



2020–21 TEST ADMINISTRATION

CAASPP and ELPAC Technical Specifications and Configuration Guide for Online Testing



California Assessment of
Student Performance and Progress



- ☀ **CAASPP Summative and Interim Assessments**
- ☀ **ELPAC Summative and Initial Assessments**
- ☀ **Alternate ELPAC Operational Field Test**
- ☀ **Test Administrator Sites**
- ☀ **Student Practice and Training Tests**
- ☀ **Test Operations Management System**
- ☀ **Online Reporting System**



2020–21 CAASPP and ELPAC Technical Specifications and Configuration Guide for Online Testing

Table of Contents

Introduction	1
Manual Content.....	2
What's New in 2020–21	2
General.....	2
Assessments	2
General Configuration.....	2
Apple and Macintosh Configuration	2
Secure Browser	3
Operating Systems for Student Testing	4
Internet Browser Requirements	5
Sections	5
Document Conventions.....	6
Intended Audience	7
Chapter 1: System Requirements	9
Supported Operating Systems for Student Testing	10
Desktops and Laptops	11
Tablets	14
Chromebooks and Chromebases.....	14
Thin Clients: NComputing and Terminal Servers for Windows	15
NComputing.....	15
Terminal Servers.....	16
Supported Web Browsers for Online Systems Associated with Testing.....	17
Supported Web Browsers by Operating System	17
Available Audio Settings by Web Browser	22
Requirements for Peripheral Equipment	23
Monitors and Screen Display Requirements.....	23
Screen Dimensions.....	23
Screen Resolution.....	23
Keyboards.....	24
External Keyboards.....	24
Mice	24
Headsets and Headphones.....	24
Speakers.....	25
Microphones	26
Chapter 2: Network Configuration	27
Network Configuration and Testing	28
Network Configuration.....	28
Guidance for Determining Required Bandwidth.....	28
Required Ports and Protocols	30
Allowlisting Test Site Resource URLs for Online Testing.....	30

Configuring Domain Name Resolution.....	30
Configuring Session Timeouts.....	30
Data Caching.....	30
Configuring Quality of Service and Traffic Shaping.....	30
Network Diagnostic Tools.....	31
The Bandwidth Diagnostic Tool.....	31
Windows-Specific Tools.....	34
MacOS–Specific Tools.....	34
Multiplatform Tools.....	35
Chapter 3: System Configuration.....	37
Hardware Configuration.....	38
Connections Between Printers and Testing Devices.....	38
Wireless Networking and Determining the Number of Wireless Access Points (WAPs).....	38
Hardware for Braille Testing.....	39
Software Configuration.....	40
Optimal Installation Scenario for Secure Browsers.....	40
Configuring Commercially Available Web Browsers.....	41
Enabling Pop-Up Windows.....	41
Preventing Auto Update on Device Operating Systems Used for Test Operations.....	42
Keyboard Navigation on the <i>Tool</i> Menu Using a Safari Browser.....	43
Configuring Devices for Online Testing with the Secure Browser.....	44
Windows Testing Device Configuration.....	44
MacOS Testing Device Configuration.....	61
Linux Testing Device Configuration.....	68
iOS or iPadOS Testing Device Configuration.....	69
Chromebook Mobile Testing Device Configuration.....	72
Configuring Network Settings for Online Testing.....	73
Windows Devices.....	73
MacOS Devices.....	73
Linux Devices.....	74
Installing CloudReady on PCs and Macs.....	74
Configurations for Testing Students Using Accessibility Resources.....	76
Chapter 4: Secure Browser Configuration.....	77
Overview of Secure Browsers.....	78
About the Secure Browser.....	78
Close External User Applications.....	79
Turn Off Background Jobs.....	79
Testing on Computers with Dual Monitors.....	80
Secure Browser Versions for Online Testing.....	81
Forbidden Application Detection.....	82
Installing the Secure Browser on Desktops and Laptops.....	83
Installing the Secure Browser on Windows.....	83
Installing the Secure Browser on an Individual Computer.....	83
Copying the Secure Browser Installation Directory to Testing Computers.....	87
Installing the Secure Browser for Use with an NComputing Terminal.....	88
Installing the Secure Browser on a Terminal Server or Windows Server.....	89
Installing the Secure Browser Without Administrator Rights.....	90
About Sharing the Secure Browser Over a Network.....	90

Uninstalling the Secure Browser on Windows	90
Secure Browser for Windows and the Microsoft Take a Test App	91
Installing the Secure Browser on macOS.....	93
Installing the Secure Browser on an Individual Apple Computer	93
Cloning the Secure Browser Installation to Other Macs.....	96
Uninstalling the Secure Browser on OS X and macOS.....	97
Installing the Secure Browser on Linux.....	97
Installing the Secure Browser on 32-Bit Versions of Linux.....	97
Installing the Secure Browser on 64-Bit Versions of Linux.....	99
Extracting the Secure Browser TAR File.....	100
Creating a Shortcut to Secure Browser 12.5.....	101
Uninstalling the Secure Browser on Linux	101
Installing the Secure Browser on Mobile Devices.....	102
Installing the Chrome OS SecureTestBrowser Kiosk App.....	102
Installing the SecureTestBrowser App on Stand-Alone Chromebooks	102
Installing the SecureTestBrowser Kiosk App on Managed Chromebooks	107
Opening the SecureTestBrowser Kiosk App and Selecting the Assessment Program	113
Installing the Secure Browser on iOS or iPadOS	115
Instructions for Installation	115
Guidance on iOS or iPadOS Classroom and Summative Testing	118
Installing the Secure Browser on Windows Mobile Devices.....	119
Proxy Settings for Desktop Secure Browsers.....	120
Specifying a Proxy Server to Use with the Secure Browser.....	120
Modifying Desktop Shortcuts to Include Proxy Settings.....	122
Modifying Desktop Shortcuts on Microsoft Windows	122
Modifying Desktop Shortcuts on macOS	123
Appendices	125
Appendix A: Operating System Support Plan for the 2020–21 Test Delivery System.....	126
Timing of Secure Browser Updates.....	126
Support Plan for Operating Systems.....	127
Windows	127
Mac.....	128
Linux	129
Apple Mobile	129
Chrome	130
Appendix B: URLs for Testing Systems	131
URLs for Nontesting Sites.....	131
URLs for Testing Sites	132
Test Administrator, Test Examiner, and Student Testing Websites	132
Online Dictionary and Thesaurus.....	133
Appendix C: Technology Coordinator Checklist.....	134
Appendix D: Scheduling Online Testing	137
Number of Devices and Hours Required to Complete Online Tests	137
Sample Test Scheduling Worksheet	137
Appendix E: Creating Group Policy Objects to Assign Logon Scripts in Microsoft Windows	138
Appendix F: Resetting Secure Browser Profiles.....	140

Resetting Secure Browser Profiles on Windows	140
Resetting Secure Browser Profiles on macOS.....	140
Resetting Secure Browser Profiles on Linux.....	142
Appendix G: User Support	143
CalTAC for LEA CAASPP and ELPAC Coordinators.....	143
Appendix H: Change Log	144

List of Tables

Table 1. Key Symbols and Document Conventions.....	6
Table 2. Supported Desktop Operating Systems.....	11
Table 3. Supported Tablets and Operating Systems.....	14
Table 4. Supported Chromebooks.....	15
Table 5. Supported NComputing Solutions	15
Table 6. Supported Terminal Servers.....	16
Table 7. Supported Web Browsers by Test Administration Websites.....	18
Table 8. Available Audio Settings by Browser	22
Table 9. Supported Headphones and Headsets.....	25
Table 10. Average Bandwidth Used by Secure Browser for Testing	29
Table 11. Ports and Protocols for the TDS.....	30
Table 12. Recommended Ratios of Devices to Wireless Access Points	39
Table 13. Secure Browsers by Operating System.....	81
Table 14. Specifying Proxy Settings Using a Shortcut or the Command Line	120
Table 15. Supported Operating Systems—Windows.....	127
Table 16. Supported Operating Systems—OS X and macOS (Intel).....	128
Table 17. Supported Operating Systems—Linux.....	129
Table 18. Supported Operating Systems—iOS or iPadOS.....	129
Table 19. Supported Operating Systems—Chrome OS	130
Table 20. URLs for Nontesting Websites.....	132
Table 21. URLs for Testing Websites.....	133
Table 22. URLs for Online Dictionary and Thesaurus	133

List of Figures

Figure 1. Sign-in web page for the training test	32
Figure 2. Run the diagnostics test	33
Figure 3. Safari Advanced preferences	43
Figure 4. <i>Local Group Policy Editor</i> window	45
Figure 5. <i>Windows Components</i> panel.....	46
Figure 6. Input Panel in the Local Group Policy Editor	47
Figure 7. Disable text prediction screen	48
Figure 8. Surface Pro 3 <i>Settings</i> interface.....	49
Figure 9. <i>Touch keyboard</i> settings interface.....	50
Figure 10. <i>Mouse Properties</i> dialog box.....	51
Figure 11. <i>Properties for Synaptics TouchPad V7.5 on PS/2 Port</i> dialog box	52
Figure 12. Control Panel <i>Sound</i> interface.....	53
Figure 13. Windows 8.0 and 8.1 Search charm.....	54
Figure 14. Windows 8.0 and 8.1 Local Group Policy Editor options	54
Figure 15. Windows 8.0 and 8.1 Local Group Policy Editor selection.....	55

Figure 16. Windows 8.0 and 8.1 <i>Run</i> dialog box	55
Figure 17. Notification in the Windows 8.0 and 8.1 <i>Command</i> window	56
Figure 18. Windows 10 <i>Search</i> box.....	56
Figure 19. Windows 10 Local Group Policy Editor options	57
Figure 20. Windows Local Group Policy Editor selection	58
Figure 21. Windows 10 <i>Search</i> box.....	58
Figure 22. <i>Local Group Policy Editor</i> screen options.....	59
Figure 23. <i>Ctrl+Alt+Del</i> <i>Options</i> settings	59
Figure 24. <i>Remove Task Manager</i> screen	60
Figure 25. “Download the Secure Profile” section	62
Figure 26. [Users & Groups] button in macOS System Preferences	63
Figure 27. <i>Users & Groups</i> window	63
Figure 28. <i>Login Options</i> window	64
Figure 29. [Accessibility] button in macOS System Preferences	65
Figure 30. Advanced Preferences options.....	66
Figure 31. Apple <i>System Preferences</i> dialog box.....	67
Figure 32. <i>App Store</i> screen.....	67
Figure 33. Notification when starting test with assessment mode	70
Figure 34. Emoji keyboard for iOS or iPadOS	70
Figure 35. [Settings] icon.....	70
Figure 36. Keyboards configuration interface	71
Figure 37. Disabled dictation	71
Figure 38. Keyboard Settings for iOS (other versions of iOS or iPadOS are similar)	72
Figure 39. Chromebook Recovery Utility	75
Figure 40. Selecting the CloudReady image	75
Figure 41. CloudReady media insertion prompt	76
Figure 42. [Download Browser] button	84
Figure 43. [CASecureBrowser] shortcut icon.....	84
Figure 44. [Download Browser] button	85
Figure 45. [CASecureBrowser] shortcut icon.....	87
Figure 46. <i>Create Shortcut</i> dialog box	92
Figure 47. [Download Browser] button	93
Figure 48. Contents of the CASecureBrowser-OSX.dmg folder	94
Figure 49. <i>Security & Privacy</i> screen for macOS.....	95
Figure 50. Apple <i>Application Support</i> configuration interface	96
Figure 51. [Download Browser] button	98
Figure 52. [CASecureBrowser] shortcut icon.....	98
Figure 53. [Download Browser] button	99
Figure 54. [CASecureBrowser] shortcut icon.....	100
Figure 55. Chromebook <i>Welcome</i> screen	103
Figure 56. Chrome OS <i>Missing</i> message.....	103
Figure 57. Turn OS Verification Off message	103
Figure 58. OS Verification Is Off message	104
Figure 59. Preparing for Developer Mode message	104
Figure 60. <i>Join WiFi Network</i> screen.....	104
Figure 61. Chromebook <i>Sign in</i> screen	105
Figure 62. Automatic Kiosk Mode message	105
Figure 63. <i>Extensions</i> screen	105

Figure 64. <i>Manage Kiosk Applications</i> screen.....	106
Figure 65. <i>Google Admin Console</i>	107
Figure 66. <i>Chrome Devices</i> screen	108
Figure 67. <i>Apps & extensions</i> drop-down list.....	108
Figure 68. <i>Kiosks</i> option	109
Figure 69. [Kiosks] tab section of the <i>Apps & Extensions</i> screen.....	109
Figure 70. <i>App Settings</i> screen	110
Figure 71. <i>Add Chrome app or extension by ID</i> screen.....	111
Figure 72. <i>Google app settings</i>	112
Figure 73. <i>Chromebook logon</i> screen	112
Figure 74. Select the state from the <i>Launchpad</i>	113
Figure 75. Select the assessment from the <i>Launchpad</i>	114
Figure 76. [Download on the App Store] button.....	116
Figure 77. <i>SecureTestBrowser</i> App Store download web page	116
Figure 78. [SecureTestBrowser] icon, iOS or iPadOS	116
Figure 79. Select the state from the <i>Launchpad</i>	117
Figure 80. Select the assessment from the <i>Launchpad</i>	118
Figure 81. The <i>Local Group Policy Editor</i> window	138
Figure 82. The <i>Logon Properties</i> dialog box.....	139
Figure 83. The <i>Add a Script</i> dialog box	139
Figure 84. Resetting the secure browser on OS X and macOS.....	141

**Acronyms and Initialisms Used in the CAASPP and ELPAC Technical Specifications
and Configuration Guide for Online Testing**

Abbreviation	Term
AIR	American Institutes for Research (now Cambium Assessment, Inc.)
CAASPP	California Assessment of Student Performance and Progress
CAI	Cambium Assessment, Inc.
CaITAC	California Technical Assistance Center
CAST	California Science Test
CDE	California Department of Education
CSA	California Spanish Assessment
DEI	Data Entry Interface
ELPAC	English Language Proficiency Assessments for California
IAHSS	Interim Assessment Hand Scoring System
IP address	internet protocol address
ISP	internet service provider
JAWS	Job Access With Speech
LAN	local area network
LEA	local educational agency
Mbps	Megabits per second
MDM	mobile device management
ORS	Online Reporting System
TCP	Transmission Control Protocol
TDS	test delivery system
TIDE	Test Information Distribution Engine
TOMS	Test Operations Management System
TTS	text-to-speech
WAP	wireless access point

Introduction

Manual Content

This manual provides information about system requirements and network, hardware, and secure browser configurations for running various testing applications used in online California Assessment of Student Performance and Progress (CAASPP) and English Language Proficiency Assessments for California (ELPAC) testing.

What's New in 2020–21

General

- In January 2020, Cambium Learning acquired AIR Assessment, the student assessment division of the American Institutes for Research (AIR). This division is now known as Cambium Assessment, Inc. (CAI).
- URLs that included “airst.com” have been updated to “cambiumast.com.”
- The mobile secure browser has been rebranded as *SecureTestBrowser* (formerly *AIRSecureTest*).
- The Teacher Hand Scoring System for the Initial ELPAC has been added to the available applications that are supported.

Assessments

- The Initial ELPAC operational assessments have been added to the list of assessments supported by the specifications and configurations described in this manual.
- The Alternate ELPAC, which is being field-tested January 12 through February 16, 2021, has been added to the list of assessments supported by the specifications and configurations described in this manual.

General Configuration

- The secure browser now validates certificates directly; a check through the Online Certificate Status Protocol is no longer made.

Apple and Macintosh Configuration

- The Secure Profile for the macOS has been updated to disable the following features:
 - Voice Control
 - The menu pop-up that appears when triple-tapping the power button on Touch Bar-enabled devices
 - Keyboard shortcuts

- The updated Secure Profile is required and can be downloaded from the [CAASPP and ELPAC Secure Browsers](#) website.
- Download of the Secure Profile is now hosted by CAI instead of Apple.
- Autonomous Single App Mode is no longer used with a device running iOS or iPadOS.
- The name of the “Automatic Assessment Configuration” in MacOS, iPadOS, and iOS is now “Assessment Mode.”

Secure Browser

Versions

The following are the updated secure browser versions for the 2020–21 CAASPP and ELPAC administrations. These are the only secure browser versions supported for testing.

Operating System	Device Type	Secure Browser Version
Apple iOS or iPadOS	Mobile	6.0
Chrome	Mobile	7.0 (August 2020)
macOS	Desktop or Laptop	12.5 or 13.0
Windows	Desktop or Laptop	12.5
Linux	Desktop or Laptop	12.5

Ancillary Software

- Job Access With Speech (JAWS®) 2021 is now supported.
- JAWS® 18 is no longer supported.



Notes:

- Chrome Secure Browser 7.0 may be used until June 2022.
- Both the Desktop Secure Browser 13.0 and macOS 10.16, which uses it, are expected to be available around October 31, 2020.

Operating Systems for Student Testing

Refer to “[Supported Operating Systems for Student Testing](#)” for complete information about operating system versions supported for the 2020–21 CAASPP and ELPAC administrations.

Additions

Operating System	Device Type	Operating System Addition
Apple iOS or Apple iPadOS	Mobile	<ul style="list-style-type: none"> Version 14 (upon release and acceptance)
Chrome	Mobile	<ul style="list-style-type: none"> Version 85+
Linux (64-bit or 32-bit)	Desktop or Laptop	<ul style="list-style-type: none"> Fedora 31 LTS (Gnome)
Linux (64-bit only)	Desktop or Laptop	<ul style="list-style-type: none"> Ubuntu 20.04 LTS (Gnome) (upon release and acceptance)
macOS	Desktop or Laptop	<ul style="list-style-type: none"> Version 10.16 (for use with secure browser version 13.0 only)
Windows	Desktop or Laptop	<ul style="list-style-type: none"> Windows 10 in S mode, 2004 (upon release and acceptance)



Note: Starting with version 10.12, the name of the Macintosh operating system is “macOS” (rather than “OS X”).

Deletions

Operating System	Device Type	Operating System Deletion
Android	Mobile	<ul style="list-style-type: none"> All versions (CAI no longer supports Android.)
Apple iOS or iPadOS	Mobile	<ul style="list-style-type: none"> Version 13.3 and below
Chrome	Mobile	<ul style="list-style-type: none"> Version 84 and below
Linux (64-bit or 32-bit)	Desktop or Laptop	<ul style="list-style-type: none"> Fedora version 29 and below Ubuntu 14.04 and below
macOS	Desktop or Laptop	<ul style="list-style-type: none"> OS X 10.9 and 10.10
Windows	Desktop or Laptop	<ul style="list-style-type: none"> Windows 7 SP1 Windows 10, version 1803 and below
Windows	Server	<ul style="list-style-type: none"> Windows Server 2008

Internet Browser Requirements

Refer to “[Supported Web Browsers for Online Systems Associated with Testing](#)” for complete information about internet browsers supported in associated systems for the 2020–21 CAASPP and ELPAC administrations.

Additions

Mobile Safari 14 will be supported for iOS and iPadOS when released and tested.

Deletions

Operating System	Device Type	Browser Deletion	Affected System
Android	Mobile	<ul style="list-style-type: none"> All 	<ul style="list-style-type: none"> All
Apple iOS or iPadOS	Mobile	<ul style="list-style-type: none"> Safari 11 and below 	<ul style="list-style-type: none"> All
Chrome	Mobile	<ul style="list-style-type: none"> (none) 	<ul style="list-style-type: none"> (none)
macOS	Desktop or Laptop	<ul style="list-style-type: none"> Safari 10 and below Firefox 59 and below Chrome 83 and below 	<ul style="list-style-type: none"> All
Linux	Desktop or Laptop	<ul style="list-style-type: none"> Firefox 59 and below Chrome 83 and below 	<ul style="list-style-type: none"> All
Windows	Desktop or Laptop	<ul style="list-style-type: none"> (none) 	<ul style="list-style-type: none"> (none)

Sections

This manual contains the technology requirements for online CAASPP and ELPAC testing for the 2020–21 test administrations, and includes the following sections:

- [Introduction](#) (this section), describes this guide.
- [Chapter 1: System Requirements](#), lists the minimum hardware and software requirements for online testing. Ensure that device hardware complies with these requirements before undertaking the tasks described in this manual.
- [Chapter 2: Network Configuration](#), provides information about configuring networks and lists helpful networking diagnostic tools.
- [Chapter 3: System Configuration](#), provides guidance regarding the proper infrastructure for printers and wireless access points with specifics for local educational agency networks and student devices.
- [Chapter 4: Secure Browser Configuration](#), provides information about configuring the secure browser on student machines and devices for online testing. The secure browser prevents students from accessing other computer or internet applications and from copying test information. It also occupies the entire computer screen.

- [Appendix A: Operating System Support Plan for the 2020–21 Test Delivery System](#), lists the operating systems supported for online CAASPP and ELPAC testing and their projected end-of-support dates.
- [Appendix B: URLs for Testing Systems](#), lists URLs that should be allowlisted in firewalls.
- [Appendix C: Technology Coordinator Checklist](#), lists the activities required to prepare a facility for online testing.
- [Appendix D: Scheduling Online Testing](#), provides a worksheet for estimating the required time to administer an online test.
- [Appendix E: Creating Group Policy Objects to Assign Logon Scripts in Microsoft Windows](#), describes how to create scripts that launch when a user logs into a Windows computer.
- [Appendix F: Resetting Secure Browser Profiles](#), provides instructions for resetting secure browser profiles.
- [Appendix G: User Support](#), provides information about contacting the California Technical Assistance Center for help.

Document Conventions

[Table 1](#) lists key symbols and typographical conventions used in this manual.

Table 1. Key Symbols and Document Conventions

Element	Description
	Warning: This symbol accompanies important information regarding actions that may cause fatal errors.
	Caution: This symbol accompanies important information regarding a task that may cause minor errors.
	Note: This symbol accompanies additional information that may be of interest.
	Additional Resources: This symbol accompanies a list of URLs for web pages or web documents that provide additional information.
	Tip: This symbol accompanies useful information on how to perform a task.
file name	Monospaced text indicates a directory, file name, or something a user enters in a field.
[text]	Text in brackets is used to indicate a link or button that is selectable.

Intended Audience

This manual is intended for the following audiences:

- Technology coordinators who are responsible for configuring the hardware, software, and network in a school's online testing environment and are familiar with the following concepts:
 - Networking—Bandwidth, firewalls, allowlisting, and proxy servers
 - Configuring operating systems—Control Panel in Windows, System Preferences in macOS, Settings in iOS and iPadOS, and the Linux command line
 - Installing software—Downloading installation packages from the internet or from a network location and installing software onto desktop or laptop computers running Windows, macOS, or Linux operating systems, or Chromebook or Apple mobile devices
 - Configuring web browsers—Settings in Chrome, Safari, and Firefox
- Network administrators who are familiar with mapping or mounting network drives and creating and running scripts at the user and host level
- Users who install and run the secure browser from an NComputing server and are familiar with operating that software and related hardware

This page is left blank intentionally.

Chapter 1: System Requirements

Supported Operating Systems for Student Testing

This section describes the supported operating systems for secure online testing. A secure online testing environment is a state in which a device is restricted from accessing prohibited computer applications (local or internet-based), or copying or sharing test data. The purpose of this environment is to maintain test security and provide a stable testing experience for students across multiple platforms.

For optimal performance, all systems should have the latest minor updates and patches installed. Major updates, including new versions, require review and testing prior to use in California Assessment of Student Performance and Progress (CAASPP) and English Language Proficiency Assessments for California (ELPAC) online testing.



Warning: Support for New Major Versions of Supported Operating Systems

- New major versions of supported operating systems must be tested by Cambium Assessment, Inc. (CAI; formerly American Institutes for Research) before they can be used for online testing. Do not upgrade to new major versions before support is announced officially. CAI also recommends users disable auto updates to keep systems from upgrading automatically. Refer to [appendix A](#) for the operating system support plan.

Desktops and Laptops



Note: ARM-powered devices, such as the Raspberry Pi, are not supported for online testing.

[Table 2](#) lists the operating systems and devices required for student testing in 2020–21. Online testing functions effectively with the minimum requirements listed. However, the recommended specifications provide improved performance.

Table 2. Supported Desktop Operating Systems

Supported Operating System	Supported Versions	Minimum Requirements	Recommended Specifications
Windows	<ul style="list-style-type: none"> 8.0 (Professional and Enterprise) 8.1 (Professional and Enterprise) 10, 10 in S mode; versions 1809–2004 (supported upon completion of version testing and acceptance) (Professional, Educational, and Enterprise) Server 2012 R2, 2016 R2 (thin client) 	<ul style="list-style-type: none"> 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) 	<ul style="list-style-type: none"> 1.4 GHZ processor 2 or more GB RAM 20 or more GB hard drive space

System Requirements |
Supported Operating Systems for Student Testing

Table 2 (continuation one)

Supported Operating System	Supported Versions	Minimum Requirements	Recommended Specifications
macOS	<ul style="list-style-type: none"> 10.11 (as OS X) 10.12–10.15 (as macOS) 10.16 (after October 31, 2020, and upon completion of version testing and acceptance) 	<ul style="list-style-type: none"> 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) 	<ul style="list-style-type: none"> 1.4 GHZ processor 2 or more GB RAM 20 or more GB hard drive space
Linux (64-bit or 32-bit)	<ul style="list-style-type: none"> Fedora 30–31 (supported upon completion of version testing and acceptance) LTS (Gnome) Ubuntu 16.04 LTS (Gnome) 	<ul style="list-style-type: none"> 1 GHZ Processor 2 GB RAM 20 GB hard drive (64-bit) Refer to the “Required for 32-bit and 64-bit Workstations” subsection in “Libraries and Packages” for a list of required packages. 	<ul style="list-style-type: none"> 1.4 GHZ processor 2 or more GB RAM 20 or more GB hard drive space Refer to the “Recommended for 32-bit and 64-bit Workstations” subsection in “Libraries and Packages” for a list of additional recommended packages.

Table 2 (continuation two)

Supported Operating System	Supported Versions	Minimum Requirements	Recommended Specifications
Linux (64-bit only)	<ul style="list-style-type: none"> • Ubuntu 18.04 LTS (Gnome) • Ubuntu 20.04 LTS (Gnome) (upon release and acceptance) 	<ul style="list-style-type: none"> • 1 GHZ Processor • 2 GB RAM • 20 GB hard drive (64-bit) • Refer to the “Required for 32-bit and 64-bit Workstations” and “Required for 64-bit Workstations Only” subsections in “Libraries and Packages” for a list of required packages. 	<ul style="list-style-type: none"> • 1.4 GHZ processor • 2 or more GB RAM • 20 or more GB hard drive space • Refer to the “Recommended for 32-bit and 64-bit Workstations” subsection in “Libraries and Packages” for a list of additional recommended packages.

Tablets



Note: Amazon Fire tablets are not supported for online testing.

[Table 3](#) lists the supported tablets, operating systems, and related requirements. Refer to “[Hardware Configuration](#)” in [chapter 3](#) for information about configuring these devices for online testing.

Table 3. Supported Tablets and Operating Systems

Operating System	Supported Version	Supported Tablets
iOS or iPadOS (iPads)	<ul style="list-style-type: none"> 12.4 13.4 14.0 	<ul style="list-style-type: none"> All iPads with a 9.7" or larger display and running a supported version of iOS or iPadOS
Windows	<ul style="list-style-type: none"> 8.0 (Professional and Enterprise) 8.1 (Professional and Enterprise) 10 (Professional, Educational, and Enterprise) 	<ul style="list-style-type: none"> Any 10" tablet running these versions of Windows is supported, but extensive testing has been done only on Surface Pro, Surface Pro 3, Asus Transformer, and Dell Venue

Chromebooks and Chromebases



Additional Resources in This Section:

- Google Chrome Enterprise Help | Auto Update Policy web page—
<https://support.google.com/chrome/a/answer/6220366?hl=en>



Cautions:

- While CAI actively works to support new versions of the Chrome operating system as they are released, automatic updates should be disabled until new versions are listed as supported. Disabling automatic updates allows CAI to review changes and address any updates that pose a potential risk to student testing. Automatic update settings are configured in the Google Admin console.
- Due to recent changes by Google, users with Chromebooks manufactured in 2017 or later who do not have an Enterprise or Education license will not be able to use those machines for assessments. Google no longer allows users without these licenses to set up kiosk mode, which is necessary to run the CAI Secure Browser.

(This change restricting kiosk mode does not affect the Chrome operating system. Any version of the Chrome OS on hardware manufactured in 2016 or earlier can be used.)

- Chrome OS includes a feature called tablet mode, which offers a touchscreen environment for supported Chromebooks and for Chrome OS tablets. CAI does not support the use of tablet mode for testing but does support touchscreen features on Chromebooks when available.

[Table 4](#) lists the supported operating systems for Chromebooks.

Table 4. Supported Chromebooks

Supported Operating Systems	Related Requirements
Chrome OS 85+	CAI will support any Chrome device that receives auto updates on the <i>stable</i> OS channel and meets the minimum operating system version requirement. CAI will not support any device that Google does not support for auto update. Refer to Google's Auto Update Policy web page for information on Google's auto update policy, including a full list of supported Chromebooks.

Thin Clients: NComputing and Terminal Servers for Windows

NComputing

[Table 5](#) lists the supported hardware and software for NComputing solutions.

Table 5. Supported NComputing Solutions

Supported Server Host	Supported Server Software	Supported Terminals
<ul style="list-style-type: none"> • Windows Server 2012 R2 • Windows Server 2016 R2 • Windows 10 	<ul style="list-style-type: none"> • vSpace PRO 10 	<ul style="list-style-type: none"> • L300, firmware version 1.13.xx • L350, firmware version 1.13.xx

Terminal Servers

[Table 6](#) lists the supported terminal servers for use with a thin client device.

Table 6. Supported Terminal Servers

Supported Terminal Servers	Supported Thin Client
<ul style="list-style-type: none"> Windows Server 2012 R2 Windows Server 2016 R2 	<p>Any thin client that supports a Windows Server is supported. 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.</p>



Warning: Security Issues with Terminal Services or Remote Desktop Connections to Servers

- 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 because students can use their local devices to search for answers. Therefore, this installation scenario is not recommended for testing. Refer to the "[Installing the Secure Browser on a Terminal Server or Windows Server](#)" subsection of [chapter 4](#) for more information.

Supported Web Browsers for Online Systems Associated with Testing

This section lists the supported web browsers for the 2020–21 California Assessment of Student Performance and Progress (CAASPP) and English Language Proficiency Assessments for California (ELPAC) online administration functions. These are the non-test-taking functions associated with student testing such as assigning student test settings and accessing the Test Administrator Interface. **The secure browser is the only type of browser students use to take in-person, online, summative assessments; the Initial ELPAC; and the Alternate ELPAC Operational Field Test.**

Supported Web Browsers by Operating System

[Table 7](#) lists the supported operating systems and corresponding web browsers for each application. Note the following about this table:

- It is recommended that recent versions of supported web browsers be used.
- Each application requires disabling pop-up blocking software and enabling JavaScript.
- Be sure to use the correct combination of operating system and web browser; for example, iOS 10.13 requires Safari 13.
- Websites for test administrators and test examiners include the Test Administrator Interface and the Data Entry Interface.

System Requirements |
Supported Web Browsers for Online Systems Associated with Testing

Table 7. Supported Web Browsers by Test Administration Websites

Operating System	Accepted Web Browser	Test Administrator Interface	Practice and Training Tests	Test Operations Management System	California Educator Reporting System	Online Reporting System	Completion Status and Roster Management	Interim Assessment Hand Scoring System	Interim Assessment Viewing System	Initial ELPAC Teacher Hand Scoring System
Windows Version 8.0 (Professional and Enterprise) Version 8.1 (Professional and Enterprise)	Chrome 83+	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Windows <ul style="list-style-type: none"> 8.0 (Professional and Enterprise) 8.1 (Professional and Enterprise) 	Firefox 60+	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Windows 10 (Professional, Educational, and Enterprise) <ul style="list-style-type: none"> Versions 1809–2004 (upon release and acceptance) 	Chrome 83+	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Windows 10 (Professional, Educational, and Enterprise) <ul style="list-style-type: none"> Versions 1809–2004 (upon release and acceptance) 	Firefox 60+	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Windows 10 in S mode (Professional, Educational, and Enterprise) <ul style="list-style-type: none"> Versions 1809–2004 (upon release and acceptance) 	Edge 83+	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Supported Web Browsers by Test Administration Websites (*continuation one*)

Operating System	Accepted Web Browser	Test Administrator Interface	Practice and Training Tests	Test Operations Management System	California Educator Reporting System	Online Reporting System	Completion Status and Roster Management	Interim Assessment Hand Scoring System	Interim Assessment Viewing System	Initial ELPAC Teacher Hand Scoring System
macOS <ul style="list-style-type: none"> Version 10.11 (as OS X) Versions 10.12–10.15 Version 10.16 (upon release and acceptance) 	Chrome 83+	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
macOS <ul style="list-style-type: none"> Versions 10.11 (as OS X) Versions 10.12–10.15 Version 10.16 (upon release and acceptance) 	Firefox 60+	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
macOS <ul style="list-style-type: none"> Versions 10.11 (as OS X) Versions 10.12–10.15 Version 10.16 (upon release and acceptance) 	Safari 9+	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

System Requirements |
Supported Web Browsers for Online Systems Associated with Testing

Supported Web Browsers by Test Administration Websites (*continuation two*)

Operating System	Accepted Web Browser	Test Administrator Interface	Practice and Training Tests	Test Operations Management System	California Educator Reporting System	Online Reporting System	Completion Status and Roster Management	Interim Assessment Hand Scoring System	Interim Assessment Viewing System	Initial ELPAC Teacher Hand Scoring System
Linux Fedora LTS (Gnome) • Versions 30–31 (upon release and acceptance)	Chrome 83+	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Linux Fedora LTS (Gnome) • Versions 30–31 (upon release and acceptance)	Firefox 60+	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Linux Ubuntu (LTS) (Gnome) • Version 16.04 • Version 20.04 (upon release and acceptance)	Chrome 83+	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Linux Ubuntu (LTS) (Gnome) • Version 16.04 • Version 20.04 (upon release and acceptance)	Firefox 60+	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Supported Web Browsers by Test Administration Websites *(continuation three)*

Operating System	Accepted Web Browser	Test Administrator Interface	Practice and Training Tests	Test Operations Management System	California Educator Reporting System	Online Reporting System	Completion Status and Roster Management	Interim Assessment Hand Scoring System	Interim Assessment Viewing System	Initial ELPAC Teacher Hand Scoring System
iOS 12.4	Safari 14	Yes	Yes	No	Yes	No	No	Yes	Yes	Yes
iOS 13.4	Safari 14	Yes	Yes	No	Yes	No	No	Yes	Yes	Yes
iPadOS 14.0	Safari 14	Yes	Yes	No	Yes	No	No	Yes	Yes	Yes
Chrome OS • Version 85+	Chrome 85+	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Available Audio Settings by Web Browser

Some test items play audio files; some students have the text-to-speech (TTS) accommodation. In either case, the student should be able to adjust the audio settings for those items. [Table 8](#) lists the browsers—secure and web—and their associated capability to modify such settings. (In some cases, the audio files for practice tests will be accessible using a web browser; for Chrome, this must be enabled explicitly.) Use [table 8](#) to ensure that a browser with the required capability is deployed. Secure browsers are displayed in bold.

Table 8. Available Audio Settings by Browser

Operating System	Browser	System Volume	TTS Volume	TTS Pitch	TTS Rate	TTS Tracking	Pause	Resume
Windows	Secure browser	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Windows	Edge web browser	Yes	Yes	Yes	Yes	Yes	No	No
Windows	Chrome web browser	Yes	Yes	Yes	Yes	Yes	No	No
Windows	Firefox web browser	No	No	No	No	Yes	No	No
macOS	Secure browser	Yes	Yes	Yes	Yes	Yes	Yes	Yes
macOS	Safari web browser	No	No	No	No	Yes	No	No
macOS	Chrome web browser	Yes	Yes	Yes	Yes	Yes	No	No
Linux	Secure browser	Yes	Yes	Yes	Yes	No	Yes	Yes
Linux	Firefox web browser	No	No	No	No	No	No	No
Linux	Chrome web browser	Yes	Yes	Yes	Yes	No	No	No
iOS or iPadOS	Mobile secure browser	No	Yes	Yes	Yes	Yes	No	No
iOS or iPadOS	Safari web browser	No	No	No	No	Yes	No	No
Chromebook	Secure browser	No	Yes	Yes	Yes	Yes	No	No
Chromebook	Chrome web browser	Yes	Yes	Yes	Yes	Yes	No	No

Requirements for Peripheral Equipment

Additional Resources in This Section:

- California Department of Education (CDE) California Assessment Accessibility Resources Matrix web document—<https://www.cde.ca.gov/ta/tg/ca/documents/caaccessibilitymtrx2021.docx>
- *Accessibility Guide for CAASPP and ELPAC Online Testing* web document—<http://www.caaspp.org/rsc/pdfs/CAASPP-ELPAC.accessibility-guide.2020-21.pdf>

This section describes the requirements for peripheral equipment: monitors, screens, keyboards, and headphones.

Monitors and Screen Display Requirements

All supported computers, laptops, netbooks, and tablets must meet the following requirements.

Screen Dimensions

Screen dimensions must be 10" or larger (iPads with a 9.7" display are included). This means that the Apple iPad Mini is **not** supported.

Screen Resolution

All devices must meet the following minimum resolution:

- Desktops, laptops, and tablets: 1024 × 768

Larger resolutions can be applied as appropriate for the monitor or screen being used. To maximize the testing experience, the device's display scale should be set to 100 percent, which keeps the amount of usable screen space within the 1024 × 768 minimum resolution for the test delivery system (TDS).

Depending on the screen size, students may need to use vertical or horizontal scroll bars to view all test-related information. Students may also use the Zoom tool in the online test to enlarge the content on the screen.

Keyboards

External Keyboards

External keyboards are strongly recommended with tablets used for testing. The intent of this recommendation is to ensure the required display area is available to allow students to read multiple sources of complex item text and respond to source evidence for analytical purposes. Students may use mechanical or manual keyboards. Wireless and Bluetooth-based keyboards are not supported.

Some external keyboards have additional “shortcut” buttons that can create security issues. These buttons may allow students to open another application or the tablet’s default on-screen keyboard, some of which can cause the security breach detector to exit a student from the TDS. Students are strongly cautioned against using keyboards that have these shortcut buttons.

Mice

Mice on mobile devices are not supported. Wired two- or three-button mice that are compatible with the operating system on desktops and laptops are supported but are not required. No other mice should be used, especially mice equipped with a “browser back” button that could create an insecure testing environment and can cause the security breach detector to exit a student from the TDS.

Headsets and Headphones

Students need headphones to listen to audio in online assessments and may use headsets to record answers to tests. What follows are some scenarios that require headphones or headsets.

- The CAASPP English language arts/literacy assessments contain audio (recorded or device-based read-aloud). Students must be provided with headphones so they have the option to clearly listen to the audio in these tests.
- The ELPAC Listening, Speaking, and Writing domains contain recorded audio. Students may be provided with headphones, so they have the option to listen to the audio either using headphones or their device speakers. For the audio capture feature in the Speaking domain, students may use the microphone on the headset (if available) or built-in microphone on the device.
- Students with the text-to-speech test setting can use headphones to listen to stimuli or test items being read aloud by the device. For more information about text-to-speech and other test settings, refer to one of the following resources:
 - [California Assessment Accessibility Resources Matrix](#) web document
 - [Accessibility Guide for CAASPP and ELPAC Online Testing](#)

- Students with the streamline designated support can use headphones along with Job Access with Speech® or other screen-reading software to complete online tests.
- Each NComputing terminal used for testing must have a USB headphone or headset.

CAASPP test site coordinators and site ELPAC coordinators should determine how many students will need headphones to ensure that there are enough available at the time of a test. [Table 9](#) lists some of the supported headphones and headsets.

Table 9. Supported Headphones and Headsets

Model	Connector	Microphone Included?	Hardware
Logitech 390	USB (wired)	Yes	All supported desktops, laptops, and Chromebases with USB port
Panasonic RP-HT21	XBS	No	All supported desktops, laptops, and Chromebases with XBS port
Logitech analog	3.5 mm	No	iOS or iPadOS
Plantronics 326	3.5 mm	Yes	All supported desktops, laptops, and Chromebases with 3.5 mm port—except NComputing terminals
Sennheiser PC 151	3.5 mm	Yes	All supported desktops, laptops, and Chromebases with 3.5 mm port—except NComputing terminals
Plantronics 355	3.5 mm	Yes	All supported desktops, laptops, and Chromebases with 3.5 mm port—except NComputing terminals
Generic headphones	3.5 mm	No	All supported desktops, laptops, and Chromebases with 3.5 mm port—except NComputing terminals
Generic headphones	USB (wired)	No	All supported desktops, laptops, and Chromebases with USB port

Speakers

Students taking the ELPAC who are not using headphones may instead hear the audio for the Listening, Speaking, and Writing domains through a device’s built-in or external speakers so that the test examiner can listen along with the student. This is recommended for one-on-one administrations of the ELPAC.

ELPAC test examiners are encouraged to test their audio systems, prior to testing, by playing the sample audio to determine the appropriate volume, sound quality, and placement of student speakers.

Microphones

The ELPAC Speaking domain uses voice capture technology. Because the Speaking domain is administered one-on-one for all grades, local educational agencies (LEAs) are encouraged to administer the Speaking test using student testing devices with built-in recording or microphone capabilities in an area where outside sounds are minimized. LEAs that do not have student testing devices with recording or microphone capabilities are not required to use the voice capture function. Headphones or headsets with microphones are not required.

Chapter 2: Network Configuration

Network Configuration and Testing

The network configuration has a significant impact on the test delivery system's (TDS') performance. An improperly configured network can slow a TDS' responsiveness and possibly impact students' scores or an assessment's integrity. The subsections in this chapter provide guidance on properly configuring the network and list popular tools for diagnosing network bottlenecks.

Finally, the network configuration must support a secure online testing environment, which is a state in which a device is restricted from accessing prohibited computer applications (local or internet-based), or copying or sharing test data. The purpose of this environment is to maintain test security and provide a stable testing experience for students across multiple platforms.

Network Configuration

This subsection provides guidance or requirements pertaining to networking configurations for online testing.

Guidance for Determining Required Bandwidth

Bandwidth is the measure of a network's capacity or utilization, usually measured in terms of bits per second. To ensure a smooth administration, Cambium Assessment, Inc. (CAI) recommends network bandwidth of at least 20 kilobits per second for each student being concurrently tested. The network should have enough bandwidth to support online testing at the required performance level. Refer to the "[Network Diagnostic Tools](#)" subsection for information about tools that check the network's bandwidth for California Assessment of Student Performance and Progress (CAASPP) and English Language Proficiency Assessments for California (ELPAC) online testing.

In an online testing environment, the bandwidth required to administer a test is influenced by the average size of the items on the test. The average size of the items on a test will vary based upon the types of items included on the test. For example, larger items, like animations, simulations, audio, or a combination of these larger items, will increase the average size of the items on a test, which affects the bandwidth requirement for the test. By contrast, tests containing smaller items, such as those containing only text, will have a smaller average item size, and will generally require less bandwidth.

The following factors also affect the required bandwidth for a given test:

- **Number of Students Testing Simultaneously**—As the number of students testing at one time increases, the required bandwidth also increases.
- **Hubs or Switches**—Local area network performance can be hindered when hubs are used instead of switches. A hub broadcasts signals from various network devices to propagate across the network, potentially saturating the network and causing traffic

competition or data collisions. When using hubs, ensure they have enough bandwidth to handle the propagation.

- **Internet service provider (ISP) Router**—For internet networks, the most common bottleneck is the ISP’s router connection, which typically operates at speeds of between 1.5 Megabits per second (Mbps) and 100 Mbps. Network administrators should spend time prior to test administration determining if their internet infrastructure has the capacity to accommodate online testing at the required performance level.
- **Encryption**—Encryption at wireless access points (WAPs) may contribute to bandwidth usage. When using use encryption, ensure the WAPs have enough bandwidth to prevent degradation of performance.
- **Required Response Time**—When a network’s bandwidth cannot service the amount of data requested by clients, latency starts to accumulate, and the students experience delays. Ensure the network’s bandwidth is high enough to support the required response times between the browsers and the servers.

[Table 10](#) displays the estimated average bandwidth used by the secure browser for testing when a test is first accessed and during subsequent testing. When designing the network for online testing, ensure that the available bandwidth can support these values.

Table 10. Average Bandwidth Used by Secure Browser for Testing

Number of Students Testing Concurrently in School or Building	Average Estimated Bandwidth Consumed During Subsequent Startup of Secure Browser	Average Estimated Bandwidth Consumed During Testing
1	8K bits per second	24K bits per second
50	400K bits per second	1200K bits per second
100	800K bits per second	2400K bits per second

Bandwidth consumed when opening the secure browser and accessing an assessment for the first time is significantly more than when opening the secure browser and accessing an assessment subsequently. This is because the initial launch of the secure browser downloads nonsecure cacheable content (not test content) that can be immediately accessed upon opening the secure browser later.

The values in the *Average Estimated Bandwidth Consumed During Testing* column are based on averages from tests in a variety of content areas and domains.

Required Ports and Protocols

[Table 11](#) lists the ports and protocols used by the TDS. Ensure that all content filters, firewalls, and proxy servers are open accordingly.

Table 11. Ports and Protocols for the TDS

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

Allowlisting Test Site Resource URLs for Online Testing

If the school’s filtering system has both internal and external filtering, the URLs for the testing sites must be allowlisted in both filters (refer to “[URLs for Testing Sites](#)”). Please refer to the filtering system’s documentation for specific instructions. Be sure to allowlist the URLs in [Appendix B: URLs for Testing Systems](#) in any multilayer filtering system (such as local and global layers). Ensure all items that handle traffic to *.tds.cambiumast.com and *.tds.airast.org have the entire certificate chain and are using the latest TLS 1.2 protocol.

Configuring Domain Name Resolution

[Appendix B: URLs for Testing Systems](#) lists the domain names for CAASPP and ELPAC online testing and nontesting applications. Ensure the testing devices have access to a DNS server that can resolve those names.

Configuring Session Timeouts

Session timeouts on proxy servers and other devices should be set to values greater than the average time it takes a student to participate in a test session or to complete a given test. For example, if a school determines that students will test in 60-minute sessions, then consider setting the session timeout to 65 or 70 minutes.

Data Caching

Data caching is a technique by which an intermediate server checks if it can serve the client’s requests instead of a downstream server. While data caching is a good strategy in some situations, its overhead is detrimental in the online testing environment. Ensure all intermediate network elements, such as proxy servers, do not cache data.

Configuring Quality of Service and Traffic Shaping

If the testing network includes devices that perform traffic shaping, packet prioritization, or Quality of Service, ensure the URLs in [Appendix B: URLs for Testing Systems](#) have high priority.

Network Diagnostic Tools

Additional Resources in This Subsection:

- CAASPP and ELPAC Diagnostic Screen web page—
https://demo.tds.airast.org/systemdiagnostic/pages/default.aspx?c=California_PT&url=https://capt.tds.airast.org/student
- CAASPP Online Practice and Training Tests Portal web page—
<http://www.caaspp.org/practice-and-training/>
- ELPAC Online Practice and Training Tests web page—<https://www.elpac.org/resources/online-practice-and-training-test/>
- Ookla Speedtest website—<https://www.speedtest.net/>

The goal of a network diagnostic tool is to determine if network bandwidth at a test site can handle the number of students assigned to test at peak volume. If the tool indicates fewer students should be tested simultaneously, try running a third-party network speed test such as Ookla’s [Speedtest](https://www.speedtest.net/). If the third-party tool also indicates a lack of proper bandwidth, determine if other activity on the network is drawing bandwidth away from machine attempting to take the test. Make adjustments to prioritize bandwidth for CAI’s websites during online testing, if possible.

Conduct a performance analysis of the networking infrastructure to identify any bottlenecks that may impact test performance. The choice of diagnostic tool depends on the operating system running the tool, the network administrator’s technical knowledge, and the desired level of network analysis. A number of network diagnostic tools are available, as described in the following subsections.

The Bandwidth Diagnostic Tool

CAI provides a diagnostic tool that can be directly accessed from the student practice and training tests logon page.

1. On the practice test logon page—accessed by selecting the **[Student Interface Practice and Training Tests]** button on either the [CAASPP Online Practice and Training Tests Portal](#) or [ELPAC Practice and Training Tests](#) web page—select the [Run Diagnostics] link, which resides under the “Guest” toggles on the sign-in page ([figure 1](#)) to open the [Diagnostic Screen](#) web page.

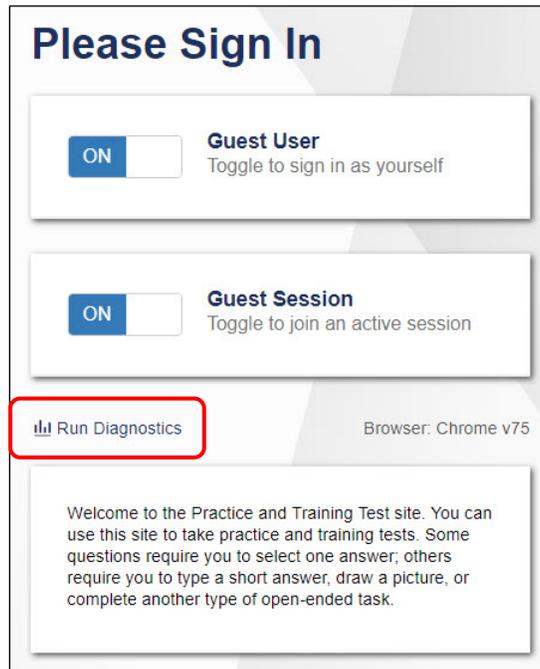


Figure 1. Sign-in web page for the training test

2. In the “Network Diagnostics” section of the [Diagnostic Screen](#) web page ([figure 2](#)), select the test that is likely to yield the highest number of concurrent users. (Note that for the California Alternate Assessment and the Alternate ELPAC Operational Field Test, which are administered one-on-one to a small number of students, usage concurrency is not typically expected to be a concern.)

Diagnostic Screen

This page allows you to check the **current** bandwidth of your network. The following operating systems and web browsers are supported:

Windows 7, 8.0, 8.1, 10, 10S, Server 2012, 2016: Mozilla, Firefox, Chrome, Edge
Mac OS 10.9-10.14: Firefox, Chrome, Safari
Linux Fedora 29-30 ; Ubuntu (LTS) 14.04, 16.04 –18.04: Firefox
Apple tablets (iPad) running iOS 11.4-13.0: Safari
Android tablets running 7.0-8.0: Google Chrome
Chromeos 75+: Google Chrome

To determine your bandwidth, select a test from the drop-down list and enter the maximum number of students likely to test at one time, then click [Run Network Diagnostics Tests].

The **[Text-to-Speech Check]** is for schools who will be administering the test, and requires the use of the secure browser. The secure browser is available from www.caaspp.org.

Your Operating System: Windows 10 **Your Browser Version:** Chrome v76

Secure Browser: false

Network Diagnostics:

Select Test: ← 2

Enter the total number of students you would like to test at one time: ← 3

4 →

Download Results: **Upload Results:**
5.367 Mbps download. 4.978 Mbps upload.

Bandwidth Summary:

Given the current load on your system, you should be able to test the requested number of students at this location. (Please note: The throughput estimates include the encryption/decryption overhead for data transfer. Throughput estimates change as the network conditions change and can vary from run to run.)

Figure 2. Run the diagnostics test

3. Select the approximate number of students who may take that test *at one time*.
4. Select **[Run Network Diagnostics Tests]**.

The tool displays the current upload and download speed as well as a general idea of whether the number of students entered in step 3 can be tested reliably. Users may want to run this test several times throughout the day to verify that upload and download speeds remain relatively consistent.

Windows-Specific Tools

Additional Resources in This Subsection:

- Microsoft NTttcp Utility: Profile and Measure Windows Networking Performance web page—<https://gallery.technet.microsoft.com/NTttcp-Version-528-Now-f8b12769>
- Paessler PRTG Network Monitor web page—<https://www.paessler.com/prtg>

PRTG Traffic Grapher

[PRTG](#) monitors bandwidth usage and other network parameters via Simple Network Management Protocol. It also contains a built-in packet sniffer. A freeware version is available.

NTttcp

[NTttcp](#) is a multithreaded, asynchronous application that sends and receives data between two or more endpoints and reports the network performance for the duration of the transfer.

Pathping

Pathping is a network utility included in Windows. It combines the functionality of the `ping` and `tracert` commands by providing details of the path between two hosts and ping-like statistics for each node in the path based on samples taken during a time period.

MacOS–Specific Tools

Additional Resources in This Subsection:

- *macOS User Guide*, Use Network Utility on Mac web page—<https://support.apple.com/guide/mac-help/use-network-utility-on-mac-ntutl001/mac>

Network Utility App

The [Network Utility](#) app is built into macOS. Network Utility provides information and troubleshooting tools for the network. It is located in the `/System/Library/CoreServices/Applications` folder.

Multiplatform Tools



Additional Resources in This Subsection:

- GitHub iperf web page—<https://github.com/esnet/iperf>
- Riverbed WinDump Overview web page—<https://www.winpcap.org/windump/>
- SourceForge The tcpdump project web page—<https://sourceforge.net/projects/tcpdump/>
- Wireshark web page—<https://www.wireshark.org/>

Wireshark

[Wireshark](#) is a network protocol analyzer. It has a large feature set and runs on most platforms including Windows, macOS, and Linux.

Tcpdump

[Tcpdump](#) is a common packet sniffer that runs from the command line on Linux and macOS. It can intercept and display data packets being transmitted or received over a network. A Windows version, [WinDump](#), is also available.

Ping, NSLookup, Netstat, and Traceroute

Ping, NSLookup, Netstat, and Traceroute comprise a set of standard UNIX network utilities. Versions of these utilities are included in Linux, Windows, and macOS.

Iperf

[Iperf](#) measures maximum TCP bandwidth, allowing the tuning of various parameters and User Datagram Protocol characteristics. Iperf reports bandwidth, delay jitter, and datagram loss.

This page is left blank intentionally.

Chapter 3: System Configuration

Hardware Configuration

Additional Resources in this Section:

- California Assessment of Student Performance and Progress (CAASPP) Accessibility Resources web page—<http://www.caaspp.org/administration/accessibility/>
- English Language Proficiency Assessments for California (ELPAC) Student Accessibility Resources web page—<https://elpac.org/test-administration/accessibility-resources/>

This section provides topology guidance for printers and wireless access points (WAPs). Note that hardware configuration requirements support a secure online testing environment, which is a state in which a device is restricted from accessing prohibited computer applications (local or internet-based), or copying or sharing test data. The purpose of this environment is to maintain test security and provide a stable testing experience for students across multiple platforms.

Connections Between Printers and Testing Devices

Test administrators and test examiners can print test session information and approve students' requests to print stimuli or test items (for students assigned the print-on-demand resource). Nevertheless, to maintain a secure test environment, the test administrator's or test examiner's device should be connected to a single local or network printer in the testing room, and only the test administrator's or test examiner's device should have access to that printer.

Wireless Networking and Determining the Number of Wireless Access Points (WAPs)

The following are the most commonly deployed wireless networking standards:

- 802.11ac has a theoretical throughput of up to 1 gigabit per second.
- 802.11n has a theoretical throughput of up to 300 megabits per second (Mbps).
- 802.11g has a theoretical throughput of up to 54 Mbps.
- 802.11b has a theoretical throughput of 11 Mbps.

The recommended number of devices supported by a single wireless connection depends on the standard used for the connection. The two most common networking standards are 802.11g (54 Mbps) and 802.11n (300 Mbps).

[Table 12](#) lists recommendations for network topology in which the wireless access point (WAP) provides 802.11g and the testing devices provide 802.11g, 802.11n, or a mixture of the two. Note that there currently are no recommendations for 802.11ac routers. Refer to the WAP documentation for specific recommendations and guidelines for these or other standards.

Table 12. Recommended Ratios of Devices to Wireless Access Points

Testing Device	Ratio of Devices to 802.11g WAP	Ratio of Devices to 802.11n WAP
802.11g	20	40
802.11n	20	40
Mix of 802.11g and 802.11n	20	40–50 (depending on the mix of wireless cards used)

Regardless of the number of WAPs, each should be configured to use Wi-Fi Protected Access II Advanced Encryption Standards (WPA2/AES) data encryption.

Hardware for Braille Testing

For information about braille hardware and software requirements, refer to the [CAASPP and ELPAC Accessibility Guide for Online Testing](#), which will be available on the CAASPP [Accessibility Resources](#) web page and the ELPAC [Student Accessibility Resources](#) web page.

Software Configuration



Warning: Scheduling Background Jobs

- Failure to schedule background jobs for times outside the testing window could result in a student's being exited from the secure browser during testing should a process begin to run.



Warning: Disabling Auto Update

- It is recommended that all application and operating system software on all devices used for test operations and student testing (in conjunction with the secure browser) be configured to turn auto update features off during testing hours. Refer to the software's documentation or Help feature to verify the software uses auto update and for instructions on disabling this feature for the duration of the local educational agency's (LEA's) or test site's selected testing window.

This section describes how to configure the operating systems and web browsers that support the operations necessary for the online testing administered via the secure browser. Note that software configuration requirements support a secure online testing environment, which is a state in which a device is restricted from accessing prohibited computer applications (local or internet-based), or copying or sharing test data. The purpose of this environment is to maintain test security and provide a stable testing experience for students across multiple platforms.

For students to access online tests, each student testing device needs Cambium Assessment, Inc.'s (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 the 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.

Optimal Installation Scenario for Secure Browsers

[Chapter 4: Secure Browser Configuration](#) describes several scenarios for installing the secure browser. However, it is strongly recommended that the secure browser be installed locally on each students' testing device rather than on a shared network drive from which students would run the secure browser as **this will compromise the stability and performance of the secure browser, especially during peak testing times**. Running the secure browser on a shared network drive creates competition among the students' clients for two resources: local area network bandwidth and shared disk drive input and output. This

performance impact can be avoided by installing the secure browser locally on each device. Additionally, running the secure browser from a shared location also creates security risks.



Warning: Testing From a Terminal or Windows Server Is Not Recommended

- Launching a secure browser from a terminal or Windows server typically does not create a secure test environment because students can use their local devices to search for answers. Additionally, this sort of configuration can compromise the stability and performance of the secure browser, especially during peak testing times, because it creates contention among students' client devices for local area network bandwidth and shared drive input and output. Therefore, this installation scenario is **not recommended for testing**.

Configuring Commercially Available Web Browsers

This subsection describes how to configure commercially available browsers (Chrome, Safari, and Firefox) that support the operations necessary for student online testing.

Enabling Pop-Up Windows

Systems used to support student California Assessment of Student Performance and Progress (CAASPP) and English Language Proficiency Assessments for California (ELPAC) testing provide informational messages or warnings using pop-up windows. Therefore, a user must enable pop-up windows on those web browsers used in support of online CAASPP and ELPAC testing systems, such as the Test Operations Management System.

The following list describes how to enable pop-up windows on many web browsers. If a web browser is not on this list, consult its user documentation.

Enabling Pop-Up Windows for All Domains

The following instructions enable pop-up windows for *all domains*. If a user prefers to limit pop-up windows to only those coming from domains involved in all aspects of CAASPP and ELPAC testing, use the instructions in the next subsection, “Enabling Pop-Up Windows Only for Domains Involved in Online Testing.”

- **Firefox (Windows):** *Menu → Options → Privacy & Security panel → “Permissions” → Uncheck the *Block pop-up windows* box.*
- **Edge:** *Menu → Settings → Site Permissions → Pop-ups and redirects → toggle *Block (Recommended)* to off or disabled.*
- **Chrome:** *Menu → Settings → Privacy and security panel → Site Settings → Pop-ups and redirects → Toggle *Blocked (recommended)* to *Allowed*.*

- **Safari:** *Safari* → *Preferences* → [**Security**] tab → Uncheck the *Block pop-up windows* box.
- **iOS or iPadOS Safari:** *Settings* → From the left side of the screen, select *Safari* → *Block Pop-ups* (toggle to “off” mode).

Enabling Pop-Up Windows Only for Domains Involved in Online Testing

Users can allow pop-up windows only from domains involved in CAASPP and ELPAC online testing. The following list describes how to enable domain-specific pop-up windows on many browsers. If a browser is not on this list, consult its user documentation. The list of domains to use in these instructions appears in [Appendix B: URLs for Testing Systems](#).

- **Firefox (Windows):** *Menu* → *Options* → *Privacy & Security* panel → “Permissions” → [**Exceptions...**] (next to *Block pop-up windows*)
- **Chrome:** *Menu* → *Settings* → *Privacy and security* panel → *Site Settings* → *Pop-ups and redirects* → Select [**Add**] (to the right of “Allow”).
- **Safari:** N/A
- **iOS or iPadOS Safari:** N/A

Preventing Auto Update on Device Operating Systems Used for Test Operations



Warning: Disabling Auto Update

- It is recommended that all application and operating system software on all devices used for test operations and student testing (in conjunction with the secure browser) be configured to turn auto update features off during testing hours. Refer to the software’s documentation or Help feature to verify the software uses auto update and for instructions on disabling this feature for the duration of the LEA’s or test site’s selected testing window.

Delaying Firefox Web Browser Updates

Quality assurance tests are conducted on the most recent Firefox web browser versions for each system except the student testing site, which requires the secure browser. Users should wait before installing new versions of Firefox, which could impact system performance. Delaying updates allows users time to review changes and verify each system works correctly with the new version.

To disable auto updates in Firefox:

- *Menu* → *Options* → “Firefox Updates” → “Allow Firefox to” → Select *Check for updates but let you choose to install them*.

Keyboard Navigation on the *Tool* Menu Using a Safari Browser

Unlike other browsers, students cannot use Safari to navigate to the *Tool* menu using standard methods on practice and training tests. To enable access the *Tool* menu using Safari, check the *Press Tab to highlight each item on a webpage* box in the “Accessibility” section of the Safari Advanced preferences, as shown in [figure 3](#).



Note: Students who have the Text-to-Speech accommodation enabled for practice tests will need to use the secure browser.

1. Open Safari.
2. Select *Preferences* from the Safari menu.
3. Select the [**Advanced**] button to open the *Advanced* window ([figure 3](#)).

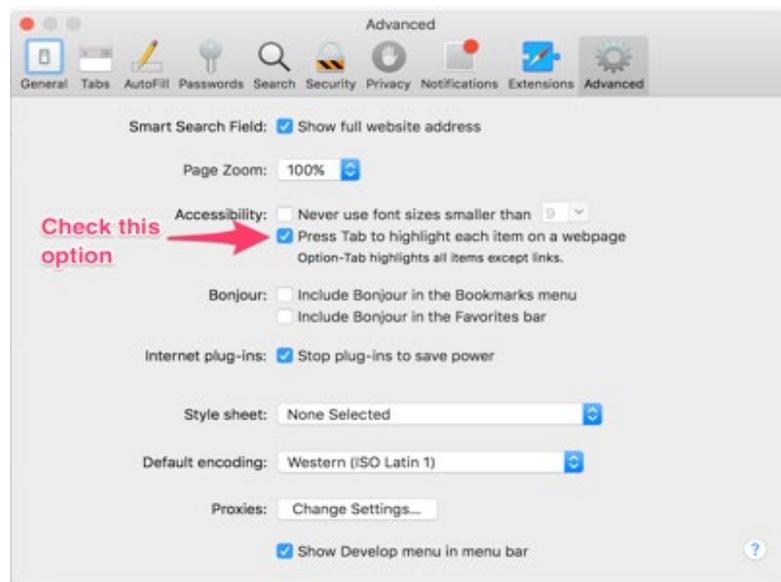


Figure 3. Safari Advanced preferences

4. Check the *Press Tab to highlight each item on a webpage* box to enable keyboard use on the *Tool* menu in practice tests.

Configuring Devices for Online Testing with the Secure Browser

This subsection describes how to configure devices for online testing.

Windows Testing Device Configuration

Installing Windows Media Pack for Windows 8.1 N and 8.1 KN



Additional Resources in This Subsection:

- Microsoft Media Feature Pack for Windows 8.1 N and Windows 8.1 KN Additions: April 2014 web page—<http://support.microsoft.com/kb/2929699/en-us>
- Microsoft Media Feature Pack for N and KN versions of Windows 8.1 Download Center web page—<https://www.microsoft.com/en-us/download/details.aspx?id=42503>
- Microsoft Feature Pack for N versions of Windows 10 web page—<https://www.microsoft.com/en-us/software-download/mediafeaturepack>
- Microsoft Windows Support | K-12 assessment unexpectedly reports apps running in the background in Windows 10 web page—<https://support.microsoft.com/en-us/help/4338725/k-12-assessment-unexpected-reports-apps-running-background-windows-10>

Some versions of Windows 8.1 and 10 are not shipped with media software installed. As a result, a user may need to install software to enable students to listen to and record audio as well as watch videos.

Microsoft provides additional information as well as a download package for devices with the following Windows 8.1 versions:

- Windows 8.1 N
- Windows 8.1 N/K with Bing
- Windows 8.1 Enterprise N
- Windows 8.1 Pro N
- Windows 8.1 Pro N/K for EDU
- Windows 10 N

A user is encouraged to download this software and ensure it works with sample websites and video and audio files prior to installing the Windows secure browser. Installation instructions are provided on Microsoft's download page.

Microsoft Resources:

- [Media Feature Pack for Windows 8.1 N and Windows 8.1 KN Editions](#) web page
- [Media Feature Pack for N and KN versions of Windows 8.1](#) web page
- [Microsoft Feature Pack for N versions of Windows 10](#) web page

Configuring Touch Input

Blocking Device Touch Input Using the Group Policy Editor

Some tablets and devices have touch features that may need to be disabled before testing. When following these instructions, note that the settings for the device the user is configuring may be slightly different than those in the figure.

To disable the touch features on these devices to edit policy settings using the Group Policy Editor:

1. Type `gpedit.msc` in the *Search* box on the *Start* menu and then select the link. The *Local Group Policy Editor* window, shown in [figure 4](#), appears.

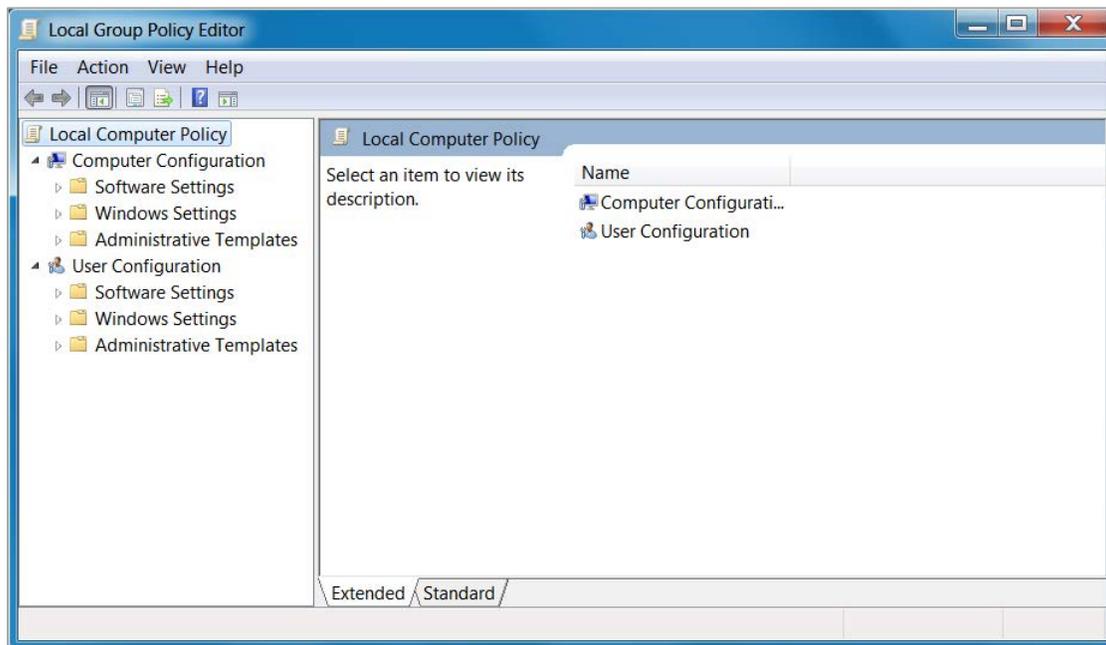


Figure 4. Local Group Policy Editor window

2. In the left pane, navigate to *Computer Configuration* → *Administrative Templates* → *Windows Components* (indicated in [figure 5](#)).

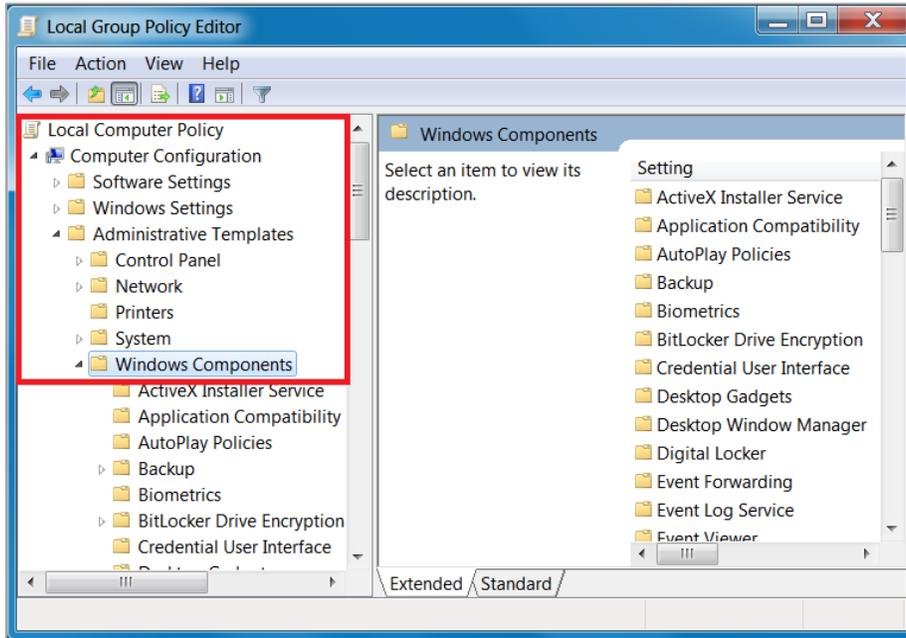


Figure 5. Windows Components panel

3. In the *Windows Components* panel in the left pane, scroll down to the **[Tablet PC]** folder icon—indicated in [figure 6](#)—and double-click it.

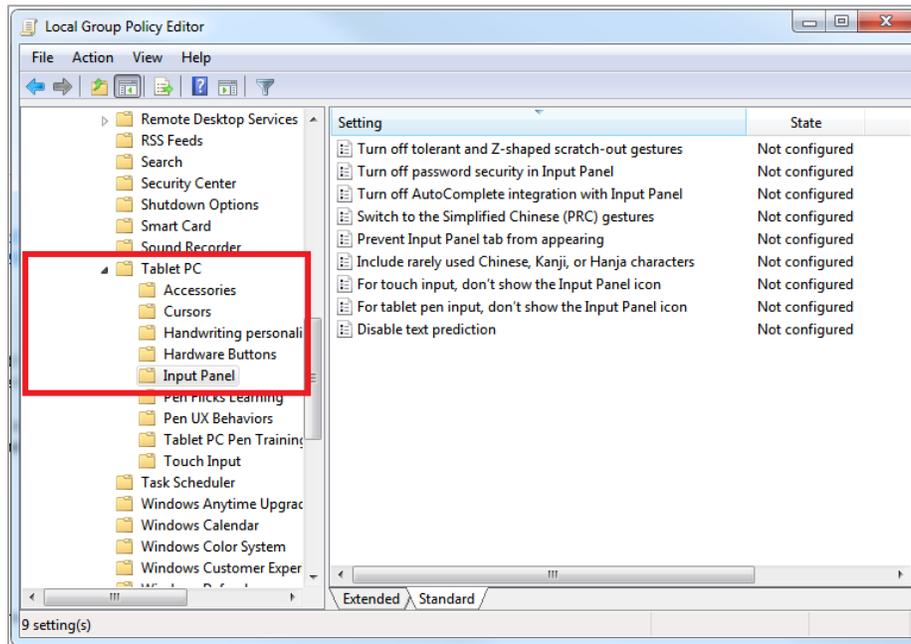


Figure 6. Input Panel in the Local Group Policy Editor

4. Double-click to select the **[Input Panel]** icon, which is also indicated in [figure 6](#).

5. In the Input Panel group, select a policy setting to view its description or double-click it to change its state; current policy settings are shown in the *State* column, indicated in [\(figure 7\)](#).

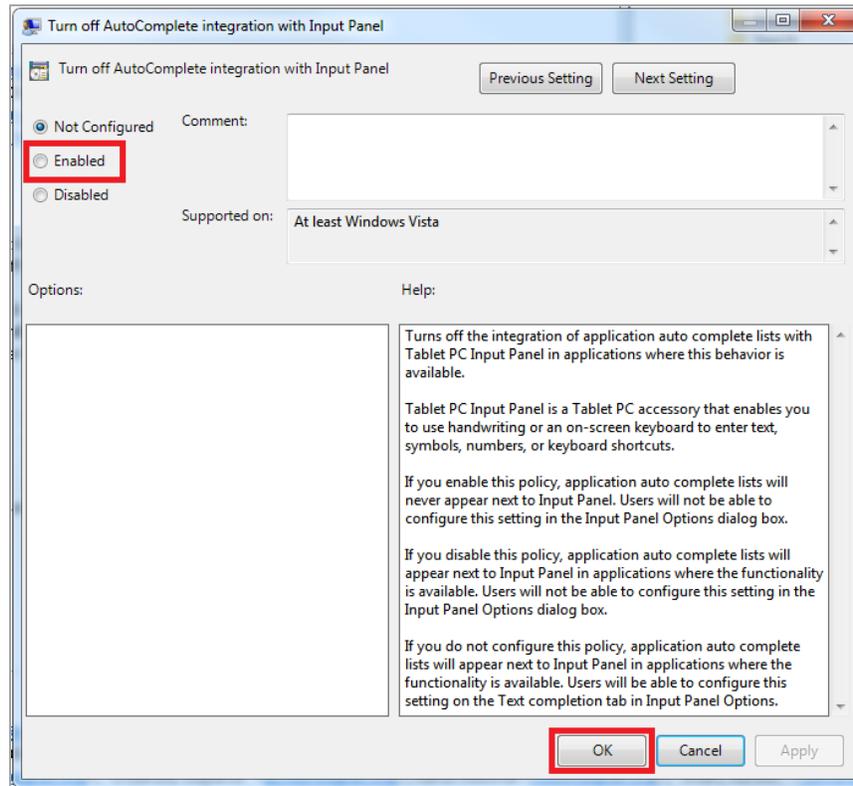


Figure 7. Disable text prediction screen

6. To enable (turn off) an item, double-click on that item in the *Setting* column to open the *Disable [policy setting]* dialog box, which is shown in [figure 7](#) for the setting “Turn off AutoComplete integration with Input Panel.” The following settings should be enabled:
 - a. Turn off AutoComplete integration with Input Panel
 - b. Prevent the **[Input Panel]** tab from appearing
 - c. For tablet pen input, do not display the **[Input Panel]** icon
 - d. For touch input, do not show the **[Input Panel]** icon
 - e. Disable text prediction

7. To enable the setting, select the *Enabled* radio button, and then select **[OK]**. This dialog box also gives the user the option to disable the setting. Select **[Apply]** and then the **[Next Setting]** or **[Previous Setting]** button to move to the next or previous item displayed in the “Settings” list.
8. Close the Local Group Policy Editor.

Configuring the Touch Keyboard on Microsoft Surface Pro Tablet

Some students using Surface Pro tablets and accessing the touch keyboard may have the touch keyboard disappear when they select outside a text box while testing or when they type an answer into a text box and then select **[Next]**. Then, the touch keyboard fails to reappear when they select inside the next text box. To avoid these issues, a student’s touch keyboard must be set to show up automatically.

When following these instructions, note that the settings for the device the user is configuring may be slightly different than those in the figure due to user interface changes by the manufacturer.

To set the touch keyboard to show up automatically:

1. Access the device’s Settings (which can be done on devices using Windows 8.1 and above by using the keyboard shortcut **[Windows] + [I]**).
2. Select **[Devices]** (indicated in [figure 8](#)).

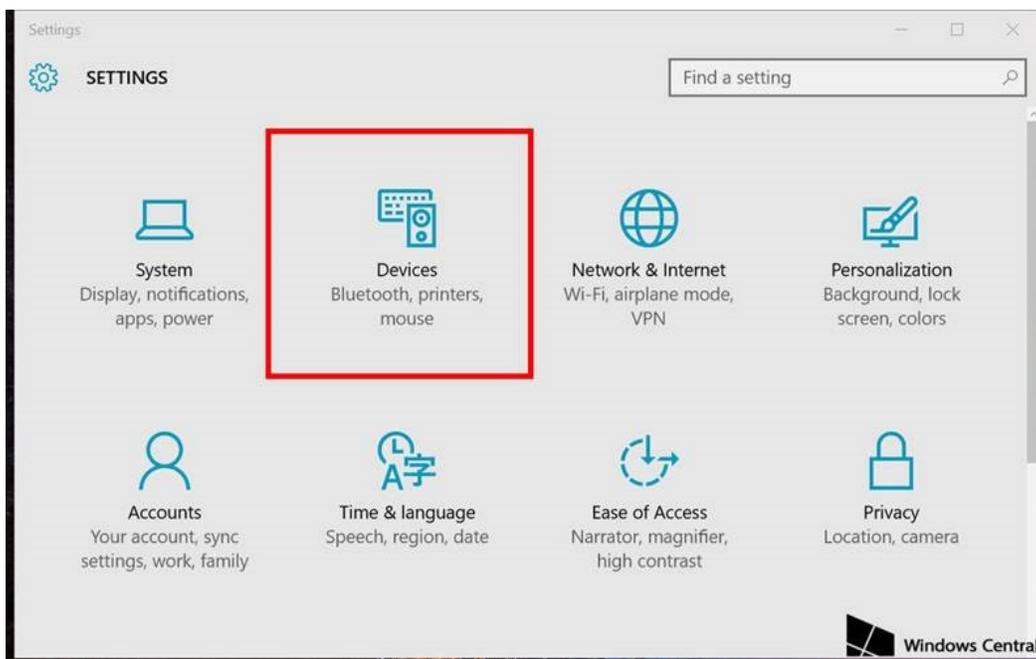


Figure 8. Surface Pro 3 Settings interface

3. Select *Typing* from the left pane (shown in [figure 9](#)).

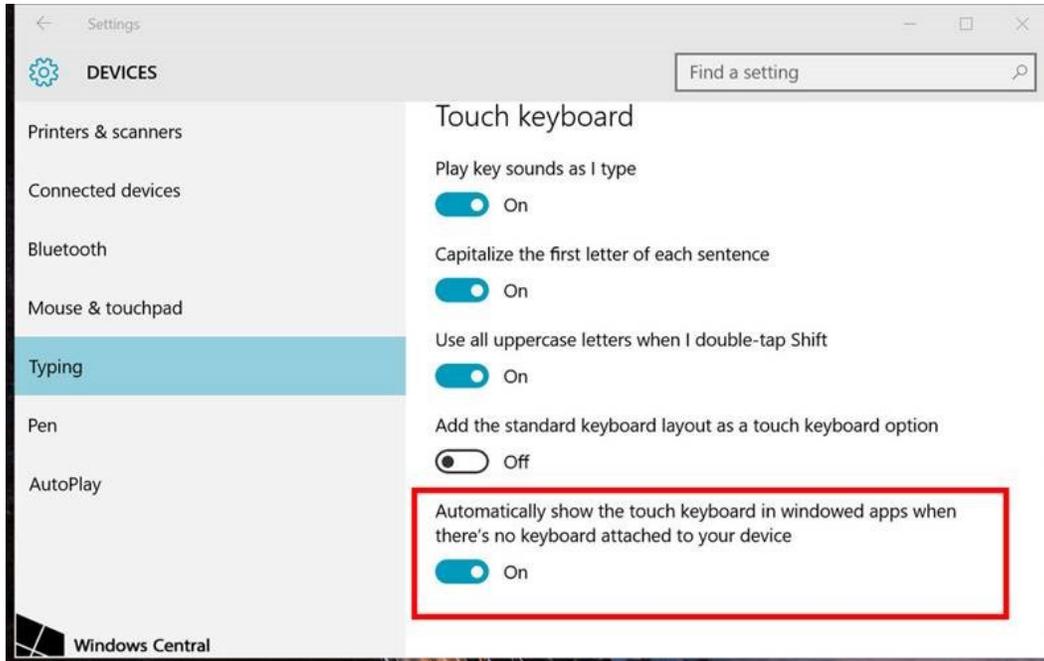


Figure 9. Touch keyboard settings interface

4. Scroll down and toggle on *Automatically show the touch keyboard in windowed apps when there's no keyboard attached to your device*, which is indicated in [figure 9](#). (Depending on the version of Windows that is running, the text might alternatively read *Show the touch keyboard or handwriting panel when not in tablet mode and there's no keyboard attached*.)

Disabling the Two-finger Scrolling Feature in HP Stream Notebooks with Synaptics TouchPad

The trackpad software on the HP Stream notebooks can cause the secure browser to close and display an “environment not secure” error. This can occur when a student tries to use the advanced trackpad features such as scrolling gesture. The Synaptics TouchPad driver is the driver that allows full use of all trackpad features. To avoid this error and having the student exited from the secure browser, disable the TouchPad two-finger scrolling feature.

To disable the TouchPad feature in HP notebooks with Synaptics TouchPad:

1. Select the Start menu [] and then type `mouse` in the *Search programs and files* field.

2. Select *Mouse* from the list of options to open the *Mouse Properties* dialog box (figure 10).

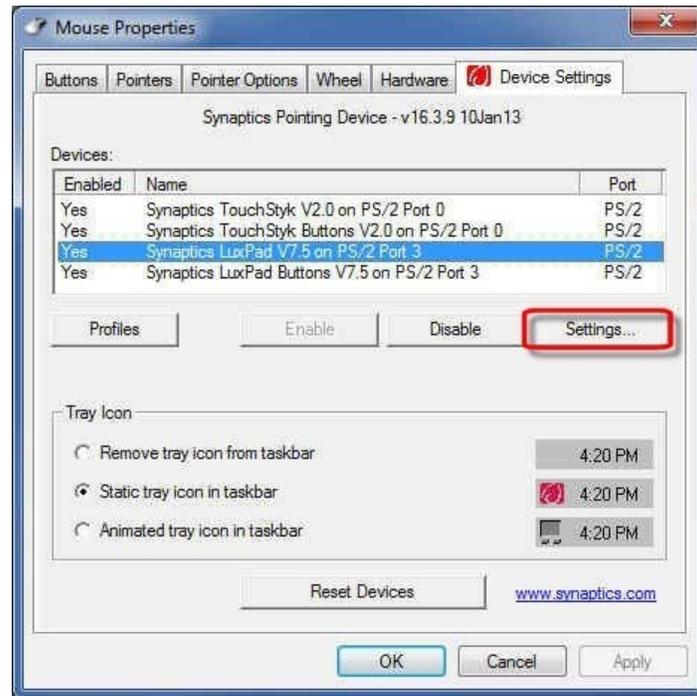


Figure 10. Mouse Properties dialog box

3. Select the [Device Settings] tab.
4. From the *Devices* list, select *Synaptics LuxPad V7.5* and then select [Settings...] (indicated in figure 10).

5. Uncheck the *Two-Finger Scrolling* box, which is indicated in [figure 11](#).

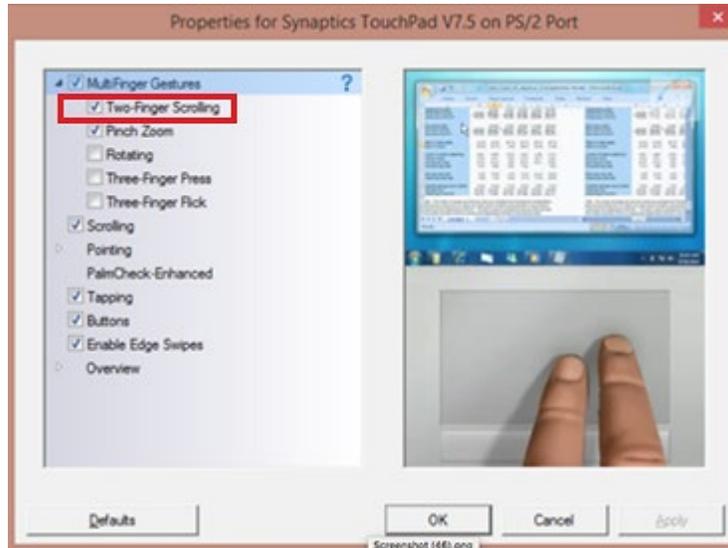


Figure 11. Properties for Synaptics TouchPad V7.5 on PS/2 Port dialog box

6. Select [**C**lose] and then [**O**K].
7. In the *Mouse Properties* dialog box, select [**A**pply].

Configuring ZoomText to Recognize the Secure Browser

When displaying a test with a print-size accommodation above 4x magnification, the secure browser automatically enters streamlined mode. To retain the standard layout of a test but display it with a print magnification above 4x, then consider using ZoomText, a magnification and screen-reading software that can be used with the secure browser.

To ensure ZoomText recognizes the secure browser:

1. If ZoomText is running, close it.
2. Go to the installation directory for ZoomText in Windows Explorer. For example, with ZoomText version 10.1:
 - C:\Program Files (x86)\ZoomText 10.1\ (Windows 64-bit)
 - C:\Program Files\ZoomText 10.1\ (Windows 32-bit)
3. In a text editor, open the file ZoomTextConfig.xml.
4. Search for line containing the D2DPatch property, similar to the following:

```
<Property name="D2DPatch" value="*,~dwm,
~firefox,~thunderbird"/>
```

5. In the value attribute, add a value to represent the California secure browser:

```
<Property name="D2DPatch" value = " *, ~dwm,  
~firefox, ~CAsecurebrowser, ~thunderbird" />
```

6. Save the file.
7. Restart ZoomText.

Disabling Automatic Volume Reduction

A feature in Windows automatically lowers or mutes the volume of some apps if Windows detects audio recording.

To disable automatic volume reduction in Windows:

1. Select **[Start]**.
2. Access "Sound." One way to do this is to navigate to *Control Panel* → *Sound*. This interface is shown in [figure 12](#).

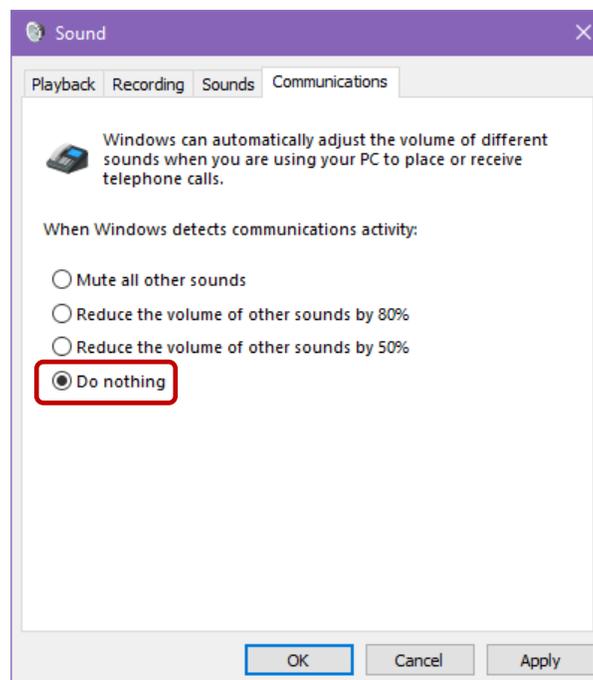


Figure 12. Control Panel *Sound* interface

3. Select the **[Communications]** tab.
4. By default, the selected option is *Reduce the volume of other sounds by 80%*. Change this to *Do nothing* (indicated in [figure 12](#)).
5. Select **[OK]**.

Disabling Fast User Switching in Windows

Microsoft Windows versions 8.0, 8.1, and 10 have a “Fast User Switching” feature that allows more than one user to be logged on at the same time. This is a security risk because students can potentially start a new Windows session during the test and use that session to search the internet for answers, pausing the test in the meantime. The following subsections describe how to disable Fast User Switching for Windows, if it is enabled.

Disabling Fast User Switching in Windows 8.0 and 8.1

To disable Fast User Switching under Windows 8.0 and 8.1:

1. In the Search charm, type `gpedit.msc` ([figure 13](#)).



Figure 13. Windows 8.0 and 8.1 Search charm

2. Double-click the [gpedit] icon in the Apps pane. The *Local Group Policy Editor* screen opens.
3. Navigate to *Computer Configuration* → *Administrative Templates* → *System* → *Logon*.
4. In the Setting pane, double-click *Hide entry points for Fast User Switching* (indicated in [figure 14](#)).

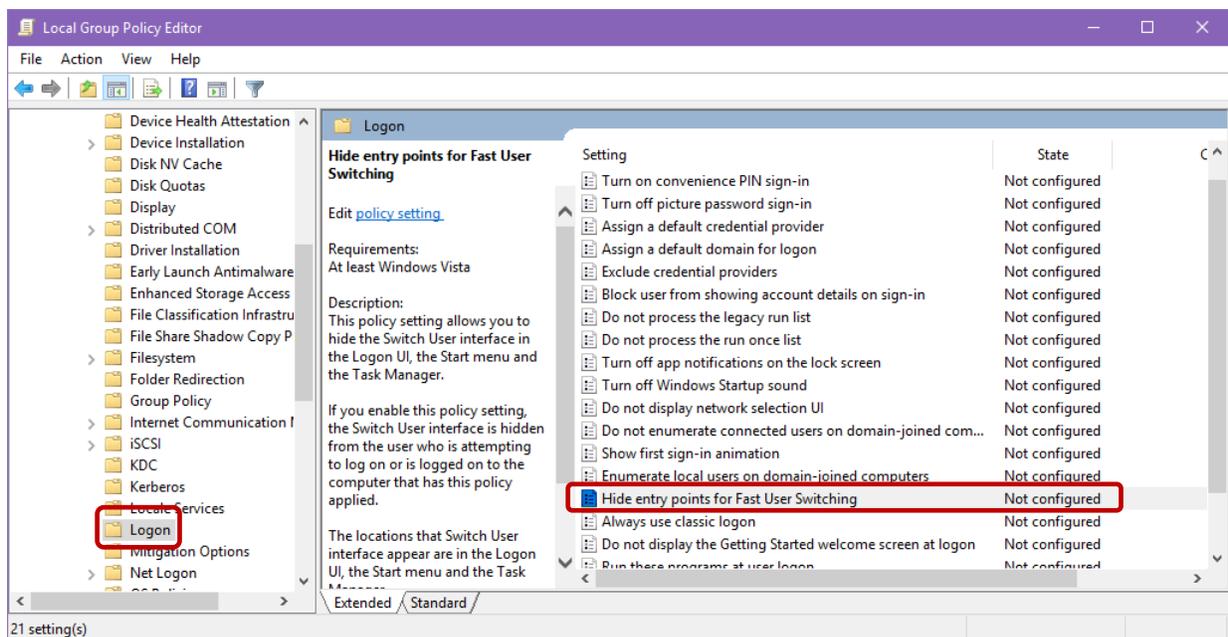


Figure 14. Windows 8.0 and 8.1 Local Group Policy Editor options

5. Select the *Enabled* radio button, and then select [OK]. Both are indicated in [figure 15](#).

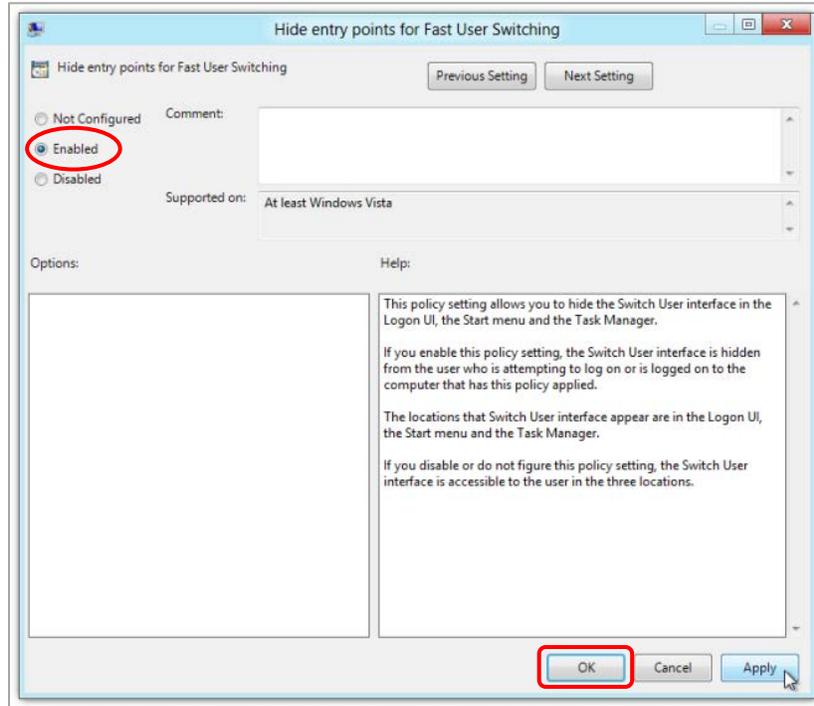


Figure 15. Windows 8.0 and 8.1 Local Group Policy Editor selection

6. In the Search charm, type `run`.
7. Select the [Run] icon in the Apps pane. The *Run* dialog box opens.
8. Enter the command `gpupdate /force` into the *Run* dialog box and then select [OK] ([figure 16](#)). (Note the space before the forward slash.)

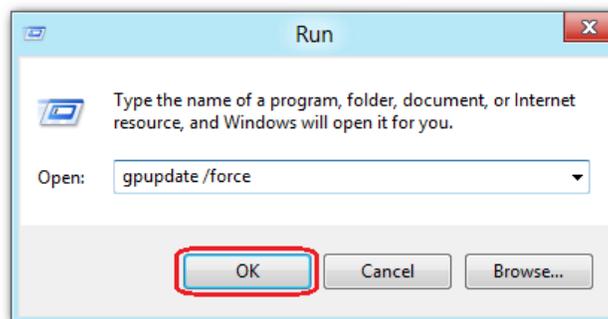


Figure 16. Windows 8.0 and 8.1 Run dialog box

9. The *Command* window opens ([figure 17](#)). The message Computer Policy update has completed successfully is the notification that Windows has successfully disabled Fast User Switching.

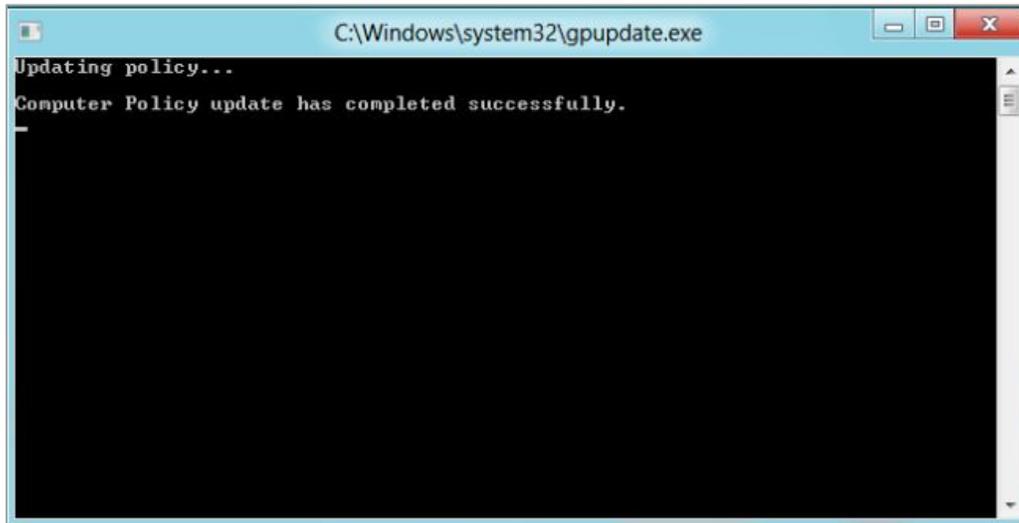


Figure 17. Notification in the Windows 8.0 and 8.1 *Command* window

Disabling Fast User Switching in Windows 10

To disable Fast User Switching under Windows 10:

1. In the task bar Search box, type `gpedit.msc` ([figure 18](#)) and then press the [Enter] key. The *Local Group Policy Editor* screen opens.

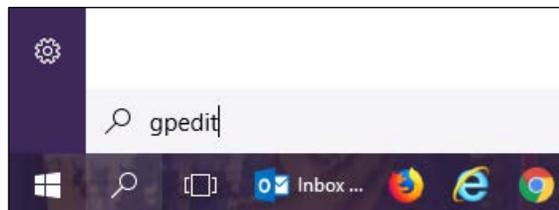


Figure 18. Windows 10 Search box

2. Navigate to Local Computer Policy → Computer Configuration → Administrative Templates → System → Logon.

- In the Setting pane, double-click *Hide entry points for Fast User Switching* (indicated in [figure 19](#)).

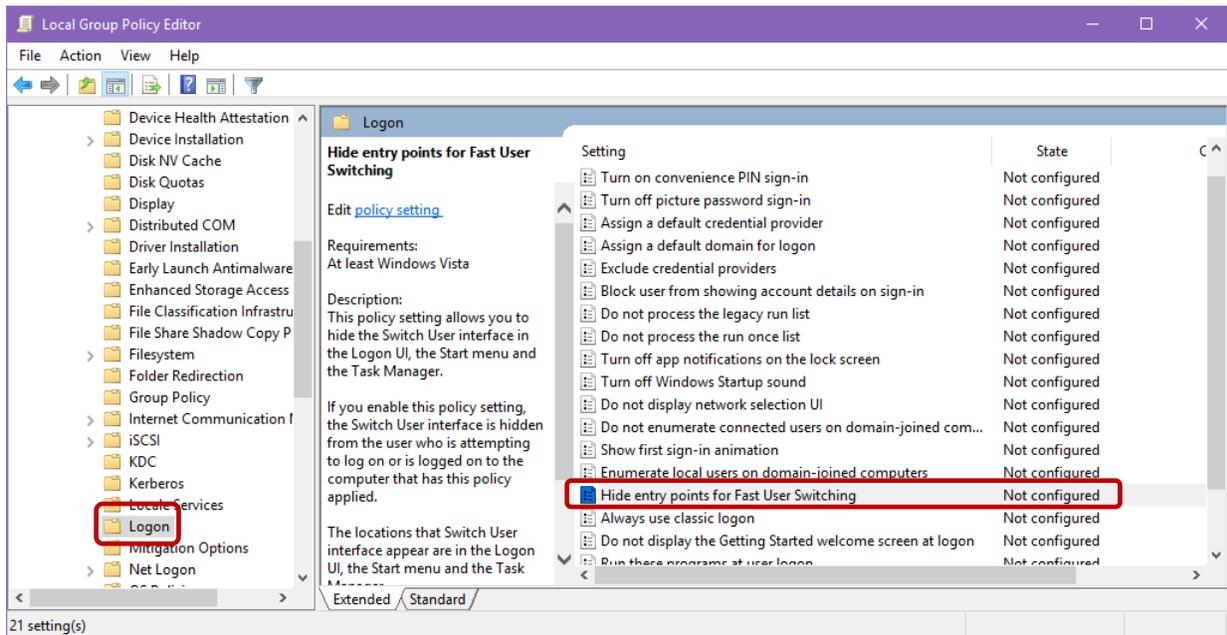


Figure 19. Windows 10 Local Group Policy Editor options

4. Select the *Enabled* radio button, and then select [OK]. Both are indicated in [figure 20](#).

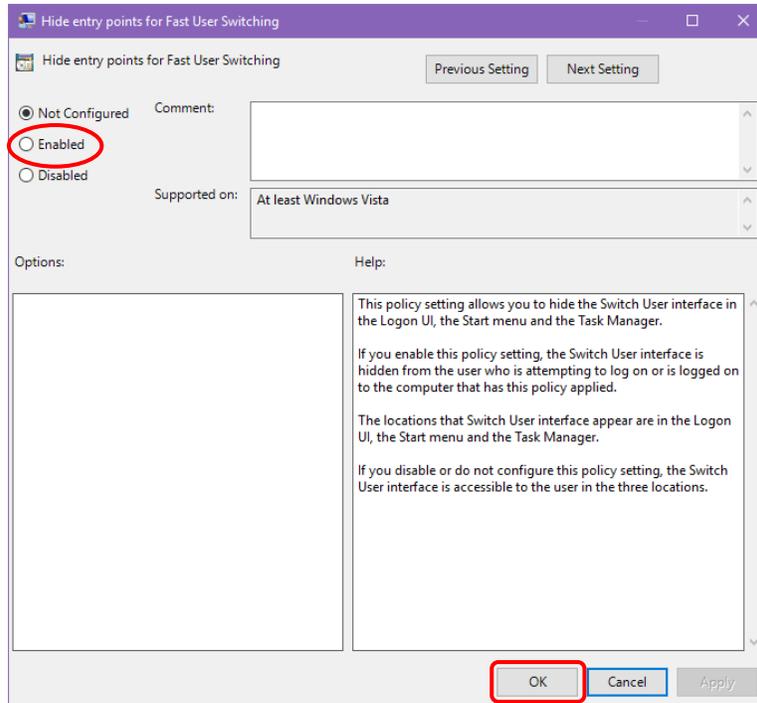


Figure 20. Windows Local Group Policy Editor selection

Disabling Task Manager

The Windows Task Manager allows users to switch to applications running in the background. This is a security risk because students can switch to other applications while running the secure browser. Disable the Task Manager in Windows 8.0, 8.1, and 10 before the start of testing to mitigate this risk.

To disable the Task Manager using the Local Group Policy Editor:

1. In the task bar *Search* box, type `gpedit.msc` ([figure 21](#)) and then press the [Enter] key. (This is the *Search* box in Windows 10.) The *Local Group Policy Editor* screen appears.

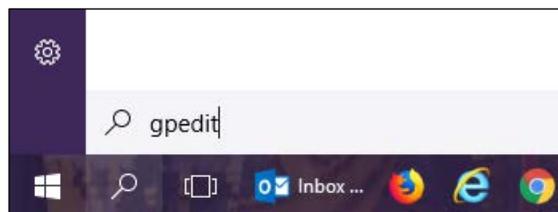


Figure 21. Windows 10 Search box

- Navigate to *User Configuration* → *Administrative Templates* → *System* → *Ctrl+Alt+Del Options* ([figure 22](#)).

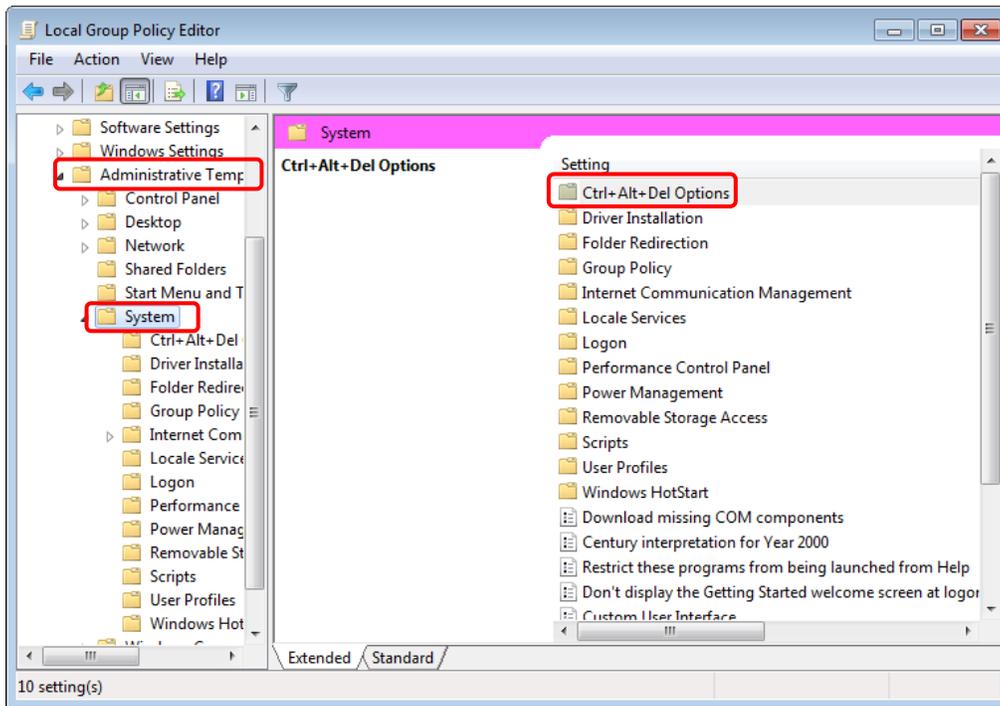


Figure 22. Local Group Policy Editor screen options

- Double-click *Ctrl+Alt+Del Options* and then *Remove Task Manager* (indicated in [figure 23](#)).

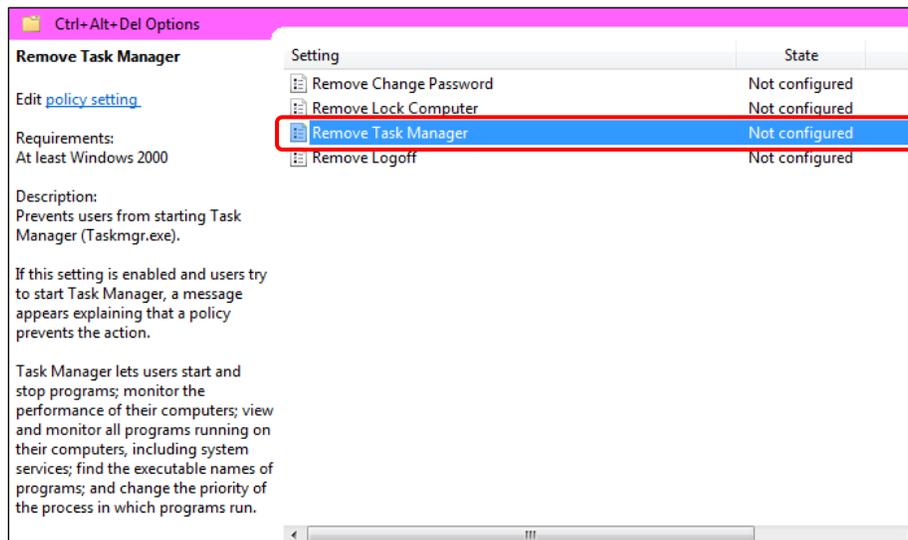


Figure 23. Ctrl+Alt+Del Options settings

4. Select the *Enabled* radio button in the *Remove Task Manager* dialog box shown in [figure 24](#), and then select [OK].

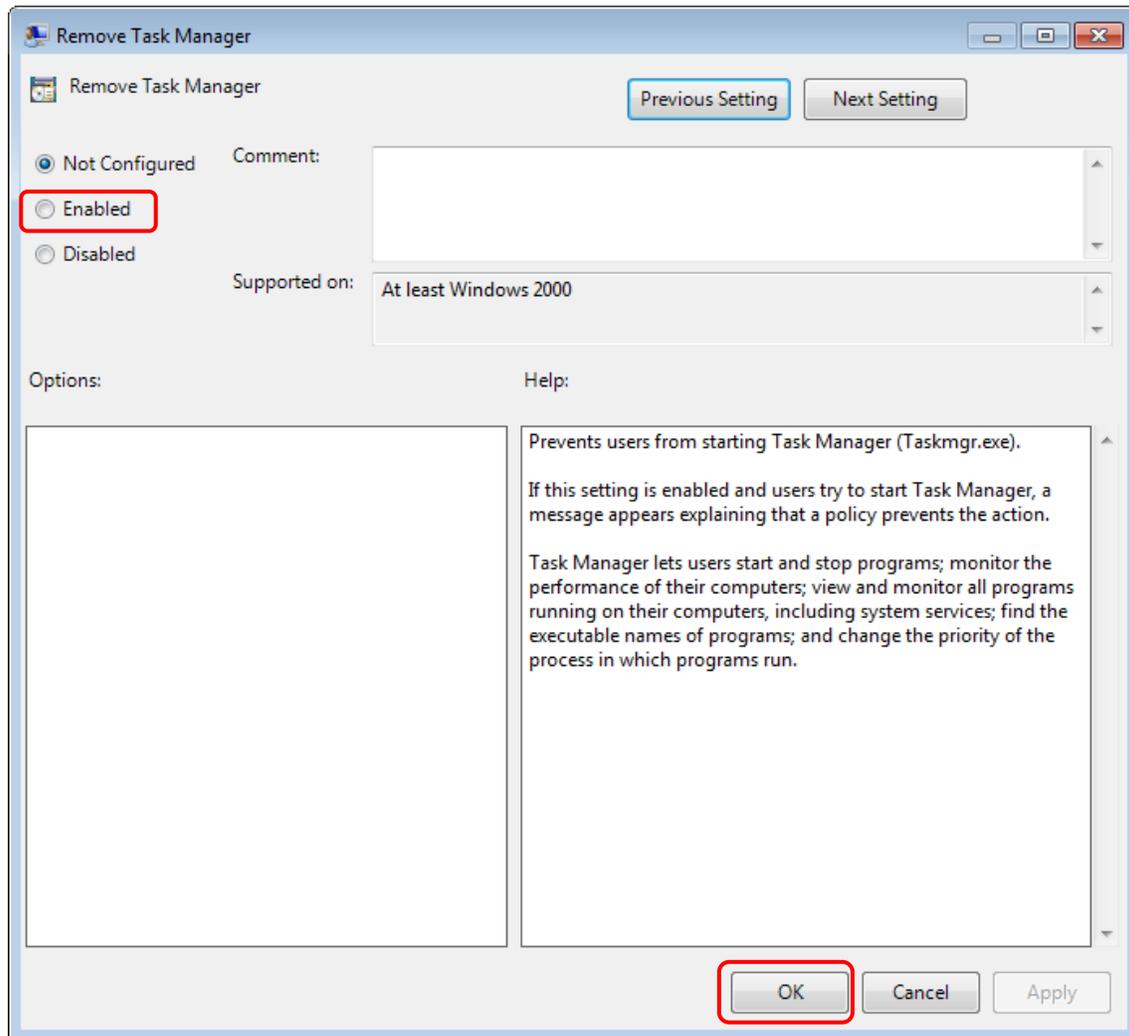


Figure 24. Remove Task Manager screen

5. Close the Local Group Policy Editor.

Disabling App Prelaunching in Windows 10



Note: The circumstance described in this subsection applies to Windows 10 users running the Microsoft Take a Test app to access the test delivery system (TDS). This does not affect users running the CAI secure browser.

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 app directly. If these forbidden apps are running in the background, a student can be unable to start the Take a Test app or will be exited from the TDS if an app launches while the Take a Test app is running.

App prelaunching can be disabled by using a PowerShell command and editing the registry. For instructions on how to disable app prelaunching, refer to the Microsoft Windows support topic, "[K-12 assessment unexpectedly reports apps running in the background in Windows 10.](#)"

MacOS Testing Device Configuration



Additional Resources in This Subsection:

- CAASPP and ELPAC Secure Browsers website—
<https://ca.portal.cambiumast.com/>
- Apple's Set up iPad and Mac to give tests and assessments support web page—
<https://support.apple.com/en-us/HT204775>

This subsection describes how to configure macOS devices for online testing.

Additionally, a feature in MacOS called Assessment Mode works with the CAI secure browser to lock down Mac device for online testing. Users in the field need to do nothing to set up Assessment Mode. Once the secure browser is launched, Assessment Mode starts automatically. For more information about Assessment Mode, including a list of features it disables, refer to Apple's [Set up iPad and Mac to give tests and assessments support](#) web page.

Several features on Mac workstations must be disabled before testing begins. Installing the Mac Secure Profile disables the hot keys for enabling Dictation, Mission Control, Spaces, Screenshots, and Dictation, as well as the trackpad gestures for accessing Lookup, Space Switching, App Exposé, Launchpad and Show Desktop. It also sets function keys to standard functions for all users of the deployed Mac, disables Voice Control, and disables the menu pop-up that appears when triple-tapping the power button on Touch Bar-enabled devices. Without Secure Profile, these settings must be disabled manually. As a result, technology coordinators are recommended to download and install the updated Secure Profile for Mac.

Following installation of the Secure Profile, users will need to disable third-party app updates, iTunes updates, and Fast User Switching, all of which are detailed in this section.

Installing the Mac Secure Profile

The Mac Secure Profile is a script that can be used to configure Mac workstations for online testing. The profile can be downloaded from the [CAASPP and ELPAC Secure Browsers](#) website. Because the Secure Profile configures the operating system regardless of the operating system's current settings, there is no configuration profile to roll back the changes. Instead, a device profile's preferences and settings should be backed up prior to installation. Once the device is no longer used for testing, the profile can be removed and the original settings can be reapplied.

To revert configurations made by the Secure Profile without a backup of the device profile's preferences and settings prior to installation, the features that were suppressed must be reenabled manually through System Preferences.

To download and install the Mac Secure Profile:

1. Select the [here] link in the "Download the Secure Profile" section on the Mac tab of the [CAASPP and ELPAC Secure Browsers](#) website to download the Mac Secure Profile ([figure 25](#)).



Figure 25. "Download the Secure Profile" section

2. Run the Mac Secure Profile installer.
3. Upon installation, restart the computer.

Disabling Fast User Switching

Fast User Switching is a feature in macOS X 10.11 and higher that allows for more than one user to be logged on 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. The following instructions describe how to disable Fast User Switching.

1. Choose the *Apple* menu → *System Preferences*.

2. Select the **[Users & Groups]** option (indicated in [figure 26](#)).

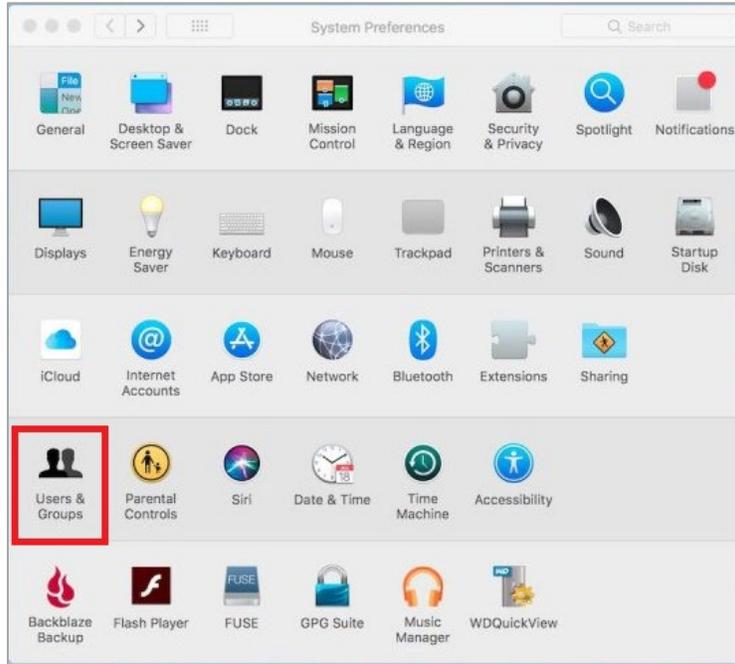


Figure 26. [Users & Groups] button in macOS System Preferences

3. If the padlock in the lower left corner of the *Users & Groups* is locked as indicated in [figure 27](#), select it and authenticate with administrator credentials.

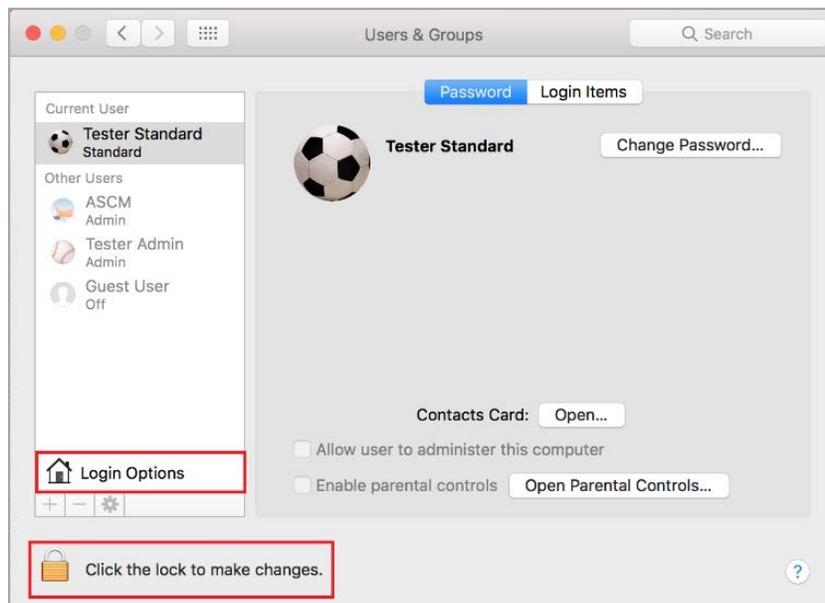


Figure 27. Users & Groups window

4. Select the **[Login Options]** button to open the *Login Options* window ([figure 28](#)).

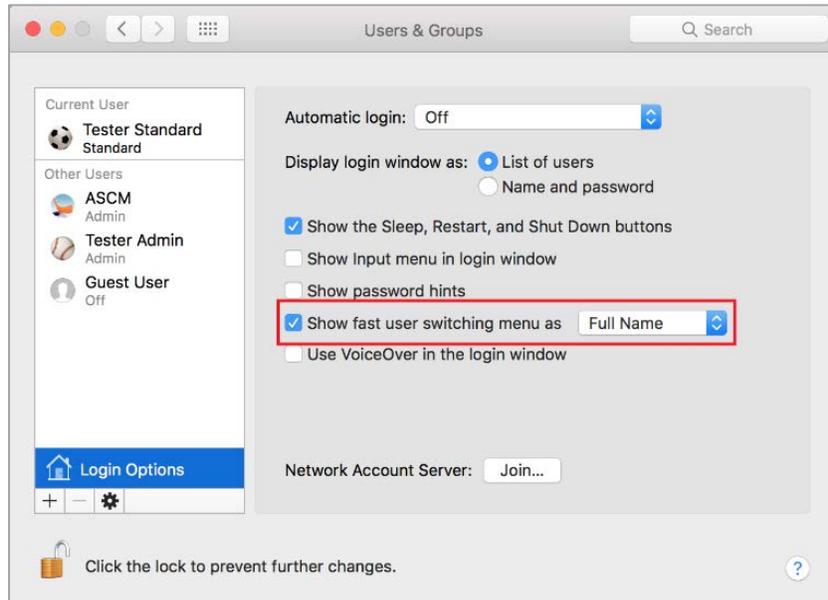


Figure 28. Login Options window

5. Uncheck the *Show fast user switching menu as...* box to disable Fast User Switching. Its icon will no longer appear in the menu bar.

Disabling the Text-to-Speech Keyboard Shortcut

A feature in macOS 10.12 and later allows users to have any text on the screen read aloud by selecting the text and hitting a preset key or set of keys on the keyboard. By default, this feature is disabled and must remain disabled so as not to compromise test security. These instructions describe how to toggle this feature.

1. Choose the *Apple* menu → *System Preferences*.

2. Select the **[Accessibility]** option (indicated in [Figure 29](#)).

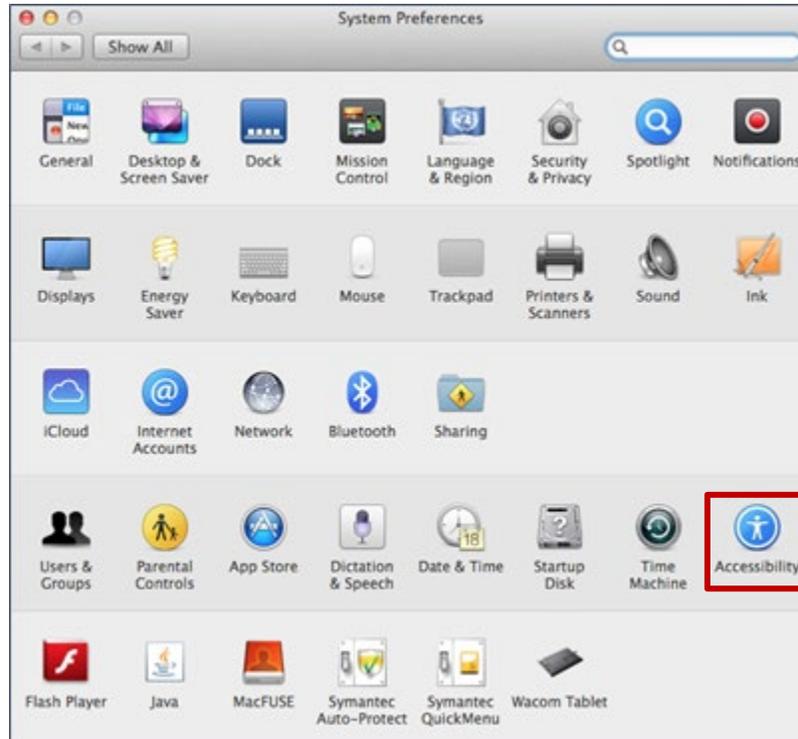


Figure 29. [Accessibility] button in macOS System Preferences

3. Select **[Speech]**
4. Uncheck the *Speak selected text when the key is pressed* box.

Disabling iTunes Updates Manually

Disable updates to iTunes prior to testing. If iTunes updates pop up during a test, the secure browser will pause the test and the student will be disconnected from the testing session.

The following instructions are based on macOS 10.13; similar instructions apply for other versions of OS X and macOS.

To disable updates to iTunes:

1. Log on to the student's account.
2. Start iTunes.
3. Select *iTunes* → *Preferences*.

- Under the **[Advanced]** tab, clear the *Check for new software updates automatically* checkbox ([figure 30](#)).



Figure 30. Advanced Preferences options

- Select **[OK]**.

Disabling Third-Party Apps Updates Manually

Updates to third-party apps may include components that compromise the testing environment. This subsection describes how to disable updates to third-party apps.

The following instructions are based on OS X 10.9; similar instructions apply for other versions of OS X and macOS.

To disable updates to third-party apps:

1. Log on to the student's account.
2. Choose the *Apple* menu → *System Preferences*. The *System Preferences* dialog box opens ([figure 31](#)).

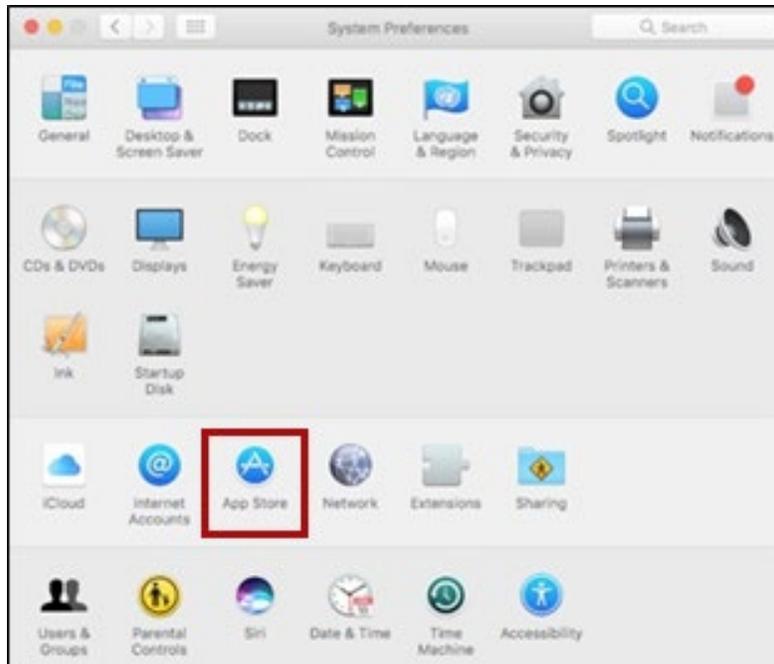


Figure 31. Apple System Preferences dialog box

3. Select the [App Store] icon. The *App Store* screen opens ([figure 32](#)).

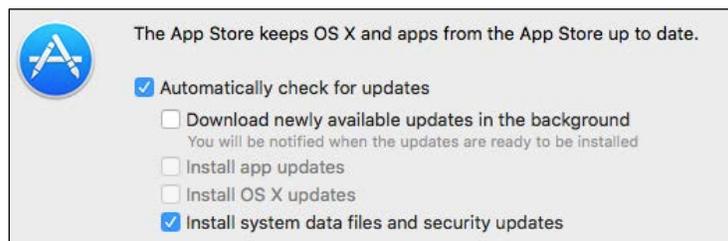


Figure 32. App Store screen

4. Check the *Automatically check for updates* box.
5. Clear the *Download newly available updates in the background* checkbox.
6. Clear the *Install app updates* checkbox.
7. Check the *Install system data files and security updates* box.

Linux Testing Device Configuration



Caution: On Linux systems, all keyboard shortcuts are disabled while taking an assessment with the secure browser. In the event of an abnormal browser exit, those shortcuts will be reset to the default state they were in before the exit, so would need to be reconfigured after the device has been used for testing.

This subsection describes how to configure Linux devices for online testing.

Libraries and Packages

Required for 32-bit and 64-bit Workstations

The following libraries and packages are required to be installed on all 32-bit and 64-bit Linux workstations:

- 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

Required for 64-bit Workstations Only

The following libraries and packages are required to be installed on all 64-bit Linux workstations in addition to the packages required for both 32-bit and 64-bit workstations:

- Sox
- Net-tools

Recommended for 32-bit and 64-bit Workstations

The following libraries and packages are recommended to be installed on all 32-bit and 64-bit Linux workstations:

- NetworkManager 0.7 or higher
- Dbus 1.0 or higher
- HAL 0.5.8 or higher

Adding the Verdana Font



Additional Resources in This Subsection:

- SourceForge: An easy way to install Microsoft's TrueType core fonts on linux web page—<http://corefonts.sourceforge.net/>

Some tests have content that requires the Verdana TrueType font. Therefore, ensure that Verdana is installed on Linux devices used for testing. The easiest way to do this is to install the Microsoft core fonts package for distribution.

- Fedora—Follow the steps in the “How to Install” section of the instructions on the [An easy way to install Microsoft's TrueType core fonts on linux](#) web page.
- Ubuntu—In a terminal window, enter the following command to install the msttcorefonts package:

```
sudo apt-get install msttcorefonts
```

Disabling the On-Screen Keyboard

Fedora and Ubuntu feature an on-screen keyboard that should be disabled before online testing. To disable the on-screen keyboard:

1. Open System Settings.
2. Select **[Universal Access]**.
3. In the “Typing” section, toggle *Screen Keyboard* to “off.”

iOS or iPadOS Testing Device Configuration

This subsection describes how to configure Apple mobile devices for online testing.

Using Assessment Mode



Additional Resources in This Subsection:

- Apple's Set up iPad and Mac to give tests and assessments support web page—<https://support.apple.com/en-us/HT204775>



Caution: Apple strongly recommends that schools use Assessment Mode to prepare iPads for online testing.

If students are using iPads with iOS or iPadOS, use Assessment Mode. This configuration includes a preset profile in the SecureTestBrowser app that automatically suppresses the features listed in [table 6](#). Assessment Mode works with the CAI secure browser to lock down an iPad for online testing. Users in the field need to do nothing to set up Assessment Mode.

Once the secure browser is launched, Assessment Mode starts automatically. For more information about Assessment Mode, including a list of features it disables, refer to Apple's [Set up iPad and Mac to give tests and assessments support](#) web page.

When a student taps **[Begin Test Now]** on an iPad with Assessment Mode, a message similar to that in [figure 33](#) appears.

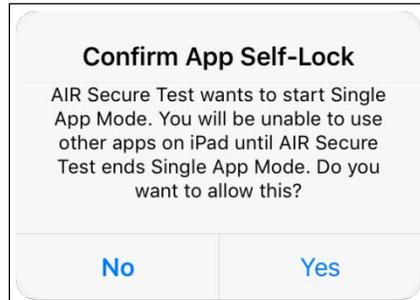


Figure 33. Notification when starting test with assessment mode

Removing the Emoji Keyboard from an iOS or iPadOS Device

Emoticons are characters that express an emotion or represent a facial expression, such as a smile or a frown. Some text messaging apps replace sequences of characters with an emoticon, such as replacing “:)” with “☺.”

iOS has an Emoji keyboard that contains emoticons ([figure 34](#)). This keyboard, if activated, can be confusing for test takers or scorers. Use the following procedure to remove the Emoji keyboard from an iOS or iPadOS device.

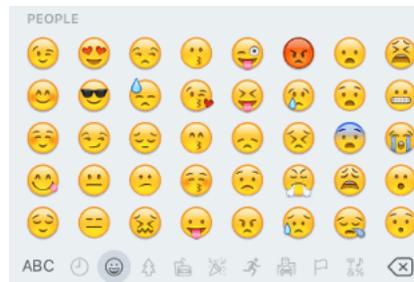


Figure 34. Emoji keyboard for iOS or iPadOS

To remove the Emoji keyboard:

1. Tap the **[Settings]** icon ([figure 35](#)).



Figure 35. [Settings] icon

2. Navigate to *General* → *Keyboard*.
3. Tap the [**Keyboards**] icon.
4. Delete *Emoji* from the list by sliding it to the left ([figure 36](#)).

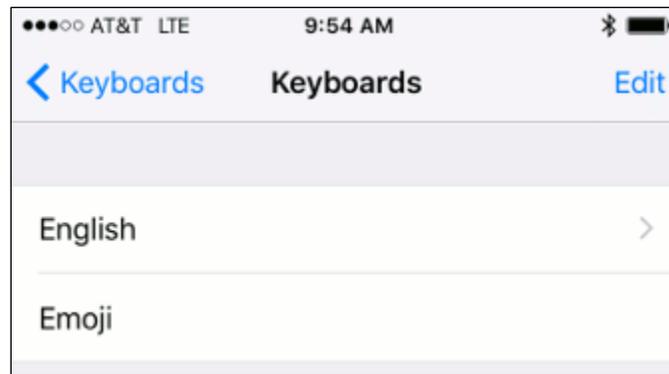


Figure 36. Keyboards configuration interface

Disabling Dictation

When students speak into an Apple mobile device, utilizing the Dictation feature that suggests words or spellings, they may compromise testing security or violate the construct of the assessment.

Take these steps to disable Dictation in an Apple device:

1. Tap the [**Settings**] icon.
2. Navigate to *General* → *Keyboard*.
3. Move the slider to turn off *Enable Dictation* ([figure 37](#)).



Figure 37. Disabled dictation

Disabling Keyboard Functions

Disable keyboard functions by taking the following steps:

1. Under Settings, tap *General* → *Keyboard*.
2. Turn off all settings ([figure 38](#)).

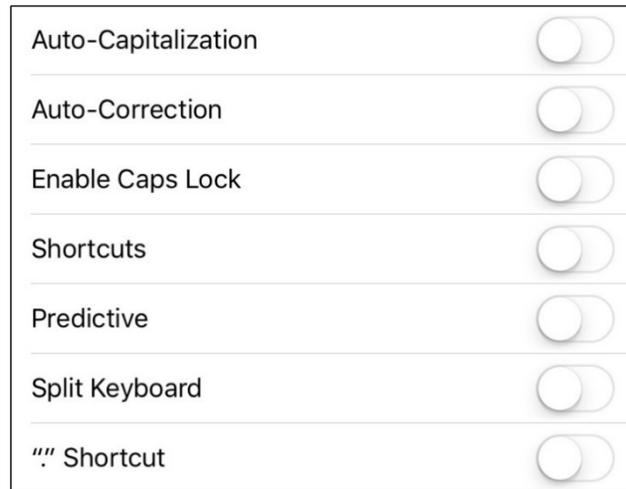


Figure 38. Keyboard Settings for iOS (other versions of iOS or iPadOS are similar)

Chromebook Mobile Testing Device Configuration

This subsection describes how to configure Chromebook mobile devices for online testing.

Disabling Auto Updates for Chrome OS

Additional Resources in This Subsection:

- Google Set Chrome device policies web page—
<https://support.google.com/chrome/a/answer/1375678>

A user may want to disable auto updates during the LEA's or test site's selected testing window to avoid unknown issues that may be introduced by future operating system updates (although versions of Chrome are presumed to be supported). For example, if Cambium Assessment, Inc. (CAI) supports up to Chrome OS version 75, and version 76 is installed on students' Chromebooks, a user can prevent auto updates to any later version. (Alternatively, a user can allow auto updates to a specific version supported by CAI; for details, refer to the next subsection "[Limiting Chrome OS Updates to a Specific Version for Managed Chrome Devices.](#)")

To disable auto updates for Chrome OS:

1. Display the *Device Settings* page by following the procedure in the [Set Chrome device policies](#) web page. The steps in that procedure assume that the Chromebooks are managed through the admin console.
2. From the *Auto Update* list, select *Stop auto-updates*.
3. Select [**Save**].

Limiting Chrome OS Updates to a Specific Version for Managed Chrome Devices

CAI has tested the operational software being used (such as the Test Administrator Interface) and the practice and training tests up to version 85 of the Chrome OS; a user may want to prevent a Chromebook from auto-updating beyond that version. (Alternatively, a user can disable auto updates entirely; for details, refer to the subsection “[Installing the SecureTestBrowser Kiosk App on Managed Chromebooks.](#)”)

To limit Chrome OS updates to a specific version:

1. Display the Device Settings page by following the procedure in the Google [Set Chrome device policies](#) web page. The steps in that procedure assume that Chromebooks are managed through the admin console.
2. From the *Auto Update* list, select *Allow auto-updates*.
3. From the *Restrict Google Chrome version to at most* list, select the required version.
4. Select [**Save**].

Configuring Network Settings for Online Testing

Local area network (LAN) settings on testing devices should be set to automatically detect network settings.

Windows Devices

Take the following steps to set LAN settings to auto detect on Windows devices:

1. Access “Internet Options.” One way to do this is to navigate to *Control Panel* → *Network and Sharing Center* → *Internet Options*.
2. In the *Internet Options* dialog box, select the [**Connections**] tab.
3. Select the [**LAN Settings**] button.
4. Check the *Automatically detect settings* box.
5. Select [**OK**] to close the *Local Area Network (LAN) Settings* dialog box.
6. Select [**OK**] to close the *Internet Options* dialog box.

MacOS Devices

To set LAN settings to auto detect on macOS devices:

1. Choose the *Apple* menu → *System Preferences*.
2. Select [**Network**].
3. Select [**Ethernet**] for wired connections or [**WiFi**] for wireless connections.
4. Select [**Advanced**].
5. Select the [**Proxies**] tab.

6. Check the *Auto Proxy Discovery* box.
7. Select **[OK]** to close the dialog box.
8. Select **[Apply]** to close the *Network* dialog box.
9. Close System Preferences.

Linux Devices

Take the following steps to set LAN settings to auto detect on Linux devices:

1. Open System Settings.
2. Open Network.
3. Select Network Proxy.
4. From the *Method* drop-down list, select *None*.
5. Select *X* to close the *Network* dialog box.

Installing CloudReady on PCs and Macs



Additional Resources in This Section:

- Google Chrome Web Store—<https://chrome.google.com/webstore/>
- Neverware website—<https://www.neverware.com/>
- Neverware Certified Models web page—<https://guide.neverware.com/supported-devices/>

CloudReady is a reduced-feature operating system, built on the same technology as Chrome OS, that runs on devices with limited resources. If the school or LEA has older devices that do not run newer versions of Windows, OS X, or MacOS, consider installing CloudReady on those devices. This installation can postpone or prevent a costly hardware upgrade. Google Management licenses are required to deploy the secure browser kiosk application.



Warning: Process Erases All Data

- The procedure described in this subsection erases all data on the device on which the user is installing CloudReady. Be sure to back up all necessary data before starting this procedure.

To install CloudReady:

1. Ensure the device on which the user is installing CloudReady meets the following requirements. It
 - a. is [supported for use with CloudReady](#);
 - b. has a USB port; and
 - c. can boot from a USB drive.

2. Visit the [Neverware](#) website to purchase a CloudReady license for the device. (Bulk licenses may be available.)
3. If a user receives a USB drive from Neverware with the CloudReady image, proceed to step 18. Otherwise, prepare a bootable image by following steps 4 through 17. Ideally, perform these steps on a device on which the Google Chrome web browser is already installed.
4. Obtain a blank 8 GB USB drive.
5. Install Google Chrome if it is not already installed.
6. In a web browser, go to the URL for the image file provided by Neverware. This URL downloads a file with a name similar to `cloudready_site646.bin`. Note the location of the file on the device.
7. Insert the USB drive into the device.
8. Start Chrome, and then navigate to the [Chrome Web Store](#).
9. Search for the app *Chromebook Recovery Utility* ([figure 39](#)).



Figure 39. Chromebook Recovery Utility

10. Select [**ADD TO CHROME**]; and in the confirmation prompt, select [**Add app**].
11. After installation has completed, select [**Launch App**].
12. Select the gear [⚙️] icon in the top-right corner and then select *Use local image* ([figure 40](#)).

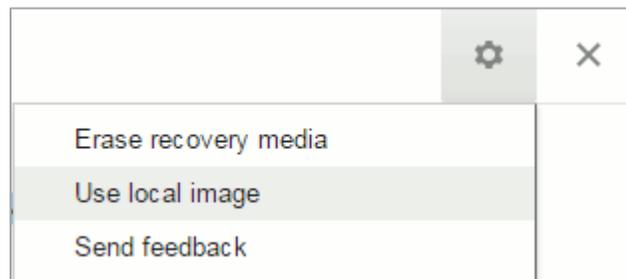


Figure 40. Selecting the CloudReady image

13. Navigate to the file image file downloaded in step 6.
14. At the prompt ([figure 41](#)), select the USB drive inserted in step 7.

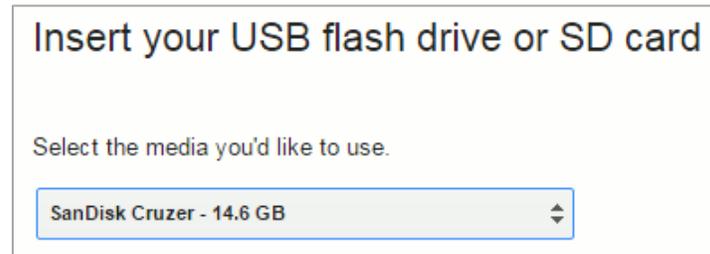


Figure 41. CloudReady media insertion prompt

15. Select [**Continue**].
16. In the next screen, select [**Create Now**]. The recovery utility creates a bootable image of CloudReady on the USB drive. This operation takes 15–30 minutes.
17. When copying is complete, eject the USB drive from the device.
18. On the device where the user is installing CloudReady, do the following:
 - a. Back up all files to be saved. The installation procedure erases all data on the device.
 - b. Boot the device from the USB drive. Booting and installation take 10–15 minutes, depending on the device. When the installation is complete, the device turns off.
 - c. Remove the USB drive and power on the device.
 - d. Install the SecureTestBrowser Kiosk App; refer to [Chapter 4: Secure Browser Configuration](#) for details.

Configurations for Testing Students Using Accessibility Resources

For information about configuring operating systems and software for testing with accessibility resources, including braille, text-to-speech and the NeoSpeech voice pack, and permissive mode, refer to the *CAASPP and ELPAC Accessibility Guide for Online Testing*, which is available on both the CAASPP and ELPAC websites.

Chapter 4: Secure Browser Configuration

Overview of Secure Browsers



Note: Configuration information and specifications for using the secure browser for administering the Initial English Language Proficiency Assessments (ELPAC) remotely will be provided on ELPAC.org as it becomes available.

The information in this section provides an overview of secure browsers and their use with online assessments. The requirement to use the secure browser to administer assessments supports a secure online testing environment, which is a state in which a device is restricted from accessing prohibited computer applications (local or internet-based), or copying or sharing test data. The purpose of this environment is to maintain test security and provide a stable testing experience for students across multiple platforms.

This section includes the following topics:

- [About the Secure Browser](#)
- [Secure Browser Versions for Online Testing](#)
- [Forbidden Application Detection](#)
- [Secure Browser Error Messages](#)

About the Secure Browser

All devices that students will use to access online assessments must have a secure browser installed on that device. The secure browser prevents students from accessing another computer or internet application or copying test information.

The secure browser is available for all major operating systems referenced throughout this guide. Technology coordinators with responsibility for managing a large number of machines across a school or local educational agency (LEA) can likely use the same tools as those used currently to push the secure browser out to all of machines at scale. For example, the secure browser ships as an MSI package that enables use of MSIEXEC.

For iPads and Chromebooks, the SecureTestBrowser app is Cambium Assessment, Inc.'s (CAI's) mobile version of the secure browser. It is available in each app store to download and install. The first time this app is opened, it will ask the user to choose the state and assessment program. The choice is saved and from then on, the mobile secure browser works just like the desktop version, allowing access operational tests, practice tests, and the network diagnostic tool. Any mobile device management utility can be used to install the secure browser on multiple managed devices and configure those devices.

This subsection contains instructions for downloading and installing the secure browsers. The LEA or school information technology staff should ensure that the secure browser has been installed correctly on all computers and devices that will be used for student testing.

While the secure browser is an integral component of test security, test administrators and test examiners perform an equally important role in preserving test integrity. Test

administrators and test examiners should be aware of requirements associated with closing external user applications, turning off background jobs, and testing on computers with dual monitors, and employ the necessary precautions while administering online assessments.

Close External User Applications

Prior to administering the online assessments, all nonrequired applications on computers and devices should be closed. After closing these applications, the secure browser can be launched.

The secure browser will not work if the device detects that a forbidden application is running. For more information, refer to the [“Forbidden Application Detection”](#) subsection.

Turn Off Background Jobs

Ensure and verify that all background jobs, such as virus scans or software auto updates, are scheduled outside of testing windows. For example, if testing takes place between 8 a.m. and 3 p.m., schedule background jobs (e.g., attendance and payroll jobs) outside of these hours.



Warning: Scheduling Background Jobs

- Failure to schedule background jobs for times outside the testing window could result in a student’s being exited from the secure browser during testing should a process begin to run.



Warning: Disabling Auto Update

- It is recommended that all application and operating system software on all devices used for test operations and student testing (in conjunction with the secure browser) be configured to turn auto update features off during testing hours. Refer to the software’s documentation or Help feature to verify the software uses auto update and for instructions on disabling this feature for the duration of the LEA’s or test site’s selected testing window.

Testing on Computers with Dual Monitors



Additional Resource in This Subsection:

- Suggested Guidelines for Physically Distancing Testing Administration web document—<http://www.caaspp.org/rsc/pdfs/Guidance-for-Physical-Distanced-Admin.docx>

Systems that use a dual monitor setup typically display an application on one monitor screen while another application is accessible on the other screen. **This typical dual monitor setup is not allowed under normal circumstances for the California Assessment of Student Performance and Progress and English Language Proficiency Assessments for California.**

However, one-on-one testing is required for the Initial and Summative ELPAC in kindergarten through grade two, parts of the Initial ELPAC for grades three and above, all grades for ELPAC Speaking, and all of the alternate assessments in both the CAASPP and ELPAC administrations. These assessments may call for the test examiner to be close to the student for ease of use and access and to promote the validity of the assessment. In these cases, a dual-monitor configuration may be necessary. Another possible situation for dual monitor use is when a test administrator or test examiner is administering a test via read-aloud and wants to have a duplicate screen to view exactly what the student is viewing for ease of reading aloud.

In these cases where a dual monitor **is allowed, monitors should be set up to “mirror” each other.** One monitor is connected to the computer running the secure browser and the other is its duplicate. School technology coordinators can assist test administrators and test examiners in setting up the two monitors to ensure they mirror each other rather than operate as independent monitors.

In these cases, all security procedures must be followed, and the test must be administered in a secure environment, to prevent others from hearing the questions or viewing the screens for a student, test administrator, or test examiner. Refer to the [Suggested Guidelines for Physically Distancing Test Administration](#) for suggested layouts.

Secure Browser Versions for Online Testing

[Table 13](#) lists the secure browsers for each operating system. A secure browser must be downloaded and installed on each device used for student testing. **LEAs that installed a secure browser with a version older than the versions listed in [table 13](#) must uninstall it before installing the secure browser for the 2020–21 school year.**

Table 13. Secure Browsers by Operating System

Operating Systems	Secure Browser
Windows 8.0 (Professional and Enterprise)	CA Secure Browser 12.5
Windows 8.1 (Professional and Enterprise)	CA Secure Browser 12.5
Windows 10 and 10 in S mode (Professional, Educational, and Enterprise), versions 1809–2004 (upon acceptance)	CA Secure Browser 12.5
Windows Server <ul style="list-style-type: none"> • 2012 R2 • 2016 R2 (thin client) 	CA Secure Browser 12.5
OS X, version 10.11 macOS <ul style="list-style-type: none"> • Versions 10.12–10.15 • Version 10.16 (upon acceptance) 	CA Secure Browser 12.5
Linux Fedora 30–31 LTS (Gnome) (64-bit or 32-bit)	CA Secure Browser 12.5
Linux Ubuntu LTS (Gnome) <ul style="list-style-type: none"> • Version 16.04 (64-bit or 32-bit) • Version 18.04 (64-bit only) • Version 20.04 (64-bit only, upon release and acceptance) 	CA Secure Browser 12.5
iOS or iPadOS <ul style="list-style-type: none"> • Version 12.4 • Version 13.4 • Version 14.0 	SecureTestBrowser Mobile Secure Browser 6.0
Chrome OS 85+	SecureTestBrowser 7.0

Forbidden Application Detection

This feature automatically detects certain applications that are prohibited from running on a computer while the secure browser is open. The secure browser checks the applications currently running on a computer when it is launched. If a forbidden application is detected, the student is denied entry and receives a message indicating the open application. Similarly, if a forbidden application launches while the student is already logged on to an assessment—for example, if a scheduled task or background job begins (e.g., antivirus scans)—the student is automatically logged off and a message is displayed.



Warning: Forbidden Applications and Testing

- If a forbidden application is launched in the background while the student is testing, the student will be automatically logged off and a message displayed. This typically occurs when a process such as a web browser or an antivirus program is triggered in the background for a software auto update to occur. It is recommended to check all software auto updates and ensure that they are scheduled to occur outside of planned testing hours.

Before administering tests, LEA technology coordinators, test administrators, and test examiners should take proper measures to ensure that forbidden applications are not running on student devices.

Installing the Secure Browser on Desktops and Laptops

This section contains installation instructions for Windows and Macintosh systems under a variety of deployment scenarios.

Installing the Secure Browser on Windows

Additional Resources in This Subsection:

- California Assessment of Student Performance and Progress (CAASPP) website—<http://www.caaspp.org/>
- CAASPP and ELPAC Secure Browsers website—<https://ca.portal.cambiumast.com/>
- English Language Proficiency Assessments for California (ELPAC) Technology Resources web page—<https://www.elpac.org/resources/technology-resources/>
- Microsoft Windows IT Pro Center | Take tests in Windows 10 web page—<https://docs.microsoft.com/en-us/education/windows/take-tests-in-windows-10>

This subsection provides instructions for installing the secure browser on computers running on versions 8.0, 8.1, 10, and 10 in S mode. (The secure browser does not run on other versions of Windows.)

The instructions in this subsection assume devices are running a 64-bit version of Windows and that the secure browser will be installed to `C:\Program Files (x86)\`. If a 32-bit version of Windows is running, adjust the installation path to `C:\Program Files\`.

Installing the Secure Browser on an Individual Computer

This subsection contains instructions for installing the secure browser on individual computers.

Installing the Secure Browser via Windows

In this scenario, a user with administrator rights installs the secure browser using standard Windows. (If a user does not have administrator rights, refer to the subsection “[Installing the Secure Browser Without Administrator Rights](#).”)

1. If a user installed a previous version of the secure browser in a location other than a default location—`C:\Program Files (x86)\CASecureBrowser\ (64 bit)` or `C:\Program Files)\CASecureBrowser\ (32 bit)`—manually uninstall the secure browser and its associated desktop shortcut. (If it was installed in the default location,

Secure Browser Configuration | Installing the Secure Browser on Desktops and Laptops

the installation package automatically removes it.) Refer to the instructions in the subsection “[Uninstalling the Secure Browser on Windows.](#)”

2. Navigate to the [CAASPP and ELPAC Secure Browsers](#) web page by going to the [CAASPP](#) website or the ELPAC [Technology Resources](#) web page and selecting the [Secure Browsers] link at either location.
3. Scroll down the [CAASPP and ELPAC Secure Browsers](#) web page to the “Download Secure Browsers” section.
4. Select the [**Windows**] tab and then select the [**Download Browser**] button (shown as highlighted in [figure 42](#)). A dialog box opens.



Figure 42. [Download Browser] button

5. Take one of the following steps; this step may vary depending on the web browser being used:
 - a. If presented with a choice to run or save the file, select [**Run**]. This opens the Secure Browser Setup wizard.
 - b. If presented only with the option to save, save the file to a convenient location. After saving the file, double-click the installation file `CASecureBrowser-Win.msi` to open the setup wizard.
6. Follow the instructions in the setup wizard. When prompted for setup type, select [**Install**].
7. Select [**Finish**] to exit the setup wizard. The following items are installed:
 - The secure browser to the default location `C:\Program Files (x86)\CASecureBrowser\ (64 bit)` or `C:\Program Files\CASecureBrowser\ (32 bit)`
 - A shortcut `CASecureBrowser` to the desktop (shown in [figure 43](#)).



Figure 43. [CASecureBrowser] shortcut icon

8. Ensure all background jobs, such as virus scans or software updates, are scheduled outside of test windows. For example, if testing takes place between 8 a.m. and 3 p.m., schedule background jobs outside of these hours.

9. *Optional:* Apply proxy settings by taking the following steps:
 - a. Right-click the [**CASecureBrowser**] shortcut icon on the desktop and select “Properties.”
 - b. Under the [**Shortcut**] tab, in the *Target* field, modify the command to specify the proxy. Refer to [table 14](#) for available forms of this command.
 - c. Select [**OK**] to close the *Properties* dialog box.

For more information about proxy settings, refer to “[Proxy Settings for Desktop Secure Browsers](#).”

10. Run the secure browser by double-clicking the [**CASecureBrowser**] shortcut icon on the desktop (shown in [figure 43](#)). The secure browser opens displaying the student logon screen. The secure browser fills the entire screen and hides the task bar.
11. To exit the secure browser, select [**CLOSE SECURE BROWSER**] in the upper-right corner of the screen.

Installing the Secure Browser via the Command Line

In this scenario, a user with administrator rights installs the secure browser from the command line. If the user does not have administrator rights, refer to the subsection “[Installing the Secure Browser Without Administrator Rights](#).”

1. If a user installed a previous version of the secure browser in a location other than C:\Program Files (x86)\ (64 bit) or C:\Program Files\ (32 bit), manually uninstall the secure browser. (If it was installed in C:\Program Files (x86)\, the installation package automatically removes it.) Refer to the instructions in the subsection “[Uninstalling the Secure Browser on Windows](#).”
2. Navigate to the [CAASPP and ELPAC Secure Browsers](#) web page by going to the [CAASPP](#) website or the ELPAC [Technology Resources](#) web page and selecting the [Secure Browsers] link at either location.
3. Scroll down the [CAASPP and ELPAC Secure Browsers](#) web page to the “Download Secure Browsers” section.
4. Select the [**Windows**] tab and then select the [**Download Browser**] button (shown in [figure 44](#)). A dialog box opens.



Figure 44. [Download Browser] button

Secure Browser Configuration | Installing the Secure Browser on Desktops and Laptops

5. Save the file on the computer (this step may vary depending on the web browser being used):
 - a. If presented with a choice to run or save the file, select [**Save**] and save the file to a convenient location.
 - b. If presented only with the option to save, save the file to a convenient location.
6. Note the full path and file name of the downloaded file, such as `c:\temp\CASecureBrowser-Win.msi`.
7. Open a command prompt as the administrator.
 - a. Type command into the *Search* field on the task bar.
 - b. Right-click the [**Command Prompt**] icon in the “Best match” section of the *Search* pop-up list.
 - c. Select *Run as administrator* from the shortcut menu.
 - d. As necessary, type the administrator password for the device. The command prompt opens.
8. Run the command `msiexec /I <Source> [/quiet] [INSTALLDIR=<Target>]`.
 - <Source> Path to the installation file, such as
`C:\temp\CASecureBrowser-Win.msi`
 - <Target> Path to the location to install the secure browser (If absent, it installs to the directory described in step [10](#); the installation program creates the directory if it does not exist.)
 - `/I` Perform an install
 - `[/quiet]` Quiet mode, no interaction

For example, the command

```
msiexec /I c:\temp\CASecureBrowser-Win.msi /quiet  
INSTALLDIR=C:\AssessmentTesting\BrowserInstallDirectory
```

installs the secure browser from the installation package at `C:\temp\CASecureBrowser-Win.msi` into the directory `C:\AssessmentTesting\BrowserInstallDirectory` using quiet mode.
9. Follow the instructions in the setup wizard. When prompted for setup type, select [**Install**].

10. Select **[Finish]** to exit the setup wizard. The following items are installed:
 - The secure browser to the default location `C:\Program Files (x86)\CASecureBrowser\ (64 bit)` or `C:\Program Files\CASecureBrowser\ (32 bit)`
 - A shortcut `CASecureBrowser` to the desktop
11. Ensure all background jobs, such as virus scans or software updates, are scheduled outside of testing windows. For example, if testing takes place between 8 a.m. and 3 p.m., schedule background jobs outside of these hours.
12. Run the secure browser by double-clicking the **[CASecureBrowser]** shortcut icon on the desktop (shown in [figure 45](#)). The secure browser opens, displaying the student logon screen. The secure browser fills the entire screen and hides the task bar.



Figure 45. [CASecureBrowser] shortcut icon

13. To exit the secure browser, select **[CLOSE SECURE BROWSER]** in the upper-right corner of the screen.

Copying the Secure Browser Installation Directory to Testing Computers

In this scenario, a network administrator installs the secure browser on one machine and copies the entire installation directory to testing computers.

1. On the machine from where the user will copy the installation directory, install the secure browser following the directions in the subsection "[Installing the Secure Browser on an Individual Computer.](#)" Note the path of the installation directory, such as `C:\Program Files (x86)\CASecureBrowser`.
2. Identify the directory on the local testing computers to which the user will copy the secure browser file (it should be the same directory on all computers). For example, a user may want to copy the directory to `C:\AssessmentTesting\`. Ensure selection of a directory in which the students can run executables.
3. Take the following steps on each local testing computer:
 - a. Ensure all background jobs, such as virus scans or software updates, are scheduled outside of testing windows. For example, if testing takes place between 8 a.m. and 3 p.m., schedule background jobs outside of these hours.

Secure Browser Configuration | Installing the Secure Browser on Desktops and Laptops

- b. Copy the installation directory used in step [1](#) from the remote machine to the directory selected in step [1](#). For example, if the target directory is `C:\AssessmentTesting\`, create a new folder `C:\AssessmentTesting\CASecureBrowser`.
- c. Copy the shortcut `C:\AssessmentTesting\CASecureBrowser\CASecureBrowser.exe - Shortcut.lnk` to the desktop.
- d. Run the secure browser by double-clicking the `CASecureBrowser` shortcut on the desktop. The secure browser opens, displaying the student logon screen. The secure browser fills the entire screen and hides the task bar.
- e. To exit the secure browser, select [**CLOSE SECURE BROWSER**] in the upper-right corner of the screen.

Installing the Secure Browser for Use with an NComputing Terminal

In this scenario, a network administrator installs the secure browser on a Windows server accessed through an NComputing terminal. Prior to testing day, the technology coordinator connects consoles to the NComputing terminal, logs on from each console to the Windows server, and starts the secure browser so it is ready for the students.

This procedure assumes that there is already a working NComputing topology with consoles able to reach the Windows server.

For a listing of supported terminals and servers for this scenario, refer to [Chapter 1: System Requirements](#).

1. Log on to the machine running the Windows server.
2. Install the secure browser following the directions in the subsection "[Installing the Secure Browser on an Individual Computer](#)."
3. Open Notepad and type the following command (no line breaks):

```
"C:\Program Files (x86)\CASecureBrowser\  
CASecureBrowser.exe" -CreateProfile %SESSIONNAME%
```

If a different installation path on the Windows server was used, use that in the previous command.

4. Save the file to the desktop as `logon.bat`.
5. Create a group policy object that runs the file `logon.bat` each time a user logs on. For details, refer to [Appendix E: Creating Group Policy Objects to Assign Logon Scripts in Microsoft Windows](#).
6. On each NComputing console, create a new [**CASecureBrowser**] desktop shortcut icon by taking the following steps. This subprocess is necessary because the default shortcut created by the installation program has an incorrect target.

- a. Connect to the NComputing terminal.
 - b. Log on to the Windows server with administrator privileges.
 - c. Delete the secure browser's shortcut currently appearing on the desktop.
 - d. Navigate to the secure browser's installation directory, usually `C:\Program Files (x86)\CASecureBrowser\`.
 - e. Right-click the file `CASecureBrowser.exe` and select *Send To → Desktop (create shortcut)*.
 - f. On the desktop, right-click the new shortcut and select *Properties*. The *Shortcut Properties* dialog box appears.
 - g. Under the [**Shortcut**] tab, in the *Target* field, type the following command:

```
"C:\Program Files(x86)\CASecureBrowser\  
CASecureBrowser.exe" -P%SESSIONNAME%
```

If a different installation path on the Windows server was used, use that in the previous command. Note that "(x86)" is not present in the directory name on 32-bit installations.
 - h. Select [**OK**] to close the *Properties* dialog box.
7. Verify the installation by double-clicking the shortcut to start the secure browser.

Installing the Secure Browser on a Terminal Server or Windows Server

In this scenario, a network administrator installs the secure browser on a server—either a terminal server or a Windows server. Testing machines then connect to the server's desktop and run the secure browser remotely. This scenario is supported on Windows server 2012 R2 and 2016 R2.



Warning: Poor Quality of Secure Browser Functionality When Launched from a Server

- Launching a secure browser from a terminal or Windows server typically does not create a secure test environment because students can use their local devices to search for answers. Additionally, this sort of configuration can compromise the stability and performance of the secure browser, especially during peak testing times, because it creates contention among students' client devices for local area network bandwidth and shared drive input and output. Therefore, this installation scenario is **not recommended for testing**.

Secure Browser Configuration | Installing the Secure Browser on Desktops and Laptops

LEA CAASPP or ELPAC coordinators should contact the California Technical Assistance Center for instructions and technical support before the secure browser is installed using this scenario.

Installing the Secure Browser Without Administrator Rights

In this scenario, the user copies the secure browser from one machine where it is installed on to another machine on which the user does not have administrator rights.

1. Log on to a device on which the secure browser is installed.
2. Copy the entire folder where the secure browser was installed (usually `C:\Program Files (x86)\CASecureBrowser`) to a removable drive or shared network location.
3. Copy the entire directory from the shared location or removable drive to any directory on the target computer.
4. In the folder where the user copied the secure browser, right-click `CASecureBrowser.exe` and select *Send To* → *Desktop (create shortcut)*.
5. Ensure all background jobs, such as virus scans or software updates, are scheduled outside of testing windows. For example, if testing takes place between 8 a.m. and 3 p.m., schedule background jobs outside of these hours.
6. Double-click the desktop shortcut to run the secure browser.

About Sharing the Secure Browser Over a Network



Warning: Sharing the Secure Browser Over a Network Is Not Recommended

- While the secure browser can be installed on a server's shared drive and then shared to each testing computer's desktop via a shortcut, CAI strongly discourages this setup as it can compromise the stability and performance of the browser, especially during peak testing times.

Uninstalling the Secure Browser on Windows

The following subsections describe how to uninstall the secure browser from the Windows interface or from the command line. Older versions of the secure browser will be automatically uninstalled during the installation of a new version.

Uninstalling via the User Interface

The following instructions may vary depending on the version of Windows.

1. Navigate to *Settings* → *System* → *Apps & features* (Windows 10) or *Control Panel* → *Add or Remove Programs* or *Uninstall a Program* (previous versions of Windows).

2. Select the secure browser program `CASecureBrowser` and select **[Remove]** or **[Uninstall]**.
3. Follow the instructions in the uninstall wizard.

Uninstalling via the Command Line

1. Open a command prompt.
2. Run the command `msiexec /X <Source> /quiet`
`<Source>` Path to the executable file, such as `C:\MSI\CASecureBrowser.exe`
`/X` Perform an uninstall
`[/quiet]` Quiet mode, no interaction
For example, the command
`msiexec /X C:\AssessmentTesting\CASecureBrowser.exe /quiet`
uninstalls the secure browser installed at `C:\AssessmentTesting\` using quiet mode.

Secure Browser for Windows and the Microsoft Take a Test App

Windows 10 and Windows 10 in S mode come with Microsoft's Take a Test app, which enforces a locked-down, secure testing environment similar to CAI's secure browser. **Users of the Take a Test app do not need to install the CA Secure Browser on the testing machine.**

Creating a Dedicated Test Account for Non-Permissive Mode Users

Users not using permissive mode should create a dedicated test account for the Take a Test app; permissive mode features will not be available when using this method. To access permissive mode features, refer to the next subsection, "[Creating Desktop Shortcuts for Permissive Mode Users](#)."



Note: Assessments administered through the Take a Test app will detect some forbidden apps are running in the background even if users do not start these apps, which causes the Take a Test app to log a user off his or her account. (For more information, refer to the Microsoft Windows help topic "[Take tests in Windows 10](#).") Because of this, CAI has disabled the forbidden app check when using the Take a Test app through a dedicated test account.

Take the following steps to create a dedicated test account:

1. Sign into the device with an administrator account.
2. Go to *Settings* → *Accounts* → *Access work or school*.

Secure Browser Configuration |
Installing the Secure Browser on Desktops and Laptops

3. Select an existing account to use as the dedicated testing account.



Note: If a user does not have an account on the device, the user can create a new account. To do this, go to *Settings* → *Accounts* → *Other Users* → *Add someone else to this PC* → [I don't have this person's sign-in information] → [Add a user without a Microsoft account].

4. In the *Enter the test's web address* field, enter `https://ca.tds.cambiumast.com/student`.
5. Select [**Save**].

The student can now sign in to the dedicated account to take the specified test.

Creating Desktop Shortcuts for Permissive Mode Users

Permissive mode users should create a desktop shortcut for the Take a Test app. Take the following steps to create a desktop shortcut for Take a Test:

1. Log on to Windows as the user taking a test.
2. Right-click on the Desktop and select *New* → *Shortcut*. The *Create Shortcut* dialog box appears ([figure 46](#)).

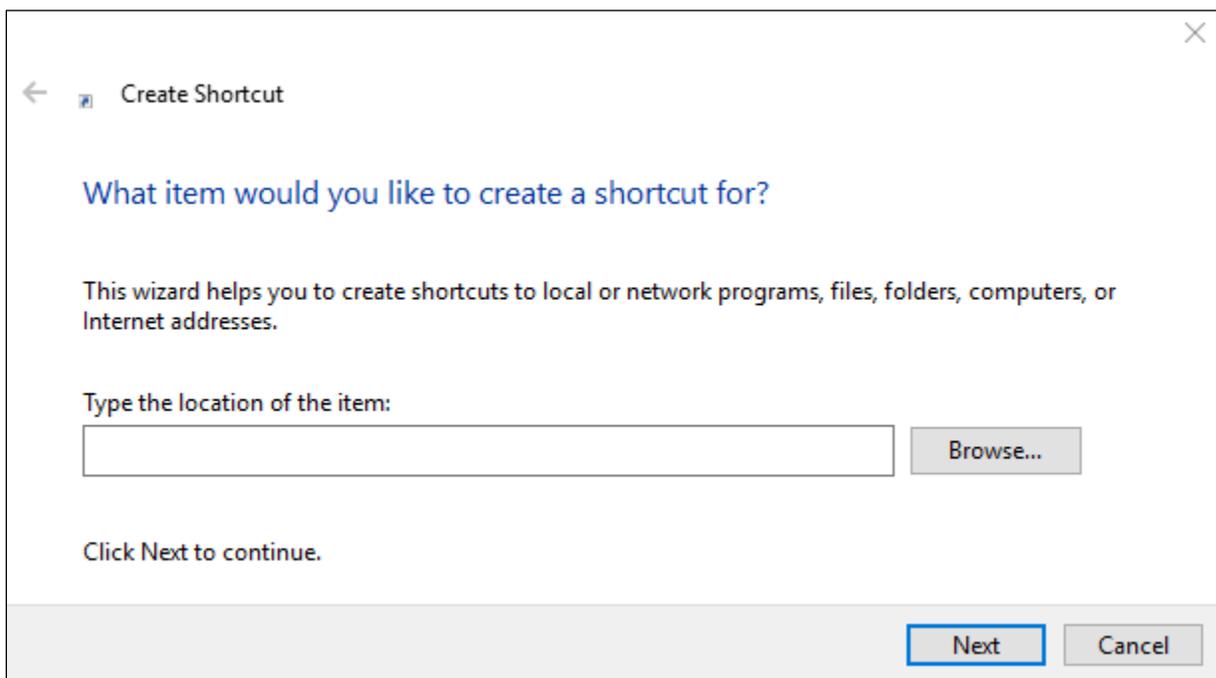


Figure 46. Create Shortcut dialog box

3. In the *Type the location of the item* field, enter `ca-edu-secureassessment:https://ca.tds.cambiumast.com/student`

4. Select **[Next]**.
5. In the next dialog box, enter a name for the shortcut in the *Type a name for this shortcut* field.
6. Select **[Finish]**.

The shortcut appears on the desktop. To run the Take a Test app, double-click the shortcut. To exit the Take a Test app, press [Ctrl] + [Alt] + [Del].

Installing the Secure Browser on macOS

Additional Resources in This Subsection:

- CAASPP website—<http://www.caaspp.org/>
- CAASPP and ELPAC Secure Browsers website—<https://ca.portal.cambiumast.com/>
- ELPAC Technology Resources web page—<https://www.elpac.org/resources/technology-resources/>

This subsection provides instructions for installing the secure browser on Macintosh desktop or laptop computers only; it does not apply to Apple mobile devices such as the iPad.

Installing the Secure Browser on an Individual Apple Computer

In this scenario, a user installs the secure browser on Apple desktop and laptop computers running OS X 10.11 or macOS 10.12 through 10.16. The steps in this procedure may vary depending on the version of OS X or macOS and the web browser.

1. Remove any previous version of the secure browser by dragging its folder to the Trash.
2. Navigate to the [CAASPP and ELPAC Secure Browsers](#) web page by going to the [CAASPP](#) website or the ELPAC [Technology Resources](#) web page and selecting the [Secure Browsers] link at either location.
3. Scroll down the [CAASPP and ELPAC Secure Browsers](#) web page to the “Download Secure Browsers” section.
4. Select the **[Mac OS X/macOS 10.11–10.15]** tab and then select the **[Download Browser]** button (shown as highlighted in [figure 47](#)). A dialog box opens.



Figure 47. [Download Browser] button

Secure Browser Configuration | Installing the Secure Browser on Desktops and Laptops

5. If prompted for a download location, select the Downloads folder.
6. Open Downloads from the dock, and then select `CASecureBrowser-OSX.dmg` to display its contents ([figure 48](#)).



Figure 48. Contents of the CASecureBrowser-OSX.dmg folder

7. **If running OS X 10.11 or above**, either hold down the [Control] key when opening the downloaded file to bypass the security on an ad hoc basis; or follow these additional steps to temporarily allow installation from any source. Otherwise, proceed to step [8](#).
 - a. Open System Preferences (*Apple* → *System Preferences*).
 - b. Select the [**Security and Privacy**] icon.

- c. In the [**General**] tab, select the lock in the bottom-left corner of the screen (indicated in [figure 49](#)) and then type the password to enable changes.

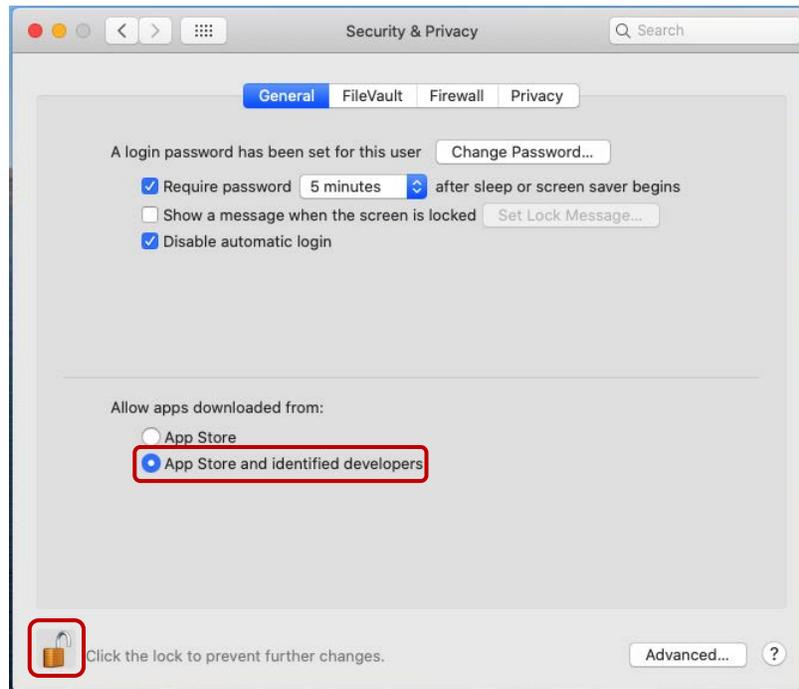


Figure 49. Security & Privacy screen for macOS

- d. In the “Allow apps downloaded from” section, first note which radio button is highlighted, and then select the *Allow from App Store and identified developers* radio button (also indicated in [figure 49](#)).
8. Drag the [**CA Secure Browser**] icon to the folder. This installs the secure browser into Applications.
 9. Ensure all background jobs, such as virus scans or software updates, are scheduled outside of test windows. For example, if testing takes place between 8 a.m. and 3 p.m., schedule background jobs outside of these hours.
 10. In Finder, navigate to *Go* → *Applications*, and then double-click *CA Secure Browser* to launch the secure browser. (The user must launch the secure browser to complete the installation.) The secure browser opens displaying the student logon screen. The secure browser fills the entire screen and hides the dock.



Caution: The secure browser disables Exposé (hot corner) settings if they are set, and the settings remain disabled after the secure browser is closed.

11. To exit the secure browser, select [**CLOSE SECURE BROWSER**] in the upper-right corner of the screen.

Secure Browser Configuration | Installing the Secure Browser on Desktops and Laptops

12. To create a desktop shortcut, from the Applications folder, drag `CASecureBrowser` to the desktop.
13. **OS X 10.11 only:** Restore security settings by reversing the process in step 7 and resetting the “**Allow apps downloaded from**” setting to what it had been previously.

Cloning the Secure Browser Installation to Other Macs

Depending on the local networking and permissions, it may be faster to install the secure browser on to a single Mac, take an image of the disk, and then copy the image to other Macs.

To clone the secure browser installation to other Macs:

1. Take the following steps on the Mac where the user will clone the installation:
 - a. Install the secure browser following the directions in the subsection “[Installing the Secure Browser on an Individual Apple Computer.](#)” Be sure to run and then close the secure browser after the installation.
 - b. In Finder, display the `Library` folder.
 - c. Open the `Application Support` folder. The *Application Support* configuration interface opens.
 - d. Delete the `CASecureBrowser` folder containing the secure browser (indicated in [figure 50](#)).
 - e. Delete the `Mozilla` folder (also indicated in [figure 50](#)).

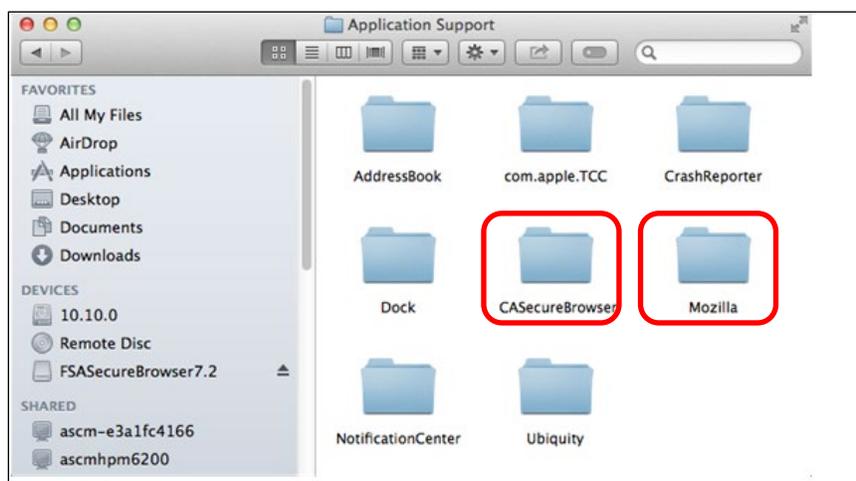


Figure 50. Apple *Application Support* configuration interface

2. Create a shell script that creates a new secure browser profile when a user logs on. The basic command to create a profile is

```
<install_directory>/Contents/MacOS/  
CASecureBrowser--CreateProfile profile_name, where profile_name is  
unique among all testing computers.
```

3. Clone the image.
4. Deploy the image to the target Macs.

Uninstalling the Secure Browser on OS X and macOS

To uninstall an OS X or macOS secure browser, drag its folder to the Trash.

Installing the Secure Browser on Linux

Additional Resources in This Subsection:

- CAASPP website—<http://www.caaspp.org/>
- CAASPP and ELPAC Secure Browsers website—<https://ca.portal.cambiumast.com/>
- ELPAC Technology Resources web page—<https://www.elpac.org/resources/technology-resources/>

This subsection provides instructions for installing the secure browser on computers running a supported Linux distribution. For additional information about Linux requirements, refer to the subsection “[Linux Testing Device Configuration](#).”

Installing the Secure Browser on 32-Bit Versions of Linux

The instructions in this subsection are for installing the Linux secure browser onto 32-bit versions of Linux systems. These instructions may vary for the individual Linux distribution.

1. Uninstall any previous versions of the secure browser by deleting the directory containing it.
2. Obtain the root or superuser password for the computer on which the user is installing the secure browser.
3. Navigate to the [CAASPP and ELPAC Secure Browsers](#) web page by going to the [CAASPP](#) website or the ELPAC [Technology Resources](#) web page and selecting the [Secure Browsers] link at either location.
4. Scroll down the [CAASPP and ELPAC Secure Browsers](#) web page to the “Download Secure Browsers” section.

Secure Browser Configuration | Installing the Secure Browser on Desktops and Laptops

5. Select the **[Linux]** tab and then select the **[Download Browser]** button (shown as highlighted in [figure 51](#)).



Figure 51. [Download Browser] button

6. Save the file to the desktop.
7. Create the `CASecureBrowser` folder on the desktop.
 - a. For Ubuntu 16.04, right-click the downloaded file `CASecureBrowserX.X-YYYY-MM-DD-i686.tar.bz2` and select **[Extract Here]** to expand the file.
 - b. For Fedora, launch the terminal, enter `tar xfjv CASecureBrowser.tar.bz2`, and then press the [Enter] key.
8. In a file manager, open the `CASecureBrowser` folder.
9. Open the terminal and go to the secure browser directory location that was extracted in the previous step. Switch to a root or superuser by typing `su [UserName]` into the terminal. When prompted, enter the root or superuser password obtained in [step 2](#).
10. Enter `install-icon.sh` into the terminal to run the `install-icon.sh` file as an executable. When prompted, enter the root or superuser password obtained in [step 2](#).
11. Enter `su [UserName]` into the terminal to switch back to the standard user. When prompted, enter the standard user password. Then, run the `install-icon.sh -i` command through the terminal to install icons for the standard user.
12. The script installs all dependent libraries and supported voice packs and creates a **[CASecureBrowser]** icon on the desktop ([figure 52](#)). In Fedora, the icon is installed in the Charm. The installation script prompts the user for the root or superuser password obtained in [step 2](#).



Figure 52. [CASecureBrowser] shortcut icon

13. Ensure all background jobs, such as virus scans or software updates, are scheduled outside of testing windows. For example, if testing takes place between 8 a.m. and 3 p.m., schedule background jobs outside of these hours.
14. If text-to-speech testing is performed on this computer, reboot it.

15. From the desktop, double-click the **[CASecureBrowser]** icon to launch the secure browser. (If an *Untrusted App Launcher* error message appears, select **[Trust and Launch]**.) The student logon screen appears. The secure browser fills the entire screen and hides any panels or launchers.
16. To exit the secure browser, select the **[X]** in the upper-right corner of the screen.

Installing the Secure Browser on 64-Bit Versions of Linux

The instructions in this subsection are for installing the Linux secure browser onto 64-bit versions of Linux systems. These instructions may vary for the individual Linux distribution.

1. Uninstall any previous versions of the secure browser by deleting the directory containing it.
2. Obtain the root or superuser password for the computer on which the user is installing the secure browser.
3. Navigate to the [CAASPP and ELPAC Secure Browsers](#) web page by going to the [CAASPP](#) website or the ELPAC [Technology Resources](#) web page and selecting the [Secure Browsers] link at either location.
4. Scroll down the [CAASPP and ELPAC Secure Browsers](#) web page to the “Download Secure Browsers” section.
5. Select the **[Linux]** tab and then select the **[Download Browser]** button (shown as highlighted in [figure 53](#)).



Figure 53. [Download Browser] button

6. Save the file to the desktop.
7. Create the CASecureBrowser folder on the desktop:
 - a. For Ubuntu 16.04, right-click the downloaded file `CASecureBrowserX.X-YYYY-MM-DD-x86_64.tar.bz2` and select **[Extract Here]** to expand the file.
 - b. For Ubuntu 18.04 and 20.04 and Fedora, launch the terminal, enter `tar xfv CASecureBrowser.tar.bz2`, and then press the [Enter] key.
8. In a file manager, open the CASecureBrowser folder.
9. Open the terminal and go to the secure browser directory location that was extracted in the previous step. Switch to a root or superuser by typing `su [UserName]` into the terminal. When prompted, enter the root or superuser password obtained in step [2](#).

Secure Browser Configuration | Installing the Secure Browser on Desktops and Laptops

10. Enter `install-icon.sh` into the terminal to run the `install-icon.sh` file as an executable. When prompted, enter the root or superuser password obtained in step 2.
11. Enter `su [UserName]` into the terminal to switch back to the standard user. When prompted, enter the standard user password. Then, run the `install-icon.sh -i` command through the terminal to install icons for the standard user.
12. The script installs all dependent libraries and supported voice packs and creates a **[CASecureBrowser]** icon on the desktop (figure 54). In Fedora 29, the icon is installed in the Charm. The installation script prompts the user for the root or superuser password obtained in step 2.



Figure 54. [CASecureBrowser] shortcut icon

13. Ensure all background jobs, such as virus scans or software updates, are scheduled outside of testing windows. For example, if testing takes place between 8 a.m. and 3 p.m., schedule background jobs outside of these hours.
14. If text-to-speech testing is performed on this computer, reboot it.
15. From the desktop, double-click the **[CASecureBrowser]** icon to launch the secure browser. (If an *Untrusted App Launcher* error message appears, select **[Trust and Launch]**.) The student logon screen appears. The secure browser fills the entire screen and hides any panels or launchers.
16. To exit the secure browser, select the **[X]** in the upper-right corner of the screen.

Extracting the Secure Browser TAR File

Users attempting to install the secure browser in Fedora 30–31 or Ubuntu 18.04 may encounter an issue where the secure browser extracts to the `Home` folder and not the `Desktop` folder. This is a feature in these operating systems and *not* an error in the secure browser. The following procedure explains how to extract the secure browser TAR file manually using terminal commands.

1. Launch Terminal.
2. Type `tar xfv [Secure Browser File Name].tar.bz2`.
3. Press **[Enter]**.

Creating a Shortcut to Secure Browser 12.5

Installation of secure browser version 12.5 on machines running Fedora or Ubuntu Linux will not automatically install a shortcut to the browser. Users must manually create a shortcut. The following procedure explains how to complete this process.

1. Open Terminal.
2. Type the following:
`cd /location of Secure Browser/`
3. Type the following:
`cd /location of Secure Browser/`
4. Press **[Enter]**.
5. Close Terminal.
6. Open the `Secure Browser` folder.
7. Select **[install-icon.sh]**; a window displaying “Do you want to run install-icon.sh or display its contents?” will appear.
8. Select **[Run]**.

Uninstalling the Secure Browser on Linux

To uninstall a secure browser, delete the directory containing it.

Installing the Secure Browser on Mobile Devices

This section contains information about installing SecureTestBrowser, the secure browser app for iOS or iPadOS and Chrome OS. For information about configuring supported tablets and Chromebooks to work with the secure browser, refer to [Chapter 3: System Configuration](#).

Installing the Chrome OS SecureTestBrowser Kiosk App

This subsection contains instructions for installing SecureTestBrowser, the secure browser app for Chrome OS, as a kiosk application.



Caution: Users with Chromebooks manufactured in 2017 or later who do not have an Enterprise or Education license will not be able to use those machines for assessments. Google does not allow users without these licenses to set up kiosk mode, which is necessary to run the CAI Secure Browser. (This restriction to kiosk mode does not affect the Chrome operating system. A user can still use any version of the Chrome OS on hardware manufactured in 2016 or earlier.)

Installing the SecureTestBrowser App on Stand-Alone Chromebooks

These instructions are for installing the SecureTestBrowser secure browser on stand-alone Chromebook devices **that were manufactured prior to 2017**.



Warning: This procedure erases all data on the Chromebook. Be sure to back up data before beginning.

1. A user should obtain the following from the network administrator:
 - The wireless network to which the Chromebook connects. This typically includes the network's service set identifier, password, and other access credentials.
 - An email address and password for logging on to Gmail.
2. Power off and then power on the Chromebook.
3. If the OS verification is Off message appears, take the following steps; otherwise, skip to step 4.
 - a. Press the [Spacebar]. In the confirmation screen, press [Enter]. The Chromebook reboots.

- b. In the *Welcome* screen shown in [figure 55](#), select a language, keyboard, and the wireless network information acquired from the network administrator, and then select [**Continue**].



Figure 55. Chromebook *Welcome* screen

- c. In the *Google Chrome OS Terms* screen, select [**Accept and continue**].
4. When the *Sign in* screen appears, wipe data from the Chromebook by taking the following steps:
 - a. Press [Esc] + [G] + [Power] ([Esc] + [Reload] + [Power]). The screen displays a yellow exclamation point (!) similar to that in [figure 56](#).



Figure 56. Chrome OS *Missing* message

- b. Press [Ctrl] + [D] to begin developer mode. A message similar to that in [figure 57](#) will appear, indicating that the user must press the [Enter] key to turn OS verification off, and that the system will reboot and clear local data.

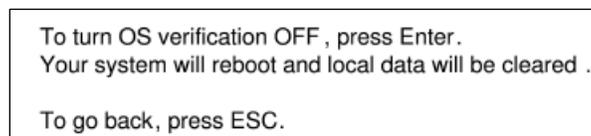


Figure 57. Turn OS Verification Off message

Secure Browser Configuration |
Installing the Secure Browser on Mobile Devices

- c. Press [Enter]. A message similar to that in [figure 58](#) will appear, indicating that verification is off and that pressing [Spacebar] will reenable it.



Figure 58. OS Verification Is Off message

- d. Press [Ctrl] + [D]. The Chromebook indicates it is transitioning to developer mode ([figure 59](#)). The transition takes approximately 10 minutes, after which the Chromebook reboots.

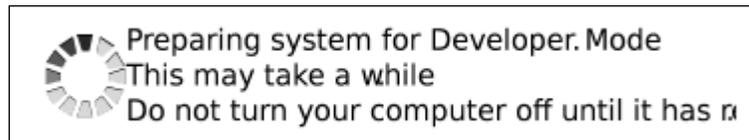


Figure 59. Preparing for Developer Mode message

- e. After the Chromebook reboots, the OS verification is Off message ([figure 58](#)) appears again.
 - f. Press the [Spacebar] and then press [Enter]. The Chromebook reboots, and the *Welcome* screen appears ([figure 55](#)).
5. In the *Welcome* screen, select a language, keyboard, and a network. The *Join WiFi Network* screen appears ([figure 60](#)).

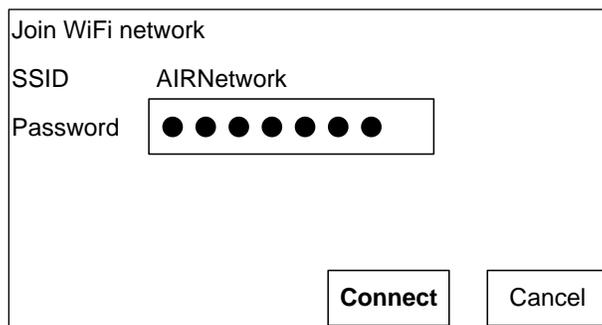


Figure 60. Join WiFi Network screen

- 6. Enter the network's password obtained in step 1.
- 7. Select [**Connect**] on the *Join WiFi Network* screen and then [**Continue**] on the *Welcome* screen.

- In the *Google Chrome OS Terms* screen, select [**Accept and continue**]. The *Sign in* screen ([figure 61](#)) appears.

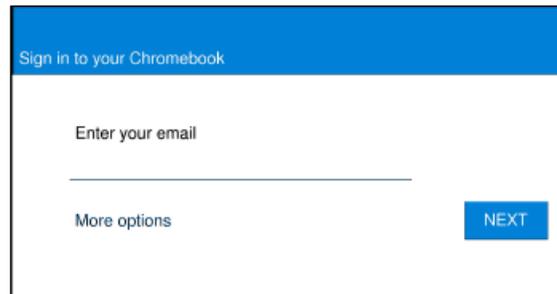


Figure 61. Chromebook *Sign in* screen

- In the *Sign in* screen, press [Ctrl] + [Alt] + [K] to open the *Automatic Kiosk Mode* screen ([figure 62](#)).

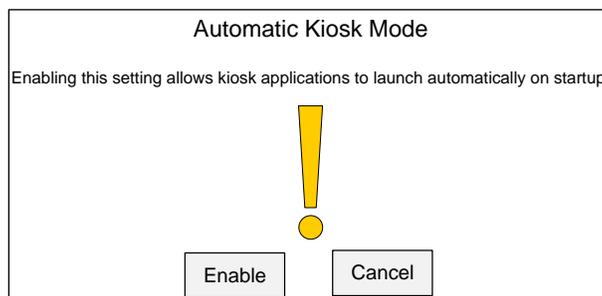


Figure 62. Automatic Kiosk Mode message

- Select [**Enable**] and then select [**OK**] to open the *Sign in* screen ([figure 61](#)).
- In the *Sign in* screen, enter the Gmail address obtained in step 1, select [**Next**], enter the password, and then select [**Next**] again.
- When the desktop opens, select the [**Chrome**] icon [- In the URL bar, enter `chrome://extensions` to open the *Extensions* screen ([figure 63](#)).



Figure 63. *Extensions* screen

Secure Browser Configuration |
Installing the Secure Browser on Mobile Devices

14. Mark the checkbox for *Developer Mode* (indicated in [figure 63](#)).
15. Select the [**Manage kiosk applications**] button—also indicated in [figure 63](#)—to open the *Manage Kiosk Applications* screen ([figure 64](#)).

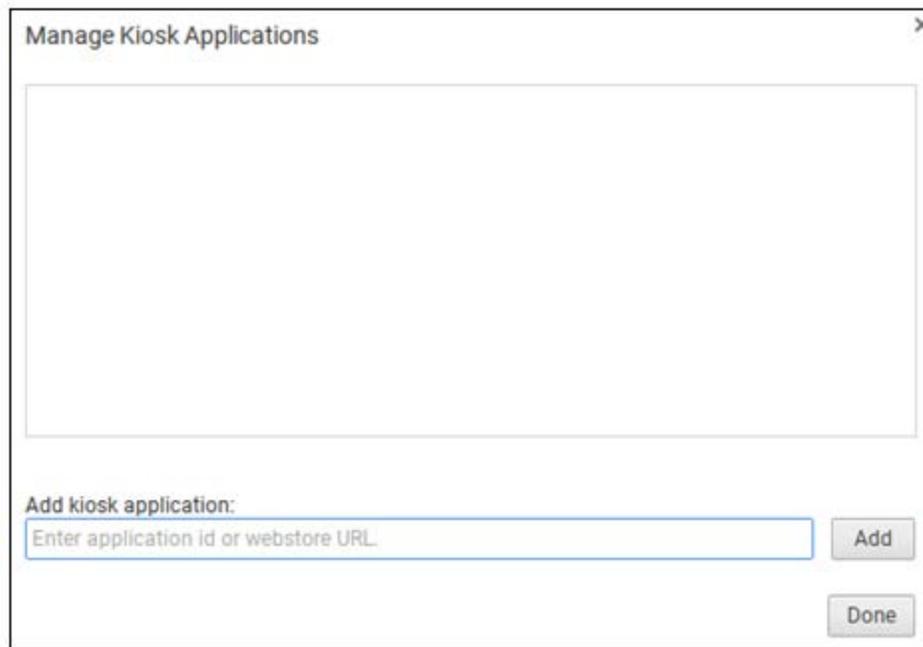


Figure 64. Manage Kiosk Applications screen

16. Take these steps in the *Manage Kiosk Applications* screen:
 - a. Enter `hblfbmjdaalalhifaaajnnodlkiloengc` into the *Add kiosk application* field.
 - b. Select [**Add**]. The `SecureTestBrowser` application appears in the *Manage Kiosk Applications* list.
 - c. Select [**Done**].
17. Select the icon in the lower-right corner and then select [**Sign Out**].
18. Back on the desktop, select [**Apps**] at the bottom of the screen and then select [**SecureTestBrowser**]. The secure browser launches.
19. If the system displays the following error message, then the secure browser is not configured to run in kiosk mode:

The `SecureTestBrowser` application requires kiosk mode to be enabled.

Reinstall the app in kiosk mode by following the procedure in this subsection.

20. Configure the test administration by following the procedure in the subsection [“Opening the SecureTestBrowser Kiosk App and Selecting the Assessment Program.”](#)

Installing the SecureTestBrowser Kiosk App on Managed Chromebooks

These instructions are for installing the SecureTestBrowser secure browser as a kiosk app on domain-managed Chromebook devices. The steps in this procedure assume that the Chromebooks are already managed through the admin console.

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.



Caution: SecureTestBrowser is not compatible with public sessions.

1. Set up a free Google Apps for Education account and enroll all managed Chromebooks.
2. As the Chromebook administrator, access the [Sign in](#) web page to log on to the Admin console.
3. When the *Google Admin* console opens, select **[Devices]**, which is indicated in [figure 65](#).

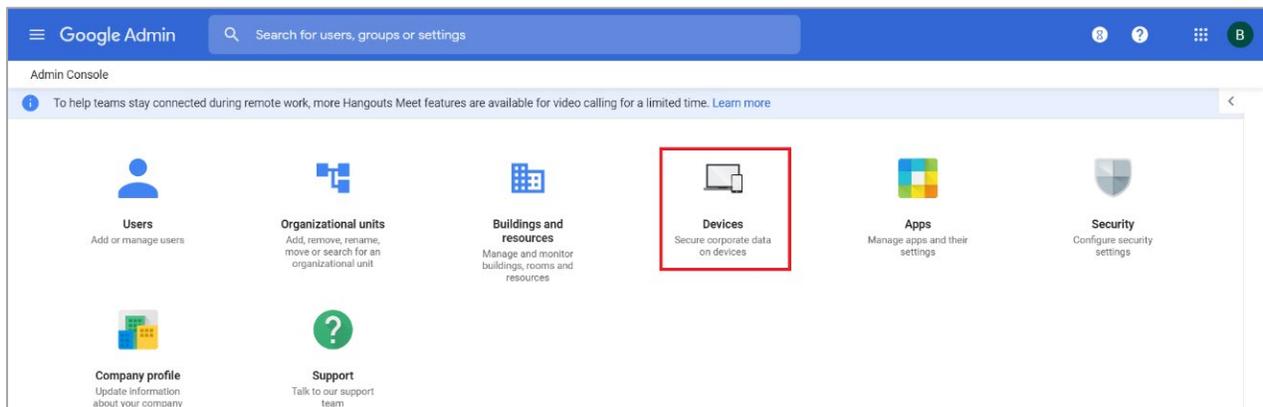


Figure 65. Google Admin Console

Secure Browser Configuration | Installing the Secure Browser on Mobile Devices

- When the *Devices* screen appears, select the [Chrome] drop-down list in the left navigation pane (indicated in [figure 66](#)).

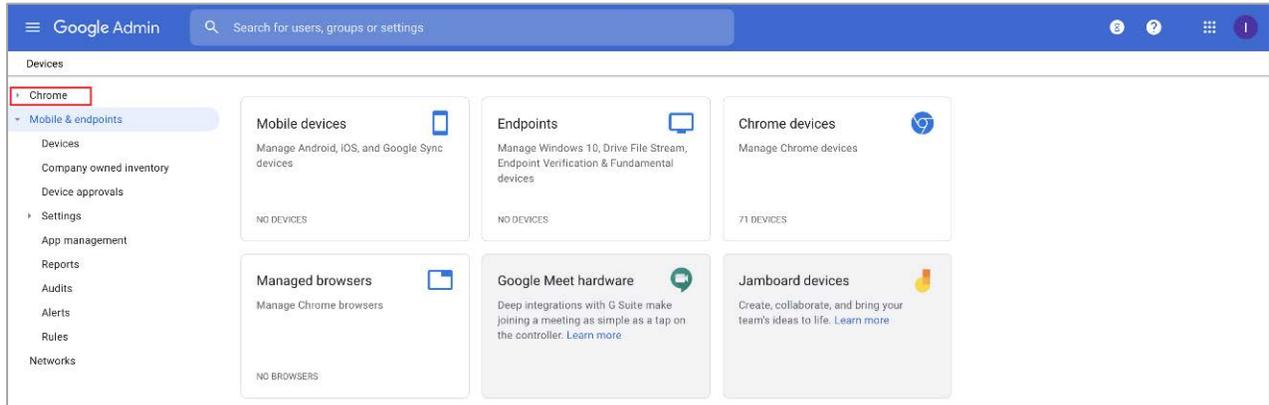


Figure 66. Chrome Devices screen

- Select [**Apps & extensions**] from the *Chrome* drop-down list (indicated in [figure 67](#)).

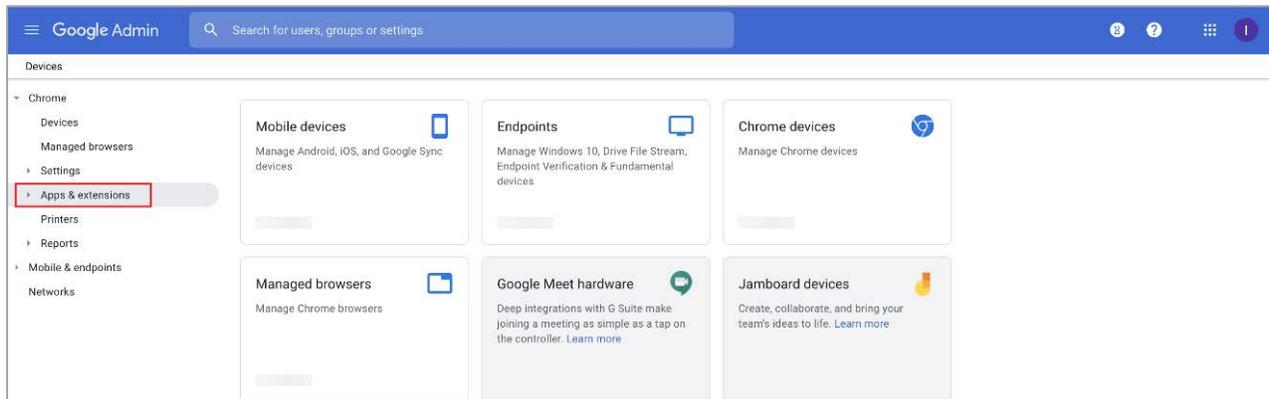


Figure 67. Apps & extensions drop-down list

6. Select *Kiosks* from the *Apps & extensions* drop-down list ([figure 68](#)).

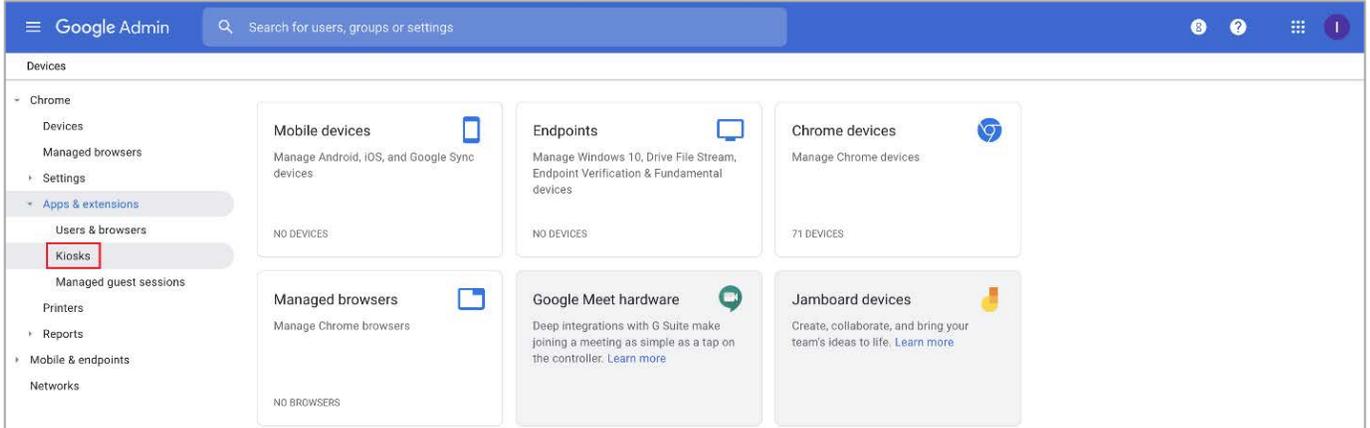


Figure 68. Kiosks option

7. The *Apps & Extensions* screen opens with the information in the **[Kiosks]** tab displayed ([figure 69](#)).

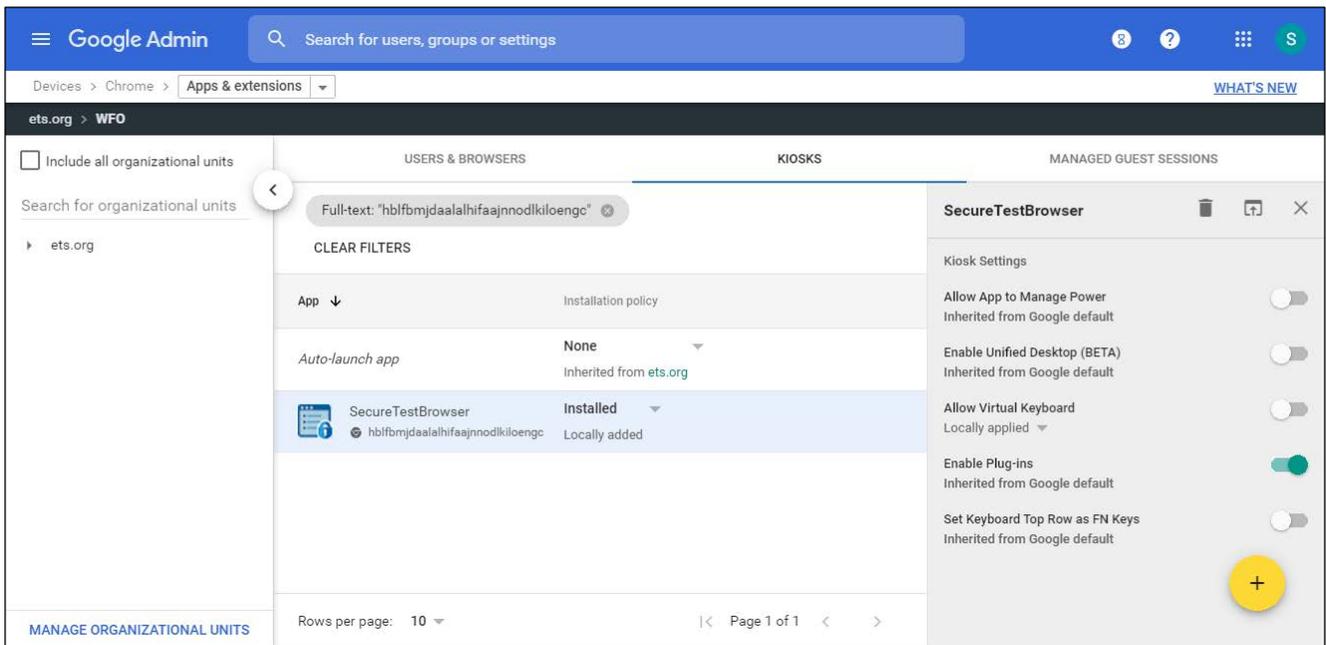


Figure 69. [Kiosks] tab section of the Apps & Extensions screen

Secure Browser Configuration |
Installing the Secure Browser on Mobile Devices

8. If the SecureTestBrowser app requires removal before deployment, remove it by selecting the app name (either AIRSecureTest or SecureTestBrowser) to display the app settings, selecting the **[Remove]** trash can [🗑️] icon (indicated in [figure 70](#)), and then selecting **[SAVE]**. Otherwise, select the **[X]** icon to the right of the **[Delete]** icon to close *App Settings* (also indicated in [figure 70](#)).

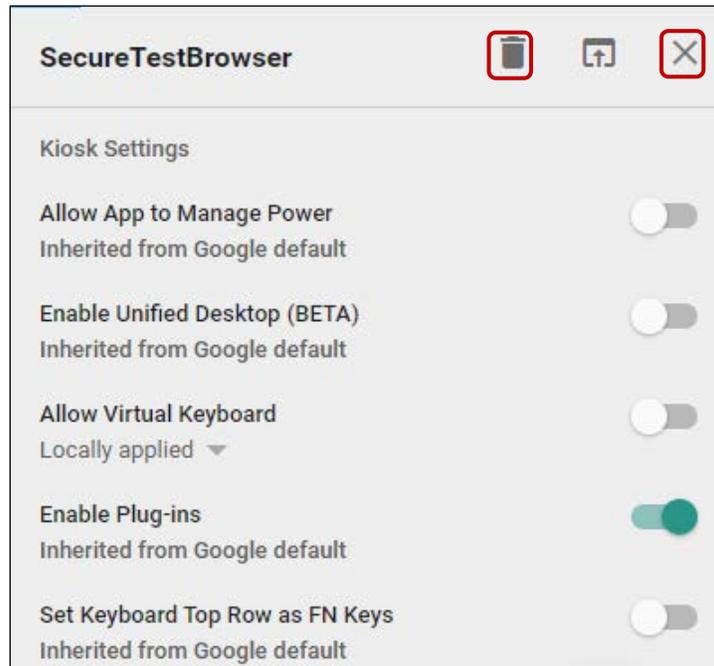
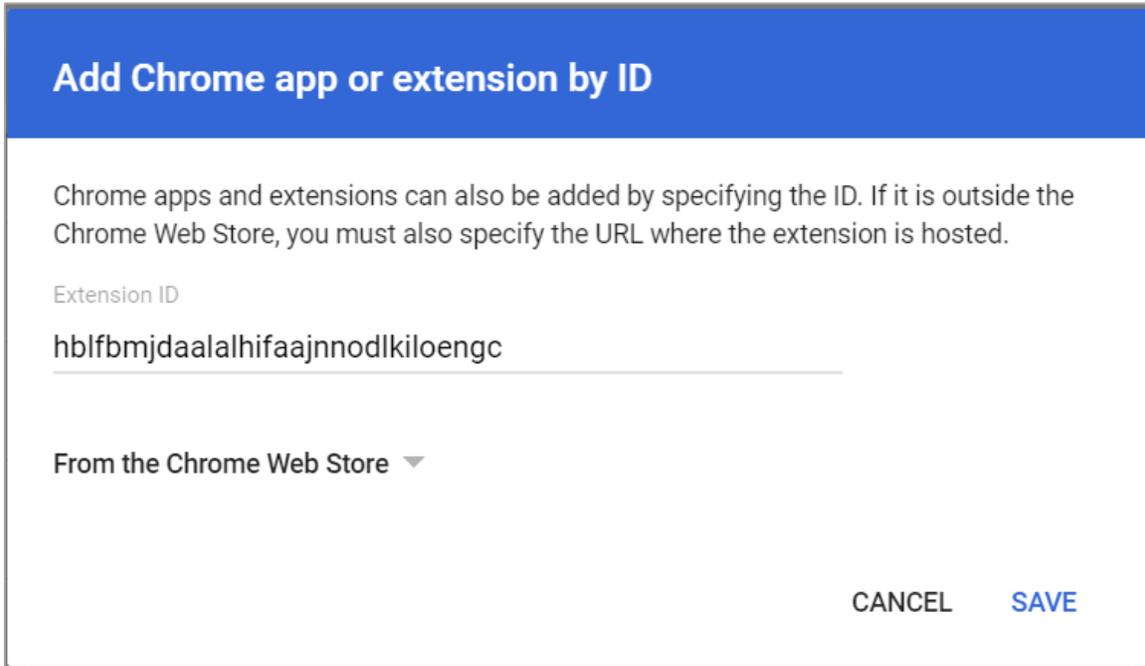


Figure 70. App Settings screen

9. Take the following steps to add the SecureTestBrowser app:
 - a. Hover over the **[Add]** plus-sign [⊕] icon (refer to [figure 69](#)).

- b. Select the [Add Chrome app or extension by ID] dotted-box [] icon to add a Chrome app or extension by ID. The *Add Chrome app or extension by ID* screen appears ([figure 71](#)).



Add Chrome app or extension by ID

Chrome apps and extensions can also be added by specifying the ID. If it is outside the Chrome Web Store, you must also specify the URL where the extension is hosted.

Extension ID

hblfbmjdaalalhifaajnnodlkiloengc

From the Chrome Web Store ▼

CANCEL SAVE

Figure 71. Add Chrome app or extension by ID screen

- c. Enter the character string `hblfbmjdaalalhifaajnnodlkiloengc` in the *Extension ID* field.
- d. Make sure that *From the Chrome Web Store* is selected in the drop-down list.
- e. Select [**Save**]. The *SecureTestBrowser* app appears in the app list.
- f. Ensure *Installed* is selected in the *Installation Policy* drop-down list.

Secure Browser Configuration | Installing the Secure Browser on Mobile Devices

- The only setting to be toggled in the “On” position is **Enable Plug-ins**. All other settings, including *Allow Virtual Keyboard*, must be toggled “Off.” This is shown in [figure 72](#). (Select [SAVE] if any edits were made.)

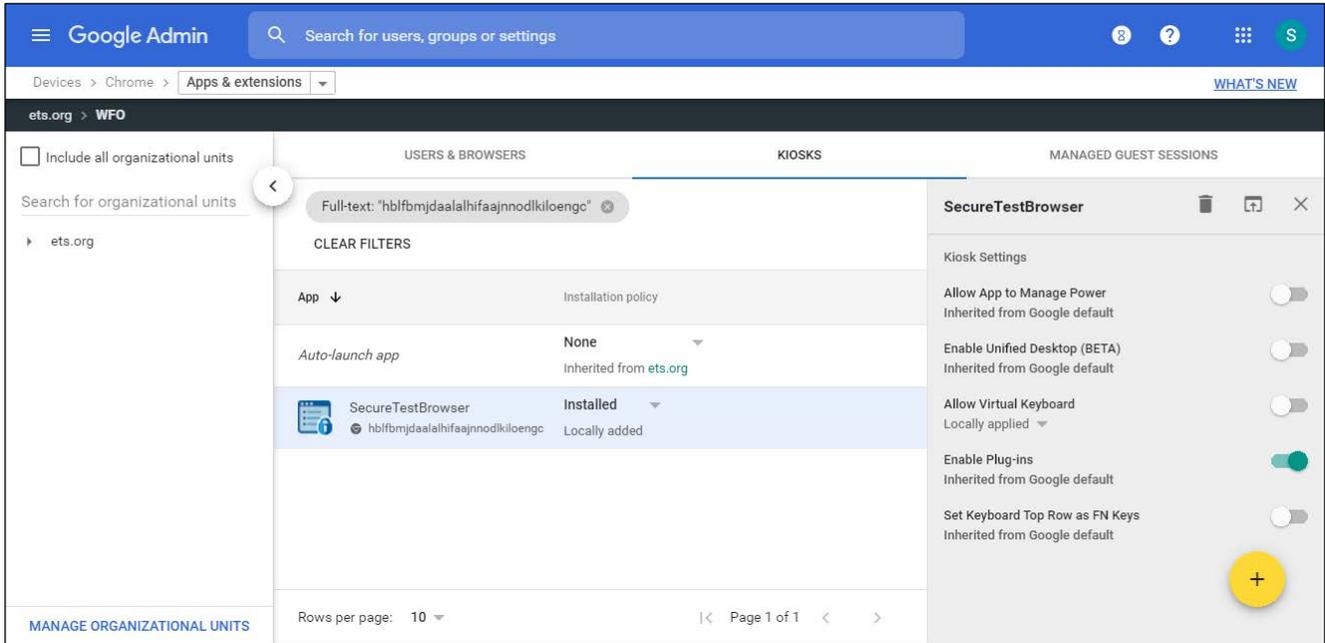


Figure 72. Google app settings



Notes:

- The SecureTestBrowser app will be installed on all managed devices the next time each managed device is turned on.
- This process may take up to 15 minutes.

- To launch the secure browser, select the [Apps] link in the menu row of the Chromebook’s logon screen and select the [**SecureTestBrowser - Secure Browser**] app (indicated in [figure 73](#)).

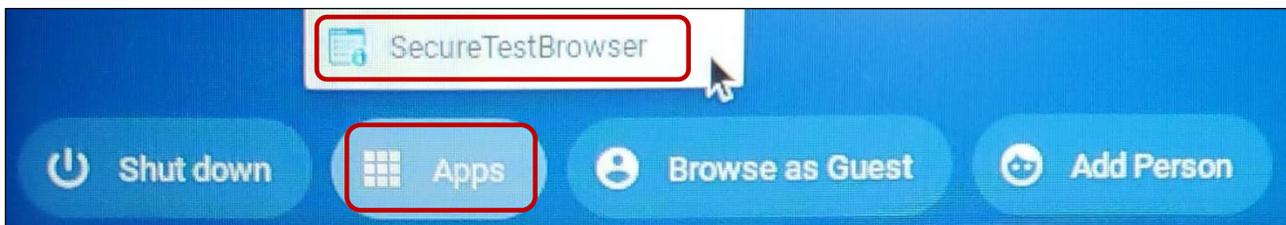
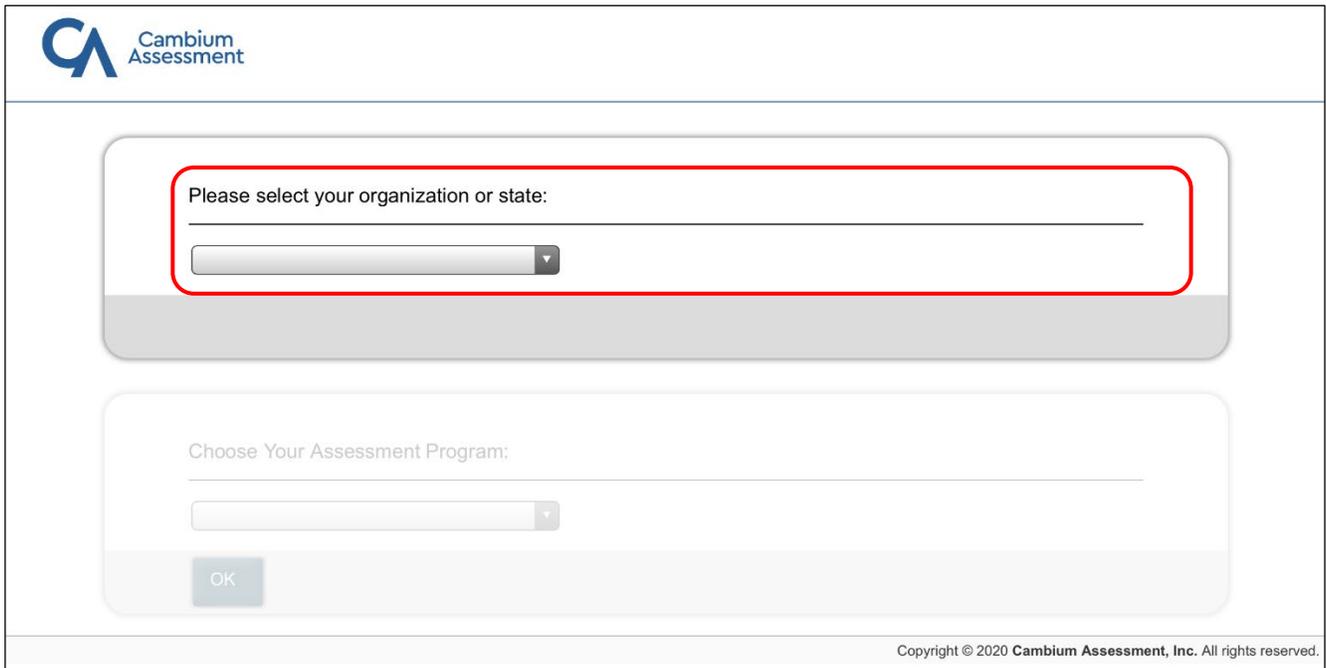


Figure 73. Chromebook logon screen

Opening the SecureTestBrowser Kiosk App and Selecting the Assessment Program

The first time the SecureTestBrowser kiosk app is opened, a Launchpad appears. The Launchpad establishes the state and test administration for students.

1. In the *Please Select Your State* drop-down list (indicated in [figure 74](#)), select *California*.



CA Cambium
Assessment

Please select your organization or state:

Choose Your Assessment Program:

OK

Copyright © 2020 Cambium Assessment, Inc. All rights reserved.

Figure 74. Select the state from the Launchpad

Secure Browser Configuration | Installing the Secure Browser on Mobile Devices

2. Select an option in the *Choose Your Assessment Program* drop-down list (indicated in [figure 75](#)).

The screenshot shows the Cambium Assessment Launchpad interface. At the top left is the Cambium Assessment logo. Below it, there are two main sections. The first section is titled "Please select your organization or state:" and contains a dropdown menu with "California" selected. The second section is titled "Choose Your Assessment Program:" and contains a dropdown menu with "California Assessment System" selected. A red rectangle highlights this second dropdown menu. Below the second dropdown menu is a blue "OK" button. At the bottom right of the screen, there is a small copyright notice: "Copyright © 2020 Cambium Assessment, Inc. All rights reserved."

Figure 75. Select the assessment from the Launchpad

3. Tap or select **[OK]**. The student logon page appears. The secure browser is now ready for students to use.

The *Launchpad* screen appears only once. The student logon page appears the next time the secure browser is launched.

Installing the Secure Browser on iOS or iPadOS



Additional Resources in This Subsection:

- Apple Configuration Profile Reference web document—
<https://developer.apple.com/business/documentation/Configuration-Profile-Reference.pdf>
- CAASPP website—<http://www.caaspp.org/>
- CAASPP and ELPAC Secure Browsers website—
<https://ca.portal.cambiumast.com/>
- ELPAC Technology Resources web page—<https://www.elpac.org/resources/technology-resources/>



Note: To run the secure browser or Classroom in iOS or iPadOS, the user must first disable any speech-to-text function such as Dictation. (Refer to the subsection “[Disabling Dictation](#)” for instructions for disabling Dictation; and “[Guidance on iOS or iPadOS Classroom and Summative Testing](#)” for more information on the Classroom app.)

Instructions for Installation

This subsection contains instructions for downloading and installing SecureTestBrowser and selecting the state and assessment program. The SecureTestBrowser Mobile Secure Browser for iPads is available from the App Store. The process for installing the secure browser is the same as for any other iOS or iPadOS application.

1. On the iPad, navigate to the [CAASPP and ELPAC Secure Browsers](#) web page by going to the [CAASPP](#) website or the ELPAC [Technology Resources](#) web page and selecting the [Secure Browsers] link at either location.
2. Scroll down the [CAASPP and ELPAC Secure Browsers](#) web page to the “Download Secure Browsers” section.
3. Select the [iOS] tab.

Secure Browser Configuration |
Installing the Secure Browser on Mobile Devices

4. Select the **[Download on the App Store]** button, shown as highlighted in [figure 76](#). (The user also can search for `SecureTestBrowser` in the App Store to find the secure browser app.)

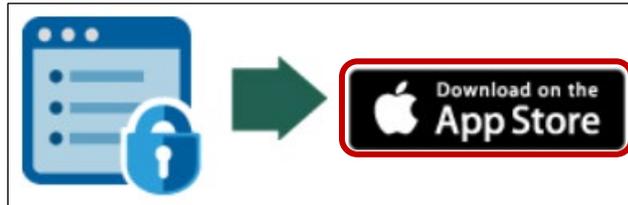


Figure 76. [Download on the App Store] button

5. The SecureTestBrowser download web page, shown in [figure 77](#), opens.

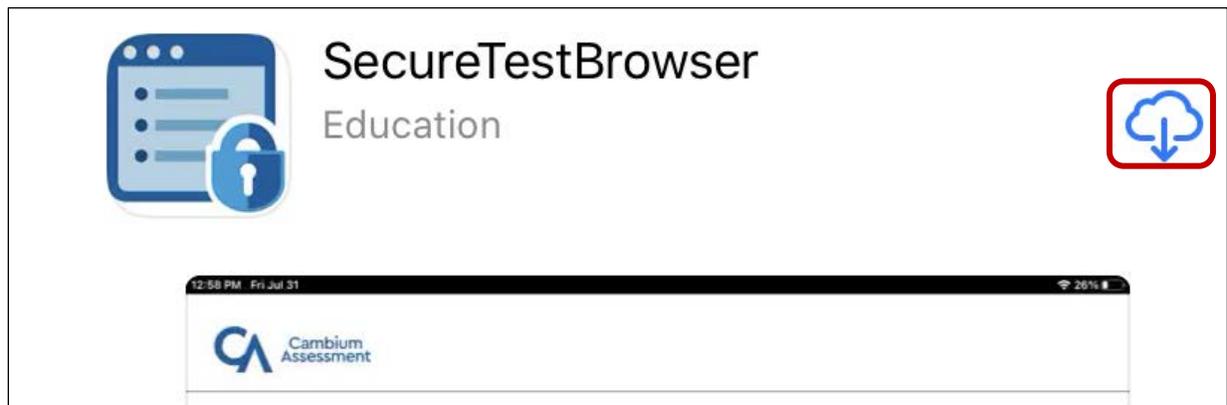


Figure 77. SecureTestBrowser App Store download web page

6. Tap the **[Download]** cloud [] icon, indicated in [figure 77](#). The iPad downloads and installs the secure browser, and the button changes to **[Open]**. (Note that the user must be signed in to the App Store to download SecureTestBrowser.)
7. After installation, a **[SecureTestBrowser]** icon like the one shown in [figure 78](#) appears on the iPad's home screen.



Figure 78. [SecureTestBrowser] icon, iOS or iPadOS

8. Tap [**Open**]. The first time the user opens SecureTestBrowser, the *Launchpad* screen appears. The Launchpad establishes the state and test administration for students.
9. In the *Please Select Your State* drop-down list (indicated in [figure 79](#)), select *California*.

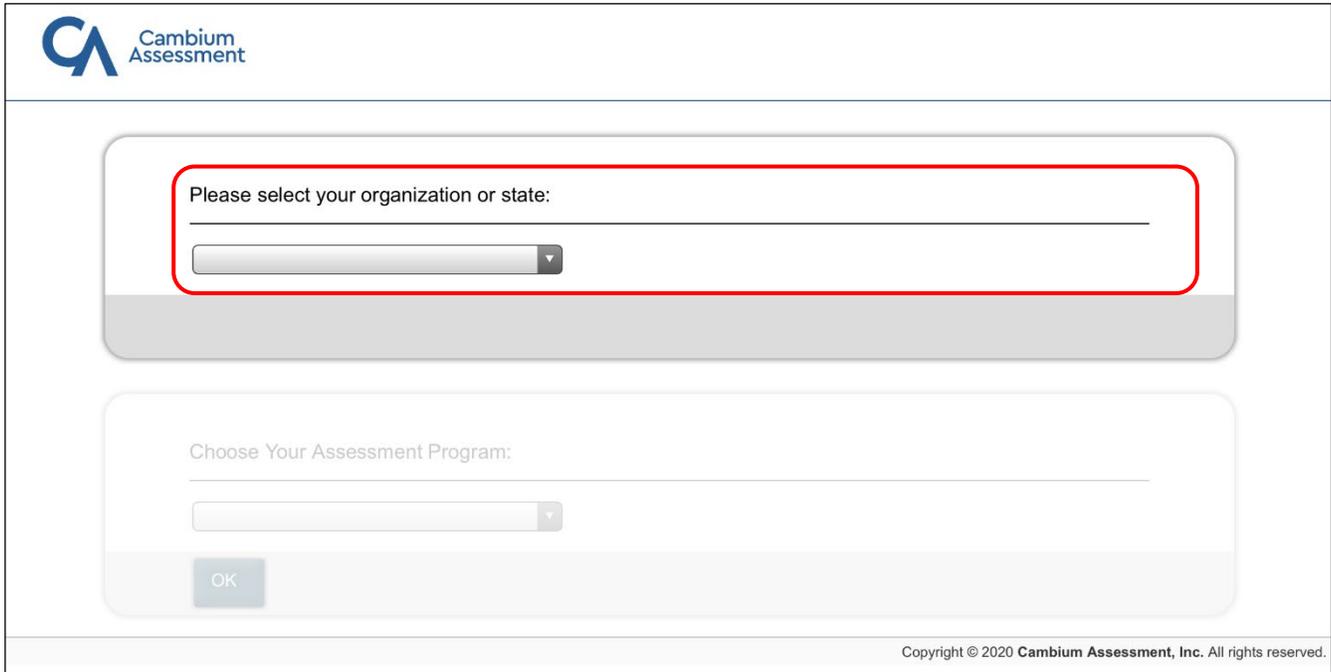


Figure 79. Select the state from the Launchpad

10. In the *Choose Your Assessment Program* drop-down list (indicated in [figure 80](#)), select *California Assessment System*.

The screenshot shows the Cambium Assessment Launchpad interface. At the top left is the Cambium Assessment logo. Below it, there are two main sections. The first section is titled 'Please select your organization or state:' and contains a dropdown menu with 'California' selected. The second section is titled 'Choose Your Assessment Program:' and contains a dropdown menu with 'California Assessment System' selected. A red rectangle highlights this second dropdown menu. Below the second dropdown menu is a blue 'OK' button. At the bottom right of the screen, there is a small copyright notice: 'Copyright © 2020 Cambium Assessment, Inc. All rights reserved.'

Figure 80. Select the assessment from the Launchpad

11. Tap **[OK]**. The student logon page opens. The secure browser is now ready for students to use.

The *Launchpad* screen appears only once. The student logon page appears the next time the secure browser is launched.

Guidance on iOS or iPadOS Classroom and Summative Testing

Classroom allows a teacher or proctor to remotely view and monitor a student's iPad. This feature can be disabled via mobile device management (MDM), by uninstalling Classroom, or by turning off Bluetooth on the teacher iPad during testing windows.

Using MDM to Disable Classroom Observation

A user can use the Boolean key `allowScreenShot` to disable access to the Classroom observation feature on student devices. This key is defined as part of the Restrictions profile payload. Refer to the Apple [Configuration Profile Reference](#) web document for instructions and more information about using this key.

Installing the Secure Browser on Windows Mobile Devices

The procedure for installing the secure browser on Windows mobile devices is the same for installing it on desktops. Refer to the subsection [“Installing the Secure Browser via Windows”](#) for details.

Proxy Settings for Desktop Secure Browsers

This section describes the commands for passing proxy settings to the secure browser, as well as how to implement those commands on the desktop computer.

Specifying a Proxy Server to Use with the Secure Browser

By default, the secure browser attempts to detect the settings for the network's web proxy server. 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. [Table 14](#) 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 [table 14](#) use the domain `fake-url.com`. When configuring for a proxy server, use the actual testing domain names as listed in [Appendix B: URLs for Testing Systems](#).

Table 14. Specifying Proxy Settings Using a Shortcut or the Command Line

Description	System	Command
Use the secure browser without any proxy	Windows	<code>CASecureBrowser.exe -proxy 0 aHR0cHM6Ly9jYS50ZHMuYWlyYXN0Lm9yZy9 zdHVkZW50</code>
Use the secure browser without any proxy	Mac	<code>./CASecureBrowser -proxy 0 aHR0cHM6Ly9jYS50ZHMuYWlyYXN0Lm9yZy9 zdHVkZW50</code>
Use the secure browser without any proxy	Linux	<code>./CASecureBrowser.sh -proxy 0 aHR0cHM6Ly9jYS50ZHMuYWlyYXN0Lm9yZy9 zdHVkZW50</code>
Set the proxy for HTTP requests only	Windows	<code>CASecureBrowser.exe -proxy 1:http:fake-url.com:8080 aHR0cHM6Ly9jYS50ZHMuYWlyYXN0Lm9yZy9 zdHVkZW50</code>
Set the proxy for HTTP requests only	Mac	<code>./CASecureBrowser -proxy 1:http:fake-url.com:8080 aHR0cHM6Ly9jYS50ZHMuYWlyYXN0Lm9yZy9 zdHVkZW50</code>

Table 14 (first continuation)

Description	System	Command
Set the proxy for HTTP requests only	Linux	<code>./CASecureBrowser.sh -proxy 1:http:fake-url.com:8080 aHR0cHM6Ly9jYS50ZHMuYWlyYXN0Lm9yZy9zdHVkZW50</code>
Set the proxy for all protocols to mimic the “Use this proxy server for all protocols” of Firefox	Windows	<code>CASecureBrowser.exe -proxy 1:*:fake-url.com:8080 aHR0cHM6Ly9jYS50ZHMuYWlyYXN0Lm9yZy9zdHVkZW50</code>
Set the proxy for all protocols to mimic the “Use this proxy server for all protocols” of Firefox	Mac	<code>./CASecureBrowser -proxy 1:*:fake-url.com:8080 aHR0cHM6Ly9jYS50ZHMuYWlyYXN0Lm9yZy9zdHVkZW50</code>
Set the proxy for all protocols to mimic the “Use this proxy server for all protocols” of Firefox	Linux	<code>./CASecureBrowser.sh -proxy 1:*:fake-url.com:8080 aHR0cHM6Ly9jYS50ZHMuYWlyYXN0Lm9yZy9zdHVkZW50</code>
Specify the URL of the PAC file	Windows	<code>CASecureBrowser.exe -proxy 2:fake-url.com aHR0cHM6Ly9jYS50ZHMuYWlyYXN0Lm9yZy9zdHVkZW50</code>
Specify the URL of the PAC file	Mac	<code>./CASecureBrowser -proxy 2:fake-url.com aHR0cHM6Ly9jYS50ZHMuYWlyYXN0Lm9yZy9zdHVkZW50</code>
Specify the URL of the PAC file	Linux	<code>./CASecureBrowser.sh -proxy 2:fake-url.com aHR0cHM6Ly9jYS50ZHMuYWlyYXN0Lm9yZy9zdHVkZW50</code>

Table 14 (second continuation)

Description	System	Command
Auto detect proxy settings	Windows	<code>CASecureBrowser.exe -proxy 4 aHR0cHM6Ly9jYS50ZHMuYWlyYXN0Lm9yZy9 zdHVkZW50</code>
Auto detect proxy settings	Mac	<code>./CASecureBrowser -proxy 4 aHR0cHM6Ly9jYS50ZHMuYWlyYXN0Lm9yZy9 zdHVkZW50</code>
Auto detect proxy settings	Linux	<code>./CASecureBrowser.sh -proxy 4 aHR0cHM6Ly9jYS50ZHMuYWlyYXN0Lm9yZy9 zdHVkZW50</code>
Use the system proxy setting (default)	Windows	<code>CASecureBrowser.exe -proxy 5 aHR0cHM6Ly9jYS50ZHMuYWlyYXN0Lm9yZy9 zdHVkZW50</code>
Use the system proxy setting (default)	Mac	<code>./CASecureBrowser -proxy 5 aHR0cHM6Ly9jYS50ZHMuYWlyYXN0Lm9yZy9 zdHVkZW50</code>
Use the system proxy setting (default)	Linux	<code>./CASecureBrowser.sh -proxy 5 aHR0cHM6Ly9jYS50ZHMuYWlyYXN0Lm9yZy9 zdHVkZW50</code>

Modifying Desktop Shortcuts to Include Proxy Settings

This subsection provides guidelines for passing a proxy setting to the secure browser. All commands in this subsection are examples only and assume that there is a shortcut for the secure browser on the student's desktop.

Modifying Desktop Shortcuts on Microsoft Windows

1. Right-click the desktop shortcut for the secure browser and select *Properties* from the shortcut menu.
2. Select the **[Shortcut]** tab.
3. If the *Target* field is disabled, do the following (otherwise, skip to step 4):
 - a. Close the *Properties* dialog box and delete the desktop shortcut for the secure browser.
 - b. **/Program Files (x86) subdirectory:** Create a new desktop shortcut in Windows Explorer by navigating to the relevant 32-bit subdirectory, `C:\Program Files (x86)\`. Right-click the file `CASecureBrowser.exe` and then select *Send To → Desktop (create shortcut)*.

- c. **/Program Files (x86) subdirectory:** Create a new desktop shortcut in Windows Explorer by navigating to `C:\Program Files\CASecureBrowser\`, right-clicking the file `CASecureBrowser.exe`, and then selecting *Send To* → *Desktop (create shortcut)*.
- d. Right-click the desktop shortcut for the secure browser and select *Properties*.
- e. Select the [**Shortcut**] tab.
4. In the *Target* field, modify the command as specified in [table 14](#). For example:

```
"C:\Program Files  
(x86)\CASecureBrowser\CASecureBrowser.exe" -proxy 1:http:fake-  
url.com:8080 aHR0cHM6Ly9jYS50ZHMuYWlyYXN0Lm9yZy9zdHVkZW50
```
5. Select [**OK**].

Modifying Desktop Shortcuts on macOS

1. In Finder, navigate to *Applications* → *Utilities* and open Terminal.
2. Change to the desktop directory.

```
cd ~/Desktop
```
3. Create a file `securebrowser.command` on the desktop using a text editor such as `pico`.

```
pico securebrowser.command.
```
4. Copy or type the following lines:

```
#!/bin/sh  
  
/Applications/CASecureBrowser.app/Contents/MacOS/./  
CASecureBrowser -proxy 1:http:fake-url.com:8080 &  
aHR0cHM6Ly9jYS50ZHMuYWlyYXN0Lm9yZy9zdHVkZW50
```
5. Be sure to specify the complete path to the secure browser and the desired proxy option. Ensure the command ends with an ampersand (&). Save the file and exit the editor by pressing [Ctrl] + [O], [Enter], and then [Ctrl] + [X].
6. Apply execute permission to the file. In Terminal, type

```
chmod a+x securebrowser.command
```
7. Close Terminal.
8. Select the `securebrowser.command` icon on the desktop. The secure browser opens with the configured proxy setting.

This page is left blank intentionally.

Appendices

Appendix A: Operating System Support Plan for the 2020–21 Test Delivery System

A supported operating system is one for which Cambium Assessment, Inc. (CAI) provides updates to the secure browser for that operating system. CAI provides such updates as the supported operating systems are updated or as bugs in the secure browser are detected and fixed.

The support plan describes CAI’s plan for supporting operating systems during the upcoming test administration and following years. This plan helps local educational agencies (LEAs) and schools manage operating system deployments based on the support timelines.

There are two parts to the support plan: the “Timing of Secure Browser Updates” subsection and [table 15](#) through [table 19](#), the supported operating systems tables.

Timing of Secure Browser Updates

CAI will support major and minor version upgrades for Windows, Macintosh, Linux, iOS or iPadOS, and Chrome OS upon the completion of internal testing following their release. CAI may provide secure browser updates for new major and minor version upgrades of Windows, Macintosh, Linux, iOS or iPadOS, and Chrome OS, if necessary.

A “major version upgrade” of an operating system is usually denoted by an increase in the version designation’s whole number. For example, the upgrade from Windows 8 to Windows 10 was a major version upgrade.

A “minor version upgrade” is usually denoted by an increase in a number after a decimal point. For example, the upgrade from OS X 10.10 to 10.11 was a minor version upgrade. For minor version upgrades to iOS or iPadOS or Chrome operating systems, CAI will provide mobile secure browser updates to ensure compatibility.

Support Plan for Operating Systems

[Table 15](#) through [table 19](#) list the operating systems and the anticipated end-of-support dates.

Windows



Notes:

- CAI’s support for a Windows operating system ends 10 school years after its release date. For the most part, this coincides with Microsoft’s official end-of-life policies for its operating systems.
- If Microsoft ends support for an operating system sooner than six years after its release, then CAI will stop supporting that system after one full school year.

Table 15. Supported Operating Systems—Windows

Supported Operating System	Release Date	Anticipated End-of-Support Date
8 (Professional and Enterprise)	October 2012	End of 2021–22 school year
8.1 (Professional and Enterprise)	October 2013	End of 2022–23 school year
10, 10 in S mode (Educational, Professional, and Enterprise) (Versions 1809–2004)	July 2015, rolling	End of 2024–25 school year
Server 2012 R2	October 2013	End of 2022–23 school year
Server 2016 R2	October 2016	End of 2025–26 school year

Mac



Notes: MacOS computers with PowerPC processors are not supported.

- Apple does not document end-of-life status for its products. CAI recommends using the most recent releases.
- As long as Apple continues to release new versions of macOS annually, CAI will support the six latest versions in 2020–21. By fall 2022, CAI will transition to a support policy of four active versions of macOS.
- If Apple ends support for an operating system sooner than six years after its release, then CAI will stop supporting that system after one full school year.

Table 16. Supported Operating Systems—OS X and macOS (Intel)

Supported Operating System	Release Date	Anticipated End-of-Support Date
10.11	September 2015	End of 2020–21 school year
10.12	September 2016	End of 2020–21 school year
10.13	September 2017	End of 2021–22 school year
10.14	September 2018	End of 2021–22 school year
10.15	October 2019	End of 2022–23 school year
10.16	October 2020	End of 2022–23 school year

Linux



Notes:

- Official Fedora support typically ends one to two years after a release.
- Ubuntu typically supports long-term support (LTS) distributions for five years after a release.
- For Linux distributions, CAI will end support at the end of a full school year after the official distributor's announced end-of-life support date.

Table 17. Supported Operating Systems—Linux

Supported Operating System	Release Date	Anticipated End-of-Support Date
Fedora 30 LTS (Gnome)	April 2019	End of 2022–23 school year
Fedora 31 LTS (Gnome)	October 2019	End of 2023–24 school year
Ubuntu 16.04 LTS (Gnome)	April 2016	End of 2020–21 school year
Ubuntu 18.04 LTS (Gnome)	April 2018	End of 2022–23 school year
Ubuntu 20.04 LTS (Gnome)	April 2020	End of 2023–24 school year

Apple Mobile



Notes:

- Supported iPads have 9.7" or larger displays and run a supported version of iOS or iPadOS.
- Apple iOS or iPadOS operating systems are released on a rolling basis.

Table 18. Supported Operating Systems—iOS or iPadOS

Supported Operating System	Release Date	Anticipated End-of-Support Date
12.4	September 2018; rolling	CAI supports the three most recent major releases of iOS or iPadOS.
13.4	March 2020; rolling	CAI supports the three most recent major releases of iOS or iPadOS.
14	Pending acceptance	CAI supports the three most recent major releases of iOS or iPadOS.

Chrome



Note: Google releases new versions of Chrome OS every six weeks. Support may require updating the Chrome kiosk application.

Table 19. Supported Operating Systems—Chrome OS

Supported Operating System	Release Date	Anticipated End-of-Support Date
85 and above	August 2020; rolling	For any given school year, CAI supports the version of Chrome OS available during the summer months and all subsequent versions. For example, if Chrome OS version 85 is released in July, it and all versions of Chrome after it will be supported until July of the following year.

Appendix B: URLs for Testing Systems

This appendix presents information about the URLs for California Assessment of Student Performance and Progress (CAASPP) and English Language Proficiency Assessments for California (ELPAC) online testing. Ensure the network's firewalls are open for these URLs.



Note: In January 2020, Cambium Learning acquired AIR Assessment, the student assessment division of the American Institutes for Research (AIR). This division is now known as Cambium Assessment, Inc. (CAI). **URLs that included “airst.org” have been updated to “cambiumast.com.”**

URLs for Nontesting Sites

[Table 20](#) lists URLs for nontesting sites, such as the Test Operations Management System (TOMS), Test Information Distribution Engine (TIDE), California Educator Reporting System (CERS), Online Reporting System (ORS), and Learning Point Navigator. Local educational agencies (LEAs) are encouraged to add these URLs to local allowlists.



Note: The Single Sign-on system provides access to the following systems using the same username and password (although the type of access is determined by the user role):

- CERS
- Data Entry Interface (DEI)
- Interim Assessment Hand Scoring System (for interim assessments)
- Interim Assessment Viewing System
- ORS
- Practice and Training Tests Site
- Teacher Hand Scoring System (for the Initial ELPAC)
- Test Administrator Interface
- TIDE (used in association with the Completion Status and Roster Management systems)
- TOMS
- Tools for Teachers

Table 20. URLs for Nontesting Websites

Destination	URL
CAASPP website	http://www.caaspp.org/
CERS	https://login.smarterbalanced.org/sso/saml2/Ooa14zrzacExSAFK5357?fromURI=https://login.smarterbalanced.org/home/smarterbalancedassessmentconsortium_cersproduction_1/Ooa17s5opaczfbT05357/aln17sbcwtNiV39Uq357
Completion Status/Roster Management	https://ca.tide.cambiumast.com
DEI	https://ca.tds.cambiumast.com/student/?a=ResponseEntry
ELPAC Teacher Hand Scoring System	https://ca-elpac.tss.cambiumast.com
ELPAC website	https://www.elpac.org/
Interim Assessment Hand Scoring System	https://ca.tss.cambiumast.com
Interim Assessment Viewing System	https://capt.tds.cambiumast.com/student/?a=ResponseEntry
ORS	https://ca.reports.cambiumast.com/
Practice and Training Test Site	https://capt.tds.cambiumast.com/student
Secure browser installation files	https://ca.portal.cambiumast.com/
SurveyGizmo (This website hosts CAASPP and ELPAC forms and surveys.)	http://www.sgizmo.com http://www.surveygizmo.com http://www.surveygizmo.eu
Test Administrator Interface	https://ca.tds.cambiumast.com/testadmin
TOMS	https://mytoms.ets.org/
Tools for Teachers	https://smartertoolsforteachers.org/

URLs for Testing Sites

Testing sites provide test items as well as support services such as dictionaries and thesauruses.

Test Administrator, Test Examiner, and Student Testing Websites

Testing servers and satellites may be added or modified during the school year to ensure an optimal testing experience. As a result, a user is strongly encouraged to allowlist at the root level. This requires using a wildcard. For the 2020–21 test administration, users should add both CAI and American Institutes for Research URLs listed in this table to the LEA allowlist.

URLs for testing websites are listed in [table 21](#).

Table 21. URLs for Testing Websites

Systems	URLs
<ul style="list-style-type: none"> • Test administrator, test examiner, and student testing websites • Assessment viewing application 	<ul style="list-style-type: none"> *.cambiumast.com *.tds.cambiumast.com *.cloud1.tds.cambiumast.com *.cloud2.tds.cambiumast.com *.airast.org *.tds.airast.org *.cloud1.tds.airast.org *.cloud2.tds.airast.org

Online Dictionary and Thesaurus

Some online assessments contain an embedded dictionary and thesaurus provided by Merriam-Webster. The Merriam-Webster internet protocol (IP) addresses listed in [table 22](#) also should be allowlisted to ensure that students can use them during testing.

Table 22. URLs for Online Dictionary and Thesaurus

Domain Name	IP Address
media.merriam-webster.com	64.124.231.250
www.dictionaryapi.com	64.124.231.250

Appendix C: Technology Coordinator Checklist

This checklist can be printed out and referred to during review of networks and devices used for testing.

- ACTIVITY: Verify that all devices at a school that will be used for online testing meet the operating system requirements.**

Estimated Time to Complete: 5–10 hours

Target Completion Date: 3–4 weeks before testing begins in the school, which can be as early as August 20, 2020

Reference: [Chapter 1: System Requirements](#)

- ACTIVITY: Verify that the school’s network and internet are properly configured for testing, conduct network diagnostics, and resolve any issues.**

Estimated Time to Complete: 5–10 hours

Target Completion Date: 3–4 weeks before testing begins in the school, which can be as early as August 20, 2020

Reference: [Chapter 2: Network Configuration](#)

- ACTIVITY: Confirm that URLs for testing sites and the online dictionary and thesaurus have been allowlisted on the server.**

Estimated Time to Complete: 30 minutes

Target Completion Date: 3–4 weeks before testing begins in the school, which can be as early as August 20, 2020

Reference: [Appendix B: URLs for Testing Systems](#)

- ACTIVITY: Verify that auto updating for all software installed on testing devices has either been turned off or configured to run before or after school hours or at some other time when testing is not scheduled.**

Estimated Time to Complete: 5–10 hours

Target Completion Date: 3–4 weeks before testing begins in the school, which can be as early as August 20, 2020

Reference: [“Turn Off Background Jobs”](#)

- ACTIVITY: Install the secure browser on all devices that will be used for testing.**

Estimated Time to Complete: 5–10 hours

Target Completion Date: 3–4 weeks before testing begins in the school, which can be as early as August 20, 2020

Reference: [Chapter 4: Secure Browser Configuration](#)

□ ACTIVITY: Review software requirements for each operating system.

Estimated Time to Complete: 5–10 hours

Target Completion Date: 1–2 weeks before testing begins in the school, which can be as early as August 20, 2020

Reference: [Chapter 3: System Configuration](#)

□ ACTIVITY: Enable pop-up windows on student devices.

Estimated Time to Complete: 5–10 hours

Target Completion Date: 1–2 weeks before testing begins in the school, which can be as early as August 20, 2020

Reference: “[Enabling Pop-Up Windows](#)”

□ ACTIVITY: On Windows devices, disable Fast User Switching. If a student can access multiple user accounts on a single device, consider disabling the Fast User Switching function.

Estimated Time to Complete: 5–10 hours

Target Completion Date: 1–2 weeks before testing begins in the school, which can be as early as August 20, 2020

Reference: “[Installing Windows Media Pack for Windows 8.1 N and 8.1 KN in Windows](#)”

□ ACTIVITY: On Mac devices, disable Fast User Switching. If a student can access multiple user accounts on a single device, consider disabling the Fast User Switching function.

Estimated Time to Complete: 5–10 hours

Target Completion Date: 1–2 weeks before testing begins in the school, which can be as early as August 20, 2020

Reference: “[Disabling Fast User Switching](#)”

□ ACTIVITY: On Mac devices, install the Mac Secure Profile.

Estimated Time to Complete: 5–10 hours

Target Completion Date: 1–2 weeks before testing begins in the school, which can be as early as August 20, 2020

Reference: “[Installing the Mac Secure Profile](#)”

□ ACTIVITY: On iPads, ensure that Assessment Mode is enabled.

Estimated Time to Complete: 5–10 hours

Target Completion Date: 1–2 weeks before testing begins in the school, which can be as early as August 20, 2020

Reference: “[Using Assessment Mode](#)”

□ ACTIVITY: On iOS or iPadOS devices, ensure that features that might pose a security risk are disabled.

Estimated Time to Complete: 5–10 hours

Target Completion Date: 1–2 weeks before testing begins in the school, which can be as early as August 20, 2020

Reference: “[iOS or iPadOS Testing Device Configuration](#)”

Appendix D: Scheduling Online Testing

Number of Devices and Hours Required to Complete Online Tests

It is recommended that schools arrange their resources to accommodate the number of students who will be testing at the same time for ease of test administration. The Sample Test Scheduling Worksheet in this appendix shows how to estimate the number of testing hours needed to administer one testing opportunity.



Note: This worksheet may need to be modified based on the network setup. Technology coordinators may want to work with the California Assessment of Student Performance and Progress test site coordinator or site English Language Proficiency Assessments for California coordinator to adapt this worksheet as necessary, so the school does not risk overloading its wired or wireless network.

Sample Test Scheduling Worksheet

For each school, enter the following for each online test:

Number	Result
Number of devices available for testing at once:	[number]
Number of students who need to take the test:	[number]
Number of test administrators and test examiners who need a device:	[number]
Estimated number of hours needed per student to complete the test: (This estimate should include approximately 15 minutes for students to get set up and logged on as well as the average estimated time to complete the test.)	[number]
Number of hours that must be scheduled to administer the test: [(students) × hours ÷ devices =]	[number]

Example:

- School A has a total of 60 student devices available for testing at once.
- 120 students in grade five will need to take the mathematics assessment.
- Number of hours needed to administer test is 120 students × 1 hour per student ÷ 60 devices = 2 hours (plus 15 minutes for setup).

Appendix E: Creating Group Policy Objects to Assign Logon Scripts in Microsoft Windows

Additional Resources in This Section:

- Microsoft Create a Group Policy Object web page—<https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/create-a-group-policy-object>
- Microsoft Create and Edit a Group Policy Object web page—[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc754740\(v=ws.11\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc754740(v=ws.11))

Some of the procedures in the subsection “[Installing the Secure Browser on Windows](#)” refer to creating a group policy object that contains instructions for Windows to execute upon certain events. The procedure in this appendix explains how to create a group policy object that runs a script when a user logs on. The script itself is saved in a file called `logon.bat`.

1. In the task bar (Windows 10), or in *Start* → *Run* (previous versions of Windows), enter `gpedit.msc` and then select the link. The *Local Group Policy Editor* window, shown in [figure 81](#), appears.

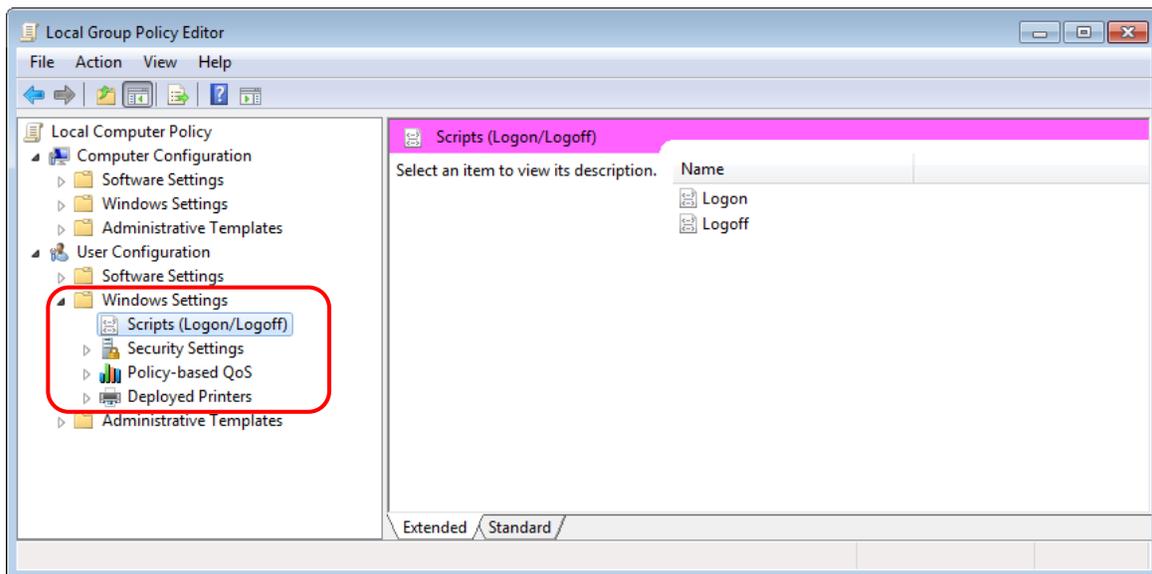


Figure 81. The *Local Group Policy Editor* window

2. Expand *Local Computer Policy* → *User Configuration* → *Windows Settings* → *Scripts (Logon/Logoff)* (indicated in [figure 81](#)).

3. Select [**Logon**] and then select [Properties]. The *Logon Properties* dialog box appears.
4. Select [**Add**] (indicated in [figure 82](#)). The *Add a Script* dialog box appears.

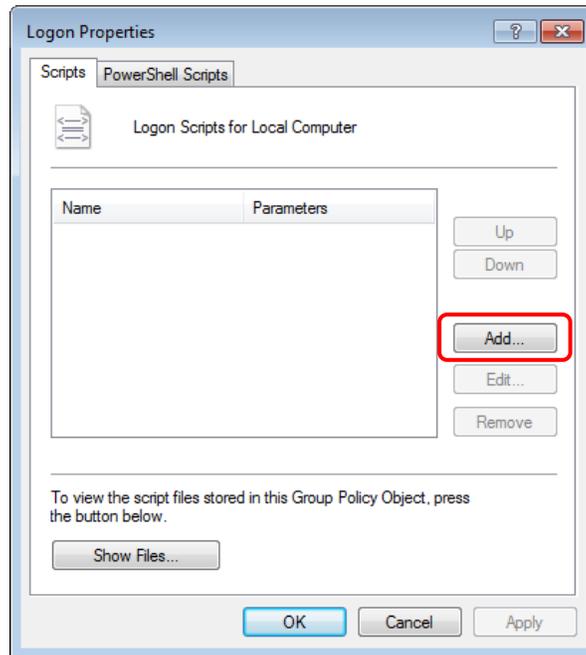


Figure 82. The *Logon Properties* dialog box

5. Select [**Browse...**] (indicated in [figure 83](#)) and navigate to the `logon.bat` to be run.

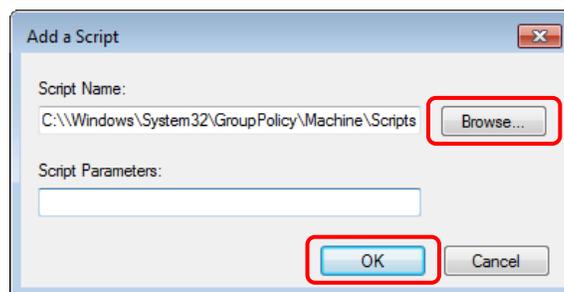


Figure 83. The *Add a Script* dialog box

6. Select [**OK**] (also indicated in [figure 83](#)) to return to the *Logon Properties* dialog box.
7. Select [**OK**] to return to the Local Group Policy Editor.
8. Close the Local Group Policy Editor.

Appendix F: Resetting Secure Browser Profiles

A user who has been advised by the California Technical Assistance Center to reset the secure browser profile should use the instructions in this appendix.

Resetting Secure Browser Profiles on Windows

1. Log on as an admin user or the user who installed the secure browser and close any open secure browsers.
2. Delete the contents of the following folders:
`C:\Users\username\AppData\Local\CAI\
C:\Users\username\AppData\Roaming\CAI\
where username is the Windows user account where the secure browser is installed. (Keep the CAI\ directories; just delete their contents.)`
3. Start the secure browser.

Resetting Secure Browser Profiles on macOS

1. Log on as the admin user or the user who installed the secure browser and close any open secure browsers.
2. Start the Finder.

3. While pressing [Option], select *Go* → *Library*. The contents of the *Library* folder appear (shown in [figure 84](#)).

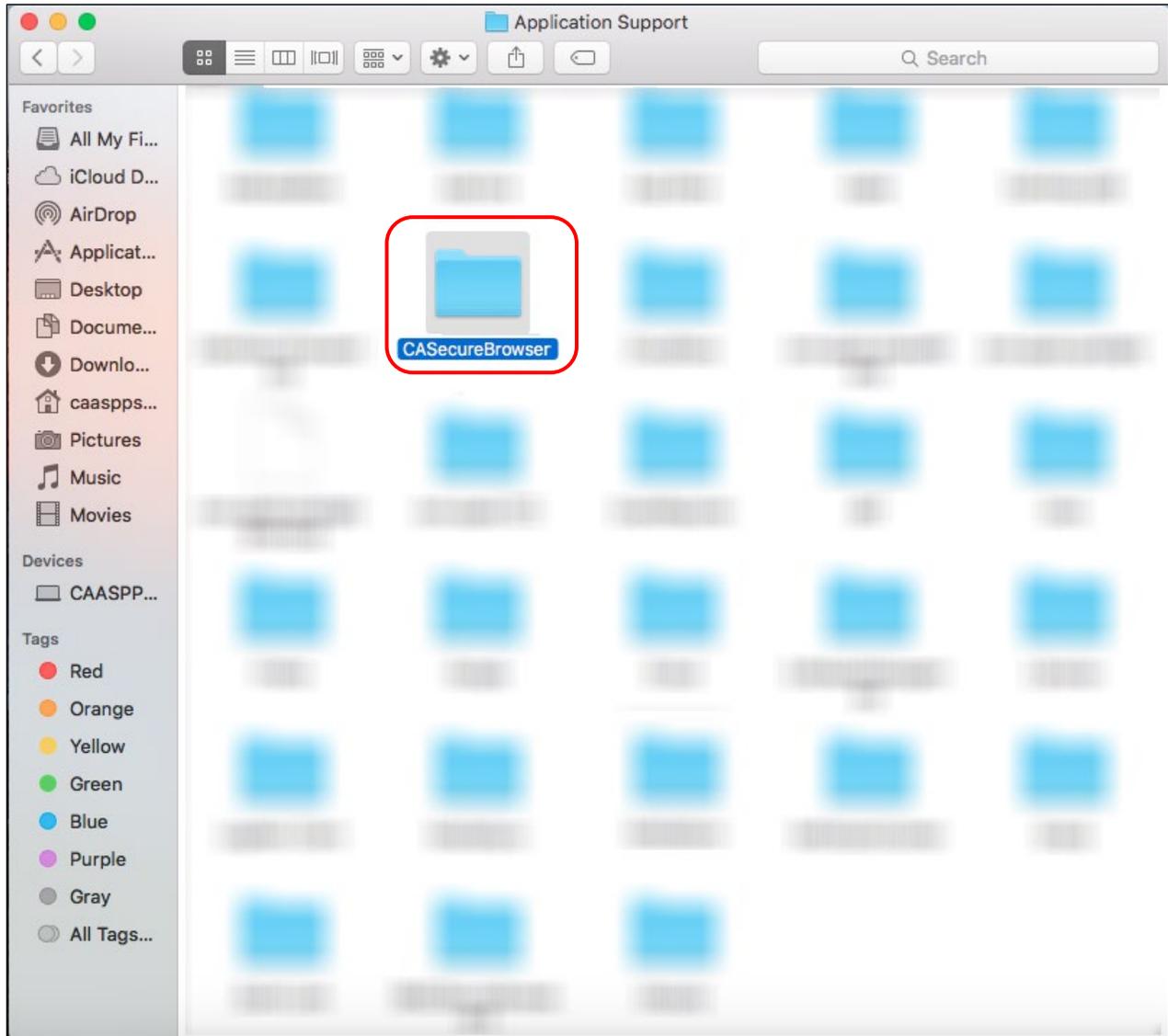


Figure 84. Resetting the secure browser on OS X and macOS

4. Open the *Caches* folder.
5. Delete the folder containing the secure browser.
6. Restart the secure browser.

Resetting Secure Browser Profiles on Linux

1. Log on as a superuser or the user who installed the secure browser and close any open secure browsers.
2. Open a terminal and delete the contents of the following directories:

```
/home/username/.cai
```

```
/home/username/.cache/cai
```

where `username` is the user account where the secure browser is installed. (Keep the directories; just delete their contents.)

3. Restart the secure browser.

Appendix G: User Support

Local educational agency (LEA) California Assessment of Student Performance and Progress (CAASPP) and English Language Proficiency Assessments for California (ELPAC) coordinators should first contact the LEA technology coordinator or system administrator prior to contacting the California Technical Assistance Center (CaITAC).

Technology coordinators, CAASPP test site coordinators, and site ELPAC coordinators should contact their LEA CAASPP or ELPAC coordinator for assistance.

CaITAC for LEA CAASPP and ELPAC Coordinators

When contacting CaITAC, a user will be asked to provide as much detail as possible about the issue(s).

CaITAC

Hours: 7 a.m. to 5 p.m., Monday–Friday

Toll-Free Phone Support: 800-955-2954

Email Support: caltac@ets.org

Websites: <http://www.caaspp.org/> and <https://www.elpac.org/>

Always include the following information:

- Test administrator or test examiner name and information technology or network contact person and contact information
- Statewide Student Identifier(s) of affected students
- Session ID for the affected student test session
- Operating system and secure browser version information
- Any error messages and codes that appeared, if applicable
- Information about the network configuration:
 - Secure browser installation (to individual devices or network)
 - Wired or wireless internet network setup



Warning: *Never* provide any other student information, as doing so may violate Family Educational Rights and Privacy Act policies.

Appendix H: Change Log

Change(s)	Section(s)	Date
[to be determined]	[to be determined]	[to be determined]
[to be determined]	[to be determined]	[to be determined]