Quick Guide for Setting Up Your Online Testing Technology

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

- Test administrators use the Test Administrator 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 application.

This document explains in four 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 TEST ADMINISTRATOR WORKSTATION

It is unlikely that any setup is required for your test administrator workstations. Nearly any modern device, including mobile devices like tablets and phones, with any modern browser can be used to access the Test Administrator Interface and administer a testing session. The Test Administrator 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 campus uses a firewall or other networking equipment that blocks access to public websites, you may need to add AIR and CAI websites to your allowlist. For a list of websites you should add to your allowlist, see the "Resources to Add to Your Allowlist for Online Testing" section in the configuration guide for your operating system.

Test administrators can print test session information. To be able to print, test administrator 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 to install the CAI Secure Browser application. The Secure Browser application 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 application 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 application 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 application is not supported for use within a virtual machine.

For a list of supported desktops, laptops, tablets, Chromebooks, and related hardware requirements, refer to the Minimum Requirements document on the Texas Assessment Program.

Installing the Secure Browser Application

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

The Secure Browser application is available for all major operating systems listed in the Minimum Requirements document. You can download the Secure Browser application from the Secure Browsers page of Texas Assessment Program website. The Texas Assessment Program website 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 campus or district, you can likely use the same tools you are already familiar with to push the Secure Browser application out to all of your machines at scale. For example, the Secure Browser application ships as an MSI package which enables use of MSIEXEC.

If you are from a small campus, you can follow the basic installation instructions on the Texas Assessment Program website to install the Secure Browser application. The Secure Browser application 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 application. If you are familiar with installing software, install the Secure Browser application the same way.

If you are running the Secure Browser application 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 is not already installed, a prompt to install it will appear the first time you launch the Secure Browser application. Rosetta 2 can also be deployed to multiple devices at once through scripting or mobile device management. For more information about Rosetta 2, including installation instructions, please see https://support.apple.com/en-us/HT211861.

For iPads and Chromebooks, the SecureTestBrowser app is CAI's mobile version of the Secure Browser application. 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 application 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 application on multiple managed devices and configure those devices.

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

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

The following documents are also available for other devices and operating systems:

- *Configurations and Troubleshooting for Linux*
- *Configurations for iPads*
- *Assistive Technology Manual*

Other Configurations

For devices running Windows, macOS, Linux, iPadOS, or Chrome OS, there are a few additional configurations that need to be made before secure testing can begin.

Several necessary configurations for Mac workstations running macOS 10.13–10.15 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 macOS 11.4 and higher and all supported versions of iPadOS called Assessment Mode (AM) (formerly known as Automatic Assessment Configuration (AAC)) handles many necessary configurations to prepare Mac workstations and 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 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 all supported versions of Windows 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 application 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 *Configurations, Troubleshooting, and Advanced Secure Browser Application Installation for Windows*.

Disabling Screen Edge Swipe for Windows 10 & Windows 11 Touchscreen Devices

Swiping inward from the edge of the display on Windows 10 and Windows 11 touchscreen devices opens the Windows notification center. If this swiping gesture is not disabled and students taking a test in the Secure Browser on a Windows 10 or Windows 11 touchscreen device swipe from the edge of the screen during a test, the notification center will open, displaying any notifications that might appear there and pausing the test. This affects all Windows 10 and Windows 11 touchscreen devices.

The Screen Edge Swipe gesture can be disabled using the Local Group Policy Editor or Registry Editor. For instructions on how to disable the Screen Edge Swipe gesture, see the "How to Disable Screen Edge Swipe" section in the document titled *Configurations, Troubleshooting, and Advanced Secure Browser Installation for Windows*.

Disabling App Prelaunching 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 did not open the apps themselves. This does not affect users running the CAI Secure Browser application.

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

Installing the Mac Secure Profile

To configure Mac workstations running macOS 10.13–10.15, begin by downloading the Mac Secure Profile from your portal and then installing 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 sets function keys to standard functions for all users of the Mac to which it is deployed and disables Voice Control and the menu pop-up that appears when triple-tapping the power button on Touch Bar-enabled devices. It also prevents 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 be restarted immediately so that all settings can take effect. The Secure Profile was last 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 *Configurations, Troubleshooting, and Advanced Secure Browser Application 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 *Configurations, Troubleshooting, and Advanced Secure Browser Application Installation for Mac*.

Disabling Fast User Switching for Mac

Fast User Switching is a feature in macOS 10.13-10.15 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 application 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 *Configurations, Troubleshooting, and Advanced Secure Browser Application 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 application 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 *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 *Configurations and Troubleshooting for Linux*.

Disabling Voice Control for iPads

iPads running any supported version of iPadOS have access to a feature called Voice Control that is not automatically disabled by Assessment Mode (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 *Configurations for iPads*.

Disabling VoiceOver for iPads

iPads running any supported version of iPadOS have access to a feature called VoiceOver that is not automatically disabled by Assessment Mode (AM) (formerly known as Automatic Assessment Configuration [AAC]). 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 *Configurations for iPads*.

Disabling Emoji Keyboard for iPads

iPads running any supported version of 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 *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.

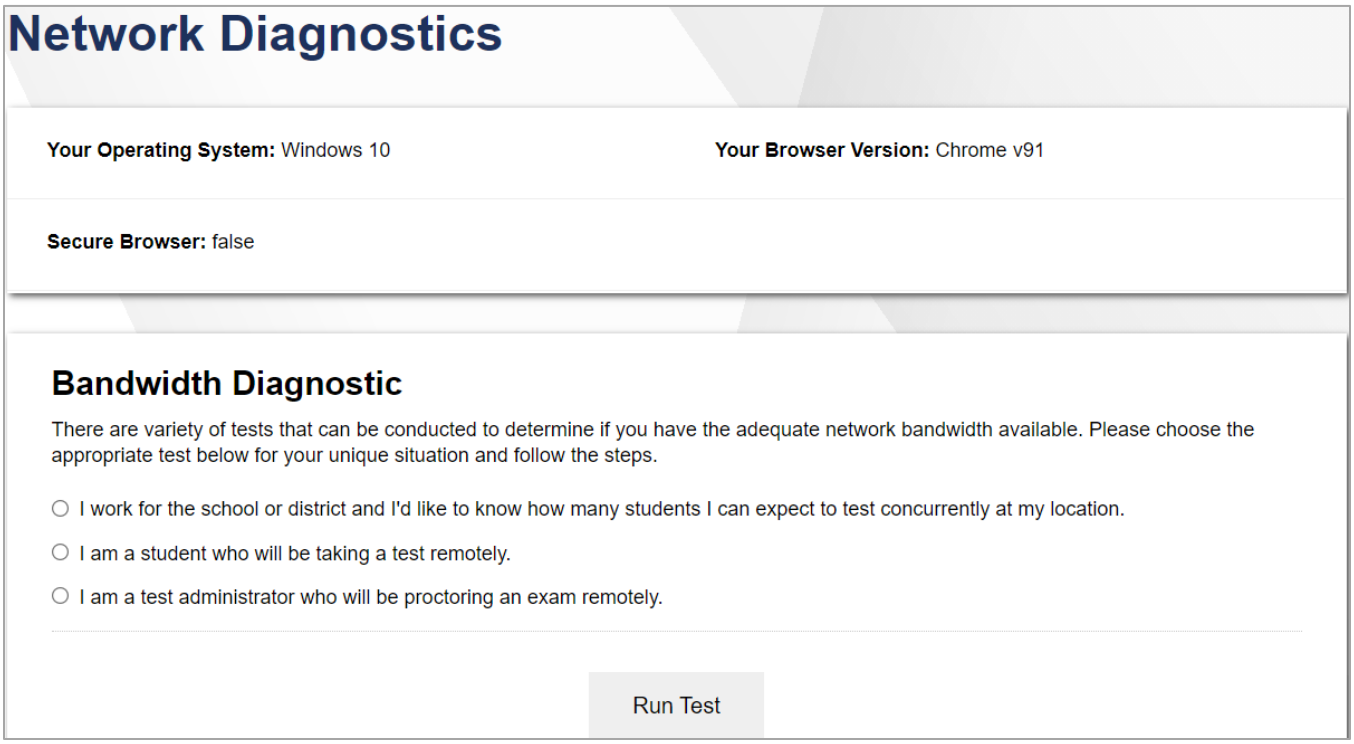
You can disable or limit Chrome OS updates through the Device Settings page on your Chromebook. From this page, you can stop auto-updates or allow auto-updates but only to a specific version. For more detailed instructions on how to disable or limit Chrome OS auto-updates, see the "How to Manage Chrome OS Auto-Updates" section in *Configurations, Troubleshooting, and Advanced Secure Browser Application 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 application or from your portal or practice test site through a conventional browser.



Once you are in the network diagnostic tool, choose the option that applies to you. Upon choosing the option, additional fields appear. Enter information as necessary and then run the test. 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 web sites during online testing.

Proxy Servers

If your Technology Coordinator has set up a proxy server at your campus, you may need to configure the Secure Browser application's proxy settings. For instructions on how to configure the Secure Browser application's proxy settings, see the "How to Configure the Secure Browser Application for Proxy Servers" section in the configuration guide for your operating system.

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, and 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 Your Allowlist for Online Testing" section in the configuration guide for your operating system.

STEP 4: CONFIGURING ASSISTIVE TECHNOLOGIES

CAI's Test Delivery System is a website that is accessed through the Secure Browser application.

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. For a list of supported technologies and configuration instructions, see the *Assistive Technology Manual*.

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

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. The following embedded features are available in the Test Delivery System:

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 iPadOS are fully compatible with the Secure Browser application. The Secure Browser application 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. The Linux Secure Browser application installation package contains English- and Spanish-language voice packs. For students who need TTS, CAI recommends using a desktop, laptop, or tablet running Windows, macOS, Linux, or 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 a full list of voice packs that have been tested and are allowed by the Secure Browser application and for instructions about configuring TTS settings, see the *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. The Test Delivery System offers an embedded STT solution. This embedded tool is supported on Windows, Mac, Linux, iPadOS, and Chrome OS. Third-party (non-embedded) STT solutions are also still supported, but the embedded tool should be used whenever possible. For more information about embedded STT, see the *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 settings be set to permissive mode. This mode, found in the Test Information Distribution Engine (TIDE) as a student test setting, temporarily lowers the security settings of the Secure Browser application 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. The following non-embedded features are available for devices running Windows or macOS:

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 *Assistive Technology Manual*.

Braille Embossers

Braille embossers are needed to access content with images in English language arts (ELA) and social sciences tests, as well as all content in mathematics and science tests. The Test Delivery

System allows students to emboss test material with test administrator approval. The software that sends print requests to the braille embosser must be installed on computers that test administrators use for test sessions. For more information about configuring supported braille embossers, see the *Assistive Technology Manual*.

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 set up 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. Though CAI recommends the embedded STT feature discussed above, STT is also 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 the *Assistive Technology Manual*.

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 Read&Write and other similar software. For more information about supported third-party apps, see the *Assistive Technology Manual*.

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 *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 the Test Delivery System 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 *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 *Assistive Technology Manual*.

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 application or through modern conventional browsers like Chrome or Firefox.

ADMINISTERING PRACTICE TESTS

To administer a practice test, complete the following steps:

1. Test administrators should open a web browser, go to the Test Administrator Practice Site, and choose a practice test to administer.
2. Students should launch the Secure Browser application and click the link for practice tests.
3. Test administrators 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 test administrator.

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

When test administrators 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. Test administrators should open a web browser and go to the Test Administrator Interface.
2. Students should launch the Secure Browser application.
3. Test administrators should give students the Session ID.
4. Students should enter the Session ID, their first name, and their Student ID.

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

Contact Texas Testing Support for any additional assistance.

CHANGE LOG

Location	Change	Date
Throughout	Cutover from 2020–2021.	6/23/21
Disabling Screen Edge Swipe for Windows 10 Touchscreen Devices	Updated topic heading and text to include all Windows 10 touchscreen devices.	10/14/21
Other Configurations	Updated macOS versions for Assessment Mode	12/13/21
Other Configurations	Updated macOS versions that use Assessment Mode to “11.4 and higher”	2/23/22
Disabling Fast User Switching for Mac	Updated macOS versions for which this configuration is necessary to “10.13-10.15”	2/23/22
Disabling Screen Edge Swipe	Added Windows 11.	4/18/22