Quick Guide for Setting Up Your Online Testing Technology

CAI's Test Delivery System (TDS) has two components: the **Test Administration Interface** and the **Student Interface**.

- Test administrators use the Test Administration 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 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 modern browser can be used to access the Test Administration site and administer a testing session. The Test Administration 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 CAI websites. For a list of websites you should whitelist, see the "Whitelisting Resources for Online Testing" section in the document titled *Configurations, Troubleshooting, and Advanced Secure Browser Installation for Windows, Mac, or Chrome OS or Configurations and Troubleshooting for Android or Linux*.

Proctors can print test session information or test items for students 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 online 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:

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 (Educational, Professional, and Enterprise) (Versions 1507-1903) 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/iPadOS (iPads) 11.4, 12.2, 12.3, 12.4, 13.2.2	All 9.7" or larger iPads running a supported version of iOS/iPadOS.
Android 7.1, 8.1	All modern Android tablets running a supported version of Android and capable of running a restricted profile.
Windows 8, 8.1 (Professional & Enterprise) 10 (Educational, Professional, & Enterprise)	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.
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. CAI 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. 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.

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:

Screen Dimensions
Screen dimensions must be 10" or larger (iPads with a 9.7" display are included).

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.

Mice
Wired two- or three-button mice can be used on desktops or laptops. Mice with "browser back" buttons should not be used.

Headphones & Headsets
Wired headphones with a 3.5 mm connector or USB headphones

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 your portal. Your portal also contains 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 your 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, Android tablets, and Chromebooks, the Secure Test (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 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.

Windows 10 and Windows 10 in S Mode come with Microsoft's Take a Test app, which enforces a locked-down, secure testing environment identical to CAI's Secure Browser. Users of the Take a Test app do not need to install the CAI Secure Browser on the testing machine. Instructions for configuring the Take a Test app can be found on your portal.

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, Android, 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 Automatic Assessment Configuration (AAC) handles many necessary configurations to prepare iPads for online testing. For more information on AAC, including a list of features it disables, please visit https://support.apple.com/en-us/HT204775#AAC. In addition to AAC 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 AAC does not currently block them.

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 "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. Users will be unable to start the Secure Browser or Take a Test 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 or Take a Test app.

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 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 take 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 "How to Disable 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 "How to Disable 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 "How to Disable 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 "How to Disable Fast User Switching" section in the document titled *Configurations, Troubleshooting, and Advanced Secure Browser Installation for Mac*.

Disabling Keyboard Shortcuts for Screenshots for Mac

Mac users can take screenshots using keyboard shortcuts. If these shortcuts are not disabled, students will be unable to sign in to a test.

Keyboard shortcuts for screenshots can be disabled through System Preferences. For instructions on how to disable keyboard shortcuts for screenshots, see the "How to Disable Keyboard Shortcuts for Screenshots" 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 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 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 iPadOS 13

iPads running iPadOS 13 have access to a feature called Voice Control that is not automatically disabled by Automatic Assessment Configuration (AAC). Voice Control allows iPad users to control an iPad using voice commands. If this feature is enabled on iPads running iPadOS 13 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 on iPads running iPadOS 13, see the "How to Disable Voice Control on iPadOS 13" section in the document titled *Configurations for iOS/iPadOS*.

Disabling VoiceOver for iOS 11 & 12

iPads running iOS 11.x or 12.x have access to a feature called VoiceOver that is not automatically disabled by Automatic Assessment Configuration (AAC).

VoiceOver is a gesture-based screen reader that allows users to receive audible descriptions of what's on the screen of their iPad. VoiceOver also changes touchscreen gestures to have different effects and adds additional gestures that allow users to move around the screen and control their iPads. If VoiceOver is not disabled on iPads running iOS 11.x or 12.x, students may be able to access unwanted apps during a test. This feature should not be available to students without an accommodation.

VoiceOver can be disabled through accessibility settings. For instructions on how to disable VoiceOver on iOS 11 or 12, see the "How to Disable VoiceOver on iOS 11 & 12" section in the document titled *Configurations for iOS/iPadOS*.

Disabling Emoji Keyboard for iOS/iPadOS

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 iOS/iPadOS*.

Enabling Secure Browser Keyboard for Android

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

You can enable the Secure Browser

keyboard through Settings. For instructions on how to enable the Secure Browser keyboard, see the "Enabling the Secure Browser Keyboard" section in the document titled *Configurations and Troubleshooting for Android*.

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.

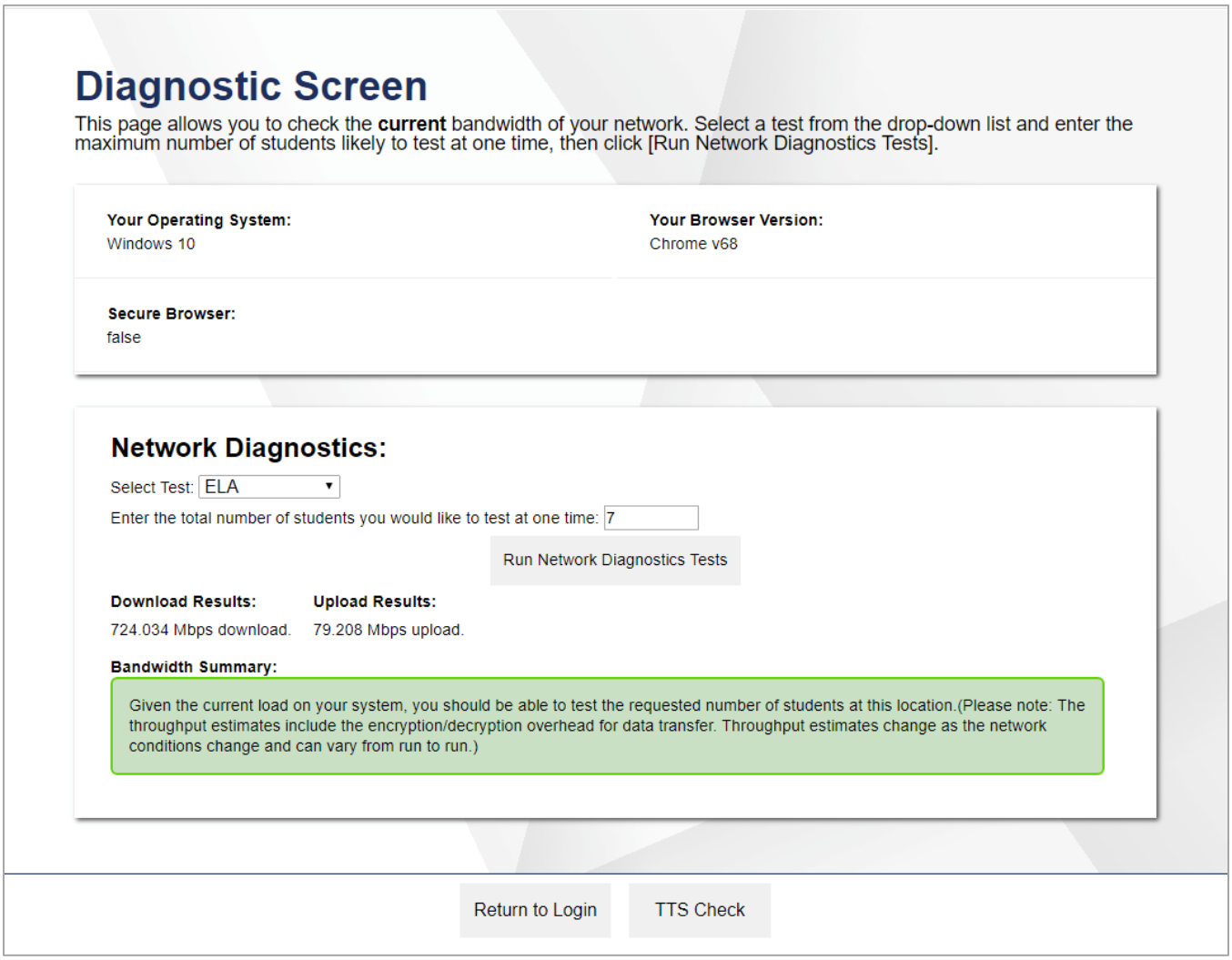
You can disable or limit Chrome OS updates through the Device Settings page on your Chromebook. From this page, you can stop auto-updates or allow auto-updates but only to a specific version. For more detailed instructions on how to disable or limit Chrome OS auto-updates, see the "How to Manage Chrome 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 online tests. The network diagnostic tool can be accessed through the Secure Browser or from your portal or practice test site 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 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 for Windows, Mac, or Chrome OS, Configurations and Troubleshooting for Android or 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 Whitelist for Online Testing" section in the document titled *Configurations, Troubleshooting, and Advanced Secure Browser Installation for Windows, Mac, or Chrome OS, Configurations and Troubleshooting for Android or Linux, or Configurations for iOS/iPadOS*.

STEP 4: CONFIGURING ASSISTIVE TECHNOLOGIES

CAI'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 the help desk or see the document titled *Assistive Technology Manual* for more information.

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. The Secure Browser recognizes voice packs that ship out of the box for Android and Chrome OS devices for playback and stop but the pause feature does not work properly on these devices. Consider testing students who need TTS on desktops or laptops running Windows or Mac or on iPads. A workaround for Chrome OS is available. It allows students to highlight a passage of text and have TTS read just that passage, eliminating the need for the pause

feature.

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

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. 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're taking the test. 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 and Proctor workstations. For student workstations, CAI supports the JAWS screen reader and most refreshable braille displays. For screen reading on ELA tests, you must have the JAWS screen reader because it is the only screen reader that supports suppressing read-aloud on reading passages. For braille files on Proctor workstations, CAI supports Duxbury Braille Translation software. Proctors need this software to emboss braille test content. To emboss tactile graphics, CAI supports ViewPlus embossers using the Tiger Software Suite (Tiger Designer and Tiger Viewer). Other screen readers may also work and should be tested in a practice test. For instructions on how to configure screen readers, see the document titled *Assistive Technology Manual*.

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, CAI does not offer an embedded STT feature. STT is available 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. Users should have a clear understanding of what third-party providers do and do not do with student information. STT is not available for Linux, iOS, Android, or Chrome OS.

Word Prediction

Word prediction software predicts words as a student types. Currently, CAI does not offer an embedded word prediction feature. Word prediction is available for Windows and Mac through the use of third-party apps like Co:Writer, Read&Write, and many others. For more information about supported third-party apps, see the document titled *Assistive Technology Manual*.

ADMINISTER 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 conventional browsers like Chrome or Firefox.

ADMINISTERING PRACTICE TESTS

To administer a practice test, complete the following steps:

1. Proctors should open a web browser, go to the Test Administration Practice and Training Site, and choose a practice test to administer.
2. Students should launch the Secure Browser and click the link for practice tests.
3. Proctors should 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 *Test Administration 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 administering a practice test.

1. Proctors should open a web browser and go to the Test Administration Site.
2. Students should launch the Secure Browser.
3. Proctors should give students the Session ID.
4. Students should enter the SessionID, their first name, and their Student ID.

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

Contact the Help Desk for any additional assistance.