

TECHNOLOGY SETUP FOR ONLINE TESTING

Cambium Assessment, Inc.'s (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 a web browser.
- Students access and complete their tests through the Student Interface via the Secure Browser.

This document explains in 4 steps how to set up technology in your schools and district:

Step 1. Setting Up the Test Administrator Computer/Device

Step 2. Setting Up Student Computers/Devices

Step 3. Configuring Your Network for Online Testing

Step 4. Configuring Assistive Technologies

STEP 1: SETTING UP THE TEST ADMINISTRATOR COMPUTER/DEVICE

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 Interface and administer a testing session. The TA Interface is a website that can be accessed through any approved and updated browser listed on the [**Supported Systems & Requirements**](#) page to administer a testing session.

If your school uses a firewall or other networking equipment that blocks access to public websites, you will need to add CAI websites to your Allowlist. For a list of websites you should add to your Allowlist, see the [!\[\]\(d3102649f02e825ddb76dc3de0190154_img.jpg\) **Configuring Network Settings for Online Testing**](#) section below.

TAs that wish to print test session information must be connected to a printer.

STEP 2: SETTING UP STUDENT COMPUTERS/DEVICES

For students to access online tests, each student computer/device needs CAI's Secure Browser installed. 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 computers/devices, you should first make sure they meet minimum hardware requirements and supported operating systems as listed on the [**Supported Systems & Requirements**](#) page. Since some Operating Systems are updated more frequently, such as Chrome and iPadOS, please be sure to check this page for the most recent supported operating systems. Please note the secure browser is not supported for use with virtual machines.

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

Screen Dimensions



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

Screen Resolution



All devices must meet the minimum resolution 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. On-screen keyboards take screen real estate away from the test and may make typing responses more difficult.

- 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 on mobile devices are not supported. Mice with "browser back" buttons should not be used.

Headphones



Wired headphones with a 3.5mm or a USB connector are supported. Bluetooth headphones are not permitted.

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 the operating systems listed on the [Supported Systems & Requirements](#) page. You can download the secure browser and find installation instructions from the [Secure Browsers](#) page on the Florida Statewide Assessments Portal.

If you are a Technology Coordinator and it is your responsibility to manage a large number of machines across your school or district, you can use the same tools you are already familiar with to push the secure browser out to all of your machines at scale. For example, the secure browser ships as an MSI package which enables use of MSIXEC.

If you are managing a small number of devices, you can follow the basic installation instructions on the portal to install the Secure Browser. The secure browser is installed the same way as most other software. You will need to download a file, open that file, and follow prompts to install the secure browser. Follow the process your team is most familiar with to install the secure browser.

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 CAI's Secure Browser on the testing machine. Instructions for configuring the Take a Test app can be found in the [Configurations, Troubleshooting, and Secure Browser Installation for Windows](#) document.

Additional installation instructions for Windows, macOS, iPadOS, Chrome OS, or Linux (including instructions on how to install the secure browser on multiple devices) can be found in the following documents on the **Secure Browsers** page tabs:

- [Configurations, Troubleshooting, and Secure Browser Installation for Windows](#)
- [Configurations, Troubleshooting, and Secure Browser Installation for macOS and iPad OS](#)
- [Configurations, Troubleshooting, and Secure Browser Installation for Linux](#)
- [Configurations, Troubleshooting, and Secure Browser Installation for Chrome OS](#)

Other Configurations

For all devices and operating systems, there are additional configurations necessary before secure testing can begin. Please refer to each individual installation guide located on the OS specific tab on [Secure Browsers](#) page.

Several necessary configurations for macOS computers/devices running macOS 10.13-10.15 are performed by installing the macOS Secure Profile.

STEP 3: CONFIGURING YOUR NETWORK FOR ONLINE DEVICES

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.

Proper configuration of your network for online testing is an important step in test preparation. When not configured correctly, students may be unable to access the secure browser.

Additionally, FDOE suggests that a guest WiFi network used for personal devices should be set up separately from the primary school WiFi network to ensure that bandwidth strength is optimal.

Adding URLs to your Allowlist, Configuring Filtering Systems, and Configuring Domain Name Resolution

Ensure your network's firewalls are open for the URLs in the table below. If your testing network includes devices that perform traffic shaping, packet prioritization, or Quality of Service, ensure these URLs have high priority. **Please note the addition of Cambium Assessment URLs.**

If both internal and external filtering systems are used, the URLs must be added to the Allowlist in both filters. Ensure your filtering system is not configured to perform packet inspection on traffic to CAI servers. Please see your vendor's documentation for specific instructions. Also, be sure to add to your Allowlist these URLs in any multilayer filtering system (such as local and global layers) and from content inspection. Ensure all items that handle traffic to *.tds.airast.org and *.tds.cambiumast.com, including proxy servers, have the entire certificate chain and are using the latest TLS 1.2 protocol.

Additionally, ensure the devices used for testing have access to a server that can resolve the below domain names.

CAI testing servers and satellites may be added or modified during the school year to ensure an optimal testing experience. As a result, you are required to add to your Allowlist at the root level. This requires using a wildcard. Moreover, it will be important to add to your Allowlist **all** the URLs listed below. CAI strongly encourages using wildcards when adding these URLs to your Allowlist, as servers may be added or removed from the field without notice.

CAI URLs for Testing Sites	
System	URLs
TA and Student Testing Sites	*.airast.org
Assessment Viewing Application (AVA)	*.tds.airast.org *.cloud1.tds.airast.org *.cloud2.tds.airast.org
For 2021-2022, users should continue to add both Cambium and AIR URLs listed in this table to their allowlist.	*.cambiumast.com *.tds.cambiumast.com .cloud1.tds.cambiumast.com .cloud2.tds.cambiumast.com .cambiumtds.com

CAI URLs for Non-Testing Sites

System	URL
Florida Portal and Secure Browser Installation Files	FSAssessments.org
Single Sign-On System	sso2.airast.org/auth/realms/florida/account sso2.cambiumast.com/auth/realms/florida/account
Practice Tests	flpt.tds.airast.org/student flpt.tds.cambiumast.com/student
Test Information Distribution Engine	fl.tide.airast.org fl.tide.cambiumast.com
PearsonAccess Next (PAN) Reporting System	fl.pearsonaccessnext.com/customer/index.action

Required Ports and Protocols

Ensure that all content filters, firewalls, and proxy servers are opened accordingly.

Ports and Protocols for the Test Delivery System

Port/Protocol	Purpose
80/TCP	HTTP (initial connection only)
443/TCP	HTTPS (secure connection)

Configuring Network Settings for Online Testing

Local Area Network (LAN) settings on testing machines should be set to automatically detect network settings.

To set LAN settings to auto-detect on Windows machines:

1. Open **Control Panel**.
2. Open **Internet Options**.
3. Click **Connections** tab.
4. Click **LAN Settings**.
5. Click the **Automatically detect settings** checkbox.
6. Click **OK** to close **Local Area Network (LAN) Settings** window.
7. Click **OK** to close **Internet Properties** window.

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. 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. Ensure all items that handle traffic to *.tds.airast.org and *.tds.cambiumast.com, including proxy servers, have the entire certificate chain and are using the latest TLS 1.2 protocol.

By default, the secure browser attempts to detect the settings for your network's web proxy server. However, users of web proxies should execute a proxy command once from the command prompt. This command does not need to be added to the secure browser shortcut. The table below lists the form of the command for different settings and operating systems. To execute these commands from the command line, change to the directory containing the secure browser's executable file.

Note the commands in the table on the next page use the domains foo.com and proxy.com. When configuring for a proxy server, use the actual testing domain names as listed in the above table [CAI URLs for Testing Sites](#).

Specifying Proxy Settings Using the Command Line		
Description	System	Command
Use the browser without any proxy	Windows	FLSecureBrowser.exe -proxy 0 aHR0cHM6Ly9mbC50ZHMuY2FtYml1bWFzdC5jb20vc3R1ZGVudA==
	macOS	./FLSecureBrowser -proxy 0 aHR0cHM6Ly9mbC50ZHMuY2FtYml1bWFzdC5jb20vc3R1ZGVudA==
	Linux	./FLSecureBrowser.sh -proxy 0 aHR0cHM6Ly9mbC50ZHMuY2FtYml1bWFzdC5jb20vc3R1ZGVudA==
Set the proxy for HTTP requests only	Windows	FLSecureBrowser.exe -proxy 1:http:foo.com:80 aHR0cHM6Ly9mbC50ZHMuY2FtYml1bWFzdC5jb20vc3R1ZGVudA==
	macOS	./FLSecureBrowser -proxy 1:http:foo.com:80 aHR0cHM6Ly9mbC50ZHMuY2FtYml1bWFzdC5jb20vc3R1ZGVudA==
	Linux	./FLSecureBrowser.sh -proxy 1:http:foo.com:80 aHR0cHM6Ly9mbC50ZHMuY2FtYml1bWFzdC5jb20vc3R1ZGVudA==
Set the proxy for all protocols to mimic the “Use this proxy server for all protocols” of Firefox	Windows	FLSecureBrowser.exe -proxy 1:/*:foo.com:80 aHR0cHM6Ly9mbC50ZHMuY2FtYml1bWFzdC5jb20vc3R1ZGVudA==
	macOS	./FLSecureBrowser -proxy 1:/*:foo.com:80 aHR0cHM6Ly9mbC50ZHMuY2FtYml1bWFzdC5jb20vc3R1ZGVudA==
	Linux	./FLSecureBrowser.sh -proxy 1:/*:foo.com:80 aHR0cHM6Ly9mbC50ZHMuY2FtYml1bWFzdC5jb20vc3R1ZGVudA==
Specify the URL of the PAC file	Windows	FLSecureBrowser.exe -proxy 2:proxy.com aHR0cHM6Ly9mbC50ZHMuY2FtYml1bWFzdC5jb20vc3R1ZGVudA==
	macOS	./FLSecureBrowser -proxy 2:proxy.com

		aHR0cHM6Ly9mbC50ZHMuY2FtYml1bWFzdC5jb20vc3R1ZGVudA==
	Linux	./FLSecureBrowser.sh -proxy 2:proxy.com aHR0cHM6Ly9mbC50ZHMuY2FtYml1bWFzdC5jb20vc3R1ZGVudA==
Auto-detect proxy settings	Windows	FLSecureBrowser.exe -proxy 4 aHR0cHM6Ly9mbC50ZHMuY2FtYml1bWFzdC5jb20vc3R1ZGVudA==
	macOS	./FLSecureBrowser -proxy 4 aHR0cHM6Ly9mbC50ZHMuY2FtYml1bWFzdC5jb20vc3R1ZGVudA==
	Linux	./FLSecureBrowser.sh -proxy 4 aHR0cHM6Ly9mbC50ZHMuY2FtYml1bWFzdC5jb20vc3R1ZGVudA==
Use the system proxy setting (default)	Windows	FLSecureBrowser.exe -proxy 5 aHR0cHM6Ly9mbC50ZHMuY2FtYml1bWFzdC5jb20vc3R1ZGVudA==
	macOS	./FLSecureBrowser -proxy 5 aHR0cHM6Ly9mbC50ZHMuY2FtYml1bWFzdC5jb20vc3R1ZGVudA==
	Linux	./FLSecureBrowser.sh -proxy 5 aHR0cHM6Ly9mbC50ZHMuY2FtYml1bWFzdC5jb20vc3R1ZGVudA==

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 web browser.

Network Diagnostics

Your Operating System: Windows 10

Your Browser Version: Chrome v94

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.

Run Test

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](https://www.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 devices attempting to take the test. If it is, try to prioritize bandwidth for CAI's websites during online testing.

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 Florida Help Desk or see the "Troubleshooting Text-to-Speech" section in the document titled *Configurations, Troubleshooting, and Secure Browser Installation* for your operating system for more information.

Supported Embedded Features

Embedded features work directly within the Test Delivery System. 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, macOS, and iPadOS 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, however, the pause feature does not work properly on these devices. The Linux Secure Browser installation package contains English- and Spanish-language voice packs. Consider testing students who need TTS on desktops or laptops running Windows, macOS, Linux, or iPadOS. A workaround for Chrome OS is

available. It allows students to highlight a passage of text and have TTS read just that passage, eliminating the need for the pause feature.

For a full list of voice packs that have been tested and are allowed by the secure browser, and for instructions for configuring TTS settings for Windows or OS X/macOS, see the "Troubleshooting Text-to-Speech" section in the document titled *Configurations, Troubleshooting, and Secure Browser Installation* for your operating system.

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. 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 document titled [*Test Administrator User Guide*](#).

HELP DESK AND USER SUPPORT

If this document does not answer your questions, please contact the Florida Help Desk. The Help Desk is open **Monday–Friday from 7:00 a.m. to 8:30 p.m. Eastern Time** (except holidays or as otherwise indicated on the Florida Statewide Assessments Portal).

Toll-Free Phone Support: 1-866-815-7246

Email Support: FloridaHelpDesk@CambiumAssessment.com

In order to help us effectively assist you with your issue or question, please be ready to provide the Florida Help Desk with detailed information that may include the following:

- Device, operating system, and browser version information
- Any error messages and codes that appeared, if applicable
- Information about your network configuration:
 - Secure browser installation (to individual machines or network)
 - Wired or wireless Internet network setup

CHANGE LOG

Location	Change	Date
Throughout Guide	Removed references to iOS and OS X.	9/2/21
<u>The Network Diagnostic Tool</u>	Updated instructions with new tool information.	9/2/21
<u>Supported Embedded Features</u>	Added Speech-to-Text feature.	9/2/21

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