps running in the background and will be kicked out of a test if the apps launch while the user is running the Secure Browser.

App pre-launching can be disabled by using a PowerShell command and editing the registry. For instructions on how to disable app pre-launching, see this page from Microsoft’s Online Windows Support.

Installing the Mac Secure Profile

To configure Mac workstations, begin by downloading the Mac Secure Profile from the digital testing portal and then install it. The Secure Profile is new for 2019-2020 and automates a lot of the previously manual steps that would need to happen to secure the deice after installing the Secure Browser. The profile, upon installation, disables the hot keys for enabling Dictation, Mission Control, and Spaces and the trackpad gestures for accessing Lookup, Space Switching, Expose, and Notification Center and also sets function keys to standard functions, for all users of the Mac that it is deployed to. Upon installing the profile, the Mac should immediately be restarted so that all settings can be taken into effect. Instructions for installing the Secure Profile are in the document titled *Configurations, Troubleshooting, and Advanced Secure Browser Installation for Mac*.

Disabling Third-party App Updates for Mac

Updates to third-party apps may include components that compromise the testing environment. These updates can be disabled through System Preferences. For instructions on how to disable updates to third-party apps, see the “Disabling Updates to Third-Party Apps” section in the document titled *Configurations, Troubleshooting, and Advanced Secure Browser Installation for Mac*.

Disabling iTunes Updates for Mac

Updates to iTunes may pop up during a test. If updates to iTunes are not disabled and they pop up during a test, the Secure Browser will pause the test.

Updates to iTunes can be disabled through System Preferences. For instructions on how to disable updates to iTunes, see the "Disabling Updates to iTunes" section in the document titled *Configurations, Troubleshooting, and Advanced Secure Browser Installation for Mac*.

Disabling Siri for Mac

Siri is a virtual assistant that uses voice commands to answer questions and perform actions on Mac desktops and laptops running macOS 10.12 or later. If Siri is not disabled, students could potentially have access to features and information that they should not have access to while taking a secure assessment.

Siri can be disabled through System Preferences. For instructions on how to disable Siri, see the "Disabling Siri" section in the document titled *Configurations, Troubleshooting, and Advanced Secure Browser Installation for Mac*.

Disabling Fast User Switching for Mac

Fast User Switching is a feature in Mac OS X 10.9 and higher that allows for more than one user to be logged in at the same time. If Fast User Switching is not disabled and students try to access it during a test, the Secure Browser will pause the test.

Fast User Switching can be disabled through System Preferences. For instructions on how to disable Fast User Switching, see the "Disabling Fast User Switching" section in the document titled *Configurations, Troubleshooting, and Advanced Secure Browser Installation for Mac*.

Disabling On-Screen Keyboard for Linux

Ubuntu and Fedora feature an on-screen keyboard that should be disabled before you administer digital tests. If the on-screen keyboard is not disabled, the keyboard might pop up on a touchscreen device and, if it does, it may provoke the Secure Browser to pause the test.

The on-screen keyboard can be disabled through System Settings. For instructions on how to disable the on-screen keyboard, see the "Disabling On-Screen Keyboard" section in the document titled *Configurations and Troubleshooting for Linux*.

Adding Verdana Font for Linux

Some test content requires the Verdana TrueType font, which is not included in builds of Fedora or Ubuntu. For instructions to add the Verdana font, see the "Adding Verdana Font" section in the document titled *Configurations and Troubleshooting for Linux*.

Managing Chrome OS Auto-Updates

New versions of Chrome OS are released regularly and tested by AIR to ensure no new features pose a risk for digital testing. However, bugs or unintentional features do sometimes show up in the latest release. Because of this, AIR recommends disabling Chrome OS auto-updates or limiting auto-updates to a version used successfully before testing begins to ensure Chromebooks remain stable during testing season.

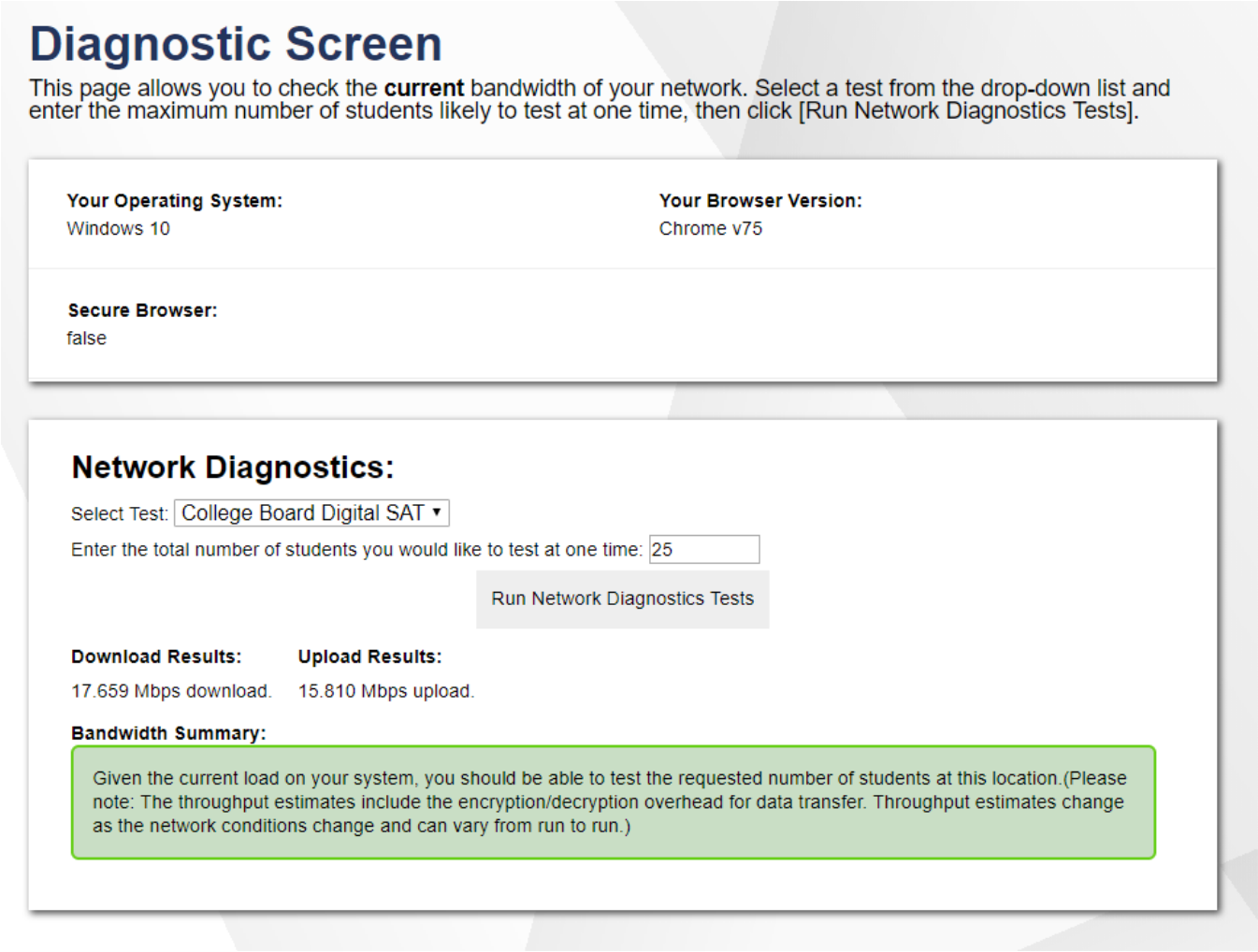
You can disable or limit Chrome OS updates through the Device Settings page on your Chromebook. From this page, you can stop auto-updates or allow auto-updates but only to a specific version. For more detailed instructions on how to disable or limit Chrome OS auto-updates, see the "Managing Chrome OS Auto-Updates" section in the document titled *Configurations, Troubleshooting, and Advanced Secure Browser Installation for Chrome OS*.

STEP 3: CONFIGURING YOUR NETWORK FOR DIGITAL TESTING

In this section, we provide some tools and recommendations to help configure your network for digital testing. To ensure a smooth administration, AIR recommends network bandwidth of at least 20 kilobits per second for each student being concurrently tested.

The Network Diagnostic Tool

AIR provides a network diagnostic tool to test your network's bandwidth to ensure it can handle administering digital tests. The network diagnostic tool can be accessed through the Secure Browser or from the Student Digital Test Preview through a conventional browser.



Once you are in the network diagnostic tool, enter the number of students you will test at peak volume and the tool will indicate if your network can handle testing. The goal of the network diagnostic tool is to determine if your network bandwidth can handle the number of students you hope to test at peak volume. If the tool indicates you should test with fewer students, try running a third-party network speed test like speedtest.net. If a third-party tool also indicates you lack proper bandwidth, determine if other activity on your network is drawing bandwidth away from the machine attempting to take the test. If it is, try to prioritize bandwidth for AIR's websites during digital testing.

Proxy Servers

If your technology coordinator has set up a proxy server at your school, you may need to configure the Secure Browser's proxy settings. For instructions on how to configure the Secure Browser's proxy settings, see the "Configuring the Secure Browser for Proxy Servers" section in *Configurations, Troubleshooting, and Advanced Secure Browser Installation for Windows, Mac, or Chrome OS or Configurations and Troubleshooting for Linux*.

Proxy servers must be configured to not cache data received from servers.

Session timeouts on proxy servers and other devices should be set to values greater than the typically scheduled testing time. For example, if test sessions are scheduled for 60 minutes, consider session timeouts of 65–70 minutes.

Traffic Shaping, Packet Prioritization, & Quality of Service

If your testing network includes devices that perform traffic shaping, packet prioritization, or Quality of Service, ensure AIR URLs have high priority. For a list of websites you should give high priority, see the "Whitelisting Resources" section in the document titled *Configurations, Troubleshooting, and Advanced Secure Browser Installation for Windows, Mac, or Chrome OS or Configurations and Troubleshooting for Linux.*

STEP 4: CONFIGURING ASSISTIVE TECHNOLOGIES

AIR's Test Delivery System is a website visible through a customized web browser.

Students who use assistive technologies with a standard web browser should be able to use those same technologies with the Test Delivery System. The best way to test compatibility with assistive technologies is by taking a practice test with those technologies turned on. If they do not work, contact Customer Service or see the College Board's resources for managing student test settings and assistive technology for digital testing, at cb.org/testsettings.

Assistive technology devices can be tested using the Student Digital Test Preview through the Secure Browser to determine if a device works College Board's assessments. Launch the Student Digital Test Preview through the Secure Browser application to evaluate functionality.

Assistive technologies must be launched on student workstations prior to launching the Secure Browser.

Supported Embedded Features

Embedded features work directly within the Test Delivery System. They can be accessed without additional third-party software.

Text-to-Speech

Text-to-speech (TTS) reads text on the screen aloud. Using TTS requires at least one voice pack to be installed on the student workstation. Voice packs that ship with the operating systems out of the box for Windows, Mac, and iOS are fully compatible with the Secure Browser, with features that include "speak" "pause" and "stop." For Chrome OS devices, the TTS function includes "Speak," "Stop Speaking," and "Speak selection" for highlighted text. Consider testing students who need TTS on the testing device prior to test day.

For a full list of voice packs that have been tested and are whitelisted for use with the Secure Browser and for instructions about configuring TTS settings for Windows or Mac, see the document titled *Assistive Technology Resource Guide*.

Supported Non-Embedded Features

Non-embedded features require the use of other hardware and/or software to make certain functionality available to students within the Test Delivery System. Non-embedded features require devices be set to permissive mode. The permissive mode, found in TIDE as a student test setting, allows the Secure Browser to interoperate with other applications, such as JAWS, NVDA, Braille display, etc. . Permissive mode is supported on Windows and Mac.

Screen Readers, Embossers, and Refreshable Braille Displays

Screen readers allow students to read text displayed on a screen with a speech synthesizer and a refreshable braille display. Screen reading requires software to be installed on the student device. For student workstations, AIR supports the JAWS screen reader and most refreshable braille displays. Other screen readers may also work and can be tested using the Student Digital Test Preview through the Secure Browser. For instructions on how to configure screen readers, see the document titled *Assistive Technology Resource Guide*.

Speech-to-Text

Speech-to-text (STT) allows a student to speak into a headset and have their speech converted into text that becomes the response that is entered into the Test Delivery System. Currently, AIR does not offer an embedded STT feature. STT is available for Windows and Mac through Dragon Naturally Speaking or other similar software. Schools and districts can use the Student Digital Test Preview through the Secure Browser to evaluate the SST, ensuring that the functions are allowed by the College Board Services for Students with Disabilities (SSD). STT is not available for Linux, iOS, or Chrome OS.

ADMINISTER DIGITAL TESTS

Before administering an operational test, get comfortable with the system by trying a practice administration. This can be accomplished on supported devices via the Secure Browser or through modern conventional browsers like Chrome or Firefox.

ADMINISTERING PRACTICE TESTS

To practice administering a test, complete the following steps:

1. Proctors should open a web browser, go to digitaltesting.collegeboard.org to access the TA Interface Practice Site, and sign in.
2. Students should launch the Secure Browser and click the link for the Digital Test Preview.
3. Proctors should start the Student Digital Test Preview and give the students the Session ID.
4. Students should click through the login pages. Students can log in anonymously as a guest or with their real account. In either case, they should use a Session ID from the proctor.

For more information about administering practice tests, see the *TA User Guide*.

When proctors and students are comfortable using the system, you are ready to administer an operational test.

ADMINISTERING OPERATIONAL TESTS

The steps for administering an operational test are nearly identical to the practice administration.

1. Proctors should open a web browser and go to the TA Interface.
2. Students should launch the Secure Browser.
3. Proctors should give students the Session ID.
4. Students should enter their **First Name**, **Registration Number**, and the **Session ID**.

For more information about administering operational tests, see the *Test Administrator User Guide*.

Customer Service and Support

If this document does not answer your questions, please contact College Board.

College Board School Day Customer Service

Phone: 855-373-6387

Follow the prompts for digital testing and listen to the options for your area of concern. Support options include the following:

- General College Board assessments questions and policies
- Technical support with AIRs digital testing systems, such as TIDE or TA Interface

Email: schooldayassessments@collegeboard.org

If you are calling for technical support, you will be asked to provide as much detail as possible about the issues you encountered.

Include the following information:

- Test coordinator name and IT/network contact person and contact information
- Registration numbers of affected students. Do not provide any other student information as doing so may violate FERPA policies.
- Test Session ID for the affected student tests
- Operating system and browser version information
- Any error messages and codes that appeared, if applicable
- Information about your network configuration:
    - Secure browser installation (to individual machines or network)
    - Wired or wireless Internet network setup

About College Board

College Board is a mission-driven not-for-profit organization that connects students to college success and opportunity. Founded in 1900, College Board was created to expand access to higher education. Today, the membership association is made up of over 6,000 of the world's leading educational institutions and is dedicated to promoting excellence and equity in education. Each year, the College Board helps more than seven million students prepare for a successful transition to college through programs and services in college readiness and college success — including the SAT® and the Advanced Placement® Program. The organization also serves the education community through research and advocacy on behalf of students, educators, and schools.

For further information, visit www.collegeboard.org.