

CALIFORNIA

Assessment of Student Performance and Progress

Technical Specifications and Configuration Guide for CAASPP Online Testing

◆ System Requirements ◆
Network Configuration ◆ System Configuration ◆
Secure Browser Configuration ◆

Summative and Interim Assessments
Test Administrator Sites
Student Practice Tests
Test Operations Management System
Online Reporting System
Interim Assessment Hand Scoring System



California Assessment of
Student Performance and Progress



Table of Contents

Introduction	1
Manual Content	2
What's New in 2018–19	2
Sections	4
Document Conventions	5
Intended Audience	5
Chapter 1. System Requirements	7
Supported Operating Systems for Student Testing	8
Desktops and Laptops	8
Tablets	12
Chromebooks and Chromebases	13
Thin Clients: NComputing and Terminal Servers for Windows	14
Supported Web Browsers for Online Systems Associated with Testing	15
Supported Web Browsers by Operating System	15
Available Audio Settings by Web Browser	19
Requirements for Peripheral Equipment	20
Monitors and Screen Display Requirements	20
Keyboards	21
Mice	21
Headsets and Headphones	21
Chapter 2. Network Configuration	23
Network Configuration and Testing	24
Network Configuration	24
Network Diagnostic Tools	27
Chapter 3. System Configuration	31
Hardware Configuration	32
Connections Between Printers and Testing Devices	32
Wireless Networking and Determining the Number of Wireless Access Points (WAPs)	32
Hardware for Braille Testing	33
Software Configuration	34
Optimal Installation Scenario for Secure Browsers	34
Configuring Commercially Available Web Browsers	35
Configuring Devices for Online Testing with the Secure Browser	39
Configuring Network Settings for Online Testing	77
Installing CloudReady on PCs and Macs	78
Configurations for Testing Students Using Accessibility Supports	80
Chapter 4. Secure Browser Configuration	81
Overview of Secure Browsers	82
About the Secure Browser	82
Secure Browser Versions for Online Testing	84
Forbidden Application Detection	85
Secure Browser Error Messages	85
Installing the Secure Browser on Desktops and Laptops	86
Installing the Secure Browser on Windows	86
Installing the Secure Browser on Mac OS X	97
Installing the Secure Browser on Linux	100

Installing the Secure Browser on Mobile Devices	104
Installing the Secure Browser on iOS	104
Installing AIRSecureTest on Android	107
Chrome OS AIRSecureTest Kiosk App	110
Installing the Secure Browser on Windows Mobile Devices	121
Proxy Settings for Desktop Secure Browsers	122
Specifying a Proxy Server to Use with the Secure Browser	122
Modifying Desktop Shortcuts to Include Proxy Settings	124
Appendices	127
Appendix A. Operating System Support Plan for the 2018–19 Test Delivery System	128
Timing of Secure Browser Updates	128
Support Plan for Operating Systems	129
Appendix B. URLs for Testing Systems	133
URLs for Nontesting Sites	133
URLs for Testing Sites	134
Appendix C. Technology Coordinator Checklist	135
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	138
Appendix F. Resetting Secure Browser Profiles	140
Resetting Secure Browser Profiles on Windows	140
Resetting Secure Browser Profiles on OS X 10.9 or Later	140
Resetting Secure Browser Profiles on Linux	141
Appendix G. User Support	142
California Technical Assistance Center for LEA CAASPP Coordinators	142
Appendix H. Change Log	143

List of Tables

Table 1. Key Symbols and Document Conventions	5
Table 2. Supported Desktop Operating Systems	9
Table 3. Supported Tablets and Operating Systems	12
Table 4. Supported Chromebooks	13
Table 5. Supported NComputing Solutions	14
Table 6. Supported Terminal Servers	14
Table 7. Supported Web Browsers by Test Administration Website	15
Table 8. Available Audio Settings by Browser	19
Table 9. Supported Headphones and Headsets	22
Table 10. Average Bandwidth Used by Secure Browser for Testing	25
Table 11. Ports and Protocols for the TDS	26
Table 12. Recommended Ratios of Devices to Wireless Access Points	33
Table 13. Profile Keys for Features in iOS 10 or Later	65
Table 14. Secure Browsers by Operating System	84
Table 15. Specifying Proxy Settings Using a Shortcut or the Command Line	122
Table 16. Supported Operating Systems—Windows	129
Table 17. Supported Operating Systems—Mac OS X (Intel)	130
Table 18. Supported Operating Systems—Linux	130

Table 19. Supported Operating Systems—iOS	131
Table 20. Supported Operating Systems—Android	132
Table 21. Supported Operating Systems—Chrome OS	132
Table 22. URLs for Nontesting Sites	133
Table 23. URLs for Testing Websites	134
Table 24. URLs for Online Dictionary and Thesaurus	134

List of Figures

Figure 1. Sign-in web page for the training test	28
Figure 2. Run the diagnostics test	29
Figure 3. Internet Explorer <i>Internet Options</i> dialog box	37
Figure 4. Internet Explorer <i>Security Settings</i> dialog box	38
Figure 5. Safari Advanced preferences	39
Figure 6. Windows Search box	40
Figure 7. <i>Local Group Policy Editor</i> screen options	40
Figure 8. Finish in the Windows <i>Local Group Policy Editor</i> screen	40
Figure 9. Windows Search charm	40
Figure 10. Windows Local Group Policy Editor options	41
Figure 11. Windows Local Group Policy Editor selection	41
Figure 12. Windows <i>Run</i> dialog box	42
Figure 13. Notification in the Windows <i>Command</i> window	42
Figure 14. Windows Search box	43
Figure 15. <i>Local Group Policy Editor</i> screen options	43
Figure 16. <i>Ctrl+Alt+Del Options</i> settings	44
Figure 17. <i>Remove Task Manager</i> screen	44
Figure 18. Windows Search box	45
Figure 19. <i>Local Group Policy Editor</i> screen	46
Figure 20. Windows Components in the Local Group Policy Editor	46
Figure 21. Input Panel in the Local Group Policy Editor	47
Figure 22. <i>Disable text prediction</i> selection	47
Figure 23. <i>Disable text prediction</i> screen	48
Figure 24. Surface Pro 3 <i>Settings</i> interface	49
Figure 25. <i>Touch keyboard</i> settings interface	50
Figure 26. <i>Mouse Properties</i> dialog box	51
Figure 27. <i>Properties for Synaptics TouchPad V7.5 on PS/2 Port</i> dialog box	51
Figure 28. Select OS X System Preferences	53
Figure 29. [Keyboard] icon	53
Figure 30. [Keyboard Shortcuts] tab	53
Figure 31. OS X Mission Control options	53
Figure 32. <i>Mission Control</i> screen	54
Figure 33. <i>Apple System Preferences</i> screen	55
Figure 34. Keyboard options	55
Figure 35. <i>App Store</i> screen	56
Figure 36. Advanced Preferences options	57
Figure 37. Trackpad Preferences options, [Point & Click] tab	58
Figure 38. Trackpad Preferences options, [More Gestures] tab	58
Figure 39. [Keyboard] button in OS X System Preferences	60
Figure 40. Dictation system preferences options in OS X	61

Figure 41. [Siri] button in OS X System Preferences	61
Figure 42. Siri system preferences options in OS X	62
Figure 43. <i>Settings</i> options in Apple Configurator	66
Figure 44. <i>Create New Profile</i> configuration options	67
Figure 45. <i>Preferences</i> options	68
Figure 46. <i>Organization Info</i> screen	69
Figure 47. <i>Apple Configurator</i> screen	70
Figure 48. Notification when starting test with automatic assessment configuration	71
Figure 49. Emoji keyboard for iOS	71
Figure 50. [Settings] icon	72
Figure 51. Keyboards configuration interface	72
Figure 52. Disabled dictation	72
Figure 53. Keyboard Settings for iOS 10 (other versions of iOS are similar)	73
Figure 54. Disable the Multi window	74
Figure 55. Disable the Samsung stylus	75
Figure 56. Chrome <i>Sign-in Settings</i> options	76
Figure 57. Chromebook Recovery Utility	79
Figure 58. Selecting the CloudReady image	79
Figure 59. CloudReady media insertion prompt	79
Figure 60. [Download Browser] button	87
Figure 61. [CASecureBrowser] shortcut icon	87
Figure 62. [Download Browser] button	88
Figure 63. [CASecureBrowser] shortcut icon	89
Figure 64. [CASecureBrowser] shortcut icon	90
Figure 65. <i>Create Shortcut</i> dialog box	96
Figure 66. [Download Browser] button	97
Figure 67. Contents of the CASecureBrowser-OSX.dmg folder	98
Figure 68. <i>Security & Privacy</i> screen for Mac OS X 10.11	98
Figure 69. Apple <i>Application Support</i> configuration interface	100
Figure 70. [Download Browser] button	101
Figure 71. [CASecureBrowser] shortcut icon	102
Figure 72. [Download on the App Store] button	105
Figure 73. AIRSecureTest App Store download web page	105
Figure 74. [AIRSecureTest] icon, iOS	105
Figure 75. Select the state from the Launchpad	106
Figure 76. Select the assessment from the Launchpad	106
Figure 77. [Get it on Google play] button	107
Figure 78. AIRSecureTest Google Play download web page	108
Figure 79. [AIRSecureTest] icon, Android	108
Figure 80. Select the state from the Launchpad	109
Figure 81. Select the assessment from the Launchpad	109
Figure 82. Chromebook <i>Welcome</i> screen	111
Figure 83. Chrome OS <i>Missing</i> message	111
Figure 84. Turn OS Verification Off message	111
Figure 85. OS Verification Is Off message	111
Figure 86. Preparing for Developer Mode message	112
Figure 87. <i>Join WiFi Network</i> screen	112
Figure 88. Chromebook <i>Sign in</i> screen	113

Figure 89. <i>Automatic Kiosk Mode</i> message	113
Figure 90. <i>Extensions</i> screen	113
Figure 91. <i>Manage Kiosk Applications</i> screen	114
Figure 92. Chrome <i>Admin console</i> screen	115
Figure 93. Chrome <i>Device management</i> screen	116
Figure 94. Chrome <i>Management</i> screen	117
Figure 95. Chrome <i>App Management</i> screen	118
Figure 96. Select [Kiosk settings]	118
Figure 97. Chrome <i>Kiosk settings</i> screen	119
Figure 98. Chromebook logon screen	120
Figure 99. Select the state from the Launchpad	120
Figure 100. Select the assessment from the Launchpad	121
Figure 101. The <i>Local Group Policy Editor</i> window	138
Figure 102. The <i>Logon Properties</i> dialog box	139
Figure 103. The <i>Add a Script</i> dialog box	139
Figure 104. Resetting the secure browser on OS X 10.9 or later	141

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

Abbreviation	Term
AIR	American Institutes for Research
ASAM	Autonomous Single App Mode
CAASPP	California Assessment of Student Performance and Progress
CaITAC	California Technical Assistance Center
CAST	California Science Test
CDE	California Department of Education
CSA	California Spanish Assessment
DEI	Data Entry Interface
IAHSS	Interim Assessment Hand Scoring System
ISP	internet service provider
LAN	local area network
LEA	local educational agency
Mbps	megabits per second
MDM	mobile device management
ORS	Online Reporting System
STS	Standards-based Tests in Spanish
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 California Assessment of Student Performance and Progress (CAASPP) testing.

What's New in 2018–19

CAASPP Assessments

The following CAASPP assessments have been added to the list of assessments supported by the specifications and configurations described in this manual:

- California Alternate Assessment for Science
- California Spanish Assessment (field test and operational assessment)

Secure Browser Versions

The following are the updated secure browser versions for the 2018–19 CAASPP administration. These are the only secure browser versions supported for testing.

Operating System	Device Type	Secure Browser Version
Android	Mobile	5
Apple iOS	Mobile	5
Chrome	Mobile	5
Macintosh OS X	Desktop/Laptop	10.3
Windows	Desktop/Laptop	10.3
Linux	Desktop/Laptop	10.3

Operating Systems for Student Testing

See “[Supported Operating Systems for Student Testing](#)” for complete information about operating system versions supported for the 2018–19 CAASPP administration.

Support

If Microsoft or Apple ends support for an operating system sooner than six years after its release, then the American Institutes for Research will stop supporting that system one full school year after support ends. *(Previously, support was offered for 10 years after its release.)*

Additions

Operating System	Device Type	Operating System Addition
Android	Mobile	<ul style="list-style-type: none"> Version 7.1 Version 8.1 Version 9 (when released and tested)
Apple iOS	Mobile	<ul style="list-style-type: none"> iOS 12 (when released and tested)
Chrome	Mobile	<ul style="list-style-type: none"> Version 67 and above
Macintosh OS X	Desktop/Laptop	<ul style="list-style-type: none"> OS 10.14 when released and tested
Windows	Desktop/Laptop	<ul style="list-style-type: none"> Windows 10 versions 1507–1803 Windows 10 version 1809 (when released and tested)
Linux	Desktop/Laptop	<ul style="list-style-type: none"> Fedora 27 Fedora 28

Deletions

Operating System	Device Type	Operating System Deletion
Android	Mobile	<ul style="list-style-type: none"> Version 6 and below
Apple iOS	Mobile	<ul style="list-style-type: none"> iOS 9
Chrome	Mobile	<ul style="list-style-type: none"> Version 66 and below
Macintosh OS X	Desktop/Laptop	<ul style="list-style-type: none"> OS 10.7 OS 10.8
Windows	Desktop/Laptop	<ul style="list-style-type: none"> (none)
Linux	Desktop/Laptop	<ul style="list-style-type: none"> Fedora 25 Fedora 26

Peripheral Support

Wireless and Bluetooth-based keyboards are no longer supported.

System Requirements

Internet Browsers

See “[Supported Web Browsers for Online Systems Associated with Testing](#)” for complete information about internet browsers supported in associated systems 2018–19 CAASPP administration.

Additions

The only new internet browser to be supported will be Safari 12 for the Apple iOS (when released and tested).

Deletions

What follows are the internet browsers that are no longer supported by CAASPP systems:

Operating System	Device Type	Browser Deletion	Affected System
Android	Mobile	• (none)	• (none)
Apple iOS	Mobile	• Safari 9 and below	• All
Chrome	Mobile	• (none)	• (none)
Macintosh OS X	Desktop/Laptop	• Safari 8 and below • Firefox 45–51	• All
Windows	Desktop/Laptop	• Internet Explorer	• Deleted for practice and training tests only
Linux	Desktop/Laptop	• (none)	• (none)

Sections

This manual contains the technology requirements for online CAASPP testing for the 2017–18 test administration contains the following sections:






- [Introduction](#) (this section), describes this guide.
- [Chapter 1, System Requirements](#), lists the minimum hardware and software requirements for online testing. Ensure your 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 2017–18 Test Delivery System](#), lists the operating systems supported for CAASPP testing and their projected end-of-support dates.
- [Appendix B, URLs for Testing Systems](#), lists URLs that should be whitelisted in your 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](#), 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 Help Desk information.

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 and/or web documents that provide additional information.
	Tip: This symbol accompanies useful information on how to perform a task.
<code>file name</code>	Monospaced text indicates a directory, file name, or something you enter 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. Technology coordinators should be familiar with the following concepts:
 - Networking—Bandwidth, firewalls, whitelisting, and proxy servers
 - Configuring operating systems—Control Panel in Windows, System Preferences in OS X, Settings in iOS, 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, Mac OS X, or Linux operating systems, or Chromebook, iPad, or Android 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.
- If you install and run the secure browser from an NComputing server, you should be familiar with operating that software and related hardware.

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 and/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) online testing.



Warning: Support for New Major Versions of Supported Operating Systems

- New major versions of supported operating systems must be tested by American Institutes for Research (AIR) before they can be used for online testing. Do not upgrade to new major versions before support is announced officially. AIR also recommends you disable auto-updates to keep systems from upgrading automatically. See [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 2017–18. 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"> • 7 SP1 (Professional and Enterprise) • 8.0 (Professional and Enterprise) • 8.1 (Professional and Enterprise) • 10, 10 in S mode; versions 1507–1803 (Professional, Educational, and Enterprise) • 10, version 1809 (Professional, Educational, and Enterprise) (supported upon completion of version testing and acceptance) • Server 2008 R2, 2012 R2, 2016 R2 (thin client) 	<ul style="list-style-type: none"> • 1.1 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 • 16 or more GB hard drive space
Mac OS X	<ul style="list-style-type: none"> • 10.9–10.13 • 10.14 (supported 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 • 16 or more GB hard drive space

System Requirements | Supported Operating Systems for Student Testing

Supported Operating System	Supported Versions	Minimum Requirements	Recommended Specifications
Linux (64-bit or 32-bit)	<ul style="list-style-type: none"> Fedora 27–28 LTS (Gnome) Ubuntu 14.04, 16.04 LTS (Gnome) 	<ul style="list-style-type: none"> 1.1 GHZ processor 1 GB RAM (32-bit) 2 GB RAM (64-bit) 16 GB hard drive space (32-bit) 20 GB hard drive space (64 bit) Required libraries/packages: <ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 1.4 GHZ processor 2 or more GB RAM 16 or more GB hard drive space Recommended libraries/packages; in addition to the required libraries listed under minimum requirements, the following should be installed: <ul style="list-style-type: none"> NetworkManager 0.7 or higher DBus 1.0 or higher HAL 0.5.8 or higher

Supported Operating System	Supported Versions	Minimum Requirements	Recommended Specifications
Linux (64-bit only)	<ul style="list-style-type: none"> • Ubuntu 18.04 LTS (Gnome) 	<ul style="list-style-type: none"> • 1 GHZ Processor • 2 GB RAM • 20 GB hard drive • Required libraries/packages: <ul style="list-style-type: none"> - 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 - GNOME 2.16 or higher - Sox - Net tools 	<ul style="list-style-type: none"> • 1.4 GHZ processor • 2 or more GB RAM • 16 or more GB hard drive space

Tablets



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

Table 3 lists the supported tablets, operating systems, and related requirements. See [Chapter 3, Hardware Configuration](#), for information about configuring these devices for online testing.

Table 3. Supported Tablets and Operating Systems

Operating System	Supported Version	Supported Tablets
iOS (iPads)	<ul style="list-style-type: none"> • 10.3 • 11.4 • 12 (supported upon completion of version testing and acceptance) 	<ul style="list-style-type: none"> • 4th generation (retina display) • 5th generation (retina display) • 6th generation (retina display) • iPad Air • iPad Air 2 • iPad Pro
Android	<ul style="list-style-type: none"> • 7.1 • 8.1 • 9 (supported upon completion of version testing and acceptance) 	<ul style="list-style-type: none"> • Lenovo Yoga Tab 3 10 • Samsung Galaxy Tab S3 • Asus ZenPad Z10
Windows	<ul style="list-style-type: none"> • 8.0 (Professional and Enterprise) • 8.1 (Professional and Enterprise) • 10 (Professional, Educational, and Enterprise) 	Any 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:

- Android for Education Help | Auto Update Policy web page—
<https://support.google.com/edu/android/answer/6220366>



Cautions:

- While AIR 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 AIR 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 AIR Secure Browser. (This change restricting kiosk mode does not affect the Chrome operating system. You can still use any version of the Chrome OS on hardware manufactured in 2016 or earlier.)
- Chrome OS includes a feature called tablet mode, which offers a touchscreen environment for supported Chromebooks and for Chrome OS tablets. AIR 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 and Chromebases.

Table 4. Supported Chromebooks

Supported Operating Systems	Related Requirements
Chrome OS 67+	AIR will support any device that Google actively supports for auto update. AIR will not support any device that Google does not support for auto update. See Google's Auto Update Policy web page for information on Google's auto update policy, including currently supported devices.

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 2008 R2 	<ul style="list-style-type: none"> vSpace Server 8.4 	<ul style="list-style-type: none"> L300, firmware version 1.12.xx
<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 M300, 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 2008 Windows Server 2012 Windows Server 2016 	Any thin client that supports a Windows Server



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. See the "[Installing the Secure Browser on a Terminal Server or Windows Server](#)" subsection of [Chapter 4, Secure Browser Configuration](#), for more information.

Supported Web Browsers for Online Systems Associated with Testing

This section lists the supported web browsers for the 2018–19 California Assessment of Student Performance and Progress (CAASPP) 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 only type of browser students use to take online assessments is the secure browser.**

Supported Web Browsers by Operating System

Table 7 lists the supported operating systems and corresponding web browsers for each application. It is recommended that you use recent versions of supported web browsers. 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 10.3 requires Safari 10.

Table 7. Supported Web Browsers by Test Administration Website

Operating System	Accepted Web Browser	TA Sites	Student Practice Test	TOMS	ORS	TIDE	IAHSS
Windows 7 SPI (Professional and Enterprise)	Chrome 67+	✓	✓	✓	✓	✓	✓
Windows 7 SPI (Professional and Enterprise)	Firefox 52+	✓	✓	✓	✓	✓	✓
Windows Version 8.0 (Professional and Enterprise) Version 8.1 (Professional and Enterprise)	Chrome 67+	✓	✓	✓	✓	✓	✓

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

Operating System	Accepted Web Browser	TA Sites	Student Practice Test	TOMS	ORS	TIDE	IAHSS
Windows <ul style="list-style-type: none"> 8.0 (Professional and Enterprise) 8.1 (Professional and Enterprise) 	Firefox 52+	✓	✓	✓	✓	✓	✓
Windows <ul style="list-style-type: none"> 8.0 (Professional and Enterprise) 8.1 (Professional and Enterprise) 	Internet Explorer 11	✓	NA	✓	✓	✓	✓
Windows 10 (Professional, Educational, and Enterprise) <ul style="list-style-type: none"> Versions 1507–1803 Version 1809 (upon acceptance) 	Chrome 67+	✓	✓	✓	✓	✓	✓
Windows 10 (Professional, Educational, and Enterprise) <ul style="list-style-type: none"> Versions 1507–1803 Version 1809 (upon acceptance) 	Firefox 52+	✓	✓	✓	✓	✓	✓
Windows 10 (Professional, Educational, and Enterprise) <ul style="list-style-type: none"> Versions 1507–1803 Version 1809 (upon acceptance) 	Internet Explorer 11	✓	NA	✓	✓	✓	✓

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

Operating System	Accepted Web Browser	TA Sites	Student Practice Test	TOMS	ORS	TIDE	IAHSS
Windows 10 in S mode (Professional, Educational, and Enterprise) <ul style="list-style-type: none"> • Versions 1507–1803 • Version 1809 (upon acceptance) 	Edge	✓	✓	✓	✓	✓	✓
Mac OS X <ul style="list-style-type: none"> • Versions 10.9–10.14 	Chrome 67+	✓	✓	✓	✓	✓	✓
Mac OS X <ul style="list-style-type: none"> • Versions 10.9–10.14 	Firefox 52+	✓	✓	✓	✓	✓	✓
Mac OS X <ul style="list-style-type: none"> • Versions 10.9–10.14 	Safari 9+	✓	✓	✓	✓	✓	✓
Linux Fedora LTS (Gnome) <ul style="list-style-type: none"> • Versions 27–28 	Chrome 67+	✓	✓	✓	✓	✓	✓
Linux Fedora LTS (Gnome) <ul style="list-style-type: none"> • Versions 27–28 	Firefox 52+	✓	✓	✓	✓	✓	✓
Linux Ubuntu (LTS) (Gnome) <ul style="list-style-type: none"> • Version 14.04 • Version 16.04 • Version 18.04 	Chrome 67+	✓	✓	✓	✓	✓	✓
Linux Ubuntu (LTS) (Gnome) <ul style="list-style-type: none"> • Version 14.04 • Version 16.04 	Firefox 52+	✓	✓	✓	✓	✓	✓
iOS 10.3	Safari 10	✓	✓	NA	NA	NA	✓
iOS 11.4	Safari 11	✓	✓	NA	NA	NA	✓
iOS 12 (upon acceptance)	Safari 12 (upon release)	✓	✓	NA	NA	NA	✓

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

Operating System	Accepted Web Browser	TA Sites	Student Practice Test	TOMS	ORS	TIDE	IAHSS
Android <ul style="list-style-type: none"> Version 7.1 Version 8.1 Version 9. (upon acceptance) 	Chrome 67+	✓	✓	NA	NA	NA	✓
Chrome OS <ul style="list-style-type: none"> Version 67+ 	Chrome 67+	✓	✓	NA	NA	NA	✓

Acronyms and initialisms used in this table are as follows:

IAHSS = Interim Assessment Hand Scoring System

DEI = Data Entry Interface

ORS = Online Reporting System

TA Sites = Test Administrator Sites

TOMS = Test Operations Management System

TIDE = Test Information Distribution Engine, comprised of Completion Status, Roster Management, and Appeals

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 you deploy a browser with the required capability. 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	Y	Y	Y	Y	Y	Y	Y
Windows	Internet Explorer 11 web browser	N	N	N	N	Y	N	N
Windows	Edge web browser	N	N	N	N	Y	N	N
Windows	Chrome web browser	Y	Y	Y	Y	Y	N	N
Windows	Firefox web browser	N	N	N	N	Y	N	N
OS X	Secure browser	Y	Y	Y	Y	Y	Y	Y
OS X	Safari web browser	N	N	N	N	Y	N	N
OS X	Chrome web browser	Y	Y	Y	Y	Y	N	N
Linux	Secure browser	Y	Y	Y	Y	N	Y	Y
Linux	Firefox web browser	N	N	N	N	N	N	N
Linux	Chrome web browser	Y	Y	Y	Y	N	N	N
iOS	Mobile secure browser	N	Y	Y	Y	Y	N	N
iOS	Safari web browser	N	N	N	N	Y	N	N
Android	Mobile secure browser	N	N	N	N	Y	N	N
Android	Chrome web browser	Y	Y	Y	Y	Y	N	N
Chromebook	Secure browser	N	Y	Y	Y	Y	N	N
Chromebook	Chrome web browser	Y	Y	Y	Y	Y	N	N

Requirements for Peripheral Equipment

Additional Resources:

- California Department of Education (CDE) Matrix One: California Assessment of Student Performance and Progress (CAASPP) System Accessibility Resources web page—<http://www.cde.ca.gov/ta/tg/ai/caasppmatrix1.asp>
- *Accessibility Guide for CAASPP Online Testing* web document—<http://www.caaspp.org/rsc/pdfs/CAASPP.accessibility-guide.2018-19.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 the following devices are **not** supported:

- Apple iPad Mini
- Google Nexus 7 and similar-sized Android tablets
- Netbooks with screen dimensions smaller than 10"

Screen Resolution

All devices must meet the following minimum resolution. Larger resolutions can be applied as appropriate for the monitor or screen being used.

- Desktops, laptops, and tablets: 1024 x 768
- Netbooks: 1024 x 600

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 must be used with tablets used for testing. The intent of this requirement 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. You are strongly cautioned against using keyboards that have these shortcut buttons.

Android Keyboards

The Android mobile secure browser requires the secure browser keyboard to disable predictive text.



Caution: Any external keyboard that has a shortcut button to open the tablet’s default keyboard is not permitted, as this default keyboard will override the mobile secure browser keyboard. For example, the EZOWare Slim Full Size Keyboard contains a shortcut button that opens the default keyboard and should **not** be used with Android tablets during testing.

Mice

Mice on mobile devices are not supported. Wireless or wired two- or three-button mice that are compatible with the operating system on desktops and laptops are supported. No other mice should be used, especially mice equipped with a “browser back” button that could create an insecure testing environment and potentially pause or force an exit from the test.

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 English language arts/literacy assessments contain audio (recorded and/or device-based read-aloud), and students must be provided with headphones so they have the option to clearly listen to the audio in these tests.

System Requirements | Requirements for Peripheral Equipment

- Students with the text-to-speech test setting can use headphones to listen to stimuli or test items being read aloud. For more information about text-to speech and other test settings, refer to one of the following resources:
 - [Matrix One](#) web page
 - [Accessibility Guide for CAASPP 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 should determine how many students will need headphones to ensure that there are enough available at the time of a test.

Table 9 lists 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, Android tablets with 3.5 mm port
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

Chapter 2. Network Configuration

Network Configuration and Testing

Your network's configuration has a significant impact on the test delivery system's (TDS's) performance. An improperly configured network can slow a TDS's responsiveness and possibly impact students' scores or an assessment's integrity. The subsections in this chapter provide guidance on properly configuring your 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 and/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. Your network should have enough bandwidth to support online testing at the required performance level. For example, if a testing program requires that web browsers display test items within 10 seconds after sending a request, then the network must have enough bandwidth to support that requirement.

In an online testing environment, the following factors contribute to determining the required bandwidth:

- **Number of Students Simultaneously Testing**—As the number of students testing at one time increases, the required bandwidth also increases.
- **Size of the Test Content**—The more items a test contains and the larger the average test item, the higher the bandwidth requirement for a given test. For example, some writing tests have a few questions to which the student composes a response, and these tests are small. In contrast, tests with animations, simulations, and/or audio are large. The size of a test's content is determined by two factors:
 1. the number of items on the test; and
 2. the average size of each item.
- **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. If you use 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 1.5M bits per second and 100M bits per second. 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. If you 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 your 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 your 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/second	5–15K bits/second
50	400K bits/second	250–750K bits/second (0.25–0.75M bits/second)
100	800K bits/second	500–1500K bits/second (0.5–1.5M bits/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 subjects.

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)

Whitelisting Test Site URLs

If the school's filtering system has both internal and external filtering, the URLs for the testing sites must be whitelisted in both filters (see [URLs for Testing Sites](#)). Please see the filtering system's documentation for specific instructions. Be sure to whitelist these URLs in any multilayer filtering system (such as local and global layers).

Configuration for Domain Name Resolution

[Appendix B, URLs for Testing Systems](#), lists the domain names for California Assessment of Student Performance and Progress (CAASPP) 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 your 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 your 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.

Configuring for Certificate Revocations

Testing servers present certificates to the clients. To use a certificate revocation list, ensure your firewalls allow the URL <http://crl.verisign.com/>.

Network Diagnostic Tools

Additional Resources:

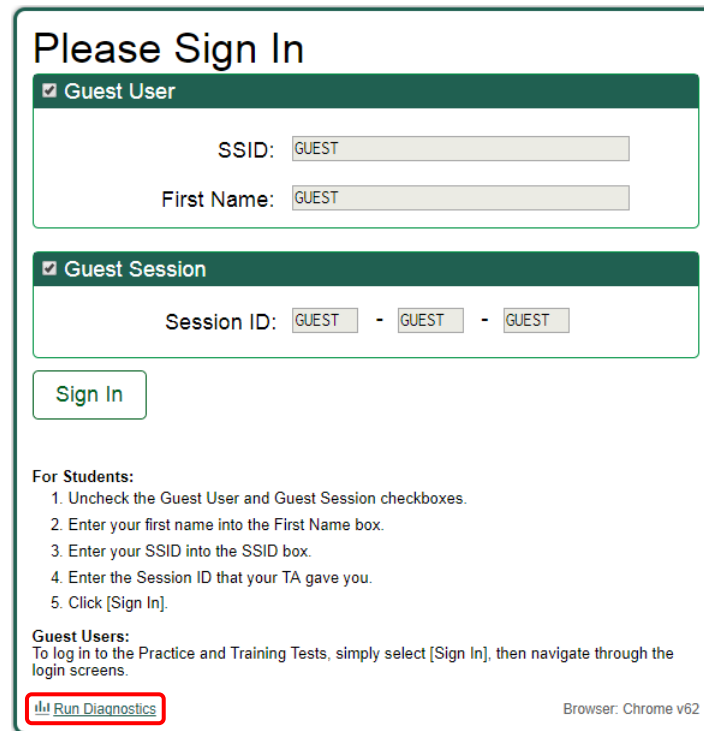
- CAASPP Online Practice and Training Tests Portal web page—<http://www.caaspp.org/practice-and-training/>
- CAASPP Diagnostic Screen web page—https://demo.tds.airast.org/systemdiagnostic/pages/default.aspx?c=California_PT&url=https://capt.tds.airast.org/student

You should conduct a performance analysis of your 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.

American Institutes for Research's (AIR's) Network/Bandwidth Diagnostic Tool

The American Institutes for Research (AIR) provides a diagnostic tool that can be directly accessed from the student practice test logon page or in the *Additional Resources* box on most caaspp.org web pages.

1. On the practice test logon page—accessed by selecting the [**Student Interface Practice and Training Tests**] button on the CAASPP [Online Practice and Training Tests Portal](#) web page—select the [Run Diagnostics] link in the lower-left corner of the sign-in page (Figure 1) to open the [Diagnostic Screen](#) web page.



Please Sign In

Guest User

SSID:

First Name:

Guest Session

Session ID: - -

For Students:

1. Uncheck the Guest User and Guest Session checkboxes.
2. Enter your first name into the First Name box.
3. Enter your SSID into the SSID box.
4. Enter the Session ID that your TA gave you.
5. Click [Sign In].

Guest Users:
To log in to the Practice and Training Tests, simply select [Sign In], then navigate through the login screens.

Browser: Chrome v62

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

2. In the “Network Diagnostics” section of the [Diagnostics 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 Assessments, which are administered one-on-one to a small number of students, usage concurrency is not typically expected to be a concern.)

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 7**

Your Browser Version: **Chrome v62**

Secure Browser: **false**

Network Diagnostics:

Select Test: ← 2

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

← 4

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

Windows-Specific Tools

Additional Resources:

- GitHub iperf web page—<https://github.com/esnet/iperf>
- 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>
- 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/>

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.

OS X–Specific Tools

Network Utility App

The OS X Network Utility app is built in to OS X.

Multiplatform Tools

Wireshark

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

Tcpdump

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

Ping, NSLookup, Netstat, Traceroute

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

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.

Chapter 3. System Configuration

Hardware Configuration



Additional Resources:

- California Assessment of Student Performance and Progress (CAASPP) Student Accessibility Resources and Test Settings web page—<http://www.caaspp.org/administration/accessibility/>

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 and/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 can print test session information and approve students' requests to print stimuli or test items (for students with the print-on-demand accommodation). Nevertheless, to maintain a secure test environment, the test administrator's device should be connected to a single local or network printer in the testing room, and only the test administrator'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 1G bits per second.
- 802.11n has a theoretical throughput of up to 300M bits per second.
- 802.11g has a theoretical throughput of up to 54M bits per second.
- 802.11b has a theoretical throughput of 11M bits per second.

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 megabits per second [Mbps]) and 802.11n (300Mbps). 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 your 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 *Accessibility Guide for CAASPP Online Testing*, which will be available on the CAASPP [Student Accessibility Resources and Test Settings](#) 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. See 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 and/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.

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 creates competition among the students' clients for two resources: local area network bandwidth and shared disk drive input/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 Quality With Servers

- 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/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; and Internet Explorer, for nontesting applications) 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) testing provide informational messages or warnings using pop-up windows. Therefore, you must enable pop-up windows on those web browsers used in support of CAASPP testing systems, such as the Test Operations Management System and the Test Administrator Interface.

The following list describes how to enable pop-up windows on many web browsers. If your 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 you prefer to limit pop-up windows to only those coming from domains involved in all aspects of CAASPP testing, use the instructions in the next subsection, “Enabling Pop-Up Windows Only for Domains Involved in CAASPP Testing.”

- **Firefox (Windows):** *Tools* → *Options* → *Content* → clear *Block pop-up windows* (Firefox on OS X and Linux is similar.)
- **Chrome:** *Menu* → *Settings* → *Show advanced settings* (at the bottom of the screen) → *Privacy* → *Content Settings* → *Pop-ups* → mark *Allow all sites to show pop-ups*
- **Chrome browser on Android tablets:** *Menu* → *Settings* → *Advanced* → *Content Settings* → *Block pop-ups* → clear the check box
- **Internet Explorer:** *Internet Options* → **[Privacy]** tab → clear *Turn On Pop-up Blocker*
- **Safari:** *Safari* → clear *Block Pop-Up Windows*
- **iOS Safari:** *Settings* → *Safari* → *Block Pop-ups* (toggle to “off” mode)

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

You can allow pop-up windows only from domains involved in CAASPP testing. The following list describes how to enable domain-specific pop-up windows on many browsers. If your 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:** *Tools* → *Options* → *Content* → select Exceptions. Enter domain names and select [**Allow**] for each.
- **Chrome:** *Menu* → *Settings* → *Show advanced settings* (at the bottom of the screen) → *Privacy* → *Content Settings* → *Pop-ups* → select Manage Exceptions. Enter the domain names and select [**Allow**] for each.
- **Internet Explorer:** [**Internet Options Privacy**] tab → *Settings*. Enter the domain names and select [**Add**] for each.
- **Safari and iOS Safari:** N/A
- **Chrome on Android tablets:** N/A

Preventing Auto Update on Device Operating Systems Used for Test Operations



Additional Resources:

- Mozilla Support Forum Response – Turning off auto-update web page—
<https://support.mozilla.org/en-US/kb/forum-response-turning-auto-update>



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. See 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. You should wait before installing new versions of Firefox, which could impact system performance. Delaying updates allows time to review changes and verify each system works correctly with the new version.

To learn how to disable auto updates for Firefox, see the [Mozilla Support Forum Response](#) for instructions. You may need to disable auto updates again after installing a newer version.

Enabling Web Fonts in Internet Explorer 11

Some applications, such as the Test Administrator Interface or the Teacher Hand Scoring System, display test items that may require web fonts. The following procedure describes how to enable web fonts in Internet Explorer 11.

To enable web fonts in Internet Explorer:

1. In Internet Explorer, open the *Tools* menu and then select *Internet Options*. The *Internet Options* dialog box opens.
2. Select the [**Security**] tab (Figure 3).

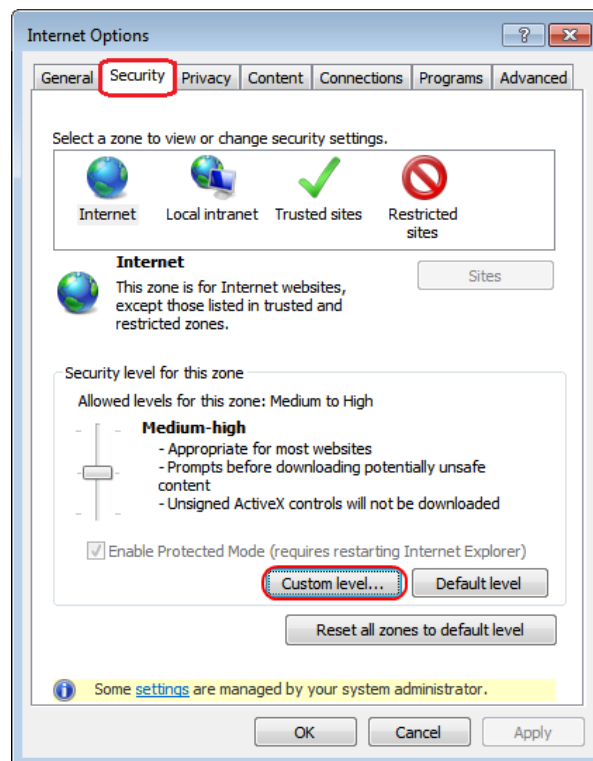


Figure 3. Internet Explorer *Internet Options* dialog box

3. Select the [**Custom Level**] button. The Security Settings dialog box opens (Figure 4).

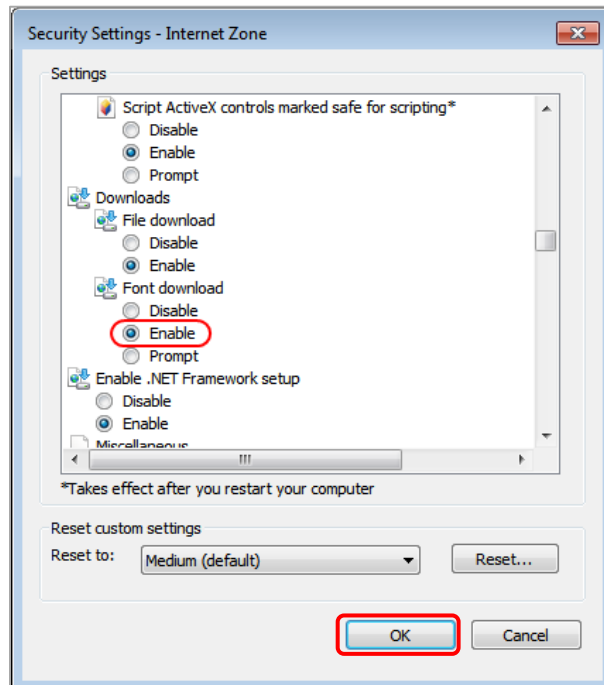


Figure 4. Internet Explorer Security Settings dialog box

4. Scroll to *Font download* and select the *Enable* radio button.
5. Select [OK]. The *Security Settings* dialog box closes.
6. Select [OK]. The *Internet Options* dialog box closes.

Keyboard Navigation to 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 5.



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

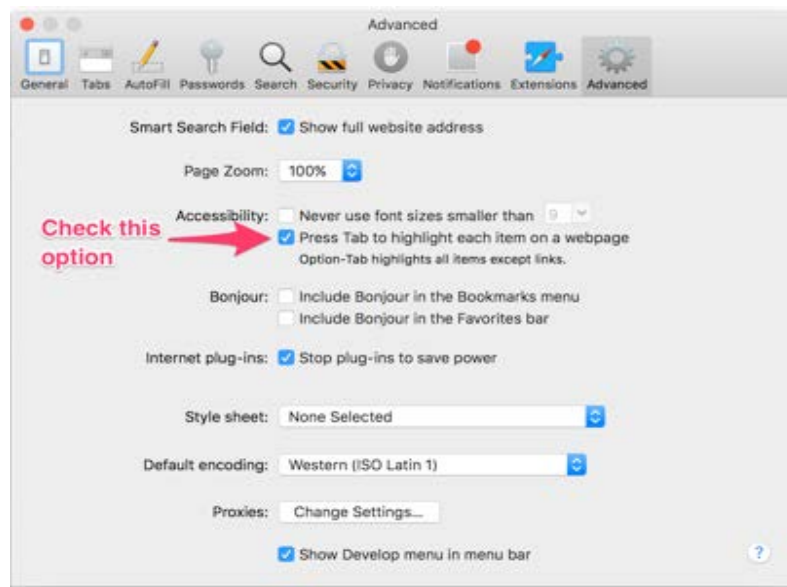


Figure 5. Safari Advanced preferences

Configuring Devices for Online Testing with the Secure Browser

This subsection describes how to configure devices for online testing.

Windows Devices

Disabling Fast User Switching in Windows

Microsoft Windows (7, 8.0, 8.1, and 10) has 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. The following subsections describe how to disable Fast User Switching for different versions of Windows. (There is no need to manually disable Fast User Switching on Windows 10.)

Disabling Fast User Switching in Windows 7

This subsection describes how to disable Fast User Switching using the Group Policy Editor.

1. Select **[Start]**.
2. Type `gpedit.msc` in the *Search programs and files* field (Figure 6) and then press the **[Enter]** key. The *Local Group Policy Editor* screen appears.



Figure 6. Windows Search box

3. Navigate to *Local Computer Policy* → *Computer Configuration* → *Administrative Templates* → *System* → *Logon* (Figure 7).

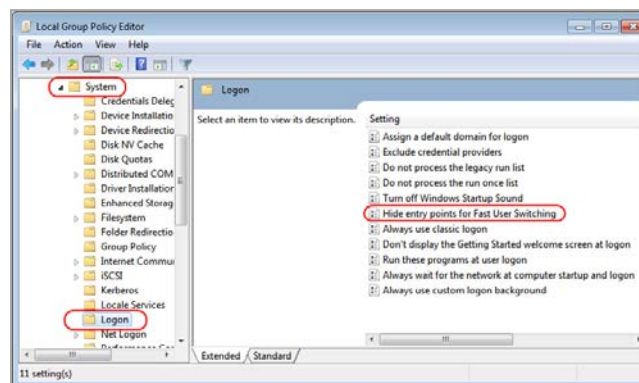


Figure 7. Local Group Policy Editor screen options

4. Double-click *Hide entry points for Fast User Switching*.
5. Select the *Enabled* radio button (Figure 8), and then select **[OK]**.

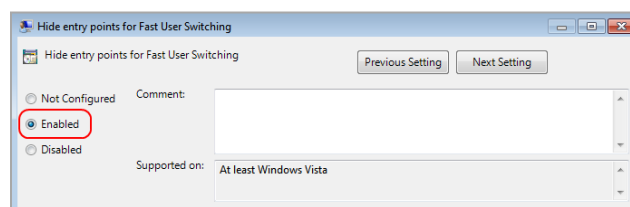


Figure 8. Finish in the Windows Local Group Policy Editor screen

6. Close the Local Group Policy Editor.

Disabling Fast User Switching in Windows 8.0 and 8.1

The following procedure describes how to disable Fast User Switching under Windows 8.0 and 8.1.

1. In the Search charm, type `gpedit.msc` (Figure 9).

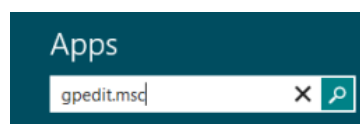


Figure 9. Windows Search charm

2. Select 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* (Figure 10).

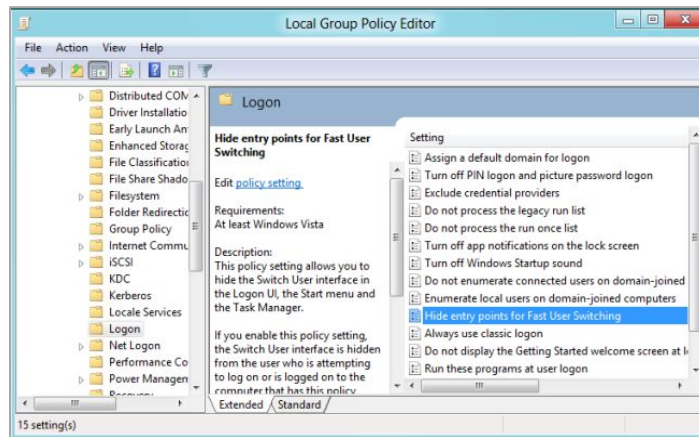


Figure 10. Windows Local Group Policy Editor options

5. Select the *Enabled* radio button, and then select **[OK]**. Both are indicated in Figure 11.

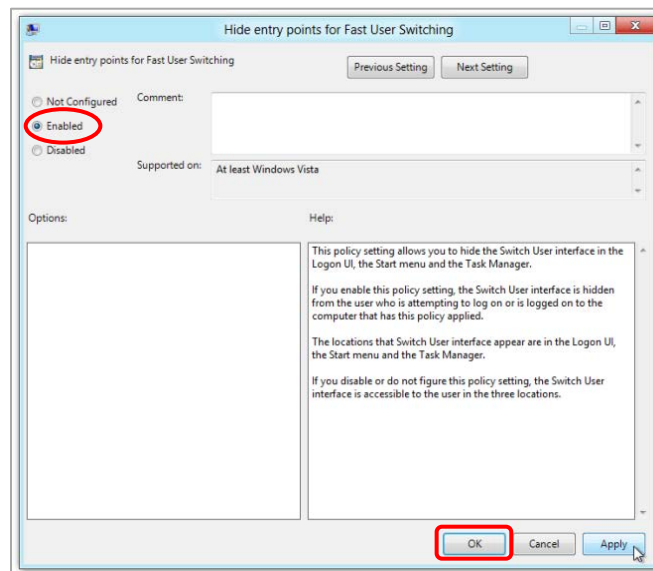


Figure 11. Windows Local Group Policy Editor selection

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 12). (Note the space before the forward slash.)

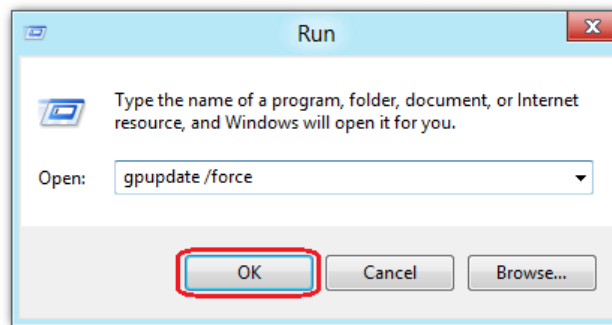


Figure 12. Windows *Run* dialog box

9. The *Command* window opens (Figure 13). The message Computer Policy update has completed successfully is your notification that Windows has successfully disabled Fast User Switching.

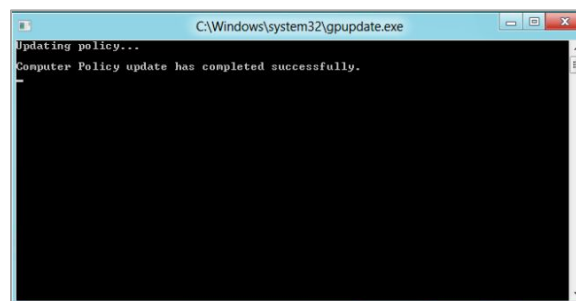


Figure 13. Notification in the Windows *Command* window

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 before the start of testing to mitigate this risk.

Because devices running Windows 7 Home Edition cannot access the Local Group Policy Editor, Task Manager is disabled using the Registry Editor.

Disabling Task Manager Using the Local Group Policy Editor

Take the following steps to disable the Task Manager using the Local Group Policy Editor:

1. Select **[Start]**.
2. Type `gpedit.msc` in the *Search programs and files* field (Figure 14) and then press the **[Enter]** key. The *Local Group Policy Editor* screen appears.

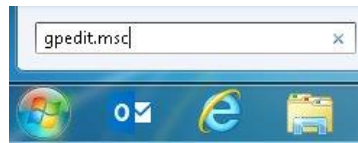


Figure 14. Windows Search box

3. Navigate to *User Configuration* → *Administrative Templates* → *System* → *Ctrl+Alt+Del Options* (Figure 15).

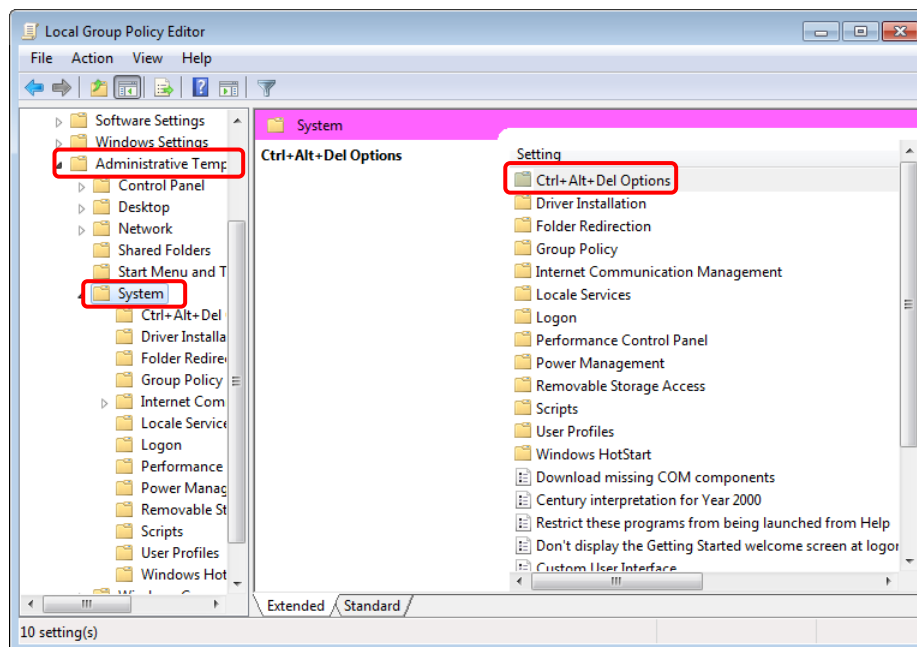


Figure 15. Local Group Policy Editor screen options

4. Double-click *Ctrl+Alt+Del Options* and then *Remove Task Manager* (indicated in Figure 16).

System Configuration | Software Configuration

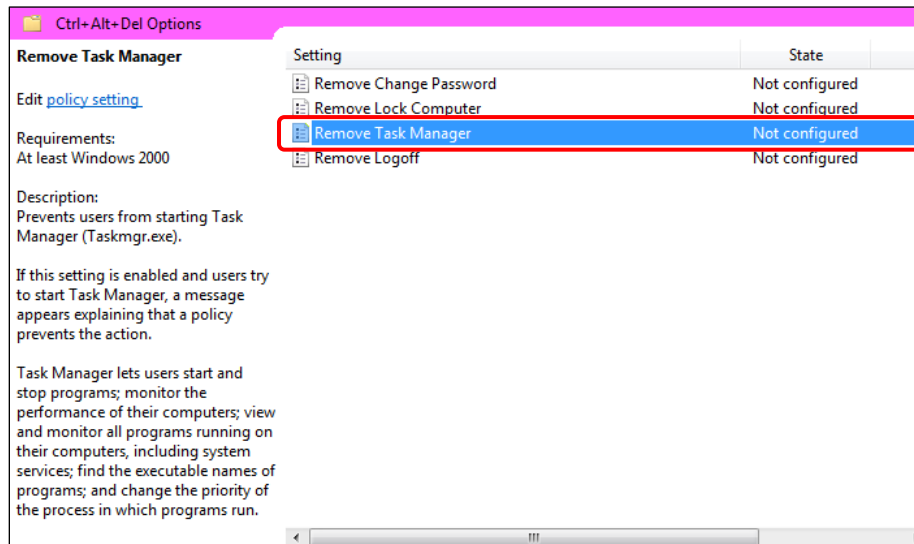


Figure 16. Ctrl+Alt+Del Options settings

5. Select the *Enabled* radio button in the *Remove Task Manager* dialog box shown in Figure 17, and then select [OK].

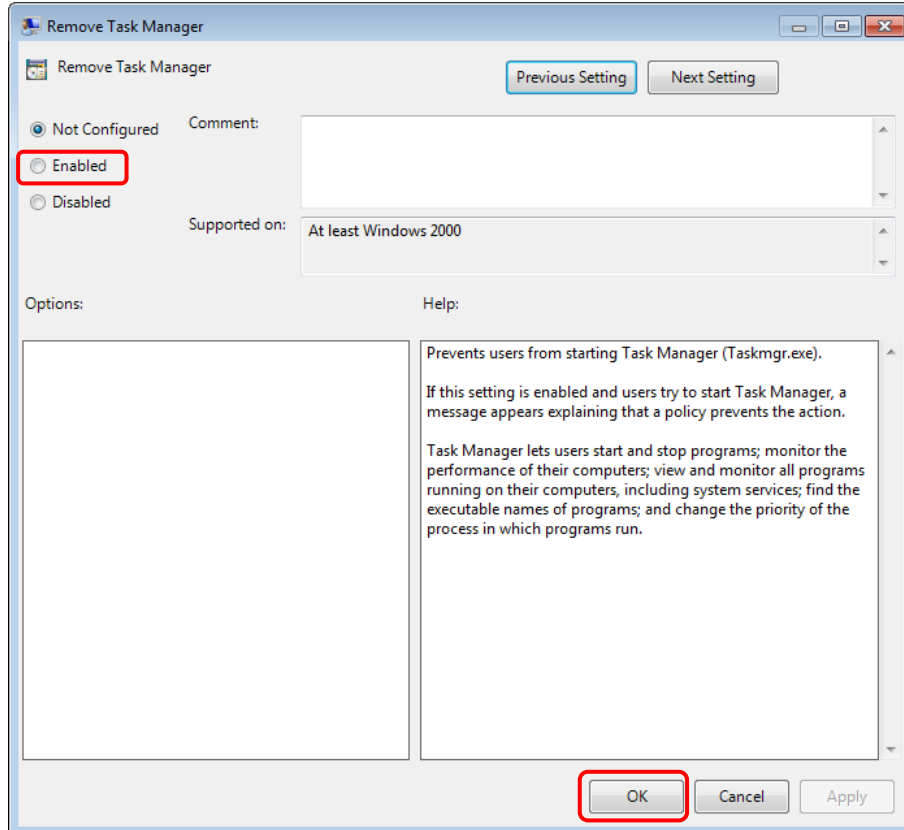


Figure 17. Remove Task Manager screen

6. Close the Local Group Policy Editor.

Disabling the Task Manager Using the Registry Editor

Take the following steps to disable the Task Manager in Windows 7 Home Edition using the Registry Editor:

1. Select **[Start]**.
2. Type `regedit.exe` in the *Search programs and files* field () and then press the [Enter] key. The *Registry Editor* screen appears.

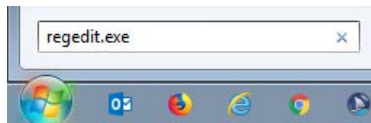


Figure 18. Windows Search box

3. Navigate to *HKEY_CURRENT_USER* → *Software* → *Microsoft* → *Windows* → *CurrentVersion* → *Policies* → *System*.
4. Double-click *DisableTaskMgr*.
5. Change the value data to 1.
6. Select **[OK]**.
7. Close the Local Group Policy Editor.

Setting 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. The following procedure describes how to disable the touch features on these devices using the Group Policy Editor to edit policy settings.

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 19, appears.
2. In the left pane, navigate to *Computer Configuration* → *Administrative Templates* → *Windows Components* (indicated in Figure 19).

System Configuration | Software Configuration

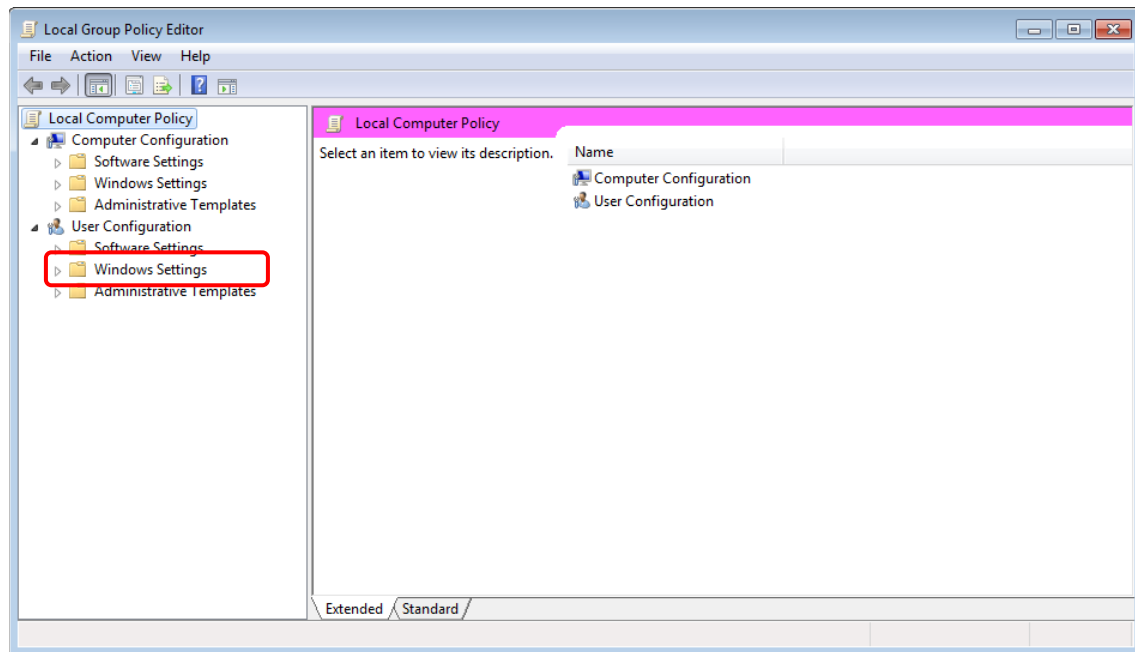


Figure 19. Local Group Policy Editor screen

3. In the Windows Components group in the right pane, scroll down to the **[Tablet PC]** folder icon—indicated in Figure 20—and double-click it.

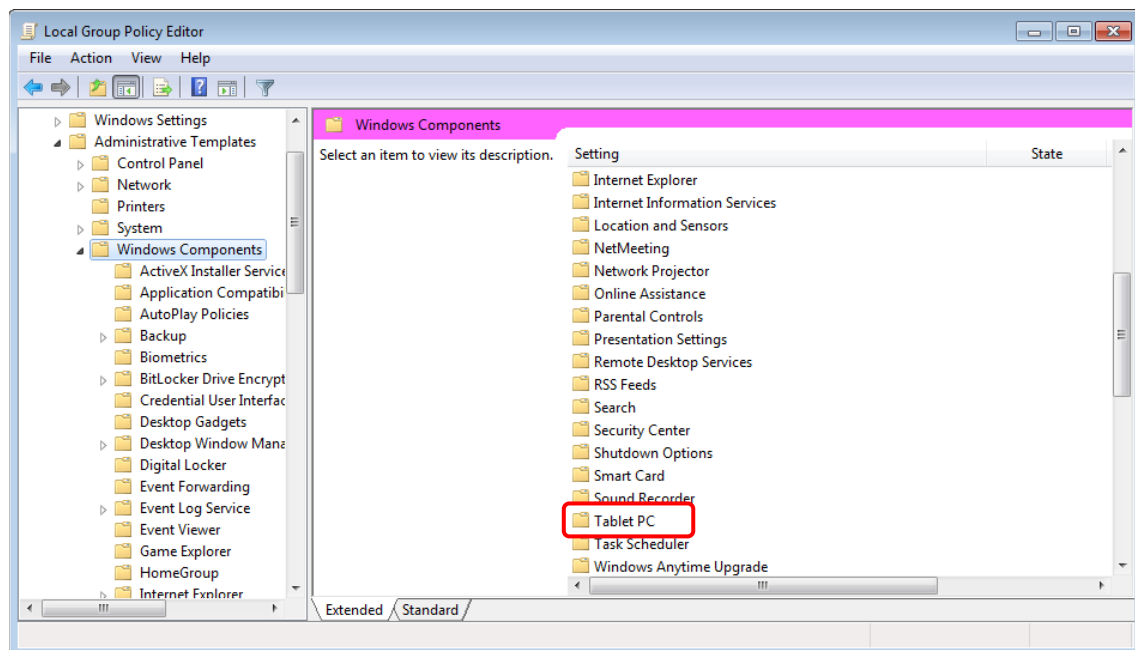


Figure 20. Windows Components in the Local Group Policy Editor

4. Double-click to select the **[Input Panel]** icon, which is indicated in Figure 21.

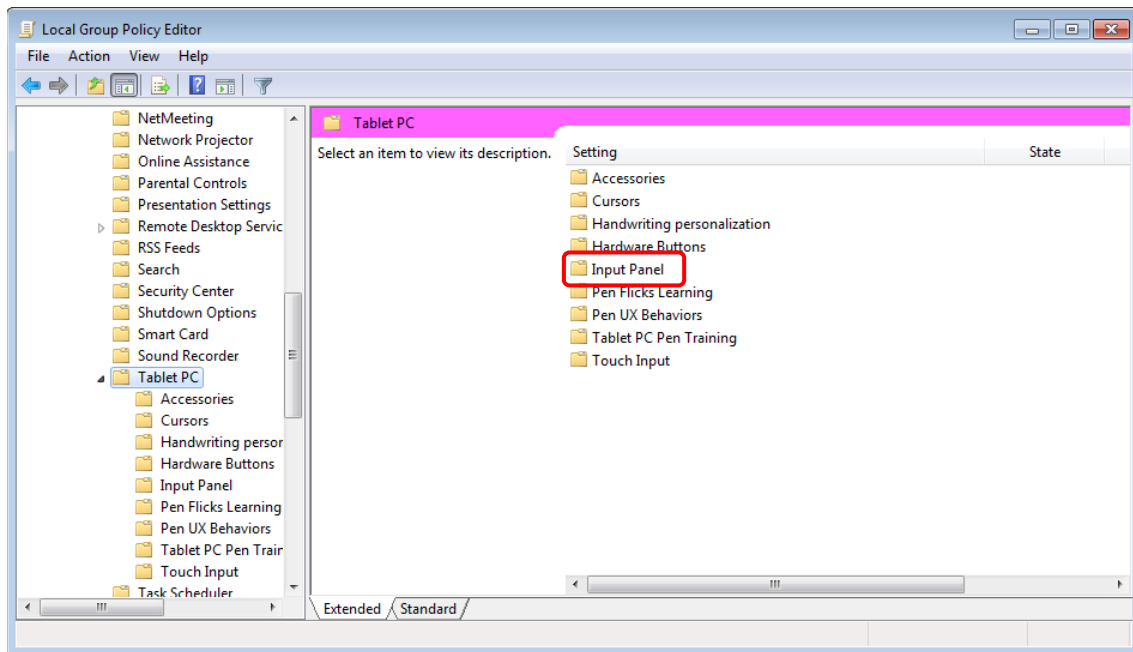


Figure 21. Input Panel in the Local Group Policy Editor

- 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 22). (Note that the settings for the device you are configuring may be slightly different than those in the figure.)

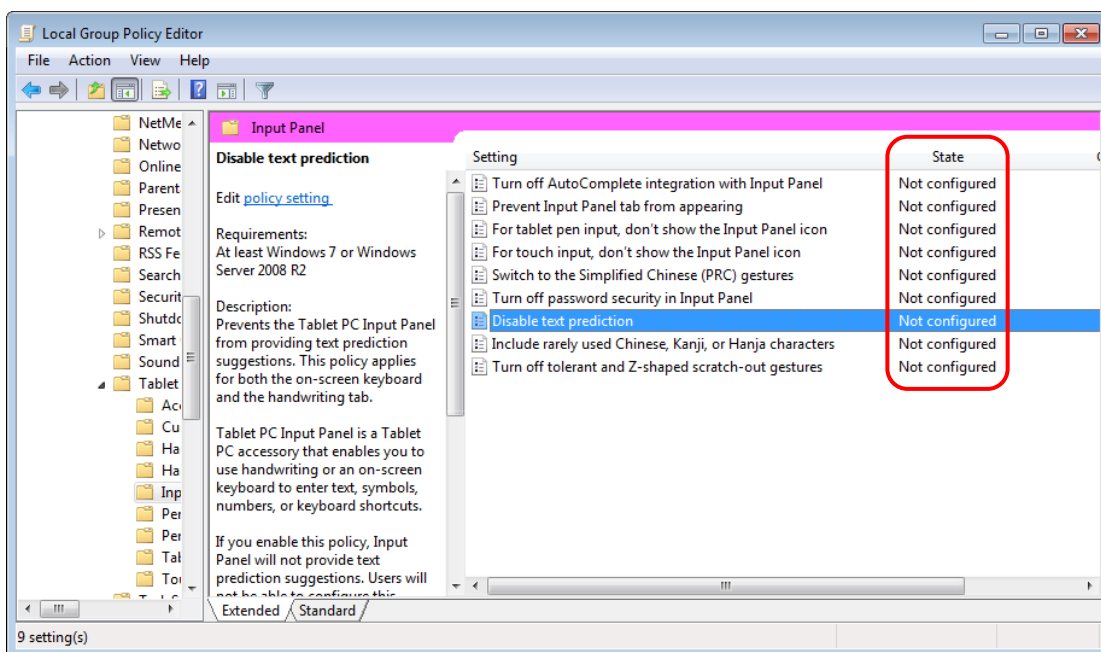


Figure 22. Disable text prediction selection

6. To enable an item, double-click on that item in the *Setting* column to open the *Disable [policy setting]* dialog box, which is shown in Figure 23 for the setting “Disable text prediction.” The following settings should be enabled:
 - a. Turn off AutoComplete integration with Input Panel
 - b. Prevent Input Panel tab from appearing
 - c. For tablet pen input, don’t show the Input Panel icon
 - d. For touch input, don’t show the Input Panel icon
 - e. Disable text prediction

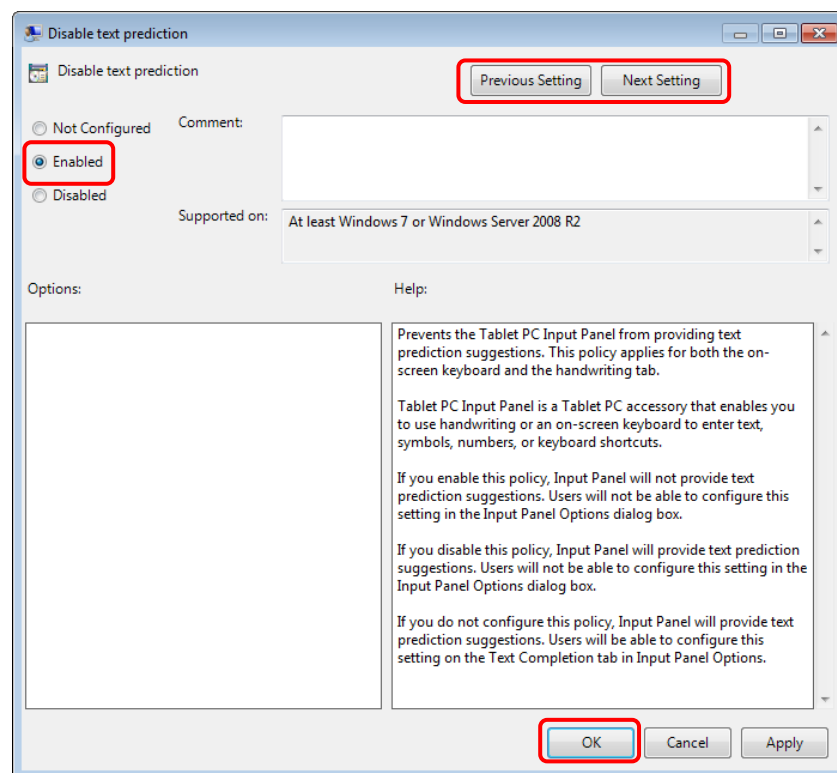


Figure 23. Disable text prediction screen

7. To enable the setting, select the *Enabled* radio button, and then select **[OK]**. This dialog box also gives you 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 3 Tablet

Some students using Surface Pro 3 tables and accessing the touch keyboard may see 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 this issue, the student’s touch keyboard must be set to show up automatically.

Take these steps 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**]).

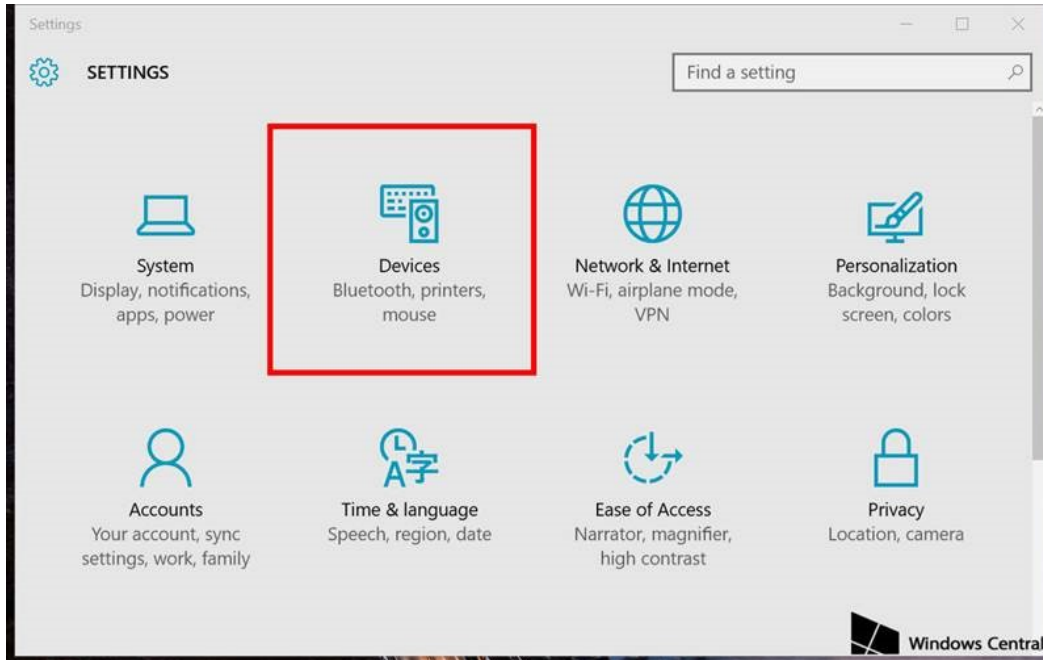


Figure 24. Surface Pro 3 Settings interface

2. Select [**Devices**] (indicated in Figure 24) and then *Typing* from the left pane (shown in Figure 25).

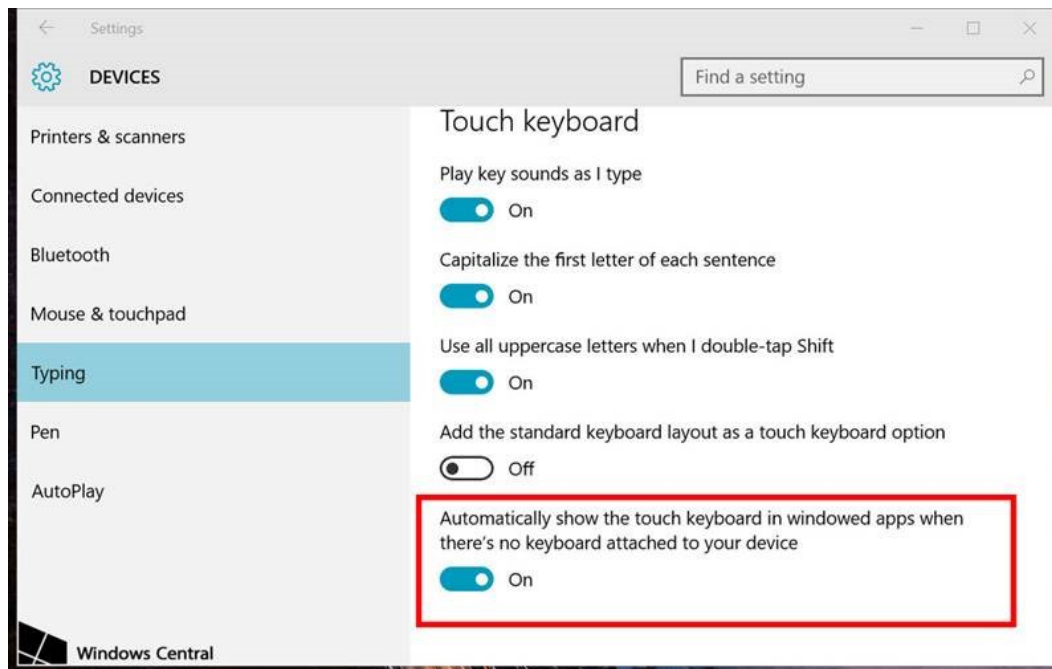



Figure 25. Touch keyboard settings interface

3. 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 25.

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.

Take these steps to disable the TouchPad feature in HP notebooks with Synaptics TouchPad:

1. Select the Start menu [mouse in the *Search programs and files* field.
2. Select Mouse from the list of options to open the *Mouse Properties* dialog box (Figure 26).

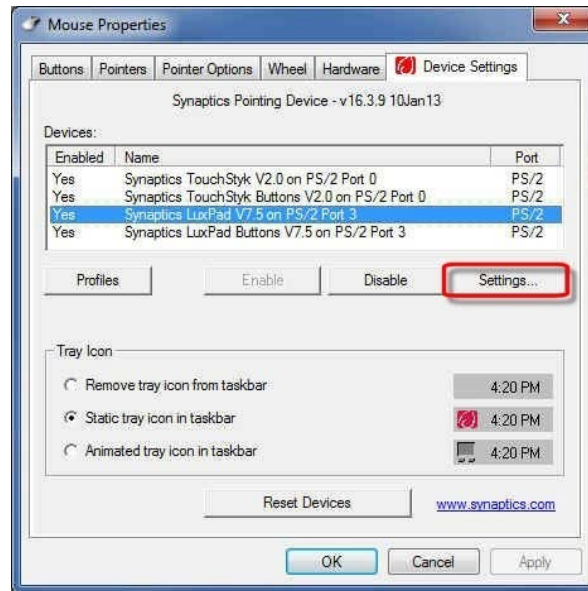


Figure 26. Mouse Properties dialog box

3. Select the [Device Settings] tab.
4. From the *Devices* list, select “Synaptics LuxPad V7.5,” and then select [Settings...] (indicated in Figure 26).
5. Uncheck the *Two-Finger Scrolling* box, which is indicated in Figure 27.

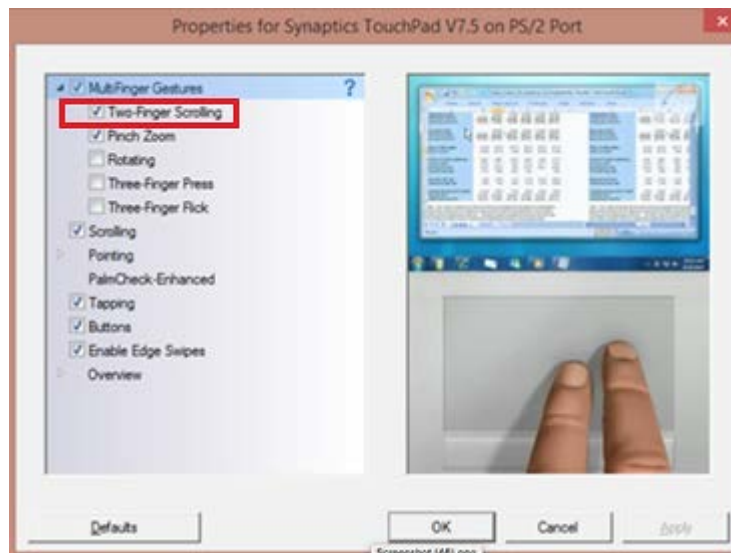


Figure 27. Properties for Synaptics TouchPad V7.5 on PS/2 Port dialog box

6. Select [Close] and then [OK].
7. In the *Mouse Properties* dialog box, select [Apply].

Installing Windows Media Pack for Windows 8.1 N and 8.1 KN

Additional Resources:

- Microsoft Media Feature Pack for Windows 8.1 N and Windows 8.1 KN Additions: April 2014 web page—<https://support.microsoft.com/en-us/help/2929699/media-feature-pack-for-windows-8.1-n-and-windows-8.1-kn-editions-april>
- Microsoft Media Feature Pack for N and KN versions of Windows 8.1 web page—<https://www.microsoft.com/en-us/download/details.aspx?id=42503>

Some versions of Windows 7, 8.1, and 10 are not shipped with media software installed. As a result, you 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

You are 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
- About
- Download

Mac OS X Devices

This subsection describes how to configure Mac OS X devices for online testing.

Disabling Exposé or Spaces

Mac OS X versions 10.9 and later include an Exposé or Spaces feature that allows running more than one desktop session. This is a security risk because students can potentially start a new desktop session during the test and use that session to search the internet for answers. The following procedure explains how to disable Exposé or Spaces on those versions of OS X. (You can disable Spaces quickly from the command line; see [Disabling Spaces and Application Launches from the Command Line](#) for details.)

To disable Spaces:

1. Choose the *Apple* menu → *System Preferences* (Figure 28).

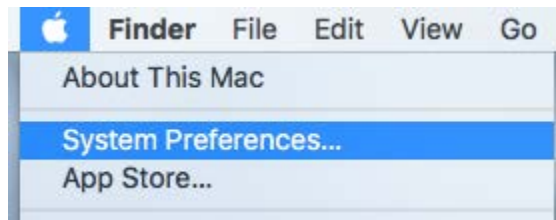


Figure 28. Select OS X System Preferences

2. Select the [**Keyboard**] icon (Figure 29). The *Keyboard* screen opens.

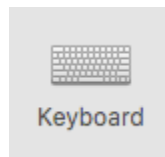


Figure 29. [Keyboard] icon

3. Select the [**Keyboard Shortcuts**] or [**Shortcuts**] tab (Figure 30).

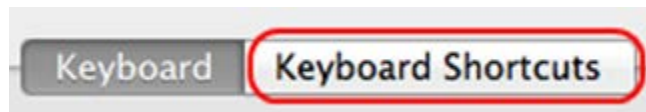


Figure 30. [Keyboard Shortcuts] tab

4. In the left panel of the screen, select [**Mission Control**]. The right panel lists all Mission Control options (Figure 31).

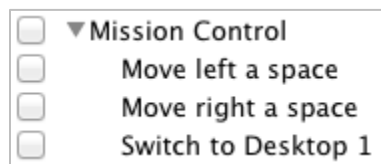


Figure 31. OS X Mission Control options

5. In the right panel, clear the following check boxes:
 - *Move left a space*
 - *Move right a space*
 - *Switch to Desktop 1*
6. Return to the *System Preferences* interface and select [**Mission Control**] to open the *Mission Control* dialog box.

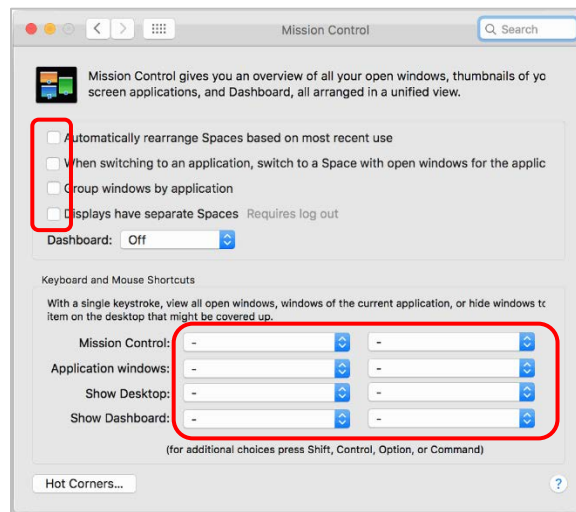


Figure 32. Mission Control screen

7. Make sure that none of the checkboxes on the top half of the screen, indicated in Figure 32, have been selected (checked).
8. In the “Keyboard and Mouse Shortcuts” section in the bottom half of the screen, indicated in Figure 32, set all the drop-down lists to “-” (hyphen) as necessary.

To re-enable Exposé or Spaces, follow steps 1–5, this time marking the boxes for spaces.

Disabling Application Launches from Function Keys

When students use the secure browser for testing, the test delivery system conducts regular checks to ensure that other applications are not open. These checks help maintain the integrity of the secure test environment.

Starting with OS X versions 10.9 and later, some Mac devices are factory configured to launch iTunes and other applications by pressing the function keys (e.g., [F8]) on the keyboard. If a student accidentally presses the function key, the secure browser assumes that a forbidden application is running and pauses the student’s test. To avoid this scenario, disable the use of function keys to launch applications.

The following instructions are based on OS X 10.11; similar instructions apply for other versions of OS X. (You can disable application launches quickly from the command line; see [Disabling Spaces and Application Launches from the Command Line](#) for details.)

To disable application launches from function keys:

1. Choose the *Apple* menu → *System Preferences*.
2. In System Preferences, select the **[Keyboard]** icon (Figure 33). The *Keyboard* screen opens.



Figure 33. Apple System Preferences screen

3. In the *Keyboard* screen, check the *Use all F1, F2, etc. keys as standard function keys* box (Figure 34).

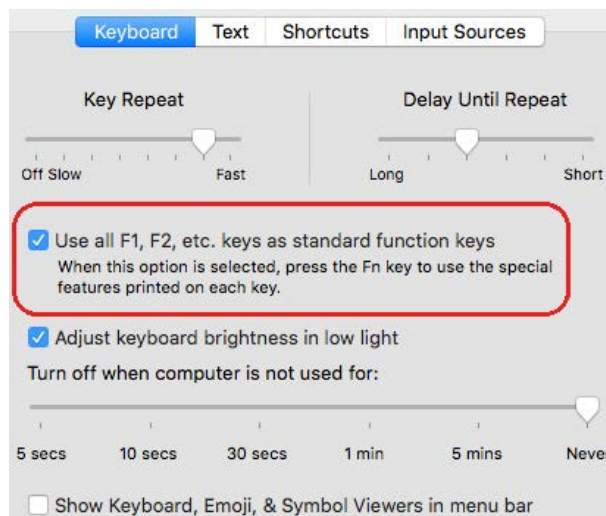


Figure 34. Keyboard options

If you need to launch iTunes or another application, press the [Fn] key and then press the desired function key. This combination will launch the application. (Doing so while taking a test causes the secure browser to pause the test.)

Disabling Custom Keys

Some Mac users have encountered “Error Code 11673 – Custom Keys Enabled” after installing the newest secure browser. The following procedure explains how to disable custom keys.

1. Choose the *Apple* menu → *System Preferences*.
2. In System Preferences, select the **[Keyboard]** icon (Figure 33). The *Keyboard* screen opens.
3. Select the **[Shortcuts]** tab.
4. Uncheck all boxes under *Mission Control* and *Screen Shots*.

Disabling Updates to Third-Party Apps

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 10.11; similar instructions apply for other versions of OS X.

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 33).
3. Select the [**App Store**] icon. The *App Store* screen opens (Figure 35).

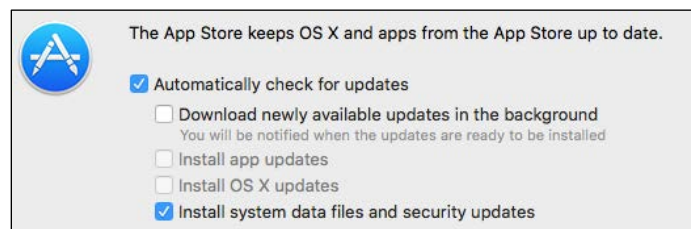


Figure 35. App Store screen

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

Disabling Updates to iTunes

Updates to iTunes may be incompatible with the secure browser. This subsection describes how to disable updates to iTunes.

The following instructions are based on OS X 10.11; similar instructions apply for other versions of OS X.

To disable updates to iTunes:

1. Log on to the student's account.
2. Start iTunes.
3. Select *iTunes* → *Preferences*.
4. Under the [**Advanced**] tab, clear the *Check for new software updates automatically* check box (Figure 36).

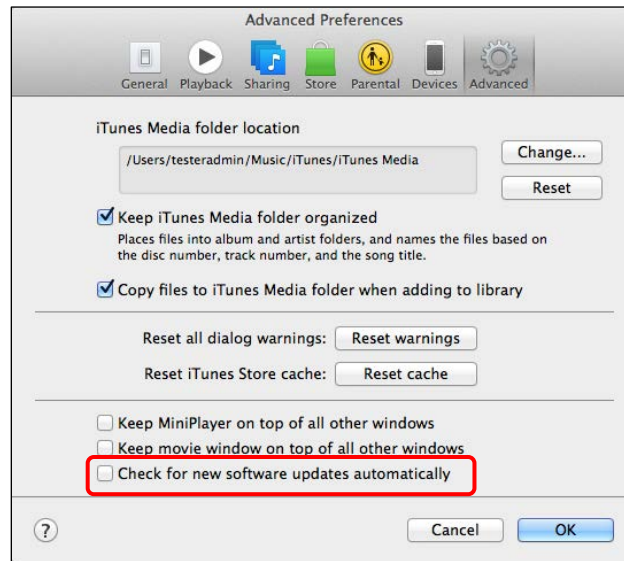


Figure 36. Advanced Preferences options

5. Select [OK].

Disabling Look-Up Gesture

OS X versions 10.9 and later include a look-up gesture function, which permits users to highlight a word and then, after tapping with three fingers on the trackpad, to access a dictionary for the highlighted word. This feature can compromise testing security. This subsection describes how to disable the look-up gesture.

The following instructions are based on OS X 10.11; similar instructions apply for other versions of OS X.

To disable updates to third-party apps:

1. Choose the *Apple* menu → *System Preferences*.
2. Select [Trackpad]. The *Trackpad Preferences* dialog box opens.
3. Select the [Point and Click] tab (Figure 37).

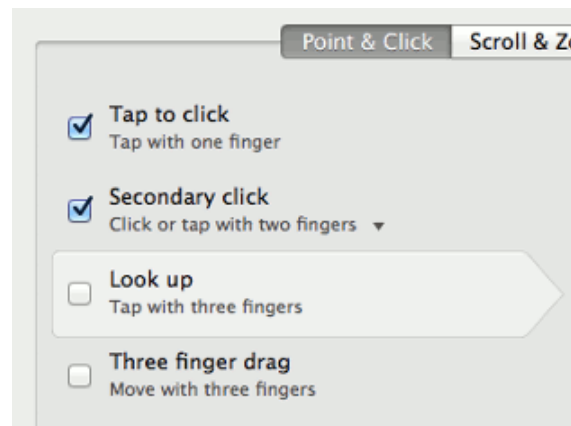


Figure 37. Trackpad Preferences options, [Point & Click] tab

4. Clear the *Look up* check box.

Disabling Display of Notification Center

OS X versions 10.10 and later include Notification Center, which displays system information when swiping to the left with two fingers from the right edge of the trackpad. Depending on its contents, Notification Center can compromise testing security. This subsection describes how to disable the gesture for displaying Notification Center.

The following instructions are based on OS X 10.10; similar instructions apply for later versions of OS X.

To disable the gesture for displaying the Notification Center:

1. Choose the *Apple* menu → *System Preferences*.
2. Select **[Trackpad]**. The Trackpad Preferences dialog box opens.
3. Select the **[More Gestures]** tab.
4. Select the *Notification Center* check box, which is highlighted in Figure 38.

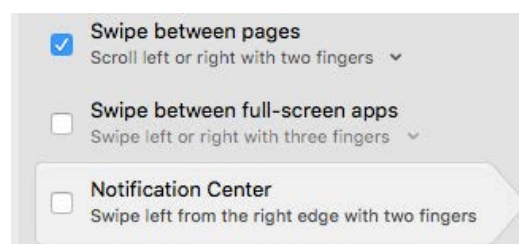


Figure 38. Trackpad Preferences options, [More Gestures] tab

Disabling Spaces and Application Launches from the Command Line

The subsections “[Disabling Exposé or Spaces](#)” and “[Disabling Application Launches from Function Keys](#)” describe how to configure OS X through the desktop. This subsection describes how to perform those configurations from the command line, which may take less

time than working through the desktop. To perform this task, you need to be familiar with logging on to OS X devices through Terminal or other terminal emulator.

To disable Spaces and application launches from the command line:

1. Log on to the device as the user that runs the secure browser.
2. Enter the following commands to modify the file `~/Library/Preferences/com.apple.symbolichotkeys.plist`:

```
defaults write com.apple.symbolichotkeys AppleSymbolicHotKeys -  
dict-add 79 "{enabled = 0; value = {parameters = (65535,123,  
262144); type = standard; }; }"  
defaults write com.apple.symbolichotkeys AppleSymbolicHotKeys -  
dict-add 80 "{enabled = 0; value = { parameters = (65535, 123,  
393216); type = 'standard'; }; }"  
defaults write com.apple.symbolichotkeys AppleSymbolicHotKeys -  
dict-add 81 "{enabled = 0; value = { parameters = (65535, 124,  
262144); type = 'standard'; }; }"  
defaults write com.apple.symbolichotkeys AppleSymbolicHotKeys -  
dict-add 82 "{enabled = 0; value = { parameters = (65535, 124,  
393216); type = 'standard'; }; }"
```



TIP: You can paste these lines into a text file, and run the file from the command line.

3. If you logged on to a device running OS X 10.9 or later, log off and then log back on.
4. If you need to restore Spaces and the default application launchers, repeat steps 1–3. In step 2, change `enabled = 0` to `enabled = 1`.

Disabling Spaces and Application Launches on Remote Devices

The subsections [“Disabling Exposé or Spaces,”](#) [“Disabling Application Launches from Function Keys,”](#) and [“Disabling Spaces and Application Launches from the Command Line”](#) describe procedures for configuring a secure test environment in OS X. This configuration is stored in the file `~/Library/Preferences/com.apple.symbolichotkeys.plist`. If you have many OS X testing devices, it may be easier to push this file to those devices instead of configuring each one individually.

You can push the configuration file to remote devices using a variety of tools, such as the following:

- Apple Remote Desktop
- Apple’s Active Directory Client and Directory Utility
- Apple’s Open Directory and Profile Manager

System Configuration | Software Configuration

- Centrifify & PowerBrokers Identity Enterprise
- File Distributor

Disabling Dictation

When students speak into an OS X 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 OS X device:

1. Choose the *Apple* menu → *System Preferences*.
2. Select the **[Keyboard]** option (indicated in Figure 39) and then *Dictation*.

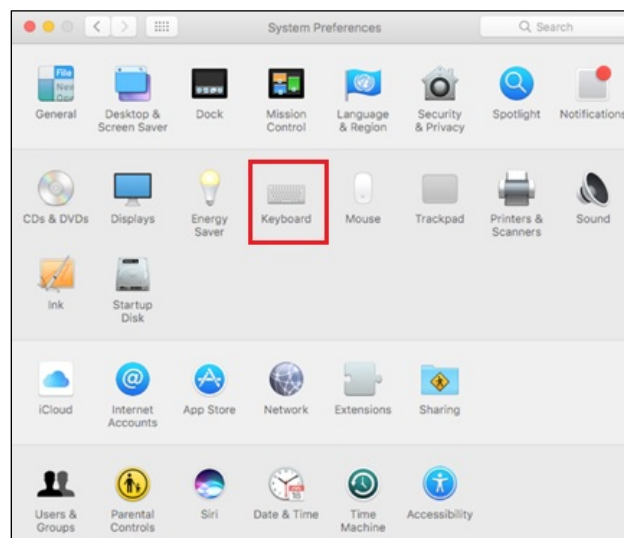


Figure 39. [Keyboard] button in OS X System Preferences

3. Select the *Off* radio button to turn the Dictation option off (Figure 40).

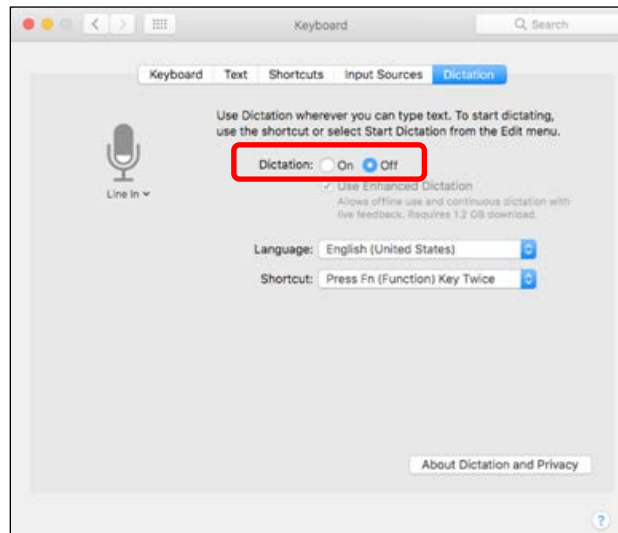


Figure 40. Dictation system preferences options in OS X

Disabling Siri

Take these steps to disable the Siri feature:

1. Choose the *Apple* menu → *System Preferences*.
2. Select [**Siri**] from the System Preferences options (Figure 41).



Figure 41. [Siri] button in OS X System Preferences

3. Uncheck the *Enable Siri* box (indicated in Figure 42).



Figure 42. Siri system preferences options in OS X

With Siri disabled, the menu bar icon is removed. Depending on the Macintosh, Siri can still be activated from the dock or the Touch Bar. It is important to note that while in a test, the AIRSecureBrowser app will detect if a user tries to enable Siri during testing and the app will disconnect the student from the test.

Disabling Text-to-Speech Keyboard Shortcut

A feature in macOS 10.12 (Sierra) and macOS 10.13 (High Sierra) allows users to have any text on the screen read aloud by selecting the text and pressing 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. What follows are the steps to take to disable this feature.

1. Choose the *Apple* menu → *System Preferences*.
2. Select [**Accessibility**] from the System Preferences options.
3. Select *Speech*.
4. To enable this feature, check the *Speak selected text when the key is pressed* box. To disable, deselect the checkbox.

Linux Devices



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.

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

Adding the Verdana Font



Additional Resources:

- 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 your 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
```

Apple Mobile Devices



Additional Resources:

- *Assessment with iPad* web document—https://images.apple.com/education/docs/Assessment_with_iPad.pdf

This subsection describes how to configure Apple mobile devices for online testing. For details on iPad device management and configuration for assessments, see the [Assessment with iPad](#) web document.

Using Autonomous Single App Mode (ASAM)

If you have iOS tablets running version 10 or higher and if you have a device running iOS version 10.10 or higher, then you can use Autonomous Single App Mode (ASAM) to quickly create a secure testing environment on all iPads used for testing. There is no need to activate ASAM on each iPad before each test session. To set up ASAM, you must also have access to a desktop or laptop running Mac OS X 10.10 or higher.



TIP: If you are using iPads with iOS 10 or later, you can use the automatic assessment configuration that comes with the AIRSecureTest app to save time with automatic assessment configuration. For details, see the instructions for [Using Automatic Assessment Configuration](#).

To manage multiple iPads using ASAM, you need to take the following steps:

[Step 1. Create a mobile device management profile.](#)

[Step 2. \(Optional\) Restrict features in iOS 10 or later.](#)

[Step 3. Create a supervisory profile.](#)

[Step 4. Place iPads in Autonomous Single App Mode.](#)

After completing these steps, each time a student starts a test, the iPad enters ASAM and the test environment is secure.

Step 1. Create a mobile device management profile.



Additional Resources:

- *Apple Configurator 2 Help* web manual—<https://help.apple.com/configurator/mac/2.0/>
- *Apple Education Deployment Guide* web manual—<https://help.apple.com/deployment/education/>
- TechRepublic Pro tip: How to Use OS X Server Profile Manager for MDM web page—<http://www.techrepublic.com/article/pro-tip-use-os-x-server-profile-manager-for-mdm/>

The first step in provisioning iPads with ASAM is to create a mobile device management (MDM) profile. Any profile with default settings is compatible with the secure browser. However, you may wish to restrict certain features in devices with iOS 10 or later (see the next step for instructions). Deploy the profile to a host that the iPads can access.

Creating an MDM profile is beyond the scope of this specification manual. The following references provide introductory information:

- [Education Deployment Guide](#)
- [Apple Configurator 2 Help](#)
- [Pro tip: How to Use OS X Server Profile Manager for MDM](#)

Step 2. (Optional) Restrict Features in iOS 10 or later.

You can restrict features in supervised devices with iOS 10 or later that may give students an unfair testing advantage, including the dictionary, predictive keyboard, spell check, and auto correction. If you wish to restrict any of these features, you may do so when creating the MDM profile for these devices.



Note: The current version of Apple Configurator does not allow you to restrict these features. You must use a third-party MDM solution such as Casper or AirWatch to create a profile that implements these restrictions.

To restrict features in iOS 10 or later:

1. In the “Custom Settings” section of the MDM solution, insert the profile key for each feature you wish to restrict. Table 13 provides a list of the relevant profile keys. Note that disabling the Dictionary also disables Share Selected Text.

Table 13. Profile Keys for Features in iOS 10 or Later

Feature	Profile Key	Recommended Value
Dictionary, Share Selected Text	<key>allowDefinitionLookup</key>	False
Predictive Keyboard	<key>allowPredictiveKeyboard</key>	False
Spell Check	<key>allowSpellCheck</key>	False
Auto Correction	<key>allowAutoCorrection</key>	False

2. The following snippet turns off the iPad's auto correction feature. The snippets for dictionary, predictive keyboard, and spell check are similar.

```
<dict>
  <key>allowAutoCorrection</key>
  <false />
  <key>PayloadDisplayName</key>
  <string>Restrictions</string>
  <key>PayloadDescription</key>
  <string>RestrictionSettings</string>
  <key>PayloadIdentifier</key>
  <string>31eb53ac-3a08-46f7-8a0a-82e872382e15.Restrictions</string>
  <key>PayloadOrganization</key>
  <string></string>
  <key>PayloadType</key>
  <string>com.apple.applicationaccess</string>
  <key>PayloadUUID</key>
  <string>56199b2c-374d-4152-bc50-166d21fa9152</string>
  <key>PayloadVersion</key>
  <integer>1</integer>
</dict>
```

Step 3. Create a supervisory profile.

To create a supervisory profile:

1. On a device running Mac 10.10 and later, download and install Apple Configurator from the Mac App Store. When the installation completes, open Apple Configurator.
2. Select [**Prepare**] and then [**Settings**]. The *Settings* screen appears (Figure 43).

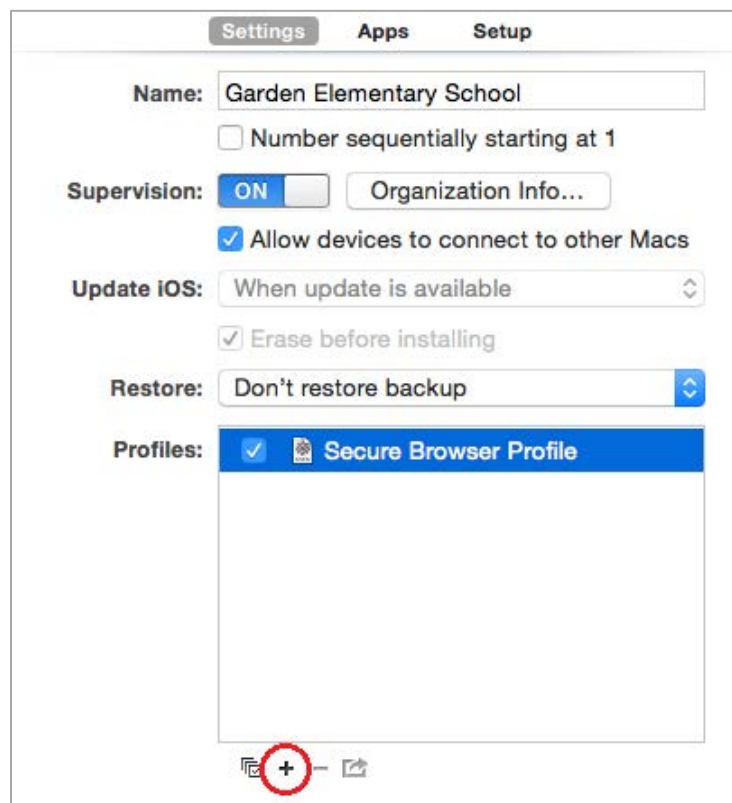


Figure 43. Settings options in Apple Configurator

3. Select **+** below the *Profiles* list (Figure 43) and select [**Create New Profile...**]. The configuration screen shown in Figure 44 appears.

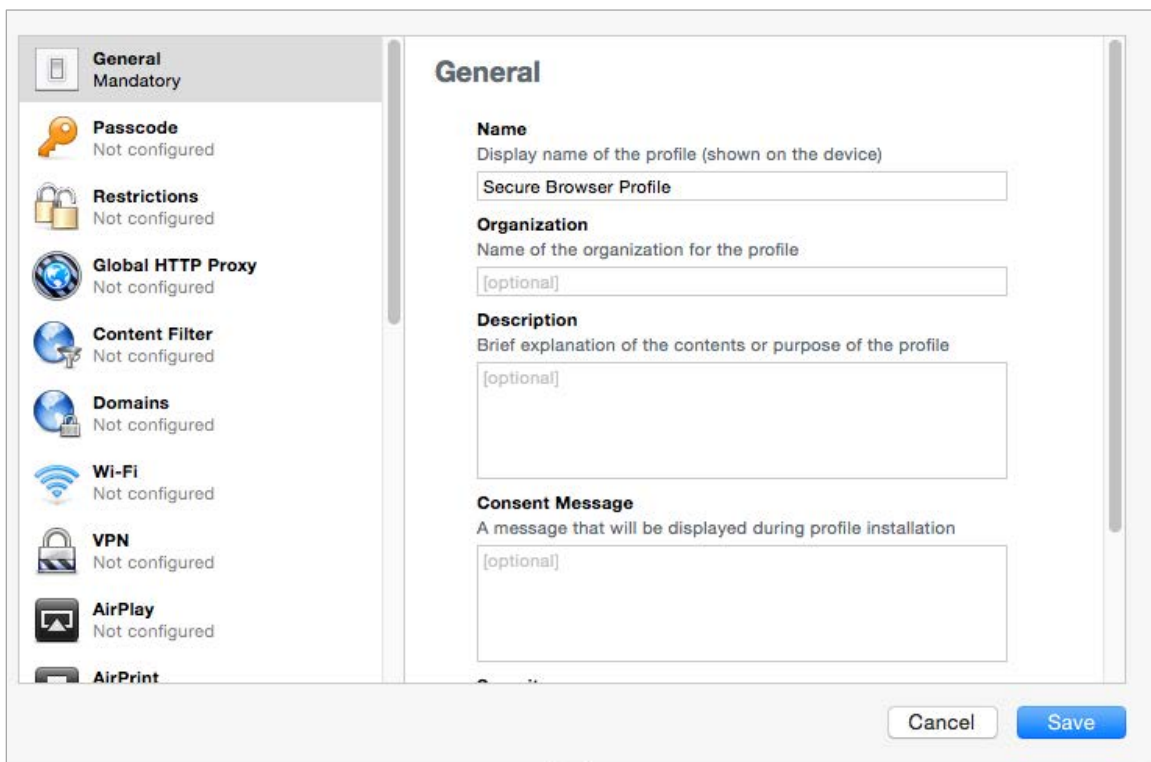



Figure 44. Create New Profile configuration options

4. In the “General” section, enter a name for the profile in the *Name* field.
5. In the “Restrictions” section, select [**Configure**]. A list of restrictions appears.
 - a. Make any required changes to the restrictions, or retain the default settings.
 - b. Select [**Save**]. You return to the [**Settings**] tab, and the profile appears in the *Profiles* list.
6. Select the [**Export**] right-arrow [] icon to export the profile to the Mac.

Creation of the supervisory profile is complete.

Step 4. Place iPads in Autonomous Single App Mode.



Additional Resources:

- CAASPP Secure Browsers website—<http://ca.browsers.airast.org/>



TIP: Before starting this procedure, connect the iPads to the Mac through a USB hub. That way you can perform the installation on multiple iPads at once.

System Configuration | Software Configuration

To install the MDM profile, supervisory profile, and secure browser:

1. On the Mac where you performed [Step 3. Create a supervisory profile](#), open the Apple Configurator.
2. From the *Apple Configurator* menu, select *Preferences*. The *Preferences* screen opens (Figure 45).

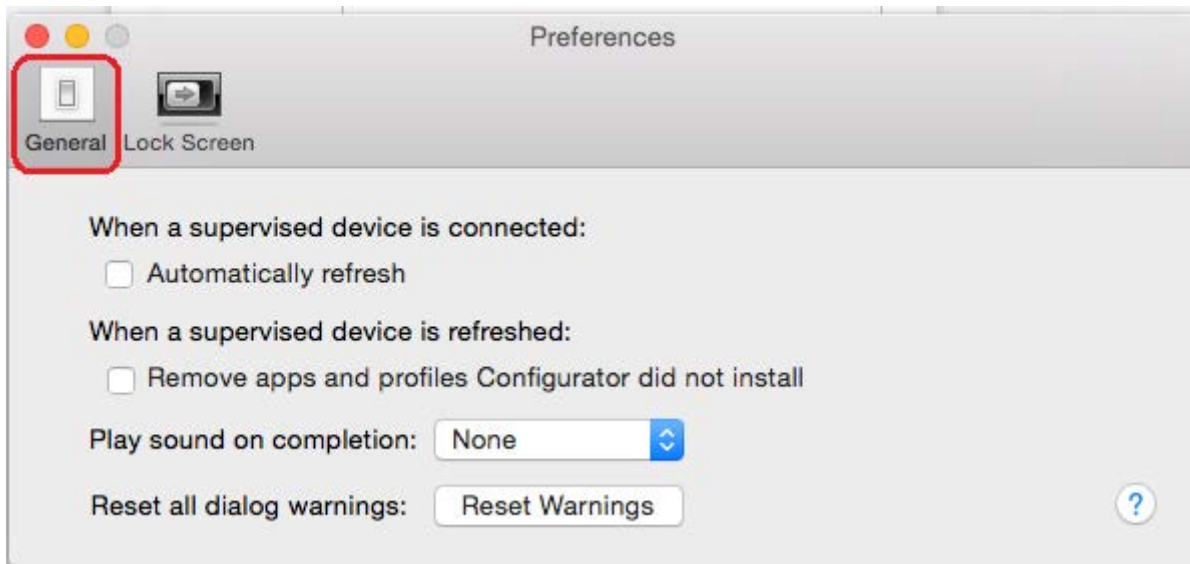


Figure 45. Preferences options

3. In the **[General]** tab, clear the *Automatically refresh* and *Remove apps and profiles Configurator did not install* check boxes.
4. Close the *Preferences* screen.
5. Back in the Apple Configurator, select **[Prepare]** and then **[Settings]**. The *Settings* screen appears (see Figure 43).
6. In the *Name* field, enter a name to apply to the iPads.
7. *Optional:* Mark the *Number sequentially starting at 1* check box. This adds a number to each iPad's name. For example, if the *Name* field says Garden Elementary School, and if three iPads are connected, each device receives a name like Garden Elementary School 1, Garden Elementary School 2, and Garden Elementary School 3.
8. Set *Supervision* to **[On]**.
9. Select **[Organization Info...]**. The *Organization Info* screen appears (Figure 46).

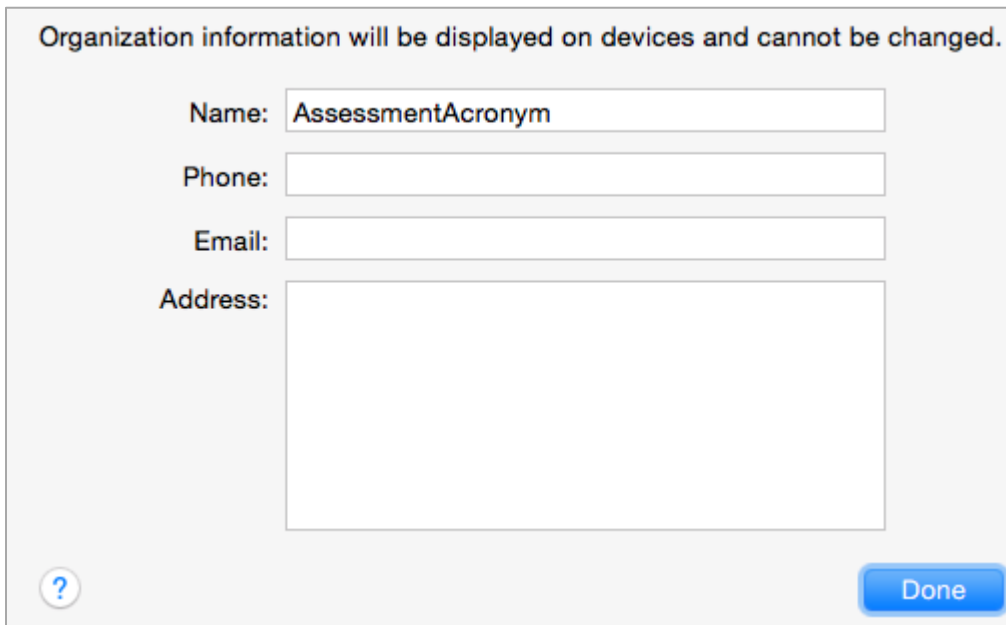


Figure 46. Organization Info screen

10. In the *Name* field, enter [Local Educational Agency Name or Test Site Name] and then select **Done**. The *Organization Info* screen closes.
11. If the profile you created in [Step 3. Create a supervisory profile](#) does not appear in the *Profiles* list, import it by taking the following steps:
 - a. Select **+** below the *Profiles* list and select **Import Profile...**
 - b. Navigate to the profile you saved as a result of this process, and then select [**Open**].
12. Check the box for the profile you want to prepare onto the iPads (see Figure 43).
13. Connect each iPad to the Mac via a USB cable or USB hub.
14. On each connected iPad, uninstall any existing versions of the secure browser.
15. In the Apple Configurator, under the [**Prepare**] tab, select the [**Prepare**] icon at the bottom of the screen. A confirmation message appears.
16. Select [**Apply**] in the confirmation message. Preparation starts and may take several minutes, after which the iPad restarts. The Apple Configurator displays progress messages during the prepare process (Figure 47).

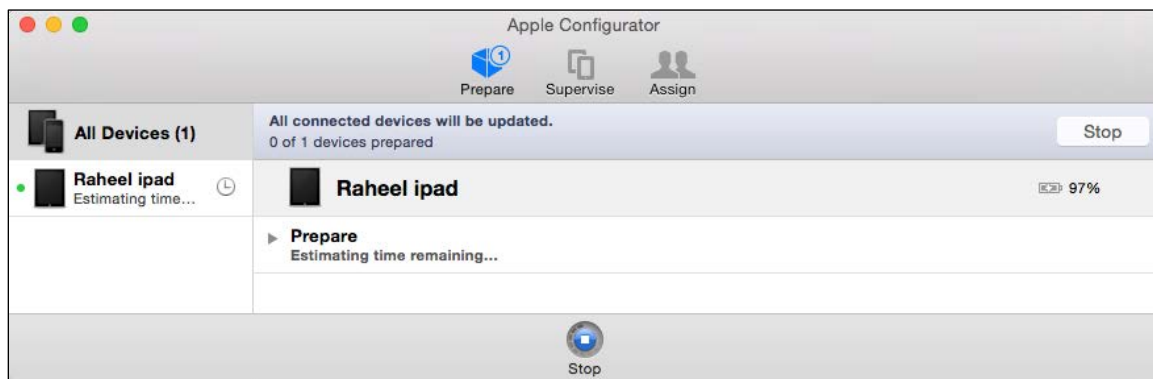


Figure 47. Apple Configurator screen



Note: Apple Configurator may force the iPads to upgrade to the latest version of iOS.

17. After the iPad restarts, follow the prompts on the iPad to configure it until the home screen appears.
18. *Optional:* Confirm the supervisory profile is installed on the iPad. Go to *Settings* → *General* → *Profiles*. The profile name you used in [Step 4. Place iPads in Autonomous Single App Mode](#) appears under *Configuration Profiles*.
19. On the iPad, download and install the MDM profile you created in [Step 1. Create a mobile device management profile](#).
20. After the MDM profile installation completes, install the secure browser onto the iPad. You can download the secure browser for iOS from the [CAASPP Secure Browsers](#) website. (Detailed instructions for installing the secure browser are in the subsection “[Installing the Secure Browser on iOS](#)” of [Chapter 4, Secure Browser Configuration](#).)
21. *Optional:* To confirm installation, attempt to open the secure browser on the testing device. If it opens and the student is able to access a practice or training test, installation was successful. If it does not, then repeat this process.
22. Repeat steps 13–21 to prepare additional iPads.
23. In the Apple Configurator, select [**Stop**] and close the Apple Configurator.

Setting the iPad into ASAM is complete. When a student starts a test, the iPad enters ASAM mode.

Using Automatic Assessment Configuration



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

If students are using iPads with iOS 10 or later, you can use Automatic Assessment Configuration. This configuration includes a preset profile in the AIRSecureTest app that automatically suppresses the features listed in Table 6.

When a student taps [**Begin Test Now**] on an iPad with Automatic Assessment Configuration, a message similar to that in Figure 48 appears.

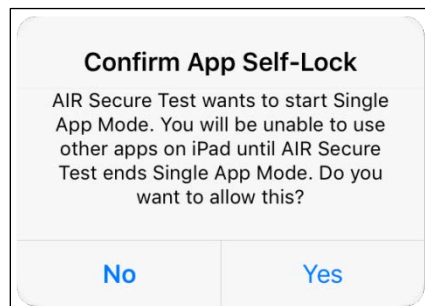


Figure 48. Notification when starting test with automatic assessment configuration

Removing the Emoji Keyboard from an iOS 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 49). This keyboard, if activated, can be confusing for test takers or scorers. Use the following procedure to remove the Emoji keyboard from an iOS device.

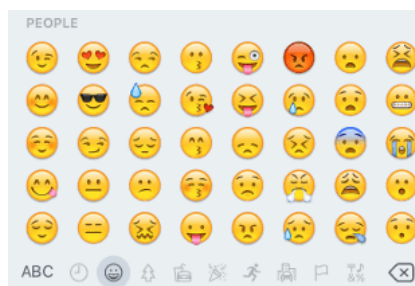


Figure 49. Emoji keyboard for iOS

To remove the Emoji keyboard:

1. Tap the [**Settings**] icon (Figure 50).



Figure 50. [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 51).

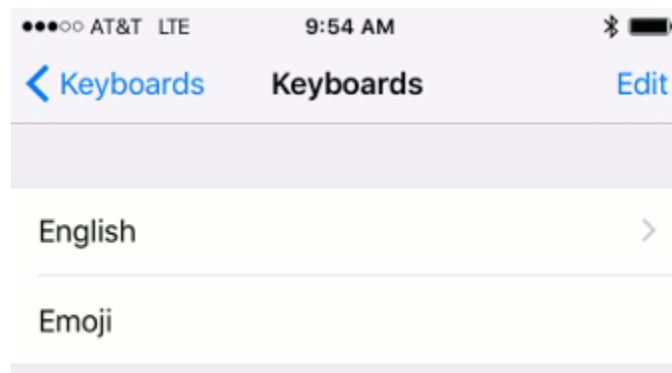


Figure 51. Keyboards configuration interface

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 OS X device:

1. Tap the [**Settings**] icon.
2. Navigate to *General* → *Keyboard*.
3. Move the slider to turn off *Enable Dictation* (Figure 52).



Figure 52. 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 53)

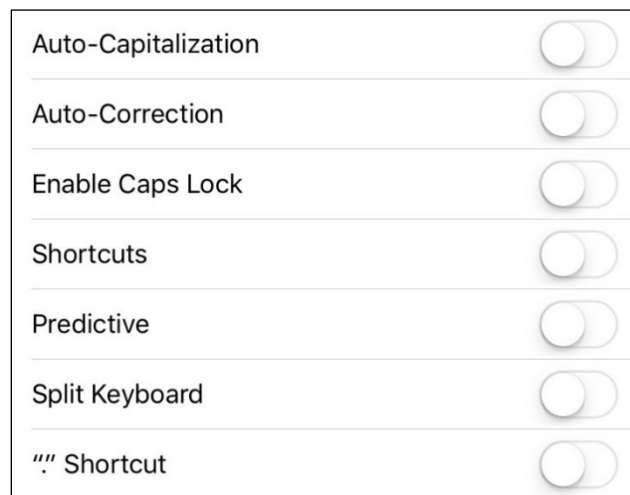


Figure 53. Keyboard Settings for iOS 10 (other versions of iOS are similar)

Android Devices

This subsection describes how to configure mobile devices running Android.

Disabling the Default Keyboard and Enabling the Secure Browser Keyboard on Android

The default keyboard for the Android allows predictive text, which may provide students with hints for answers to tests. For this reason, the secure browser for Android requires that a mobile secure browser keyboard be configured for the secure browser itself. The secure browser keyboard is a basic keyboard, with no row for predictive text functionality.



Note about the Secure Browser Keyboard and General Settings:

- Once the secure browser keyboard is set, it becomes the default keyboard for all Android tablet applications, not just for the secure browser. If you want to return to the default Android keyboard after using the secure browser, you will need to navigate to *Settings* → *Language & Input* and uncheck the secure browser keyboard.
- If you change back to the default Android keyboard, you will be prompted to select the secure browser keyboard the next time you open the secure browser. The secure browser will not allow you to access the student logon page until the secure browser keyboard has been selected.

The following procedure describes how to enable the secure browser keyboard.

1. Open Settings.
2. Open General Management
3. Open Language and Input.
4. Open On-Screen Keyboard.
5. Select *Manage keyboards*.
6. Set AIR Secure Test to on by selecting its checkbox. A confirmation box will appear.
7. Select [OK].

Disabling the Multi Window on Samsung Tablets

Samsung tablets are equipped with a Multi window feature to display app launchers. Depending on the available app launchers, the Multi window can compromise testing security. To avoid this scenario, disable the Multi window on Samsung tablets.

The following instructions are based on Android 5.0.2 on a Samsung Galaxy Tab4; similar instructions apply for other versions of Android on Samsung tablets.

To disable the Multi window:

1. Tap [Settings].
2. Navigate to *Device* → *Sound and display*.
3. Turn off the Multi window using the slider (indicated in Figure 54).

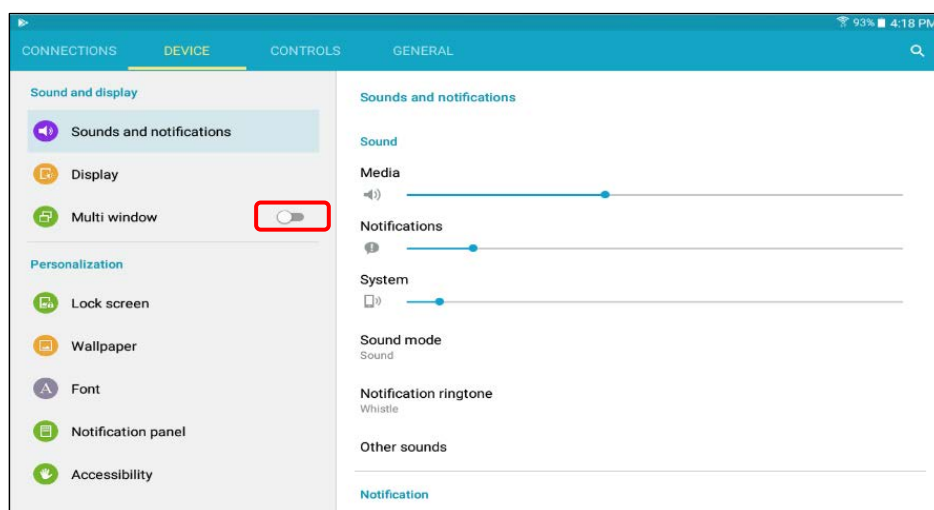


Figure 54. Disable the Multi window

Disabling the Stylus on Samsung Galaxy Note

The Samsung Galaxy Note stylus, S Pen, is capable of launching apps—a situation that can compromise testing security. To avoid this scenario, disable the stylus feature.

To disable the stylus:

1. Tap [**Settings**].
2. Navigate to *Controls* → *Voice and input methods*.
3. Tap **S Pen**.
4. Disable all of the available features (Figure 55).

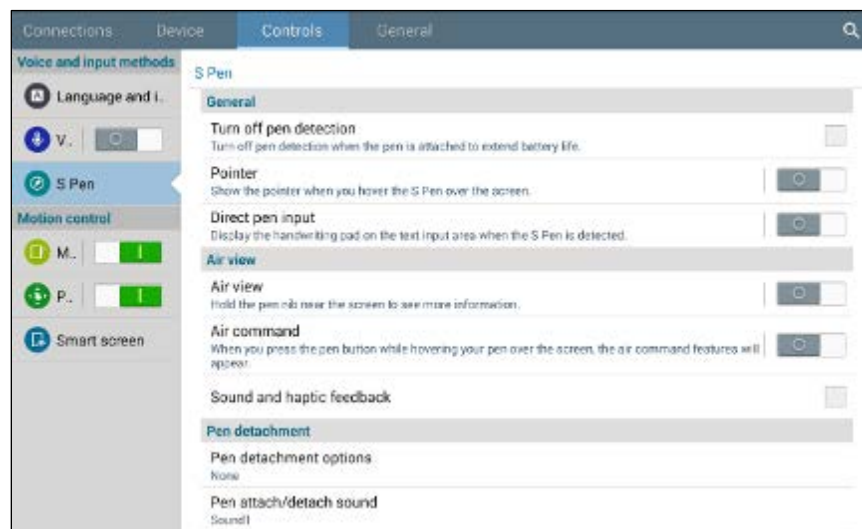


Figure 55. Disable the Samsung stylus

Chromebook Mobile Devices

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

Disabling Auto Updates for Chrome OS

Additional Resources:

- Google Manage Chrome device settings web page—
<https://support.google.com/chrome/a/answer/1375678?hl=en>

You may want to disable auto updates during your 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 AIR supports up to Chrome OS version 67, and version 67 is installed on your students’ Chromebooks, you can prevent auto updates to any later version. (Alternatively, you can allow auto updates to a specific version supported by AIR; for details, see 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 [Manage Chrome device settings](#) 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*.

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

AIR has tested CAASPP operational software (such as the Test Administrator Interface) and the practice and training tests up to version 51 of the Chrome OS; you may want to prevent your Chromebooks from auto-updating beyond that version. (Alternatively, you can disable auto updates entirely; for details, see the subsection “[Installing the AIRSecureTest 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 [Manage Chrome device settings](#) web page. The steps in that procedure assume that your 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**].

Securing Chrome OS for High-Stakes Assessments

1. Access *Google Admin Console: Device Management* → *Chrome management* → *Device settings* → *Sign-in restriction*.
2. Select the *Do not allow any user to sign-in* option from the *Restrict sign-in* list (Figure 56).

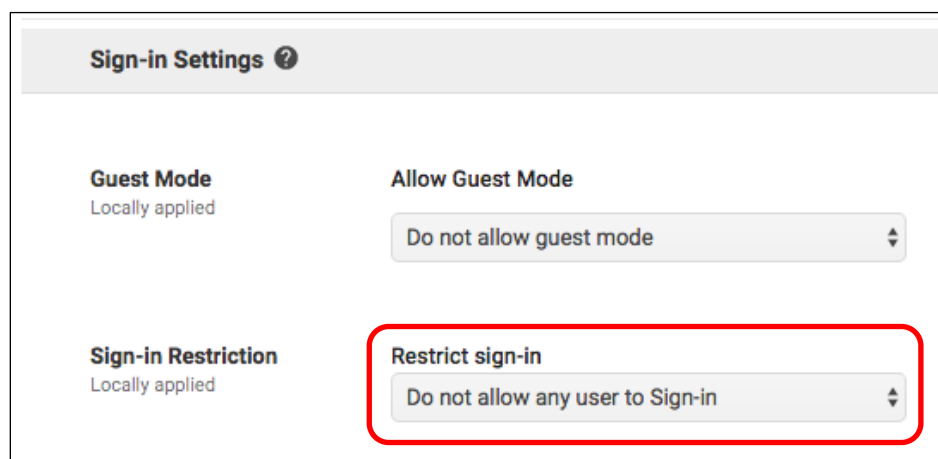


Figure 56. Chrome Sign-in Settings options

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 Properties* 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 Properties* dialog box.
7. Close the Control Panel.

Mac OS Devices

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

- Google Chrome Web Store—<https://chrome.google.com/webstore/>
- Neverware website—<https://www.neverware.com/>
- Neverware Certified Model Finder 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 your school or local educational agency has older devices that do not run newer versions of Windows or OS X, consider installing CloudReady on those devices. This installation can postpone or prevent a costly hardware upgrade.



Warning: Process Erases All Data

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


Take these steps to install CloudReady:

1. Ensure the device on which you are installing CloudReady meets the following requirements:
 - 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 you received 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 to you by Neverware. This URL downloads a file with a name similar to `cloudready_site646.bin`. Note the location of the file on your 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 57).



Figure 57. 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 58).

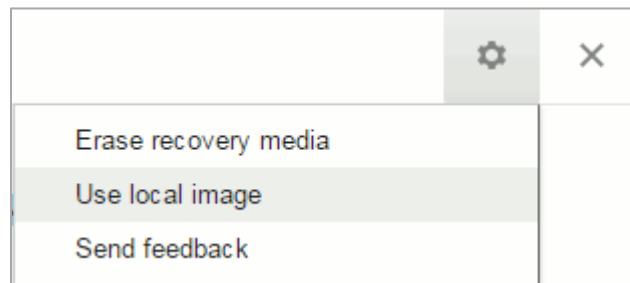


Figure 58. Selecting the CloudReady image

13. Navigate to the file image file you downloaded in step 6.
14. At the prompt (Figure 59), select the USB drive you inserted in step 7.

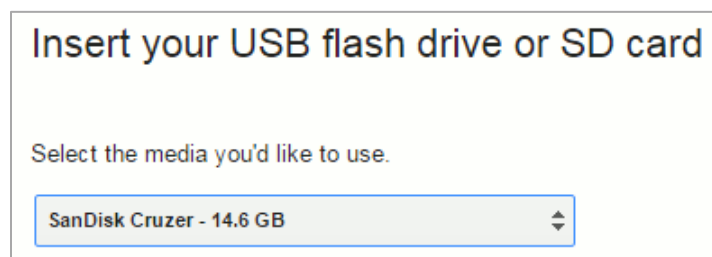


Figure 59. CloudReady media insertion prompt

15. Select **[Continue]**.

16. In the next screen, select [**Create Now**]. The recovery utility creates a bootable image of CloudReady onto 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 you are installing CloudReady, do the following:
 - a. Back up all files you want to save. 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, your device turns off.
 - c. Remove the USB drive and power on the device.
 - d. Install the AIRSecureTest Kiosk App; see [Chapter 4, Secure Browser Configuration](#) for details.

Configurations for Testing Students Using Accessibility Supports



Additional Resources:

- CAASPP Student Accessibility Resources and Test Settings web page—
<http://www.caaspp.org/administration/accessibility/>

For information about configuring operating systems and software for testing with accessibility supports, including braille, text-to-speech and the NeoSpeech voice pack, and permissive mode, refer to the *Accessibility Guide for CAASPP Online Testing*, which will be available on the CAASPP [Student Accessibility Resources and Test Settings](#) web page.

Chapter 4. Secure Browser Configuration

Overview of Secure Browsers

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 and/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 other computer or internet applications or copying test information. **All devices that will be used for testing must have the correct secure browser installed.**

This subsection contains instructions for downloading and installing the secure browsers. Your local educational agency (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 the following requirements 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, see 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 your 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. See 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

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 for California Assessment of Student Performance and Progress assessments.**

However, in extremely rare circumstances, 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 rare cases where a dual monitor **is allowed, monitors should be set up to "mirror" each other.** School technology coordinators can assist test administrators 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 administered in a secure environment to prevent others from hearing the questions or viewing the student or test administrator screens.

Secure Browser Versions for Online Testing

Table 14 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 14 must uninstall it before installing the secure browser for the 2018–19 school year.**

Table 14. Secure Browsers by Operating System

Operating Systems	Secure Browser
Windows 7 SP1 (Professional and Enterprise)	10.3
Windows 8.0 (Professional and Enterprise)	10.3
Windows 8.1 (Professional and Enterprise)	10.3
Windows 10 and 10 in S mode (Professional, Educational, and Enterprise) <ul style="list-style-type: none"> • Versions 1507–1803 • Version 1809 (upon acceptance) 	10.3
Windows Server <ul style="list-style-type: none"> • 2008 • 2012 • 2016 (thin client) 	10.3
Mac OS X <ul style="list-style-type: none"> • Versions 10.9–10.14 	10.3
Linux Fedora 25–26 LTS (Gnome)	10.3
Linux Ubuntu LTS (Gnome) <ul style="list-style-type: none"> • Version 14.04 • Version 16.04 • Version 18.04 	10.3
iOS (iPads) <ul style="list-style-type: none"> • Version 10.3 • Version 11.4 • Version 12 	AIRSecureTest Mobile Secure Browser 5
Android <ul style="list-style-type: none"> • Version 7.1 • Version 8.1 • Version 9 	AIRSecureTest Mobile Secure Browser 5
Chrome OS 67+ and above	AIRSecureTest kiosk application 5

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 (e.g., Internet Explorer) or an antivirus program is triggered in the background in order 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.

Secure Browser Error Messages

Secure Browser Not Detected

The test delivery system (TDS) automatically detects whether a device is using the secure browser to access the online assessments.

Unable to Establish a Connection with the Test Delivery System

If a device fails to establish a connection with the TDS, the system will display a message noting this. This is most likely to occur if there is a network-related problem. The cause can be anything from a network cable not being plugged in, to the firewall not allowing access to the site.

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:

- California Assessment of Student Performance and Progress (CAASPP) Portal website—<http://www.caaspp.org/>
- CAASPP Secure Browsers website—<http://ca.browsers.airast.org/>
- 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 7 SP1, 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 you are running a 32-bit version of Windows, 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 you do not have administrator rights, refer to the subsection “[Installing the Secure Browser Without Administrator Rights](#).”)

1. If you 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 you installed in the default location, the installation package automatically removes it.) See the instructions in the subsection “[Uninstalling the Secure Browser on Windows](#).”
2. Navigate to the [CAASPP Secure Browsers](#) web page by going to the [CAASPP Portal](#) website and selecting the [**Secure Browsers**] button.

3. Scroll down the [CAASPP 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 60). A dialog box opens.



Figure 60. [Download Browser] button

5. Take one of the following steps; this step may vary depending on the web browser you are using:
 - 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 61).



Figure 61. [CASecureBrowser] shortcut icon

8. Ensure all background jobs, such as virus scans or software updates, are scheduled outside of test windows. For example, if your 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. See Table 15 for available forms of this command.
 - c. Select **[OK]** to close the *Properties* dialog box.

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

For more information about proxy settings, see [Proxy Settings for Desktop Secure Browsers](#).

10. Run the secure browser by double-clicking the **[CA Secure Browser]** shortcut icon on the desktop (shown in Figure 61). 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 you do not have administrator rights, refer to the subsection [“Installing the Secure Browser Without Administrator Rights.”](#)

1. If you 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 you installed in `C:\Program Files (x86)\`, the installation package automatically removes it.) See the instructions in the subsection [“Uninstalling the Secure Browser on Windows.”](#)
2. Navigate to the [CAASPP Secure Browsers](#) web page by going to the [CAASPP Portal](#) website and selecting the **[Secure Browsers]** button.
3. Scroll down the [CAASPP 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 62). A dialog box opens.



Figure 62. [Download Browser] button

5. Save the file on the computer (this step may vary depending on the web browser you are using):
 - 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.
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 where you want 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 test windows. For example, if your 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 63). The secure browser opens, displaying the student logon screen. The secure browser fills the entire screen and hides the task bar.

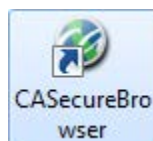


Figure 63. [CASecureBrowser] shortcut icon

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

Sharing the Secure Browser over a Network



Warning: Testing Quality over a Network

- 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/output. Therefore, this installation scenario is **not recommended for testing**.

In this scenario, you install the secure browser on a server's shared drive, and you also create a shortcut to the secure browser's executable on each testing computer's desktop. This assumes that all testing computers have access to the shared drive.

1. On the remote computer from where the students run the secure browser, install the secure browser following the directions in the subsection "[Installing the Secure Browser on an Individual Computer](#)."
2. On each testing device, sign in and take the following steps:
 - a. Ensure all background jobs, such as virus scans or software updates, are scheduled outside of test windows. For example, if your testing takes place between 8 a.m. and 3 p.m., schedule background jobs outside of these hours.
 - b. Copy the desktop shortcut `CASecureBrowser` from the remote device to the directory `C:\Users\Public\Public Desktop`.
 - c. Run the secure browser by double-clicking the [**CASecureBrowser**] shortcut icon on the desktop (shown in Figure 64). The secure browser opens, displaying the student logon screen. The secure browser fills the entire screen and hides the task bar.

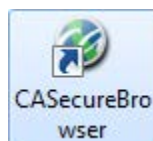


Figure 64. [**CASecureBrowser**] shortcut icon

- d. 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 you 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 you will copy the secure browser file (it should be the same directory on all computers). For example, you may want to copy the directory to `c:\AssessmentTesting\`. Ensure you select a directory in which the students can run executables.
3. On each local testing computer, do the following:
 - a. Ensure all background jobs, such as virus scans or software updates, are scheduled outside of test windows. For example, if your testing takes place between 8 a.m. and 3 p.m., schedule background jobs outside of these hours.
 - b. Copy the installation directory used in step 1 from the remote machine to the directory you selected in step 1. For example, if the target directory is `c:\AssessmentTesting\`, you are creating 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 to the Windows server, and starts the secure browser so it is ready for the students.

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

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

For a listing of supported terminals and servers for this scenario, see [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 you used a different installation path on the Windows server, 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, see [Appendix E, Creating Group Policy Objects to Assign Logon ScriptsAppendixE](#).
6. On each NComputing console, create a new **[CASecureBrowser]** desktop shortcut 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 you used a different installation path on the Windows server, 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 2008.



Warning: Testing Quality with Servers

- 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/output. Therefore, this installation scenario is **not recommended for testing**.

Local educational agency CAASPP 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, you copy the secure browser from one machine where it is installed onto another machine on which you do 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 you 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 test windows. For example, if your 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.

Uninstalling the Secure Browser on Windows

The following subsections describe how to uninstall the secure browser from Windows or from the command line.

Uninstalling via the User Interface

The following instructions may vary depending on your 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 comes with Microsoft's Take a Test app, which enforces a locked-down, secure testing environment identical to AIR's secure browser. Users of the Take a Test app do not need to install the AIR 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, see 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, see the Microsoft Windows help topic [Take tests in Windows 10](#)) Because of this, AIR 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 > Work or school Access > Set up an account for taking tests*.
3. Select an existing account to use as the dedicated testing account.



Note: If you do not have an account on the device, you can create a new account. To do this, go to *Settings > Accounts > Family & 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.airast.org/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 65. *Create Shortcut* dialog box).

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

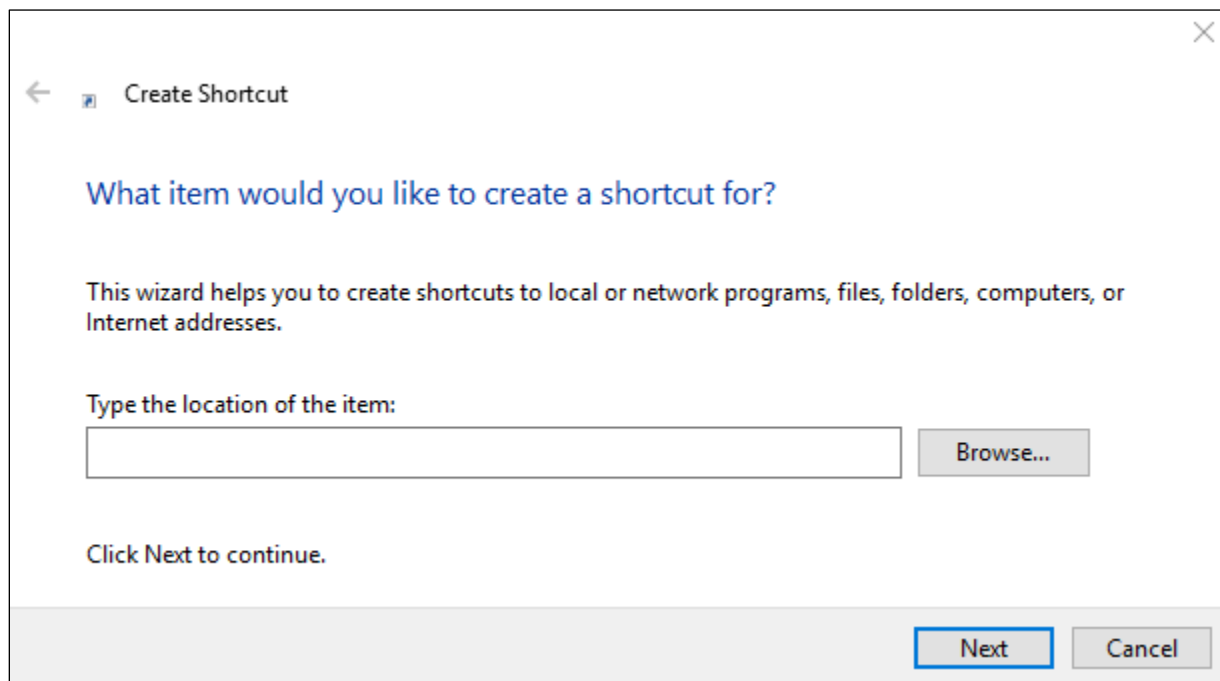


Figure 65. Create Shortcut dialog box

3. In the *Type the location of the item* field, enter
`ca-edu-secureassessment:https://ca.tds.airast.org/student`
4. Select [**N**ext].
5. In the next dialog box, enter a name for the shortcut in the *Type a name for this shortcut* field.
6. Select [**F**inish].

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 Mac OS X



Additional Resources:

- California Assessment of Student Performance and Progress (CAASPP) Portal website—<http://www.caaspp.org/>
- CAASPP Secure Browsers website—<http://ca.browsers.airast.org/>

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 Mac OS X 10.9 through 10.14. The steps in this procedure may vary depending on your version of Mac OS X and your web browser.

1. Remove any previous version of the secure browser by dragging its folder to the Trash.
2. Navigate to the [CAASPP Secure Browsers](#) web page by going to the [CAASPP Portal](#) website and selecting the [**Secure Browsers**] button.
3. Scroll down the [CAASPP Secure Browsers](#) web page to the “Download Secure Browsers” section.
4. Select the [**Mac OS X 10.9–10.14**] tab and then select the [**Download Browser**] button (shown as highlighted in Figure 66). A dialog box opens.



Figure 66. [**Download Browser**] button

5. If you are prompted for a download location, select your Downloads folder.

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

6. Open Downloads from the dock, and then select `CASecureBrowser-OSX.dmg` to display its contents (Figure 67).

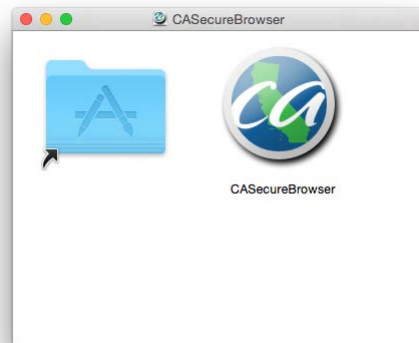


Figure 67. Contents of the CASecureBrowser-OSX.dmg folder

7. **If you are running Mac OS X 10.11**, 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 68) and then type your password to enable changes.

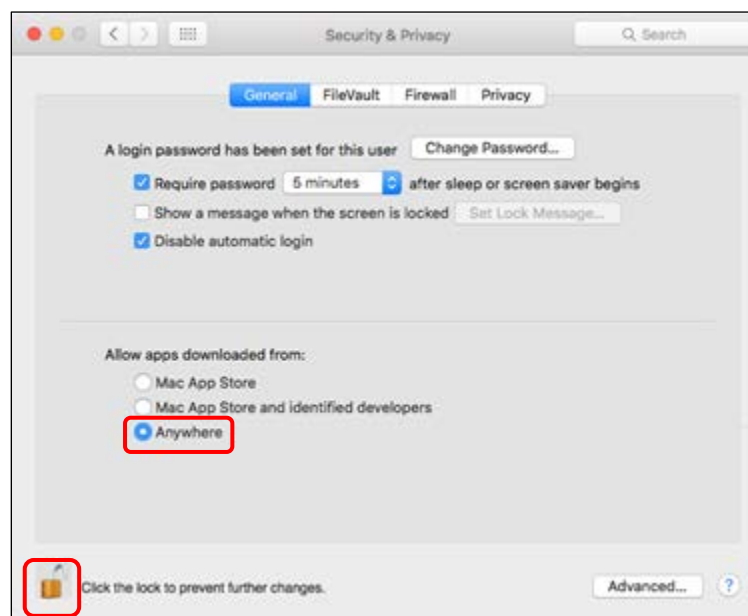


Figure 68. Security & Privacy screen for Mac OS X 10.11

- d. In the “Allow apps downloaded from” section, first note which radio button is highlighted, and then select the *Anywhere* radio button (also indicated in Figure 68).
- e. Select [**Allow From Anywhere**] in the confirmation message.
8. Drag the [**CASecureBrowser**] 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 your testing takes place between 8 a.m. and 3 p.m., schedule background jobs outside of these hours.
10. Disable Mission Control/Spaces. Instructions for disabling Spaces are in [Chapter 3, Hardware Configuration](#).
11. In Finder, navigate to *Go* → *Applications*, and then double-click *CASecureBrowser* to launch the secure browser. (You 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.

12. To exit the secure browser, select [**CLOSE SECURE BROWSER**] in the upper-right corner of the screen.
13. To create a desktop shortcut, from the Applications folder, drag *CASecureBrowser* to the desktop.
14. **Mac 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 your networking and permissions, it may be faster to install the secure browser onto 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. On the Mac from where you will clone the installation, do the following:
 - 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.

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

- d. Delete the `CASecureBrowser` folder containing the secure browser (indicated in Figure 69).
- e. Delete the `Mozilla` folder (also indicated in Figure 69).

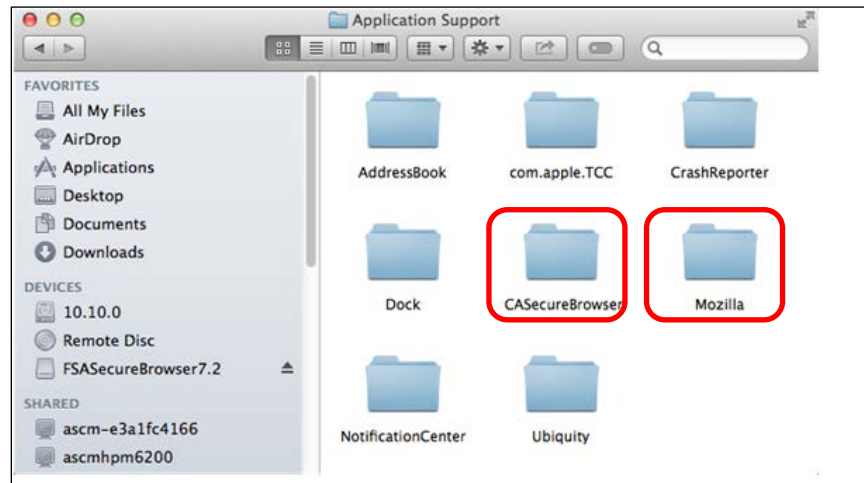


Figure 69. Apple *Application Support* configuration interface

2. Create a shell script that creates a new secure browser profile when a user logs in. 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 OS X image.
4. Deploy the image to the target Macs.

Uninstalling the Secure Browser on OS X

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

Installing the Secure Browser on Linux

Additional Resources:

- California Assessment of Student Performance and Progress (CAASPP) Portal website—<http://www.caaspp.org/>
- CAASPP Secure Browsers website—<http://ca.browsers.airast.org/>

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 “[Configuring Linux for Online Testing with the Secure Browser](#).”

Installing the Secure Browser on 32- or 64-Bit Distributions

The instructions in this subsection are for installing the Linux secure browser onto 32- or 64-bit versions of Linux systems. These instructions may vary for your 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 you are installing the secure browser.
3. Navigate to the [CAASPP Secure Browsers](#) web page by going to the [CAASPP Portal](#) website and selecting the [**Secure Browsers**] button.
4. Scroll down the [CAASPP 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 70).



Figure 70. [Download Browser] button

6. Save the file to the desktop.
7. Right-click the downloaded file `CASecureBrowserX.X-YYYY-MM-DD-i686.tar.bz2` (32-bit) or `CASecureBrowserX.X-YYYY-MM-DD-x86_64.tar.bz2` (64-bit), and select [**Extract Here**] to expand the file. This creates the `CASecureBrowser` folder on the desktop.
8. In a file manager, open the `CASecureBrowser` folder.
9. For Ubuntu, disable automatic running of scripts by doing the following (otherwise skip to step 10):
 - a. From the menu bar, select *Edit* → *Preferences*.
 - b. On the [**Behavior**] tab, select the *Ask each time* radio button.
 - c. Select [**Close**].
10. Change the installation script to executable by taking the following steps:
 - a. Right-click the file `install-icon.sh`, and select *Properties* from the shortcut menu.
 - b. On the [**Permissions**] tab, check the *Allow executing file as a program* box.
 - c. Select [**Close**].

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

11. Right-click the file `install-icon.sh` and select *Open* from the shortcut menu. In the next dialog box, select **[Run in Terminal]**. The installation program runs and creates a **[CA Secure Browser]** icon on the desktop (shown in Figure 71). The installation script prompts you for the root or superuser password you obtained in step 2.



Figure 71. [CA Secure Browser] shortcut icon

12. Enter the password. The script installs all dependent libraries and supported voice packs, and creates a **[CA Secure Browser]** icon on the desktop.
13. Ensure all background jobs, such as virus scans or software updates, are scheduled outside of test windows. For example, if your 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 **[CA Secure Browser]** icon to launch the secure browser. 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 **[CLOSE SECURE BROWSER]** in the upper-right corner of the screen.

Extracting the Secure Browser TAR File

Users attempting to install the secure browser on Fedora 27–28 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 10

Installation of secure browser version 10 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 AIRSecureTest, the secure browser app for iOS, Android, and Chrome OS. For information about configuring supported tablets and Chromebooks to work with the secure browser, refer to [Chapter 3, Hardware Configuration](#).

Installing the Secure Browser on iOS



Additional Resources:

- Apple Configuration Profile Reference web page—
<https://developer.apple.com/library/content/featuredarticles/iPhoneConfigurationProfileRef/Introduction/Introduction.html>
- California Assessment of Student Performance and Progress (CAASPP) Portal website—<http://www.caaspp.org/>
- CAASPP Secure Browsers website—<http://ca.browsers.airast.org/>



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



TIP: To install the secure browser on many iOS devices simultaneously, consider using Autonomous Single App Mode. For more information, see the subsection “[Using Autonomous Single App Mode \(ASAM\)](#).”

Instructions for Installation

This subsection contains instructions for downloading and installing AIRSecureTest and selecting your state and assessment program. The process for installing the secure browser is the same as for any other iOS application.

1. On the iPad, navigate to the [CAASPP Secure Browsers](#) web page by going to the [CAASPP Portal](#) website and selecting the [Secure Browsers] button.
2. Scroll down the [CAASPP Secure Browsers](#) web page to the “Download Secure Browsers” section.
3. Select the [iOS] tab.

4. Select the **[Download on the App Store]** button, shown as highlighted in Figure 72. (You also can search for AIRSecureTest in the App Store to find the secure browser app.)

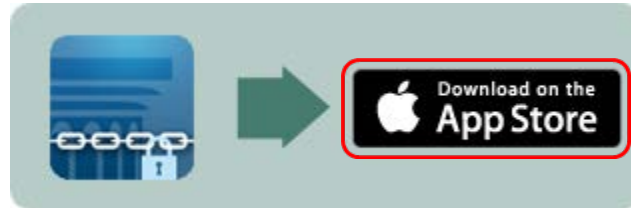


Figure 72. [Download on the App Store] button

5. The AIRSecureTest download web page, shown in Figure 73, opens.

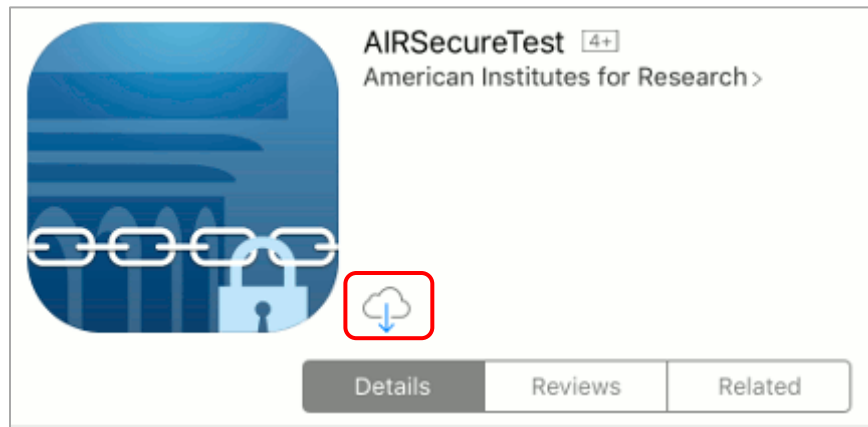


Figure 73. AIRSecureTest App Store download web page


6. Tap the **[Download]** cloud  icon, indicated in Figure 73. The iPad downloads and installs the secure browser, and the button changes to **[Open]**. (Note that you must be signed in to the App Store to download AIRSecureTest.)
7. After installation, an **[AIRSecureTest]** icon like the one shown in Figure 74 appears on the iPad's home screen.



Figure 74. [AIRSecureTest] icon, iOS

8. Tap **[Open]**. The first time you open AIRSecureTest, the *Launchpad* screen appears. The Launchpad establishes the state and test administration for your students.
9. In the *Please Select Your State* drop-down list (indicated in Figure 75), select *California*.

Secure Browser Configuration | Installing the Secure Browser on Mobile Devices

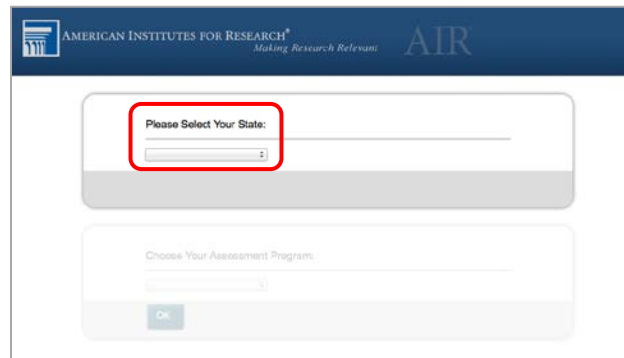


Figure 75. Select the state from the Launchpad

10. In the *Choose Your Assessment Program* drop-down list (indicated in Figure 76), select California Assessment System.

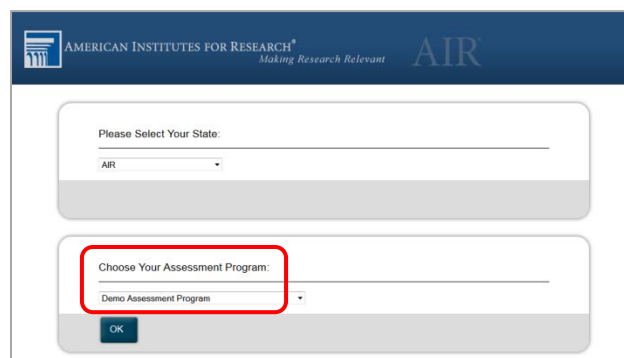


Figure 76. Select the assessment from the Launchpad

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 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

You 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. See the Apple [Configuration Profile Reference](#) web page for instructions and more information about using this key.

Installing AIRSecureTest on Android



Additional Resources:

- California Assessment of Student Performance and Progress (CAASPP) Portal website—<http://www.caaspp.org/>
- CAASPP Secure Browsers website—<http://ca.browsers.airast.org/>
- Google Admin console Sign in web page—<https://admin.google.com>

You can download AIRSecureTest from the [CAASPP Secure Browsers](#) web page or from the Google Play store. The process for installing the secure browser is the same as for any other Android application.

Downloading and Installing the Android AIRSecureTest Mobile Secure Browser

1. On your Android tablet, navigate to the [CAASPP Secure Browsers](#) web page by going to the [CAASPP Portal](#) website and selecting the [**Secure Browsers**] button.
2. Scroll down the [CAASPP Secure Browsers](#) web page to the “Download Secure Browsers” section.
3. Tap the [**Android**] tab.
4. Tap [**Get it on Google play**], shown as highlighted in Figure 77. (You can also search for AIRSecureTest in the Google Play store to find the secure browser app.)

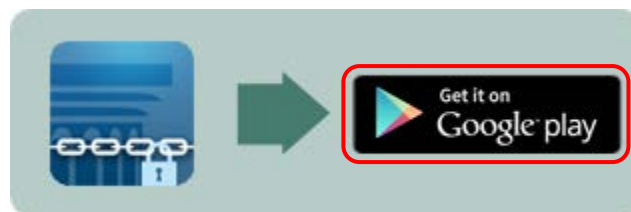


Figure 77. [Get it on Google play] button

5. The AIRSecureTest download web page appears (Figure 78).

Secure Browser Configuration | Installing the Secure Browser on Mobile Devices



Figure 78. AIRSecureTest Google Play download web page

6. Tap [**Install**] and then tap [**Accept**]. The tablet downloads and installs the secure browser. (Note that you must be signed in to Google Play to download AIRSecureTest.)
7. Open Settings.
8. Tap [**Cloud and accounts**]
9. Tap [**Users**].
10. Tap [**Add user or profile**].
11. Tap [**Restricted profile**]. The new profile opens with a list.
12. Tap [**New profile**], enter a name, and then tap [**OK**].
13. Enable *AIRSecure Browser* from the list. Users will have access to the secure browser in the restricted profile; all other apps will be disabled.
14. Tap [**Back**]
15. Swipe down from the top of the table with two fingers to open Quick Settings.
16. Tap [**Switch user**].
17. Tap the [**AIRSecureTest**] icon like the one shown in Figure 79 on the tablet's home page.

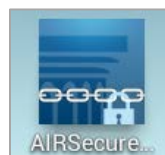


Figure 79. [AIRSecureTest] icon, Android

18. Tap [**Open**]. The first time you open AIRSecureTest, the *Launchpad* screen appears. The Launchpad establishes the state and test administration for your students.
19. In the *Please Select Your State* drop-down list (indicated in Figure 80), select *California*.

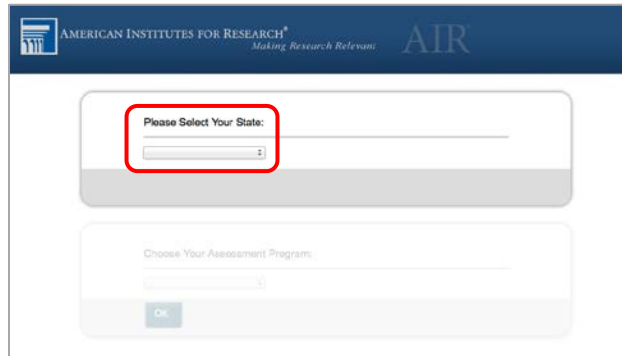


Figure 80. Select the state from the Launchpad

20. In the *Choose Your Assessment Program* drop-down list (shown in Figure 81), select *California Assessment of Student Performance and Progress*.

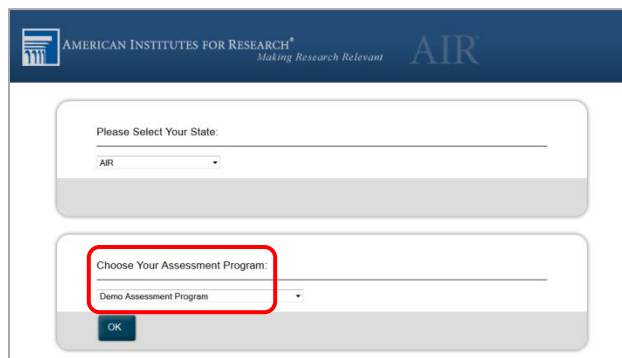


Figure 81. Select the assessment from the Launchpad

21. Tap [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.



Caution:

- If the secure browser keyboard has not been selected via device settings on Android tablets, it will need to be selected upon opening the AIRSecureTest app.
- For more information about the Android secure browser keyboard, including instructions for enabling it, refer to [Chapter 3, Hardware Configuration](#).

Chrome OS AIRSecureTest Kiosk App

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



Caution: 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 AIR Secure Browser. (This change restricting kiosk mode does not affect the Chrome operating system. You can still use any version of the Chrome OS on hardware manufactured in 2016 or earlier.)

Installing the AIRSecureTest Kiosk App on Standalone Chromebooks

These instructions are for installing the AIRSecureTest secure browser on standalone Chromebook devices.



Warning: This procedure erases all data on the Chromebook. Be sure to back up any data you want to keep before you begin.

1. Obtain the following from your 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 your 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 82, select your language, keyboard, and the wireless network information you acquired from the network administrator, and then select [**Continue**].



Figure 82. 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] +  +  ([Esc] + [**Reload**] + [**Power**]). The screen displays a yellow exclamation point (!) similar to that in Figure 83.



Figure 83. Chrome OS *Missing* message

- b. Press [Ctrl] + [D] to begin developer mode. A message similar to that in Figure 84 will appear.

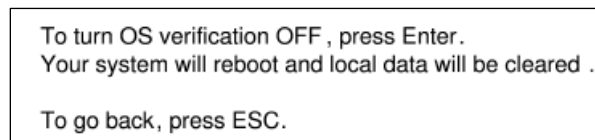


Figure 84. Turn OS Verification Off message

- c. Press [Enter]. A message similar to that in Figure 85 will appear.



Figure 85. OS Verification Is Off message

Secure Browser Configuration | Installing the Secure Browser on Mobile Devices

- d. Press [Ctrl] + [D]. The Chromebook indicates it is transitioning to developer mode (Figure 86). The transition takes approximately 10 minutes, after which the Chromebook reboots.

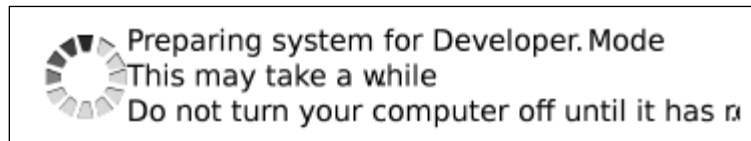


Figure 86. Preparing for Developer Mode message

- e. After the Chromebook reboots, the OS verification is Off message (Figure 85) appears again.
 - f. Press the [Spacebar] and then press [Enter]. The Chromebook reboots, and the *Welcome* screen appears (Figure 82).
5. In the *Welcome* screen, select your language, keyboard, and a network. The *Join WiFi Network* screen appears (Figure 87).

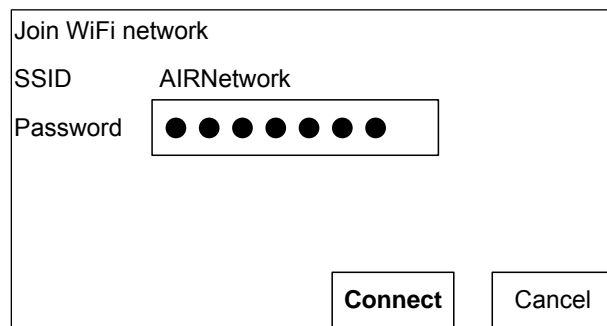


Figure 87. Join WiFi Network screen

6. Enter the network's password you obtained in step 1.
7. Select [**Connect**] on the *Join WiFi Network* screen and then [**Continue**] on the *Welcome* screen.
8. In the *Google Chrome OS Terms* screen, select [**Accept and continue**]. The *Sign in* screen (Figure 88) appears.

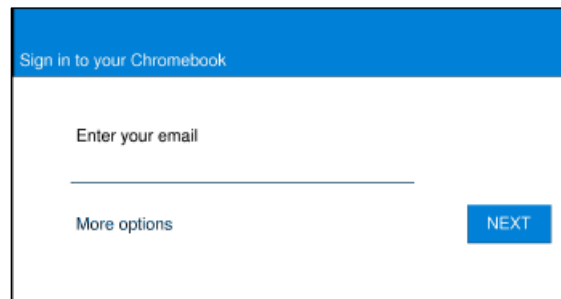


Figure 88. Chromebook *Sign in* screen

- In the *Sign in* screen, press [Ctrl] + [Alt] + [K] to open the *Automatic Kiosk Mode* screen (Figure 89).

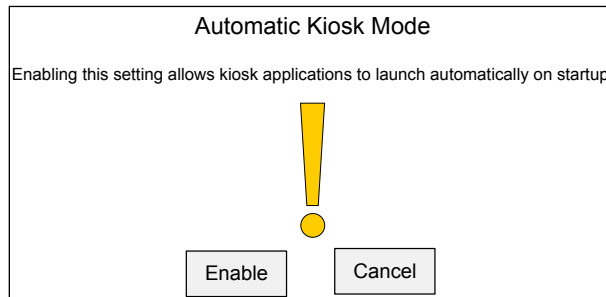


Figure 89. Automatic Kiosk Mode message

- Select [Enable] and then select [OK] to open the *Sign in* screen (Figure 88).
- In the *Sign in* screen, enter your email address, select [Next], enter the password, and then select [Next] again.
- When the desktop opens, select the [Chrome] icon [img alt="Chrome logo" data-bbox="595 625 615 640]] to open Chrome.
- In the URL bar, enter `chrome://extensions` to open the *Extensions* screen (Figure 90).

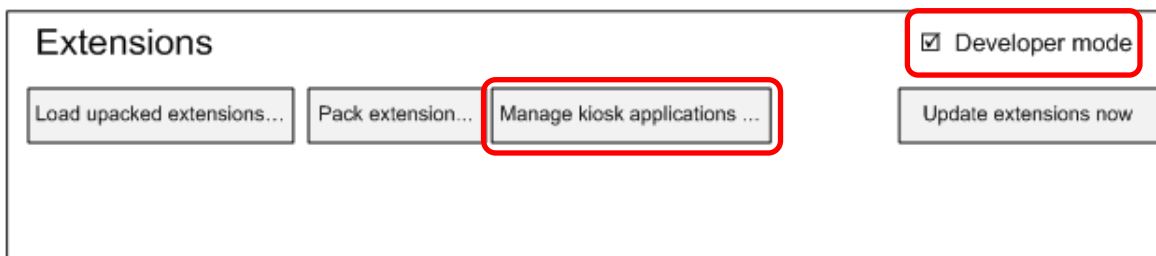


Figure 90. Extensions screen

- Mark the check box for *Developer Mode* (indicated in Figure 90).
- Select the [Manage kiosk applications] button—also indicated in Figure 90—to open the *Manage Kiosk Applications* screen (Figure 91).

Secure Browser Configuration | Installing the Secure Browser on Mobile Devices

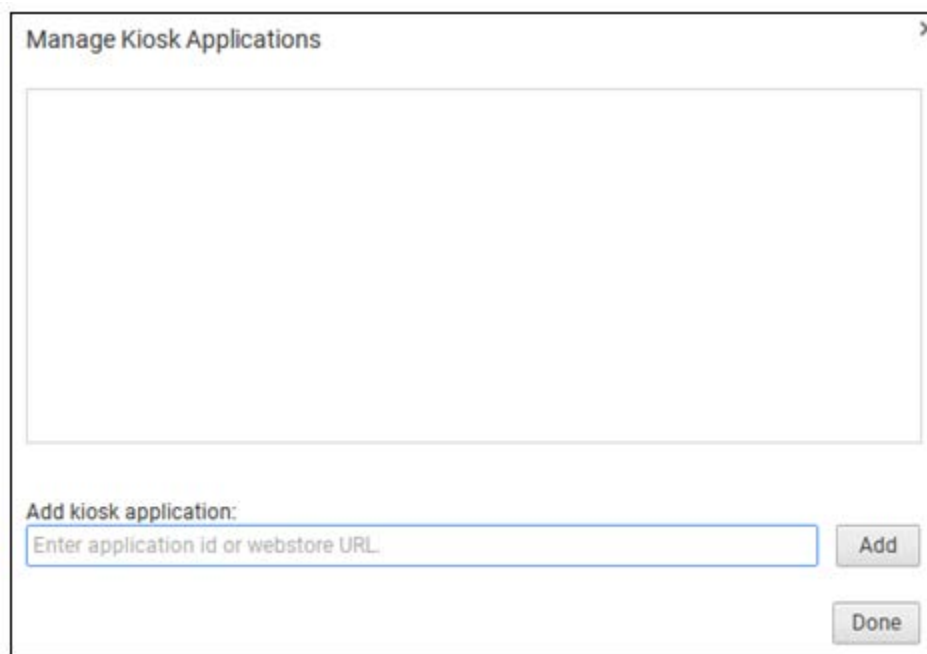


Figure 91. Manage Kiosk Applications screen

16. Take these steps in the *Manage Kiosk Applications* screen:
 - a. Enter the following into the *Add kiosk application* field:
hblfbmjdaalalhifaaajnnodlkiloengc
 - b. Select [**Add**]. The AIRSecureTest application appears in the Manage Kiosk Applications list.
 - c. Select [**Done**].
17. Select your 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 [**AIRSecureTest**]. The secure browser launches.
19. If you receive the following error message, then the secure browser is not configured to run in kiosk mode:

The AIRSecureTest application requires kiosk mode to be enabled.
You need to re-install 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 AIRSecureTest Kiosk App and Selecting the Assessment Program.](#)"

Installing the AIRSecureTest Kiosk App on Managed Chromebooks

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



Caution: AIRSecureTest is not compatible with public sessions.

1. Set up your 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 your Admin console using your Google Apps for Education account.
3. Select **[Device management]** (indicated in Figure 92).

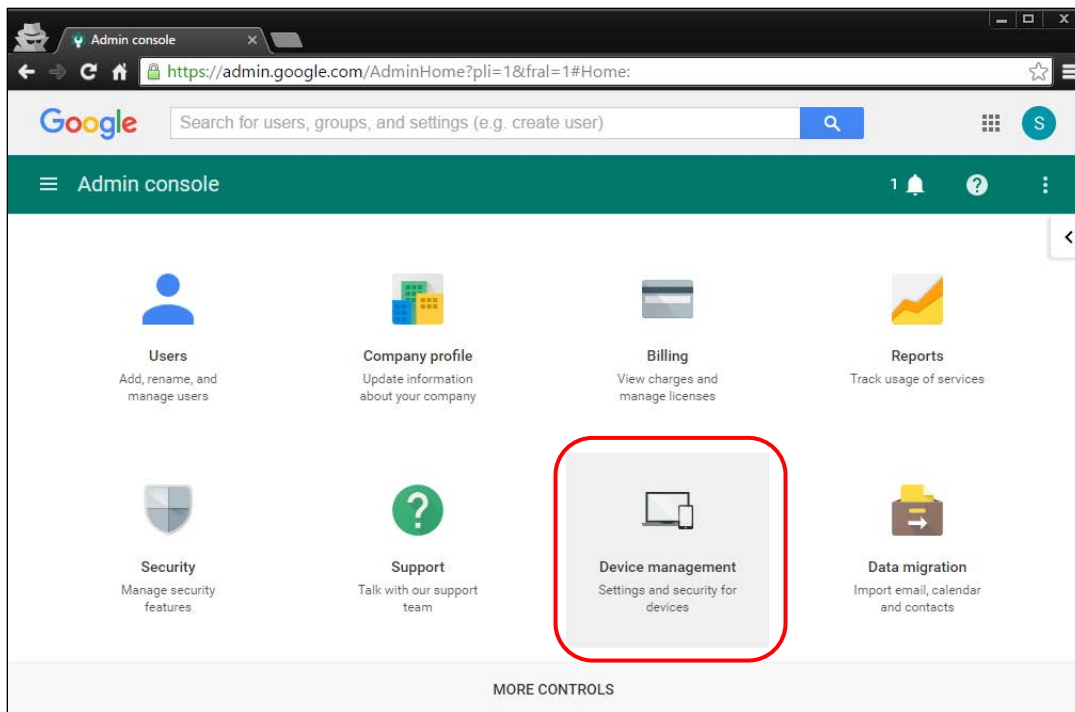


Figure 92. Chrome Admin console screen

Secure Browser Configuration | Installing the Secure Browser on Mobile Devices

4. When the *Device management* screen appears, select the [Chrome Management] link (indicated in Figure 93).

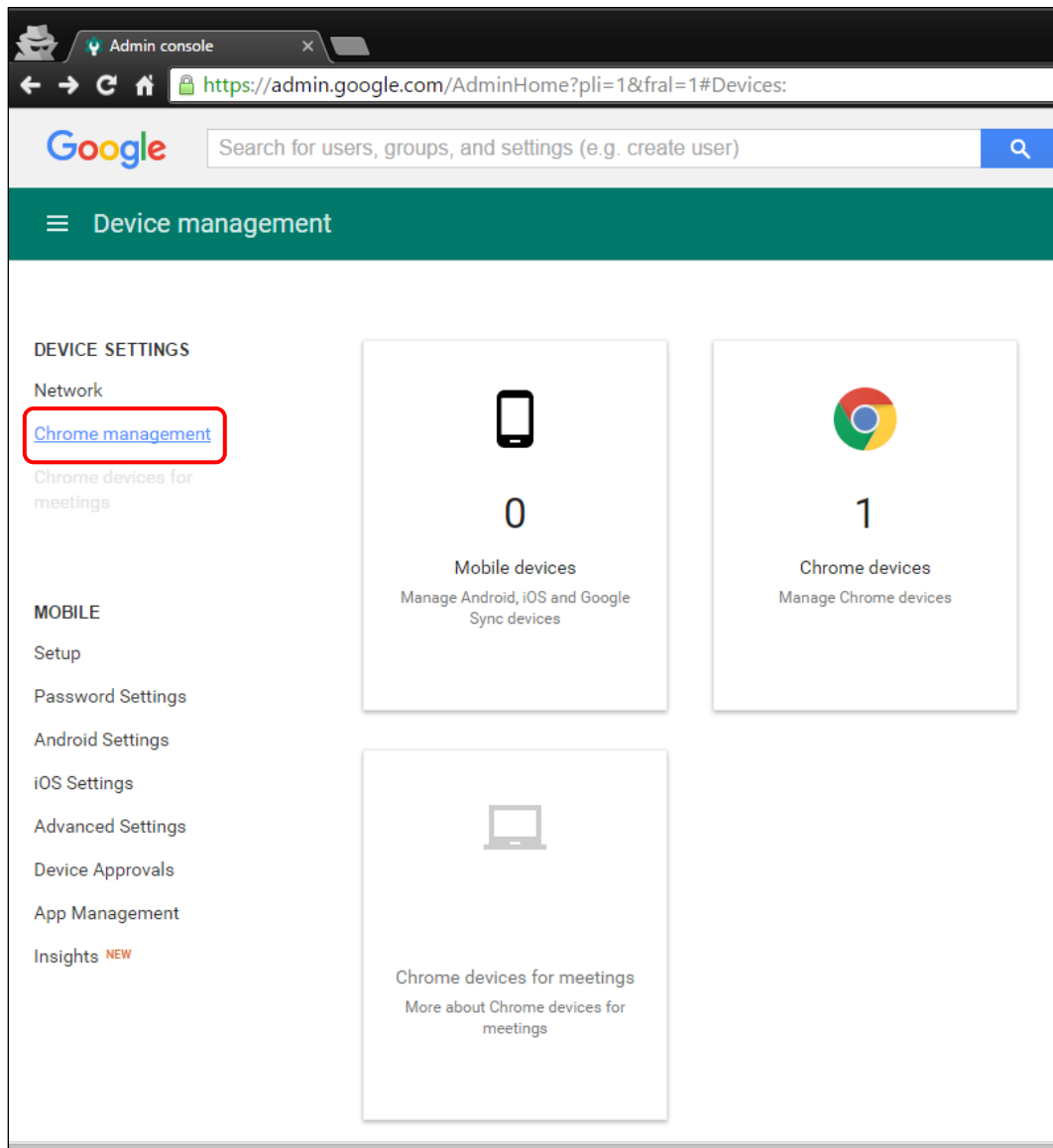


Figure 93. Chrome Device management screen

5. In the *Chrome Management* screen, select [**App Management**] (indicated in Figure 94).

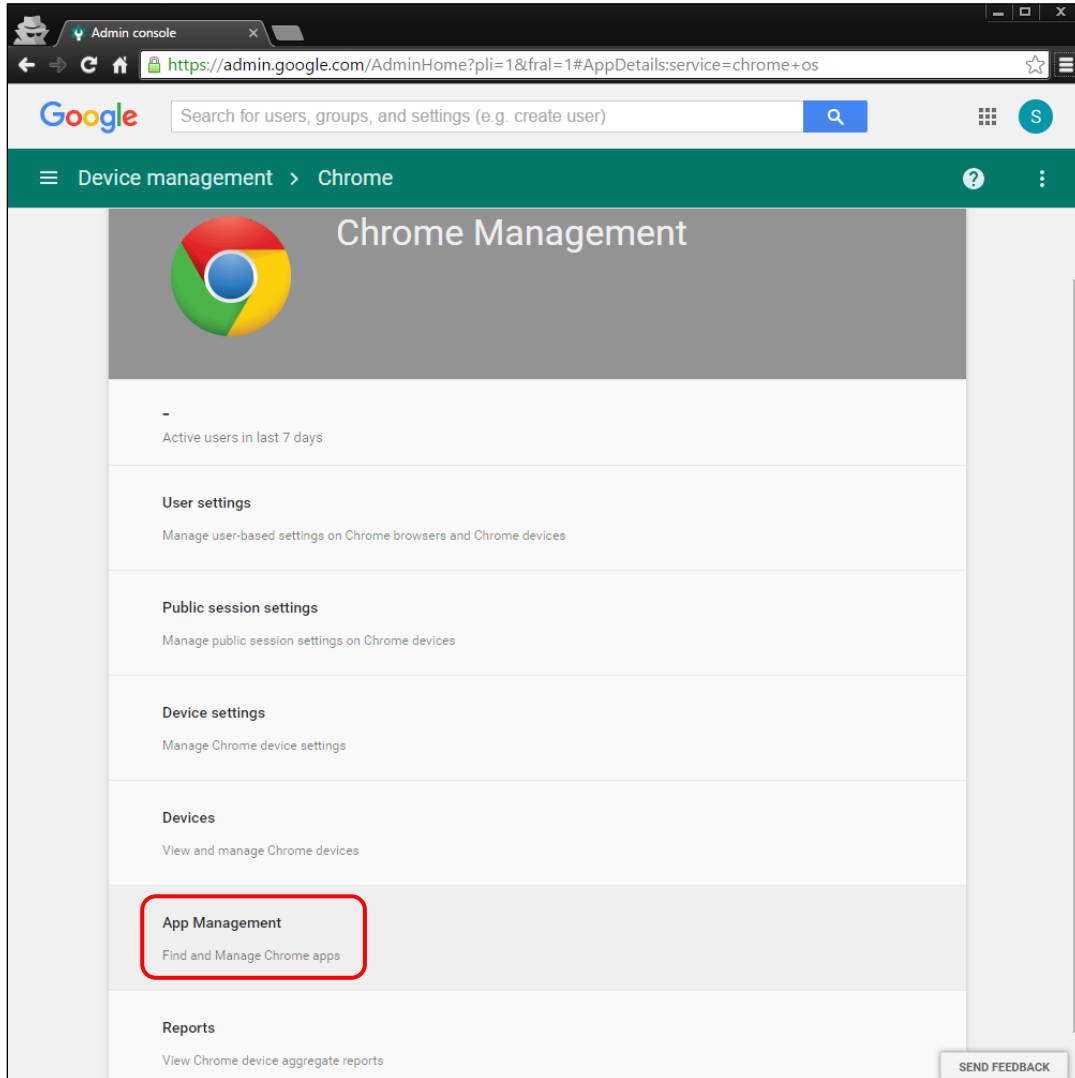


Figure 94. Chrome Management screen

6. In the left column of the *App Management* screen, enter AIRSecureTest or hblfbmjdaalalhi faa jnnodlkiloengc in the *Find or Update Apps* field (indicated in Figure 95).

Secure Browser Configuration | Installing the Secure Browser on Mobile Devices

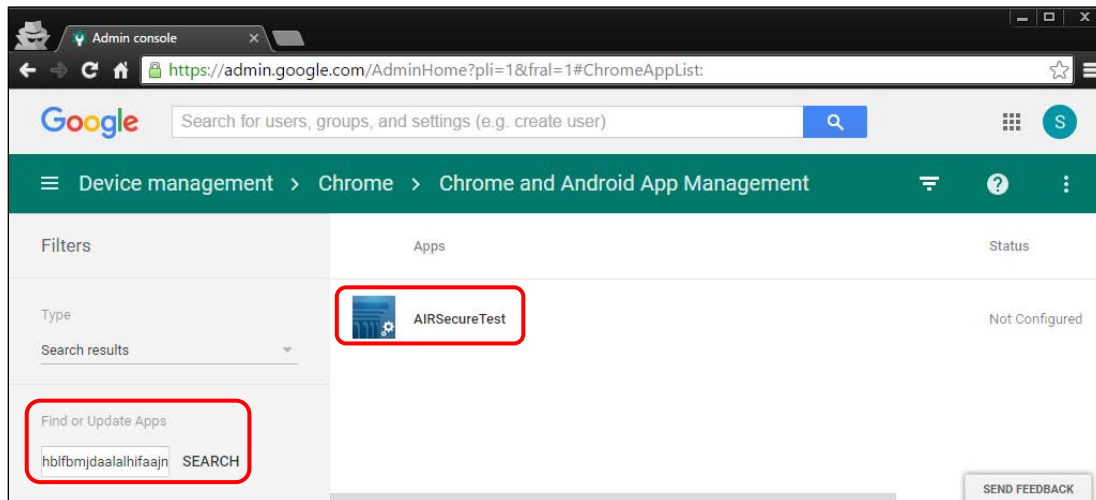


Figure 95. Chrome App Management screen

7. Select the [Kiosk settings | Deploy this app as a Kiosk App] link (indicated in Figure 96).

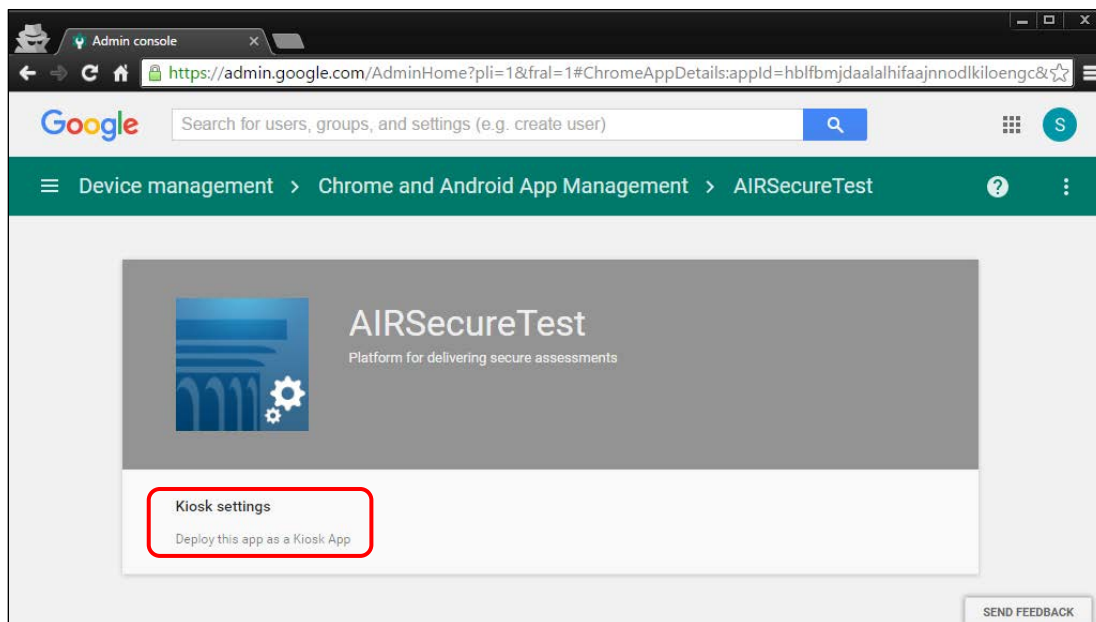


Figure 96. Select [Kiosk settings]

8. Select your organization in the *Org* column on the right (indicated in Figure 97).

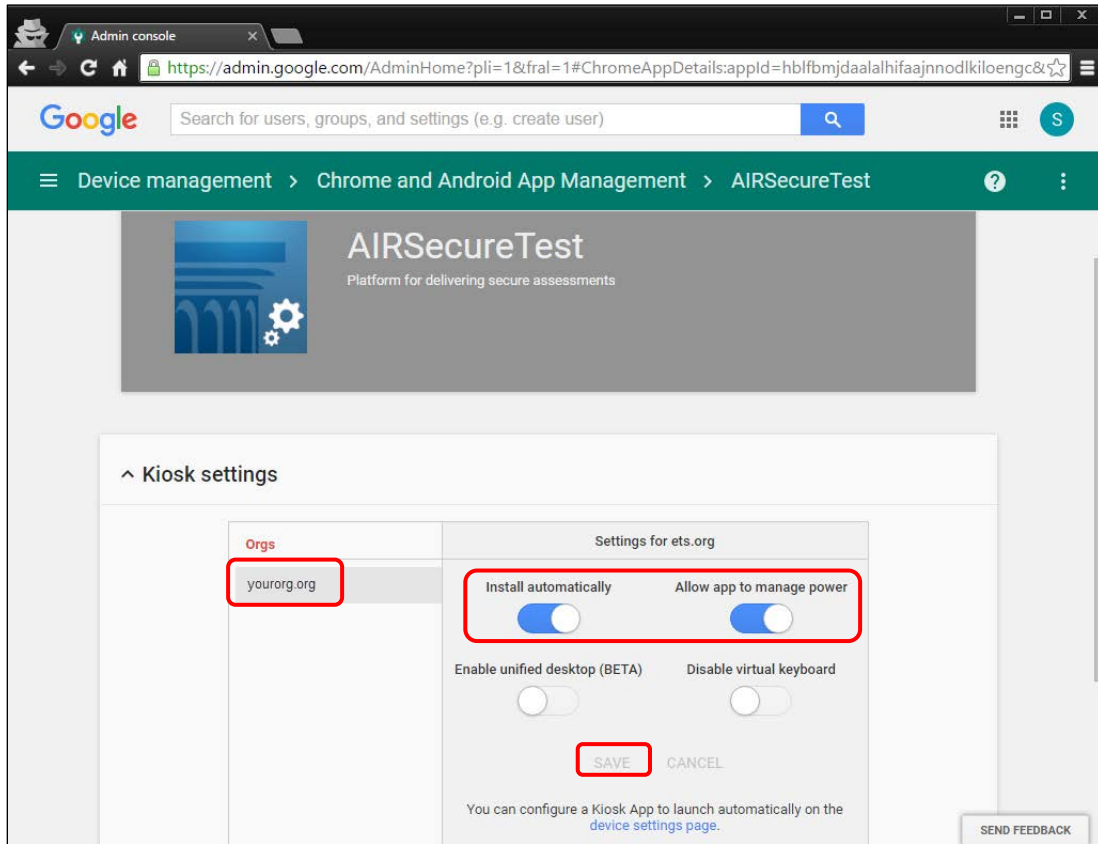


Figure 97. Chrome Kiosk settings screen

9. Make sure the sliders are set to the right to enable the *Install automatically* and *Allow app to manage power* settings and then select [**Save**] (indicated in Figure 97).



Notes:

- The AIRSecureTest application will now appear on all devices you have selected.
- This process may take up to 15 minutes.

10. To launch the secure browser, select the [Apps] link in the menu row of the Chromebook's logon screen and select the [**AIRSecureTest - Secure Browser**] app (indicated in Figure 98).

Secure Browser Configuration | Installing the Secure Browser on Mobile Devices

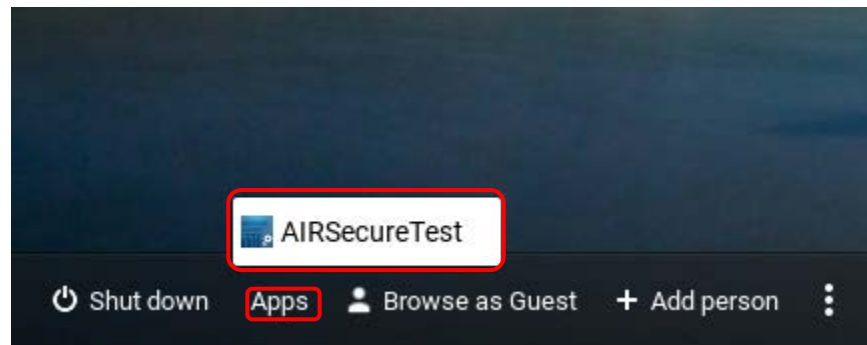


Figure 98. Chromebook logon screen

Opening the AIRSecureTest Kiosk App and Selecting the Assessment Program

The first time you open the AIRSecureTest kiosk app, a Launchpad appears. The Launchpad establishes the state and test administration for your students.

1. In the *Please Select Your State* drop-down list (indicated in Figure 99), select *California*.

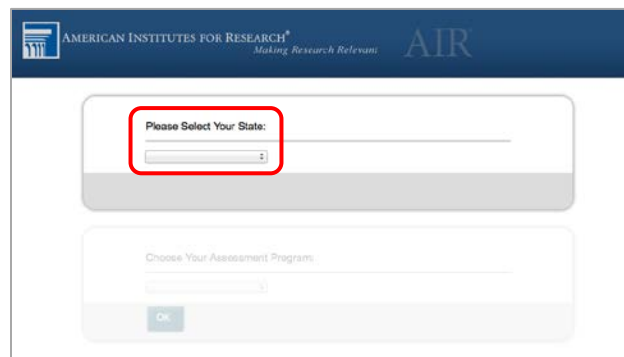


Figure 99. Select the state from the Launchpad

2. In the *Choose Your Assessment Program* drop-down list (indicated in Figure 100), the option *California Assessment of Student Performance and Progress* should already be selected.

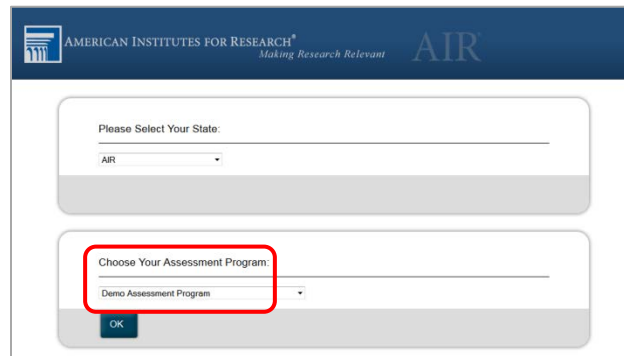


Figure 100. Select the assessment from the Launchpad

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 Windows Mobile Devices

The procedure for installing the secure browser on Windows mobile devices is the same for installing it on desktops. See 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 your 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 15 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 15 uses the domain `fake-url.com`. When configuring for a proxy server, use your actual testing domain names as listed in [Appendix B, URLs for Testing Systems](#).

Table 15. 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 10.9–10.14	<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:80 aHR0cHM6Ly9jYS50ZHMuYWlyYXN0Lm9yZy9 zdHVkZW50</code>
Set the proxy for HTTP requests only	Mac 10.9–10.14	<code>./CASecureBrowser -proxy 1:http:fake-url.com:80 aHR0cHM6Ly9jYS50ZHMuYWlyYXN0Lm9yZy9 zdHVkZW50</code>

Description	System	Command
Set the proxy for HTTP requests only	Linux	<code>./CASecureBrowser.sh -proxy 1:http:fake-url.com:80 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:80 aHR0cHM6Ly9jYS50ZHMuYWlyYXN0Lm9yZy9zdHVkZW50</code>
Set the proxy for all protocols to mimic the “Use this proxy server for all protocols” of Firefox	Mac 10.9–10.14	<code>./CASecureBrowser -proxy 1:*:fake-url.com:80 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:80 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 10.9–10.14	<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>
Auto detect proxy settings	Windows	<code>CASecureBrowser.exe -proxy 4 aHR0cHM6Ly9jYS50ZHMuYWlyYXN0Lm9yZy9zdHVkZW50</code>
Auto detect proxy settings	Mac 10.9–10.14	<code>./CASecureBrowser -proxy 4 aHR0cHM6Ly9jYS50ZHMuYWlyYXN0Lm9yZy9zdHVkZW50</code>

Secure Browser Configuration | Proxy Settings for Desktop Secure Browsers

Description	System	Command
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 10.9–10.14	<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. **If you have a /Program Files (x86) subdirectory:** Create a new desktop shortcut in Windows Explorer by navigating to your relevant 32-bit subdirectory, `C:\Program Files (x86)\`. Right-click the file `CASecureBrowser.exe` and then select *Send To → Desktop (create shortcut)*.
 - c. **If you do not have a /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.

- In the *Target* field, modify the command as specified in Table 15. For example:

```
"C:\Program Files  
(x86)\CAsecureBrowser\CAsecureBrowser.exe" -proxy 1:http:fake-  
url.com:80 aHR0cHM6Ly9jYS50ZHMuYWlyYXN0Lm9yZy9zdHVkZW50
```
- Select **[OK]**.

Modifying Desktop Shortcuts on Mac OS X

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

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

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

```
#!/bin/sh  
  
/Applications/CAsecureBrowser.app/Contents/MacOS/./  
CAsecureBrowser -proxy 1:http:fake-url.com:80 &  
aHR0cHM6Ly9jYS50ZHMuYWlyYXN0Lm9yZy9zdHVkZW50
```
- 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]**.
- Apply execute permission to the file. In Terminal, type

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

This page is left blank intentionally.

Appendices

Appendix A. Operating System Support Plan for the 2018–19 Test Delivery System

A supported operating system is one for which American Institutes for Research (AIR) provides updates to the secure browser for that operating system. AIR 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 AIR’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 16, the Supported Operating Systems table.

Timing of Secure Browser Updates

AIR will support major and minor version upgrades for Windows, Macintosh, Linux, iOS, Android, and Chrome OS upon the completion of internal testing following their release. AIR may provide secure browser updates for new major and minor version upgrades of Windows, Macintosh, Linux, iOS, Android, 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 is 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 Mac OS 10.9 to 10.10 is a minor version upgrade. For minor version upgrades to iOS, Android, or Chrome operating systems, AIR will provide mobile secure browser updates to ensure compatibility.

Support Plan for Operating Systems

Table 16 through Table 21 list the operating systems and the anticipated end-of-support dates. The shaded cells in Table 16 and Table 18 indicate that AIR ends support for operating systems after the 2018–19 school year.

Table 16. Supported Operating Systems—Windows

Supported Operating System	Release Date	Anticipated End-of-Support Date
7 SP1 (Professional and Enterprise)	Oct. 2009	End of 2019–20 school year
8 (Professional and Enterprise)	Oct. 2012	End of 2021–22 school year
8.1 (Professional and Enterprise)	Oct. 2013	End of 2022–23 school year
10, 10 in S mode (Educational, Professional, and Enterprise) (Versions 1507–1803 and 1809 upon acceptance)	July 2015	End of 2024–25 school year
Server 2008 R2	Oct. 2009	End of 2019–20 school year
Server 2012 R2	Oct. 2013	End of 2022–23 School Year
Server 2016 R2	Oct. 2016	End of 2025–26 school year



Notes:

- AIR’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 or Apple ends support for an operating system sooner than six years after its release, then AIR will stop supporting that system after one full school year.

Table 17. Supported Operating Systems—Mac OS X (Intel)

Supported Operating System	Release Date	Anticipated End-of-Support Date
10.9	Oct. 2013	End of 2019–20 school year
10.10	Oct. 2014	End of 2020–21 school year
10.11	Sept. 2015	End of 2021–22 school year
10.12	Sept. 2016	End of 2022–23 school year
10.13	Sept. 2017	End of 2023–24 school year
10.14	Pending acceptance	End of 2024–25 school year



Notes: Mac OS X computers with PowerPC processors are not supported.

- Apple does not document end-of-life status for its products. AIR recommends using the most recent releases.
- AIR support for a given version of OS X ends 10 school years after its release date.
- If Microsoft or Apple ends support for an operating system sooner than six years after its release, then AIR will stop supporting that system after one full school year.

Table 18. Supported Operating Systems—Linux

Supported Operating System	Release Date	Anticipated End-of-Support Date
Fedora 27 LTS (Gnome)	Nov. 2017	End of 2019–20 school year
Fedora 28 (LTS Gnome)	May 2018	End of 2020–21 school year
Ubuntu 14.04 LTS (Gnome)	April 2014	End of 2018–19 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



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, AIR will end support at the end of a full school year after the official distributor’s announced end-of-life support date.

Table 19. Supported Operating Systems—iOS

Supported Operating System	Release Date	Anticipated End-of-Support Date
10.3	Sept. 2014	Apple iOS operating systems are released on a rolling basis. AIR supports the three most recent major releases of iOS.
11.4	Jan. 2016	Apple iOS operating systems are released on a rolling basis. AIR supports the three most recent major releases of iOS.
12	Pending acceptance	Apple iOS operating systems are released on a rolling basis. AIR supports the three most recent major releases of iOS.



Note: Supported iPads are as follows:

- 4th Generation (retina display)
- 5th Generation (retina display)
- 6th Generation (retina display)
- iPad Air
- iPad Air 2
- iPad Pro

Table 20. Supported Operating Systems—Android

Supported Operating System	Release Date	Anticipated End-of-Support Date
7.1	Aug. 2016; rolling	Android operating systems are released on a rolling basis. AIR supports the three most recent minor releases of Android.
8.1	Aug. 2016; rolling	Android operating systems are released on a rolling basis. AIR supports the three most recent minor releases of Android.
9	Aug. 2016; rolling (Pending acceptance)	Android operating systems are released on a rolling basis. AIR supports the three most recent minor releases of Android.



Notes:

- Android 7.0 has been released but is not yet formally supported, pending its inclusion in the Google for Education program.
- Supported tablets are the Lenovo Yoga Tab 3 10; Samsung Galaxy Tab S3; and Asus ZenPad Z10.

Table 21. Supported Operating Systems—Chrome OS

Supported Operating System	Release Date	Anticipated End-of-Support Date
67 and above	June 2018; rolling	For any given school year, AIR supports the version of Chrome OS available during the summer months and all subsequent versions. For example, if Chrome OS version 67 is released in July, it and all versions of Chrome after it will be supported until July of the following year.



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

Appendix B. URLs for Testing Systems

This appendix presents information about the URLs for California Assessment of Student Performance and Progress (CAASPP) testing. Ensure your network’s firewalls are open for these URLs.

URLs for Nontesting Sites

Table 22 lists URLs for nontesting sites, such as the Test Information Distribution Engine (TIDE), Online Reporting System (ORS), and Learning Point Navigator.



Note: The Single Sign On System, which allows users to access using one username and password, provides access to the following systems (although the type of access is determined by the user role):

- Test Operations Management System (TOMS)
- ORS
- Test Administrator Interface
- TIDE (used to file appeals)
- Interim Assessment Hand Scoring System (for interim assessments)

Table 22. URLs for Nontesting Sites

Destination	URL
CAASPP Portal	http://www.caaspp.org/
Secure browser installation files	http://ca.browsers.airast.org/
TOMS	https://caaspp.ets.org/
Single Sign-On System	(The full URL varies by system such as TOMS or the Test Administrator Interface.)
SurveyGizmo (This website hosts CAASPP forms and surveys.)	http://www.sgizmo.com http://www.surveygizmo.com http://www.surveygizmo.eu

URLs for Testing Sites

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

Test Administrator 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, you are strongly encouraged to whitelist at the root level. This requires using a wildcard. URLs for testing websites are listed in Table 23.

Table 23. URLs for Testing Websites

Systems	URLs
<ul style="list-style-type: none"> • Test Administrator and Student Testing Sites • Assessment Viewing Application 	*.airast.org *.tds.airast.org *.cloud1.tds.airast.org *.cloud2.tds.airast.org
<ul style="list-style-type: none"> • Certificate revocation list 	http://crl.verisign.com/

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 24 also should be whitelisted to ensure that students can use them during testing.

Table 24. 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	Estimated Time to Complete	Target Completion Date	Reference
<input type="checkbox"/>	Verify that all of your school's devices that will be used for online testing meet the operating system requirements.	5–10 hours	3–4 weeks before testing begins in your school	Chapter 1, System Requirements
<input type="checkbox"/>	Verify that your school's network and internet are properly configured for testing, conduct network diagnostics, and resolve any issues.	5–10 hours	3–4 weeks before testing begins in your school	Chapter 2, Network Configuration
<input type="checkbox"/>	Confirm that URLs for testing sites and the online dictionary and thesaurus have been whitelisted on your server.	30 minutes	3–4 weeks before testing begins in your school	Appendix B, URLs for Testing Systems
<input type="checkbox"/>	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.	5–10 hours	3–4 weeks before testing begins in your school	Turn Off Background Jobs
<input type="checkbox"/>	Install the secure browser on all devices that will be used for testing.	5–10 hours	3–4 weeks before testing begins in your school	Chapter 4, Secure Browser Configuration
<input type="checkbox"/>	Review software requirements for each operating system.	5–10 hours	1–2 weeks before testing begins in your school	Chapter 3, Software Configuration

Secure Browser Configuration | Proxy Settings for Desktop Secure Browsers

	Activity	Estimated Time to Complete	Target Completion Date	Reference
<input type="checkbox"/>	Enable pop-up windows on student devices.	5–10 hours	1–2 weeks before testing begins in your school	Enabling Pop-Up Windows
<input type="checkbox"/>	On Windows devices, disable Fast User Switching. If a student can access multiple user accounts on a single device, you are encouraged to disable the Fast User Switching function.	5–10 hours	1–2 weeks before testing begins in your school	Disabling Fast User Switching in Windows
<input type="checkbox"/>	On Mac devices , disable Spaces or Exposé in Mission Control.	5–10 hours	1–2 weeks before testing begins in your school	Disabling Exposé or Spaces
<input type="checkbox"/>	On iPads , ensure that Automatic Assessment Configuration is enabled.	5–10 hours	1–2 weeks before testing begins in your school	Using Automatic Assessment Configuration
<input type="checkbox"/>	On iOS devices, ensure that features that might pose a security risk are disabled.	5–10 hours	1–2 weeks before testing begins in your school	Configuring Apple Mobile Devices for Online Testing with the Secure Browser
<input type="checkbox"/>	On Android tablets, ensure that the secure browser keyboard is enabled.	5–10 hours	1–2 weeks before testing begins in your school	Configuring Android for Online Testing with the Secure Browser

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 your network setup. Technology coordinators may want to work with the California Assessment of Student Performance and Progress test site coordinator to adapt this worksheet as necessary so your 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 of students who need to take the test:	[]
Number of test administrators who need a device:	[]
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 in as well as the average estimated time to complete the test.	[]
Number of hours that must be scheduled to administer the test: (students + test administrators) × hours ÷ devices =	[]

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: 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

Additional Resources:

- Microsoft IT Pro Center | Create a Group Policy Object (Windows 10, Windows Server 2016) web page—<https://docs.microsoft.com/en-us/windows/security/identity-protection/windows-firewall/create-a-group-policy-object>
- Microsoft IT Pro Center | 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 101, appears.

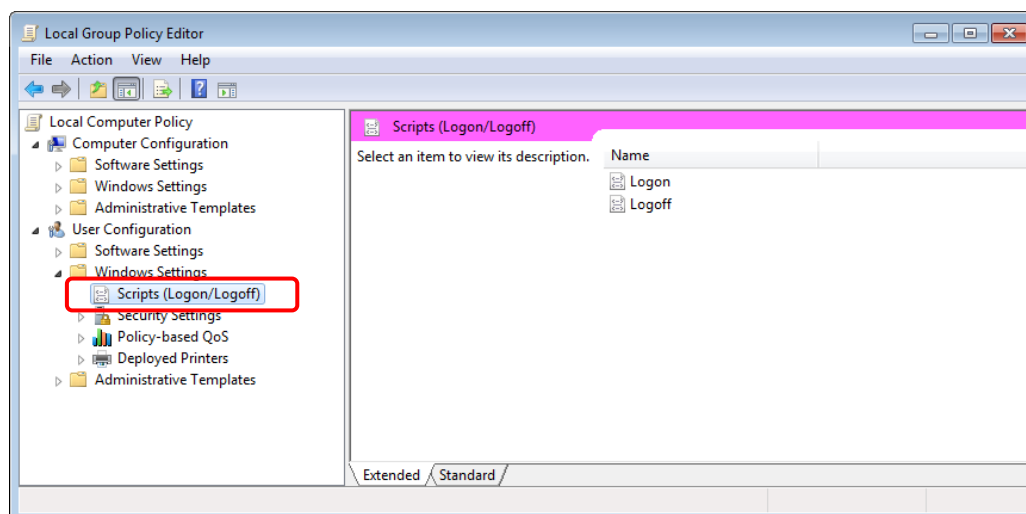


Figure 101. The *Local Group Policy Editor* window

2. Expand *Local Computer Policy* → *User Configuration* → *Windows Settings* → *Scripts (Logon/Logoff)* (indicated in Figure 101).
3. Select [**Logon**] and then select [**Properties**]. The *Logon Properties* dialog box appears.

4. Select [**Add**] (indicated in Figure 102). The *Add a Script* dialog box appears.

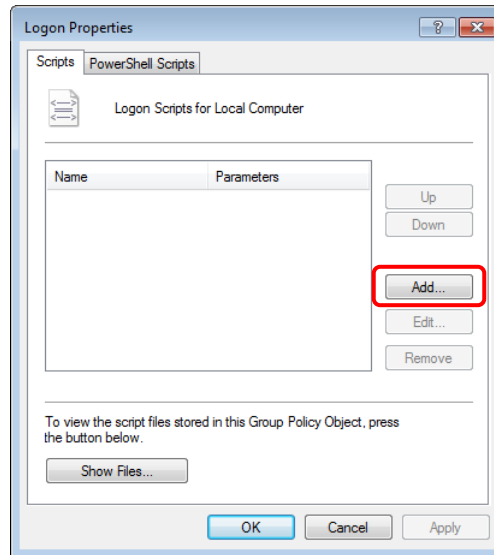


Figure 102. The *Logon Properties* dialog box

5. Select [**Browse...**] (indicated in Figure 103) and navigate to the `logon.bat` you want to run.

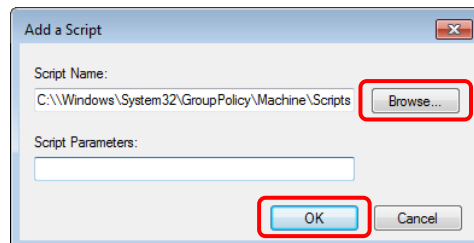


Figure 103. The *Add a Script* dialog box

6. Select [**OK**] (also indicated in Figure 103) 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

If you have been advised by the California Technical Assistance Center to reset the secure browser profile, use the instructions in this appendix.

Resetting Secure Browser Profiles on Windows

1. Log on as 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\AIR\
C:\Users\username\AppData\Roaming\AIR\
where username is the Windows user account where the secure browser is installed.
(Keep the AIR\ directories; just delete their contents.)`
3. Start the secure browser.

Resetting Secure Browser Profiles on OS X 10.9 or Later

1. Log on as 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 104).

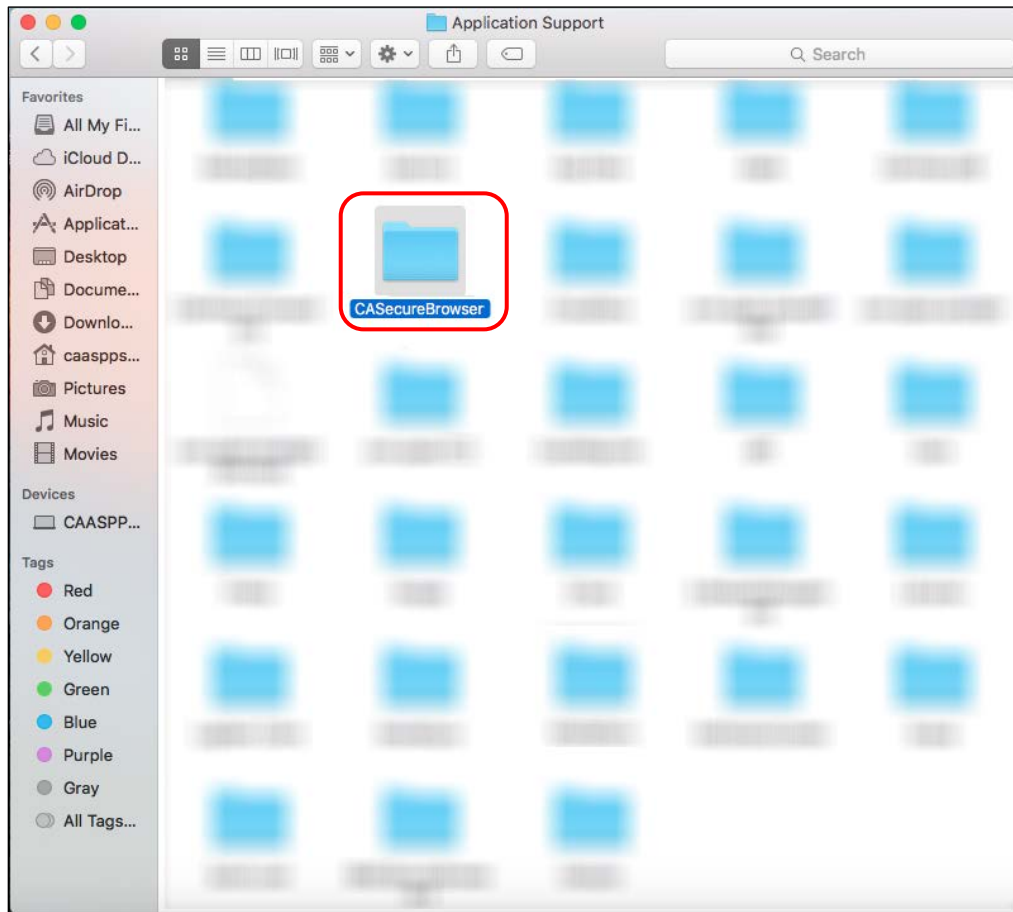


Figure 104. Resetting the secure browser on OS X 10.9 or later

4. Open the Application Support 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 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/.air  
/home/username/.cache/air
```

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) coordinators should first contact your LEA technology coordinator or system administrator prior to contacting the California Technical Assistance Center (CaITAC).

Technology coordinators and CAASPP test site coordinators should contact their LEA CAASPP coordinators for assistance.

California Technical Assistance Center for LEA CAASPP Coordinators

If you must contact CaITAC, you will be asked to provide as much detail as possible about the issue(s) you encountered.

CaITAC

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

Toll-Free Phone Support: 800-955-2954

Email Support: caltac@ets.org

Website: <http://www.caaspp.org/>

Always include the following information:

- Test administrator or test examiner name and information technology/network contact person and contact information
- Statewide Student Identifier(s) of affected students
- Results 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 your 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]