Quick Guide for Setting Up Your Online Testing Technology

Cambium Assessment, Inc. (CAI)'s Test Delivery System (TDS) has two components: the **Test Administrator (TA) Interface** and the **Student Interface**.

- TAs 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 four steps how to set up technology in your corporation and schools:

Step 1. Setting up the TA 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 TEST ADMINISTRATOR WORKSTATION

It is unlikely that any setup is required for your TA workstations. The TA Interface is a website. Nearly any modern device with any modern browser can be used to access the TA Interface site and administer a testing session. Per IDOE policy[1], the TA workstation should be a school-provided device, and not a TA's personal device. Smart phones should not be used to administer assessments.

If your school uses a firewall or other networking equipment that blocks access to public websites, you may need to add CAI websites to your allowlist. For a list of websites you should add to your allowlist, see the "Which Resources to Add to your Allowlist 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 Linux, or Configurations for iOS/iPadOS*.

TAs can print test session information or test items for students with the print-on-demand. accommodation. To be able to print, TA workstations must be connected to a printer.

STEP 2: SETTING UP STUDENT WORK STATIO NS

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 the device is supported. Please note the Secure Browser is not supported for use within a virtual machine. Please be sure to check the Indiana Assessment Portal's Secure Browsers and Supported Browsers pages to stay up-to-date with any issues with recent operating system releases.

The following table contains a list of supported operating systems and related hardware requirements for desktops and laptops:

Desktops and Laptops		
Supported Operating Systems	**Minimum Requirements**	**Recommended Specifications**
Windows 8, 8.1 (Professional and Enterprise) 10 (Educational, Professional, and Enterprise) (Versions 1809-2004[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/macOS 10.11-10.15, 11 (Big Sur)[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 30-31[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 RaspberryPi are not supported for online testing.

The following table contains a list of supported operating systems for tablets and Chromebooks:

Tablets and Chrome books	
Supported Operating Systems	**Supported Tablets**
iOS/iPadOS (iPads[b]) 12.4, 13.4-13.7, 14[a]	All 9.7" or larger iPads running a supported version of iOS/iPadOS.
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 83-86, 87[a]	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.
b. When using iOS, ensure the English keyboard is installed and set as the default.

The following table contains 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

The following table contains a list of supported terminal servers for Windows:

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 not a secure test environment.

The following table contains a list of supported operating systems and corresponding web browsers for each CAI application:

Supported Operating Systems	Supported Devices	Supported Web Browsers	TA Sites, Released Item Repository	TIDE, ORS
Windows				
8 (Professional and Enterprise) 8.1 (Professional and Enterprise)	Desktops/Laptops	Chrome 84+	✓	✓
		Firefox 60+	✓	✓
10 (Educational, Professional, and Enterprise) (Versions 1809-2004[c])	Desktops/Laptops	Chrome 84+	✓	✓
		Firefox 60+	✓	✓
		Edge 17+	✓	✓
Server 2012 R2, 2016 R2 (thin client)	Desktops/Laptops	Chrome 84+	✓	✓
		Firefox 60+	✓	✓
Mac				
10.11-10.15, 11 (Big Sur)[c]	Desktops/Laptops	Chrome 84+	✓	✓
		Firefox 60+	✓	✓
		Safari 11+	✓	✓
Linux				
Fedora 30-31[c] LTS (Gnome)	Desktops/Laptops	Chrome 84+	✓	✓
		Firefox 60+	✓	✓
Ubuntu 16.04, 18.04, 20.04[c] LTS (Gnome)	Desktops/Laptops	Chrome 84+	✓	✓
		Firefox 60+	✓	✓

Supported Operating Systems	Supported Devices	Supported Web Browsers	TA Sites, Released Item Repository	TIDE, ORS[a]
iOS[b]				
12.4	All 9.7" or larger iPads running a supported version of iOS/iPadOS.	Safari 12	✓	
13.4-13.7	All 9.7" or larger iPads running a supported version of iOS/iPadOS.	Safari 13	✓	
14[c]	All 9.7" or larger iPads running a supported version of iOS/iPadOS.	Safari 14[c]	✓	
Chrome OS				
83-86, 87[c]	Chromebooks	Chrome 84+	✓	

a. TIDE and ORS can be accessed with iOS and Chrome devices; however, these devices are not fully supported due to the upload and download functionality frequently utilized within the two systems.
b. When using iOS, ensure the English keyboard is installed and set as the default keyboard.
c. Support for this version will begin upon the completion of testing following its release

Devices running CloudReady or 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 Resolution

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.

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 can be used. Wireless (Bluetooth) headphones are not permitted, as they pose a threat to test security.

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

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. **CAI updates the Secure Browser annually and makes it available at the beginning of each new school year. When updating from a previous version of the desktop Secure Browser for Windows, Mac, or Linux, the previous version must be uninstalled prior to installing the current version. The updated mobile secure browsers for iOS and Chrome OS are available in their respective App and Web stores; iOS and Chrome OS devices with the previous year's mobile secure browser will auto-update to the new year's browser. The mobile secure browsers for iOS and Chrome OS only need to be installed if doing so on a device for the first time.**

The Secure Browser is available for all major operating systems listed above. Secure Browser downloads and basic installation directions are available on the Indiana Assessment Portal at https://indiana.portal.cambiumast.com/secure-browsers.stml.

If you are a Technology Coordinator responsible for managing 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 to install the Secure Browser, as it is installed the same way as most other software. After downloading the installation file, open it, and then follow the prompts along the way to install the Secure Browser.

For iPads and Chromebooks, the SecureTestBrowser 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.

For advanced installation instructions for Windows, Mac, or Chrome OS, including instructions on how to install the Secure Browser on multiple devices, or additional configurations and troubleshooting, 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*
- *Configurations for iOS/iPadOS*

Other Configurations

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

A feature built into iOS/iPadOS called Assessment Mode (AM) (formerly known as Automatic Assessment Configuration) 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#AM. 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 (described at the end of this section) are not currently blocked by AM and must not be available to students without an accommodation.

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 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. 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.

How to Install the Mac Secure Profile

Several necessary configurations for Mac workstations can be performed by installing the Mac Secure Profile. CAI recommends installing the Mac Secure Profile, as it reduces the number of steps needed to set up Mac devices for online testing; however, the Mac Secure Profile is not required for online testing. 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 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 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 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.*

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*.

Disabling Voice Control for iPadOS 13

iPads running any supported version of iOS/iPadOS have access to a feature called Voice Control that is not automatically disabled by AM. 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 iOS/iPadOS*.

Disabling VoiceOver for iPads

iPads running any supported version of iOS/iPadOS have access to a feature called VoiceOver that is not automatically disabled by AM. VoiceOver is a gesture-based screen reader that allows users to receive audible descriptions of what is 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, 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, see the "How to Disable VoiceOver" section in the document titled *Configurations for iPads*.

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.

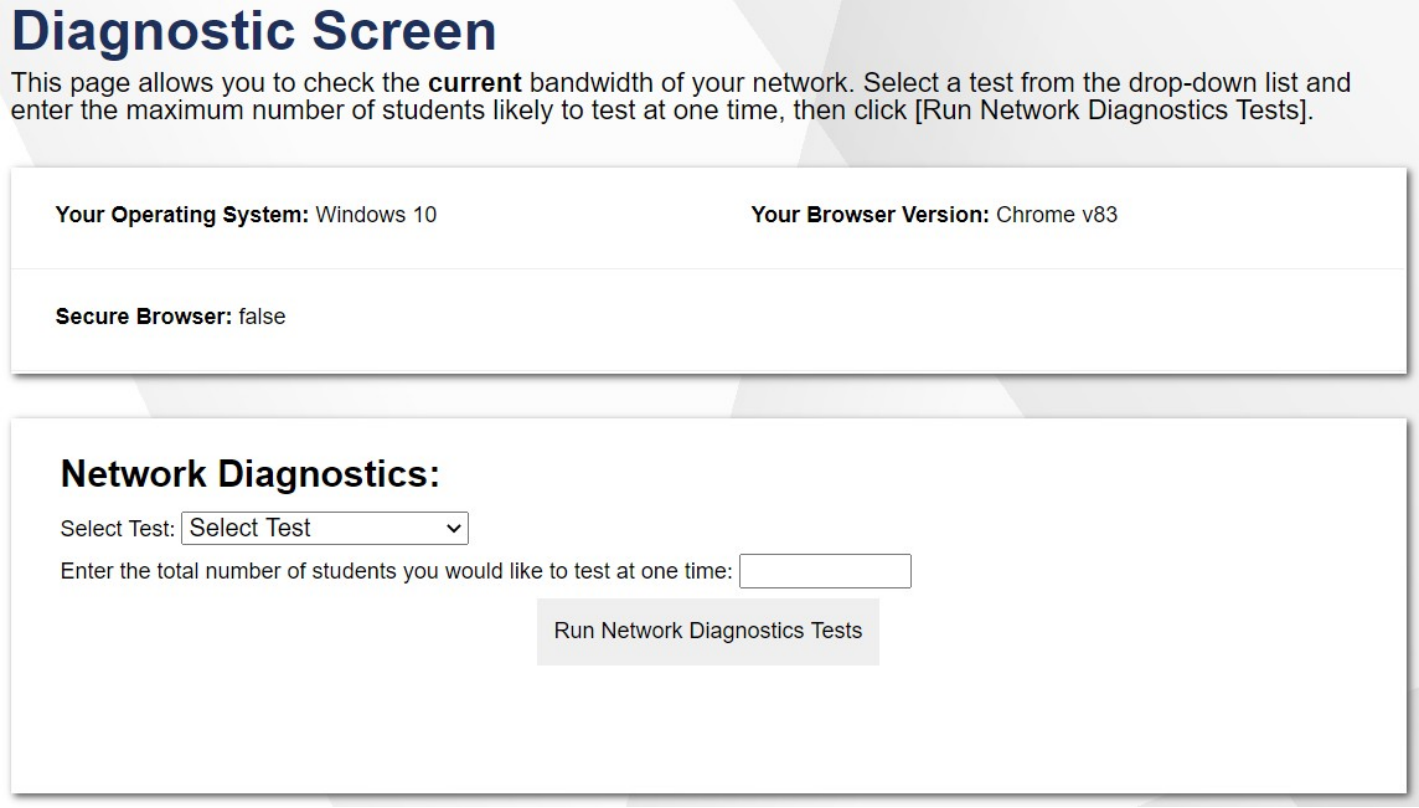
The emoji keyboard can be disabled through keyboard settings. For instructions on how to disable the emoji keyboard, see the "How to Disable the Emoji Keyboard" section in the document titled *Configurations for iOS/iPadOS*.

STEP 3: CONFIG URING YOUR NETWORK FOR ONLINE TESTING

This section includes 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, a conventional browser, the Indiana Assessment Portal, or the Released Items Repository (RIR) site.



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, 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 or adjust your testing schedule to reduce your number of concurrent users.

Proxy Servers

If a proxy server is set up 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 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 you Allowlist 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 Linux, or Configurations for iOS/iPadOS*.

STEP 4: CONFIG URING ASSISTIVE TECHNO LOGIES

CAI's TDS 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 TDS. 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 TDS. 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 Chrome OS

devices for playback and stop but the pause feature is not available on these devices.
Consider testing students who need TTS on desktops or laptops running Windows or Mac or on iPads. All devices allow students with TTS to highlight a selection of text and have TTS read just that section. This eliminates the need for the pause feature.

For a full list of voice packs that have been tested and are allowed 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 TDS. Non-embedded features require devices to be set to permissive mode. Permissive mode, found in TIDE as a student accommodation, 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.

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 TDS. 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, or Chrome OS. For more information about STT, see the document titled *Assistive Technology Manual*.

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 the document titled *Assistive Technology Manual*.

Braille Embossers

Braille embossers are needed to access content with images in English/Language Arts (ELA) and Social Studies tests, as well as all content in Mathematics and Science tests. TDS allows students to emboss test material with TA approval. The software that sends print requests to the braille embosser must be installed on computers that TAs use for test sessions. For more information about configuring supported braille embossers, see the document titled *Assistive Technology Manual*.

Refreshable Braille Displays

Refreshable Braille Displays (RBDs) are used to read text-only content on ILEARN tests, while braille embossers are needed to read any content with images in ELA and Social Studies 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.

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 the document titled *Assistive Technology Manual*.

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 the document titled *Assistive Technology Manual*.

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 the document titled *Assistive Technology Manual*.

ADMINISTER ONLINE TESTS

Before administering an operational test, familiarize yourself with the system by administering a RIR test or practice test. RIR tests can be administered on supported devices via the Secure Browser or through a modern conventional browser. Practice test can be administered on supported devices via the secure browser

ADMINISTERING RELEASED ITEMS REPOSISTORY (RIR) TESTS

To administer a RIR test, complete the following steps:

1. TAs should open a web browser, go to the RIR TA Site, and select a RIR test to administer.
2. Students should launch the Secure Browser and click the link for RIR tests or go to the RIR URL and toggle off Guest Session.
3. TAs should give the students the Session ID.
4. Students can log in anonymously as a guest or with their first name and STN. In either case, they should use a Session ID from the TA.
5. Students should click through the login pages.

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

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

ADMINISTERING PRACTICE & OPERATIONAL TESTS

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

1. TAs should open a web browser, go to the TA Site, and select a practice test to administer.
2. Students should launch the Secure Browser.
3. TAs should give students the Session ID.
4. Students should enter their first name, STN, and their Session ID.
5. *I AM* practice tests are not separate from *I AM* operational tests. The *I AM* practice tests are part of the operational test, and will not be available until the *I AM* test window

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

Appendix. Change Log

Updates to this guide after July 19, 2019 are noted.

Section	Description of Change
STEP 2: Setting Up Student Workstations	Updated table of supported tablets and Chromebooks.
STEP 2: Setting Up Student Workstations	Added information on disabling keyboard shortcuts for screenshots on Mac OS.
STEP 2: Setting Up Student Workstations	Added official support for Chrome OS through v78
STEP 2: Setting Up Student Workstations	Added updated guidance on Mac Secure Profile
STEP 2: Setting Up Student Workstations	Updated table of supported OS
STEP 2: Setting Up Student Workstations	Added note for CloudReady and NeverWare support
STEP 2: Setting Up Student Workstations	Added guidance for disabling iOS 13 Voice features
STEP 2: Setting Up Student Workstations	Added official support for Chrome OS through v80
STEP 2: Setting Up Student Workstations	Added official support for Windows 10 desktop versions 1507-1909
Throughout	CAI replaced a reference to AIR within text, URLs, or email address.
Installing the Mac Secure Profile	Added Voice Control to the list of features disabled by the Secure Profile and added note describing updates to the Secure Profile for 2020-2021.
Installing the Secure Browser	Changed “Secure Test” to “SecureTestBrowser”
Setting up the Test Administrator Workstation	Changed all references of “whitelist” to “allowlist” or “add to your allowlist”

Throughout	Removed language referencing Android
Setting Up Student Workststations	Updated supporting OS versions for Windows, Mac, Linux, iOS/iPadOS, and Chrome OS. Removed Android
Setting Up Student Workststations	Apple rebranded AAC mode as Assessment Mode. Update throughout section.
Setting Up Student Workststations	Remove next section “Disabling Siri for Mac”
Setting Up Student Workststations	Remove next section “Disabling Keyboard Shortcuts for Mac”
Setting Up Student Workststations	Remove section “Enabling Secure Browser Keyboard for Android”
Setting Up Student Workststations	Updates throughout section to reflect this configuration is necessary for all supported versions of iOS/iPadOS and AAC mode rebranded to Assessment Mode.
Setting Up Student Workststations	Removed section “Screen Readers, Ebossers, and Visible Braille Displays
Setting Up Student Workststations	Added new section “Braille Embossers”
Setting Up Student Workststations	Added new section “Refreshable Braille Displays
Setting Up Student Workststations	Added new section “Alternative Computer Inputs
Setting Up Student Workststations	Added new section “Assistive Keyboard and Mouse Input”
Setting Up Student Workststations	Added new section “Screen Magnification”
Pgs. 3, 5	Updated iOS and Chrome OS support
Pgs. 3, 5	Added clarity for supported iOS and Chrome OS.
Pgs. 2, 4	Renamed Mac OS X 10.16 to 11 (Big Sur)