Hawaiʻi Statewide Assessment Program

Quick Guide for Setting Up Your Online Testing Technology

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

- Test administrators 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 school:

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 TA workstations. Nearly any modern device, including mobile devices like tablets and phones, with any modern browser can be used to access the TA Live 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 CAI websites to your allowlist. For a list of websites you should add to your allow list, see the “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-request accommodation. To be able to print, TA 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 8.1 (Professional and Enterprise) 10, 10 in S Mode (Educational, Professional, and Enterprise) (Versions 1909-21H1, 21H2[a]) 11 (Version 21H2)[b] Server 2012 R2, 2016 R2 (thin client)	1 GHZ 64-bit Processor[c] 2 GB RAM 20 GB hard drive	1.4 GHZ 64-bit Processor 2 or more GB RAM 20 or more GB hard drive space
macOS[d] 10.13-10.15, 11.4-11.6, 12-12.3	1 GHZ 64-bit Processor[e] 2 GB RAM 20 GB hard drive	1.4 GHZ 64-bit Processor 2 or more GB RAM 20 or more GB hard drive space
Linux[f] Fedora 32-33[a] LTS (Gnome) Ubuntu 18.04, 20.04 LTS (Gnome)	1 GHZ 64-bit Processor 2 GB RAM 20 GB hard drive Required libraries/packages: • GTK+ 3.14 or higher • X.Org 1.0 or higher (1.7+ recommended) • libstdc++ 4.8.1 or higher • glibc 2.17 or higher	1.4 GHZ 64-bit 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 • GNOME 2.16 or higher • PulseAudio

a. Support for this version is anticipated upon the completion of testing following its release.
b. Known Issue in Windows 11: The network diagnostic tool identifies Windows 11 as Windows 10.
c. 64-bit Intel, AMD, and ARM devices are supported. ARM devices require x64 emulation.
d. Students who need access to permissive mode tools must use macOS 10.13-10.15.
e. 64-bit Intel and Apple silicon devices are supported. Apple silicon devices require Rosetta 2.
f. 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:

Tablets & Chromebooks	
Supported Operating Systems	**Supported Devices**
iPadOS • 13.7 • 14.5 – 14.8 • 15.1 – 15.4	All 9.7” or larger iPads running a supported version of iPadOS.
Windows • 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[a] • 91+	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 and be attached to a management domain. The devices are required to be attached to the management console to run in kiosk mode, which is required to run the Secure Browser for testing. 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 Known Issues in Supported Versions of Chrome OS:

- Sometimes, text-to-speech (TTS) does not work properly the first time it is invoked. Users who encounter this issue should reinvoke TTS. This issue exists in Chrome OS 91 and 92.
- Students testing on the Secure Browser on Chromebooks can restore or minimize the Secure Browser while the Chromebook is in kiosk mode. Because kiosk mode blocks access to all other applications on the device, this issue is noncritical and poses no security concerns. When the user returns to the Secure Browser, they are taken back to the login page. This issue exists in Chrome OS 91 and 92.
- Students testing on Chromebooks with touchscreens can access the Chrome OS context menu while taking a test. This presents no security concerns with the test being taken. This issue exists in Chrome OS 91, 92, and 93.
- A lag or delay in text-to-speech causes audio to lose sync with text the student is focused on. This issue exists in Chrome OS 94-99.

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[a]	vSpace PRO 10	L300, L350, firmware version 1.13.xx
Windows 11[a]	vSpace PRO 12	L350, firmware version 1.13.xx

a. USB redirect does not work in Windows 10 or Windows 11.

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

<table>
<tr><th colspan="2">Terminal Servers</th></tr>
<tr><th>Supported Terminal Server</th><th>Supported Thin Client</th></tr>
<tr><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>
</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:

Testing Device	Requirement
Screen Dimensions	Screen dimensions must be 10” or larger (iPads with a 9.7” display are included).
Monitors & Displays	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	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.
Headphones & Headsets	Wired headphones or headsets with a 3.5 mm or USB connector. While Bluetooth devices are supported, their use is discouraged due to issues with pairing multiple devices in the same lab.

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 the HSAP portal at https://alohahsap.org by clicking on the “Secure Browsers” page. The HSAP 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, complex, or complex area, you can likely use the same tools you are already familiar with to push the Secure Browser out to all of your machines at scale. For example, the Secure Browser ships as a MSI package which enables use of MSIEXEC.

If you are from a small school, you can follow the basic installation instructions on the AlohaHSAP.org 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 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, complexes, or complex areas 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, MacOS, Linux, iPadOS, Chrome OS, there are a few additional configurations before secure testing can begin.

Several necessary configurations for Mac workstations running macOS 10.13-10.15 can be performed by installing the optional Mac Secure Profile. For more information, see the section titled “Installing the Mac Secure Profile” below.

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 see this page from Apple Support. 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 it during a test, the Secure Browser will pause the test. If you plan to use the Take a Test app on a dedicated test account on a Windows 10 device, do not disable fast user switching, as it causes the machine to enter an infinite loop when rebooted.

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 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 and 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 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 Take a Test app 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 Take a Test app. 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

NOTE: The Mac Secure Profile is **optional** and once installed will affect all profiles on the device. CAI recommends that schools only install the Mac Secure Profile on devices that are solely used for testing. Before you install the Secure Profile, you should back up your device profile’s preferences and settings. Once the device is no longer used for testing, the Secure Profile can be removed, and your original settings can be manually reapplied.

To configure Mac workstations running macOS 10.13-10.15 more efficiently, begin by downloading the optional Mac Secure Profile from the 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 should 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 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.

If the optional Mac Secure Profile is not used, 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 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 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 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 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.

If the optional Mac Secure Profile is not used, Siri must 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 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.

If the optional Mac Secure Profile is not used, keyboard shortcuts for screenshots must 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 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 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 iOS/iPadOS*.

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 the document titled *Configurations for iOS/iPadOS*.

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.

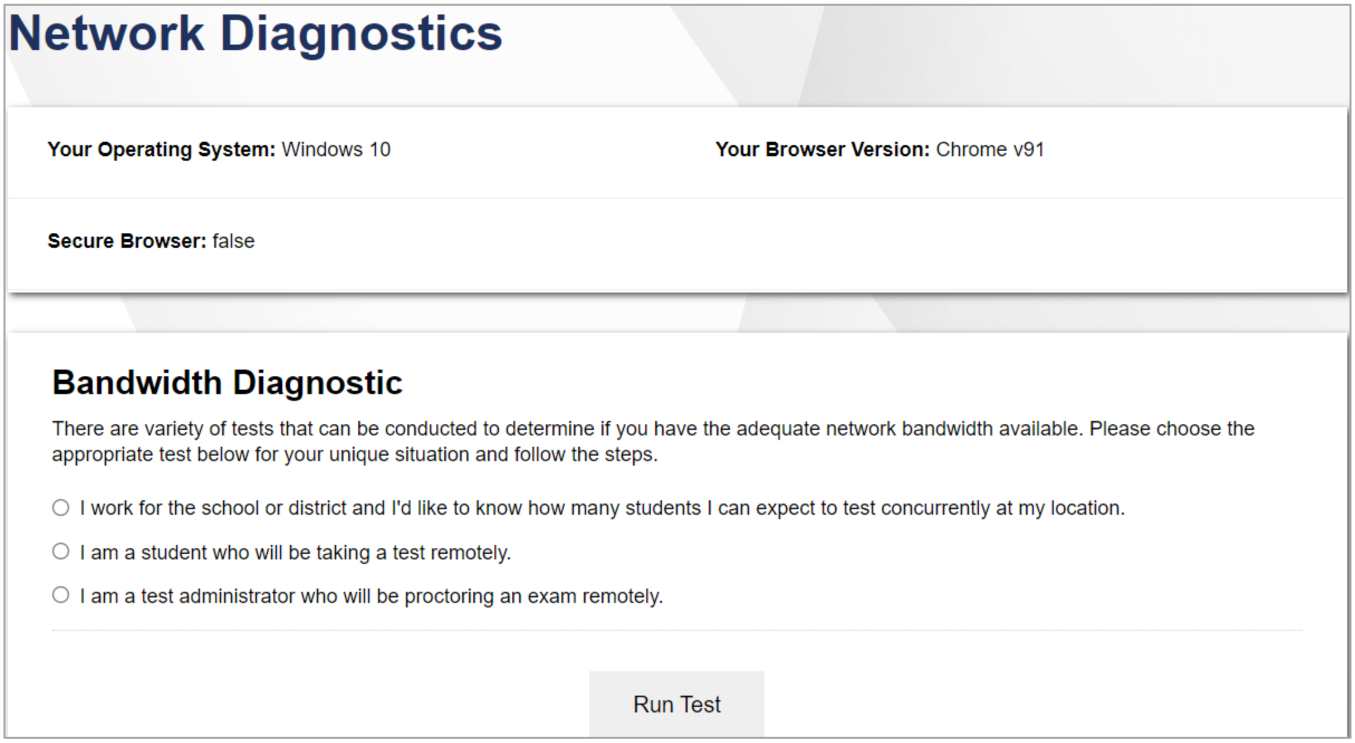
You can disable or limit Chrome OS updates through the Device Settings page on your Chromebook. From this page, you can stop auto-updates or allow auto-updates but only to a specific version. For more detailed instructions on how to disable or limit Chrome OS auto-updates, see the “How to Manage Chrome 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 by clicking on Run Diagnostics on the student login page.



Network Diagnostics

Your Operating System: Windows 10

Your Browser Version: Chrome v91

Secure Browser: false

Bandwidth Diagnostic

There are variety of tests that can be conducted to determine if you have the adequate network bandwidth available. Please choose the appropriate test below for your unique situation and follow the steps.

○ I work for the school or district and I'd like to know how many students I can expect to test concurrently at my location.

○ I am a student who will be taking a test remotely.

○ I am a test administrator who will be proctoring an exam remotely.

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 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 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 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*.

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 HSAP Help Desk or see the document titled *Assistive Technology Manual*, available on the HSAP portal resources page, for more information. 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 in TIDE. They can be accessed without additional third-party software. Students may need an accommodation to access certain embedded features. Please see the *TIDE User Guide*, available on the HSAP portal resources page, for more information.

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. The Secure Browser recognizes voice packs that ship out of the box Chrome OS devices for playback and stop but the pause feature does not work properly on these devices. The Linux Secure Browser installation package contains English- and Spanish-language voice packs. For students who need the use of 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 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. 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. 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 ELA and Social Sciences tests, as well as all content in Mathematics and Science tests. The Test Delivery System (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 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. The Test Delivery System (TDS) now offers an embedded Speech-to-Text (STT) solution. This embedded tool is supported on Windows, Mac, Linux, iPadOS, and Chrome OS. Though CAI recommends the embedded STT feature discussed above, third-party (non-embedded) STT solutions are also still supported and 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. For more information about embedded and third-party STT, see the document titled *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 Co:Writer, Read&Write, and many others. For more information about supported third-party apps, see the document titled *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 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 a summative test, get comfortable with the system by administering a training or practice test. Training and practice tests can be administered on supported devices via the Secure Browser or through modern conventional browsers like Chrome or Firefox.

ADMINISTERING TRAINING AND PRACTICE TESTS

To administer a training or practice test, complete the following steps:

1. TAs should open a web browser, go to the TA Training Site, and choose a training or practice test to administer.
2. Students should launch the Secure Browser and click the link for practice tests.
3. TAs 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 TA.

For more information about administering practice tests, see the *Guide to Administering the Online HSAP Assessments*, available on the HSAP portal resources page.

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

ADMINISTERING SUMMATIVE TESTS

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

1. TAs should open a web browser and go to the TA Live Site.
2. Students should launch the Secure Browser.
3. TAs 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 *Guide to Administering the Online HSAP Assessments*, available on the HSAP portal resources page.

CHANGE LOG

Location	Change	Date
Table of Supported Desktops and Laptops	Added Windows 11 with footnote stating support is anticipated upon completion of testing following release. Added support for macOS 11.5 and 11.6.	11/8/21
Testing Devices Table	Updated requirements for Headphones & Headsets to include note about Bluetooth devices.	11/8/21
Table of Supported Tablets and Chromebooks	Added support for iPadOS 14.6, 14.7, and 14.8. Updated footnote explaining all known issues in supported versions of Chrome OS.	11/8/21
Table of Supported Tablets and Chromebooks	Added support for iPadOS 15.1.	12/28/21
Other Configurations	Updated macOS versions for Assessment Mode.	12/28/21
Table of Supported Tablets and Chromebooks	Updated footnote explaining known issues in Chrome OS 96.	1/11/22
Table of Supported Tablets and Chromebooks	Added support for iPadOS 15.2. Updated note about Chromebooks manufactured in 2017 or later.	2/3/22
Desktops & Laptops Support Table	Added macOS 12-12.2. Added footnote about permissive mode access to macOS. Reordered footnotes throughout table.	2/24/22
Other Configurations	Updated macOS versions that use Assessment Mode to “11.4 and higher.”	2/24/22
Disabling Fast User Switching for Mac	Updated macOS versions for which this configuration is necessary to “10.13-10.15.”	2/24/22

Disabling Screen Edge Swipe for Windows 10 Touchscreen Devices	Updated topic heading and text to include all Windows 10 touchscreen devices.	2/24/22
Table of Supported Desktops and Laptops	Added support for Windows 10 21H1. Added anticipated support for Windows 10 21H2 pending the completion of internal testing.	3/3/22
Table of Supported Tablets and Chromebooks	Added support for iPadOS 15.3.	3/3/22
Table of Supported Tablets and Chromebooks	Added Chrome OS 97 & 98 to the last bullet in the table footnote explaining known issues in Chrome OS.	3/24/22
Table of Supported Desktops and Laptops	Added support for macOS 12.3.	4/4/22
Table of Supported Tablets and Chromebooks	Added Chrome OS 99 to the last bullet in the table footnote explaining known issues in Chrome OS.	4/4/22
Table of Supported Tablets and Chromebooks	Added support for iPadOS 15.4.	4/18/22
Table of Supported Desktops and Laptops	Added support for Windows 11 with new footnote, and reordered footnotes.	4/18/22
NComputing Support Table	Added support for Windows 11 with footnote. Added same footnote to Windows 10.	4/18/22
Disabling Screen Edge Swipe	Added Windows 11.	4/18/22