Quick Guide for Setting Up Your Digital Testing Technology

For Digital Tests in the SAT® Suite of Assessments

Spring 2021

Published March 26, 2021
Prepared by Cambium Assessment, Inc.

Descriptions of the operation of the Test Information Distribution Engine, Test Delivery System, and related systems are property of Cambium Assessment, Inc (CAI) and are used with the permission of CA

To learn more visit digitaltesting.collegeboard.org
Quick Guide for Setting Up Your Digital Testing Technology

CAI’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 test administrator workstation**
**Step 2. Setting up student workstations**
**Step 3. Configuring your network for online 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 supported 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 add AIR and CAI websites to the Allowlist. For a list of websites you should add to the Allowlist, see the “Resources to add to the Allowlist for Online Testing” section in the documents titled *Configurations, Troubleshooting, and Advanced Secure Browser Installation for Windows, Mac, Chrome OS or Configurations and Troubleshooting for Linux,* or *Configurations for iOS/iPadOS.*

Proctors can print test session information with the print-on-request accommodation. To be able to print, proctor workstations must be connected to a printer.

### STEP 2: SETTING UP STUDENT WORKSTATIONS

In order for students to access digital tests, each student workstation needs CAI’s Secure Browser installed on it. The Secure Browser is CAI’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. Please note the Secure Browser is not supported for use within a virtual machine.
For a list of supported desktops and laptops and related hardware requirements, see the following table:

<table>
<thead>
<tr>
<th>Supported Operating Systems</th>
<th>Minimum Requirements</th>
<th>Recommended Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Windows</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8, 8.1 (Professional and Enterprise)</td>
<td>1 GHZ Processor</td>
<td>1.4 GHZ Processor</td>
</tr>
<tr>
<td>10, (Educational, Professional, and Enterprise) (Versions 1809 - 20H2)</td>
<td>1 GB RAM (32-bit)</td>
<td>2 or more GB RAM</td>
</tr>
<tr>
<td>Server 2012 R2, 2016 R2 (thin client)</td>
<td>2 GB RAM (64-bit)</td>
<td>20 or more GB hard drive space</td>
</tr>
<tr>
<td></td>
<td>16 GB hard drive (32-bit)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>20 GB hard drive (64-bit)</td>
<td></td>
</tr>
<tr>
<td><strong>Mac OS X/macOS</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.11-11 (Big Sur)</td>
<td>1 GHZ Processor</td>
<td>1.4 GHZ Processor</td>
</tr>
<tr>
<td></td>
<td>1 GB RAM (32-bit)</td>
<td>2 or more GB RAM</td>
</tr>
<tr>
<td></td>
<td>2 GB RAM (64-bit)</td>
<td>20 or more GB hard drive space</td>
</tr>
<tr>
<td></td>
<td>16 GB hard drive (32-bit)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>20 GB hard drive (64-bit)</td>
<td></td>
</tr>
<tr>
<td><strong>Linux (64-bit or 32-bit)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fedora 30-31 LTS (Gnome)</td>
<td>1 GHZ Processor</td>
<td>1.4 GHZ Processor</td>
</tr>
<tr>
<td>Ubuntu 16.04 LTS (Gnome)</td>
<td>1 GB RAM (32-bit)</td>
<td>2 or more GB RAM</td>
</tr>
<tr>
<td></td>
<td>2 GB RAM (64-bit)</td>
<td>20 or more GB hard drive space</td>
</tr>
<tr>
<td></td>
<td>16 GB hard drive (32-bit)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>20 GB hard drive (64-bit)</td>
<td></td>
</tr>
<tr>
<td>Required libraries/packages:</td>
<td>GTK+ 2.18 or higher</td>
<td></td>
</tr>
<tr>
<td></td>
<td>GLib 2.22 or higher</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Pango 1.14 or higher</td>
<td></td>
</tr>
<tr>
<td></td>
<td>X.Org 1.0 or higher (1.7+ recommended)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>libstdc++ 4.3 or higher</td>
<td></td>
</tr>
<tr>
<td></td>
<td>libreadline6:i386 (required for Ubuntu only)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>GNOME 2.16 or higher</td>
<td></td>
</tr>
<tr>
<td><strong>Linux (64-bit only)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ubuntu 18.04, 20.04 LTS (Gnome)</td>
<td>1 GHZ Processor</td>
<td>1.4 GHZ Processor</td>
</tr>
<tr>
<td></td>
<td>2 GB RAM</td>
<td>2 or more GB RAM</td>
</tr>
<tr>
<td></td>
<td>20 GB hard drive space</td>
<td>20 or more GB hard drive space</td>
</tr>
<tr>
<td>In addition to all libraries and packages listed above, Ubuntu 18.04 LTS (Gnome) also requires the following libraries:</td>
<td>Sox</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Net-tools</td>
<td></td>
</tr>
</tbody>
</table>

a Support for this version is anticipated upon the completion of testing following its release.
b Intel, AMD, and ARM devices are supported. ARM devices require x64 emulation.
c Intel and Apple silicon devices are supported. Apple silicon devices require Rosetta 2.
d Raspberry Pi and other similar single-board computers are not supported for testing.
For a list of supported tablets and Chromebooks, see the following table:

<table>
<thead>
<tr>
<th>Tablets and Chromebooks</th>
<th>Supported Operating Systems</th>
<th>Supported Tablets</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>iOS/iPadOS (iPads)</strong></td>
<td>12.4, 13.4-13.7, 14 - 14.4</td>
<td>All 9.7” or larger iPads running a supported version of iOS/iPadOS.</td>
</tr>
<tr>
<td><strong>Windows</strong></td>
<td>8, 8.1 (Professional &amp; Enterprise) 10 (Educational, Professional, &amp; Enterprise)</td>
<td>CAI 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.</td>
</tr>
<tr>
<td><strong>Chrome OS</strong></td>
<td>83+</td>
<td>For a full list of supported Chromebooks, see <a href="https://support.google.com/chrome/a/answer/6220366">https://support.google.com/chrome/a/answer/6220366</a>. 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. This change restricting kiosk mode does not affect the Chrome operating system. You can still use any version of Chrome OS on hardware manufactured in 2016 or earlier. Chromebooks running in Tablet Mode and tablets running Chrome OS are not supported. Touchscreen features can be used on Chromebooks when available. CAI only supports versions of Chrome OS released on Google's stable channel.</td>
</tr>
</tbody>
</table>

a Support for this version is anticipated upon the completion of testing following its release.
b A known issue with Chrome OS 88 and 89 sometimes prevents text-to-speech (TTS) from working properly the first time it is invoked. Users who encounter this issue should reinvoke TTS.

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

<table>
<thead>
<tr>
<th>NComputing</th>
<th>Supported Server Host</th>
<th>Supported Server Software</th>
<th>Supported Terminal</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Windows Server 2012 R2</td>
<td>vSpace PRO 10</td>
<td>L300, L350, firmware version 1.13.xx</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2016 R2</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Windows 10</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Terminal Servers</th>
<th>Supported Terminal Server</th>
<th>Supported Thin Client</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Windows Server 2012 R2, 2016 R2</td>
<td>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. Please note using a terminal services or remote desktop connection to access a Windows Server or workstation that has the Secure Browser installed is typically not a secure test environment.</td>
</tr>
</tbody>
</table>
Devices running CloudReady NeverWare are also supported. For information on supported devices and installation instructions, please visit https://www.neverware.com.

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

<table>
<thead>
<tr>
<th>Testing Device</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Screen Dimensions</strong></td>
<td>Screen dimensions must be 10” or larger (iPads with a 9.7” display are supported).</td>
</tr>
<tr>
<td><strong>Monitors &amp; Displays</strong></td>
<td>All devices must meet the minimum resolution of 1024 x 768. Larger resolutions can be applied as appropriate for the monitor or screen being used. For the best experience, your device’s display scale should be set to 100% to keep the amount of usable screen real estate within the 1024x768 minimum resolution for TDS. A secure testing environment can only be guaranteed when using a single display. A multi-monitor configuration is not supported.</td>
</tr>
</tbody>
</table>
| **Keyboards** | For the best possible testing experience, the use of external keyboards is highly recommended for tablets that will be used for testing. On-screen keyboards take screen real estate away from the test and may make typing responses more difficult. For iPads, the following are examples of external keyboards you might use:  
- iPad 8th Generation: Logitech Rugged Combo or Logitech Combo Touch  
- iPad Air 3rd Generation: Apple Magic Keyboard or Apple Smart Folio Keyboard  
- iPad Pro: Air Keyboard |
| **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 an 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.

If you are running the Secure Browser on Apple silicon devices, you must first install Rosetta 2.
Rosetta 2 may already be installed on your Apple silicon device if you needed it to run another Intel-based application. If it not already installed, a prompt to install it will appear the first time you launch the Secure Browser. Rosetta 2 can also be deployed to multiple devices at once through scripting or mobile device management (MDM). For more information about Rosetta 2, including instructions to install it, please see https://support.apple.com/en-us/HT211861.

For iPads and Chromebooks, the SecureTestBrowser (formerly AIRSecureTest) app is CAI’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

### Other Configurations

For devices running Windows, Mac, Linux, iOS, 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 built into iOS/iPadOS called Assessment Mode (AM) (formerly known as Automatic Assessment Configuration (AAC)) handles many necessary configurations to prepare iPads for online testing. For more information on AM, including a list of features it disables, please visit https://support.apple.com/en-us/HT204775. In addition to AM disabling features listed at the URL above, there are a few additional features in iOS/iPadOS that must be disabled prior to the administration of online testing. These features, which are listed below, should not be available to students without an accommodation and AM does not currently block them.

### Disabling Fast User Switching for Windows

Fast User Switching is a feature in Windows 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 another user account 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 “How to Disable 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 is 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. This does not affect users running the CAI 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 your portal and then install it. The profile, upon installation, disables the hot keys for enabling Mission Control, Spaces, Screenshots, and Dictation and the trackpad gestures for accessing Lookup, App Exposé, Launchpad, and Show Desktop. It also sets function keys to standard functions for all users of the Mac to which it is deployed, disables Voice Control, and disables the menu pop-up that appears when triple-tapping the power button on Touch Bar-enabled devices. An update for Spring 2021 added the ability to prevent the device from receiving files via AirDrop and the ability to have your Mac identify items under the pointer. Upon installing the profile, the Mac should immediately be restarted so that all settings can take effect. The Secure Profile has been updated for Spring 2021. If you have previously installed an older version of the Secure Profile, you must download and install the new version from the link on your portal. 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 “How to Disable Updates to Third-Party Apps” 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 10.11 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 another user account 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 “How to Disable Fast User Switching” section in the document titled Configurations, Troubleshooting, and Advanced Secure Browser Installation for Mac.

Disabling Sleep Mode for macOS 11

Sleep mode should be disabled on macOS 11 devices prior to testing. If sleep mode is not disabled and the device enters sleep mode while the student is testing, the student’s testing experience may be disrupted. Sleep mode can be disabled through System Preferences. For instructions on how to disable sleep mode, see the “How to Disable Sleep Mode on macOS 11” 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 online 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 “How to Disable On-Screen Keyboard” section in the document titled Configurations.
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 on how to add the Verdana font, see the “How to Add Verdana Font” section in the document titled Configurations and Troubleshooting for Linux.

Disabling Voice Control for iPads

iPads running any supported version of iOS/iPadOS have access to a feature called Voice Control that is not automatically disabled by Assessment Mode (AM) (formerly known as Automatic Assessment Configuration (AAC)). Voice Control allows iPad users to control an iPad using voice commands. If this feature is enabled on iPads that are used for testing, students may be able to access unwanted apps, such as web browsers, during a test.

Voice Control is disabled by default. If it has never been enabled on an iPad, you have nothing to do. If it has been enabled, you must disable it before a student takes a test. Voice Control can be disabled through accessibility settings. For instructions on how to disable Voice Control, see the “How to Disable Voice Control” section in the document titled Configurations for iPads.

Disabling Emoji Keyboard for iPads

iPads running any supported version of iOS/iPadOS have an emoji keyboard enabled by default. If the emoji keyboard is not disabled, students will be able to enter emoticons into a test, which can be confusing for scorers.

The emoji keyboard can be disabled through keyboard settings. For instructions on how to disable the emoji keyboard, see the “How to Disable the Emoji Keyboard” section in the document titled Configurations for iPads.

Managing Chrome OS Auto-Updates

New versions of Chrome OS are released regularly and tested by CAI to ensure no new features pose a risk for online testing. However, bugs or unintentional features do sometimes show up in the latest release. Because of this, CAI recommends disabling Chrome OS auto-updates or limiting auto-updates to a version used successfully before summative 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 “How to Manage 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 ONLINE TESTING

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

The Network Diagnostic Tool

CAI 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 supported 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 CAI’s websites during online 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 “How to Configure the Secure Browser for Proxy Servers” section in Configurations, Troubleshooting, and Advanced Secure Browser Installation Guide for Windows, Mac, or Chrome OS, Configurations and Troubleshooting for Linux, or Configurations for iOS/iPadOS.

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 CAI URLs have high priority. For a list of websites you should give high priority, see the “Which Resources to add to the Allowlist for Online Testing” section in the document titled Configurations, Troubleshooting, and Advanced Secure Browser Installation Guide for Windows, Mac, or Chrome OS, Configurations and Troubleshooting for Linux, or Configurations for iOS/iPadOS.

STEP 4: CONFIGURING ASSISTIVE TECHNOLOGIES

CAI’s Test Delivery System is a website that is accessed through a Secure Browser.

Students who use assistive technologies with a supported 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 with the College Board’s assessments. Launch the Student Digital Test Preview through the Secure Browser application to evaluate functionality. For a list of supported technologies and configuration instructions, see cb.org/testsettings.

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

Supported Embedded Features
Embedded features are built into the Test Delivery System and can be accessed through settings. They can be accessed without additional third-party software. To use these embedded features, students need an accommodation.

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/iPadOS are fully compatible with the Secure Browser. The Secure Browser works with voice packs that ship out of the box for Chrome OS devices, but the pause feature does not work properly on these devices. For students who need the use of TTS, CAI recommends using a desktop, laptop, or tablet running Windows, Mac OS X/macOS, or iOS/iPadOS. If a Chromebook is being used, there is a workaround that allows students to highlight a
passage of text and have TTS read just that passage, eliminating the need for the pause feature.

For instructions about configuring TTS settings for Windows or Mac, see “Configure Text-to-Speech” at cb.org/testsettings.

For a full list of voice packs that have been tested and are added to the Allowlist by the Secure Browser see below. Supported Voice Packs for these operating systems are supported:

- Chrome™ OS
- Windows
- Mac®
- iOS/iPadOS

If students need to use a voice pack that’s not listed above, test it with the secure browser in the Student Digital Test Preview to make sure it works.

See cb.org/testsettings

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 settings be set to permissive mode. This mode, found in TIDE as a student test setting, temporarily lowers the security settings of the Secure Browser so that the student can interoperate with other software on the device, like JAWS or ZoomText, while they are taking the test. Permissive mode is supported on Windows and Mac. Permissive mode is not available for Linux, iPads, or Chromebooks. Users of these devices who need assistive technology supports should use CAI’s embedded tools.

Screen Readers

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 workstation. For a list of supported screen readers and configuration instructions, see cb.org/testsettings.

Refreshable Braille Displays

Refreshable Braille Displays (RBDs) are used to read text-only content on ELA, Mathematics, and Social Sciences tests, while Braille embossers are needed to read any content with images in ELA and Social Sciences tests, as well as advanced content in Mathematics and Science tests. RBDs must be properly setup before they can be used by students. For information about installing and setting up RBDs, refer to the product’s provided instructions and manuals.

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. STT is available through third-party software for Windows and Mac through Dragon Naturally Speaking or other similar software. Users should verify the security and privacy policies of any third-party software before deciding to use that software. Many STT providers send a student’s audio recording to the cloud for processing. This should be disabled before use so sensitive testing data is not sent to third parties. Users should have a clear understanding of what third-party providers do and do not do with student information. For more information regarding STT and possible solutions for other operating systems, see cb.org/testsettings.

Alternative Computer Inputs

Alternative Computer Input (ACI) tools allow students to interact with a computer without using a traditional mouse and keyboard setup. CAI does not include any embedded alternative computer input tools, but it supports several third-party alternative computer input technologies. For more information about supported third-party
alternative computer inputs, see cb.org/testsettings.

Assistive Keyboard and Mouse Input
Assistive Keyboard and Mouse Input tools provide additional support to students who need to use a keyboard and mouse in order to respond to test items. CAI does not include any embedded assistive keyboard and mouse input tools, as these tools typically involve the use of special hardware, but TDS does support several third-party assistive keyboard and mouse input tools. For more information about supported third-party assistive keyboard and mouse input solutions, see cb.org/testsettings.

Screen Magnification
Screen magnifier assistive technology enlarges the content displayed on the computer screen in order to assist students who need the content magnified. Although TDS supports some non-embedded screen magnifier tools from third parties, it is recommended that students use the embedded zoom tools in TDS. For more information about screen magnifier assistive technology, see cb.org/testsettings.
ADMINISTERING ONLINE TESTS

Before administering an operational test, get comfortable with the system by administering a practice test. Practice tests can be administered on supported devices via the Secure Browser or through modern supported browsers.

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 PRACTICE TESTS

To administer a practice 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.

ADMINISTERING OPERATIONAL TESTS

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

1. Proctors should open a web browser and go to the TA Site.
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.

Contact the Help Desk for any additional assistance.
Customer Service and Support
If this document does not answer your questions, please contact the 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 CAIs 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, 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 https://www.collegeboard.org.